

Splunk

Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst



NEW QUESTION 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

Answer: A

Explanation:

The correct Splunk search that returns results in the most performant way is index=foo host=i-478619733 | stats range(_time) as duration by src_ip | bin duration span=5min | stats count by duration, host. This search is optimized by:

? Starting with the most specific search criteria (index and host) to reduce the data set.

? Applying aggregation functions (stats) early, which helps minimize the amount of data processed in subsequent commands.

? Using binto group data efficiently before performing further statistical calculations.

? Search Optimization:

? Performance Considerations:

? Splunk Search Documentation: The official Splunk documentation provides guidelines on how to construct efficient searches, including the best practices for using stats, bin, and indexing.

? Splunk Performance Tuning Guides: These guides offer in-depth advice on optimizing searches for speed and efficiency, with examples of common pitfalls and how to avoid them.

NEW QUESTION 2

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

Answer: D

Explanation:

Adaptive Response is a feature in Splunk's Enterprise Security (ES) framework that allows security teams to automate actions and responses based on alerts or notable events. This feature is pivotal for orchestrating automated incident response processes, reducing the time between detection and response, and integrating Splunk with external systems to trigger appropriate actions.

? Purpose: Adaptive Response enables the automation of specific tasks or workflows

based on security events detected by Splunk ES. For instance, it can trigger actions such as isolating a compromised host, blocking IP addresses, or enriching data by querying additional sources when a notable event occurs.

? Mechanism: When a notable event is identified within the Splunk platform, Adaptive

Response can execute a series of predefined actions. These actions can be configured within the Splunk interface, allowing them to run automatically or with manual approval depending on the organization's needs. This capability is essential for streamlining security operations, especially in environments where quick response is critical.

? Integration with External Applications: One of the key features of Adaptive

Response is its ability to integrate with third-party security tools and solutions. This integration extends the capabilities of Splunk by allowing it to interact with other systems like firewalls, intrusion prevention systems (IPS), endpoint detection and response (EDR) tools, and ticketing systems. This ensures a coordinated and comprehensive defense mechanism.

? Usage in Security Operations: Security analysts often rely on Adaptive Response

for managing and automating common security tasks, such as:

? Splunk Documentation: Splunk Enterprise Security has detailed guides and resources explaining how Adaptive Response functions within the platform and how to configure and use it effectively. You can access the official documentation for more in-depth technical instructions and examples.

? Splunk Education: Splunk offers training courses specifically for Splunk ES, where Adaptive Response is covered as a key topic. These resources provide practical insights and best practices from experienced Splunk users.

? Security Analyst Community Discussions: Forums and community discussions are excellent resources where analysts share their experiences and configurations using Adaptive Response, often with detailed examples and troubleshooting tips.

References: Adaptive Response is a powerful tool for any Security Operations Center (SOC) aiming to enhance their incident response capabilities, making it a critical feature within Splunk's Enterprise Security framework.

NEW QUESTION 3

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

Answer: D

Explanation:

According to Splunk's Common Information Model (CIM) documentation, when investigating network alerts, the IP address of the host from which an attacker is moving (source) is typically stored in the src_ip field. The host field generally refers to the name of the host that logged the event, dest refers to the destination IP, and src_nt_host refers to the NetBIOS name of the source host. The src_ip field is specifically used to denote the source IP address in the context of network communication, which is critical for tracing lateral movement.

NEW QUESTION 4

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

themost likelycause?

New Search

✓ 1 event (1/18/23 6:00:00.000 PM to 1/19/23 6:03:52.000 PM) No Event Sampling ▾

Job ▾

Events (1)

Patterns

Statistics

Visualization

Format Timeline ▾

— Zoom Out

+ Zoom to Selection

× Deselect

List ▾

Format

20 Per Page ▾

< Hide Fields

All Fields

i Time

Event

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a index 1

linecount 1

a splunk_server 1

+ Extract New Fields

> 1/19/23

5:09:59.000 PM

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FF8D9}" /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2023-01-19T17:09:59"/><EventRecordID>33288</EventRecordID><Correlation><Execution ProcessID="10440" ThreadID="2904"/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>FYODOR-L.splunkshirtcompany.com</Computer><Security UserID="S-1-5-18"/></System><EventData><Data Name="UtcTime">2023-01-19T17:09:59</Data><Data Name="ProcessGuid">{EBF7A186-CCB6-5B58-0000-00109D240102}</Data><Data Name="ProcessId">10260</Data><Data Name="Image">C:\Windows\Temp\hdoor.exe</Data><Data Name="FileVersion">?</Data><Data Name="Description">?</Data><Data Name="Product">?</Data><Data Name="Company">?</Data><Data Name="CommandLine">"C:\windows\temp\hdoor.exe" -hbs 192.168.9.1-192.168.9.50 /b /m /n</Data><Data Name="CurrentDirectory">C:\windows\temp</Data><Data Name="User">fyodor@splunkshirtcompany.com</Data><Data Name="LogonGuid">{EBF7A186-8503-5B57-0000-0020981C0901}</Data><Data Name="LogonId">0x1091c98</Data><Data Name="TerminalSessionId">3</Data><Data Name="IntegrityLevel">High</Data><Data Name="Hashes">MD5=586EF56F4D8963DD546163AC31C865D7,SHA256=99925199059EE049F7AEDA8904C2F58DFBA86671FD7A59898D60B72F26EF737C</Data><Data Name="ParentProcessGuid">{EBF7A186-C442-5B58-0000-00109914D901}</Data><Data Name="ParentProcessId">6360</Data><Data Name="ParentImage">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name="ParentCommandLine">"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc SQBmACgAJABQAFMAVgBFAHIAUwBJAG8AbgBUAGEAYgBs</Data></EventData></Event>

- 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 exctract command to their search pipeline.
D. The analyst is not in the Drooer Search Mode and should switch to Smart or Verbose.

