Splunk.SPLK-3001.v2026-09-23.q52

Exam Code:	SPLK-3001
Exam Name:	Splunk Enterprise Security Certified Admin Exam
Certification Provider:	Splunk
Free Question Number:	52
Version:	v2026-09-23
# of views:	103
# of Questions views:	520
https://www.freecram.net/torrent/Splunk.SPLK-3001.v2026-09-23.q52.html	

NEW QUESTION: 1
Where are attachments to investigations stored?
A. KV Store
B. notable index
C. attachments.csv lookup
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments
Answer: A (LEAVE A REPLY)
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

NEW QUESTION: 2
An administrator wants to ensure that none of the ES indexed data could be compromised through tampering.
What feature would satisfy this requirement?
A. Index consistency.
B. Data integrity control.
C. Indexer acknowledgement.
D. Index access permissions.
Answer: (SHOW ANSWER)
https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html

NEW QUESTION: 3
What does the Common Information Model primarily provide within Splunk Enterprise Security?
A. Standardized field mappings enabling consistent searches across diverse security data sources.
B. Distributed search replication ensuring high availability for clustered search head environments.

C. Automated malware detection using machine learning-based endpoint behavioral analytics continuously deployed.
D. Indexed archive retention supporting long-term regulatory compliance and governance requirements automatically.
Answer: (SHOW ANSWER)
CIM normalizes data fields across different technologies, allowing reusable searches, dashboards, and detections to operate consistently regardless of source vendor formats.

NEW QUESTION: 4
The Brute Force Access Behavior Detected correlation search is enabled, and is generating many false positives. Assuming the input data has already been validated.
How can the correlation search be made less sensitive?
A. Edit the search and modify the notable event status field to make the notable events less urgent.
B. Edit the search, look for where or xswhere statements, and after the threshold value being compared to make it less common match.
C. Edit the search, look for where or xswhere statements, and alter the threshold value being compared to make it a more common match.
D. Modify the urgency table for this correlation search and add a new severity level to make notable events from this search less urgent.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 5
How is it possible to navigate to the ES graphical Navigation Bar editor?
A. Configure -> Navigation Menu
B. Configure -> General -> Navigation
C. Settings -> User Interface -> Navigation -> Click on "Enterprise Security"
D. Settings -> User Interface -> Navigation Menus -> Click on "default" next to SplunkEnterpriseSecuritySuite
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

NEW QUESTION: 6
What tools does the Risk Analysis dashboard provide?
A. High risk threats.
B. Notable event domains displayed by risk score.
C. A display of the highest risk assets and identities.
D. Key indicators showing the highest probability correlation searches in the environment.
Answer: (SHOW ANSWER)

https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis

NEW QUESTION: 7
Which columns in the Assets lookup are used to identify an asset in an event?
A. src, dvc, dest
B. cidr, port, netbios, saml
C. ip, mac, dns, nt_host
D. host, hostname, url, address
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Formatassetoridentitylist

NEW QUESTION: 8
Which settings indicates that the correlation search will be executed as new events are indexed?
A. Always-On
B. Real-Time
C. Scheduled
D. Continuous
Answer: (SHOW ANSWER)
Real-time searches run continuously, processing events as they are indexed, and are used for immediate detection and alerting.

NEW QUESTION: 9
Which of the following actions would not reduce the number of false positives from a correlation search?
A. Reducing the severity.
B. Removing throttling fields.
C. Increasing the throttling window.
D. Increasing threshold sensitivity.
Answer: (SHOW ANSWER)
Reducing the severity of a correlation search does not impact the actual number of false positives generated. Instead, it changes how critical those alerts appear but does not affect the underlying logic or frequency of the alerts.

