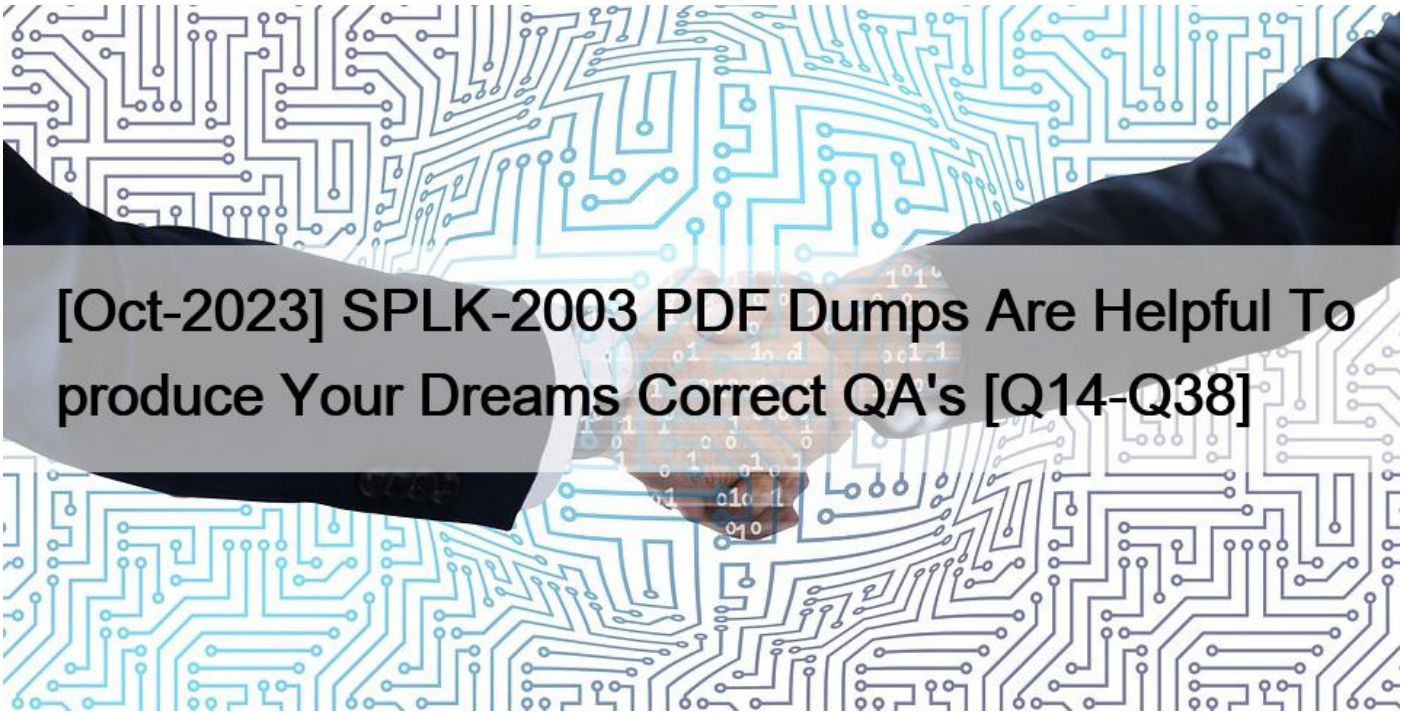
[Oct-2023 SPLK-2003 PDF Dumps Are Helpful To produce Your Dreams Correct QA's [Q14-Q38



[Oct-2023 SPLK-2003 PDF Dumps Are Helpful To produce Your Dreams Correct QA's New SPLK-2003 exam Free Sample Questions to Practice Q14. When is using decision blocks most useful?

* When selecting one (or zero) possible paths in the playbook.
* When processing different data in parallel.
* When evaluating complex, multi-value results or artifacts.
* When modifying downstream data hi one or more paths in the playbook.

Explanation

Decision blocks are most useful when selecting one (or zero) possible paths in the playbook. Decision blocks allow the user to define one or more conditions based on action results, artifacts, or custom expressions, and execute the corresponding path if the condition is met. If none of the conditions are met, the playbook execution ends. Decision blocks are not used for processing different data in parallel, evaluating complex, multi-value results or artifacts, or modifying downstream data in one or more paths in the playbook. Reference, page 15.

Q15. 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

* Enter the two queries in the asset as comma separated values.
* Configure the second query in the Phantom app for Splunk.
* Install a second Splunk app and configure the query in the second app.
* Configure a second Splunk asset with the second query.

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.

Q16. In this image, which container fields are searched for the text “Malware”?

ertify.vceprep.com

* Event Name and Artifact Names.
* Event Name, Notes, Comments.
* Event Name or ID.

