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*

nosavotor 1 month, 4 weeks 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*

Community vote distribution

A (100%)

ProfessorJayy 2 months, 3 weeks 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*

nosavotor 1 month, 4 weeks 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*

zisturordi 6 days, 4 hours 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 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks ago

I'm not sure about that

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*

nosavotor 1 month, 4 weeks 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.

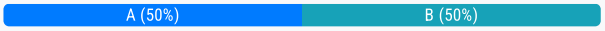
B. Add this information to the risk_message.

C. Create another detection for this information.

D. Allowlist more events based on this information.

Suggested Answer: *A*

Community vote distribution



CeeCapi 3 weeks, 2 days 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 1 times

Nss_dfir 1 month, 3 weeks 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 1 times

ProfessorJayy 2 months, 3 weeks ago

Selected Answer: B

see previous comment

upvoted 1 times

ProfessorJayy 2 months, 3 weeks 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 1 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*

nosavotor 1 month, 4 weeks 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*

Community vote distribution

A (100%)

CeeCapi 3 weeks, 2 days 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 month, 3 weeks 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 1 times

ProfessorJayy 2 months, 3 weeks 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*

CeeCapi 3 weeks, 2 days 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 1 times

nosavotor 1 month, 4 weeks 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*

christophe_ciwr 1 week ago

Selected Answer: D

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

upvoted 1 times

CeeCapi 3 weeks, 2 days 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 month, 1 week ago

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

upvoted 1 times

b14de41 1 month, 1 week ago

Should be "A" for Architect

upvoted 2 times

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

CeeCapi 3 weeks, 2 days 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 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

Community vote distribution

A (50%) C (50%)

CeeCapi 3 weeks, 2 days 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 month, 2 weeks 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 1 times

Nss_dfir 1 month, 2 weeks ago

Selected Answer: A

A. Operational

upvoted 1 times

Nss_dfir 1 month, 2 weeks ago

A. Operational

upvoted 1 times

DevinArchie 3 months ago

Wrong Answer.

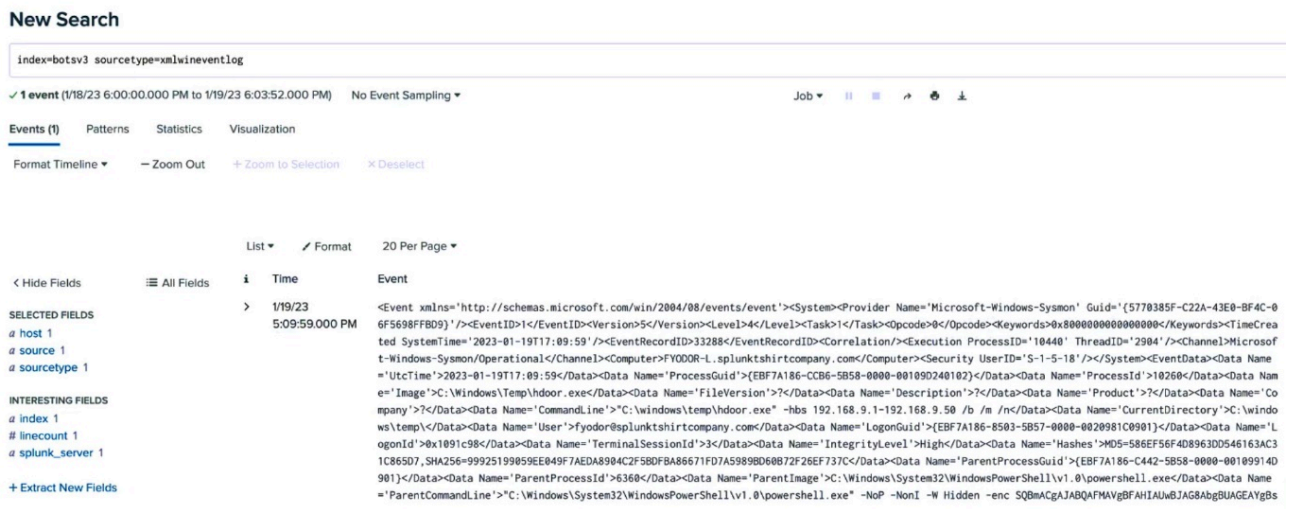
Correct answer is A:

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*

hd14 1 month, 1 week ago

A

I don't think I have field extraction authority.

upvoted 1 times

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks 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*

nosavotor 1 month, 4 weeks ago

Friends could you please confirm this answer

upvoted 1 times