

Splunk.SPLK-5001.v2026-09-25.q61

Exam Code:	SPLK-5001
Exam Name:	Splunk Certified Cybersecurity Defense Analyst
Certification Provider:	Splunk
Free Question Number:	61
Version:	v2026-09-25
# of views:	103
# of Questions views:	611
https://www.freecram.net/torrent/Splunk.SPLK-5001.v2026-09-25.q61.html	

NEW QUESTION: 1

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. Web
- B. Network traffic
- C. Authentication
- D. Endpoint

Answer: (SHOW ANSWER)

NEW QUESTION: 2

Long-tail analysis is a threat-hunting technique used for which of the following?

- A. Identifying and analyzing infrequent but potentially important events.
- B. Identifying and analyzing common events.
- C. Identifying and analyzing only the data from the last month.
- D. Identifying and analyzing only the data from the last week.

Answer: (SHOW ANSWER)

Long-tail analysis focuses on the "long tail" of a data distribution - those rare or low-frequency events - which often surface subtle indicators of compromise that bulk analysis might miss.

NEW QUESTION: 3

Which field is automatically added to search results when assets are properly defined and enabled in Splunk Enterprise Security?

- A. user
- B. src_category
- C. src_ip
- D. asset_category

Answer: (SHOW ANSWER)

NEW QUESTION: 4

Which of the following roles is commonly responsible for selecting and designing the infrastructure and tools that a security analyst utilizes to effectively complete their job duties?

- A. Security Engineer
- B. SOC Manager
- C. Threat Intelligence Analyst
- D. Security Architect

Answer: ([SHOW ANSWER](#))

The Security Architect is responsible for selecting and designing the security infrastructure and tools. They define the overall security framework, choose the appropriate technologies, and ensure the tools and systems support the analysts' ability to detect, investigate, and respond to threats effectively.

NEW QUESTION: 5

What is the recommended approach when handling a security incident?

- A. Follow a pre-defined incident response plan.
- B. Ignore the incident if it seems minor.
- C. Rely solely on antivirus software.
- D. Take immediate actions based on intuition.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

Which of the following is not considered a type of default metadata in Splunk?

- A. Source of data
- B. Timestamps
- C. Host name
- D. Event description

Answer: ([SHOW ANSWER](#))

Splunk's default metadata includes the host, source (path or origin), sourcetype, index, and timestamp fields. There is no built-in "event description" metadata field - descriptions are derived from the event content itself, not stored as default metadata.

NEW QUESTION: 7

Which Splunk ES feature detects complex behavior over a "period of time" instead of "point in time" alerting?

- A. Notable Based Alerting (NBA)
- B. Risk Based Alerting (RBA)
- C. Adaptive Actions
- D. Analytic Stories

Answer: B ([LEAVE A REPLY](#))

Risk Based Alerting evaluates and accumulates risk scores for entities over a defined time window, enabling detection of evolving threats across a period rather than at a single point in time.

NEW QUESTION: 8

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: ([SHOW ANSWER](#))

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 10

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 11

An analyst is investigating a network alert for suspected lateral movement from one Windows host to another Windows host. According to Splunk CIM documentation, the IP address of the host from which the attacker is moving would be in which field?

- A. src_nt_host
- B. dest
- C. host
- D. src_ip

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 12

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. stats
- C. rename
- D. eval

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 13

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 14

According to David Bianco's Pyramid of Pain, which indicator type is least effective when used in continuous monitoring?

- A. NetworM-lost artifacts
- B. TTPs
- C. Domain names
- D. Hash values

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 15

A threat hunter generates a report containing the list of users who have logged in to a particular database during the last 6 months, along with the number of times they have each authenticated. They sort this list and remove any user names who have logged in more than 6 times. The remaining names represent the users who rarely log in, as their activity is more suspicious. The hunter examines each of these rare logins in detail.

This is an example of what type of threat-hunting technique?

