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.geekcert.com/splk-2003.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the simplest way to pass data between playbooks?

A. Action results

B. File system

C. Artifacts

D. KV Store

Correct Answer: A

Passing data between playbooks in Splunk Phantom is most efficiently done through action results. Playbooks are composed of actions, which are individual steps that perform operations. When an action is executed, it generates results, which can include data like IP addresses, usernames, or any other relevant information. These results can be passed to subsequent playbooks as input, allowing for a seamless flow of information and enabling complex automation sequences. Other methods, like using the file system, artifacts, or KV Store, are less direct and can be more complex to implement for this purpose.

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

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: B

Splunk SOAR (formerly Phantom) utilizes its own embedded search engine for querying and analyzing data within the platform. This search engine is specifically designed to cater to the unique data structures and use cases of security automation and orchestration, including searching through containers, artifacts, actions, and more. While Splunk SOAR can integrate with external Splunk instances for enhanced data analysis and search capabilities, the platform\\'s primary, out-of-the-box search functionality is provided by its embedded Phantom search engine.

QUESTION 4

Which of the following can be done with the System Health Display?

A. Create a temporary, edited version of a process and test the results.

B. Partially rewind processes, which is useful for debugging.

C. View a single column of status for SOAR processes. For metrics, click Details.

D. Reset DECIDED to reset playbook environments back to at-start conditions.

Correct Answer: C

System Health Display is a dashboard that shows the status and performance of the SOAR processes and components, such as the automation service, the playbook daemon, the DECIDED process, and the REST API. One of the things that can be done with the System Health Display is to reset DECIDED, which is a core component of the SOAR automation engine that handles the execution of playbooks and actions. Resetting DECIDED can be useful for troubleshooting or debugging purposes, as it resets the playbook environments back to at-start conditions, meaning that any changes made by the playbooks are discarded and the playbooks are reloaded. To reset DECIDED, you need to click on the Reset DECIDED button on the System Health Display dashboard. Therefore, option D is the correct answer, as it is the only option that can be done with the System Health Display. Option A is incorrect, because creating a temporary, edited version of a process and testing the results is not something that can be done with the System Health Display, but rather with the Debugging dashboard, which allows you to modify and run a process in a sandbox environment. Option B is incorrect, because partially rewinding processes, which is useful for debugging, is not something that can be done with the System Health Display, but rather with the Rewind feature, which allows you to go back to a previous state of a process and resume the execution from there. Option C is incorrect, because viewing a single column of status for SOAR processes is not something that can be done with the System Health Display, but rather with the Status Display dashboard, which shows a simplified view of the SOAR processes and their status.

1: Web search results from search_web(query="Splunk SOAR Automation Developer System Health Display")

QUESTION 5

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.