Free Questions for SPLK-3001 by certscare

Shared by Leach on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following actions can improve overall search performance?

Options:

A- Disable indexed real-time search.

B- Increase priority of all correlation searches.

C- Reduce the frequency (schedule) of lower-priority correlation searches.

D- Add notable event suppressions for correlation searches with high numbers of false positives.

Answer:

A

Question 2

Question Type: MultipleChoice

The Brute Force Access Behavior Detected correlation search is enabled, and is generating many false positives. Assuming the input data has already been validated. How can the correlation search be made less sensitive?

Options:

A- Edit the search and modify the notable event status field to make the notable events less urgent.

B- Edit the search, look for where or xswhere statements, and after the threshold value being compared to make it less common match.

C- Edit the search, look for where or xswhere statements, and alter the threshold value being compared to make it a more common match.

D- Modify the urgency table for this correlation search and add a new severity level to make notable events from this search less urgent.

Answer:

B

Question 3

Question Type: MultipleChoice

After installing Enterprise Security, the distributed configuration management tool can be used to create which app to configure indexers?

Options:

A- Splunk_DS_ForIndexers.spl

B- Splunk_ES_ForIndexers.spl

C- Splunk_SA_ForIndexers.spl

D- Splunk_TA_ForIndexers.spl

Answer:

D

Question 4

Question Type: **MultipleChoice**

Who can delete an investigation?

Options:

A- ess_admin users only.

B- The investigation owner only.

C- The investigation owner and ess-admin.

D- The investigation owner and collaborators.

Answer:

A

Question 5

Question Type: MultipleChoice

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?

Options:

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.

Answer:

D

Explanation:

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 6

Question Type: MultipleChoice

What tools does the Risk Analysis dashboard provide?

Options:

A- High risk threats.

B- Notable event domains displayed by risk score.

C- A display of the highest risk assets and identities.

D- Key indicators showing the highest probability correlation searches in the environment.

Answer:

C

Question 7

Question Type: MultipleChoice

An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?

Options:

A- OS: 32 bit, RAM: 16 MB, CPU: 12 cores

B- OS: 64 bit, RAM: 32 MB, CPU: 12 cores

C- OS: 64 bit, RAM: 12 MB, CPU: 16 cores

D- OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Answer:

C

Question 8

Question Type: MultipleChoice

How is it possible to navigate to the ES graphical Navigation Bar editor?

Options:

A- Configure -> Navigation Menu

B- Configure -> General -> Navigation

C- Settings -> User Interface -> Navigation -> Click on "Enterprise Security"

D- Settings -> User Interface -> Navigation Menus -> Click on "default" next to SplunkEnterpriseSecuritySuite

Answer:

B

Question 9

Question Type: MultipleChoice

Which data model populated the panels on the Risk Analysis dashboard?

Options:

A- Risk

B- Audit

C- Domain analysis

D- Threat intelligence

Answer:

A

Question 10

Question Type: MultipleChoice

Where are attachments to investigations stored?

Options:

A- KV Store

B- notable index

C- attachments.csv lookup

D- <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments

Answer:

A

Question 11

Question Type: MultipleChoice

Which settings indicated that the correlation search will be executed as new events are indexed?

Options:

A- Always-On

B- Real-Time

C- Scheduled

D- Continuous

Answer:

C