Splunk.SPLK-3001.v2023-09-01.q91

Exam Code:	SPLK-3001
Exam Name:	Splunk Enterprise Security Certified Admin Exam
Certification Provider:	Splunk
Free Question Number:	91
Version:	v2023-09-01
# of views:	103
# of Questions views:	947
https://www.freecram.net/torrent/Splunk.SPLK-3001.v2023-09-01.q91.html	

NEW QUESTION: 1
When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?
A. Nothing, there are no additional steps for add-ons.
B. Configure the add-ons via the Content Management dashboard.
C. Disable the add-ons until they are ready to be used, then enable the add-ons.
D. Configure the add-ons according to their README or documentation.
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/Install/Planyourdatainputs

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)
Reference:
the.html

NEW QUESTION: 3
Which data model populated the panels on the Risk Analysis dashboard?
A. Risk
B. Audit
C. Domain analysis

D. Threat intelligence
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

NEW QUESTION: 4
Which indexes are searched by default for CIM data models?
A. notable and default
B. All indexes
C. _internal and summary
D. summary and notable
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which of the following are examples of sources for events in the endpoint security domain dashboards?
A. Investigation final results status.
B. Workstations, notebooks, and point-of-sale systems.
C. Lifecycle auditing of incidents, from assignment to resolution.
D. REST API invocations.
Answer: (SHOW ANSWER)

NEW QUESTION: 6
When investigating, what is the best way to store a newly-found IOC?
A. Add it in a text note to the investigation.
B. Click the "Add IOC" button.
C. Click the "Add Artifact" button.
D. Paste it into Notepad.
Answer: (SHOW ANSWER)

NEW QUESTION: 7
After managing source types and extracting fields, which key step comes next In the Add-On Builder?
A. Map to data models.
B. Configure data collection.
C. Create alert actions.
D. Validate and package
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which of the following is a recommended pre-installation step?

A. Download the latest version of KV Store from MongoDBxom.
B. Install the latest Python distribution on the search head.
C. Configure search head forwarding.
D. Disable the default search app.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
ES apps and add-ons from $SPLUNK_HOME/etc/appsshould be copied from the staging instance to what location on the cluster deployer instance?
A. $SPLUNK_HOME/etc/master-apps/
B. $SPLUNK_HOME/etc/system/local/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/var/run/searchpeers/
Answer: (SHOW ANSWER)
The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/ etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in $SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into $SPLUNK_HOME/etc/ disabled-apps on staging

NEW QUESTION: 10
What kind of value is in the red box in this picture?

A. A risk score.
B. A source ranking.
C. An event priority.
D. An IP address rating.

Answer: C (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

NEW QUESTION: 11
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)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Formatassetoridentitylist

NEW QUESTION: 12
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)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

NEW QUESTION: 13
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: (SHOW ANSWER)
Explanation/Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

NEW QUESTION: 14
Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?
A. VIP

B. Priority
C. Importance
D. Criticality
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 15
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)
Reference:
https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

NEW QUESTION: 16
Accelerated data requires approximately how many times the daily data volume of additional storage space per year?
A. 2.5
B. 3.4
C. 1.0
D. 5.7
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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)

NEW QUESTION: 18
"10.22.63.159", "websvr4", and "00:26:08:18: CF:1D" would be matched against what in ES?
A. An asset.
B. A device.
C. A user.
D. An identity.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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)
Explanation/Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

NEW QUESTION: 20
What kind of value is in the red box in this picture?

A. A risk score.
B. A source ranking.
C. An event priority.
D. An IP address rating.
Answer: (SHOW ANSWER)

Explanation/Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

NEW QUESTION: 21
Which of the following is a key feature of a glass table?
A. Rigidity.
B. Interactive investigations.
C. Customization.
D. Strong data for later retrieval.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?
A. VIP
B. Priority
C. Importance
D. Criticality
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 23
Enterprise Security's dashboards primarily pull data from what type of knowledge object?
A. Data models
B. Tstats
C. KV Store
D. Dynamic lookups
Answer: (SHOW ANSWER)

NEW QUESTION: 24
What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?
A. 50 GB
B. 100 GB
C. 300 GB
D. 500 MB
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

NEW QUESTION: 25
What can be exported from ES using the Content Management page?
A. Any content type listed in the Content Management page.
B. Only correlation searches, glass tables, and workbench panels.
C. Only correlation searches, managed lookups, and glass tables.
D. Only correlation searches.
Answer: A (LEAVE A REPLY)
Reference:
%20content%20from%20Splunk%20Enterprise%20Security%20as,from%20the%20Content%20Management%20page.&text=You%20can%20export%20any%20type,%2C%20data%20models%2C%20and%20views.

