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 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 pre-packaged app delivers security content and detections on a regular, ongoing basis for Enterprise Security and SOAR?

A. SSE
B. ESCU
C. Threat Hunting
D. InfoSec

Answer: B

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

NEW QUESTION 5
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

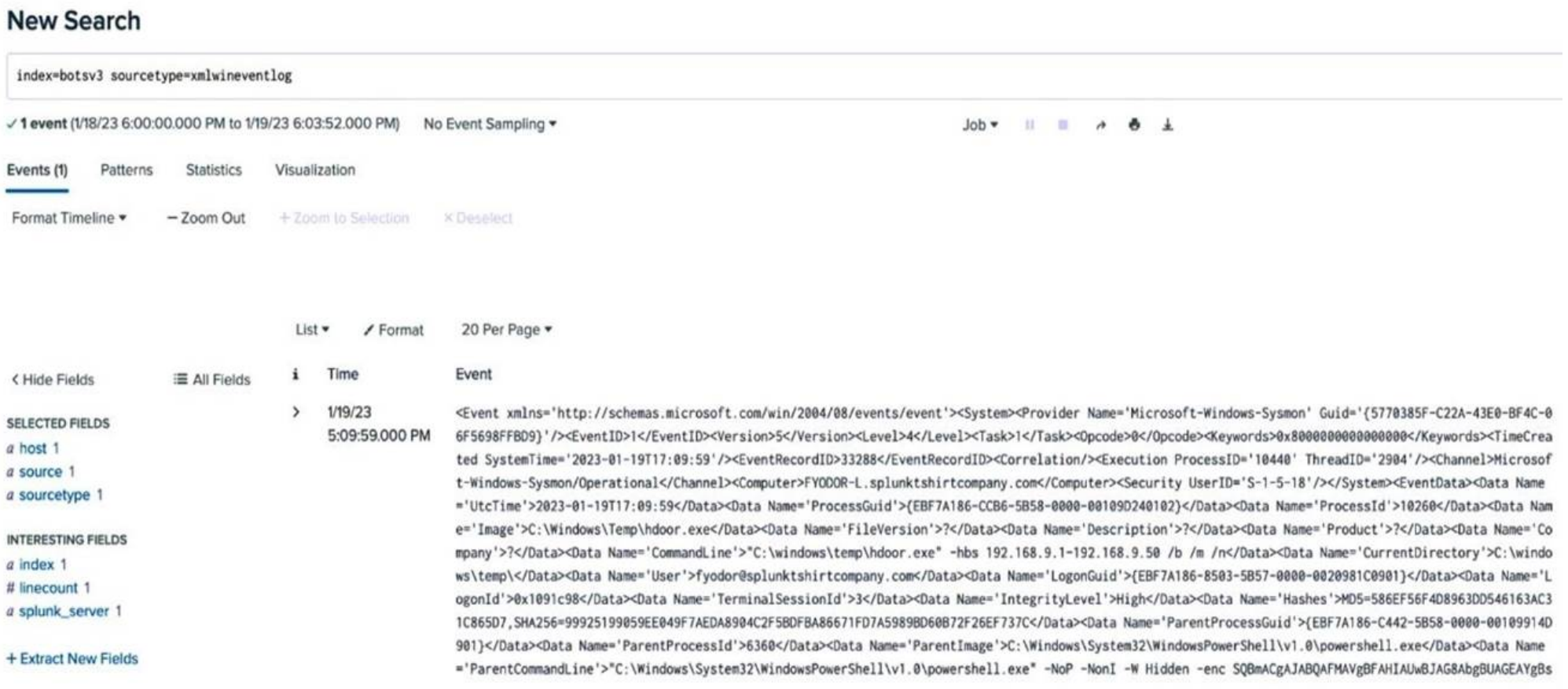
NEW QUESTION 6
An IDS signature is designed to detect and alert on logins to a certain server, but only if they occur from 6:00 PM - 6:00 AM. If no IDS alerts occur in this window, but the signature is known to be correct, this would be an example of what?

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
An analyst is building a search to examine Windows XML Event Logs, but the initial search is not returning any extracted fields. Based on the above image, what is themost likelycause?



A. The analyst does not have the proper role to search this data.
B. The analyst is searching newly indexed data that was improperly parsed.

C. The analyst did not add the excract command to their search pipeline.
D. The analyst is not in the Drooer Search Mode and should switch to Smart or Verbose.

Answer: D

Explanation:
In Splunk, when an analyst is building a search and finds that extracted fields are not appearing, it often relates to the search mode being used.Smart ModeorVerbose Modeare better suitedfor field extraction as they allow Splunk to automatically extract and display fields based on the data being searched.
? Search Modes in Splunk:
? Incorrect Options:
? Splunk Documentation:Search modes and their impact on field extraction.