- A. Outlier Frequency Analysis
- B. Co-Occurrence Analysis
- C. Least Frequency of Occurrence Analysis
- D. Time Series Analysis

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 16

The Lockheed Martin Cyber Kill Chain breaks an attack lifecycle into several stages. A threat actor modified the registry on a compromised Windows system to ensure that their malware would automatically run at boot time. Into which phase of the Kill Chain would this fall?

- A. Delivery
- B. Act on Objectives
- C. Exploitation
- D. Installation

Answer: ([SHOW ANSWER](#))

Valid SPLK-5001 Dumps shared by EduDump.com for Helping Passing SPLK-5001 Exam! EduDump.com now offer the **newest SPLK-5001 exam dumps**, the EduDump.com SPLK-5001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-5001 dumps with Test Engine here:

<https://www.edudump.com/exams/Splunk/SPLK-5001/premium/> (144 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 17

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. index=foo host=i-478619733 | transaction src_ip | stats count by host
- C. index=foo | transaction src_ip | stats count by host | search host=i-478619733
- D. | stats range(_time) as duration by src_ip | index=foo host=i-478619733 | bin duration span=5min | stats count by duration, host

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 18

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

- A. 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.
- B. Hypothesis-driven hunts are typically executed on newly ingested data sources, while data-driven hunts are not.
- C. 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.
- D. Data-driven hunts always require more data to search through than hypothesis-driven hunts.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 19

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. Cross-Site scripting attack.
- B. Database injection attack.
- C. Distributed denial of service attack.
- D. Denial of service attack.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 20

As an analyst, tracking unique users is a common occurrence. The Security Operations Center (SOC) manager requested a search with results in a table format to track the cumulative downloads by distinct IP address. Which example calculates the running total of distinct users over time?

eventtype="download" | bin _time span=1d as day | table clientip day

- A. user
eventtype="download" | bin _time span=1d as day | stats values(clientip)
- B. as ips dc(clientip) by user | table day ips
eventtype="download" | bin _time span=1d as day | stats values(clientip)
- C. as ips dc(clientip) by day
eventtype="download" | bin _time span=1d as day | stats values(clientip)
- D. as ips dc(clientip) by day | streamstats dc(ips) as "Cumulative total"

Answer: ([SHOW ANSWER](#))

This search first bins events by day and uses stats to list each day's distinct IPs (ips) and count them (dc(clientip)). The streamstats dc(ips) as "Cumulative total" then computes a running distinct count of all IPs seen up through each day, giving the cumulative total you need.

NEW QUESTION: 21

In Splunk, what feature would an analyst leverage to drilldown on an IP address field to query third-party intelligence for that IP?

- A. Notable drilldown
- B. Alert action
- C. Workflow action
- D. Adaptive Response action

Answer: ([SHOW ANSWER](#))

Workflow actions let you click on a field value, like an IP address, in search results or dashboards and invoke external lookups or queries (for example, sending the IP to a threat-intel service) directly from the Splunk UI.

NEW QUESTION: 22

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 are world writable thus allowing attackers a place to drop, stage, and execute malware on a system without needing to worry about file permissions.
- B. Temp directories aren't owned by any particular user, making it difficult to track the process owner when files are executed.
- 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 flagged as non-executable, meaning that no files stored within can be executed, and this executable was run from that directory.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 23

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 above rex command is correctly written.

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 24

Which of the following compliance frameworks was specifically created to measure the level of cybersecurity maturity within an organization?

- A. PCI-DSS
- B. GDPR
- C. FISMA
- D. CMMC

Answer: ([SHOW ANSWER](#))

The Cybersecurity Maturity Model Certification (CMMC) was designed to assess and certify an organization's cybersecurity maturity across defined levels, ensuring progressive improvement in security practices. Other frameworks like PCI_DSS, GDPR, and FISMA set requirements but do not define graduated maturity levels.