Answer: D

Explanation:

In Splunk, when an analyst is building a search and finds that extracted fields are not appearing, it often relates to the search mode being used. Smart Mode or Verbose Mode are better suited for field extraction as they allow Splunk to automatically extract and display fields based on the data being searched.

? Search Modes in Splunk:

? Incorrect Options:

? Splunk Documentation: Search modes and their impact on field extraction.

NEW QUESTION 5

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

Answer: B

Explanation:

The Risk Framework in Splunk Enterprise Security is designed to raise the threat profile of individuals or assets based on their activities. It allows security teams to assign risk scores to users or devices that engage in suspicious or anomalous behaviors, making it easier to identify entities that may require further investigation.

? Risk Framework:

? Incorrect Options:

? Splunk Documentation: Detailed information on the Risk Framework and how it integrates with other security features in Splunk ES.

NEW QUESTION 6

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

Answer: C

Explanation:

Tactical intelligence provides 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.

? Tactical Intelligence:

? Incorrect Options:

? CTI Frameworks: Standards such as the MITRE ATT&CK framework, which classify tactical intelligence within the spectrum of threat intelligence.

NEW QUESTION 7

Which of the following is a tactic used by attackers, rather than a technique?

- A. Gathering information about a target.
- B. Establishing persistence with a scheduled task.
- C. Using a phishing email to gain initial access.
- D. Escalating privileges via UAC bypass.

Answer: A

Explanation:

Tactics are the overarching objectives or strategies attackers use during their operations, while techniques are the specific methods used to achieve these tactics. In this case, gathering information about a target (often referred to as Reconnaissance) is a tactic because it represents a high-level objective of understanding the target. The other options provided (persistence, phishing, privilege escalation) are specific techniques used to achieve the broader goals or tactics.

NEW QUESTION 8

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.

Answer: D

Explanation:

A threat hunt is an iterative process where a hypothesis is developed and tested against data in an environment to detect the presence of threats or adversarial tactics, techniques, and procedures (TTPs).

? Understanding the Hypothesis:

? Search and Analysis:

? Evaluation of the Hypothesis:

? Successful Threat Hunt:

? MITRE ATT&CK Framework: Understanding how threat actors utilize tactics like Cobalt Strike for C2 can be aligned with TTPs in the framework, helping to build effective hypotheses.

? Threat Hunting Resources: Books like "The Threat Hunter's Handbook" often describe scenarios where proving a negative (i.e., the absence of a threat) is a valid and successful outcome of a hunt.

Outcome of the Threat Hunt: References:

NEW QUESTION 9

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. Moles
- C. Annotations
- D. Framework mapping

Answer: D

Explanation:

Splunk Enterprise Security provides a feature called Framework Mapping that allows correlation searches to be mapped to specific cybersecurity frameworks, including NIST 800-171, which is crucial for DoD contractors. This mapping provides context to the analyst by showing how particular searches align with compliance requirements, aiding in continuous monitoring and reassessment as mandated by the DoD. This feature is integral for organizations that need to demonstrate compliance with NIST guidelines and other security frameworks.

NEW QUESTION 10

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

Answer: C

Explanation:

In Splunk, the rare command is used to return the least common values in a field. This command is particularly useful for anomaly detection, as it helps identify unusual or infrequent occurrences in a dataset, which may indicate potential security issues.

? rare Command:

? Incorrect Options:

? Splunk Command Documentation: rare command usage for identifying uncommon values.

NEW QUESTION 10

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.

Answer: C

Explanation:

The primary difference between a Distributed Denial of Service (DDoS) attack and a Denial of Service (DoS) attack is in the source of the attack. A DDoS attack involves multiple compromised systems (often part of a botnet) attacking a single target, overwhelming it with traffic or requests. In contrast, a DoS attack typically involves a single source attacking the target. The goal of both attacks is to make a service unavailable, but DDoS attacks are usually more difficult to defend against because of their distributed nature.

NEW QUESTION 15

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)`

Answer: A

Explanation:

The `coalesce` function in Splunk is used to return the first non-null value from a list of fields. The SPL `| eval src = coalesce(src,machine_name)` allows the analyst to dynamically populate the `src` field with the value from `machine_name` if `src` is empty. This is a useful technique when dealing with inconsistent data sources or during field extraction issues, ensuring that the analyst can continue their investigation without missing critical events.

NEW QUESTION 16

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

Answer: D

Explanation:

The scenario describes an attack where thousands of failed login attempts are made using various usernames and passwords, which is indicative of a Credential Stuffing attack. This type of attack involves using lists of stolen credentials (usernames and passwords) obtained from previous data breaches to attempt to gain unauthorized access to user accounts. Attackers take advantage of the fact that many users reuse passwords across multiple sites. Unlike Password Spraying (which tries a few common passwords against many accounts) or Password Cracking (which tries to guess or decrypt passwords), credential stuffing leverages large datasets of valid credentials obtained from other breaches.

Top of Form Bottom of Form

NEW QUESTION 17

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SPLK-5001 Practice Exam Features:

- * SPLK-5001 Questions and Answers Updated Frequently
- * SPLK-5001 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-5001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-5001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-5001 Practice Test Here](#)