



Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

What feature of Enterprise Security downloads threat intelligence data from a web server?

- A. Threat Service Manager
- B. Threat Download Manager
- C. Threat Intelligence Parser
- D. Threat Intelligence Enforcement

Answer: B

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 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 Responses 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

What does the Security Posture dashboard display?

- A. Active investigations and their status.
- B. A high-level overview of notable events.
- C. Current threats being tracked by the SOC.
- D. A display of the status of security tools.

Answer: B

Explanation:

The Security Posture dashboard is designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a Security Operations Center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.

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

NEW QUESTION 10

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

Answer: D

Explanation:

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

NEW QUESTION 15

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 16

Which of the following is a key feature of a glass table?

- A. Rigidity.
- B. Customization.
- C. Interactive investigations.
- D. Strong data for later retrieval.

Answer: B

NEW QUESTION 19

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 24

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 25

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 28

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 33

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 37

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 39

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 44

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 46

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 47

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.

Answer: B

Explanation:

Reference: <https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html>

NEW QUESTION 50

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 52

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 57

.....

Relate Links

100% Pass Your SPLK-3001 Exam with Exambible Prep Materials

<https://www.exambible.com/SPLK-3001-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>