

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

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



NEW QUESTION 1

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. Therat Intelligence Enforcement

Answer: B

NEW QUESTION 2

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 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 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 5

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 6

Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?

- A. Indexes might crash.
- B. Indexes might be processing.
- C. Indexes might not be reachable.
- D. Indexes have different settings.

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf>

NEW QUESTION 7

What kind of value is in the red box in this picture?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

- A. A risk score.
- B. A source ranking.
- C. An event priority.
- D. An IP address rating.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector>

NEW QUESTION 8

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 9

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 10

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 10

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 14

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 18

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 22

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 24

Which component normalizes events?

- A. SA-CIM.
- B. SA-Notable.
- C. ES application.
- D. Technology add-on.

Answer: A

Explanation:

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

NEW QUESTION 29

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 34

.....

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