# 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**

On a multi-tenant Phantom server, what is the default tenant\\'s ID?

A. 0

B. Default

C. 1

D. *

Correct Answer: C

The correct answer is C because the default tenant\\'s ID is 1. The tenant ID is a unique identifier for each tenant on a multi-tenant Phantom server. The default tenant is the tenant that is created when Phantom is installed and contains all the existing data and assets. The default tenant\\'s ID is always 1 and cannot be changed. Other tenants have IDs that are assigned sequentially starting from 2. See Splunk SOAR Documentation for more details. In a multi-tenant Splunk SOAR environment, the default tenant is typically assigned an ID of 1. This ID is system-generated and is used to uniquely identify the default tenant within the SOAR database and system configurations. The default tenant serves as the primary operational environment before any additional tenants are configured, and its ID is crucial for database operations, API calls, and internal reference within the SOAR platform. Understanding and correctly using tenant IDs is essential for managing resources, permissions, and data access in a multi-tenant SOAR setup.

**QUESTION 2**

Which of the following actions will store a compressed, secure version of an email attachment with suspected malware for future analysis?

A. Copy/paste the attachment into a note.

B. Add a link to the file in a new artifact.

C. Use the Files tab on the Investigation page to upload the attachment.

D. Use the Upload action of the Secure Store app to store the file in the database.

Correct Answer: D

To securely store a compressed version of an email attachment suspected of containing malware for future analysis, the most effective approach within Splunk SOAR is to use the Upload action of the Secure Store app. This app is specifically designed to handle sensitive or potentially dangerous files by securely storing them within the SOAR database, allowing for controlled access and analysis at a later time. This method ensures that the file is not only safely contained but also available for future forensic or investigative purposes without risking exposure to the malware. Options A, B, and C do not provide the same level of security and functionality for handling suspected malware files, making option D the most appropriate choice.

Secure Store app is a SOAR app that allows you to store files securely in the SOAR database. The Secure Store app provides two actions: Upload and Download. The Upload action takes a file as an input and stores it in the SOAR database in a compressed and encrypted format. The Download action takes a file ID as an input and retrieves the file from the SOAR database and decrypts it. The Secure Store app can be used to store files that contain sensitive or malicious data, such as email attachments with suspected malware, for future analysis. Therefore, option D is the correct answer, as it states the action that will store a compressed, secure version of an email attachment with suspected malware for future analysis. Option A is incorrect, because copying and pasting the attachment into a note will not store the file securely, but rather expose the file content to anyone who can view the note. Option B is incorrect, because adding a link to the file in a new artifact will not store the file securely, but rather create a reference to the file location, which may not be accessible or reliable. Option C is incorrect, because using the Files tab on the Investigation page to upload the attachment will not store the file securely, but rather store the file in the SOAR file system, which may not be encrypted or compressed. Web search results from search_web(query="Splunk SOAR Automation Developer store email attachment with suspected malware")

**QUESTION 3**

Is it possible to import external Python libraries such as the time module?

A. No.

B. No, but this can be changed by setting the proper permissions.

C. Yes, in the global block.

D. Yes. from a drop-down menu.

Correct Answer: C

In Splunk SOAR, it is possible to import external Python libraries, such as the time module, within the scope of a playbook\\'s global code block. The global block allows users to define custom Python code, including imports of standard Python libraries that are included in the Phantom platform\\'s Python environment. This capability enables the extension of playbooks\\' functionality with additional Python logic, making playbooks more powerful and versatile in their operations.

**QUESTION 4**

Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?

A. Non-Human

B. Automation

C. Automation Engineer

D. Service Account

Correct Answer: A

In Splunk SOAR, the \\'Non-Human\\' role is appropriate for accounts that are used exclusively to execute automated tasks. This role is designed for service accounts that interact with the SOAR platform programmatically rather than through a human user. It ensures that the account has the necessary permissions to perform automated actions while restricting access that would be unnecessary or inappropriate for a non-human entity.

**QUESTION 5**

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.

Latest SPLK-2003 Dumps    SPLK-2003 PDF Dumps    SPLK-2003 Braindumps