EXAMTOPICS

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



CERTIFICATION TEST

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

Question #1 *Topic 1*

Phishing belongs which of the following MITRE ATT&CK tactics?

A. Initial Access, Persistence

B. Persistence, Command and Control

C. Reconnaissance, Persistence

D. Reconnaissance, Initial Access

Suggested Answer: *D*
Official Answer: D

pkevinkou Most Recent 3 years, 1 month ago

Selected Answer: D

D, Correct

upvoted 1 times

Question #2 *Topic 1*

When creating a BIOC rule, which XQL query can be used?

A. dataset = xdr_data | filter event_sub_type = PROCESS_START and action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

B. dataset = xdr_data | filter event_type = PROCESS and event_sub_type = PROCESS_START and action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

C. dataset = xdr_data | filter action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe" | fields action_process_image

D. dataset = xdr_data | filter event_behavior = true event_sub_type = PROCESS_START and action_process_image_name ~= ".*?\.(?:pdf|docx)\.exe"

Suggested Answer: *B*
Official Answer: B

nobody165456131354 Most Recent 2 years, 7 months ago

Selected Answer: B

Correct answer is: B A: missing event_type C: wrong action_process_image D: wrong event_behaviour

upvoted 1 times

9smiles 3 years, 2 months ago

Correct answer is: B

"The XQL query must at a minimum filter on the event_type field in order for it to be a valid BIOC rule."

upvoted 1 times

Question #3 *Topic 1*

Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

A. Security Manager Dashboard

B. Data Ingestion Dashboard

C. Security Admin Dashboard

D. Incident Management Dashboard

Suggested Answer: *C*
Official Answer: C

danups Most Recent 1 year, 11 months ago

Selected Answer: C

A is wrong due to the Security Manager report provides a mix of incident related widgets and a breakdown of agent statuses and versions.

C is about incidents only, including their MTTR.

upvoted 1 times

Mmalacan 2 years ago

Selected Answer: C

the correct answer is c, the security admin dashboard show the MTTR

upvoted 1 times

Chiquitabandita 2 years, 5 months ago

Selected Answer: C

per the admin guide

upvoted 1 times

XuannnnOAO 2 years, 10 months ago

A is wrong. C is correct answer

upvoted 2 times

unns12 2 years, 10 months ago

A is wrong. C is correct answer

upvoted 2 times

cneru1 3 years, 2 months ago

C is the Correct answers. It is on the Security Admin dashboard - upper right hand side

upvoted 1 times

Indy_k 3 years, 5 months ago

C is the right answer. Mean Time to Resolution (MTTR) metric are inside Security Admin Dashboard

upvoted 1 times

Question #4 *Topic 1*

What are two purposes of “Respond to Malicious Causality Chains” in a Cortex XDR Windows Malware profile? (Choose two.)

A. Automatically close the connections involved in malicious traffic.

B. Automatically kill the processes involved in malicious activity.

C. Automatically terminate the threads involved in malicious activity.

D. Automatically block the IP addresses involved in malicious traffic.

Suggested Answer: *A, D*
Official Answer: AD

kadirerol Most Recent 1 year, 10 months ago
ın depend of below document I selected answer AD.
upvoted 1 times

news088 2 years, 9 months ago
selected answer AD https://live.paloaltonetworks.com/t5/community-blogs/cortex-xdr-agent-7-3-new-features/ba-p/383329
upvoted 2 times

sharkk43 2 years, 9 months ago
Selected Answer: AD
I say it's A and D because of what I'm just reading off the official course in the section "Respond to Malicious Causality Chains". It goes like this: "When the Cortex XDR agent detects a malicious activity, the Respond to Malicious Causality Chains module inspects the network connections opened by the processes involved in the attack to identify malicious IP addresses." To me that's A nd D not A and C.
upvoted 3 times

sharkk43 2 years, 9 months ago
Forgot to add the second part: "If such network connections are found, this protection module can automatically close all the network connections and block new connection requests from these IP addresses."
upvoted 3 times

XuannnnOAO 2 years, 10 months ago
CD is correct
upvoted 1 times

unns12 2 years, 10 months ago
CD is correct
upvoted 2 times

Karreldanam 3 years, 2 months ago
Selected Answer: AD
(Windows only) Respond to Malicious Causality Chains.

When the Cortex XDR agent identifies a remote network connection that attempts to perform malicious activity—such as encrypting endpoint files—the agent can automatically block the IP address to close all existing communication and block new connections from this IP address to the endpoint. When Cortex XDRblocks an IP address per endpoint, that address remains blocked throughout all agent profiles and policies, including any host-firewall policy rules. You can view the list of all blocked IP addresses per endpoint from the Action Center, as well as unblock them to re-enable communication as appropriate.
upvoted 3 times

Question #5 *Topic 1*

When creating a custom XQL query in a dashboard, how would a user save that XQL query to the Widget Library?

A. Click the three dots on the widget and then choose “Save” and this will link the query to the Widget Library.

B. This isn’t supported, you have to exit the dashboard and go into the Widget Library first to create it.

C. Click on “Save to Action Center” in the dashboard and you will be prompted to give the query a name and description.

D. Click on “Save to Widget Library” in the dashboard and you will be prompted to give the query a name and description.

Suggested Answer: *D*
Official Answer: D

Chiquitabandita Most Recent 2 years, 5 months ago

Selected Answer: D

Select Save to Widget Library to pivot to the Widget Library and generate a custom widget based on the query results. from admin guide pg. 212

upvoted 1 times

unns12 2 years, 10 months ago

D - SAVE AS WITH 2 choices only 'QUERY library' or 'widget to library'

upvoted 1 times

cneru1 3 years, 2 months ago

its actually "save as" then 4 choices - BIOC Rule - Correlation Rule - Query to Library- Widget to Library.

upvoted 1 times

Question #6 *Topic 1*

What license would be required for ingesting external logs from various vendors?