NEW QUESTION: 26
What does the Security Posture dashboard display?
A. Active investigations and their status.
B. A high-level overview of notable events.
C. Current threats being tracked by the SOC.
D. A display of the status of security tools.
Answer: (SHOW ANSWER)
The Security Posture dashboard is designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a Security Operations Center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/SecurityPosturedashboard

NEW QUESTION: 27
What feature of Enterprise Security downloads threat intelligence data from a web server?
A. Threat Download Manager
B. Therat Intelligence Enforcement
C. Threat Intelligence Parser
D. Threat Service Manager
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: 28
Which of the following are the default ports that must be configured for Splunk Enterprise Security to function?

A. SplunkWeb (8043), Splunk Management (8088), KV Store (8191)
B. SplunkWeb (8000), Splunk Management (8089), KV Store (8191)
C. SplunkWeb (8390), Splunk Management (8323), KV Store (8672)
D. SplunkWeb (8068), Splunk Management (8089), KV Store (8000)
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.4.1/User/Howurgencyisassigned

NEW QUESTION: 30
What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?

A. ess_reviewer
B. ess_analyst
C. ess_user
D. ess_admin
Answer: (SHOW ANSWER)

NEW QUESTION: 31
Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?
A. A suffix of .spl
B. A prefix of CIM_
C. A prefix of TECH_
D. A prefix of Splunk_TA_
Answer: (SHOW ANSWER)

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

NEW QUESTION: 33
Both "Recommended Actions" and "Adaptive Response Actions" use adaptive response. How do they differ?
A. Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.
B. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
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 Responses to an analyst, Adaptive Response Actions run them automatically.
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

NEW QUESTION: 35
Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?
A. Priority

B. Importance
C. VIP
D. Criticality
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which settings indicated 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)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

NEW QUESTION: 37
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)
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION: 38
How is it possible to navigate to the list of currently-enabled ES correlation searches?
A. Settings -> Searches, Reports, and Alerts -> Filter by Name of "Correlation"
B. Configure -> Correlation Searches -> Select Status "Enabled"
C. Configure -> Content Management -> Select Type "Correlation" and Status "Enabled"
D. Settings -> Searches, Reports, and Alerts -> Select App of "SplunkEnterpriseSecuritySuite" and filter by "- Rule"
Answer: (SHOW ANSWER)

NEW QUESTION: 39
What should be used to map a non-standard field name to a CIM field name?
A. Field alias.
B. Search time extraction.
C. Tag.
D. Eventtype.
Answer: (SHOW ANSWER)

Explanation

NEW QUESTION: 40

Where is the Add-On Builder available from?

A. The ES installation package

B. GitHub

C. www.splunk.com

D. SplunkBase

Answer: (SHOW ANSWER)

NEW QUESTION: 41

Which of the following is part of tuning correlation searches for a new ES installation?

A. Configuring correlation result storage.

B. Configuring correlation adaptive responses.

C. Configuring correlation notable event index.

D. Configuring correlation permissions.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 42

Which of the following threat intelligence types can ES download? (Choose all that apply)

A. STIX/TAXII

B. Text

C. VulnScanSPL

D. SplunkEnterpriseThreatGenerator

Answer: (SHOW ANSWER)

NEW QUESTION: 43

What do threat gen searches produce?

A. Threat Intel in KV Store collections.

B. Threat correlation searches.

C. Threat notables in the notable index.

D. Events in the threat_activity index.

Answer: (SHOW ANSWER)

Explanation

https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

NEW QUESTION: 44

At what point in the ES installation process should Splunk_TA_ForIndexes.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. Splunk_TA_ForIndexers.spl is installed first.
C. After installing ES on the search head(s) and running the distributed configuration management tool.
D. When adding apps to the deployment server.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
Which of the following threat intelligence types can ES download? (Choose all that apply)
A. Text
B. SplunkEnterpriseThreatGenerator
C. VulnScanSPL
D. STIX/TAXII
Answer: (SHOW ANSWER)

NEW QUESTION: 46
How is it possible to navigate to the list of currently-enabled ES correlation searches?
A. Configure -> Content Management -> Select Type "Correlation" and Status "Enabled"
B. Configure -> Correlation Searches -> Select Status "Enabled"
C. Settings -> Searches, Reports, and Alerts -> Select App of "SplunkEnterpriseSecuritySuite" and filter by
"- Rule"
D. Settings -> Searches, Reports, and Alerts -> Filter by Name of "Correlation"
Answer: (SHOW ANSWER)

NEW QUESTION: 47
Which settings indicated 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)
Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

NEW QUESTION: 48
Which of the following actions would not reduce the number of false positives from a correlation search?
A. Increasing threshold sensitivity.
B. Reducing the severity.
C. Increasing the throttling window.
D. Removing throttling fields.
Answer: (SHOW ANSWER)

NEW QUESTION: 49
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)

