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

Splunk Enterprise Security Certified Admin

QUESTION 1

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.

Correct Answer: B

Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logsthe.html

QUESTION 2

What can be exported from ES using the Content Management page?

A. Only correlation searches, managed lookups, and glass tables.

B. Only correlation searches.

C. Any content type listed in the Content Management page.

D. Only correlation searches, glass tables, and workbench panels.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Export#:~:text=as%20an%20app-,Export%20content%20from%20Splunk%20Enterprise%20Security%20as,from%20the%20Conte nt%20Management%20page.andtext=You%20can%20export%20any%20type,%2C%20data%20models%2C%20and%20views.

QUESTION 3

"10.22.63.159", "websvr4", and "00:26:08:18: CF:1D" would be matched against what in ES?

A. A user.

B. A device.

C. An asset.

D. An identity.

Correct Answer: B

QUESTION 4

Where are attachments to investigations stored?

A. KV Store

B. notable index

C. attachments.csv lookup D. /etc/apps/SA-Investigations/default/ui/views/attachments

Correct Answer: A

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

QUESTION 5

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