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

What do assets provide for app functionality?

A. Assets provide location, credentials, and other parameters needed to run actions.

B. Assets provide hostnames, passwords, and other artifacts needed to run actions.

C. Assets provide Python code, REST API, and other capabilities needed to run actions.

D. Assets provide firewall, network, and data sources needed to run actions.

Correct Answer: A

The correct answer is A because assets provide location, credentials, and other parameters needed to run actions. Assets are configurations that define how Phantom connects to external systems or devices, such as firewalls, endpoints, or threat intelligence sources. Assets specify the app, the IP address or hostname, the username and password, and any other settings required to run actions on the target system or device. The answer B is incorrect because assets do not provide hostnames, passwords, and other artifacts needed to run actions, which are data objects that can be created or retrieved by playbooks. The answer C is incorrect because assets do not provide Python code, REST API, and other capabilities needed to run actions, which are provided by apps. The answer D is incorrect because assets do not provide firewall, network, and data sources needed to run actions, which are external systems or devices that can be connected to by assets. Reference: Splunk SOAR Admin Guide, page 45. Assets in Splunk Phantom are configurations that contain the necessary information for apps to connect to external systems and services. This information can include IP addresses, domain names, credentials like usernames and passwords, and other necessary parameters such as API keys or tokens. These parameters enable the apps to perform actions like running queries, executing commands, or gathering data. Assets do not provide the actual Python code, REST API capabilities, or network infrastructure; they are the bridge between the apps and the external systems with the configuration data needed for successful communication and action execution

QUESTION 2

Why is it good playbook design to create smaller and more focused playbooks? (select all that apply)

A. Reduces amount of playbook data stored in each repo.

B. Reduce large complex playbooks which become difficult to maintain.

C. Encourages code reuse in a more compartmentalized form.

D. To avoid duplication of code across multiple playbooks.

Correct Answer: BCD

Creating smaller and more focused playbooks in Splunk SOAR is considered good design practice for several reasons:

B: It reduces complexity, making playbooks easier to maintain. Large, complex playbooks can become unwieldy and difficult to troubleshoot or update.

C: Encourages code reuse, as smaller playbooks can be designed to handle specific tasks that can be reused across different scenarios.

D: Avoids duplication of code, as common functionalities can be centralized within specific playbooks, rather than

having the same code replicated across multiple playbooks.

This approach has several benefits, such as:

Reducing large complex playbooks which become difficult to maintain. Smaller playbooks are easier to read, debug, and update.

Encouraging code reuse in a more compartmentalized form. Smaller playbooks can be used as building blocks for multiple scenarios, reducing the need to write duplicate code.

Improving performance and scalability. Smaller playbooks can run faster and consume less resources than larger playbooks.

The other options are not valid reasons for creating smaller and more focused playbooks. Reducing the amount of playbook data stored in each repo is not a significant benefit, as the playbook data is not very large compared to other types of

data in Splunk SOAR. Avoiding duplication of code across multiple playbooks is a consequence of code reuse, not a separate goal.

QUESTION 3

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 4

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.

Correct Answer: A

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. In Splunk Phantom, to determine which app actions are available, a user can add an action block to the playbook canvas area within the visual playbook editor. The action block will present a list of available apps and their associated actions that the user can choose from. This method provides a user-friendly way to browse and select from the various actions that can be incorporated into the automation workflows (playbooks). The visual playbook editor is a key component of Phantom, allowing users to design, edit, and manage playbooks via a graphical interface.

QUESTION 5

A user selects the New option under Sources on the menu. What will be displayed?

A. A list of new assets.

B. The New Data Ingestion wizard.

C. A list of new data sources.

D. A list of new events.

Correct Answer: B

Selecting the New option under Sources in the Splunk SOAR menu typically initiates the New Data Ingestion wizard. This wizard guides users through the process of configuring new data sources for ingestion into the SOAR platform. It is designed to streamline the setup of various data inputs, such as event logs, threat intelligence feeds, or notifications from other security tools, ensuring that SOAR can receive and process relevant security data efficiently. This feature is crucial for expanding SOAR\\'s monitoring and response capabilities by integrating diverse data sources. Options A, C, and D do not accurately describe what is displayed when the New option under Sources is selected, making option B the correct choice. New Data Ingestion wizard allows you to create a new data source for Splunk SOAR (On- premises) by selecting the type of data, the ingestion method, and the configuration options. The other options are incorrect because they do not match the description of the New option under Sources on the menu. For example, option A refers to a list of new assets, which is not related to data ingestion. Option C refers to a list of new data sources, which is not what the New option does. Option D refers to a list of new events, which is not the same as creating a new data source.