Splunk

Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

NEW QUESTION 1
While testing the dynamic removal of credit card numbers, an analyst lands on using therexcommand. What mode needs to be set to in order to replace the defined values with X?

```
| makeresults
| eval ccnumber="511388720478619733"
| rex field=ccnumber mode=???"s/(\d{4}-){3)/XXXX-XXXX-XXXX-/g"
```

Please assume that the aboverexcommand is correctly written.

A. sed
B. replace
C. mask
D. substitute

Answer: A

Explanation:
Therexcommand in Splunk can be used to extract or replace data using regular expressions. To dynamically replace values with a specific pattern, such as replacing credit card numbers with "X", the mode needs to be set tosed. Thesedmode allows for string replacement within a field using regular expressions, enabling the substitution of matching patterns with a specified string.

NEW QUESTION 2
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 3
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 4
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

Answer: D

Explanation:
The MITRE ATT&CK framework categorizes Tactics, Techniques, and Procedures (TTPs) used by attackers. It is a globally accessible knowledge base of adversarial tactics and techniques based on real-world observations, and it is widely used by cybersecurity professionals to understand and defend against various cyber threats.
? Tactics, Techniques, and Procedures (TTPs):
? MITRE ATT&CK Framework:MITRE ATT&CK organizes these TTPs into a matrix that reflects different stages of an attack lifecycle, from initial access to exfiltration. The framework helps security teams by:
? Why MITRE ATT&CK:Unlike compliance-focused frameworks like NIST 800-53 or ISO 27000, which provide security controls and best practices, MITRE ATT&CK is specifically focused on the behavior of adversaries. This focus makes it an invaluable resource for understanding how attacks unfold and how to counteract them.
? MITRE ATT&CK Website:The official site provides detailed information on each tactic and technique, along with examples of how they have been used in real-world attacks.
? Threat Intelligence Platforms:Many platforms integrate with MITRE ATT&CK, providing enhanced detection and response capabilities by mapping security events to the framework.
? Security Research Papers:Numerous papers and reports analyze specific attacks using the ATT&CK framework, offering insights into its practical applications in cybersecurity defense.
References:MITRE ATT&CK is a foundational tool in modern cybersecurity, providing a detailed and actionable understanding of adversary behaviors that can be

directly applied to enhance an organization's defensive posture.

NEW QUESTION 5
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 6
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 7
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 8
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.

Answer: A

Explanation:
In Splunk, field extractions are essential for transforming raw log data into structured fields that are easier to work with during analysis. When the question refers to an analyst identifying helpful information in the raw logs that assists them in determining suspicious activity, the most effective way to streamline this process is throughfield extraction. This allows the Splunk system to automatically parse and tag the necessary data, making it more accessible for searches, dashboards, and alerts.
Let??s break down whyoption A: Create a field extraction for this informationis the best approach:
? Field Extraction Overview:
? Why Field Extraction?
? Comparison to Other Options:
? Cybersecurity Defense Analyst Best Practices:
References:
? Splunk Documentation: Field Extraction in Splunk
? Cybersecurity defense techniques emphasize the importance of making log data actionable, which aligns with common practices in Incident Detection & Response (IDR) environments. Structured data is key to this effort, and field extraction is a critical part of transforming raw logs into useful intelligence

NEW QUESTION 9
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 10
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 10
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

Answer: D

Explanation:
For creating a custom dashboard focused on typosquatting, theNew Domain Analysisdashboard in Splunk Enterprise Security (ES) would be a relevant starting point. Typosquatting typically involves the registration of domains similar to legitimate domains to deceive users, which is closely related to the analysis of newly registered or observed domains. This dashboard already includes tools and visualizations for monitoring and analyzing domain name activity, which can be adapted for the specific needs of monitoring for typosquatting.

NEW QUESTION 12
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

Answer: A

Explanation:
The scenario described is an example ofLeast Frequency of Occurrence Analysis. This threat-hunting technique focuses on identifying events or behaviors that occur infrequently, under the assumption that rare activities could indicate abnormal or suspicious behavior. By filtering out users who log in frequently and focusing on those with rare login attempts, the threat hunter aims to identify potentially suspicious activity that warrants further investigation. This technique is particularly effective in detecting stealthy attacks that might evade more common detection methods.
Top of Form Bottom of Form

NEW QUESTION 17
According to Splunk CIM documentation, which field in the Authentication Data Model represents the user who initiated a privilege escalation?

A. username
B. src_user_id
C. src_user

D. dest_user

Answer: C

Explanation:
According to Splunk CIM (Common Information Model) documentation, thesrc_userfield in the Authentication Data Model represents the user who initiated an action, including privilege escalation. This field is used to track the source user responsible for generating an authentication event, which is critical in understanding and responding to potential security incidents involving privilege escalation. The other fields likedest_userorusernamehave different roles, focusing on the target of the action or the general username involved.
Top of Form Bottom of Form

NEW QUESTION 20
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 24
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 aCredential Stuffingattack. 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. UnlikePassword Spraying(which tries a few common passwords against many accounts) orPassword 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 25
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.

Answer: D

Explanation:
In Splunk Enterprise Security, theRisk Event Timelineprovides a chronological view of risk events associated with a particular Risk Object, such as a user or device. This timeline helps analysts visualize and understand the sequence and nature of risk events over time, aiding in the investigation of security incidents.
? Risk Event Timeline:
? Incorrect Options:
? Splunk Documentation:Risk Event Timeline in Splunk Enterprise Security provides step-by-step details on how to access and interpret the timeline.

NEW QUESTION 26
......