

# 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.

? Using binto 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 using stats, bin, and indexing.

? Splunk Performance Tuning Guides: These guides offer in-depth advice on optimizing searches for speed and efficiency, with examples of common pitfalls and how to avoid them.

### NEW QUESTION 2

Which 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:

The TERM() 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 using TERM(), 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 3

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:

The Enterprise 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 4

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 5

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

| makeresults

| eval ccnumber="511388720478619733"

| rex field=ccnumber mode=???s/(\\d{4}-){3}/XXXX-XXXX-XXXX-/g"  
Please assume that the aboverexcommand is correctly written.

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 6**

An analyst is investigating how an attacker successfully performs a brute-force attack to gain a foothold into an organizations systems. In the course of the investigation the analyst determines that the reason no alerts were generated is because the detection searches were configured to run against Windows data only and excluding any Linux data. This is an example of what?

- A. A True Positive.
- B. A True Negative.
- C. A False Negative.
- D. A False Positive.

**Answer:** C

**Explanation:**

This scenario is an example of aFalse Negativebecause the detection mechanisms failed to generate alerts for a brute-force attack due to a misconfiguration—specifically, the exclusion of Linux data from the detection searches. A False Negative occurs when a security control fails to detect an actual malicious activity that it is supposed to catch, leading to undetected attacks and potential breaches.

**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 the most likely cause?

**New Search**

index=botsv3 sourcetype=xmlwineventlog

✓ 1 event (1/18/23 6:00:00.000 PM to 1/19/23 6:03:52.000 PM) No Event Sampling

Job

Events (1)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deselect

Hide Fields

All Fields

Time

Event

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

a index 1

# linecount 1

a splunk\_server 1

+ Extract New Fields

1/19/23

5:09:59.000 PM

<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFB09}" /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime="2023-01-19T17:09:59"/><EventRecordID>33288</EventRecordID><Correlation><Execution ProcessID="10440" ThreadID="2904"/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>FY000R-L.splunkshirtcompany.com</Computer><Security UserID="S-1-5-18"/></System><EventData><Data Name="UtcTime">2023-01-19T17:09:59</Data><Data Name="ProcessGuid">{EBF7A186-CCB6-5B58-0000-00109D240102}</Data><Data Name="ProcessId">10260</Data><Data Name="Image">C:\Windows\Temp\hdoor.exe</Data><Data Name="FileVersion">?</Data><Data Name="Description">?</Data><Data Name="Product">?</Data><Data Name="Company">?</Data><Data Name="CommandLine">"C:\windows\temp\hdoor.exe" -hbs 192.168.9.1-192.168.9.50 /b /m /n</Data><Data Name="CurrentDirectory">C:\windows\temp</Data><Data Name="User">fyodor@splunkshirtcompany.com</Data><Data Name="LogonGuid">{EBF7A186-8503-5B57-0000-0020981C0901}</Data><Data Name="LogonId">0x1091c98</Data><Data Name="TerminalSessionId">3</Data><Data Name="IntegrityLevel">High</Data><Data Name="Hashes">MD5=586EF56F408963DD546163AC31C865D7,SHA256=99925199059EE049F7AEDA8904C2F58DFBA86671FD7A59898D60B72F26EF737C</Data><Data Name="ParentProcessGuid">{EBF7A186-C442-5B58-0000-00109914D901}</Data><Data Name="ParentProcessId">6360</Data><Data Name="ParentImage">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data><Data Name="ParentCommandLine">"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc SQBmACgAJABQAFMAVgBFAHIAUwBJAG8AbgBUAGEAYgBs</Data></EventData></Event>

- 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 exctract 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 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, making taking containment action on a compromised host the 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 the Endpoint data 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 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. Escalating privileges via UAC bypass.

**Answer:** A

**Explanation:**

Tactics are the overarching objectives or strategies attackers use during their operations, while techniques are the specific methods used to achieve these tactics. In this case, gathering information about a target (often referred to as Reconnaissance) is a tactic because it represents a high-level objective of understanding the target. The other options provided (persistence, phishing, privilege escalation) are specific techniques used to achieve the broader goals or tactics.

