EXAMTOPICS

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



CERTIFICATION TEST

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

Question #1 *Topic 1*

Which Enterprise Security framework provides a mechanism for running preconfigured actions within the Splunk platform or integrating with external applications?

A. Asset and Identity

B. Notable Event

C. Threat Intelligence

D. Adaptive Response

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

MJD20 Most Recent 1 year, 2 months ago

Selected Answer: D

I just did the exam. I got only 30% of these questions. So, prepare well, and don't only count on these... They are outdated! Feel like I paid €80 for nothing....

upvoted 1 times

nosavotor 1 year, 11 months ago

I'm not sure about that

upvoted 1 times

Question #2 *Topic 1*

Which of the following Splunk Enterprise Security features allows industry frameworks such as CIS Critical Security Controls, MITRE ATT&CK, and the Lockheed Martin Cyber Kill Chain® to be mapped to Correlation Search results?

A. Annotations

B. Playbooks

C. Comments

D. Enrichments

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

a50b9c8 Most Recent 1 year, 5 months ago

Selected Answer: A

A. Annotations

upvoted 1 times

ProfessorJayy 1 year, 12 months ago

Selected Answer: A

A. Annotations Explanation: Annotations in Splunk Enterprise Security allow industry frameworks such as CIS Critical Security Controls, MITRE ATT&CK, and the Lockheed Martin Cyber Kill Chain® to be mapped to Correlation Search results. This helps analysts understand and categorize security events within the context of these frameworks.

upvoted 2 times

Question #3 *Topic 1*

Which of the following is the primary benefit of using the CIM in Splunk?

A. It allows for easier correlation of data from different sources.

B. It improves the performance of search queries on raw data.

C. It enables the use of advanced machine learning algorithms.

D. It automatically detects and blocks cyber threats.

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 1 times

Question #4 *Topic 1*

Tactics, Techniques, and Procedures (TTPs) are methods or behaviors utilized by attackers. In which framework are these categorized?

A. NIST 800-53

B. ISO 27000

C. CIS18

D. MITRE ATT&CK

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

a50b9c8 Most Recent 1 year, 5 months ago

Selected Answer: D

D. MITRE ATT&CK

upvoted 1 times

zisturordi 1 year, 9 months ago

ATT&CK is a model that attempts to systematically categorize adversary behavior. The main components of the model are: - Tactics, represents “why” or the reason an adversary is performing an action - Techniques, represents “how” adversaries achieve tactical goals by performing an action - Sub-techniques, a more specific or lower-level description of adversarial behavior - Procedures, specific implementation or in-the-wild use the adversary uses for techniques or sub-techniques

upvoted 1 times

nosavotor 1 year, 11 months ago

Someone please verify the accuracy of this answer

upvoted 2 times

Question #5 *Topic 1*

A threat hunter executed a hunt based on the following hypothesis:
As an actor, I want to plant rundll32 for proxy execution of malicious code and leverage Cobalt Strike for Command and Control.
Relevant logs and artifacts such as Sysmon, netflow, IDS alerts, and EDR logs were searched, and the hunter is confident in the conclusion that Cobalt Strike is not present in the company's environment.
Which of the following best describes the outcome of this threat hunt?

A. The threat hunt was successful because the hypothesis was not proven.

B. The threat hunt failed because the hypothesis was not proven.

C. The threat hunt failed because no malicious activity was identified.

D. The threat hunt was successful in providing strong evidence that the tactic and tool is not present in the environment.

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Could someone help me confirm if this is correct
upvoted 1 times

Question #6 *Topic 1*

An analyst notices that one of their servers is sending an unusually large amount of traffic, gigabytes more than normal, to a single system on the Internet. There doesn't seem to be any associated increase in incoming traffic.
What type of threat actor activity might this represent?

A. Data exfiltration

B. Network reconnaissance

C. Data infiltration

D. Lateral movement

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Wildcards are not efficient
upvoted 1 times

Question #7 *Topic 1*

In which phase of the Continuous Monitoring cycle are suggestions and improvements typically made?

A. Define and Predict

B. Establish and Architect

C. Analyze and Report

D. Implement and Collect

Suggested Answer: *C*
Official Answer: C

nosavotor Most Recent 1 year, 11 months ago

Could someone help me confirm the correctness of this answer

upvoted 1 times

Question #8 *Topic 1*

An analyst is not sure that all of the potential data sources at her company are being correctly or completely utilized by Splunk and Enterprise Security. Which of the following might she suggest using, in order to perform an analysis of the data types available and some of their potential security uses?

A. Splunk ITSI

B. Splunk Security Essentials

C. Splunk SOAR

D. Splunk Intelligence Management

Suggested Answer: *B*

Official Answer: B

Community vote distribution

B (100%)

bustoss_max Most Recent 1 year, 1 month ago

Selected Answer: B

okok ok

upvoted 1 times

bustoss_max 1 year, 1 month ago

Selected Answer: B

I am sure

upvoted 1 times

nosavotor 1 year, 11 months ago

Im not sure how to respond to that

upvoted 1 times

Question #9 *Topic 1*

During their shift, an analyst receives an alert about an executable being run from C:\Windows\Temp. Why should this be investigated further?

