Splunk.SPLK-2003.v2024-03-05.q40

Exam Code:	SPLK-2003
Exam Name:	Splunk Phantom Certified Admin
Certification Provider:	Splunk
Free Question Number:	40
Version:	v2024-03-05
# of views:	1792
# of Questions views:	400
https://www.freepdfdumps.com/Splunk.SPLK-2003.v2024-03-05.q40.html	

NEW QUESTION: 1
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.
Answer: A (LEAVE A REPLY)
Explanation
The correct answer is A because using Django queries, using curl to create a container and add artifacts to it, and removing temporary lists are examples of things commonly done with the Phantom REST APP. The Phantom REST APP is a built-in app that allows you to interact with the Phantom server using REST API calls. You can use the run query action to execute Django queries on the Phantom database and return the results as JSON. You can use the curl command to send HTTP requests to the Phantom server and perform various operations, such as creating containers, adding artifacts, running playbooks, etc. You can use the remove list action to delete temporary lists that are no longer needed. See Splunk SOAR Documentation for more details.

NEW QUESTION: 2
When working with complex datapaths, which operator is used to access a sub-element inside another element?
A. .(dot)

B. :(colon)
C. !(pipe)
D. *(asterisk)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
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.
Answer: A (LEAVE A REPLY)
Explanation
A user can determine which app actions are available by adding an action block to a playbook canvas area.
The action block will show a list of all the apps installed on the Phantom system and the actions supported by each app. The other options do not provide a comprehensive view of the app actions available. Reference, page 11.

NEW QUESTION: 4
How is it possible to evaluate user prompt results?
A. Set action_result. summary. response to required.
B. Set action_result.summary. status to required.
C. Add a decision Mode
D. Set the user prompt to reinvoke if it times out.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 5
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: B (LEAVE A REPLY)
Explanation
The main purpose of using a customized workbook is to guide user activity and coordination during event analysis and case operations. Workbooks can be customized to

include different phases, tasks, and instructions for the users. The other options are not valid purposes of using a customized workbook. See Workbooks for more information.

NEW QUESTION: 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: (SHOW ANSWER)
Explanation
A child playbook can access the parent playbook's action results by using the scope parameter when configuring the playbook block in the parent. The scope parameter allows the user to specify which action results from the parent playbook should be passed to the child playbook as input parameters. Child playbooks cannot access parent playbook data while the parent is still running, and setting the scope to ALL when starting the child does not affect the data access. The parent can create an artifact with the data needed by the child, but this is not the only mechanism to do so. Reference, page 17.

NEW QUESTION: 7
How can an individual asset action be manually started?
A. With the > action button in the Investigation page.
B. With the > asset button in the asset configuration section.
C. By executing a playbook in the Playbooks section.
D. With the > action button in the analyst queue page.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
After a playbook has run, where are the results stored?
A. Splunk Index
B. Case
C. Container
D. Log file
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the

phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a data object in Phantom, but can be a data source for Phantom. Reference: Splunk SOAR User Guide, page 19.

NEW QUESTION: 9
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: D (LEAVE A REPLY)
Explanation
The correct answer is D because to run two different on_poll searches, you need to configure a second Splunk asset with the second query. The on_poll search is the query that Phantom uses to fetch events from Splunk and create containers and artifacts. You can only specify one on_poll search per Splunk asset. If you want to run another on_poll search, you need to create another Splunk asset with a different name and IP address and configure the second query in the asset settings. See Splunk SOAR Documentation for more details.

NEW QUESTION: 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. from a drop down menu.
D. Yes, in the global block.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
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: (SHOW ANSWER)
Explanation
A user can get the playbook results for a single artifact by using the run playbook dialog and setting the scope to the artifact. This will execute the playbook on the selected artifact only and show the results in the Investigation page. The other options are not valid ways to get the playbook results for a single artifact.
See Running playbooks for more information.

NEW QUESTION: 12
Which is the primary system requirement that should be increased with heavy usage of the file vault?
A. Number of processors.
B. Amount of storage.
C. Amount of memory.
D. Bandwidth of network.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
What values can be applied when creating Custom CEF field?
A. Name
B. Name, Data Type
C. Name, Data Type, Severity
D. Name, Value
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
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: C (LEAVE A REPLY)
Explanation
The correct answer is C because the error message indicates that the playbook debugger's scope is set to new.

The scope option determines which containers are used for debugging the playbook. If the scope is set to new, the debugger will only use containers that are created after the debugger is started. If the scope is set to all, the debugger will use all containers that match the playbook's filter criteria. The error message means that the debugger did not find any new containers with parameters to pass to the phantom.act() function. See Splunk SOAR Documentation for more details.

NEW QUESTION: 15
Which Phantom VPE Nock S used to add information to custom lists?
A. Action blocks
B. Decision blocks
C. Filter blocks
D. API blocks
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
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.
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because filter blocks can be used to select data for use by other blocks. Filter blocks can filter data from the container, artifacts, or custom lists based on various criteria, such as field name, value, operator, etc. Filter blocks can also join data from multiple sources using the join action. The output of the filter block can be used as input for other blocks, such as decision, format, prompt, etc. See Splunk SOAR Documentation for more details.

