

Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam



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

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 3

What does the risk framework add to an object (user, server or other type) to indicate increased risk?

- A. An urgency.
- B. A risk profile.
- C. An aggregation.
- D. A numeric score.

Answer: C

Explanation:

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

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

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 6

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 7

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 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

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

Which data model populated the panels on the Risk Analysis dashboard?

- A. Risk
- B. Audit
- C. Domain analysis
- D. Threat intelligence

Answer: A

Explanation:

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

NEW QUESTION 10

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 13

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 15

.....

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](#)