A. Temp directories aren't owned by any particular user, making it difficult to track the process owner when files are executed.

B. Temp directories are flagged as non-executable, meaning that no files stored within can be executed, and this executable was run from that directory.

C. Temp directories contain the system page file and the virtual memory file, meaning the attacker can use their malware to read the in memory values of running programs.

D. Temp directories are world writable thus allowing attackers a place to drop, stage, and execute malware on a system without needing to worry about file permissions.

Suggested Answer: *D*
Official Answer: D

nosavotor 1 year, 11 months ago
I'm not sure about that
upvoted 1 times

nosavotor 1 year, 11 months ago
I'm not sure about thathave you tried asking chat gpt?
upvoted 1 times

MJD20 Most Recent 1 year, 2 months ago
have you tried asking chat gpt?
upvoted 1 times

Question #10 *Topic 1*

An analyst would like to visualize threat objects across their environment and chronological risk events for a Risk Object in Incident Review. Where would they find this?

A. Running the Risk Analysis Adaptive Response action within the Notable Event.

B. Via a workflow action for the Risk Investigation dashboard.

C. Via the Risk Analysis dashboard under the Security Intelligence tab in Enterprise Security.

D. Clicking the risk event count to open the Risk Event Timeline.

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Friends could you please confirm this answer
upvoted 1 times

Question #11 *Topic 1*

A Risk Rule generates events on Suspicious Cloud Share Activity and regularly contributes to confirmed incidents from Risk Notables. An analyst realizes the raw logs these events are generated from contain information which helps them determine what might be malicious.
What should they ask their engineer for to make their analysis easier?

A. Create a field extraction for this information.

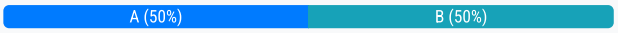
B. Add this information to the risk_message.

C. Create another detection for this information.

D. Allowlist more events based on this information.

Suggested Answer: *A*
Official Answer: A

Community vote distribution



CeeCapi Most Recent 1 year, 9 months ago

Option B. Add this information to the risk_message is indeed a viable and effective choice, especially in the context of Risk-Based Alerting (RBA) in Splunk. By adding key information to the risk_message, you enhance the context around each risk event, allowing the analyst to quickly view relevant details without needing to drill down into raw logs. This approach can streamline investigations by summarizing essential details directly within the notable events, making the process faster and more efficient for the analyst. In this case, both A and B can be good options, but B might offer more immediate context within the Incident Review, especially if the goal is to have critical information surfaced directly in risk events.

upvoted 3 times

Nss_dfir 1 year, 10 months ago

Selected Answer: A

Creating a field extraction allows the analyst to easily access and utilize specific data points within the raw logs, making it more efficient to analyze and correlate with the suspicious activity. This will enhance their ability to determine the nature of the activity and its potential maliciousness.

upvoted 2 times

ProfessorJayy 1 year, 12 months ago

Selected Answer: B

see previous comment

upvoted 2 times

ProfessorJayy 1 year, 12 months ago

B. Add this information to the risk_message. Explanation: The risk_message field in Splunk's Enterprise Security contains details about why a particular risk event was generated. By asking the engineer to add the relevant information from the raw logs to the risk_message, the analyst can have easy access to important context directly within the risk events, making their analysis more efficient without needing to refer back to the raw logs constantly.

upvoted 4 times

Question #12 *Topic 1*

What device typically sits at a network perimeter to detect command and control and other potentially suspicious traffic?

A. Host-based firewall

B. Web proxy

C. Endpoint Detection and Response

D. Intrusion Detection System

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago

Could someone help me confirm if this is correct

upvoted 1 times

Question #13 *Topic 1*

Upon investigating a report of a web server becoming unavailable, the security analyst finds that the web server's access log has the same log entry millions of times:
147.186.119.200 - - [28/Jul/2023:12:04:13 -0300] "GET /login/ HTTP/1.0" 200 3733
What kind of attack is occurring?

A. Denial of Service Attack

B. Distributed Denial of Service Attack

C. Cross-Site Scripting Attack

D. Database Injection Attack

Suggested Answer: *B*
Official Answer: B

Community vote distribution
A (100%)

CeeCapi Most Recent 1 year, 9 months ago
A. Denial of Service Attack The repeated identical log entry suggests a Denial of Service (DoS) attack, where a single source floods the server with requests to make it unavailable to legitimate users. Since there is no indication of multiple IP addresses, it is likely a DoS rather than a Distributed Denial of Service (DDoS) attack, which would involve multiple sources.
upvoted 1 times

Nss_dfir 1 year, 10 months ago
Selected Answer: A
A. Denial of Service Attack. This suggests that the web server is being overwhelmed by repeated requests from a single source (the IP address 147.186.119.200), which can lead to the server becoming unavailable to legitimate users. If the attack were coming from multiple sources, it would be classified as a Distributed Denial of Service (DDoS) attack, but in this case, the log indicates a single source.
upvoted 2 times

ProfessorJayy 1 year, 12 months ago
Selected Answer: A
only one ip, DoS?
upvoted 2 times

Question #14 *Topic 1*

According to David Bianco's Pyramid of Pain, which indicator type is least effective when used in continuous monitoring?

A. Domain names

B. TTPs

C. Network/Host artifacts

D. Hash values

Suggested Answer: *D*
Official Answer: D

CeeCapi Most Recent 1 year, 9 months ago

D. Hash values According to David Bianco's Pyramid of Pain, hash values are considered the least effective indicator for continuous monitoring because they are easy for attackers to change. This means that using hash values as indicators creates minimal pain for attackers, as they can simply modify the file slightly to generate a new hash and evade detection.

upvoted 2 times

nosavotor 1 year, 11 months ago

Friends could you please confirm this answer

upvoted 1 times

Question #15 *Topic 1*

An analysis of an organization's security posture determined that a particular asset is at risk and a new process or solution should be implemented to protect it. Typically, who would be in charge of implementing the new process or solution that was selected?

A. Security Architect

B. SOC Manager

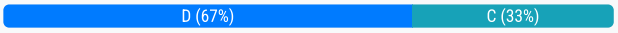
C. Security Engineer

D. Security Analyst

Suggested Answer: *C*

Official Answer: C

Community vote distribution



ckditro Most Recent 1 year, 8 months ago

Selected Answer: C

Solutions sit with engineers, not analyst or above. Architects design, Managers are more responsible for people and processes.

upvoted 1 times

CeeCapi 1 year, 9 months ago

Splunk - Splk - 5001 Exam questions changed. When can we expect update. Stated update November 21 but I can't find any update. Almost new set of questions start showing up. Thanks

upvoted 3 times

christophe_ciwr 1 year, 9 months ago

Selected Answer: D

D. Architect: Chooses and implements tools and Solutions. Engineer creates and test detections.

upvoted 2 times

CeeCapi 1 year, 9 months ago

A Security Engineer is typically in charge of implementing new security processes or solutions to protect organizational assets. They are responsible for deploying, configuring, and maintaining security technologies and solutions as part of safeguarding the organization's infrastructure.

upvoted 1 times

b14de41 1 year, 10 months ago

Correction: see question #43, so C is correct for this one.

upvoted 1 times

b14de41 1 year, 10 months ago

Should be "A" for Architect

upvoted 3 times

nosavotor 1 year, 11 months ago

Someone please verify the accuracy of this answer

upvoted 1 times

Question #16 *Topic 1*

Which of the following is a correct Splunk search that will return results in the most performant way?

A. index=foo host=i-478619733 | stats range(_time) as duration by src_ip | bin duration span=5min | stats count by duration, host

B. | stats range(_time) as duration by src_ip | index=foo host=i-478619733 | bin duration span=5min | stats count by duration, host

C. index=foo host=i-478619733 | transaction src_ip |stats count by host

D. index=foo | transaction src_ip |stats count by host | search host=i-478619733

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Im not sure how to respond to that
upvoted 1 times

Question #17 *Topic 1*

There are many resources for assisting with SPL and configuration questions. Which of the following resources feature community-sourced answers?

A. Splunk Answers

B. Splunk Lantern

C. Splunk Guidebook

D. Splunk Documentation

Suggested Answer: *A*
Official Answer: A

Community vote distribution
A (100%)

8e22337 Most Recent 1 year, 1 month ago

Selected Answer: A

https://community.splunk.com/?_gl=1*pzeg8c*_gcl_au*MTgwNjI1MTM4My4xNzUzMjIxMjY3*FPAU*MTgwNjI1MTM4My4xNzUzMjIxMjY3*_ga*MTgwNzI0NTkwNS4xNzQ1OTQyMDM5*_ga_5EPM2P39FV*czE3NTMyODQ1MDkkbzQ4JGcwJHQxNzUzMjg0NTA5JGo2MCRsMCRoODY5MDE4Njk3*_fplc*MVg0TTM4YXh1SSUyRk5ESnNLMUY0cWk0QyUyRldpb2lOJTJCTzNydXdnb2NPV0RmczZBUyUyRnVLblZENnVpTHJnR2ZyRHBUWkYyRndyV3c4NXg1VGZ5WlpUUEMxM1F1S0pyZjhoem5EbmdjckVEM1A2QUhpa3NmcnlCcmRYbEJjaXdJUWclM0QlM0Q.

upvoted 1 times

nosavotor 1 year, 11 months ago

Could someone help me confirm the correctness of this answer

upvoted 1 times

Question #18 *Topic 1*

A successful Continuous Monitoring initiative involves the entire organization. When an analyst discovers the need for more context or additional information, perhaps from additional data sources or altered correlation rules, to what role would this request generally escalate?

A. SOC Manager

B. Security Analyst

C. Security Engineer

D. Security Architect

Suggested Answer: *C*
Official Answer: C

CeeCapi Most Recent 1 year, 9 months ago

D. Security Architect Here's a clarification: Security Architect: Primarily responsible for designing and planning the overall security architecture and framework. They make high-level decisions about what data sources, tools, and rules are necessary to protect the organization. If the analyst identifies a need for more context or new data sources, the Security Architect will review and design how these fit into the broader security strategy. Security Engineer: Focused on the hands-on implementation and configuration of security tools and systems. If the Security Architect approves the need for new data sources or changes in correlation rules, the Security Engineer would typically take action to integrate these into the existing systems and ensure they're functioning as expected. So, when an analyst identifies a need for more data sources or rules, the request typically goes to the Security Architect for review. If approved, it is often then passed to the Security Engineer for implementation.

upvoted 1 times

nosavotor 1 year, 11 months ago

Could someone help me confirm the correctness of this answer

upvoted 1 times

Question #19 *Topic 1*

Splunk Enterprise Security has numerous frameworks to create correlations, integrate threat intelligence, and provide a workflow for investigations. Which framework raises the threat profile of individuals or assets to allow identification of people or devices that perform an unusual amount of suspicious activities?