NEW QUESTION: 10
What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?
Freecram.net
A. 50 GB
B. 100 GB
C. 300 GB
D. 500 MB
Answer: (SHOW ANSWER)

https://docs.splunk.com/Documentation/ES/4.7.4/Install/DeploymentPlanning#Splunk_Enterprise_system_requirement

NEW QUESTION: 11
Adaptive response action history is stored in which index?
A. cim_modactions
B. modular_history
C. cim_adaptiveactions
D. modular_action_history
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

NEW QUESTION: 12
What do threat gen searches produce?
A. Threat correlation searches.
B. Threat intel in KV Store collections.
C. Events in the threat_activity index.
D. Threat notables in the notable index.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

NEW QUESTION: 13
Which of the following is a way to test for a property normalized data model?
A. Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.
B. Run a | datamodel search, compare results to the CIM documentation for the datamodel.
C. Use Audit -> Normalization Audit and check the Errors panel.
D. Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.
Answer: (SHOW ANSWER)

NEW QUESTION: 14
In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?
A. Save the settings.
B. Apply the correct tags.
C. Run the correct search.
D. Visit the CIM dashboard.
Answer: (SHOW ANSWER)
The order would be: Eventtypes -> Tags -> Data model definition -> Data model acceleration -> Searches

NEW QUESTION: 15
What does the risk framework add to an object (user, server or other type) to indicate increased risk?
A. An urgency.
B. A risk profile.
C. An aggregation.
D. A numeric score.
Answer: (SHOW ANSWER)
This numeric score quantifies the level of risk associated with the object, allowing for better assessment and prioritization of potential threats.

NEW QUESTION: 16
When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?
A. $fieldname$
B. "fieldname"
C. %fieldname%
D. _fieldname_
Answer: (SHOW ANSWER)
This notation allows dynamic content to be included in the notable event, pulling directly from the fields within the event data itself.

Valid SPLK-3001 Dumps shared by EduDump.com for Helping Passing SPLK-3001 Exam! EduDump.com now offer the **newest SPLK-3001 exam dumps**, the EduDump.com SPLK-3001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-3001 dumps with Test Engine here: https://www.edudump.com/exams/Splunk/SPLK-3001/premium/ (**118** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 17
The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of data.
What data model should be checked for potential errors such as skipped searches?
A. Web
B. Risk
C. Performance
D. Authentication
Answer: (SHOW ANSWER)

https://docs.splunk.com/Documentation/ES/6.6.0/Admin/Dashboardrequirements - check user activity dashboard, remote access panel

NEW QUESTION: 18
A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications. All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance.
What is the best practice for installing ES?
A. Install ES on the existing search head.
B. Add a new search head and install ES on it.
C. Increase the number of CPUs and amount of memory on the search head, then install ES.
D. Delete the non-CIM-compliant apps from the search head, then install ES.
Answer: (SHOW ANSWER)
https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

NEW QUESTION: 19
Which object in Splunk ES stores external threat indicators such as malicious IP addresses?
A. Threat intelligence collections maintain imported indicators for security event matching processes.
B. Summary indexes archive accelerated search results for optimized reporting performance requirements.
C. Search macros simplify repetitive search syntax within enterprise security correlation searches.
D. Event sequencing configurations define ordered detection logic for incident investigation workflows.
Answer: (SHOW ANSWER)
Threat intelligence collections store imported indicators that Splunk ES compares against indexed events to identify communications or activity involving known threats.

NEW QUESTION: 20
What feature of Enterprise Security downloads threat intelligence data from a web server?
A. Threat Service Manager
B. Threat Download Manager
C. Threat Intelligence Parser
D. Threat Intelligence Enforcement
Answer: (SHOW ANSWER)
The Threat Intelligence Framework provides a modular input (Threat Intelligence Downloads) that handles the majority of configurations typically needed for downloading intelligence files & data. To access this modular input, you simply need to create a stanza in your Inputs.conf file called "threatlist".

NEW QUESTION: 21

Both 'Recommended Actions' and 'Adaptive Response Actions' use adaptive response. How do they differ?
A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
D. Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.
Answer: B (LEAVE A REPLY)
Identifying Recommended Adaptive Responses will highlight those actions for the analyst when looking at the list of response actions available, making it easier to find them among the longer list of available actions.

