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.
? Usingbinto 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 usingstats,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 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.

Answer: C

Explanation:
When creating performant searches in Splunk, it is a best practice to utilize specific fields to return only the data that is required. This approach minimizes the amount of data processed and speeds up search performance. By explicitly specifying the fields of interest using commands likefields, you reduce the overhead on Splunk??s processing engine, leading to faster and more efficient queries. In contrast, using wildcards or overly broad searches can lead to slower performance due to the increased data volume being processed.
Top of Form Bottom of Form

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 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 4
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 5
The following list contains examples of Tactics, Techniques, and Procedures (TTPs):
* 1. Exploiting a remote service
* 2. Lateral movement

* 3. Use EternalBlue to exploit a remote SMB server In which order are they listed below?

A. Tactic, Technique, Procedure
B. Procedure, Technique, Tactic
C. Technique, Tactic, Procedure
D. Tactic, Procedure, Technique

Answer: A

Explanation:
The examples provided correspond to Tactics, Techniques, and Procedures (TTPs) in the following order:
? Lateral movement– This is aTactic. Tactics represent the goals or objectives of an adversary, such as moving laterally within a network to gain broader access.
? Exploiting a remote service– This is aTechnique. Techniques are specific methods used to achieve a tactic, such as exploiting a service to move laterally.
? Use EternalBlue to exploit a remote SMB server– This is aProcedure. Procedures are the detailed steps or specific implementations of a technique, such as using the EternalBlue exploit to target SMB vulnerabilities.
Thus, the correct order isTactic, Technique, Procedure.

NEW QUESTION 6
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

Answer: D

Explanation:
AnIntrusion Detection System (IDS)typically sits at the network perimeter and is designed to detect suspicious traffic, including command and control (C2) traffic and other potentially malicious activities.
? Intrusion Detection Systems:
? Incorrect Options:
? Network Security Practices:IDS implementation is a standard practice for perimeter security to detect early signs of network intrusion.

NEW QUESTION 7
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

Answer: A

Explanation:
Splunk Answersis a community-driven Q&A platform where users can ask questions and share knowledge about Splunk. It is known for providing community-sourced answers to a wide rangeof questions, including SPL (Search Processing Language) queries, configuration issues, and general best practices. Users can contribute by answering questions based on their own experiences, making it a valuable resource for troubleshooting and learning.
? B. Splunk Lantern:This is a resource for best practices, how-tos, and use case guides, but it??s not a community-sourced Q&A platform.
? C. Splunk Guidebook:This is not a known resource in the context of community- sourced answers.
? D. Splunk Documentation:While highly detailed and official, it is not community- sourced but rather maintained by Splunk's own teams.
? Splunk Answers Platform:Splunk Answers
Incorrect Options:References:

NEW QUESTION 8
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

Answer: C

Explanation:
In most organizations, the Security Engineer is typically responsible for implementing new processes or solutions that have been selected to protect assets. This role involves the practical application of security tools, technologies, and practices to safeguard the organization??s infrastructure and data.
? Role of Security Engineer:
? Contrast with Other Roles:
? Job Descriptions and Industry Standards:Detailed descriptions of Security Engineer roles in job postings and industry standards highlight their responsibilities in implementing security solutions.
? Security Operations Best Practices:These documents and guidelines often outline the division of responsibilities in a security team, confirming that Security Engineers are the primary implementers.

NEW QUESTION 9
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 10
Which of the following data sources can be used to discover unusual communication within an organization??s network?

A. EDS
B. Net Flow
C. Email
D. IAM

Answer: B

Explanation:
NetFlow data is a powerful data source for monitoring and analyzing network traffic patterns within an organization. It provides detailed information about the flow of data between devices on a network, including source and destination IP addresses, ports, and protocols. By analyzing NetFlow data, security analysts can detect unusual communication patterns that may indicate malicious activity, such as lateral movement, data exfiltration, or communication with command and control servers. Other options like EDS (Endpoint Detection Systems), Email, and IAM (Identity and Access Management) are also valuable, but NetFlow is specifically designed for network traffic analysis.
Top of Form Bottom of Form

NEW QUESTION 10
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

Answer: A

Explanation:
Splunk Enterprise Security (ES) provides various features to enhance security monitoring, analysis, and incident response. One of the powerful features in Splunk ES isAnnotations. This feature allows security analysts to map and categorize correlation search results according to well-known industry frameworks such as the CIS Critical Security Controls, MITRE ATT&CK, and the Lockheed Martin Cyber Kill Chain®.
? Purpose of Annotations:
? How Annotations Work:
? Integration with Frameworks:
Annotations in Splunk ES:Practical Example:Consider a correlation search that detects unusual behavior indicating potential lateral movement within a network. If this alert is annotated with a reference to the MITRE ATT&CK framework, it might map to techniques like "T1021 - Remote Services," which is associated with the lateral movement tactic. This mapping not only categorizes the event but also helps in planning the next steps for containment and investigation.
? Efficiency in Response:By aligning alerts with industry frameworks, annotations
help in quickly identifying the nature and potential impact of a threat.
? Consistency in Analysis:Provides a standardized method for categorizing and responding to alerts, ensuring that all analysts interpret and react to threats in a consistent manner.
? Improved Reporting:Allows for better visualization and reporting of threats according to established frameworks, making it easier to communicate risks and actions to stakeholders.
? Splunk Documentation:Annotations in Splunk ES
? MITRE ATT&CK Framework:MITRE ATT&CK®
? Lockheed Martin Cyber Kill Chain®:Cyber Kill Chain
? CIS Critical Security Controls:CIS Controls
Why Annotations Are Important:References:

NEW QUESTION 13
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

Answer: C

Explanation:
In an organization, theSecurity Architectis typically responsible for designing new processes or selecting the tools necessary to protect assets that are identified as being at risk. The Security Architect has the expertise to design a comprehensive security solution that addresses the specific needs of the organization, considering various factors like existing infrastructure, threatlandscape, and compliance requirements. They work closely with other roles, such as Security Engineers, to implement these solutions.

