Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

NEW QUESTION 1
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: D

Explanation:
Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

NEW QUESTION 2
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 3
“10.22.63.159”, “websvr4”, and “00:26:08:18: CF:1D” would be matched against what in ES?

A. A user.
B. A device.
C. An asset.
D. An identity.

Answer: B

NEW QUESTION 4
Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

A. Lookup searches.
B. Summarized data.
C. Security metrics.
D. Metrics store searches.

Answer: C

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

NEW QUESTION 5
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: A

NEW QUESTION 6
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 7
Which of the following threat intelligence types can ES download? (Choose all that apply)

A. Text
B. STIX/TAXII
C. VulnScanSPL
D. SplunkEnterpriseThreatGenerator

Answer: B

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

NEW QUESTION 8
Enterprise Security's dashboards primarily pull data from what type of knowledge object?

A. Tstats
B. KV Store
C. Data models
D. Dynamic lookups

Answer: C

Explanation:
Reference: https://docs.splunk.com/Splexicon:Knowledgeobject

NEW QUESTION 9
If a username does not match the 'identity' column in the identities list, which column is checked next?

A. Email.
B. Nickname
C. IP address.
D. Combination of Last Name, First Name.

Answer: C

NEW QUESTION 10
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 10
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: A

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

NEW QUESTION 13
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: A

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

NEW QUESTION 18
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 21
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 24
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-3001 Practice Exam Features:

* SPLK-3001 Questions and Answers Updated Frequently

* SPLK-3001 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-3001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-3001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year