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
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

Answer: A

Explanation:
Hacktivismrefers to the use of hacking techniques by an Advanced Persistent Threat (APT) group to promote a political agenda or social cause. Unlike other motivations such as financial gain or espionage, the primary goal of hacktivism is to disrupt, damage, or deface systems to draw attention to a cause or to protest against something the group opposes.
? Hacktivism:
? Incorrect Options:
? Cybersecurity Literature:Books and articles on APT motivations often highlight hacktivism as a distinct category with a focus on ideological or political goals.

NEW QUESTION 3
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 4
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 integrationextends 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 5
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 6
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 7
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 8
Which of the following use cases is best suited to be a Splunk SOAR Playbook?

A. Forming hypothesis for Threat Hunting
B. Visualizing complex datasets.
C. Creating persistent field extractions.
D. Taking containment action on a compromised host

Answer: D

Explanation:
Splunk SOAR (Security Orchestration, Automation, and Response) playbooks are designed to automate security tasks, makingtaking containment action on a compromised hostthe best-suited use case. A SOAR playbook can automate the response actions such as isolating a host, blocking IPs, or disabling accounts, based on predefined criteria. This reduces response time and minimizes the impact of security incidents. The other options, like forming hypotheses for threat hunting or visualizing datasets, are more manual processes and less suited for automation via a playbook.

NEW QUESTION 9
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 10
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
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 14
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 18
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 22
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. NetworM-lost artifacts
D. Hash values

Answer: D

Explanation:
? Pyramid of Pain Overview:The Pyramid of Pain categorizes indicators based on how difficult they are for attackers to alter:
? Why Hash Values Are Least Effective:
? David Bianco's Pyramid of Pain Blog Post:Bianco??s original post and related materials provide a deep dive into why hash values are the least effective and why focusing on higher-level indicators is more impactful for security operations.
? Threat Intelligence Reports:Many reports emphasize the importance of focusing on TTPs over simpler indicators like hash values to build a more resilient detection and response strategy.

NEW QUESTION 24
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 28
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 32
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 33
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 35
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 40

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 45
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 50
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 53
A Cyber Threat Intelligence (CTI) team delivers a briefing to the CISO detailing their view of the threat landscape the organization faces. This is an example of what type of Threat Intelligence?

A. Tactical
B. Strategic
C. Operational
D. Executive

Answer: B

Explanation:
A briefing delivered by a Cyber Threat Intelligence (CTI) team to a Chief Information Security Officer (CISO) detailing the overall threat landscape is an example ofStrategicThreat Intelligence. Strategic intelligence focuses on high-level analysis of broader trends, threat actors, and potential risks to the organization over time. It is designed to inform senior leadership and influence long-term security strategies and policies. This contrasts withTacticalintelligence, which deals with immediate threats and actionable information, andOperationalintelligence, which is more focused on the details of specific threat actors or campaigns.

NEW QUESTION 56
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.

Answer: D

Explanation:
Notable Events in Splunk Enterprise Security are configured as part of a correlation search, where an Adaptive Response Action can be set to create a Notable Event when certain conditions are met. These correlation searches are pre-defined or custom searches that look for specific patterns of interest, such as security incidents or anomalies. The use of Adaptive Response Actions within these searches allows for the automated creation of Notable Events, which can then be investigated by security analysts. This configuration is a crucial part of Splunk's security operations capabilities.

NEW QUESTION 60
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 65
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 69
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 74
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 78
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 81
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 86
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 88
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 90
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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