Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

https://www.2passeasy.com/dumps/SPLK-5001/

NEW QUESTION 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 ()

Answer: D

Explanation:
TheTERM()search command in Splunk allows an analyst to match a specific term exactly as it appears, even if it contains characters that are usually considered minor breakers, such as periods or underscores. By usingTERM(), the search engine treats everything inside the parentheses as a single term, which is especially useful for searching log data where certain values (like IP addresses or filenames) should be matched exactly as they appear in the logs.

NEW QUESTION 2
Which of the following is not considered an Indicator of Compromise (IOC)?

A. A specific domain that is utilized for phishing.
B. A specific IP address used in a cyberattack.
C. A specific file hash of a malicious executable.
D. A specific password for a compromised account.

Answer: D

Explanation:
Indicators of Compromise (IOCs) are artifacts that are used to identify potential malicious activity within a network or system. Common IOCs include domains, IP addresses, and file hashes that are associated with malicious activity. However, a specific password, while potentially sensitive, is not typically considered an IOC because it is more of a credential than an artifact indicating a compromise. IOCs are used to detect and respond to threats, while compromised credentials are a result of those threats.

NEW QUESTION 3
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

Answer: B

Explanation:
TheEnterprise Security Content Update (ESCU)app is a pre-packaged app that delivers security content and detections on a regular, ongoing basis for Splunk Enterprise Security (ES) and Splunk SOAR. ESCU provides regular updates with new correlation searches, dashboards, and other content that help organizations stay up-to-date with the latest threats and detection techniques. This app is specifically designed to enhance the capabilities of Splunk ES by providing out-of-the-box security content that can be customized and used immediately.

NEW QUESTION 4
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 thesrc_ipfield. Thehostfield generally refers to the name of the host that logged the event,destrefers to the destination IP, andsrc_nt_hostrefers to the NetBIOS name of the source host. Thesrc_ipfield is specifically used to denote the source IP address in the context of network communication, which is critical for tracing lateral movement.

NEW QUESTION 5
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.

Answer: A

Explanation:
In the context of Intrusion Detection Systems (IDS), determining whether an event is a True Negative, True Positive, False Negative, or False Positive depends on the system's detection and the reality of the situation.
Let's break down the scenario: IDS Signature Explanation:
The IDS is set to detect and alert on logins to a server, but only if they happen during a specific time window, from 6:00 PM to 6:00 AM.
The question states that no alerts occur during this time frame, but the IDS signature is known to be correct.
Understanding Detection Terms:
True Positive: The IDS correctly detects an intrusion or suspicious activity that is actually happening.
True Negative: The IDS does not detect any activity because no suspicious or malicious activity is occurring, and this lack of detection is correct.
False Positive: The IDS detects an intrusion or activity, but it is a false alarm (i.e., there is no real threat).
False Negative: The IDS fails to detect a real intrusion or activity when it should have, missing a legitimate alert.
Applying the Scenario:
In this case, no IDS alerts occurred during the specified time frame. If there were no actual logins during this period and the signature was designed correctly, then the absence of alerts is expected and appropriate.
Since no suspicious logins occurred, and the IDS did not trigger any alerts, this situation represents a True Negative—the system correctly identified that there was no suspicious activity to alert on.
Why the Answer is "True Negative":
The IDS signature is working as expected.
The condition that would trigger an alert (logins during the specified time) did not happen, so the lack of alerts is a correct response.
Therefore, this is classified as a True Negative because no malicious activity took place, and the IDS correctly refrained from raising an alert.
Comparison to Other Options:
* B. True Positive – This would indicate that an alert occurred because of actual suspicious activity, but in this case, no alerts occurred.
* C. False Negative – This would mean that suspicious activity occurred, but the IDS failed to detect it. In this case, there was no activity to detect, so this option is not correct.
* D. False Positive – This would suggest the IDS raised an alert when no suspicious activity happened, but again, no alerts occurred, so this doesn??t apply.
References:
Cybersecurity analysts working with IDS systems frequently use concepts like True Negative and False Positive in evaluating the effectiveness of their detection tools.
The correct handling of such detection cases is critical to minimizing unnecessary alerts (False Positives) and ensuring real threats are not missed (avoiding False Negatives).