A. Cortex XDR Pro per Endpoint

B. Cortex XDR Vendor Agnostic Pro

C. Cortex XDR Pro per TB

D. Cortex XDR Cloud per Host

Suggested Answer: *C*
Official Answer: C

danups 1 year, 11 months ago

Selected Answer: B

Cortex XDR Vendor Agnostic Pro: This license is designed to handle logs from various vendors, suggesting that it supports ingestion of diverse external logs.

Cortex XDR Pro per TB: This license is based on the volume of data (per terabyte), which is suitable for high volumes of log data but may not specifically address the vendor-agnostic nature.

If the key factor is the volume of data rather than the specific sources of the logs, Cortex XDR Pro per TB would indeed be a better choice, but the question is clear: "for ingesting external logs from VARIOUS VENDORS".

I will go for "B" on this.

upvoted 1 times

danups Most Recent 1 year, 11 months ago

NVM. Changing my answer to "C". Sorry for the confusion.

upvoted 1 times

Chiquitabandita 2 years, 5 months ago

Selected Answer: C

LICENSE TYPE: Ingesting Logs and Data from external sources requires a Cortex XDR Pro per GB license. To receive Syslog data from an external source, you must fi rst set up the Syslog Collector applet on a Broker VM within your network.

upvoted 1 times

9smiles 2 years, 11 months ago

From CXPAG: Ingesting logs and data requires a Cortex XDR Pro per GB license.

They have now changed the name of the license to "Pro per GB license" instead of TB.

upvoted 2 times

Question #7 *Topic 1*

An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

A. DDL Security

B. Hot Patch Protection

C. Kernel Integrity Monitor (KIM)

D. Dylib Hijacking

Suggested Answer: *D*
Official Answer: D

Chiquitabandita Most Recent 2 years, 5 months ago

Selected Answer: D

Mac operating systems" from admin guide pg. 85

upvoted 2 times

Karreldanam 3 years, 2 months ago

Selected Answer: D

Dylib Hijacking

Prevents Dylib-hijacking attacks where the attacker attempts to load dynamic libraries on Mac operating systems from unsecured locations to gain control of a process.

upvoted 4 times

Question #8 *Topic 1*

What is the purpose of the Unit 42 team?

A. Unit 42 is responsible for automation and orchestration of products

B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

C. Unit 42 is responsible for threat research, malware analysis and threat hunting

D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Suggested Answer: *C*
Official Answer: C

danups Most Recent 1 year, 11 months ago

Selected Answer: C

C - absolutely

upvoted 1 times

9smiles 2 years, 11 months ago

Correct answer is C

upvoted 1 times

Question #9 *Topic 1*

Which Type of IOC can you define in Cortex XDR?

A. destination port

B. e-mail address

C. full path

D. App-ID

Suggested Answer: *C*
Official Answer: C

Chiquitabandita Most Recent 2 years, 5 months ago

Selected Answer: C

ii. TYPE indicates the type of indicators, such as Full Path, File Name, Domain, and Hash.

upvoted 3 times

Karreldanam 3 years, 2 months ago

Selected Answer: C

5.1.1 Explain the purpose and use of the IOC technique Indicators of compromise (IOCs) are the artifacts that are considered malicious or suspicious. IOCs are static and based on criteria such as: ● Full path ● File name ● Domain ● Destination IP address ● MD5 hash ● SHA-256

upvoted 3 times

Question #10 *Topic 1*

When viewing the incident directly, what is the “assigned to” field value of a new Incident that was just reported to Cortex?

A. Pending

B. It is blank

C. Unassigned

D. New

Suggested Answer: *C*
Official Answer: C

cneru1 Highly Voted 3 years, 1 month ago
from Admin Guide: Assigned To: The user to which the incident is assigned. The assignee tracks which analyst is responsible for investigating the threat. Incidents that have not been assigned have a status of Unassigned. https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Incidents
upvoted 5 times

tobaja Most Recent 2 years, 3 months ago
Selected Answer: C
C. Unassigned
upvoted 1 times

Chiquitabandita 2 years, 5 months ago
Selected Answer: C
in the admin guide pg. 230
upvoted 1 times

nobody165456131354 2 years, 5 months ago
Selected Answer: C
Unassigned
upvoted 1 times

jose010696 2 years, 7 months ago
Selected Answer: C
C. is the right answer.
upvoted 2 times

darylmaeb24 2 years, 9 months ago
C. Unassigned
upvoted 1 times

Indy_k 3 years, 5 months ago
C is the right answer. It's the status field that will be set to New. The assigned to field will be set to Unassigned
upvoted 4 times

Question #11 *Topic 1*

In incident-related widgets, how would you filter the display to only show incidents that were “starred”?

A. Create a custom XQL widget

B. This is not currently supported

C. Create a custom report and filter on starred incidents

D. Click the star in the widget

Suggested Answer: *D*
Official Answer: D

kadirerol Most Recent 2 years, 1 month ago

Selected Answer: D

d is correcrt answer

upvoted 2 times

Chiquitabandita 2 years, 5 months ago

Selected Answer: D

pg. 675 in guide

upvoted 1 times

9smiles 2 years, 11 months ago

Selected Answer: D

D is correct. Tried this

upvoted 4 times

Question #12 *Topic 1*

Where would you view the WildFire report in an incident?

