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.geekcert.com/splk-3001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

How is it possible to navigate to the list of currently-enabled ES correlation searches?

A. Configure -> Correlation Searches -> Select Status "Enabled"

B. Settings -> Searches, Reports, and Alerts -> Filter by Name of "Correlation"

C. Configure -> Content Management -> Select Type "Correlation" and Status "Enabled"

D. Settings -> Searches, Reports, and Alerts -> Select App of "SplunkEnterpriseSecuritySuite" and filter by "-Rule"

Correct Answer: C

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

QUESTION 2

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.

Correct Answer: A

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

QUESTION 3

Which of the following steps will make the Threat Activity dashboard the default landing page in ES?

A. From the Edit Navigation page, drag and drop the Threat Activity view to the top of the page.

B. From the Preferences menu for the user, select Enterprise Security as the default application.

C. From the Edit Navigation page, click the \\'Set this as the default view" checkmark for Threat Activity.

D. Edit the Threat Activity view settings and checkmark the Default View option.

Correct Answer: C

QUESTION 4

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.

Correct Answer: D

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

QUESTION 5

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.

Correct Answer: B

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

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