NEW QUESTION: 17
Which app allows a user to run Splunk queries from within Phantom?

A. Phantom App for Splunk.
B. Splunk App for Phantom?
C. Splunk App for Phantom Reporting.
D. The Integrated Splunk/Phantom app.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
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: B (LEAVE A REPLY)
Explanation
The Phantom API command to create a custom list is phantom.create_list(). This command takes a list name and an optional description as parameters and returns a list ID if successful. The other commands are not valid Phantom API commands. phantom.add_list() is a Python function that can be used in custom code blocks to add data to an existing list. Reference, page 5.

NEW QUESTION: 19
When working with complex data paths, which operator is used to access a sub-element inside another element?
A. !(pipe)
B. *(asterisk)
C. :(colon)
D. .(dot)
Answer: D (LEAVE A REPLY)
Explanation
The correct answer is D because the dot (.) operator is used to access a sub-element inside another element when working with complex datapaths. For example, if the datapath is container['artifacts'][0]['cef']['sourceAddress'], the dot operator is used to access the sourceAddress sub-element inside the cef element. The answer A is incorrect because the pipe (!) operator is used to chain multiple filters or functions when working with complex datapaths. For example, if the datapath is container['artifacts'][0]['cef']['sourceAddress']! startswith('10.'), the pipe operator is used to apply the startswith function to the sourceAddress element. The answer B is incorrect because the asterisk (*) operator is used to iterate over all the elements of an array when working with complex datapaths. For example, if the datapath is container['artifacts'][*]['cef']['sourceAddress'], the asterisk operator is used to access the sourceAddress element of all the artifacts in the container. The answer C is incorrect because the colon (:) operator is used to specify a range of

elements in an array when working with complex datapaths. For example, if the datapath is container['artifacts'][0:5]['cef']['sourceAddress'], the colon operator is used to access the sourceAddress element of the first five artifacts in the container. Reference: Splunk SOAR Playbook Development Guide, page 28.

NEW QUESTION: 20
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
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because without customizing container status within Phantom, the three types of status for a container are New, Open, and Resolved. A container is a data object that represents an event or incident that needs to be investigated or remediated. A container has a status attribute that indicates its current state. The default values for the status attribute are New, Open, and Resolved. New means that the container has been created but not yet processed. Open means that the container is being processed by a playbook or a user. Resolved means that the container has been processed and closed. You can customize the container status values in the Phantom UI by going to Administration > Product Settings > Container Status. See Splunk SOAR Documentation for more details.

NEW QUESTION: 21
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. .../result/artifact?_query_cef_filepath_icontains="results
C. ...rest/artifacts/filePath="%results%"
D. .../result/artifacts/cef/filePath= '%results%"
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
How does a user determine which app actions are available?
A. Add an action block to a playbook canvas area.
B. From the Apps menu, click the supported actions dropdown for each app.
C. In the visual playbook editor, click Active and click the Available App Actions dropdown.
D. Search the Apps category in the global search field.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
Which of the following is a step when configuring event forwarding from Splunk to Phantom?
A. Map CIM to CEF fields.
B. Map CEF to CIM fields.
C. Create a Splunk alert that uses the event_forward.py script to send events to Phantom.
D. Create a saved search that generates the JSON for the new container on Phantom.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
After enabling multi-tenancy, which of the Mowing is the first configuration step?
A. Change the tenant permissions.
B. Set default tenant base address.
C. Configure the default tenant.
D. Select the associated tenant artifacts.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 25
In addition to full backups. Phantom supports what other backup type using backup?
A. Snapshot
B. Incremental
C. Partial
D. Differential
Answer: A (LEAVE A REPLY)
Explanation
Phantom supports two types of backups: full and snapshot. A full backup creates a complete copy of the Phantom system, including all data, configuration, and apps. A snapshot backup creates a copy of the Phantom system configuration and apps, but not the data. Incremental and differential backups are not supported by Phantom. Reference, page 4.

NEW QUESTION: 26
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. The first playbook is performing poorly.
B. Synchronous execution has not been configured.
C. Incorrect Join configuration on the second playbook.
D. The steep option for the second playbook is not set to a long enough interval.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 27
What is enabled if the Logging option for a playbook's settings is enabled?
A. The playbook will write detailed execution information into the spawn.log.
B. More detailed information is available in the debug window.
C. More detailed logging information Is available m the Investigation page.
D. All modifications to the playbook will be written to the audit log.
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Without customizing container status within Phantom, what are the three types of status for a container?
A. Low, Medium, High
B. New, In Progress, Closed
C. Low, Medium, Critical
D. Mew, Open, Resolved
Answer: (SHOW ANSWER)

NEW QUESTION: 29
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.

Answer: A (LEAVE A REPLY)

Explanation

The correct answer is A because the image shows the search interface of the Splunk SOAR product, where the user can search for events and artifacts based on various criteria. The image shows that the user has entered the text "Malware" in the search bar, which means that the search will look for events and artifacts that have the term "Malware" in their name. The answer B is incorrect because the search interface does not search for notes or comments, which are separate entities in the Splunk SOAR product. The answer C is incorrect because the search interface does not search for event ID, which is a unique identifier for each event. Reference: Splunk SOAR User Guide, page 21.