A. next to relevant Key Artifacts in the incidents details page

B. under Response --> Action Center

C. under the gear icon --> Agent Audit Logs

D. on the HUB page at apps.paloaltonetworks.com

Suggested Answer: *A*
Official Answer: A

Davina07 Highly Voted 3 years, 2 months ago

Selected Answer: A

I vote A

upvoted 6 times

cneru1 Highly Voted 3 years, 2 months ago

It is definitely A

upvoted 5 times

Navo27 Most Recent 2 years, 3 months ago

Selected Answer: A

If you are analyzing an incident, right-click the incident and View Incident. From the Key Artifacts involved in the incident, select the file for which you want to view the WildFire report and open (WF-report-icon.png). Alternatively, if you are analyzing an alert, right-click the alert and Analyze. You can open (WF-report-icon.png) the WildFire report of any file included in the alert Causality Chain.

upvoted 1 times

Bsharif 2 years, 4 months ago

The option A is correct answer. Watch the video "Cyber Expert: How to Investigate & Solve a Cyber Attack | Cortex XDR" (https://www.youtube.com/watch?v=P3AnLBcHZ4o&list=PLBpoVs10QWXJKYqv3ss7ZNdbSUzvKZJh6&index=2)- Time line 2:24/4:46

upvoted 1 times

Zubair2131 2 years, 5 months ago

A is the Correct Answer

upvoted 1 times

Chiquitabandita 2 years, 5 months ago

Selected Answer: A

"The WildFire verdict displays next to relevant Key Artifacts in the incidents details page, the causality view, and within the Live Terminal view of processes."

From the cortex xdr admin guide

upvoted 1 times

jose010696 2 years, 8 months ago

Selected Answer: A

that,s ok.

upvoted 1 times

darylmaeb24 2 years, 9 months ago

This should be letter A

upvoted 2 times

sharkk43 2 years, 9 months ago

Yeah, it's A

upvoted 2 times

unns12 2 years, 10 months ago

A - open incident and check

upvoted 2 times

im2ca 3 years ago

Correct Answer is A

upvoted 3 times

escar 3 years, 3 months ago

the question is about wf report in the incident Should be A

upvoted 4 times

examlog 3 years, 4 months ago

D. on the HUB page at apps.paloaltonetworks.com Correct Answer

upvoted 1 times

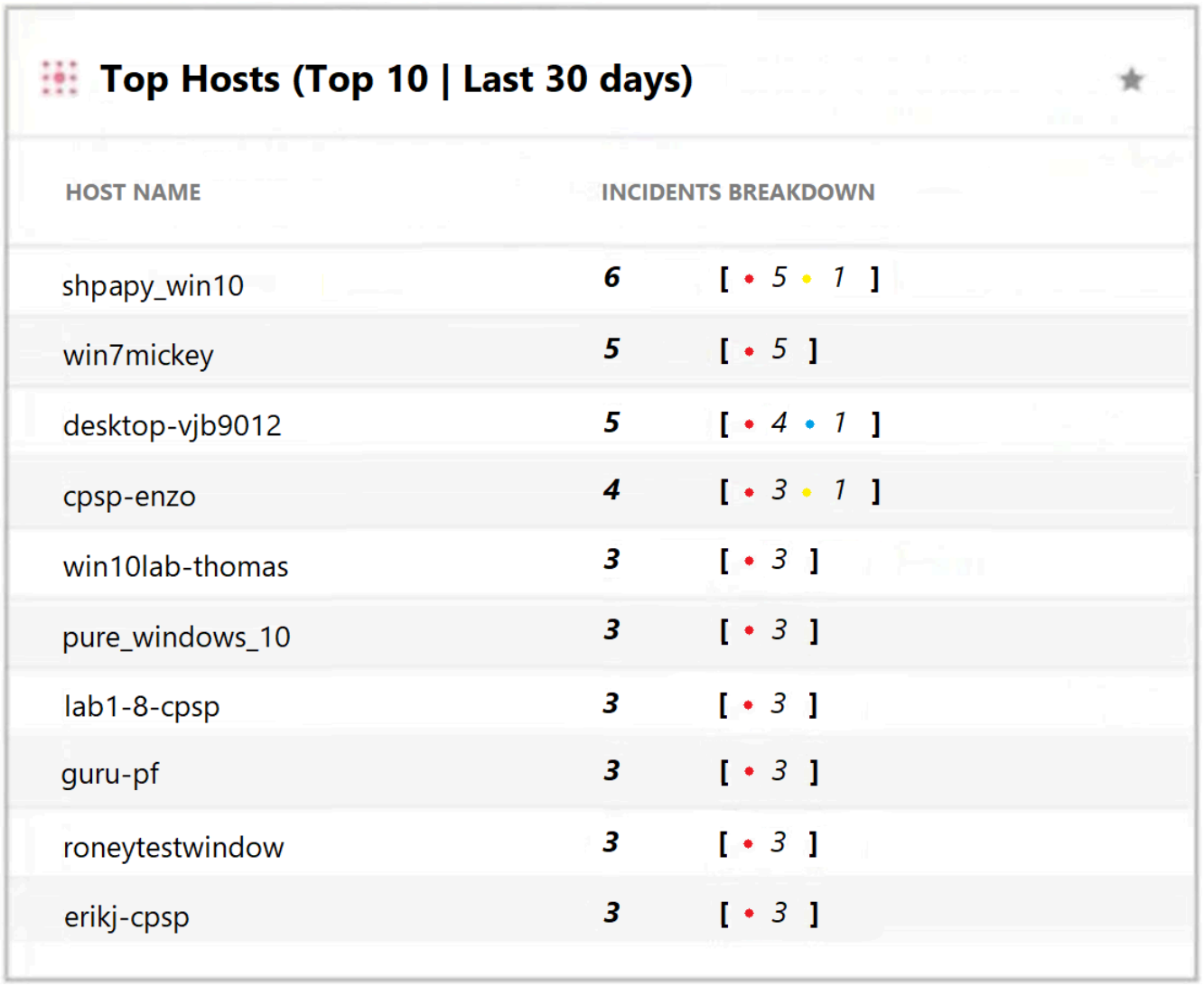
Indy_k 3 years, 5 months ago

A seem to be the correct answer.

upvoted 4 times

Question #13 *Topic 1*

What does the following output tell us?