A. Threat Intelligence Framework

B. Risk Framework

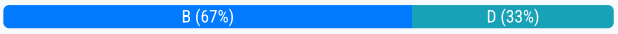
C. Notable Event Framework

D. Asset and Identity Framework

Suggested Answer: *B*

Official Answer: B

Community vote distribution



jeremyleebee Most Recent 5 months ago

Selected Answer: B

Correct Answer: B Reasoning: While Asset and Identity Framework do in fact enrich data for the threat profile for people and devices, it does NOT itself raise the threat score. Only Risk Framework actually raises the score. I think this is a not great question that is more likely used for sampling on the exam itself, but by semantics and documentation, I believe B is the most correct answer.

upvoted 1 times

edwardsid_111 1 year, 1 month ago

Selected Answer: B

Question asks for "unusual amounts of activity" this clearly points to a risk score which is being accumulated against something by risk rules so B is the correct answer

upvoted 1 times

12la12 1 year, 6 months ago

Selected Answer: D

The correct answer is: D. Asset and Identity Framework Explanation: The Asset and Identity Framework is specifically designed to raise the threat profile of individuals (identities) or devices (assets) by correlating events with contextual information. It achieves this by: Enriching raw events with metadata about assets (devices, servers) and identities (users, service accounts). Aggregating suspicious activities tied to specific entities (e.g., repeated failed logins from a user or unusual data transfers from a server). Providing contextual prioritization (e.g., flagging a high-risk activity if it involves a privileged account or a mission-critical server).

upvoted 1 times

nosavotor 1 year, 11 months ago

Wildcards are not efficient

upvoted 1 times

Question #20 *Topic 1*

While the top command is utilized to find the most common values contained within a field, a Cyber Defense Analyst hunts for anomalies. Which of the following Splunk commands returns the least common values?

A. least

B. uncommon

C. rare

D. base

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

8e22337 Most Recent 1 year, 1 month ago

Selected Answer: C

top/rare Displays the most/least common values of a field.

upvoted 1 times

nosavotor 1 year, 11 months ago

Could someone help me confirm the correctness of this answer

upvoted 1 times

Question #21 *Topic 1*

The Lockheed Martin Cyber Kill Chain® breaks an attack lifecycle into several stages. A threat actor modified the registry on a compromised Windows system to ensure that their malware would automatically run at boot time. Into which phase of the Kill Chain would this fall?

A. Act on Objectives

B. Exploitation

C. Delivery

D. Installation

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 1 times

Question #22 *Topic 1*

A Risk Notable Event has been triggered in Splunk Enterprise Security, an analyst investigates the alert, and determines it is a false positive. What metric would be used to define the time between alert creation and close of the event?

A. MTTR (Mean Time to Respond)

B. MTBF (Mean Time Between Failures)

C. MTTA (Mean Time to Acknowledge)

D. MTTD (Mean Time to Detect)

Suggested Answer: *A*

Official Answer: A

Community vote distribution

A (100%)

8e22337 Most Recent 1 year, 1 month ago

Selected Answer: A

Mean time to respond (MTTR): MTTR is the average time it takes an analyst to respond to an incident. A lower MTTR indicates that analysts are responding to incidents more quickly. Threat topology visualization reduces MTTR.

upvoted 1 times

nosavotor 1 year, 11 months ago

Friends could you please confirm this answer

upvoted 1 times

Question #23 *Topic 1*

An analyst needs to create a new field at search time. Which Splunk command will dynamically extract additional fields as part of a Search pipeline?

A. rex

B. fields

C. regex

D. eval

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Friends could you please confirm this answer
upvoted 1 times

Question #24 *Topic 1*

Which of the following is considered Personal Data under GDPR?

A. The birth date of an unidentified user.

B. An individual's address including their first and last name.

C. The name of a deceased individual.

D. A company's registration number.

Suggested Answer: *B*
Official Answer: B

nosavotor Most Recent 1 year, 11 months ago
Im not sure how to respond to that
upvoted 1 times

Question #25 *Topic 1*

What goal of an Advanced Persistent Threat (APT) group aims to disrupt or damage on behalf of a cause?

A. Hacktivism

B. Cyber espionage

C. Financial gain

D. Prestige

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Im not sure how to respond to that
upvoted 1 times

Question #26 *Topic 1*

A Cyber Threat Intelligence (CTI) team produces a report detailing a specific threat actor's typical behaviors and intent. This would be an example of what type of intelligence?