NEW QUESTION: 30

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 debugger's scope is set to all.

C. The playbook is using an incorrect container.

D. The playbook debugger's scope is set to new.

Answer: (SHOW ANSWER)

NEW QUESTION: 31

What are the differences between cases and events?

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

Events: only include low-level incident artifacts.

B. Cases: contain a collection of containers.

Events: contain potential threats.

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

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

D. Case: potential threats.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 32
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
Answer: B (LEAVE A REPLY)
Explanation
A filter block with only one condition configured which states:
artifact.*.cef .sourceAddress !- , would permit only non-null IP addresses to pass forward to the next block. The !- operator means "is not null". The other options are not valid because they either include null values or other fields than sourceAddress. See Filter block for more details.

NEW QUESTION: 33
How can the debug log for a playbook execution be viewed?
A. Open the playbook in the Visual Playbook Editor, and select Debug Logs in Settings.
B. On the Investigation page, select Debug Log from the playbook's action menu in the Recent Activity panel.
C. In Administration > System Health > Playbook Run History, select the playbook execution entry, then select Log.
D. Click Expand Scope m the debug window.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 34
How can the debug log for a playbook execution be viewed?
A. On the Investigation page, select Debug Log from the playbook's action menu in the Recent Activity panel.
B. Click Expand Scope m the debug window.
C. In Administration > System Health > Playbook Run History, select the playbook execution entry, then select Log.
D. Open the playbook in the Visual Playbook Editor, and select Debug Logs in Settings.
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because the Administration > System Health > Playbook Run History page allows viewing the debug log for any playbook execution by selecting the playbook execution entry and then selecting Log. The debug log contains information such as the start and end time, the status, the input parameters, the output results, and any errors or exceptions for each block in the playbook. The answer A is incorrect because the

Investigation page does not have a Debug Log option in the playbook's action menu in the Recent Activity panel. The answer B is incorrect because the Expand Scope option in the debug window does not show the debug log for a playbook execution, but the details of the current container and its artifacts.
The answer D is incorrect because the Visual Playbook Editor does not have a Debug Logs option in Settings, but a Debug Mode option that allows testing the playbook with sample data. Reference: Splunk SOAR User Guide, page 100.

NEW QUESTION: 35
Which of the following can be configured in the ROI Settings?
A. Analyst hours per month.
B. Time lost.
C. Number of full time employees (FTEs).
D. Annual analyst salary.
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because the number of full time employees (FTEs) is one of the settings that can be configured in the Return on Investment (ROI) Settings page. This setting is used to calculate the ROI metrics based on the number of analysts in the organization. The answer A is incorrect because the analyst hours per month is not a configurable setting, but a calculated metric based on the FTEs and the average hours per month. The answer B is incorrect because the time lost is not a configurable setting, but a calculated metric based on the number of incidents and the average time lost per incident. The answer D is incorrect because the annual analyst salary is not a configurable setting, but a calculated metric based on the FTEs and the average salary per analyst. Reference: Splunk SOAR Admin Guide, page 131.

NEW QUESTION: 36
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.
Answer: (SHOW ANSWER)
Explanation
The Logging option for a playbook's settings enables more detailed logging information to be available in the Investigation page. This can help with debugging and troubleshooting the playbook execution. The other options are not related to the Logging option. See Playbook settings for more information.

NEW QUESTION: 37

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. Rename the event_id field from the notable event to splunkNotableEventId.
B. Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.
C. Add a custom field to the container named event_id and set the custom field's data type to splunk notable event id.
D. Include the notable event's event_id field and set the artifacts label to aplunk notable event id.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
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 playbook debugger's scope is set to all.
B. The playbook is using an incorrect container.
C. The container has artifacts not parameters.
D. The playbook debugger's scope is set to new.
Answer: (SHOW ANSWER)
Explanation
The correct answer is C because the error message indicates that the playbook debugger's scope is set to new.
The scope option determines which containers are used for debugging the playbook. If the scope is set to new, the debugger will only use containers that are created after the debugger is started. If the scope is set to all, the debugger will use all containers that match the playbook's filter criteria. The error message means that the debugger did not find any new containers with parameters to pass to the phantom.act() function. See Splunk SOAR Documentation for more details.

NEW QUESTION: 39
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. Within the UI: Select from the main menu Administration > System Health > Backup.
C. Within the UI: Select from the main menu Administration > Product Settings > Backup.
D. On the command line enter: sudo phenv python ibackup.pyc --backup -backup-type full, then sudo phenv python ibackup.pyc --setup.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
How can a child playbook access the parent playbook's action results?
A. When configuring the playbook block in the parent, add the desired results in the Scope parameter.
B. By setting scope to ALL when starting the child.
C. Child playbooks can access parent playbook data while the parent Is still running.
D. The parent can create an artifact with the data needed by the did.
Answer: B (LEAVE A REPLY)