A. There is one low severity incident.

B. Host shpapy_win10 had the most vulnerabilities.

C. There is one informational severity alert.

D. This is an actual output of the Top 10 hosts with the most malware.

Suggested Answer: *A*
Official Answer: A

9smiles Highly Voted 2 years, 11 months ago

Selected Answer: A

Answer should be A. The blue color codes for low severity incidents.

upvoted 7 times

Bsharif Most Recent 2 years, 4 months ago

D is wrong, cause it is about MALWARE and not INCIDENT. While the question is showing the Top 10 hosts with INCIDENTS. Ref.: Ref.: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Dashboard-Widgets See under TOP HOSTS in the table.

upvoted 1 times

Conkerzin 2 years, 5 months ago

answer is A.

upvoted 1 times

Chiquitabandita 2 years, 5 months ago

Selected Answer: A

I agree that A is right for the 1 blue low severity

upvoted 1 times

SpTester 2 years, 7 months ago

Selected Answer: A

Answer should be A. The blue color codes for low severity incidents.

upvoted 2 times

Question #14 *Topic 1*

Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?

A. Sensor Engine

B. Causality Analysis Engine

C. Log Stitching Engine

D. Causality Chain Engine

Suggested Answer: *B*
Official Answer: B

danups Most Recent 1 year, 11 months ago

Selected Answer: B

Causality Analysis Engine: This engine analyzes relationships between different alerts and determines the most relevant artifacts. It aggregates alerts related to the same underlying event into a cohesive incident, providing a comprehensive view of the security situation.

Causality Chain Engine: This engine helps in understanding the sequence and relationship between events but is more focused on the detailed timeline and chaining of related events.

upvoted 1 times

Bsharif 2 years, 4 months ago

B is the right answer. Check: Ref.: Ref.: https://docs-cortex.paloaltonetworks.com/r/Cortex-XSIAM/Cortex-XSIAM-Administrator-Guide/Concepts

upvoted 1 times

Chiquitabandita 2 years, 5 months ago

Selected Answer: B

pg . 12

upvoted 1 times

9smiles 2 years, 11 months ago

Selected Answer: B

From CXPAD:

The Causality Analysis Engine determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident.

upvoted 4 times

Question #15 *Topic 1*

Which type of BIOC rule is currently available in Cortex XDR?

A. Threat Actor

B. Discovery

C. Network

D. Dropper

Suggested Answer: *D*
Official Answer: D

Bsharif 2 years, 4 months ago
Option D: Dropper is the right answer. im2ca has labeled all types of BIOC Rule. Which can be found under: Ref.: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/BIOC-Rule-Details
upvoted 1 times

_tips 2 years, 11 months ago
Selected Answer: D
Dropper
upvoted 1 times

im2ca 3 years ago
D is the only correct answer.

Type of BIOC rule:

Collection Credential Access Dropper Evasion Execution Evasive Exfiltration File Privilege Manipulation File Type Obfuscation Infiltration Lateral Movement Other Persistence Privilege Escalation Reconnaissance Tampering
upvoted 4 times

Karreldanam 3 years, 2 months ago
Selected Answer: D
Type of BIOC rule: ● Collection ● Credential Access ● Dropper ● Evasion ● Execution ● Evasive ● Exfiltration ● File Privilege Manipulation ● File Type Obfuscation ● Infiltration ● Lateral Movement ● Other ● Persistence ● Privilege Escalation ● Reconnaissance ● Tampering
upvoted 2 times

PANW 3 years, 1 month ago
https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/BIOC-Rule-Details
upvoted 1 times

escar 3 years, 3 months ago
Selected Answer: B
Both B & D are correct??
upvoted 1 times

danups Most Recent 1 year, 11 months ago
Actually in the current version both "Dropper" and "Discovery" are valid BIOC rule types; however due to the time of creation of this exam I would guess it was designed without considering the "Discovery" type as an option, so I would go for "Dropper" (D)
upvoted 1 times

cneru1 3 years, 2 months ago
No Just D
upvoted 1 times

Question #16 *Topic 1*

In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the singer?

A. In the Restrictions Profile, add the file name and path to the Executable Files allow list.

B. Create a new rule exception and use the singer as the characteristic.

C. Add the signer to the allow list in the malware profile.

D. Add the signer to the allow list under the action center page.

Suggested Answer: *C*
Official Answer: C

danups 1 year, 11 months ago

Selected Answer: C

C is the right answer since in the malware profile you can add items to the allowed list based on the signer.

A is wrong, I mean you can do it but that is not what the question is asking for lol

upvoted 1 times

danups Most Recent 1 year, 10 months ago

It's worth to mention that creating an allow list based on digital signer used to be available in the malware protection profile but in older versions, on the very newer versions this feature has changed and is not available on that profile anymore. There is a new feature called "Legacy Agent Exceptions" under Settings > Exceptions Configurations and you basically have to create a rule exception based on your needs such as the digital signer. So if the question is expecting an updated answer then the right choice would be "B", probably on the real exam the question is worded different.

upvoted 1 times

0707bc6 2 years, 4 months ago

Selected Answer: C

Option A will allow only a specific executable while option C will allow this Signer in general which is the point of this question.

upvoted 1 times

Chiquitabandita 2 years, 4 months ago

Selected Answer: A

https://live.paloaltonetworks.com/t5/cortex-xdr-discussions/blocking-of-ioc-in-cortex-xdr/td-p/516052

changing answer to A

upvoted 1 times

Chiquitabandita 2 years, 4 months ago

sorry this is the wrong question for this answer, I still believe it to be C

upvoted 1 times

Chiquitabandita 2 years, 4 months ago

Selected Answer: C

I agree with C based on links below

upvoted 1 times

sharkk43 2 years, 9 months ago

I'd say C is for 3.5 version and older and B is for newer versions:

