SPLK-3001$^{\text{Q\&As}}$

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

QUESTION 1

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.

Correct Answer: D

Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/ features.html

QUESTION 2

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.

Correct Answer: A

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

QUESTION 3

How is it possible to navigate to the ES graphical Navigation Bar editor?

A. Configure -> Navigation Menu

B. Configure -> General -> Navigation

C. Settings -> User Interface -> Navigation -> Click on "Enterprise Security"

D. Settings -> User Interface -> Navigation Menus -> Click on "default" next to SplunkEnterpriseSecuritySuite

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/
Customizemenubar#Restore_the_default_navigation

QUESTION 4

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.

Correct Answer: C

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

QUESTION 5

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.

Correct Answer: D

QUESTION 6

The option to create a Short ID for a notable event is located where?

A. The Additional Fields.

B. The Event Details.

C. The Contributing Events.

D. The Description.

Correct Answer: B

https://docs.splunk.com/Documentation/ES/6.4.1/User/Takeactiononanotableevent

QUESTION 7

Following the Installation of ES, an admin configured Leers with the ?s_uso r role the ability to close notable events. How would the admin restrict these users from being able to change the status of Resolved notable events to closed?

A. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the closed status.

B. From the Status Configuration windows select the closed status. Remove ess_use r from the status transitions for the Resolved status.

C. In Enterprise Security, give the ess_user role the own Notable Events permission.

D. From Splunk Access Controls, select the ess_user role and remove the edit_notabie_events capability.

Correct Answer: B

QUESTION 8

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

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

QUESTION 9

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.

Correct Answer: C

QUESTION 10

What do threat gen searches produce?

A. Threat Intel in KV Store collections.

B. Threat correlation searches.

C. Threat notables in the notable index.

D. Events in the threat_activity index.

Correct Answer: D

https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

---

QUESTION 11

Which argument to the | tstats command restricts the search to summarized data only?

A. summaries=t

B. summaries=all

C. summariesonly=t

D. summariesonly=all

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

---

QUESTION 12

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.

Correct Answer: A

QUESTION 13

How is it possible to specify an alternate location for accelerated storage?

A. Configure storage optimization settings for the index.

B. Update the Home Path setting in indexes, conf

C. Use the tstatsHomePath setting in props, conf

D. Use the tstatsHomePath Setting in indexes, conf

Correct Answer: C

QUESTION 14

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

Correct Answer: D

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

QUESTION 15

Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?

A. Security domains.

B. Threat intel.

C. Assets.

D. Domains.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Manageinternallookups

Latest SPLK-3001 Dumps SPLK-3001 VCE Dumps SPLK-3001 Exam Questions