NEW QUESTION: 50
What does the risk framework add to an object (user, server or other type) to indicate increased risk?
A. A numeric score.
B. An aggregation.
C. A risk profile.
D. An urgency.
Answer: (SHOW ANSWER)

NEW QUESTION: 51
What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?
A. ess_admin
B. ess_analyst
C. ess_user
D. ess_reviewer
Answer: (SHOW ANSWER)

NEW QUESTION: 52
After data is ingested, which data management step is essential to ensure raw data can be accelerated by a Data Model and used by ES?
A. Applying Tags.
B. Normalization to the Splunk Common Information Model.
C. Normalization to Customer Standard.
D. Extracting Fields.
Answer: (SHOW ANSWER)

NEW QUESTION: 53
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. Either use new app names or always include both existing and new content.
D. Always include existing and new content for each export.
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: 54
Which indexes are searched by default for CIM data models?
A. notable and default
B. summary and notable
C. _internal and summary
D. All indexes
Answer: (SHOW ANSWER)
Explanation/Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

NEW QUESTION: 55
What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?
A. Configure -> Incident Management -> Incident Review Settings -> Event Management
B. Configure -> Incident Management -> Incident Review Settings -> Table Attributes
C. Configure -> Incident Management -> Notable Event Statuses
D. Configure -> Content Management -> Type: Correlation Search
Answer: (SHOW ANSWER)

NEW QUESTION: 56

Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?

A. A prefix of CIM_

B. A suffix of .spl

C. A prefix of TECH_

D. A prefix of Splunk_TA_

Answer: (SHOW ANSWER)

Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

NEW QUESTION: 57

Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. Lifecycle auditing of incidents, from assignment to resolution.

B. Workstations, notebooks, and point-of-sale systems.

C. REST API invocations.

D. Investigation final results status.

Answer: (SHOW ANSWER)

NEW QUESTION: 58

Where is the Add-On Builder available from?

A. GitHub

B. SplunkBase

C. www.splunk.com

D. The ES installation package

Answer: (SHOW ANSWER)

Reference:
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

NEW QUESTION: 59

Analysts have requested the ability to capture and analyze network traffic dat a. The administrator has researched the documentation and, based on this research, has decided to integrate the Splunk App for Stream with ES.

Which dashboards will now be supported so analysts can view and analyze network Stream data?

A. User Intelligence dashboards.

B. Web Intelligence dashboards.

C. Endpoint dashboards.

D. Protocol Intelligence dashboards.

Answer: (SHOW ANSWER)

NEW QUESTION: 60
What is the first step when preparing to install ES?
A. Install ES.
B. Determine the data sources used.
C. Determine the hardware required.
D. Determine the size and scope of installation.
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 61
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)
Explanation
Explanation/Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

NEW QUESTION: 62
Which of the following are data models used by ES? (Choose all that apply.)
A. Web
B. Anomalies
C. Authentication
D. Network Traffic
Answer: (SHOW ANSWER)
Explanation/Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

NEW QUESTION: 63

Which of the following features can the Add-on Builder configure in a new add-on?
A. Summarize data.
B. Translate data.
C. Expire data.
D. Normalize data.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
What does the risk framework add to an object (user, server or other type) to indicate increased risk?
A. A risk profile.
B. An urgency.
C. An aggregation.
D. A numeric score.
Answer: (SHOW ANSWER)

NEW QUESTION: 65
ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?
A. $SPLUNK_HOME/etc/master-apps/
B. $SPLUNK_HOME/etc/system/local/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/var/run/searchpeers/
Answer: (SHOW ANSWER)
The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in $SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into $SPLUNK_HOME/etc/disabled-apps on staging

NEW QUESTION: 66
Which of the following is part of tuning correlation searches for a new ES installation?
A. Configuring correlation permissions.
B. Configuring correlation result storage.
C. Configuring correlation notable event index.
D. Configuring correlation adaptive responses.
Answer: (SHOW ANSWER)

NEW QUESTION: 67
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 -> Nslookup
B. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
C. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
Answer: (SHOW ANSWER)

NEW QUESTION: 68
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)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

NEW QUESTION: 69
Which of the following is a way to test for a property normalized data model?
A. Use Audit -> Normalization Audit and check the Errors panel.
B. Run a | datamodelsearch, compare results to the CIM documentation for the datamodel.
C. Run a | loadjobsearch, look at tag values and compare them to known tags based on the encoding.
D. Run a | datamodelsearch and compare the results to the list of data models in the ES normalization guide.
Answer: (SHOW ANSWER)
Explanation/Reference:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

NEW QUESTION: 70
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: D (LEAVE A REPLY)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

NEW QUESTION: 71
How should an administrator add a new lookup through the ES app?
A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions
B. Upload the lookup file in Settings -> Lookups -> Lookup table files
C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups
D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups

NEW QUESTION: 72
ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?
A. $SPLUNK_HOME/etc/system/local/
B. $SPLUNK_HOME/var/run/searchpeers/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/etc/master-apps/
Answer: (SHOW ANSWER)
The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in $SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into $SPLUNK_HOME/etc/disabled-apps on staging

NEW QUESTION: 73
What are adaptive responses triggered by?
A. By correlation searches and users on the threat analysis dashboard.
B. By correlation searches and users on the incident review dashboard.
C. By custom tech add-ons and users on the risk analysis dashboard.
D. By correlation searches and custom tech add-ons.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
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)
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis

NEW QUESTION: 75
Where is it possible to export content, such as correlation searches, from ES?
A. Export content dashboard
B. Settings Menu -> ES -> Export
C. Content exporter
D. Configure -> Content Management
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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)
Explanation/Reference: https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html

NEW QUESTION: 77
Adaptive response action history is stored in which index?

A. modular_history
B. cim_modactions
C. modular_action_history
D. cim_adaptiveactions
Answer: (SHOW ANSWER)

NEW QUESTION: 78
What is the main purpose of the Dashboard Requirements Matrix document?
A. Identifies which data model(s) depend on each dashboard.
B. Identifies the searches used by the dashboards.
C. Provides instructions for customizing each dashboard for local data models.
D. Identifies on which data model(s) each dashboard depends.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
What is the first step when preparing to install ES?
A. Determine the data sources used.
B. Install ES.
C. Determine the hardware required.
D. Determine the size and scope of installation.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 80
Which setting is used in indexes.conf to specify alternate locations for accelerated storage?
A. thawedPath
B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript
Answer: (SHOW ANSWER)
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

NEW QUESTION: 81
If a username does not match the 'identity' column in the identities list, which column is checked next?
A. IP address.
B. Email.
C. Combination of Last Name, First Name.
D. Nickname
Answer: (SHOW ANSWER)

NEW QUESTION: 82
Where should an ES search head be installed?
A. On a server with a new install of Splunk.
B. On any Splunk server.
C. On a Splunk server with top level visibility.
D. On a Splunk server running Splunk DB Connect.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
When ES content is exported, an app with a .splextension is automatically created.
What is the best practice when exporting and importing updates to ES content?
A. Do not use the .splextension when naming an export.
B. Either use new app names or always include both existing and new content.
C. Always include existing and new content for each export.
D. Use new app names each time content is exported.
Answer: (SHOW ANSWER)

NEW QUESTION: 84
Who can delete an investigation?
A. The investigation owner only.
B. ess_admin users only.
C. The investigation owner and collaborators.
D. The investigation owner and ess-admin.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 85
Which data model populates the panels on the Risk Analysis dashboard?
A. Risk
B. Audit
C. Domain analysis
D. Threat intelligence
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

NEW QUESTION: 86
Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?
A. Domains.
B. Assets.

C. Security domains.
D. Threat intel.
Answer: (SHOW ANSWER)

NEW QUESTION: 87
A newly built custom dashboard needs to be available to a team of security analysts In ES. How is It possible to Integrate the new dashboard?
A. Create a new role Inherited from es_analyst, make the dashboard permissions read-only, and make this dashboard the default view for the new role.
B. Add links on the ES home page to the new dashboard.
C. Set the dashboard permissions to allow access by es_analysts and use the navigation editor to add it to the menu.
D. Add the dashboard to a custom add-in app and install it to ES using the Content Manager.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following are data models used by ES? (Choose all that apply)
A. Network Traffic
B. Web
C. Authentication
D. Anomalies
Answer: (SHOW ANSWER)

NEW QUESTION: 89
When investigating, what is the best way to store a newly-found IOC?
A. Click the "Add Artifact" button.
B. Click the "Add IOC" button.
C. Paste it into Notepad.
D. Add it in a text note to the investigation.
Answer: (SHOW ANSWER)

NEW QUESTION: 90
What do threat gen searches produce?
A. Threat Intel in KV Store collections.
B. Events in the threat_activity index.
C. Threat correlation searches.
D. Threat notables in the notable index.
Answer: (SHOW ANSWER)

NEW QUESTION: 91

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: (SHOW ANSWER)

Reference:

https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/features.html

Valid SPLK-3001 Dumps shared by PassTestKing.com for Helping Passing SPLK-3001 Exam! PassTestKing.com now offer the **newest SPLK-3001 exam dumps**, the PassTestKing.com SPLK-3001 exam **questions have been updated** and **answers have been corrected** get the **newest** PassTestKing.com SPLK-3001 dumps with Test Engine here: https://www.passtestking.com/Splunk/SPLK-3001-practice-exam-dumps.html (**100** Q&As Dumps, **35%OFF** **Special Discount Code:** **freecram**)