NEW QUESTION 16
Which of the Enterprise Security frameworks provides additional automatic context and correlation to fields that exist within raw data?

A. Asset and Identity
B. Threat Intelligence
C. Adaptive Response
D. Risk

Answer: A

Explanation:
TheAsset and Identityframework within Splunk Enterprise Security provides additional automatic context and correlation to fields that exist within raw data. By associating IP addresses, usernames, and other identifiers with known assets and identities within the organization, this framework enhances the context of security events and facilitates moreaccurate and meaningful analysis. This allows analysts to better understand the impact of security incidents and to prioritize their responses based on the criticality of the assets involved.
Top of Form Bottom of Form

NEW QUESTION 19
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

Answer: A

Explanation:
? Unusual Traffic Patterns:
? Possible Threat Activities:
Scenario Analysis:Conclusion:Given the evidence of large data transfers to a single external system without corresponding inbound traffic,data exfiltrationis the most likely scenario. This suggests that an adversary has compromised the server and is extracting valuable or sensitive data from the organization.
? Data Exfiltration Techniques:Techniques such as those documented in the MITRE
ATT&CK framework (e.g.,T1041 - Exfiltration Over C2 Channel) detail how attackers move data out of a network.
? Incident Response Playbooks:Many incident response frameworks emphasize monitoring for unusual outbound traffic as a primary indicator of data exfiltration.

NEW QUESTION 20
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

Answer: C

Explanation:
Thestatscommand is used to generate statistics, such as counts, over specific fields. In this case, the commandindex=security_logs eventtype=failed_login | stats count as failed_attempts by src_ip | sort -failed_attemptscreates a temporary table that counts the number of failed login attempts (failed_attempts) for each source IP (src_ip). Thesort -failed_attemptsensures the results are ordered by the number of failed attempts in descending order, making it easier for an analyst to identify problematic IPs.

NEW QUESTION 21
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

Answer: A

Explanation:

Themakeresultscommand in Splunk is used to generate a single-row result that can be used to create test data within a search pipeline. This command is particularly useful for testing and experimenting with SPL commands on a small set of synthetic data without relying on existing logs or events in the Splunk index. It is commonly used by analysts who want to test commands or SPL syntax before applying them to real data.

NEW QUESTION 25
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.

Answer: D

Explanation:
An executable running from theC:\Windows\Tempdirectory is a significant red flag because temporary directories are often world writable, meaning any user or process can write files to them. This characteristic makes these directories an attractive
target for attackers who want to drop, stage, and execute malware without worrying about restrictive file permissions.
? Temp Directories Characteristics:
? Security Risks:
? Investigation Importance:The fact that an executable is running fromC:\Windows\Tempwarrants further investigation to determine whether it is malicious. Analysts should check:
? Windows Security Best Practices:Documentation on how to secure temp directories and monitor for suspicious activity is available from both Microsoft and various security communities.
? Incident Response Playbooks:Many playbooks include steps for investigating suspicious activity in temp directories as part of broader malware detection and response strategies.
? MITRE ATT&CK Framework:Techniques involving the use of temporary directories are well-documented in the framework, offering insights into how adversaries leverage these locations during an attack.

NEW QUESTION 28
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 29
An analyst is attempting to investigate a Notable Event within Enterprise Security. Through the course of their investigation they determined that the logs and artifacts needed to investigate the alert are not available.
What event disposition should the analyst assign to the Notable Event?

A. Benign Positive, since there was no evidence that the event actually occurred.
B. False Negative, since there are no logs to prove the activity actually occurred.
C. True Positive, since there are no logs to prove that the event did not occur.
D. Other, since a security engineer needs to ingest the required logs.

Answer: D

Explanation:
In this scenario, the analyst cannot conclude whether the Notable Event is a true positive or a false positive due to the absence of necessary logs and artifacts. The appropriate eventdisposition in this case is "Other," as it indicates that further action is required, such as ingesting the missing logs. The involvement of a security engineer to ensure the necessary data is available for proper investigation is implied, making "Other" the most suitable option.

NEW QUESTION 31
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)

Answer: A

Explanation:
In incident response and cybersecurity operations, Mean Time to Respond (MTTR) is a key metric. It measures the average time it takes from when an alert is created to when it is resolved or closed. In the scenario, an analyst identifies a Risk Notable Event as a false positive and closes it; the time taken from the alert's creation to its closure is what MTTR measures. This metric is crucial in understanding how efficiently a security team responds to alerts and incidents, thus contributing to overall security posture improvement.

NEW QUESTION 33
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 35
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 40
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

Answer: A

Explanation:
In Splunk, therexcommand is used to extract fields from raw event data using regular expressions. This command allows analysts to dynamically extract additional fields as part of a search pipeline, which is crucial for creating new fields during search time based on specific patterns found in the log data. Therexcommand is highly flexible and powerful, making it essential for refining and manipulating data in a Splunk environment. The other options (fields,regex,eval) have their uses, butrexis specifically designed for dynamic field extraction.

NEW QUESTION 42
......