Splunk

Exam SPLK-2003

Splunk SOAR Certified Automation Developer Exam

Version: 3.0

[Total Questions: 58]

Question No : 1

A user wants to get the playbook results for a single artifact. Which steps will accomplish the?

A. Use the contextual menu from the artifact and select run playbook.
B. Use the run playbook dialog and set the scope to the artifact.
C. Create a new container including Just the artifact in question.
D. Use the contextual menu from the artifact and select the actions.

Answer: C

Question No : 2

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

A. Action blocks
B. Filter blocks
C. API blocks
D. Decision blocks

Answer: C

Question No : 3

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

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 No : 4

Which of the following are the steps required to complete a full backup of a Splunk

Phantom deployment' Assume the commands are executed from /opt/phantom/bin and that no other backups have been made.

A. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup.pyc --backup.
B. On the command line enter: sudo phenv python ibackup.pyc --backup —backup-type full, then sudo phenv python ibackup.pyc --setup.
C. Within the UI: Select from the main menu Administration > System Health > Backup.
D. Within the UI: Select from the main menu Administration > Product Settings > Backup.

Answer: B

Question No : 5

Which of the following is a step when configuring event forwarding from Splunk to Phantom?

A. Map CIM to CEF fields.
B. Create a Splunk alert that uses the event_forward.py script to send events to Phantom.
C. Map CEF to CIM fields.
D. Create a saved search that generates the JSON for the new container on Phantom.

Answer: C

Question No : 6

A customer wants to design a modular and reusable set of playbooks that all communicate with each other. Which of the following is a best practice for data sharing across playbooks?

A. Use the py-postgresq1 module to directly save the data in the Postgres database.
B. Cal the child playbooks getter function.
C. Create artifacts using one playbook and collect those artifacts in another playbook.
D. Use the Handle method to pass data directly between playbooks.

Answer: A

Question No : 7

When analyzing events a working on a case, significant items can be marked as evidence. Where can ail of a case's evidence items be viewed together?

A. Workbook page Evidence tab.
B. Evidence report.
C. Investigation page Evidence tab.
D. At the bottom of the Investigation page widget panel.

Answer: C

Question No : 8

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 : 9

When working with complex datapaths, which operator is used to access a sub-element inside another element?

A. !(pipe)
B. *(asterisk)
C. :(colon)
D. .(dot)

Answer: A

Question No : 10

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 : 11

What is the main purpose of using a customized workbook?

A. Workbooks automatically implement a customized processing of events using Python code.
B. Workbooks guide user activity and coordination during event analysis and case operations.
C. Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
D. Workbooks may not be customized; only default workbooks are permitted within Phantom.

Answer: D

Question No : 12

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

A. SAML3
B. PIV/CAC
C. Biometrics
D. OpenID

Answer: A

Question No : 13

Which is the primary system requirement that should be increased with heavy usage of the file vault?

A. Amount of memory.
B. Number of processors.
C. Amount of storage.

D. Bandwidth of network.

Answer: C

Question No : 14

How is it possible to evaluate user prompt results?

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 No : 15

Configuring Phantom search to use an external Splunk server provides which of the following benefits?

A. The ability to run more complex reports on Phantom activities.
B. The ability to ingest Splunk notable events into Phantom.
C. The ability to automate Splunk searches within Phantom.
D. The ability to display results as Splunk dashboards within Phantom.

Answer: C

Question No : 16

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 : 17

An active playbook can be configured to operate on all containers that share which attribute?

A. Artifact
B. Label
C. Tag
D. Severity

Answer: B

Question No : 18

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

A. Splunk Index
B. Case
C. Container
D. Log file

Answer: D

Question No : 19

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 : 20

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?

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 No : 21

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 : 22

After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

A. The new object ID.
B. The new object name.
C. The full CEF name.
D. The PostGres UUID.

Answer: D

Question No : 23

How does a user determine which app actions are available?

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.