A. Operational

B. Executive

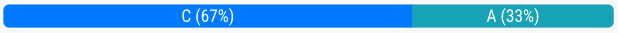
C. Tactical

D. Strategic

Suggested Answer: *D*

Official Answer: D

Community vote distribution



8e22337 Most Recent 1 year, 1 month ago

Selected Answer: A

based on the study guide it matches closer with A. Operational

upvoted 1 times

CeeCapi 1 year, 9 months ago

D. Strategic Strategic intelligence provides a high-level overview of a threat actor's behaviors, capabilities, and intent, often focusing on long-term trends and goals. This type of intelligence helps organizations understand the broader threat landscape and anticipate potential future risks, making it valuable for decision-makers in planning and resource allocation.

upvoted 1 times

Nss_dfir 1 year, 10 months ago

Selected Answer: C

Answer: C Explanation: Tactical intelligenceprovides insights into the specific behaviors, tools, and techniques used by threat actors. When a Cyber Threat Intelligence (CTI) team produces a report detailing a threat actor's typical behaviors and intent, they are delivering tactical intelligence. This type of intelligence is actionable and directly supports defenders in identifying, mitigating, and responding to threats in a timely manner.

upvoted 4 times

Nss_dfir 1 year, 10 months ago

Selected Answer: A

A. Operational

upvoted 1 times

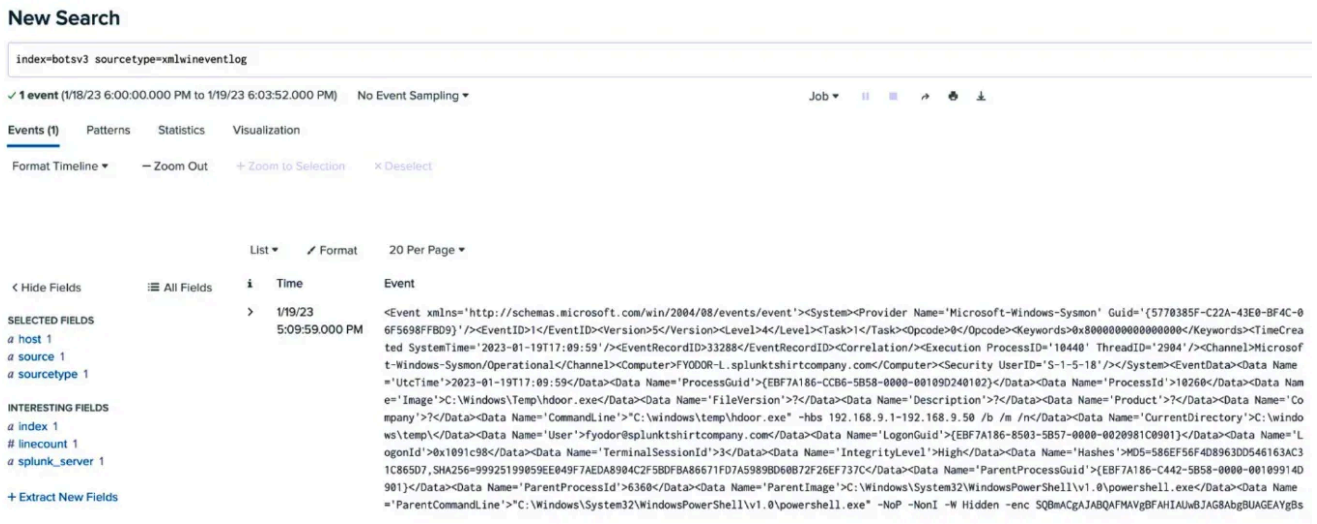
DevinArchie 2 years ago

Wrong Answer. Correct answer is A: Explanation Operational: Operational threat intelligence provides information about the actors behind threats, their motivations, and their capabilities. It can also provide information about emerging threats and trends. Operational threat intelligence is typically used by security managers to make informed decisions about security investments and priorities.

upvoted 3 times

Question #27 *Topic 1*

An analyst is building a search to examine Windows XML Event Logs, but the initial search is not returning any extracted fields. Based on the above image, what is the most likely cause?



A. The analyst does not have the proper role to search this data.

B. The analyst is searching newly indexed data that was improperly parsed.

C. The analyst did not add the extract command to their search pipeline.

D. The analyst is not in the proper Search Mode and should switch to Smart or Verbose.

Suggested Answer: *C*

Official Answer: C

Community vote distribution

D (50%) B (50%)

e7def26 Most Recent 1 month, 2 weeks ago

Selected Answer: D

D I believe When Splunk is in Fast Mode, field extraction is minimized to improve search performance. As a result, many search-time extracted fields are not displayed. Switching to Smart or Verbose mode enables automatic field extraction and makes those fields available in the search results.

upvoted 1 times

nosavotor 3 months ago

D. The analyst is not in the proper Search Mode and should switch to Smart or Verbose.

upvoted 1 times

hd14 1 year, 10 months ago

A I don't think I have field extraction authority.

upvoted 1 times

8e22337 1 year, 1 month ago

Selected Answer: B

The sourcetype=xmlwineventlog is applied. The raw event data is XML and appears unparsed — all the key-value pairs are still embedded inside the XML string. No field extractions have occurred, which suggests field extractions did not trigger at index time or search time. If Splunk had parsed it properly, you'd see structured fields like User, CommandLine, or ProcessId extracted. Why the other options are incorrect: A. The analyst does not have the proper role... If this were the case, they likely wouldn't see any data at all. C. The analyst did not add the extract command... The extract command (kv, xmlkv, etc.) can help, but field extraction should be automatic if the sourcetype is configured correctly. D. The analyst is not in the proper Search Mode... Search mode (Fast, Smart, Verbose) affects event and field visibility, but this issue is parsing-related, not visibility-related.