NEW QUESTION: 22
After managing source types and extracting fields, which key step comes next in the Add-On Builder?
A. Configure data collection.
B. Validate and package.
C. Create alert actions.
D. Map to data models.
Answer: (SHOW ANSWER)
This step ensures that the data is appropriately structured and aligned with the Common Information Model (CIM), facilitating better integration and usability within the Splunk environment.

NEW QUESTION: 23
How is notable event urgency calculated?
A. Asset priority and threat weight.
B. Alert severity found by the correlation search.
C. Asset or identity risk and severity found by the correlation search.
D. Severity set by the correlation search and priority assigned to the associated asset or identity.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 24
Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?
A. SplunkWeb (8000), Splunk Management (8089), KV Store (8191)
B. SplunkWeb (8088), Splunk Management (8089), KV Store (8000)

C. SplunkWeb (8043), Splunk Management (8088), KV Store (8191)
D. SplunkWeb (8386), Splunk Management (8926), KV Store (8106)
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/Splunk/8.1.2/Security/SecureSplunkonyournetwork

NEW QUESTION: 25
When using distributed configuration management to create the Splunk_TA_ForIndexers package, which three files can be included?
A. indexes.conf, props.conf, transforms.conf
B. web.conf, props.conf, transforms.conf
C. inputs.conf, props.conf, transforms.conf
D. eventtypes.conf, indexes.conf, tags.conf
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

NEW QUESTION: 26
Which dashboard is commonly used to review and triage notable security events?
A. Incident review dashboard centralizes analyst triage and investigation management workflows effectively.
B. Protocol intelligence dashboard analyzes network communication protocol distribution and bandwidth utilization.
C. Search activity dashboard tracks user-generated search execution and resource consumption statistics.
D. Monitoring console dashboard measures infrastructure health across distributed Splunk deployment components continuously.
Answer: (SHOW ANSWER)
Incident Review is the primary workspace for analysts to triage, prioritize, assign, and investigate notable events generated by correlation searches.

NEW QUESTION: 27
How is it possible to specify an alternate location for accelerated storage?
A. Use the tStatsHomePath setting in indexes.conf
B. Update the Home Path setting in indexes.conf
C. Use the tstatsHomePath setting in props.conf
D. Configure storage optimization settings for the index.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/latest/Install/Datamodels#Configuring_storage_volumes

NEW QUESTION: 28
Where is it possible to export content, such as correlation searches, from ES?

A. Content exporter
B. Configure -> Content Management
C. Export content dashboard
D. Settings Menu -> ES -> Export
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

NEW QUESTION: 29
Which Splunk ES feature automatically prioritizes notable events by predefined security risk scores?
A. Risk-based alerting calculates cumulative entity risk from correlated detections.
B. Data model acceleration improves search speed across indexed enterprise datasets.
C. Adaptive response actions trigger automated remediation after notable event generation.
D. Asset and identity correlation enriches events with contextual organizational metadata.
Answer: (SHOW ANSWER)
Risk-based alerting aggregates risk modifiers from multiple detections, helping analysts prioritize entities showing suspicious patterns instead of investigating isolated low-priority alerts individually.

NEW QUESTION: 30
Which data model populates the panels on the Risk Analysis dashboard?
A. Audit
B. Domain analysis
C. Risk
D. Threat intelligence
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Who can delete an investigation?
A. ess_admin users only.
B. The investigation owner only.
C. The investigation owner and ess-admin.
D. The investigation owner and collaborators.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

Valid SPLK-3001 Dumps shared by EduDump.com for Helping Passing SPLK-3001 Exam! EduDump.com now offer the **newest SPLK-3001 exam dumps**, the EduDump.com SPLK-3001 exam **questions have been updated** and **answers have been corrected** get the

newest EduDump.com SPLK-3001 dumps with Test Engine here: https://www.edudump.com/exams/Splunk/SPLK-3001/premium/ (**118** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 32
At what point in the ES installation process should Splunk_TA_ForIndexers.spl be deployed to the indexers?
A. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.
B. When adding apps to the deployment server.
C. Splunk_TA_ForIndexers.spl is installed first.
D. After installing ES on the search head(s) and running the distributed configuration management tool.
Answer: (SHOW ANSWER)

