Free Questions for SPLK-2003 by dumpshq

Shared by Spencer on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which Phantom API command is used to create a custom list?

Options:

A- phantom.add_list()

B- phantom.create_list()

C- phantom.include_list()

D- phantom.new_list()

Answer:

A

Question 2

Question Type: **MultipleChoice**

What are the differences between cases and events?

Options:

A- Case: potential threats.

Events: identified as a specific kind of problem and need a structured approach.

B- Cases: only include high-level incident artifacts.

Events: only include low-level incident artifacts.

C- Cases: contain a collection of containers.

Events: contain potential threats.

D- Cases: incidents with a known violation and a plan for correction.

Events: occurrences in the system that may require a response.

Answer:

A

Question 3

Question Type: MultipleChoice

Which of the following accurately describes the Files tab on the Investigate page?

Options:

A- A user can upload the output from a detonate action to the the files tab for further investigation.

B- Files tab items and artifacts are the only data sources that can populate active cases.

C- Files tab items cannot be added to investigations. Instead, add them to action blocks.

D- Phantom memory requirements remain static, regardless of Files tab usage.

Answer:

D

Question 4

Question Type: **MultipleChoice**

When is using decision blocks most useful?

Options:

A- When selecting one (or zero) possible paths in the playbook.

B- When processing different data in parallel.

C- When evaluating complex, multi-value results or artifacts.

D- When modifying downstream data hi one or more paths in the playbook.

Answer:

A

Question 5

Question Type: **MultipleChoice**

How is it possible to evaluate user prompt results?

Options:

A- Set action_result.summary. status to required.

B- Set the user prompt to reinvoke if it times out.

C- Set action_result. summary. response to required.

D- Add a decision Mode

Answer:

B

Question 6

Question Type: **MultipleChoice**

Which Phantom VPE Nock S used to add information to custom lists?

Options:

A- Action blocks

B- Filter blocks

C- API blocks

D- Decision blocks

Answer:

C

Question 7

Question Type: MultipleChoice

Which app allows a user to run Splunk queries from within Phantom?

Options:

A- Splunk App for Phantom?

B- The Integrated Splunk/Phantom app.

C- Phantom App for Splunk.

D- Splunk App for Phantom Reporting.

Answer:

A

Question 8

Question Type: MultipleChoice

A user wants to use their Splunk Cloud instance as the external Splunk instance for Phantom. What ports need to be opened on the Splunk Cloud instance to facilitate this? Assume default ports are in use.

Options:

A- TCP 8088 and TCP 8099.

B- TCP 80 and TCP 443.

C- Splunk Cloud is not supported.

D- TCP 8080 and TCP 8191.

Answer:

D

Question 9

Question Type: MultipleChoice

How does a user determine which app actions are available?

Options:

A- Add an action block to a playbook canvas area.

B- Search the Apps category in the global search field.

C- From the Apps menu, click the supported actions dropdown for each app.

D- In the visual playbook editor, click Active and click the Available App Actions dropdown.

Answer:

B

Question 10

Question Type: **MultipleChoice**

How can a child playbook access the parent playbook's action results?

Options:

A- Child playbooks can access parent playbook data while the parent Is still running.

B- By setting scope to ALL when starting the child.

C- When configuring the playbook block in the parent, add the desired results in the Scope parameter.

D- The parent can create an artifact with the data needed by the did.

Answer:

B