upvoted 1 times

hd14 1 year, 10 months ago

A I don't think I have field extraction authority.it says proper role to search this data. If you didn't have authority, you wouldn't even see the data.

upvoted 1 times

supremesplunker 1 year, 7 months ago

it says proper role to search this data. If you didn't have authority, you wouldn't even see the data.

upvoted 1 times

nosavotor 1 year, 11 months ago

Could someone please verify the accuracy of this answer

upvoted 2 times

Question #28 *Topic 1*

An organization is using Risk-Based Alerting (RBA). During the past few days, a user account generated multiple risk observations. Splunk refers to this account as what type of entity?

A. Risk Factor

B. Risk Index

C. Risk Analysis

D. Risk Object

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 1 times

Question #29 *Topic 1*

When searching in Splunk, which of the following SPL commands can be used to run a subsearch across every field in a wildcard field list?

A. foreach

B. rex

C. makeresults

D. transaction

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago

Could someone help me confirm if this is correct

upvoted 1 times

Question #30 *Topic 1*

How are Notable Events configured in Splunk Enterprise Security?

A. During an investigation.

B. As part of an audit.

C. Via an Adaptive Response Action in a regular search.

D. Via an Adaptive Response Action in a correlation search.

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Wildcards are not efficient
upvoted 1 times

Question #31 *Topic 1*

An analyst is investigating a network alert for suspected lateral movement from one Windows host to another Windows host. According to Splunk CIM documentation, the IP address of the host from which the attacker is moving would be in which field?

A. host

B. dest

C. src_nt_host

D. src_ip

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

supremesplunker Most Recent 1 year, 7 months ago

Selected Answer: D

It has to be D because host is for Splunk audit logs. dest, obviously not. src_nt_host is for network sessions (DHCP and VPN traffic), so by getting rid of all the options, must be D.

upvoted 2 times

nosavotor 1 year, 11 months ago

Im not sure how to respond to that

upvoted 1 times

Question #32 *Topic 1*

Which of the following data sources can be used to discover unusual communication within an organization's network?

A. EDS

B. NetFlow

C. Email

D. IAM

Suggested Answer: *B*
Official Answer: B

nosavotor Most Recent 1 year, 11 months ago

Friends could you please confirm this answer

upvoted 1 times

Question #33 *Topic 1*

When threat hunting for outliers in Splunk, which of the following SPL pipelines would filter for users with over a thousand occurrences?

A. | sort by user | where count > 1000

B. | stats count by user | where count > 1000 | sort - count

C. | top user

D. | stats count(user) | sort - count | where count > 1000

Suggested Answer: *B*
Official Answer: B

nosavotor Most Recent 1 year, 11 months ago
Someone please verify the accuracy of this answer
upvoted 1 times

Question #34 *Topic 1*

The United States Department of Defense (DoD) requires all government contractors to provide adequate security safeguards referenced in National Institute of Standards and Technology (NIST) 800-171. All DoD contractors must continually reassess, monitor, and track compliance to be able to do business with the US government.
Which feature of Splunk Enterprise Security provides an analyst context for the correlation search mapping to the specific NIST guidelines?

A. Comments

B. Notes

C. Annotations

D. Framework mapping

Suggested Answer: *D*
Official Answer: D

Community vote distribution
D (50%) C (50%)

Tatakon Most Recent 9 months ago

Selected Answer: D

The questions here, Which feature provides correlation search mapping, both Comments,Notes and Annotation are key for investigation purpose but don't map to compliance

upvoted 1 times

MJD20 1 year, 2 months ago

Selected Answer: C

Framework Mapping is not a feature in Splunk. Annotations is a feature where NIST can be tagged

upvoted 1 times

CeeCapi 1 year, 9 months ago

Answer - C. Annotations Annotations in Splunk Enterprise Security allow correlation searches to be tagged with relevant frameworks, like NIST 800-171, CIS, or MITRE ATT&CK. This tagging provides context to the analyst, showing how specific searches align with these frameworks. It effectively maps correlation searches to compliance guidelines or security frameworks. Framework mapping isn't an official Splunk Enterprise Security feature or term. The closest feature that performs this mapping function in Splunk is indeed Annotations. So, C. Annotations is correct because it is the feature in Splunk Enterprise Security designed for mapping correlation searches to frameworks like NIST.

upvoted 3 times

nosavotor 1 year, 11 months ago

I'm not sure about that

upvoted 1 times

nosavotor 1 year, 11 months ago

I'm not sure about thatwhere you sure about any of the questions?

upvoted 1 times

supremesplunker Highly Voted 1 year, 7 months ago

where you sure about any of the questions?

upvoted 5 times

Question #35 *Topic 1*

An analyst is investigating the number of failed login attempts by IP address. Which SPL command can be used to create a temporary table containing the number of failed login attempts by IP address over a specific time period?