"Add a Disable Prevention Rule Cortex XDR enables you to generate granular exceptions to prevention actions defined for your endpoints. You can specify signers, command line, or processes to exclude from the prevention actions triggered by specific security modules. This may be useful when you have processes that are essential to your organization and must not be terminated. Cortex XDR still generates Alerts from the disabled rules." Checking inside my client's platform that's what I can see and we're running 3.7 currently. Info taken from here: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Add-a-Disable-Prevention-Rule

upvoted 2 times

im2ca 3 years ago

the correct option to prevent the Cortex XDR Agent from blocking the execution of a file based on the digital signer may vary depending on the specific version and configuration of the Cortex XDR Agent. However, based on the given options, the most appropriate choice would be:

C. Add the signer to the allow list in the malware profile.

By adding the digital signer to the allow list in the malware profile, you are essentially telling the Cortex XDR Agent to trust files signed by that specific signer and allow their execution without being blocked.

It's worth noting that cybersecurity measures and software configurations can change over time, so it's essential to refer to the official documentation or the latest guidelines provided by the product's vendor for the most up-to-date information. Additionally, configuring security software requires careful consideration and should be performed by knowledgeable and authorized personnel to ensure the system's security.

upvoted 2 times

Question #17 *Topic 1*

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?

A. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.

B. Enable DLL Protection on all servers but there might be some false positives.

C. Create IOCs of the malicious files you have found to prevent their execution.

D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.

Suggested Answer: *A*
Official Answer: A

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: A

To configure the Global Behavioral Threat Protection Rules:

Define the Action mode to take when the Cortex XDR agent detects malicious causality chains:

Block (default)—Block all processes and threads in the event chain up to the CGO.

Report—Allow the activity but report it to Cortex XDR.

Disabled—Disable the module and do not analyze or report the activity.

upvoted 1 times

Chiquitabandita 2 years, 4 months ago

I had seen about 4 questions from this site, that are very similar and can't really confirm which is the best answer. I keep coming up with a similar solution would be to create a BIOC rule for this situation but that is not one of the choices, it is different from a BTP rule, which to my research does not allow creation of rules to the general public. I had wondered if they possibly got the question mistranscribed from the source. Anyone have any other sources? C looks like it could be a good choice except as, 9smiles has suggested it is detection, not prevention, and the question asks for prevention.

upvoted 1 times

9smiles 2 years, 11 months ago

Please provide a reference for your claim im2ca. I have not been able to find any supporting documentation for this. Probably you are talking about custom prevention rules, which are basically BIOC rules that you add to restriction profiles see [1], but BTP Rules are something else and their database is not available to the public [2].

[1]: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Create-a-BIOC-Rule [2]: https://live.paloaltonetworks.com/t5/cortex-xdr-discussions/about-behavioral-threat-protection-btp-rules/td-p/395977

upvoted 2 times

im2ca 3 years ago

Correct is A: You can create BTP Rules in Cortex XDR .

upvoted 2 times

9smiles 3 years, 2 months ago

About BTP rules: Prevents sophisticated attacks that leverage built-in OS executables and common administration utilities by continuously monitoring endpoint activity for malicious causality chains. You are not able to create these - only create exceptions and turn them off so A cannot be correct.

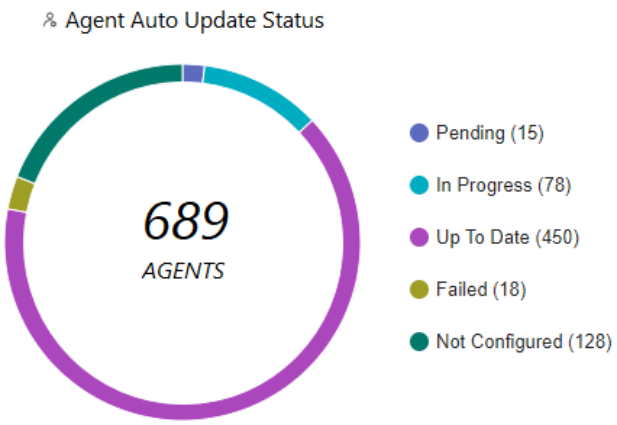
C can also not be correct since IOCs lead to detections, and do not prevent the file from running.

My guess would be B

upvoted 2 times

Question #18 *Topic 1*

Which statement is true based on the following Agent Auto Upgrade widget?



A. There are a total of 689 Up To Date agents.

B. Agent Auto Upgrade was enabled but not on all endpoints.

C. Agent Auto Upgrade has not been enabled.

D. There are more agents in Pending status than In Progress status.

Suggested Answer: *B*
Official Answer: B

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: B

admin guide pg. 287 and 128 clients are not configured according to this graph

upvoted 1 times

9smiles 3 years, 2 months ago

Correct answer: B

upvoted 2 times

Question #19 *Topic 1*

What is the purpose of targeting software vendors in a supply-chain attack?

A. to take advantage of a trusted software delivery method.

B. to steal users' login credentials.

C. to access source code.

D. to report Zero-day vulnerabilities.

Suggested Answer: *A*
Official Answer: A

examlog Highly Voted 3 years, 4 months ago

A. A. to take advantage of a trusted software delivery method. Correct Answer

upvoted 6 times

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: A

https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

upvoted 1 times

SpTester 2 years, 7 months ago

Selected Answer: A

It's to mimic the trusted software/hardware and get into networks. Answer A

upvoted 1 times

9smiles 2 years, 11 months ago

Selected Answer: A

Correct answer: A

upvoted 1 times

Davina07 3 years, 2 months ago

Selected Answer: A

Agree to A

upvoted 4 times

Question #20 *Topic 1*

What is the standard installation disk space recommended to install a Broker VM?

