SPLK-2003 Q&As

Splunk SOAR Certified Automation Developer

Pass Splunk SPLK-2003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/splk-2003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is a reason to create a new role in SOAR?

A. To define a set of users who have access to a special label.

B. To define a set of users who have access to a restricted app.

C. To define a set of users who have access to an event\\'s reports.

D. To define a set of users who have access to a sensitive tag.

Correct Answer: A

Creating a new role in Splunk SOAR is often done to define a set of users who have specific access rights, such as access to a special label. Labels in SOAR can be used to categorize data and control access. By assigning a role with access to a particular label, administrators can ensure that only a specific group of users can view or interact with containers, events, or artifacts that have been tagged with that label, thus maintaining control over sensitive data or operations.

QUESTION 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()

Correct Answer: B

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. To create a custom list in Splunk Phantom, the appropriate API command used is phantom.create_list(). This function allows for the creation of a new list that can be used to store data such as IP addresses, file hashes, or any other information that you want to track or reference across multiple playbooks or within different parts of the Phantom platform. The custom list is a flexible data structure that can be leveraged for various use cases within Phantom, including data enrichment, persistent storage of information, and cross-playbook data sharing.

QUESTION 3

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.

Correct Answer: A

Debug logs are essential for troubleshooting and understanding the execution flow of a playbook in Splunk Phantom. The debug log for a playbook execution can be viewed by navigating to the Investigation page of a specific event or container. Within the Recent Activity panel, there is an action menu associated with each playbook run. Selecting "Debug Log" from this menu will display the detailed execution log, showing each action taken, the results of those actions, and any errors or messages generated during the playbook run.

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

The Phantom REST API, often interacted with through the Phantom REST APP, is a powerful tool for automating and integrating Splunk SOAR with other systems. Common uses of the Phantom REST APP include using Django queries to interact with the SOAR database, using curl commands to programmatically create containers and add artifacts to them, and configuring action blocks within playbooks for automated actions. This flexibility allows for a wide range of automation and integration possibilities, enhancing the SOAR platform\\'s capability to respond to security incidents and manage data.

QUESTION 5

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

Correct Answer: C

In Splunk Phantom, user prompts are actions that require human input. To evaluate the results of a user prompt, you can set the response requirement in the action result summary. By setting action_result.summary.response to required, the playbook ensures that it captures the user\\'s input and can act upon it. This is critical in scenarios where subsequent actions depend on the choices made by the user in response to a prompt. Without setting this, the playbook would not have a defined way to handle the user response, which might lead to incorrect or unexpected playbook behavior.

Latest SPLK-2003 Dumps SPLK-2003 Practice Test SPLK-2003 Braindumps