Splunk SOAR Certified Automation Developer Exam

Splunk SPLK-2003

Version Demo

Total Demo Questions: 10

Total Premium Questions: 58

QUESTION NO: 1

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

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 NO: 2

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

A. phantom.add_list()

B. phantom.create_list()

C. phantom.include_list()

D. phantom.new_list()

ANSWER: A

QUESTION NO: 3

Is it possible to import external Python libraries such as the time module?

A. No.

B. No, but this can be changed by setting the proper permissions.

C. Yes, in the global block.

D. Yes. from a drop down menu.

ANSWER: C

QUESTION NO: 4

What values can be applied when creating Custom CEF field?

A. Name

B. Name, Data Type

C. Name, Value

D. Name, Data Type, Severity

ANSWER: D

QUESTION NO: 5

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

A. superuser, administrator

B. phantomcreate. phantomedit

C. phantomsearch, phantomdelete

D. admin,user

ANSWER: A

QUESTION NO: 6

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

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

QUESTION NO: 7

Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

A. Notes

B. Actions

C. Service level agreement (SLA) expiration

D. Playbooks

ANSWER: B

QUESTION NO: 8

After a playbook has run, where are the results stored?

A. Splunk Index

B. Case

C. Container

D. Log file

ANSWER: D

QUESTION NO: 9

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

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 NO: 10

How can an individual asset action be manually started?

A. With the > action button in the analyst queue page.

B. By executing a playbook in the Playbooks section.

C. With the > action button in the Investigation page.

D. With the > asset button in the asset configuration section.

ANSWER: C