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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

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

In Splunk SOAR, when working on a case and analyzing events, items marked as significant evidence are aggregated for review. These evidence items can be collectively viewed on the Investigation page under the Evidence tab. This centralized view allows analysts to easily access and review all marked evidence related to a case, facilitating a streamlined analysis process and ensuring that key information is readily available for investigation and decision-making.

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

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: C

The global block within a Splunk SOAR playbook is primarily used to import external packages or define global variables that will be utilized across various parts of the playbook. This block sets the stage for the playbook by ensuring that all necessary libraries, modules, or predefined variables are available for use in subsequent actions, decision blocks, or custom code segments within the playbook. This practice promotes code reuse and efficiency, enabling more sophisticated and powerful playbook designs by leveraging external functionalities.

QUESTION 4

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

Correct Answer: D

The severity of a container in Splunk Phantom can be set manually or automatically during the ingestion process. In addition to these methods, playbooks can also change the severity of a container. Playbooks are automated workflows that define a series of actions based on certain triggers and conditions. Within a playbook, actions can be defined to adjust the severity level of a container depending on the analysis of the event data, the outcome of actions taken, or other contextual factors. This dynamic adjustment allows for a more accurate and responsive incident prioritization as new information becomes available during the investigation process.

QUESTION 5

When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible?

A. Install a second Splunk app and configure the query in the second app.

B. Configure the second query in the Splunk App for SOAR Export.

C. Enter the two queries in the asset as comma separated values.

D. Configure a second Splunk asset with the second query.

Correct Answer: C

In Splunk SOAR, if a user needs to run two different on_poll searches for a Splunk Cloud instance, the way to achieve this is to configure a second Splunk asset specifically for the second query. Each asset can be configured with its own

on_poll search, allowing multiple searches to be run at their respective intervals. This method provides flexibility and ensures that each search can be managed and configured individually.

The correct way to run two different on_poll searches from a Splunk Cloud instance to Splunk SOAR is to configure a second Splunk asset with the second query. Each Splunk asset in Splunk SOAR can only have one query for the on_poll

event, which defines which events to pull in and when to pull them in. Therefore, if you need to run two different queries, you need to create two separate Splunk assets and configure them with the respective queries. The other options are

either not possible or not effective for this purpose. For example:

Installing a second Splunk app in Splunk SOAR will not help, as the app is just a container for the actions and assets, not the source of the data.

Configuring the second query in the Splunk App for SOAR Export will not work, as this app is used to forward events from the Splunk platform to Splunk SOAR, not to pull them in.

Entering the two queries in the asset as comma separated values will not work, as the asset will only accept one valid query for the on_poll event.

Latest SPLK-2003 Dumps SPLK-2003 PDF Dumps SPLK-2003 Exam Questions