A. 1GB disk space

B. 2GB disk space

C. 512GB disk space

D. 256GB disk space

Suggested Answer: *C*
Official Answer: C

Chiquitabandita Most Recent 2 years, 5 months ago

Selected Answer: C

admin guide pg. 603

upvoted 1 times

9smiles 3 years, 2 months ago

Correct answer is C

From the CXPAG (Cortex XDR Pro Administrator Guide): Before you set up the broker VM, verify you meet the following requirements.

Hardware: For standard installation, use a minimum of a 4-core processor, 8GB RAM, and 512GB disk. If you only intend to use the broker VM for agent proxy, you can use a 2-core processor. If you intend to use the broker VM for agent installer and content caching, you must use an 8-core processor.

upvoted 3 times

Question #21 *Topic 1*

Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

A. in the macOS Malware Protection Profile to indicate allowed signers

B. in the Linux Malware Protection Profile to indicate allowed Java libraries

C. SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles

D. in the Windows Malware Protection Profile to indicate allowed executables

Suggested Answer: *D*
Official Answer: D

danups Most Recent 1 year, 11 months ago

Selected Answer: C

Can't find any hash related configuration within malware profiles

upvoted 1 times

Chiquitabandita 2 years, 4 months ago

Selected Answer: D

● CreatesaRuleException based onthePROCESSSHA256fieldforIOCrules that hit more than 100 endpoints over a 72-hour period.

Changing answer to D for this part in the study guide :
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf

upvoted 1 times

Bradl 2 years, 8 months ago

C is the answer

upvoted 3 times

darylmaeb24 2 years, 9 months ago

answer C

upvoted 2 times

examlog 2 years, 9 months ago

Correct Answer: D

upvoted 1 times

9smiles 3 years, 2 months ago

Answer is C,

Allow list has been moved from Prevention Profiles to Exceptions Configuration

upvoted 3 times

escar 3 years, 3 months ago

I think it should be C, cannot find any configuration on malware profile related to hash value allow

upvoted 4 times

Question #22 *Topic 1*

How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

A. by encrypting the disk first.

B. by utilizing decoy Files.

C. by retrieving the encryption key.

D. by patching vulnerable applications.

Suggested Answer: *B*
Official Answer: B

danups Most Recent 1 year, 11 months ago

Selected Answer: B

Unit42 through in-depth threat intel investigations understand and grab potential Ransomware behaviors such as common file paths or processes affected in order to build decoy files and enhance the ransomware detection. These decoy files are sent through content updates.

upvoted 1 times

nividan 2 years, 11 months ago

Correct Answer: B Behavior-Based Ransomware Protection This module protects against encryption-based behavior associated with ransomware by analyzing and stopping ransomware activity before any data loss occurs. To combat these attacks, Cortex XDR employs decoy files to attract the ransomware. When the ransomware attempts to write to, rename, move, delete, or encrypt the decoy files, the Cortex XDR agent analyzes the behavior and prevents the ransomware from encrypting and holding files hostage. When configured to operate in Prevention Mode, the Cortex XDR agent blocks the process attempting to manipulate the decoy files. When you configure this module in Notification Mode, the agent logs a security event.

upvoted 1 times

9smiles 3 years, 2 months ago

My answer would be: B

upvoted 2 times

Question #23 *Topic 1*

What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

A. Netflow Collector

B. Syslog Collector

C. DB Collector

D. Pathfinder

Suggested Answer: *B*
Official Answer: B

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: B

I agree with the link below

upvoted 1 times

XuannnnOAO 2 years, 9 months ago

B is correct~ https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/External-Data-Ingestion-Vendor-Support

upvoted 1 times

im2ca 3 years ago

Correct is B

upvoted 1 times

Davina07 3 years, 2 months ago

I think B: "To ingest data, you must set up the Syslog Collector applet on a broker VM within your network."

upvoted 4 times

9smiles 3 years, 2 months ago

I mean: B

upvoted 2 times

9smiles 3 years, 2 months ago

Correct answer: C

From the PCDRA Study Guide:

7.5.2 Describe how to use the Broker to ingest third-party alerts ... To ingest data, you must set up the Syslog Collector applet on a broker VM within your network.

upvoted 2 times

Question #24 *Topic 1*

In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?

A. Agent Proxy

B. Agent Installer and Content Caching

C. Syslog Collector

D. CSV Collector

Suggested Answer: *B*
Official Answer: B

danups 1 year, 11 months ago

Selected Answer: A

Agent Proxy: This component acts as an intermediary between the Cortex XDR agents and the Cortex XDR cloud. It requires a strong cipher SHA256-based SSL certificate to secure the communication between the agents and the proxy, ensuring the integrity and confidentiality of the data transmitted to the Cortex XDR Instance in the Cloud.

upvoted 1 times

danups Most Recent 1 year, 10 months ago

Changing answer to "B", 9smiles is right

upvoted 1 times

9smiles 3 years, 2 months ago

Correct answer: B

From the Cortex XDR Pro Administrators Guide (CXPAG):

Agent Installer and Content Caching: Requires you upload a strong cipher SHA256-based SSL certificates when you setup the Broker VM.

upvoted 4 times

Question #25 *Topic 1*

When is the wss (WebSocket Secure) protocol used?