NEW QUESTION: 25

An analyst is looking for known C2 communication in a few billion NetFlow records, using a query similar to the following:

```
index=network sourcetype=netflow src_ip=149.151.100.4 src_port=908
```

```
protocol=ip
```

This query works, but due to the sheer size of the index, it is very slow. Which of the following SPL commands might the analyst use when rewriting their SPL to speed up the search?

- A. table
- B. tstats
- C. accelerate
- D. lookup

Answer: ([SHOW ANSWER](#))

The tstats command leverages Splunk's indexed time-series (tsidx) data structures to perform statistical queries far more efficiently than raw-event searches. By rewriting the query to use tstats against the netflow data model (or a custom data model that maps your NetFlow source types), the search engine can pull counts or other stats directly from the tsidx files, dramatically reducing I/O and speeding up the lookup of known C2 communication.

NEW QUESTION: 26

Which of the following use cases is best suited to be a Splunk SOAR Playbook?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 27

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 spraying
- C. Password cracking
- D. Credential stuffing

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 28

In which phase of the Continuous Monitoring cycle are suggestions and improvements typically made?

- A. Implement and Collect
- B. Define and Predict
- C. Establish and Architect
- D. Analyze and Report

Answer: (SHOW ANSWER)

NEW QUESTION: 29

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?



- A. The analyst is searching newly indexed data that was improperly parsed.
- B. The analyst did not add the extract command to their search pipeline.
- C. The analyst does not have the proper role to search this data.
- D. The analyst is not in the Droover Search Mode and should switch to Smart or Verbose.

Answer: (SHOW ANSWER)

NEW QUESTION: 30

Which of the following is considered Personal Data under GDPR?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 31

An analyst is attempting to investigate a Notable Event within Enterprise Security. Through the course of their investigation they determined that the logs and artifacts needed to investigate the alert are not available.

What event disposition should the analyst assign to the Notable Event?

- A. Benign Positive, since there was no evidence that the event actually occurred.
- B. False Negative, since there are no logs to prove the activity actually occurred.
- C. True Positive, since there are no logs to prove that the event did not occur.
- D. Other, since a security engineer needs to ingest the required logs.

Answer: ([SHOW ANSWER](#))

Valid SPLK-5001 Dumps shared by EduDump.com for Helping Passing SPLK-5001 Exam! EduDump.com now offer the **newest SPLK-5001 exam dumps**, the EduDump.com SPLK-5001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-5001 dumps with Test Engine here:

<https://www.edudump.com/exams/Splunk/SPLK-5001/premium/> (144 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 32

While investigating a finding in Splunk, an analyst manually searches for threat intelligence matches and adds them to a list if they come back as malicious. Then, they send a request to contain the compromised host.

What would be the best solution to fully automate this process?

- A. An intelligence response action.
- B. A SOAR playbook triggered by the detection.
- C. Document those steps in the team's runbook.
- D. A model-assisted threat hunt.

Answer: ([SHOW ANSWER](#))

A Splunk SOAR playbook can ingest the notable event, automatically query threat_intel, update lists for malicious indicators, and execute containment actions on the affected host - all in one end_to_end, fully automated workflow.

NEW QUESTION: 33

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: ([SHOW ANSWER](#))

NEW QUESTION: 34

There are different metrics that can be used to provide insights into SOC operations. If Mean Time to Respond is defined as the total time it takes for an Analyst to disposition an event, what is the typical starting point for calculating this metric for a particular event?

- A. When the malicious event occurs.
- B. When the end users are notified about the issue.
- C. When a Notable Event is triggered.
- D. When the SOC Manager is informed of the issue.

Answer: ([SHOW ANSWER](#))

Mean Time to Respond (MTTR) typically begins when a Notable Event is triggered in Splunk Enterprise Security. This marks the point at which the SOC becomes aware of a potential issue, initiating the response process. The metric captures how quickly analysts can investigate and resolve the event from that trigger point.

NEW QUESTION: 35

Which of the following is a best practice when creating performant searches within Splunk?