A. index=security_logs eventtype=failed_login | eval count as failed_attempts by src_ip | sort -failed_attempts

B. index=security_logs eventtype=failed_login | transaction count as failed_attempts by src_ip | sort -failed_attempts

C. index=security_logs eventtype=failed_login | stats count as failed_attempts by src_ip | sort -failed_attempts

D. index=security_logs eventtype=failed_login | sum count as failed_attempts by src_ip | sort -failed_attempts

Suggested Answer: *C*
Official Answer: C

nosavotor Most Recent 1 year, 11 months ago
Could someone please verify the accuracy of this answer
upvoted 1 times

Question #36 *Topic 1*

The field file_acl contains access controls associated with files affected by an event. In which data model would an analyst find this field?

A. Malware

B. Alerts

C. Vulnerabilities

D. Endpoint

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Could someone help me confirm if this is correct
upvoted 1 times

Question #37 *Topic 1*

A threat hunter generates a report containing the list of users who have logged in to a particular database during the last 6 months, along with the number of times they have each authenticated. They sort this list and remove any user names who have logged in more than 6 times. The remaining names represent the users who rarely log in, as their activity is more suspicious. The hunter examines each of these rare logins in detail.
This is an example of what type of threat-hunting technique?

A. Least Frequency of Occurrence Analysis

B. Co-Occurrence Analysis

C. Time Series Analysis

D. Outlier Frequency Analysis

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 1 times

Question #38 *Topic 1*

What is the main difference between hypothesis-driven and data-driven Threat Hunting?

A. Data-driven hunts always require more data to search through than hypothesis-driven hunts.

B. Data-driven hunting tries to uncover activity within an existing data set, hypothesis-driven hunting begins with a potential activity that the hunter thinks may be happening.

C. Hypothesis-driven hunts are typically executed on newly ingested data sources, while data-driven hunts are not.

D. Hypothesis-driven hunting tries to uncover activity within an existing data set, data-driven hunting begins with an activity that the hunter thinks may be happening.

Suggested Answer: *B*
Official Answer: B

nosavotor Most Recent 1 year, 11 months ago
Could someone please verify the accuracy of this answer
upvoted 1 times

Question #39 *Topic 1*

The Security Operations Center (SOC) manager is interested in creating a new dashboard for typosquatting after a successful campaign against a group of senior executives. Which existing ES dashboard could be used as a starting point to create a custom dashboard?

A. IAM Activity

B. Malware Center

C. Access Anomalies

D. New Domain Analysis

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 1 times

Question #40 *Topic 1*

What is the main difference between a DDoS and a DoS attack?

A. A DDoS attack is a type of physical attack, while a DoS attack is a type of cyberattack.

B. A DDoS attack uses a single source to target a single system, while a DoS attack uses multiple sources to target multiple systems.

C. A DDoS attack uses multiple sources to target a single system, while a DoS attack uses a single source to target a single or multiple systems.

D. A DDoS attack uses a single source to target multiple systems, while a DoS attack uses multiple sources to target a single system.

Suggested Answer: *C*
Official Answer: C

nosavotor Most Recent 1 year, 11 months ago
Could someone help me confirm the correctness of this answer
upvoted 2 times

Question #41 *Topic 1*

A Cyber Threat Intelligence (CTI) team delivers a briefing to the CISO detailing their view of the threat landscape the organization faces. This is an example of what type of Threat Intelligence?

A. Tactical

B. Strategic

C. Operational

D. Executive

Suggested Answer: *B*
Official Answer: B

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 2 times

Question #42 *Topic 1*

An analyst is examining the logs for a web application's login form. They see thousands of failed logon attempts using various usernames and passwords. Internet research indicates that these credentials may have been compiled by combining account information from several recent data breaches.
Which type of attack would this be an example of?

A. Credential sniffing

B. Password cracking

C. Password spraying

D. Credential stuffing

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 1 times

Question #43 *Topic 1*

An analysis of an organization's security posture determined that a particular asset is at risk and a new process or solution should be implemented to protect it. Typically, who would be in charge of designing the new process and selecting the required tools to implement it?

A. SOC Manager

B. Security Engineer

C. Security Architect

D. Security Analyst

Suggested Answer: *C*
Official Answer: C

nosavotor Most Recent 1 year, 11 months ago
Could someone please verify the accuracy of this answer
upvoted 1 times

Question #44 *Topic 1*

After discovering some events that were missed in an initial investigation, an analyst determines this is because some events have an empty src field. Instead, the required data is often captured in another field called machine_name.
What SPL could they use to find all relevant events across either field until the field extraction is fixed?

A. | eval src = coalesce(src,machine_name)

B. | eval src = src + machine_name

C. | eval src = src . machine_name

D. | eval src = tostring(machine_name)

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Could someone help me confirm if this is correct
upvoted 1 times

Question #45 *Topic 1*

An analyst would like to test how certain Splunk SPL commands work against a small set of data. What command should start the search pipeline if they wanted to create their own data instead of utilizing data contained within Splunk?

A. makeresults

B. rename

C. eval

D. stats

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago

I'm not sure about that

upvoted 1 times

Question #46 *Topic 1*

What is the following step-by-step description an example of?

