Free Questions for SPLK-3001 by go4braindumps

Shared by Norris on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

A set of correlation searches are enabled at a new ES installation, and results are being monitored. One of the correlation searches is generating many notable events which, when evaluated, are determined to be false positives.

What is a solution for this issue?

Options:

A- Suppress notable events from that correlation search.

B- Disable acceleration for the correlation search to reduce storage requirements.

C- Modify the correlation schedule and sensitivity for your site.

D- Change the correlation search's default status and severity.

Answer:

A

Question 2

Question Type: MultipleChoice

Accelerated data requires approximately how many times the daily data volume of additional storage space per year?

Options:

A- 3.4

B- 5.7

C- 1.0

D- 2.5

Answer:

A

Question 3

Question Type: MultipleChoice

When installing Enterprise Security, what should be done after installing the add-ons necessary for normalizing data?

Options:

A- Configure the add-ons according to their README or documentation.

B- Disable the add-ons until they are ready to be used, then enable the add-ons.

C- Nothing, there are no additional steps for add-ons.

D- Configure the add-ons via the Content Management dashboard.

Answer:

A

Question 4

Question Type: MultipleChoice

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

Options:

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

Answer:

C

Question 5

Question Type: **MultipleChoice**

A security manager has been working with the executive team en long-range security goals. A primary goal for the team Is to Improve managing user risk in the organization. Which of the following ES features can help identify users accessing inappropriate web sites?

Options:

A- Configuring the identities lookup with user details to enrich notable event Information for forensic analysis.

B- Make sure the Authentication data model contains up-to-date events and is properly accelerated.

C- Configuring user and website watchlists so the User Activity dashboard will highlight unwanted user actions.

D- Use the Access Anomalies dashboard to identify unusual protocols being used to access corporate sites.

Answer:

C

Question 6

Question Type: **MultipleChoice**

Which of the following is part of tuning correlation searches for a new ES installation?

Options:

A- Configuring correlation notable event index.

B- Configuring correlation permissions.

C- Configuring correlation adaptive responses.

D- Configuring correlation result storage.

Answer:

A

Question 7

Question Type: **MultipleChoice**

What do threat gen searches produce?

Options:

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.

Answer:

D

Explanation:

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

Question 8

Question Type: **MultipleChoice**

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

Options:

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.

Answer:

C

Question 9

Question Type: MultipleChoice

What is an example of an ES asset?

Options:

A- MAC address

B- User name

C- Server

D- People

Answer:

A

20%
DISCOUNT