Free Questions for SPLK-3001 by dumpssheet

Shared by Woodward on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is an adaptive action that is configured by default for ES?

Options:

A- Create notable event

B- Create new correlation search

C- Create investigation

D- Create new asset

Answer:

A

Question 2

Question Type: MultipleChoice

Which of the following is a Web Intelligence dashboard?

Options:

A- Network Center

B- Endpoint Center

C- HTTP Category Analysis

D- stream :http Protocol dashboard

Answer:

C

Question 3

Question Type: **MultipleChoice**

What is the default schedule for accelerating ES Datamodels?

Options:

A- 1 minute

B- 5 minutes

C- 15 minutes

D- 1 hour

Answer:

B

Question 4

Question Type: MultipleChoice

What is the first step when preparing to install ES?

Options:

A- Install ES.

B- Determine the data sources used.

C- Determine the hardware required.

D- Determine the size and scope of installation.

Answer:

D

Question 5

Question Type: MultipleChoice

An administrator wants to ensure that none of the ES indexed data could be compromised through tampering. What feature would satisfy this requirement?

Options:

A- Index consistency.

B- Data integrity control.

C- Indexer acknowledgement.

D- Index access permissions.

Answer:

B

Explanation:

the.html

Question 6

Question Type: MultipleChoice

Which component normalizes events?

Options:

A- SA-CIM.

B- SA-Notable.

C- ES application.

D- Technology add-on.

Answer:

A

Question 7

Question Type: **MultipleChoice**

Which of the following ES features would a security analyst use while investigating a network anomaly notable?

Options:

A- Correlation editor.

B- Key indicator search.

C- Threat download dashboard.

D- Protocol intelligence dashboard.

Answer:

D