1. The attacker devises a non-default beacon profile with Cobalt Strike and embeds this within a document.
2. The attacker creates a unique email with the malicious document based on extensive research about their target.
3. When the victim opens this document, a C2 channel is established to the attacker's temporary infrastructure on a compromised website.

A. Tactic

B. Policy

C. Procedure

D. Technique

Suggested Answer: *D*

Official Answer: D

Community vote distribution

C (100%)

fufflybunny Most Recent 1 year, 1 month ago

Selected Answer: C

It's procedure

upvoted 1 times

Nss_dfir 1 year, 10 months ago

Selected Answer: C

C. Procedure A procedure is a specific series of steps or actions taken to accomplish a task. In this case, the steps described outline a specific method the attacker uses to carry out their malicious activity, which qualifies as a procedure.

upvoted 2 times

DevinArchie 2 years ago

C. Procedures are the detailed steps that are taken to implement the techniques. The description provided outlines a step-by-step sequence of actions an attacker takes to deploy and execute an attack, which includes creating a beacon profile, crafting a malicious document, and establishing a command and control (C2) channel.

upvoted 2 times

Question #47 *Topic 1*

Which of the following is a best practice when creating performant searches within Splunk?

A. Utilize the transaction command to aggregate data for faster analysis.

B. Utilize Aggregating commands to ensure all data is available prior to Streaming commands.

C. Utilize specific fields to return only the data that is required.

D. Utilize multiple wildcards across fields to ensure returned data is complete and available.

Suggested Answer: *C*

Official Answer: C

Community vote distribution

C (100%)

jeremyleebee Most Recent 5 months ago

Selected Answer: C

Correct Answer: C Reasoning: Splunk's entire training foundation teaches that using specific, detailed fields to return only the data required is the MOST efficient way to utilize Splunk as a whole. If you can exclude irrelevant information from your SPL queries, you will maximize efficiency and therefore improve performant searches within Splunk. Documentation states this a million times.

upvoted 1 times

nosavotor 1 year, 11 months ago

Someone please verify the accuracy of this answer

upvoted 1 times

Question #48 *Topic 1*

Which pre-packaged app delivers security content and detections on a regular, ongoing basis for Enterprise Security and SOAR?

A. SSE

B. ESCU

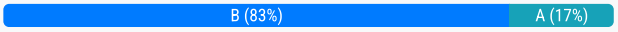
C. Threat Hunting

D. InfoSec

Suggested Answer: *B*

Official Answer: B

Community vote distribution



laurenchristopher Highly Voted 1 year, 1 month ago

Selected Answer: B

While SSE (Splunk Security Essentials) also offers pre-built detections and content, it may not have the same extensive coverage or regular update frequency as ESCU. SSE focuses on providing foundational detections and use cases for establishing a baseline security posture.

upvoted 5 times

fufflybunny 1 year, 1 month ago

Selected Answer: A

it should A. It has most of the components pre-built to be used by SOAR

upvoted 1 times

nosavotor 1 year, 11 months ago

Im not sure how to respond to that

upvoted 1 times

Question #49 *Topic 1*

Which search command allows an analyst to match whatever is inside the parentheses as a single term in the index, even if it contains characters that are usually recognized as minor breakers such as periods or underscores?

A. CASE()

B. LIKE()

C. FORMAT()

D. TERM()

Suggested Answer: *D*
Official Answer: D

nosavotor Most Recent 1 year, 11 months ago
Wildcards are not efficient
upvoted 1 times

Question #50 *Topic 1*

Which field is automatically added to search results when assets are properly defined and enabled in Splunk Enterprise Security?

A. asset_category

B. src_ip

C. src_category

D. user

Suggested Answer: *C*

Official Answer: C

Community vote distribution

A (100%)

laurenchristopher Most Recent 1 year, 1 month ago

Selected Answer: A

It is A. It is predefined and enabled. src_category is not.

upvoted 1 times

CeeCapi 1 year, 9 months ago

A. asset_category In Splunk Enterprise Security, when assets are properly defined and enabled, the asset_category field is automatically added to search results. This field helps categorize assets based on predefined asset groups, providing context and enabling more effective analysis and correlation of security events. The reason C. src_category is not the correct answer is because: src_category is not a default field automatically added by Splunk Enterprise Security when assets are defined. It is not part of the standard asset framework in Splunk ES. asset_category is the correct field because it provides categorization based on the asset framework in Splunk ES, allowing the platform to associate specific attributes or categories with assets in the system. When assets are configured properly, asset_category is added to provide this contextual information. In contrast, src_category is not a recognized field specifically linked to the asset framework in Splunk ES.

upvoted 3 times

nosavotor 1 year, 11 months ago

Is this answer accurate friends

upvoted 1 times

Question #51 *Topic 1*

An IDS signature is designed to detect and alert on logins to a certain server, but only if they occur from 6:00 PM - 6:00 AM. If no IDS alerts occur in this window, but the signature is known to be correct, this would be an example of what?

A. A True Negative.

B. A True Positive.

C. A False Negative.

D. A False Positive.

Suggested Answer: *A*
Official Answer: A

nosavotor Most Recent 1 year, 11 months ago
Is this answer accurate friends
upvoted 1 times