Splunk

Exam Questions SPLK-5001

Splunk Certified Cybersecurity Defense Analyst

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 of the following is considered Personal Data under GDPR?

A. The birth date of an unidentified user.
B. An individual's address including their first and last name.
C. The name of a deceased individual.
D. A company's registration number.

Answer: B

Explanation:
Under the General Data Protection Regulation (GDPR), Personal Data is any information relating to an identified or identifiable natural person. An individual's address, combined with their first and last name, clearly identifies a person, making it Personal Data under GDPR. The other options provided do not meet the GDPR criteria for Personal Data: the birth date of an unidentified user does not identify a person, the name of a deceased individual is not covered under GDPR, and a company??s registration number pertains to an entity rather than a natural person.
Top of Form Bottom of Form

NEW QUESTION 4
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 5
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 6
Splunk Enterprise Security has numerous frameworks to create correlations, integrate threat intelligence, and provide a workflow for investigations. Which framework raises the threat profile of individuals or assets to allow identification of people or devices that perform an unusual amount of suspicious activities?

A. Threat Intelligence Framework
B. Risk Framework
C. Notable Event Framework
D. Asset and Identity Framework

Answer: B

Explanation:
TheRisk Frameworkin Splunk Enterprise Security is designed to raise the threat profile of individuals or assets based on their activities. It allows security teams to assign risk scores to users or devices that engage in suspicious or anomalous behaviors, making it easier to identify entities that may require further investigation.
? Risk Framework:
? Incorrect Options:
? Splunk Documentation:Detailed information on the Risk Framework and how it integrates with other security features in Splunk ES.

NEW QUESTION 7
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 8
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 9
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 10

Which of the following is the primary benefit of using the CIM in Splunk?

A. It allows for easier correlation of data from different sources.
B. It improves the performance of search queries on raw data.
C. It enables the use of advanced machine learning algorithms.
D. It automatically detects and blocks cyber threats.

Answer: A

Explanation:
The Common Information Model (CIM) in Splunk is a crucial component that allows for the normalization and standardization of data across various sources. By using CIM, disparate data sources can be mapped to a common schema, which makes it significantly easier to correlate and analyze data across different logs and systems.
? Purpose of CIM:CIM provides a standardized format for fields and event types
across various data sources in Splunk. This normalization allows analysts to use consistent field names and structures when performing searches, regardless of the original data source's format.
? Benefit of Easier Correlation:One of the primary challenges in security operations
is correlating data from different sources—like firewalls, intrusion detection systems (IDS), endpoint security solutions, and network logs—to identify potential security incidents. CIM facilitates this by ensuring that all relevant data adheres to a common schema, enabling seamless correlation and analysis. For example, CIM allows a security analyst to write a single query that can apply to data from multiple sources, simplifying the detection of complex threats.
? How it Works:CIM is implemented through data models in Splunk, which act as a
blueprint for mapping and transforming raw data into a structured format. These data models cover a wide range of security domains, such as authentication, network traffic, and malware, ensuring that data from different security tools can be
easily integrated and analyzed together.
? Use Cases:The primary use cases for CIM include:
? Splunk CIM Documentation:The official documentation provides comprehensive guides on how to implement and use CIM for various data sources, including detailed field mappings and examples.
? Splunk Security Essentials:This resource offers practical examples and pre-built use cases that utilize CIM for effective security operations.
? Community Blogs and Discussions:Many experienced Splunk users share best practices for using CIM in forums and blogs, where they discuss real-world applications and troubleshooting tips.

NEW QUESTION 10
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 11
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 16
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 19
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 20
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 21
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 26
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 31
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 36
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 37
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 41
Upon investigating a report of a web server becoming unavailable, the security analyst finds that the web server??s access log has the same log entry millions of times: 147.186.119.200 - - [28/Jul/2023:12:04:13 -0300] "GET /login/ HTTP/1.0" 200 3733
What kind of attack is occurring?

A. Denial of Service Attack
B. Distributed Denial of Service Attack
C. Cross-Site Scripting Attack
D. Database Injection Attack

Answer: A

Explanation:
The log entry showing the same request repeated millions of times indicates aDenial of Service (DoS) Attack, where the server is overwhelmed by a flood of requests to a specific resource, in this case, the/login/page. This type of attack is aimed at making the server unavailable to legitimate users by exhausting its resources.
? Denial of Service Attack:
? Incorrect Options:
? Web Server Security:Understanding DoS attacks is critical for securing web servers and mitigating these types of disruptions.

NEW QUESTION 42
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 43
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 46

.....

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