Free Questions for SPLK-2003 by go4braindumps

Shared by Lopez on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What values can be applied when creating Custom CEF field?

Options:

A- Name

B- Name, Data Type

C- Name, Value

D- Name, Data Type, Severity

Answer:

D

Question 2

Question Type: MultipleChoice

Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

Options:

A- Add a filter block to al restricted playbooks that Titters for runRole - 'Admin''.

B- Add a tag with restricted access to the restricted playbooks.

C- Make sure the Execute Playbook capability is removed from al roles except admin.

D- Place restricted playbooks in a second source repository that has restricted access.

Answer:

A

Question 3

Question Type: **MultipleChoice**

Which app allows a user to send Splunk Enterprise Security notable events to Phantom?

Options:

A- Any of the integrated Splunk/Phantom Apps

B- Splunk App for Phantom Reporting.

C- Splunk App for Phantom.

D- Phantom App for Splunk.

Answer:

A

Question 4

Question Type: MultipleChoice

What are indicators?

Options:

A- Action result items that determine the flow of execution in a playbook.

B- Action results that may appear in multiple containers.

C- Artifact values that can appear in multiple containers.

D- Artifact values with special security significance.

Answer:

C

Question 5

Question Type: MultipleChoice

On a multi-tenant Phantom server, what is the default tenant's ID?

Options:

A- 0

B- Default

C- 1

D- *

Answer:

D

Question 6

Question Type: MultipleChoice

When configuring a Splunk asset for Phantom to connect to a SplunkC loud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible

Options:

A- Enter the two queries in the asset as comma separated values.

B- Configure the second query in the Phantom app for Splunk.

C- Install a second Splunk app and configure the query in the second app.

D- Configure a second Splunk asset with the second query.

Answer:

A

Question 7

Question Type: MultipleChoice

After enabling multi-tenancy, which of the Mowing is the first configuration step?

Options:

A- Select the associated tenant artifacts.

B- Change the tenant permissions.

C- Set default tenant base address.

D- Configure the default tenant.

Answer:

B

Question 8

Question Type: MultipleChoice

What does a user need to do to have a container with an event from Splunk use context-aware actions designed for notable events?

Options:

A- Include the notable event's event_id field and set the artifacts label to aplunk notable event id.

B- Rename the event_id field from the notable event to splunkNotableEventId.

C- Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.

D- Add a custom field to the container named event_id and set the custom field's data type to splunk notable event id.

Answer:

D

Question 9

Question Type: MultipleChoice

During a second test of a playbook, a user receives an error that states: 'an empty parameters list was passed to phantom.act()." What does this indicate?

Options:

A- The container has artifacts not parameters.

B- The playbook is using an incorrect container.

C- The playbook debugger's scope is set to new.

D- The playbook debugger's scope is set to all.

Answer:

A

Question 10

Question Type: **MultipleChoice**

Phantom supports multiple user authentication methods such as LDAP and SAML2. What other user authentication method is supported?

Options:

A- SAML3

B- PIV/CAC

C- Biometrics

D- OpenID

Answer:

A

Question 11

Question Type: MultipleChoice

Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?

Options:

A- superuser, administrator

B- phantomcreate. phantomedit

C- phantomsearch, phantomdelete

D- admin,user

Answer:

A