A. when the Cortex XDR agent downloads new security content

B. when the Cortex XDR agent uploads alert data

C. when the Cortex XDR agent connects to WildFire to upload files for analysis

D. when the Cortex XDR agent establishes a bidirectional communication channel

Suggested Answer: *D*
Official Answer: D

9smiles Most Recent 3 years, 2 months ago
Correct answer: D

From beacon: WebSocket is a stateful, full-duplex communication protocol that allows a two-way interactive communication between a Cortex XDR instance and Cortex XDR agents. This type of communication allows data transfers in real-time by keeping sessions for a longer durations. When you perform one of these critical response actions from the Cortex XDR management console, the Cortex XDR instance establishes a session between the instance itself and the targeted endpoint. Then, the session is kept alive even after the response action is complete. Live Terminal is among these response actions.
upvoted 3 times

Question #26 *Topic 1*

With a Cortex XDR Prevent license, which objects are considered to be sensors?

A. Syslog servers

B. Third-Party security devices

C. Cortex XDR agents

D. Palo Alto Networks Next-Generation Firewalls

Suggested Answer: *C*
Official Answer: C

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: C

https://pupuweb.com/pcdra-exam-question-answer-cortex-xdr-prevent-license-objects-sensors/

upvoted 1 times

9smiles 3 years, 2 months ago

Answer I think is: C

Syslog Collector is not included in XDR Prevent, only Pro Pr. TB. Pro Pr. TB is also required for External vendors, meaning Third Party security devices. Prevent does not include a firewall, leaving only C since

"Cortex XDR uses your existing Palo Alto Networks products as sensors to collect logs and telemetry data."

upvoted 1 times

Question #27 *Topic 1*

Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

A. Cortex XDR Pro per TB

B. Host Insights

C. Cortex XDR Pro per Endpoint

D. Cortex XDR Cloud per Host

Suggested Answer: *D*
Official Answer: D

9smiles Highly Voted 3 years, 2 months ago

Correct answer is: D

CXPAD: "To protect a Kubernetes or similar container orchestrator endpoint, Cortex XDR requires a Cortex Cloud per Host license."

upvoted 5 times

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: D

admin pg 16

upvoted 2 times

Question #28 *Topic 1*

What kind of the threat typically encrypts user files?

A. ransomware

B. SQL injection attacks

C. Zero-day exploits

D. supply-chain attacks

Suggested Answer: *A*
Official Answer: A

PaddyAdallah Most Recent 2 years, 11 months ago

Correct answer is : A

upvoted 1 times

9smiles 2 years, 11 months ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

Question #29 *Topic 1*

When using the “File Search and Destroy” feature, which of the following search hash type is supported?

A. SHA256 hash of the file

B. AES256 hash of the file

C. MD5 hash of the file

D. SHA1 hash of the file

Suggested Answer: *A*
Official Answer: A

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: A

I agree with the link below

upvoted 1 times

_tips 2 years, 11 months ago

Selected Answer: A

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Search-and-Destroy-Malicious-Files

Search File section

To search by hash, enter the file SHA256 value. When you search by hash, you can also search for deleted instances of this file on the endpoint.

upvoted 2 times

Question #30 *Topic 1*

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

A. Broker VM Pathfinder

B. Local Agent Proxy

C. Local Agent Installer and Content Caching

D. Broker VM Syslog Collector

Suggested Answer: *B*
Official Answer: B

b1gd1g Highly Voted 3 years, 1 month ago

B. Cortex XDR in restricted networks where endpoints do not have a direct connection to the internet, setup the Broker VM to act as a proxy

upvoted 6 times

abd1234 Most Recent 2 years, 2 months ago

Selected Answer: B

https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Prevent-Administrator-Guide/Activate-the-Local-Agent-Settings

upvoted 1 times

abd1234 2 years, 2 months ago

Selected Answer: B

Sorry I mistakenly selected C, it should be B.

To deploy Cortex XDR in restricted networks where endpoints do not have a direct connection to the internet, setup the Broker VM to act as a proxy that routes all the traffic between the Cortex XDR management server and XDR agents/XDR Collectors via a centralized and controlled access point

upvoted 1 times

abd1234 2 years, 2 months ago

Selected Answer: C

To deploy Cortex XDR in restricted networks where endpoints do not have a direct connection to the internet, setup the Broker VM to act as a proxy that routes all the traffic between the Cortex XDR management server and XDR agents/XDR Collectors via a centralized and controlled access point...

upvoted 1 times

Chiquitabandita 2 years, 4 months ago

Selected Answer: B

I agree it is B

upvoted 1 times

darylmaeb24 2 years, 9 months ago

Correct Answer B

upvoted 1 times

Blahziblah 2 years, 9 months ago

Selected Answer: B

I believe the answer is B.

Here is the admin guide, see the second bullet: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Activate-the-Local-Agent-Settings

Caching just means it will cache the data, but if it doesn't have the data it will try to go get it. This won't work in an isolated network so C isn't correct.

upvoted 2 times

Question #31 *Topic 1*

What is by far the most common tactic used by ransomware to shut down a victim's operation?

A. preventing the victim from being able to access APIs to cripple infrastructure

B. denying traffic out of the victims network until payment is received

C. restricting access to administrative accounts to the victim

D. encrypting certain files to prevent access by the victim

Suggested Answer: *D*
Official Answer: D

Chiquitabandita Most Recent 2 years, 4 months ago
admin guide pg/ 82 hints that this might be the answer
upvoted 1 times

Chiquitabandita 2 years, 4 months ago
Selected Answer: D
I didn't find it the guide but I think it is common knowledge that ransomware does this action
upvoted 1 times

GGP23 2 years, 5 months ago
Selected Answer: D
D is correct.
upvoted 1 times

ninya69 2 years, 9 months ago
D - correct
upvoted 2 times

Question #32 *Topic 1*

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques.