NEW QUESTION: 33
Which of the following features can the Add-on Builder configure in a new add-on?
A. Expire data.
B. Normalize data.
C. Summarize data.
D. Translate data.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

NEW QUESTION: 34
What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?
A. Configure -> Incident Management -> Notable Event Statuses
B. Configure -> Content Management -> Type: Correlation Search
C. Configure -> Incident Management -> Incident Review Settings -> Event Management
D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/CustomizeIR
Change Incident Review columns
You can change the columns displayed on the Incident Review dashboard.
Review the existing columns in Incident Review - Table Attributes.
Use the action column to edit, remove, or change the order of the available columns.
Add custom columns by selecting Insert below or selecting More..., then Insert above.

NEW QUESTION: 35
When ES content is exported, an app with a .spl extension is automatically created.

What is the best practice when exporting and importing updates to ES content?

A. Use new app names each time content is exported.

B. Do not use the .spl extension when naming an export.

C. Always include existing and new content for each export.

D. Either use new app names or always include both existing and new content.

Answer: (SHOW ANSWER)

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

NEW QUESTION: 36

What kind of value is in the red box in this picture?



A. A risk score.

B. An event priority.

C. An IP address rating.

D. A source ranking.

Answer: (SHOW ANSWER)

NEW QUESTION: 37

Which of the following is an adaptive action that is configured by default for ES?

A. Create new asset

B. Create notable event

C. Create investigation

D. Create new correlation search

Answer: (SHOW ANSWER)

https://docs.splunk.com/Documentation/ES/6.6.2/Admin/Configureadaptiveresponse#Included_adaptive_response_actions

NEW QUESTION: 38

What is the purpose of the KV Store in Splunk Enterprise Security?

A. Store structured application data supporting lookups and ES functionality requirements.

B. Accelerate distributed searches using clustered index replication optimization across environments automatically.

C. Normalize raw authentication events into Common Information Model compliant field structures.
D. Visualize executive dashboards summarizing enterprise-wide security incident management statistics efficiently.
Answer: (SHOW ANSWER)
KV Store provides flexible structured storage used for lookups, investigation workflows, risk data, and application state management inside Enterprise Security deployments.

NEW QUESTION: 39
After installing Enterprise Security, the distributed configuration management tool can be used to create which app to configure indexers?
A. Splunk_DS_ForIndexers.spl
B. Splunk_ES_ForIndexers.spl
C. Splunk_SA_ForIndexers.spl
D. Splunk_TA_ForIndexers.spl
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

NEW QUESTION: 40
Which tool is used to update indexers in ES?
A. Distributed Configuration Management
B. Index Updater
C. indexes.conf
D. Splunk_TA_ForIndexers.spl
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/7.1.1/Install/InstallTechnologyAdd-ons

NEW QUESTION: 41
Which two fields combine to create the Urgency of a notable event?
A. Priority and Severity.
B. Priority and Criticality.
C. Criticality and Severity.
D. Precedence and Time.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.4.1/User/Howurgencyisassigned

NEW QUESTION: 42
Which component normalizes events?
A. SA-Notable.
B. ES application.
C. SA-CIM.

D. Technology add-on.
Answer: (SHOW ANSWER)

NEW QUESTION: 43
Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?
A. Security domains.
B. Threat intel.
C. Assets.
D. Domains.
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

NEW QUESTION: 44
What is an example of an ES asset?
A. MAC address
B. User name
C. People
D. Server
Answer: D (LEAVE A REPLY)
In the context of Enterprise Security (ES), an asset typically refers to physical or virtual devices within the network, such as servers, workstations, or network devices.

