SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/splk-3001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

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.

Correct Answer: B

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

QUESTION 2

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"

Correct Answer: C

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

QUESTION 3

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.

Correct Answer: D

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

QUESTION 4

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

A. thawedPath

B. tstatsHomePath

C. summaryHomePath

D. warmToColdScript

Correct Answer: B

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

QUESTION 5

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

Correct Answer: D

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

QUESTION 6

To which of the following should the ES application be uploaded?

A. The indexer.

B. The KV Store.

C. The search head.

D. The dedicated forwarder.

Correct Answer: C

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

QUESTION 7

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?

A. Configure the add-ons according to their README or documentation.

B. Disable the add-ons until they are ready to be used, then enable the add-ons.

C. Nothing, there are no additional steps for add-ons.

D. Configure the add-ons via the Content Management dashboard.

Correct Answer: A

QUESTION 8

Accelerated data requires approximately how many times the daily data volume of additional storage space per year?

A. 3.4

B. 5.7

C. 1.0

D. 2.5

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Install/Datamodels

QUESTION 9

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.

Correct Answer: B

Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logsthe.html

QUESTION 10

Which feature contains scenarios that are useful during ES Implementation?

A. Use Case Library

B. Correlation Searches

C. Predictive Analytics

D. Adaptive Responses

Correct Answer: B

Reference: https://www.splunk.com/pdfs/professional-services/2019/splunk-enterprise-securityimplementation-success.pdf

QUESTION 11

Which component normalizes events?

A. SA-CIM.

B. SA-Notable.

C. ES application.

D. Technology add-on.

Correct Answer: A

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

QUESTION 12

How is it possible to specify an alternate location for accelerated storage?

A. Configure storage optimization settings for the index.

B. Update the Home Path setting in indexes, conf

C. Use the tstatsHomePath setting in props, conf

D. Use the tstatsHomePath Setting in indexes, conf

Correct Answer: C

QUESTION 13

Which tool Is used to update indexers In E5?

A. Index Updater

B. Distributed Configuration Management

C. indexes.conf

D. Splunk_TA_ForIndexeres. spl

Correct Answer: B

QUESTION 14

What is the bar across the bottom of any ES window?

A. The Investigator Workbench.

B. The Investigation Bar.

C. The Analyst Bar.

D. The Compliance Bar.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/User/Startaninvestigation

QUESTION 15

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_user

B. ess_admin

C. ess_analyst

D. ess_reviewer

Correct Answer: B

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