- A. Utilize multiple wildcards across fields to ensure returned data is complete and available.
- 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 the transaction command to aggregate data for faster analysis.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 36

In the context of cybersecurity, what does the term "SIEM" stand for?

- A. Systematic Intrusion and Event Monitoring.
- B. Safety Intranet and Event Maintenance.
- C. Security Incident and Event Management.
- D. Secure Internet and Email Management.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 37

Which Splunk search mode is best for searches that contain commands such as chart, timechart, and top, but the analyst still wants results in the events tab?

- A. Verbose
- B. Smart
- C. Adaptive
- D. Fast

Answer: ([SHOW ANSWER](#))

Verbose mode tells Splunk to retrieve and display all raw events and full field extractions, even when you use transforming commands like chart, timechart, or top. This ensures your statistical results appear alongside the underlying events in the Events tab.

NEW QUESTION: 38

Which argument would an analyst use to search only accelerated data contained in the Network Traffic Data Model with the tstatscommand?

- A. accelerated=true
- B. datamodel=accelerated
- C. summariesonly=true
- D. dataset=accelerated

Answer: C ([LEAVE A REPLY](#))

Adding summariesonly=true to your tstats call ensures it queries only the accelerated (summarized) portions of the Network Traffic data model, maximizing performance.

NEW QUESTION: 39

Which of the following is not a component of the Splunk Security Content library (ESCU, SSE)?

- A. Correlation searches
- B. Reports
- C. Validated architectures
- D. Dashboards

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 40

What do frameworks and standards help accomplish in the cybersecurity landscape?

- A. Improve interoperability and consistency.
- B. Promote isolation between security teams.
- C. Decrease the number of data sources.
- D. Create new vulnerabilities.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 41

In Splunk Risk-Based Alerting, what are a set of conditions that dynamically adjust risk scores for an entity, such as an asset or identity?

- A. Risk values
- B. Risk factors
- C. Risk entities
- D. Risk entries

Answer: ([SHOW ANSWER](#)**)**

In Splunk Risk-Based Alerting, risk factors are sets of conditions that dynamically adjust the risk scores of entities such as assets or identities. They provide context-aware scoring by increasing or decreasing risk values based on specific attributes or behaviors.

NEW QUESTION: 42

Outlier detection is an analysis method that groups together data points into high density clusters.

Data points that fall outside of these high density clusters are considered to be what?

- A. Anomalies
- B. Baselined
- C. Non-conformatives
- D. Inconsistencies

Answer: ([SHOW ANSWER](#)**)**

In outlier detection, points that lie outside the high-density clusters - i.e., those not fitting into any cluster - are by definition anomalies, as they deviate significantly from the normal data distribution.

NEW QUESTION: 43

An analysis of an organization's security posture determined that a particular asset is at risk and a new process or solution should be implemented to protect it. Typically, who would be in charge of designing the new process and selecting the required tools to implement it?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

An analyst has been asked to report on VPC Flow traffic to their EC2 instances in AWS and wants to only examine blocked connections for source and destination IP address pairs. In order to filter down to just the pertinent data, the analyst is only looking for source IP addresses which are attempting to connect to over five destination IP addresses and which have over a thousand blocked connections. Additionally, leadership would like to only see the applicable source IP addresses and a list of the destination IP addresses in the report and nothing else.

Which of the following Splunk searches meets these requirements?

A.

```
index=aws sourcetype=aws:cloudwatchlogs:vpcflow action=blocked
| fields src_ip, dest_ip
| stats count values(dest_ip) as listDestinations by src_ip
| eval numDestinations=len(listDestinations)
| where numDestinations > 5 AND count > 1000
| table src_ip, listDestinations
```

B.

```
index=aws sourcetype=aws:cloudwatchlogs:vpcflow action=blocked
| fields src_ip, dest_ip
| stats count dc(dest_ip) as numDestinations values(dest_ip) as listDestinations by src_ip
| where numDestinations > 5 AND count > 1000
| fields - count numDestinations
```