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.

Q17. What is the simplest way to pass data between playbooks?

* Action results
* File system
* Artifacts
* KV Store

Q18. How can the debug log for a playbook execution be viewed?

* On the Investigation page, select Debug Log from the playbook’s action menu in the Recent Activity panel.
* Click Expand Scope m the debug window.
* In Administration > System Health > Playbook Run History, select the playbook execution entry, then select Log.
* Open the playbook in the Visual Playbook Editor, and select Debug Logs in Settings.

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.

Q19. 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.
* TCP 8088 and TCP 8099.
* TCP 80 and TCP 443.
* Splunk Cloud is not supported.
* TCP 8080 and TCP 8191.

Explanation

A user who wants to use their Splunk Cloud instance as the external Splunk instance for Phantom needs to open TCP 8088 and TCP 8099 ports on the Splunk Cloud instance. TCP 8088 is used for the HTTP Event Collector (HEC) service, which allows Phantom to send data to Splunk Cloud. TCP 8099 is used for the Splunk REST API service, which allows Phantom to query data from Splunk Cloud. The other port combinations are not valid for this scenario. Splunk Cloud is supported as an external Splunk instance for Phantom. Reference, page 6.

Q20. 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?
* Use the py-postgresq1 module to directly save the data in the Postgres database.
* Cal the child playbooks getter function.
* Create artifacts using one playbook and collect those artifacts in another playbook.
* Use the Handle method to pass data directly between playbooks.

Explanation

The correct answer is C because creating artifacts using one playbook and collecting those artifacts in another playbook is a best practice for data sharing across playbooks. Artifacts are data objects that are associated with a container and can be used to store information such as IP addresses, URLs, file hashes, etc. Artifacts can be created using the add artifact action in any playbook block and can be collected using the get artifacts action in the filter block. Artifacts can also be used to trigger active playbooks based on their label or type. See Splunk SOAR Documentation for more details.

Q21. What is the main purpose of using a customized workbook?
* Workbooks automatically implement a customized processing of events using Python code.
* Workbooks guide user activity and coordination during event analysis and case operations.
* Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
* Workbooks may not be customized; only default workbooks are permitted within Phantom.

Q22. Without customizing container status within Phantom, what are the three types of status for a container?
* New, In Progress, Closed
* Low, Medium, High
* Mew, Open, Resolved
* Low, Medium, Critical

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.

Q23. After enabling multi-tenancy, which of the Mowing is the first configuration step?
* Select the associated tenant artifacts.
* Change the tenant permissions.
* Set default tenant base address.
* Configure the default tenant.

Q24. Within the 12A2 design methodology, which of the following most accurately describes the last step?
* List of the apps used by the playbook.
* List of the actions of the playbook design.
* List of the outputs of the playbook design.
* List of the data needed to run the playbook.

Q25. Within the 12A2 design methodology, which of the following most accurately describes the last step?
* List of the apps used by the playbook.
* List of the actions of the playbook design.
* List of the outputs of the playbook design.
* List of the data needed to run the playbook.

Explanation

The correct answer is C because the last step of the 12A2 design methodology is to list the outputs of the playbook design. The outputs are the expected results or outcomes of the playbook execution, such as sending an email, creating a ticket, blocking an IP, etc. The outputs should be aligned with the objectives and goals of the playbook. See Splunk SOAR Certified Automation Developer for more details.

Q26. How does a user determine which app actions are available?
* Add an action block to a playbook canvas area.
* Search the Apps category in the global search field.
* From the Apps menu, click the supported actions dropdown for each app.
* In the visual playbook editor, click Active and click the Available App Actions dropdown.

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.

Q27. Which of the following will show all artifacts that have the term results in a filePath CEF value?
* …/rest/artifact?_filter_cef_filePath_icontain=”results”
* …rest/artifacts/filePath=”%results%”
* …/result/artifacts/cef/filePath= ‘%results%”

* …/result/artifact?_query_cef_filepath_icontains=”results

Explanation

The correct answer is A because the _filter parameter is used to filter the results based on a field value, and the icontain operator is used to perform a case-insensitive substring match. The filePath field is part of the Common Event Format (CEF) standard, and the cef_ prefix is used to access CEF fields in the REST API. The answer B is incorrect because it uses the wrong syntax for the REST API. The answer C is incorrect because it uses the wrong endpoint (result instead of artifact) and the wrong syntax for the REST API. The answer D is incorrect because it uses the wrong syntax for the REST API and the wrong spelling for the icontains operator.

Reference: Splunk SOAR REST API Guide, page 18.

