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

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

QUESTION 1

An active playbook can be configured to operate on all containers that share which attribute?

A. Artifact

B. Label

C. Tag

D. Severity

Correct Answer: B

The correct answer is B because an active playbook can be configured to operate on all containers that share a label. A label is a user-defined attribute that can be applied to containers to group them by a common characteristic, such as source, type, severity, etc. Labels can be used to filter containers and trigger active playbooks based on the label value. See Splunk SOAR Documentation for more details. In Splunk SOAR, labels are used to categorize containers (such as incidents or events) based on their characteristics or the type of security issue they represent. An active playbook can be configured to trigger on all containers that share a specific label, enabling targeted automation based on the nature of the incident. This functionality allows for efficient and relevant playbook execution, ensuring that the automated response is tailored to the specific requirements of the container\\'s category. Labels serve as a powerful organizational tool within SOAR, guiding the automated response framework to act on incidents that meet predefined criteria, thus streamlining the security operations process.

QUESTION 2

Which of the following is an asset ingestion setting in SOAR?

A. Polling Interval

B. Tag

C. File format

D. Operating system

Correct Answer: A

The asset ingestion setting \\'Polling Interval\\' within Splunk SOAR determines how frequently the SOAR platform will poll an asset to ingest data. This setting is crucial for assets that are configured to pull in data from external sources at regular intervals. Adjusting the polling interval allows administrators to balance the need for timely data against network and system resource considerations. An asset ingestion setting is a configuration option that allows you to specify how often SOAR should poll an asset for new data. Data ingestion settings are available for assets such as QRadar, Splunk, and IMAP. To configure ingestion settings for an asset, you need to navigate to the Asset Configuration page, select the Ingest Settings tab, and edit the Polling Interval field. The Polling Interval is the number of seconds between each poll request that SOAR sends to the asset. Therefore, option A is the correct answer, as it is the only option that is an asset ingestion setting in SOAR. Option B is incorrect, because Tag is not an asset ingestion setting, but a way of labeling an asset for easier identification and filtering. Option C is incorrect, because File format is not an asset ingestion setting, but a way of specifying the format of the data that is ingested from an asset. Option D is incorrect, because Operating system is not an asset ingestion setting, but a way of identifying the type of system that an asset runs on. Configure ingest settings for a Splunk SOAR (On-premises) asset

QUESTION 3

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?

A. Use the py-postgresq1 module to directly save the data in the Postgres database.

B. Cal the child playbooks getter function.

C. Create artifacts using one playbook and collect those artifacts in another playbook.

D. Use the Handle method to pass data directly between playbooks.

Correct Answer: C

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. In the context of Splunk SOAR, one of the best practices for data sharing across playbooks is to create artifacts in one playbook and use another playbook to collect and utilize those artifacts. Artifacts in Splunk SOAR are structured data related to security incidents (containers) that playbooks can act upon. By creating artifacts in one playbook, you can effectively pass data and context to subsequent playbooks, allowing for modular, reusable, and interconnected playbook designs. This approach promotes efficiency, reduces redundancy, and enhances the playbook\\'s ability to handle complex workflows.

QUESTION 4

What are the components of the I2A2 design methodology?

A. Inputs, Interactions, Actions, Apps

B. Inputs, Interactions, Actions, Artifacts

C. Inputs, Interactions, Apps, Artifacts

D. Inputs, Interactions, Actions, Assets

Correct Answer: B

I2A2 design methodology is a framework for designing playbooks that consists of four components:

Inputs: The data that is required for the playbook to run, such as artifacts, parameters, or custom fields.

Interactions: The blocks that allow the playbook to communicate with users or other systems, such as prompts, comments, or emails.

Actions: The blocks that execute the core logic of the playbook, such as app actions, filters, decisions, or utilities.

Artifacts: The data that is generated or modified by the playbook, such as new artifacts, container fields, or notes.

The I2A2 design methodology helps you to plan, structure, and test your playbooks in a modular and efficient way.

Therefore, option B is the correct answer, as it lists the correct components of the I2A2 design methodology. Option A is

incorrect, because apps are not a component of the I2A2 design methodology, but a source of actions that can be used in the playbook. Option C is incorrect, for the same reason as option A. Option D is incorrect, because assets are not a

component of the I2A2 design methodology, but a configuration of app credentials that can be used in the playbook.

Use a playbook design methodology in Administer Splunk SOAR (Cloud) The I2A2 design methodology is an approach used in Splunk SOAR to structure and design playbooks. The acronym stands for Inputs, Interactions, Actions, and

Artifacts. This methodology guides the creation of playbooks by focusing on these four key components, ensuring that all necessary aspects of an automated response are considered and effectively implemented within the platform.

QUESTION 5

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.