NEW QUESTION: 45
Which of the following ES features would a security analyst use while investigating a network anomaly notable?
A. Correlation editor.
B. Key indicator search.
C. Threat download dashboard.
D. Protocol intelligence dashboard.
Answer: D (LEAVE A REPLY)
https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

NEW QUESTION: 46
An administrator is asked to configure an "Nslookup" adaptive response action, so that it appears as a selectable option in the notable event's action menu when an analyst is working in the Incident Review dashboard.
What steps would the administrator take to configure this option?
A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

B. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup
C. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
Answer: (SHOW ANSWER)

Valid SPLK-3001 Dumps shared by EduDump.com for Helping Passing SPLK-3001 Exam! EduDump.com now offer the **newest SPLK-3001 exam dumps**, the EduDump.com SPLK-3001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-3001 dumps with Test Engine here: https://www.edudump.com/exams/Splunk/SPLK-3001/premium/ (**118** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 47
ES needs to be installed on a search head with which of the following options?
A. No other apps.
B. Any other apps installed.
C. All apps removed except for TA-*.
D. Only default built-in and CIM-compliant apps.
Answer: (SHOW ANSWER)
This ensures compatibility and proper functionality of the ES app, avoiding potential conflicts with non-compliant or non-default apps.

NEW QUESTION: 48
What is the primary purpose of adaptive response actions within Splunk Enterprise Security?
A. Automate security workflows and integrate remediation actions with external systems.
B. Accelerate correlation searches using optimized data model search summarization processes.
C. Store historical threat intelligence indicators within dedicated indexed lookup repositories.
D. Generate executive compliance reports based on indexed notable security event trends.
Answer: (SHOW ANSWER)
Adaptive response actions extend ES capabilities by triggering automated workflows, ticketing, notifications, or containment activities through integrated third-party security platforms.

NEW QUESTION: 49
A customer site is experiencing poor performance. The UI response time is high and searches take a very long time to run. Some operations time out and there are errors in the scheduler logs, indicating too many concurrent searches are being started. 6 total correlation searches are scheduled and they have already been tuned to weed out false positives.
Which of the following options is most likely to help performance?

A. Increase memory and CPUs on the search head(s) and add additional indexers.
B. Add heavy forwarders between the universal forwarders and indexers so inputs can be parsed before indexing.
C. If indexed realtime search is enabled, disable it for the notable index.
D. Change the search heads to do local indexing of summary searches.
Answer: (SHOW ANSWER)

NEW QUESTION: 50
Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?
Freecram.net
A. VIP
B. Priority
C. Importance
D. Criticality
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.6.2/User/Howurgencyisassigned

NEW QUESTION: 51
Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?
A. Indexers might crash.
B. Indexers might be processing.
C. Indexers might not be reachable.
D. Indexers have different settings.
Answer: D (LEAVE A REPLY)
https://community.splunk.com/t5/Splunk-Enterprise-Security/Splunk-Enterprise-Security-requires-a-deployment-client-but/m-p/279749

NEW QUESTION: 52
An administrator is provisioning one search head prior to installing ES.
What are the reference minimum requirements for OS, CPU, and RAM for that machine?
A. OS: 32 bit, RAM: 16 MB, CPU: 12 cores
B. OS: 64 bit, RAM: 32 MB, CPU: 12 cores
C. OS: 64 bit, RAM: 12 MB, CPU: 16 cores
D. OS: 64 bit, RAM: 32 MB, CPU: 16 cores
Answer: (SHOW ANSWER)
https://docs.splunk.com/Documentation/ES/6.4.0/Install/DeploymentPlanning

Valid SPLK-3001 Dumps shared by EduDump.com for Helping Passing SPLK-3001 Exam! EduDump.com now offer the **newest SPLK-3001 exam dumps**, the EduDump.com SPLK-3001 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SPLK-3001 dumps with Test Engine here: https://www.edudump.com/exams/Splunk/SPLK-3001/premium/ (**118** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)