Splunk.SPLK-5001.v2026-01-07.q50

Exam Code:	SPLK-5001
Exam Name:	Splunk Certified Cybersecurity Defense Analyst
Certification Provider:	Splunk
Free Question Number:	50
Version:	v2026-01-07
# of views:	117
# of Questions views:	500
https://www.freepdfdumps.com/Splunk.SPLK-5001.v2026-01-07.q50.html	

NEW QUESTION: 1
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: (SHOW ANSWER)

NEW QUESTION: 2
What is the first phase of the Continuous Monitoring cycle?
A. Respond and Recover
B. Define and Predict
C. Assess and Evaluate
D. Monitor and Protect
Answer: B (LEAVE A REPLY)

NEW QUESTION: 3
Which of the following data sources can be used to discover unusual communication within an organization's network?
A. IAM
B. Net Flow
C. EDS
D. Email
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
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. | top user
C. | stats count(user) | sort - count | where count > 1000
D. | stats count by user | where count > 1000 | sort - count
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
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. Enrichments
B. Comments
C. Playbooks
D. Annotations
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
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 Object
D. Risk Analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
Which of the following use cases is best suited to be a Splunk SOAR Playbook?
A. Forming hypothesis for Threat Hunting
B. Creating persistent field extractions.
C. Taking containment action on a compromised host
D. Visualizing complex datasets.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Which field is automatically added to search results when assets are properly defined and enabled in Splunk Enterprise Security?
A. src_ip
B. asset_category

C. user
D. src_category
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
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: (SHOW ANSWER)

NEW QUESTION: 10
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. mask
D. substitute
Answer: (SHOW ANSWER)

NEW QUESTION: 11
Which stage of continuous monitoring involves adding data, creating detections, and building drilldowns?
A. Analyze and Report
B. Respond and Review
C. Establish and Architect
D. Implement and Collect
Answer: D (LEAVE A REPLY)

NEW QUESTION: 12

Which of the following data sources would be most useful to determine if a user visited a recently identified malicious website?

A. Web Proxy Logs

B. Intrusion Detection Logs

C. Web Server Logs

D. Active Directory Logs

Answer: (SHOW ANSWER)

NEW QUESTION: 13

The eval SPL expression supports many types of functions. Which of these function categories is not valid with eval?

A. Threat functions

B. Comparison and Conditional functions

C. Text functions

D. JSON functions

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

Refer to the exibit.

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 not in the Drooer Search Mode and should switch to Smart or Verbose.

C. The analyst is searching newly indexed data that was improperly parsed.

D. The analyst did not add the excract command to their search pipeline.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 15

Enterprise Security has been configured to generate a Notable Event when a user has quickly authenticated from multiple locations between which travel would be impossible. This would be considered what kind of an anomaly?

A. Access Anomaly
B. Endpoint Anomaly
C. Threat Anomaly
D. Identity Anomaly
Answer: A (LEAVE A REPLY)

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. Framework mapping
B. Annotations
C. Moles
D. Comments
Answer: (SHOW ANSWER)

NEW QUESTION: 17
What Splunk feature would enable enriching public IP addresses with ASN and owner information?

A. Using makersanita to add the ASMs to the search.
B. Using lookup to include relevant information.
C. Using oval commands to calculate the ASM.
D. Using rex to extract this information at search time.
Answer: (SHOW ANSWER)

NEW QUESTION: 18

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. Denial of service attack.
C. Distributed denial of service attack.
D. Database injection attack.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 19
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. Asset and Identity
B. Adaptive Response
C. Notable Event
D. Investigation Management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 20
Which Splunk Enterprise Security dashboard displays authentication and access-related data?
A. Audit dashboards
B. Asset and Identity dashboards
C. Access dashboards
D. Endpoint dashboards
Answer: C (LEAVE A REPLY)

NEW QUESTION: 21
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 = tostring(machine_name)
B. | eval src = src . machine_name
C. | eval src = src + machine_name
D. | eval src = coalesce(src,machine_name)
Answer: (SHOW ANSWER)

NEW QUESTION: 22

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 Lantern
C. Splunk Answers
D. Splunk Guidebook
Answer: C (LEAVE A REPLY)

NEW QUESTION: 23
Which of the Enterprise Security frameworks provides additional automatic context and correlation to fields that exist within raw data?
A. Risk
B. Asset and Identity
C. Threat Intelligence
D. Adaptive Response
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
A threat hunter is analyzing incoming emails during the past 30 days, looking for spam or phishing campaigns targeting many users. This involves finding large numbers of similar, but not necessarily identical, emails. The hunter extracts key datapoints from each email record, including the sender's address, recipient's address, subject, embedded URLs, and names of any attachments. Using the Splunk App for Data Science and Deep Learning, they then visualize each of these messages as points on a graph, looking for large numbers of points that occur close together. This is an example of what type of threat-hunting technique?
A. Time Series Analysis
B. Most Frequency of Occurrence Analysis
C. Least Frequency of Occurrence Analysis
D. Clustering
Answer: (SHOW ANSWER)

NEW QUESTION: 25
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:
[51.125.121.100 - [28/01/2006:10:27:10 -0300] "POST /cgi-bin/shurdown/ HTTP/1.0" 200 3304]
What kind of attack is most likely occurring?
A. Database injection attack.
B. Denial of service attack.
C. Distributed denial of service attack.
D. Cross-Site scripting attack.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
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. Create another detection for this information.
C. Allowlist more events based on this information.
D. Add this information to the risk message.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
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 a Notable Event is triggered.
B. When the SOC Manager is informed of the issue.
C. When the malicious event occurs.
D. When the end users are notified about the issue.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
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 (LEAVE A REPLY)

