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 a best practice when creating performant searches within Splunk?

A. Utilize the transaction command to aggregate data for faster analysis.
B. Utilize Aggregating commands to ensure all data is available prior to Streaming commands.
C. Utilize specific fields to return only the data that is required.
D. Utilize multiple wildcards across fields to ensure returned data is complete and available.

Answer: C

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

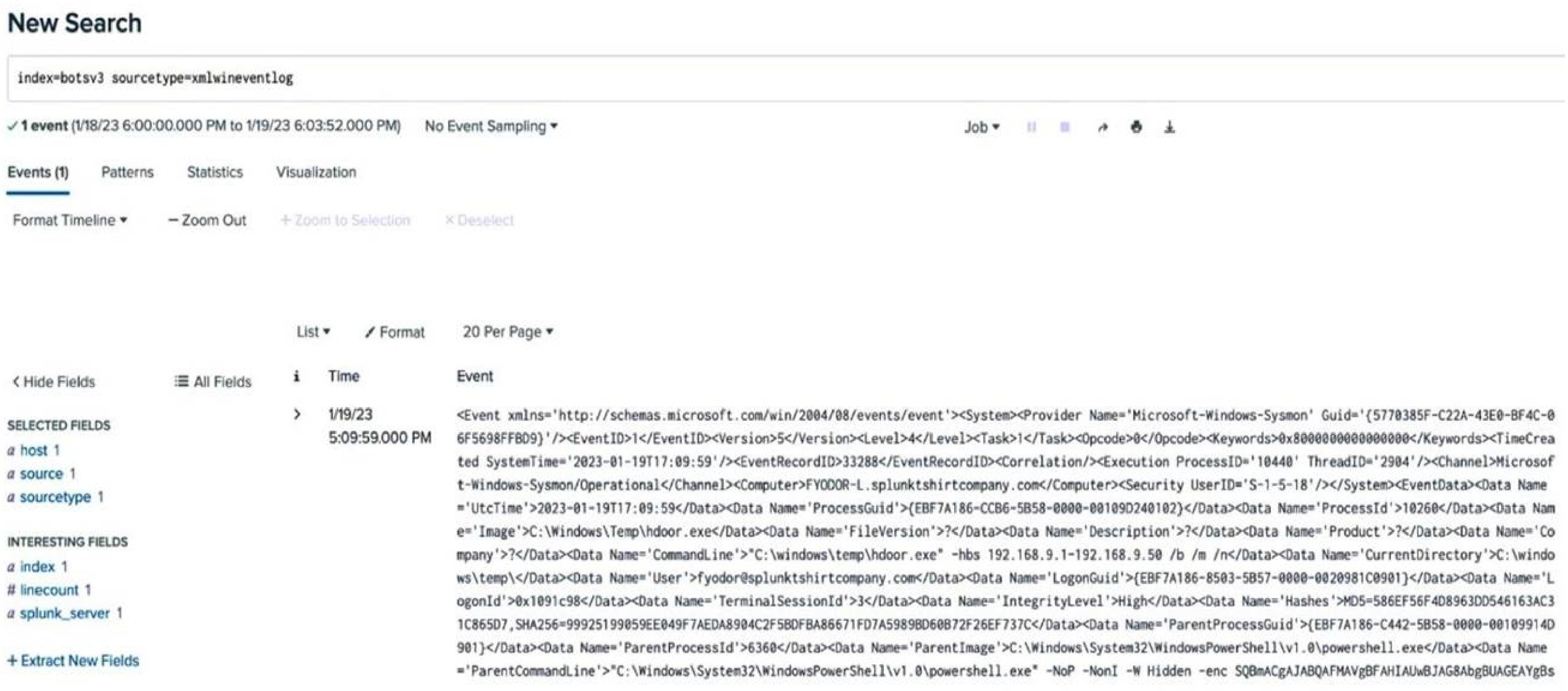
NEW QUESTION 3
An analyst is investigating how an attacker successfully performs a brute-force attack to gain a foothold into an organizations systems. In the course of the investigation the analyst determines that the reason no alerts were generated is because the detection searches were configured 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 4
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?



```
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 ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a index 1
# linecount 1
a splunk_server 1

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-0
6F5698FFBD9}'/><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCrea
ted SystemTime='2023-01-19T17:09:59'/><EventRecordID>33288</EventRecordID><Correlation/><Execution ProcessID='10440' ThreadID='2904'/><Channel>Microsof
t-Windows-Sysmon/Operational</Channel><Computer>FYODOR-L.splunktshirtcompany.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 Nam
e='Image'>C:\Windows\Temp\hdoor.exe</Data><Data Name='FileVersion'>?</Data><Data Name='Description'>?</Data><Data Name='Product'>?</Data><Data Name='Co
mpany'>?</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:\windo
ws\temp\</Data><Data Name='User'>fyodor@splunktshirtcompany.com</Data><Data Name='LogonGuid'>{EBF7A186-8503-5B57-0000-0020981C0901}</Data><Data Name='L
ogonId'>0x1091c98</Data><Data Name='TerminalSessionId'>3</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>MD5=586EF56F4D8963DD546163AC3
1C865D7,SHA256=99925199059EE049F7AEDA8904C2F5BDFBA86671FD7A5989BD60B72F26EF737C</Data><Data Name='ParentProcessGuid'>{EBF7A186-C442-5B58-0000-00109914D
901}</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
```

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 5
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 6
When threat hunting for outliers in Splunk, which of the following SPL pipelines would filter for users with over a thousand occurrences?

A. | sort by user | where count > 1000
B. | stats count by user | where count > 1000 | sort - count
C. | top user
D. | stats count(user) | sort - count | where count > 1000

Answer: B

Explanation:
In Splunk, to filter users with over a thousand occurrences, the pipeline| stats count by user | where count > 1000 | sort - countis most effective. Thestats count by usercommand generates a count of occurrences for each user. Thewhereclause then filters out only those users who have more than 1000 occurrences. Finally,sort - countsorts the results in descending order by count. This approach is efficient for identifying outliers, such as users with a high number of events.

NEW QUESTION 7
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 8
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 9
There are many resources for assisting with SPL and configuration questions. Which of the following resources feature community-sourced answers?

A. Splunk Answers
B. Splunk Lantern
C. Splunk Guidebook
D. Splunk Documentation

Answer: A

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

NEW QUESTION 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

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 15
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 19
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 23
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 26
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 29
A Risk Notable Event has been triggered in Splunk Enterprise Security, an analyst investigates the alert, and determines it is a false positive. What metric would be used to define the time between alert creation and close of the event?

A. MTTR (Mean Time to Respond)
B. MTBF (Mean Time Between Failures)
C. MTTA (Mean Time to Acknowledge)
D. MTTD (Mean Time to Detect)

Answer: A

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

NEW QUESTION 33
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 36
......