NEW QUESTION 6
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

Answer: C

Explanation:
? Continuous Monitoring Cycle:This cycle is part of a broader security strategy that involves constantly assessing and managing the security state of an organization's information systems. The phases generally include defining metrics, collecting data, analyzing it, reporting findings, and implementing improvements.
? Analyze and Report Phase:
? Purpose of Recommendations:The goal of this phase is to ensure that the organization??s security measures are continuously improved based on the latest data and threat landscape. It is a critical step in maintaining an effective security program that adapts to new challenges.
? NIST SP 800-137:This publication provides guidelines on continuous monitoring of information systems, detailing the processes involved, including the Analyze and Report phase.
? Security Operations Center (SOC) Best Practices:Many SOC frameworks emphasize the importance of the Analyze and Report phase in

NEW QUESTION 7
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

Answer: B

Explanation:
In Splunk, to filter users with over a thousand occurrences, the pipeline| stats count by user | where count > 1000 | sort - countis most effective. Thestats count by usercommand generates a count of occurrences for each user. Thewhereclause then filters out only those users who have more than 1000 occurrences. Finally,sort - countsorts the results in descending order by count. This approach is efficient for identifying outliers, such as users with a high number of events.

NEW QUESTION 8
An analyst investigates an IDS alert and confirms suspicious traffic to a known malicious IP. What Enterprise Security data model would they use to investigate which process initiated the network connection?

A. Endpoint
B. Authentication
C. Network traffic
D. Web

Answer: A

Explanation:
To investigate which process initiated a network connection, an analyst would use theEndpointdata model in Splunk Enterprise Security. The Endpoint data model

contains fields related to processes, file activity, and host-level data, which are essential for tracing back the source of suspicious network activity to the specific process or application that initiated it. This is crucial for understanding the scope of an attack and determining the origin of malicious network traffic.
Top of Form Bottom of Form

NEW QUESTION 9
Which of the following is a best practice for searching in Splunk?

A. Streaming commands run before aggregating commands in the Search pipeline.
B. Raw word searches should contain multiple wildcards to ensure all edge cases are covered.
C. Limit fields returned from the search utilizing the cable command.
D. Searching over All Time ensures that all relevant data is returned.

Answer: A

Explanation:
In Splunk,streaming commandsprocess each event individually as it is passed through the search pipeline and should be placed beforeaggregating commands, which operate on the entire set of results at once. This best practice ensures efficient processing and minimizes resource usage, as streaming commands reduce the amount of data before aggregation occurs. This approach leads to faster and more efficient searches. In contrast, the other options, such as using wildcards excessively or searching over all time, can lead to performance issues and excessive data processing.

NEW QUESTION 10
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 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.
? 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 10
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. Escalatingprivileges via UAC bypass.

Answer: A

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

NEW QUESTION 13
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

Answer: D

Explanation:
Thefile_aclfield, which contains access controls associated with files affected by an event, is part of theEndpointdata model in Splunk. The Endpoint data model is designed to include information related to file access, process activity, and user activity on endpoints. Fields likefile_aclare critical for understanding permissions and potential security risks associated with file access and manipulation, which are key aspects of endpoint security monitoring.

NEW QUESTION 14
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

Answer:

C

Explanation:
In Splunk Enterprise Security, when assets are properly defined and enabled, the fieldsrc_categoryis automatically added to search results. This field categorizes the source IP addresses according to their asset classification, which helps in analyzing and filtering search results based on the type of assets involved in an event. Proper asset and identity management within Splunk ES enhances the ability to contextualize and prioritize security incidents.

