SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-3001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What are adaptive responses triggered by?

A. By correlation searches and users on the incident review dashboard.

B. By correlation searches and custom tech add-ons.

C. By correlation searches and users on the threat analysis dashboard.

D. By custom tech add-ons and users on the risk analysis dashboard.

Correct Answer: D

QUESTION 2

A newly built custom dashboard needs to be available to a team of security analysts In ES. How is It possible to Integrate the new dashboard?

A. Add links on the ES home page to the new dashboard.

B. Create a new role Inherited from es_analyst, make the dashboard permissions read-only, and make this dashboard the default view for the new role.

C. Set the dashboard permissions to allow access by es_analysts and use the navigation editor to add it to the menu.

D. Add the dashboard to a custom add-in app and install it to ES using the Content Manager.

Correct Answer: C

QUESTION 3

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 4

Which lookup table does the Default Account Activity Detected correlation search use to flag known default accounts?

A. Administrative Identities

B. Local User Intel

C. Identities

D. Privileged Accounts

Correct Answer: C

QUESTION 5

Enterprise Security\\'s dashboards primarily pull data from what type of knowledge object?

A. Tstats

B. KV Store

C. Data models

D. Dynamic lookups

Correct Answer: C

Reference: https://docs.splunk.com/Splexicon:Knowledgeobject