NEW QUESTION: 29
What feature of Splunk Security Essentials (SSE) allows an analyst to see a listing of current on-boarded data sources in Splunk so they can view content based on available data?
A. Data Source Onboarding Guides
B. Security Content
C. Data Inventory
D. Security Data Journey
Answer: C (LEAVE A REPLY)

NEW QUESTION: 30

Splunk Enterprise Security has numerous frameworks to create correlations, integrate threat intelligence, and provide a workflow for investigations. Which framework raises the threat profile of individuals or assets to allow identification of people or devices that perform an unusual amount of suspicious activities?
A. Notable Event Framework
B. Risk Framework
C. Asset and Identity Framework
D. Threat Intelligence Framework
Answer: B (LEAVE A REPLY)

NEW QUESTION: 31
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. rex
B. transaction
C. makeresults
D. foreach
Answer: D (LEAVE A REPLY)

NEW QUESTION: 32
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 Architect
B. Security Engineer
C. SOC Manager
D. Security Analyst
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
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. Informational
C. True positive
D. Benign
Answer: D (LEAVE A REPLY)

NEW QUESTION: 34
Rotating encryption keys after a security incident is most closely linked to which security concept?
A. Availability
B. Obfuscation
C. Integrity
D. Confidentiality
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
A Cyber Threat Intelligence (CTI) team produces a report detailing a specific threat actor's typical behaviors and intent. This would be an example of what type of intelligence?
A. Operational
B. Strategic
C. Tactical
D. Executive
Answer: C (LEAVE A REPLY)

NEW QUESTION: 36
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. Least Frequency of Occurrence Analysis
B. Co-Occurrence Analysis
C. Time Series Analysis
D. Outlier Frequency Analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 37
According to Splunk CIM documentation, which field in the Authentication Data Model represents the user who initiated a privilege escalation?
A. src_user
B. src_user_id

C. username
D. dest_user
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
Which dashboard in Enterprise Security would an analyst use to generate a report on users who are currently on a watchlist?
A. Identity Center
B. Identity Tracker
C. Access Tracker
D. Access Center
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
The following list contains examples of Tactics, Techniques, and Procedures (TTPs):
* Exploiting a remote service
* Extend movement
* Use EternalBlue to exploit a remote SMB server
In which order are they listed below?
A. Tactic, Technique, Procedure
B. Tactic, Procedure, Technique
C. Procedure, Technique, Tactic
D. Technique, Tactic, Procedure
Answer: (SHOW ANSWER)

NEW QUESTION: 40
What is the term for a model of normal network activity used to detect deviations?
A. A cluster.
B. A data model.
C. A baseline.
D. A time series.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
Upon investigating a report of a web server becoming unavailable, the security analyst finds that the web server's access log has the same log entry millions of times:
147.186.119.200 - - [28/Jul/2023:12:04:13 -0300] "GET /login/ HTTP/1.0" 200 3733 What kind of attack is occurring?
A. Database Injection Attack
B. Cross-Site Scripting Attack
C. Distributed Denial of Service Attack

D. Denial of Service Attack
Answer: D (LEAVE A REPLY)

NEW QUESTION: 42
Which of the following is a reason to use Data Model Acceleration in Splunk?
A. To rapidly compare the use of various algorithms to detect anomalies.
B. To retrieve data faster than from a raw index.
C. To normalize the data associated with threats.
D. To quickly model various responses to a particular vulnerability.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
An adversary uses "LoudWiner" to hijack resources for crypto mining. What does this represent in a TTP framework?
A. Procedure
B. Technique
C. Tactic
D. Problem
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following is a best practice when creating performant searches within Splunk?
A. Utilize specific fields to return only the data that is required.
B. Utilize Aggregating commands to ensure all data is available prior to Streaming commands.
C. Utilize multiple wildcards across fields to ensure returned data is complete and available.
D. Utilize the transaction command to aggregate data for faster analysis.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 45
Which of the following use cases is best suited to be a Splunk SOAR Playbook?
A. Visualizing complex datasets.
B. Creating persistent field extractions.
C. Forming hypothesis for Threat Hunting
D. Taking containment action on a compromised host
Answer: (SHOW ANSWER)

NEW QUESTION: 46
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. rare

B. least
C. uncommon
D. base
Answer: (SHOW ANSWER)

NEW QUESTION: 47
The field file_acl contains access controls associated with files affected by an event. In which data model would an analyst find this field?
A. Malware
B. Endpoint
C. Alerts
D. Vulnerabilities
Answer: B (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following is a best practice for searching in Splunk?
A. Limit fields returned from the search utilizing the cable command.
B. Searching over All Time ensures that all relevant data is returned.
C. Streaming commands run before aggregating commands in the Search pipeline.
D. Raw word searches should contain multiple wildcards to ensure all edge cases are covered.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following is not a component of the Splunk Security Content library (ESCU, SSE)?
A. Reports
B. Dashboards
C. Correlation searches
D. Validated architectures
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
Which argument searches only accelerated data in the Network Traffic Data Model with tstats?

A. accelerate=true
B. dataset=accelerated
C. datamodel=accelerated
D. summariesonly=true
Answer: D (LEAVE A REPLY)