NEW QUESTION 8
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 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 13
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
The United States Department of Defense (DoD) requires all government contractors to provide adequate security safeguards referenced in National Institute of Standards and Technology (NIST) 800-171. All DoD contractors must continually reassess, monitor, and track compliance to be able to do business with the US government.
Which feature of Splunk Enterprise Security provides an analyst context for the correlation search mapping to the specific NIST guidelines?

A. Comments
B. Moles
C. Annotations
D. Framework mapping

Answer: D

Explanation:
Splunk Enterprise Security provides a feature calledFramework Mappingthat allows correlation searches to be mapped to specific cybersecurity frameworks, including NIST 800-171, which is crucial for DoD contractors. This mapping provides context to the analyst by showing how particular searches align with compliance requirements, aiding in continuous monitoring and reassessment as mandated by the DoD. This feature is integral for organizations that need to demonstrate compliance with NIST guidelines and other security frameworks.

NEW QUESTION 21
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 25
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 30
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 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 44
What is the main difference between a DDoS and a DoS attack?

A. A DDoS attack is a type of physical attack, while a DoS attack is a type of cyberattack.
B. A DDoS attack uses a single source to target a single system, while a DoS attack uses multiple sources to target multiple systems.
C. A DDoS attack uses multiple sources to target a single system, while a DoS attack usesa single source to target a single or multiple systems.
D. A DDoS attack uses a single source to target multiple systems, while a DoS attack uses multiple sources to target a single system.

Answer: C

Explanation:
The primary difference between a Distributed Denial of Service (DDoS) attack and a Denial of Service (DoS) attack is in the source of the attack. ADDoSattack involves multiple compromised systems (often part of a botnet) attacking a single target, overwhelming it with traffic or requests. In contrast, aDoSattack typically involves a single source attacking the target. The goal of both attacks is to make a service unavailable, but DDoS attacks are usually more difficult to defend against because of their distributed nature.

NEW QUESTION 47
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 48
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
Which stage of continuous monitoring involves adding data, creating detections, and building drilldowns?

A. Implement and Collect
B. Establish and Architect
C. Respond and Review
D. Analyze and Report

Answer: A

Explanation:
In the context of continuous monitoring, theImplement and Collectstage involves adding data sources, creating detections, and building drilldowns. This stage is focused on the practical setup and configuration necessary to ensure that monitoring systems are properly gathering the necessary data and that the relevant detection mechanisms are in place to identify potential threats. Other stages, such asAnalyze and Report, are more focused on the interpretation and presentation of this data after collection.

NEW QUESTION 61
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 64
An analyst is not sure that all of the potential data sources at her company are being correctly or completely utilized by Splunk and Enterprise Security. Which of the following might she suggest using, in order to perform an analysis of the data types available and some of their potential security uses?

A. Splunk ITSI
B. Security Essentials
C. SOAR
D. Splunk Intelligence Management

Answer: B

Explanation:
Splunk Security Essentials is a powerful tool that an analyst can use to analyze the data types available and understand their potential security uses. It provides a framework for exploring how different data sources can be leveraged within Splunk to enhance security monitoring and detection capabilities.
? Splunk Security Essentials:This app is designed to help users maximize the value
of their data by providing examples of security use cases, detection searches, and best practices tailored to the available data sources. It offers a comprehensive overview of how various types of data can be used within Splunk, making it easier for analysts to identify gaps in data utilization.
? Data Source Analysis:Through Splunk Security Essentials, an analyst can:
? Why Security Essentials:This tool is particularly useful for organizations looking to ensure that they are fully utilizing their available data within Splunk Enterprise Security. It provides actionable insights and examples that can help analysts fine- tune their security operations and improve threat detection.
? Splunk Security Essentials Documentation:The official documentation provides detailed instructions on how to use the app to analyze data sources and implement best practices for security monitoring.
? User Community Discussions:Many Splunk users share their experiences and strategies for using Security Essentials to optimize their security posture in forums and blogs.

NEW QUESTION 67
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 69
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 73
A successful Continuous Monitoring initiative involves the entire organization. When an analyst discovers the need for more context or additional information, perhaps from additional data sources or altered correlation rules, to what role would this request generally escalate?

A. SOC Manager
B. Security Analyst
C. Security Engineer
D. Security Architect

Answer: C

Explanation:
In a successful Continuous Monitoring initiative, when an analyst identifies the need for more context or additional information, the request typically escalates to aSecurity Engineer. Security Engineers are responsible for the integration and configuration of additional data sources, and they can alter correlation rules or enhance data ingestion pipelines to provide the necessary context for analysts.
? Security Engineer:
? Incorrect Options:
? Continuous Monitoring Best Practices:Industry standards emphasize the role of Security Engineers in maintaining and enhancing security monitoring systems. Role

NEW QUESTION 74
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 78
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 83
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 84
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 88
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 89
.....

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