

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

<https://www.2passeasy.com/dumps/SPLK-3001/>



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

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 3

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

Answer: B

Explanation:

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

NEW QUESTION 4

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: B

Explanation:

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

NEW QUESTION 5

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 6

At what point in the ES installation process should Splunk_TA_ForIndexers.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 7

“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 8

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 9

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 -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup
- C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup
- D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

Answer: D

NEW QUESTION 10

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: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables>

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 15

Where is the Add-On Builder available from?

- A. GitHub
- B. SplunkBase
- C. www.splunk.com
- D. The ES installation package

Answer: B

Explanation:

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

NEW QUESTION 16

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.

Answer: C

Explanation:

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

NEW QUESTION 18

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 23

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 24

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 28

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 32

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 33

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: D

NEW QUESTION 35

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-3001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-3001 Product From:

<https://www.2passeasy.com/dumps/SPLK-3001/>

Money Back Guarantee

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