A. Exfiltration, Command and Control, Collection

B. Exfiltration, Command and Control, Privilege Escalation

C. Exfiltration, Command and Control, Impact

D. Exfiltration, Command and Control, Lateral Movement

Suggested Answer: *D*
Official Answer: D

Chiquitabandita 2 years, 4 months ago

Selected Answer: D

it does list those three but in the picture next to it in the guide, it shows impact as well but does not describe it.

upvoted 2 times

BS166 Most Recent 2 years, 3 months ago

@ Chiquitabandita: you are right. It means the option D is correct answer. -Execution -Persistence -Discovery -Lateral Movement -Command and Control -Exfiltration

upvoted 1 times

XuannnnOAO 2 years, 9 months ago

D is correct, refer to the official document:https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Analytics-Concepts

upvoted 2 times

Question #33 *Topic 1*

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

A. Assign incidents to an analyst in bulk.

B. Change the status of multiple incidents.

C. Investigate several Incidents at once.

D. Delete the selected Incidents.

Suggested Answer: *A, B*
Official Answer: AB

danups Most Recent 1 year, 11 months ago

Selected Answer: AB

A y B, I just checked it in the tool

upvoted 1 times

Chiquitabandita 2 years, 4 months ago

Selected Answer: AB

I agree it is AB

upvoted 1 times

MatchaLatte 2 years, 5 months ago

Selected Answer: AB

A, B https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Incidents

Check box to select one or more incidents on which to perform the following actions.

- Assign incidents to an analyst in bulk - Change the status of multiple incidents - Change the severity of multiple incidents

upvoted 2 times

ninya69 2 years, 9 months ago

A, B - You can change status/severity/assignee for all incidents as well as star/merge the incidents.

upvoted 1 times

Question #34 *Topic 1*

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

A. It is true positive.

B. It is false positive.

C. It is a false negative.

D. It is true negative.

Suggested Answer: *B*
Official Answer: B

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: B

the follow up question is what to do about this. I think you would put an exception to the policy, not touch wildfire.

upvoted 1 times

ninya69 2 years, 9 months ago

B Palo alto study guide - 4.1.4: False positive—An event that produces an alarm when no attack has taken place

upvoted 1 times

Question #35 *Topic 1*

What is the outcome of creating and implementing an alert exclusion?

A. The Cortex XDR agent will allow the process that was blocked to run on the endpoint.

B. The Cortex XDR console will hide those alerts.

C. The Cortex XDR agent will not create an alert for this event in the future.

D. The Cortex XDR console will delete those alerts and block ingestion of them in the future.

Suggested Answer: *B*
Official Answer: B

Chiquitabandita Most Recent 2 years, 4 months ago

Selected Answer: B

"Alert Exclusion rules specify match criteria for alerts that you want to suppress."

upvoted 1 times

XuannnnOAO 2 years, 9 months ago

B is correct, refer to the official document:https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-Administrator-Guide/Exception-Configuration

upvoted 1 times

Question #36 *Topic 1*

Which statement is true for Application Exploits and Kernel Exploits?

A. The ultimate goal of any exploit is to reach the application.

B. Kernel exploits are easier to prevent then application exploits.

C. The ultimate goal of any exploit is to reach the kernel.

D. Application exploits leverage kernel vulnerability.

Suggested Answer: *C*
Official Answer: C

danups Most Recent 1 year, 11 months ago

Selected Answer: C

Kernel exploits are harder to prevent and is their ultimate goal for further control of an endpoint.

upvoted 1 times

abd1234 2 years, 2 months ago

Selected Answer: C

Kernel is the goal.

upvoted 2 times

0707bc6 2 years, 4 months ago

Selected Answer: C

It's clearly stated in Beacon > Cortex XDR 3: Getting Started with Endpoint Protection > Cortex XDR 3: Exploit Protection > Application Exploit Prevention > Application Exploits and Kernel Exploits
https://beacon.paloaltonetworks.com/uploads/resource_courses/targets/2394329/original/index.html?_courseId=905962#/page/612c6346db387a0de433778d

upvoted 3 times

Chiquitabandita 2 years, 4 months ago

Selected Answer: A

I think it is A, only because the other answers feel wrong but I can't find definite reason why A is right

upvoted 1 times

besik 2 years, 5 months ago

Selected Answer: C

The attacker's ultimate goal is to reach the kernel because if he reaches the kernel, he can do anything he wants and to execute something he will not need privileged access. There are many mitigation techniques with Application Exploits but not many for the kernel.

upvoted 2 times

7e078ca 2 years, 6 months ago

C, From https://beacon.paloaltonetworks.com

upvoted 3 times

SpTester 2 years, 7 months ago

Selected Answer: A

I vote A because exploit does NOT nead to reach the kernel. So not C. Kernel exploits are really hard to defend against as it's the very root of the OS. So not B. Definitively not D. So remains an A.

So how can I explain that it is A? I would say with this circle that Palo Alto commonly spreads on the internet: https://www.paloaltonetworks.co.uk/research/apac-ondemand-webinar-2016-how-to-complete-the-security-puzzle-with-wildfire-and-traps

Usually they say if we can interrupt one part of the exploit the chain will be broken. So in the center we got the application of an exploit permitted. Hence why I vote A. Ultimate goal of an exploit is to reach application.

upvoted 2 times

_tips 2 years, 11 months ago

Regarding to this page https://www.csoonline.com/article/571799/exploit-chains-explained-how-and-why-attackers-target-multiple-vulnerabilities.html

“The goal with exploit chain attacks is to gain kernel/root/system level access to compromise a system in order to execute an attack,”

he answer is C

upvoted 2 times

_tips 2 years, 11 months ago

Selected Answer: A

Exploit Protection Overview An exploit is a sequence of commands that takes advantage of a bug or vulnerability in a software application or process. Attackers use these exploits to access and use a system to their advantage. Blocking any attempt to exploit a vulnerability in the chain will block the entire exploitation attempt. https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Prevent-Administrator-Guide/Endpoint-Protection

upvoted 2 times

Torben10 3 years, 1 month ago

Selected Answer: C

C should be right.

upvoted 4 times