C.

```
index=aws sourcetype=aws:cloudwatchlogs:vpcflow action=blocked
| fields src_ip, dest_ip
| stats count values(dest_ip) as listDestinations by src_ip
| eval numDestinations=len(listDestinations)
| where numDestinations > 5 AND count > 1000
| fields - count numDestinations
```

```
index=aws sourcetype=aws:cloudwatchlogs:vpcflow action=blocked
| fields src_ip, dest_ip
| stats count(dest_ip) as numDestinations values(dest_ip) as listDestinations by src_ip
| where numDestinations > 5 AND count > 1000
| fields src_ip, listDestinations
```

D.

Answer: ([SHOW ANSWER](#))

The first search meets all the requirements - it filters to blocked traffic, aggregates per source IP, computes the number of distinct destinations, applies the ">5 destinations AND >1000 blocks" criteria, and then uses table src_ip, listDestinations to display only the source IPs and their destination lists.

NEW QUESTION: 45

In Splunk SPL, which command is used to filter and group results based on specific fields?

- A. stats
- B. fields
- C. filter
- D. eval

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 46

What device typically sits at a network perimeter to detect command and control and other potentially suspicious traffic?

- A. Web proxy
- B. Intrusion Detection System
- C. Endpoint Detection and Response
- D. Host-based firewall

Answer: ([SHOW ANSWER](#))

Valid SPLK-5001 Dumps shared by EduDump.com for Helping Passing SPLK-5001 Exam! EduDump.com now offer the **newest SPLK-5001 exam dumps**, the EduDump.com SPLK-5001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-5001 dumps with Test Engine here:

<https://www.edudump.com/exams/Splunk/SPLK-5001/premium/> (144 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 47

What is the main difference between a Denial of Service (DoS) attack and a Distributed Denial of Service (DDoS) attack?

- A. The DoS attack is illegal, while the DDoS attack is a legal form of cybersecurity testing.
- B. The DoS attack aims to exfiltrate sensitive data, while the DDoS attack aims to disrupt services by overwhelming resources.
- C. The DoS attack targets a single device, while the DDoS attack targets multiple devices.
- D. The DoS attack is carried out by a single threat actor, while the DDoS attack involves multiple threat actors.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 48

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 49

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 50

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. Malware Center
- B. Access Anomalies
- C. New Domain Analysis
- D. IAM Activity

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 51

Which of the following SPL searches is likely to return results the fastest?

- A. src_port=2938 AND protocol=tcp | stats count by src_ip | search
- B. src_ip=1.2.3.4
index=network src_port=2938 protocol=tcp | stats count by src_ip |
- C. search src_ip=1.2.3.4
index=network sourcetype=netflow src_ip=1.2.3.4 src_port=2938
- D. protocol=tcp | stats count
src_ip=1.2.3.4 src_port=2938 protocol=tcp | stats count

Answer: ([SHOW ANSWER](#))

Chosen option is the most efficient because it restricts the search to a specific index and sourcetype and applies all field filters (src_ip, src_port, protocol) at the very start. This minimizes the volume of data scanned before invoking the lighter-weight stats command, making it faster than searches that leave out index/sourcetype constraints or postpone filtering.

NEW QUESTION: 52

What is the following step-by-step description an example of?

1. The attacker devises a non-default beacon profile with Cobalt Strike and embeds this within a document.
2. The attacker creates a unique email with the malicious document based on extensive research about their target.
3. When the victim opens this document, a C2 channel is established to the attacker's temporary infrastructure on a compromised website.

- A. Policy
- B. Procedure
- C. Technique
- D. Tactic

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 53

Which Splunk Enterprise Security framework provides a way to identify incidents from events and then manage the ownership, triage process, and state of those incidents?

- A. Investigation Management
- B. Notable Event
- C. Asset and Identity
- D. Adaptive Response

Answer: ([SHOW ANSWER](#))

The Investigation Management framework in Splunk ES takes notable events and creates incidents, then provides the workflows and tools to assign ownership, track triage progress, and manage incident states from open through resolution.

