SPLK-3001 Dumps

Splunk Enterprise Security Certified Admin Exam

https://www.certleader.com/SPLK-3001-dumps.html

NEW QUESTION 1
The Add-On Builder creates Splunk Apps that start with what?

A. DA-
B. SA-
C. TA-
D. App-

Answer: C

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

NEW QUESTION 2
Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. REST API invocations.
B. Investigation final results status.
C. Workstations, notebooks, and point-of-sale systems.
D. Lifecycle auditing of incidents, from assignment to resolution.

Answer: D

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

NEW QUESTION 3
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: C

Explanation:
Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

NEW QUESTION 4
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: A

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

NEW QUESTION 5
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: C

Explanation:
Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata

NEW QUESTION 6
Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath
B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Accelerateddatamodels

NEW QUESTION 7
How is it possible to navigate to the list of currently-enabled ES correlation searches?

A. Configure -> Correlation Searches -> Select Status "Enabled"
B. Settings -> Searches, Reports, and Alerts -> Filter by Name of "Correlation"
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: A

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

NEW QUESTION 8
At what point in the ES installation process should Splunk_TA_ForIndexes.spl be deployed to the indexers?

A. When adding apps to the deployment server.
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. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.

Answer: B

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

NEW QUESTION 9
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: D

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

NEW QUESTION 10
To observe what network services are in use in a network's activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?

A. Intrusion Center
B. Protocol Analysis
C. User Intelligence
D. Threat Intelligence

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

NEW QUESTION 10
Adaptive response action history is stored in which index?

A. cim_modactions
B. modular_history
C. cim_adaptiveactions
D. modular_action_history

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

NEW QUESTION 13
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: D

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

NEW QUESTION 17
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: C

Explanation:
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 22
What kind of value is in the red box in this picture?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

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

Answer: C

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

NEW QUESTION 26
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: B

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

NEW QUESTION 28
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: B

Explanation:
Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

NEW QUESTION 29
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

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations

NEW QUESTION 32
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: B

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizemenubar#Restore_the_default_navigation

NEW QUESTION 33
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: C

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

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: A

NEW QUESTION 36
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

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

NEW QUESTION 38
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: B

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION 41
Which of the following actions can improve overall search performance?

A. Disable indexed real-time search.
B. Increase priority of all correlation searches.
C. Reduce the frequency (schedule) of lower-priority correlation searches.
D. Add notable event suppressions for correlation searches with high numbers of false positives.

Answer: A

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

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

NEW QUESTION 49
Which component normalizes events?

A. SA-CIM.
B. SA-Notable.
C. ES application.
D. Technology add-on.

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

NEW QUESTION 53
What is the default schedule for accelerating ES Datamodels?

A. 1 minute
B. 5 minutes
C. 15 minutes
D. 1 hour

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

NEW QUESTION 55
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your SPLK-3001 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-3001-dumps.html