Q28. Which app allows a user to run Splunk queries from within Phantom?

* Splunk App for Phantom?
* The Integrated Splunk/Phantom app.
* Phantom App for Splunk.
* Splunk App for Phantom Reporting.

Explanation

The Phantom App for Splunk allows a user to run Splunk queries from within Phantom. This app provides actions such as run query, ingest events, and save search, which enable the user to interact with Splunk from Phantom playbooks or the Phantom UI. The other apps are not relevant for this use case. The Splunk App for Phantom is used to send data from Splunk to Phantom. The Integrated Splunk/Phantom app is a deprecated app that was replaced by the Splunk App for Phantom. The Splunk App for Phantom Reporting is used to generate reports on Phantom activity from Splunk. Reference, page 1.

Q29. 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.

* On the command line enter: rode sudo python ibackup.pyc –setup, then audo phenv python ibackup.pyc

–backup.

* On the command line enter: sudo phenv python ibackup.pyc –backup -backup-type full, then sudo phenv python ibackup.pyc –setup.
* Within the UI: Select from the main menu Administration > System Health > Backup.
* Within the UI: Select from the main menu Administration > Product Settings > Backup.

Explanation

The correct answer is B because the steps required to complete a full backup of a Splunk Phantom deployment are to first run the –backup –backup-type full command and then run the –setup command.

The –backup command creates a backup file in the /opt/phantom/backup directory. The –backup-type full option specifies that the backup file includes all the data and configuration files of the Phantom server.

The –setup command creates a configuration file that contains the encryption key and other information needed to restore the backup file. See Splunk SOAR Certified Automation Developer Track for more details.

Q30. 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?

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

Explanation

The correct answer is D because synchronous execution has not been configured. Synchronous execution is a feature that allows you to control the order of execution of playbook blocks. By default, Phantom executes playbook blocks asynchronously, meaning that it does not wait for one block to finish before starting the next one. This can cause problems when you have dependencies between blocks or when you call other playbooks.

To enable synchronous execution, you need to use the sync action in the run playbook block and specify the name of the next block to run after the called playbook completes. See Splunk SOAR Documentation for more details.

Q31. A user wants to get the playbook results for a single artifact. Which steps will accomplish the?
* Use the contextual menu from the artifact and select run playbook.
* Use the run playbook dialog and set the scope to the artifact.
* Create a new container including Just the artifact in question.
* Use the contextual menu from the artifact and select the actions.

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.

Q32. Which of the following is the complete list of the types of backups that are supported by Phantom?
* Full backups.
* Full, delta, and incremental backups.
* Full and incremental backups.
* Full and delta backups.

Explanation

The correct answer is D because the Splunk SOAR product supports two types of backups: full and delta. A full backup is a complete backup of the entire Splunk SOAR system, including the configuration, data, and files. A delta backup is a partial backup of the Splunk SOAR system, which only includes the changes that have occurred since the last full backup. The answer A is incorrect because the Splunk SOAR product supports more than one type of backup. The answer B is incorrect because the Splunk SOAR product does not support incremental backups, which are backups of the changes that have occurred since the last backup of any type. The answer C is incorrect because the Splunk SOAR product does not support incremental backups, which are backups of the changes that have occurred since the last backup of any type. Reference: Splunk SOAR Admin Guide, page 67.

Q33. How can a child playbook access the parent playbook’s action results?
* Child playbooks can access parent playbook data while the parent Is still running.
* By setting scope to ALL when starting the child.
* When configuring the playbook block in the parent, add the desired results in the Scope parameter.
* The parent can create an artifact with the data needed by the did.

Q34. How can a child playbook access the parent playbook’s action results?
* Child playbooks can access parent playbook data while the parent Is still running.
* By setting scope to ALL when starting the child.
* When configuring the playbook block in the parent, add the desired results in the Scope parameter.
* The parent can create an artifact with the data needed by the did.

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.

Q35. Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?
* superuser, administrator
* phantomcreate. phantomedit
* phantomsearch, phantomdelete
* admin,user

Q36. Which of the following can be configured in the ROl Settings?
* Analyst hours per month.
* Time lost.
* Number of full time employees (FTEs).
* Annual analyst salary.

Q37. 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?
* Workbook page Evidence tab.
* Evidence report.
* Investigation page Evidence tab.
* At the bottom of the Investigation page widget panel.

Q38. Which Phantom API command is used to create a custom list?
* phantom.add_list()
* phantom.create_list()
* phantom.include_list()
* phantom.new_list()

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.

Cover SPLK-2003 Exam Questions Make Sure You 100% Pass: https://www.vceprep.com/SPLK-2003-latest-vce-prep.html]