NEW QUESTION: 54

Which Splunk resource provides pre-built content for assessing data sources and threat intelligence capabilities?

- A. Splunk Add-on for Microsoft Exchange
- B. Splunk Lantern
- C. Splunk Enterprise Security (ES)
- D. Splunk Security Essentials

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 55

An analyst working in Splunk Enterprise Security notices that a configured detection is not being triggered as expected by authentication data coming from a particular source. The detection uses data models to perform a search so they have looked at the data and confirmed it is CIM compliant. What else could be wrong?

- A. The data is missing the authentication tag.
- B. The data is missing the access tag.
- C. The data is missing the authentication field.
- D. The data is missing the access field.

Answer: ([SHOW ANSWER](#))

In Splunk Enterprise Security, data models rely on tags to recognize and categorize events properly. Even if the data is CIM-compliant, if it lacks the authentication tag, the data won't populate the Authentication data model, and detections using that model won't trigger. Proper tagging is essential for data to be included in the right data model.

NEW QUESTION: 56

Which part of the CIA triad is the opposite of destruction of information?

- A. Availability
- B. Integrity
- C. Confidentiality
- D. Continuity

Answer: ([SHOW ANSWER](#))

In the CIA triad, Integrity ensures that information remains accurate, complete, and unaltered.

The opposite of destruction or unauthorized modification of information is maintaining its integrity.

NEW QUESTION: 57

Storing log checksums in a public blockchain system is most closely linked to which security concept?

- A. Obfuscation
- B. Confidentiality
- C. Availability
- D. Integrity

Answer: D ([LEAVE A REPLY](#))

Storing log checksums in a public blockchain ensures that logs cannot be altered without detection. This directly supports Integrity, as the blockchain provides an immutable record that validates the authenticity and completeness of the logs.

NEW QUESTION: 58

How are Notable Events configured in Splunk Enterprise Security?

- A. As part of an audit.
- B. During an investigation.
- C. Via an Adaptive Response Action in a regular search.
- D. Via an Adaptive Response Action in a correlation search.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 59

During an investigation it is determined that an event is suspicious but expected in the environment. Out of the following, what is the best disposition to apply to this event?

- A. False positive
- B. True positive
- C. Informational
- D. Benign

Answer: ([SHOW ANSWER](#))

A benign disposition is applied when an event is indeed suspicious but ultimately expected and non-threatening in the given environment. This differentiates it from a false positive (incorrect detection) or a true positive (confirmed malicious activity).

NEW QUESTION: 60

The Security Operations team would like to track improvements after customizing dashboards to help analysts triage security alerts more efficiently. Which metric would they use?

- A. Mean Time to Detect
- B. Recovery Time
- C. Dwell Time
- D. Mean Time to Respond

Answer: A ([LEAVE A REPLY](#))

By customizing dashboards to streamline alert triage, you shorten the interval between an alert's occurrence and its identification by analysts - exactly what Mean Time to Detect measures.

NEW QUESTION: 61

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 Analysis
- B. Risk Factor
- C. Risk Object
- D. Risk Index

Answer: D ([LEAVE A REPLY](#))

Valid SPLK-5001 Dumps shared by EduDump.com for Helping Passing SPLK-5001 Exam! EduDump.com now offer the **newest SPLK-5001 exam dumps**, the EduDump.com SPLK-5001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-5001 dumps with Test Engine here:

<https://www.edudump.com/exams/Splunk/SPLK-5001/premium/> (144 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

Valid SPLK-5001 Dumps shared by EduDump.com for Helping Passing SPLK-5001 Exam! EduDump.com now offer the **newest SPLK-5001 exam dumps**, the EduDump.com SPLK-5001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-5001 dumps with Test Engine here:

<https://www.edudump.com/exams/Splunk/SPLK-5001/premium/> (144 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)