**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 12**

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 called Framework Mapping that 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 20**

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. NetworkM-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 22**

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 a POST /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 a Denial of Service (DoS) attack because 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 26**

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 is Annotations. 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 30**

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 uses a 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. A DDoS attack involves multiple compromised systems (often part of a botnet) attacking a single target, overwhelming it with traffic or requests. In contrast, a DoS attack 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 32**

An analyst notices that one of their servers is sending an unusually large amount of traffic, gigabytes more than normal, to a single system on the Internet. There doesn't seem to be any associated increase in incoming traffic.

What type of threat actor activity might this represent?

- A. Data exfiltration
- B. Network reconnaissance
- C. Data infiltration
- D. Lateral movement

**Answer:** A

**Explanation:**

? Unusual Traffic Patterns:

? Possible Threat Activities:

Scenario Analysis: Conclusion: Given the evidence of large data transfers to a single external system without corresponding inbound traffic, data exfiltration is the most likely scenario. This suggests that an adversary has compromised the server and is extracting valuable or sensitive data from the organization.

? Data Exfiltration Techniques: Techniques such as those documented in the MITRE

ATT&CK framework (e.g., T1041 - Exfiltration Over C2 Channel) detail how attackers move data out of a network.

? Incident Response Playbooks: Many incident response frameworks emphasize monitoring for unusual outbound traffic as a primary indicator of data exfiltration.

**NEW QUESTION 36**

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:**

The coalesce function 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 the `src` field with the value from `machine_name` if `src` is 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 39**

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, the `Implement and Collect` stage 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 as `Analyze and Report`, are more focused on the interpretation and presentation of this data after collection.

**NEW QUESTION 40**

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 42**

What is the main difference between hypothesis-driven and data-driven Threat Hunting?

- A. Data-driven hunts always require more data to search through than hypothesis-driven hunts.
- B. Data-driven hunting tries to uncover activity within an existing data set, hypothesis-driven hunting begins with a potential activity that the hunter thinks may be happening.
- C. Hypothesis-driven hunts are typically executed on newly ingested data sources, while data-driven hunts are not.
- D. Hypothesis-driven hunting tries to uncover activity within an existing data set, data-driven hunting begins with an activity that the hunter thinks may be happening.

**Answer:** B

**Explanation:**

The main difference between hypothesis-driven and data-driven threat hunting lies in the approach. In hypothesis-driven hunting, the hunter starts with a theory or hypothesis about what kind of malicious activity might be occurring and then searches the data to confirm or refute that hypothesis. On the other hand, data-driven hunting involves sifting through existing datasets to uncover patterns, anomalies, or activities that were not initially suspected. Hypothesis-driven approaches are more focused and often guided by threat intelligence or knowledge of attacker behaviors, while data-driven approaches rely on broad data analysis to identify unexpected threats.

**NEW QUESTION 46**

When searching in Splunk, which of the following SPL commands can be used to run a subsearch across every field in a wildcard field list?

- A. `foreach`
- B. `rex`
- C. `makeresults`
- D. `transaction`

**Answer:** A

**Explanation:**

The `foreach` command in Splunk is used to iterate over a list of fields that match a wildcard expression and apply a subsearch or function to each of them. This is particularly useful when you need to perform an operation across multiple fields dynamically identified by a wildcard pattern. None of the other options (`rex`, `makeresults`, or `transaction`) are designed for this specific purpose. The `foreach` command allows for flexible and efficient processing of multiple fields without having to explicitly name them all.

**NEW QUESTION 47**

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:**

The stats command is used to generate statistics, such as counts, over specific fields. In this case, the command `index=security_logs eventtype=failed_login | stats count as failed_attempts by src_ip | sort -failed_attempts` creates a temporary table that counts the number of failed login attempts (failed\_attempts) for each source IP (src\_ip). The sort -failed\_attempts ensures 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 51**

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 53**

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, the New Domain Analysis dashboard 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 56**

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 a Denial 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 60**

An analyst is examining the logs for a web application's login form. They see thousands of failed login 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 a Credential Stuffing attack. 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. Unlike Password Spraying (which tries a few common passwords against many accounts) or Password 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 61**

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 66**

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 architectures are 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 69**

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, the `rex` command 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. The `rex` command 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, but `rex` is specifically designed for dynamic field extraction.

**NEW QUESTION 70**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SPLK-5001 Practice Test Here](#)**