Splunk.SPLK-2003.by.Tony.36q

Number: SPLK-2003
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: SPLK-2003

Exam Name: Splunk SOAR Certified Automation Developer

Exam A

QUESTION 1
Which of the following applies to filter blocks?

A. Can select which blocks have access to container data.
B. Can select assets by tenant, approver, or app.
C. Can be used to select data for use by other blocks.
D. Can select containers by seventy or status.

Correct Answer: A
Section:

QUESTION 2
A user has written a playbook that calls three other playbooks, one after the other. The user notices that the second playbook starts executing before the first one completes. What is the cause of this behavior?

A. Incorrect Join configuration on the second playbook.
B. The first playbook is performing poorly.
C. The steep option for the second playbook is not set to a long enough interval.
D. Synchronous execution has not been configured.

Correct Answer: A
Section:

QUESTION 3
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.

Correct Answer: A
Section:

QUESTION 4
Which of the following are examples of things commonly done with the Phantom REST APP

A. Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists.
B. Use Django queries; use Docker to create a container and add artifacts to it; remove temporary lists.
C. Use Django queries; use curl to create a container and add artifacts to it; add action blocks.
D. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.

Correct Answer: C

Section:

QUESTION 5

Which of the following are the default ports that must be configured on Splunk to allow connections from Phantom?

A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)

B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)

C. SplunkWeb (8421), SplunkD (8061), HTTP Collector (8798)

D. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)

Correct Answer: D
Section:

QUESTION 6

Without customizing container status within Phantom, what are the three types of status for a container?

A. New, In Progress, Closed

B. Low, Medium, High

C. Mew, Open, Resolved

D. Low, Medium, Critical

Correct Answer: A
Section:

QUESTION 7

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

Correct Answer: A
Section:

QUESTION 8

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

Correct Answer: A
Section:

QUESTION 9

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.

Correct Answer: A
Section:

QUESTION 10
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.

Correct Answer: D
Section:

QUESTION 11
After enabling multi-tenancy, which of the Mowing is the first configuration step?

A. Select the associated tenant artifacts.
B. Change the tenant permissions.
C. Set default tenant base address.
D. Configure the default tenant.

Correct Answer: B
Section:

QUESTION 12
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.

Correct Answer: A
Section:

QUESTION 13
On a multi-tenant Phantom server, what is the default tenant's ID?

A. 0

B. Default

C. 1

D. *

Correct Answer: D
Section:

QUESTION 14
What are indicators?

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.

Correct Answer: C
Section:

QUESTION 15
Which app allows a user to send Splunk Enterprise Security notable events to Phantom?

A. Any of the integrated Splunk/Phantom Apps

B. Splunk App for Phantom Reporting.

C. Splunk App for Phantom.

D. Phantom App for Splunk.

Correct Answer: A
Section:

QUESTION 16
Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

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.

Correct Answer: A
Section:

QUESTION 17
What values can be applied when creating Custom CEF field?

A. Name

B. Name, Data Type

C. Name, Value

D. Name, Data Type, Severity

Correct Answer: D
Section:

QUESTION 18
What is enabled if the Logging option for a playbook's settings is enabled?

A. More detailed logging information Is available m the Investigation page.
B. All modifications to the playbook will be written to the audit log.
C. More detailed information is available in the debug window.
D. The playbook will write detailed execution information into the spawn.log.

Correct Answer: D
Section:

QUESTION 19
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.

Correct Answer: C
Section:

QUESTION 20
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.

Correct Answer: C
Section:

QUESTION 21
What is the default embedded search engine used by Phantom?

A. Embedded Splunk search engine.
B. Embedded Phantom search engine.
C. Embedded Elastic search engine.
D. Embedded Django search engine.

Correct Answer: C
Section:

QUESTION 22
A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit which of the following data to pass forward to the next block?

A. Null IP addresses
B. Non-null IP addresses
C. Non-null destinationAddresses
D. Null values

Correct Answer: D
Section:

QUESTION 23
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.

Correct Answer: C
Section:

QUESTION 24
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.

Correct Answer: D
Section:

QUESTION 25
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.

Correct Answer: C
Section:

QUESTION 26
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.

Correct Answer: C
Section:

QUESTION 27
Which of the following will show all artifacts that have the term results in a filePath CEF value?

A. .../rest/artifact?_filter_cef_filePath_icontain="results"
B. ...rest/artifacts/filePath="%results%"
C. .../result/artifacts/cef/filePath= '%results%"
D. .../result/artifact?_query_cef_filepath_icontains="results

Correct Answer: D
Section:

QUESTION 28
Which of the following can be configured in the ROl Settings?

