



Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

NEW QUESTION 1

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 2

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 3

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 4

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 | datamodel search, compare results to the CIM documentation for the datamodel.
- C. Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.
- D. Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

Answer: B

Explanation:

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

NEW QUESTION 5

When investigating, what is the best way to store a newly-found IOC?

- A. Paste it into Notepad.
- B. Click the "Add IOC" button.
- C. Click the "Add Artifact" button.
- D. Add it in a text note to the investigation.

Answer: B

NEW QUESTION 6

Which of the following are data models used by ES? (Choose all that apply)

- A. Web
- B. Anomalies
- C. Authentication
- D. Network Traffic

Answer: B

Explanation:

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/>

NEW QUESTION 7

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 8

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 9

Where is it possible to export content, such as correlation searches, from ES?

- A. Content exporter
- B. Configure -> Content Management
- C. Export content dashboard
- D. Settings Menu -> ES -> Export

Answer: B

Explanation:

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

NEW QUESTION 10

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 10

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: B

Explanation:

Reference: <https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf>

NEW QUESTION 14

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 19

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 21

An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?

- A. OS: 32 bit, RAM: 16 MB, CPU: 12 cores
- B. OS: 64 bit, RAM: 32 MB, CPU: 12 cores
- C. OS: 64 bit, RAM: 12 MB, CPU: 16 cores
- D. OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware>

NEW QUESTION 22

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 27

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 31

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 33

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-3001 Practice Test Here](#)