NEW QUESTION 19
An analyst is looking at Web Server logs, and sees the following entry as the last web request that a server processed before unexpectedly shutting down:
147.186.119.107 - - [28/Jul/2006:10:27:10 -0300] "POST /cgi-bin/shutdown/ HTTP/1.0" 200 3333
What kind of attack is most likely occurring?

A. Distributed denial of service attack.
B. Denial of service attack.
C. Database injection attack.
D. Cross-Site scripting attack.

Answer: B

Explanation:
The log entry indicates aPOST /cgi-bin/shutdown/request, which suggests that a command was sent to shut down the server via a CGI script. This kind of activity is indicative of aDenial of Service (DoS) attackbecause it involves sending a specific command that causes the server to stop functioning or shut down. This is different from a Distributed Denial of Service (DDoS) attack, which typically involves overwhelming the server with traffic rather than exploiting a specific command.

NEW QUESTION 20
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, therarecommand 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 24
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

Answer: D

Explanation:
The step-by-step description provided is an example of aTechniqueas defined in the MITRE ATT&CK framework. Techniques are the specific methods adversaries use to achieve their objectives during an attack, such as establishing command and control (C2) channels or delivering payloads via phishing emails. In this scenario, the attacker uses a non-default beacon profile in Cobalt Strike, sends a malicious document via email, and establishes a C2 channel once the victim interacts with the document, all of which are examples of adversary techniques.

NEW QUESTION 26
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:
Thecoalescefunction 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 thesrcfield with the value frommachine_nameifsrcis 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 30
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

Answer: D

Explanation:
In Splunk??s Risk-Based Alerting (RBA) framework, aRisk Objectrefers to the specific entity (such as a user account, IP address, or host) that is associated with risk observations. When auser account generates multiple risk observations, it is labeled as a Risk Object, allowing security teams to track and manage risk more effectively.
? Risk Object:
? Incorrect Options:
? Splunk RBA Documentation:Detailed descriptions of how Risk Objects function within the Risk-Based Alerting framework.

NEW QUESTION 34
The eval SPL expression supports many types of functions. Which of these function categories is not valid with eval?

A. JSON functions
B. Text functions
C. Comparison and Conditional functions
D. Threat functions

Answer: D

Explanation:
TheevalSPL expression in Splunk supports several categories of functions, includingJSON functions(e.g.,spath),Text functions(e.g.,substr,trim), andComparison and Conditional functions(e.g.,if,case). However,Threat functionsis not a valid category within theevalcommand. Theevalcommand is primarily used for transforming and manipulating data in various ways, but it does not include a category specifically for threat-related functions.

NEW QUESTION 36
Which of the following is not a component of the Splunk Security Content library (ESCU, SSE)?

A. Dashboards
B. Reports
C. Correlation searches
D. Validated architectures

Answer: D

Explanation:
The Splunk Security Content library, which includes apps like ESCU (Enterprise Security Content Update) and SSE (Splunk Security Essentials), primarily consists of Dashboards, Reports, and Correlation Searches.Validated architecturesare not a component of these content libraries. Instead, validated architectures refer to predefined, best-practice designs for deploying and configuring Splunk in a way that ensures optimal performance and scalability,which is separate from the content libraries focused on delivering security detections and visualizations.
Top of Form Bottom of Form

NEW QUESTION 37
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

Answer: D

Explanation:
The Lockheed Martin Cyber Kill Chain® is a widely recognized framework that breaks down the stages of a cyber attack. The stages are: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. The scenario described—modifying the registry on a compromised Windows system to ensure malware runs at boot time—fits into theInstallationphase. This phase involves placing a persistent backdoor or other malicious software on the victim's system, ensuring it can be executed again, even after a system reboot. By modifying the registry, the attacker is achieving persistence, a classic example of the Installation phase.

NEW QUESTION 38
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-5001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-5001 Product From:

https://www.2passeasy.com/dumps/SPLK-5001/

Money Back Guarantee

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