A. Analyst hours per month.
B. Time lost.
C. Number of full time employees (FTEs).
D. Annual analyst salary.

Correct Answer: D
Section:

QUESTION 29
Which of the following expressions will output debug information to the debug window in the Visual Playbook Editor?

A. phantom.debug()
B. phantom.exception()
C. phantom.print ()
D. phantom.assert()

Correct Answer: D
Section:

QUESTION 30
Which of the following supported approaches enables Phantom to run on a Windows server?

A. Install the Phantom RPM in a GNU Cygwin implementation.
B. Run the Phantom OVA as a cloud instance.
C. Install the Phantom RPM file in Windows Subsystem for Linux (WSL).

D. Run the Phantom OVA as a virtual machine.

Correct Answer: B
Section:

QUESTION 31
Which of the following can the format block be used for?

A. To generate arrays for input into other functions.
B. To generate HTML or CSS content for output in email messages, user prompts, or comments.
C. To generate string parameters for automated action blocks.
D. To create text strings that merge state text with dynamic values for input or output.

Correct Answer: D
Section:

QUESTION 32
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.

Correct Answer: C
Section:

QUESTION 33
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)

Correct Answer: A
Section:

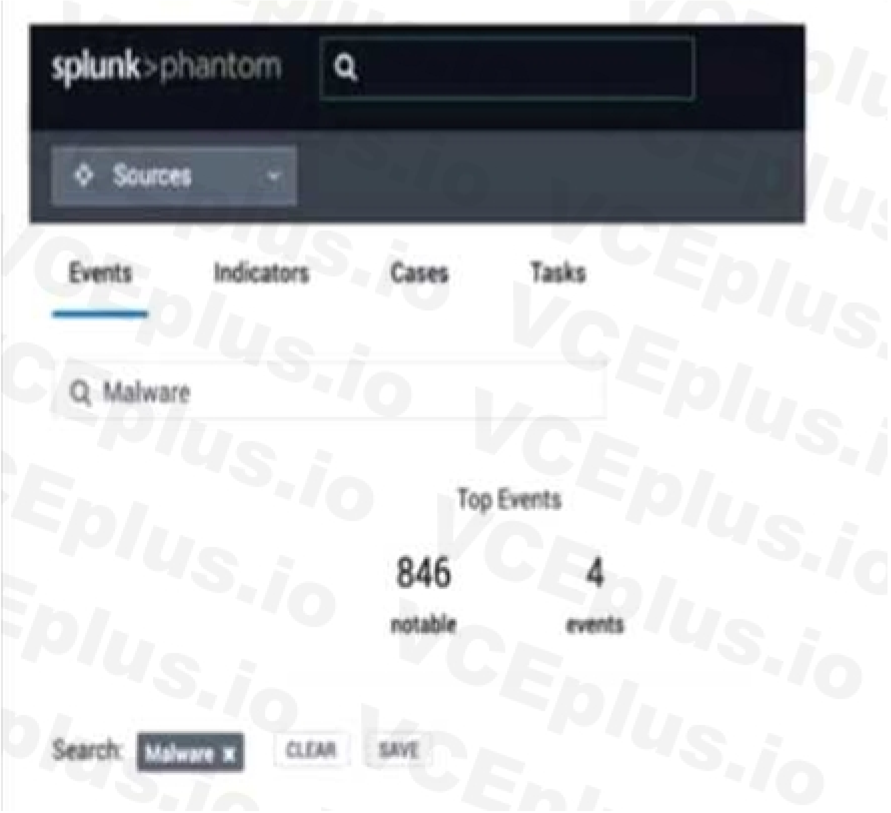
QUESTION 34
Which of the following is a best practice for use of the global block?

A. Execute code at the beginning of each run of the playbook.
B. Declare outputs which will be selectable within playbook blocks.
C. Import packages which will be used within the playbook.
D. Execute custom code after each run of the playbook.

Correct Answer: A

Section:

QUESTION 35
In this image, which container fields are searched for the text "Malware"?



A. Event Name and Artifact Names.
B. Event Name, Notes, Comments.
C. Event Name or ID.

Correct Answer: A
Section:

QUESTION 36
Which of the following is the complete list of the types of backups that are supported by Phantom?

A. Full backups.
B. Full, delta, and incremental backups.
C. Full and incremental backups.
D. Full and delta backups.

Correct Answer: C
Section: