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

Which is the primary system requirement that should be increased with heavy usage of the file vault?

A. Amount of memory.

B. Number of processors.

C. Amount of storage.

D. Bandwidth of network.

Correct Answer: C

The primary system requirement that should be increased with heavy usage of the file vault is the amount of storage. The file vault is a secure repository for storing files on Phantom. The more files are stored, the more storage space is needed. The other options are not directly related to the file vault usage. See [File vault] for more information. Heavy usage of the file vault in Splunk SOAR necessitates an increase in the amount of storage available. The file vault is used to securely store files associated with cases, such as malware samples, logs, and other artifacts relevant to an investigation. As the volume of files and the size of stored data grow, ensuring sufficient storage capacity becomes critical to maintain performance and ensure that all necessary data is retained for analysis and evidence.

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

A user has written a playbook that calls three other playbooks, one after the other. The user notices that the second playbook starts executing before the first one completes. What is the cause of this behavior?

A. Incorrect Join configuration on the second playbook.

B. The first playbook is performing poorly.

C. The steep option for the second playbook is not set to a long enough interval.

D. Synchronous execution has not been configured.

Correct Answer: D

The correct answer is D because synchronous execution has not been configured. Synchronous execution is a feature that allows you to control the order of execution of playbook blocks. By default, Phantom executes playbook blocks asynchronously, meaning that it does not wait for one block to finish before starting the next one. This can cause problems when you have dependencies between blocks or when you call other playbooks. To enable synchronous execution, you need to use the sync action in the run playbook block and specify the name of the next block to run after the called playbook completes. See Splunk SOAR Documentation for more details. In Splunk SOAR, playbooks can be executed either synchronously or asynchronously. Synchronous execution ensures that a playbook waits for a called playbook to complete before proceeding to the next step. If the second playbook starts executing before the first one completes, it indicates that synchronous execution was not configured for the playbooks. Without synchronous execution, playbooks will execute independently of each other\\'s completion status, leading to potential overlaps in execution. This behavior can be controlled by properly configuring the playbook execution settings to ensure that dependent playbooks complete their tasks in the desired order.

QUESTION 4

How is a Django filter query performed?

A. By adding parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo".

B. phantom/rest/search/app/contains/"sumo"

C. Browse to the Django Filter Query Editor in the Administration panel.

D. Install the SOAR Django App first, then configure the search query in the App editor.

Correct Answer: A

Django filter queries in Splunk SOAR are performed by appending filter parameters directly to the REST API URL. This allows users to refine their search and retrieve specific data. For example, to filter containers by tags containing the word

"sumo", the following URL structure would be used:

https:///rest/container?_filter_tags_contains="sumo". This format enables users to construct dynamic queries that can filter results based on specified criteria within the Django framework used by Splunk SOAR.

The correct way to perform a Django filter query in Splunk SOAR is to add parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo". This will return a list of containers that have the tag "sumo" in

them. You can use various operators and fields to filter the results according to your needs. For more details, see Query for Data and Use filters in your Splunk SOAR (Cloud) playbook to specify a subset of artifacts before further processing.

The other options are either incorrect or irrelevant for this question. For example:

Phantom/rest/search/app/contains/"sumo" is not a valid URL for a Django filter query. It will return an error message saying "Invalid endpoint".

There is no Django Filter Query Editor in the Administration panel of Splunk SOAR. You can use the REST API Tester to test your queries, but not to edit them.

There is no SOAR Django App that needs to be installed or configured for performing Django filter queries. Splunk SOAR uses the Django framework internally, but you do not need to install or use any additional apps for this purpose.

QUESTION 5

What are indicators?

A. Action result items that determine the flow of execution in a playbook.

B. Action results that may appear in multiple containers.

C. Artifact values that can appear in multiple containers.

D. Artifact values with special security significance.

Correct Answer: D

Indicators within the context of Splunk SOAR refer to artifact values that have special security significance. These are typically derived from the data within artifacts and are identified as having particular importance in the analysis and investigation of security incidents. Indicators might include items such as IP addresses, domain names, file hashes, or other data points that can be used to detect, correlate, and respond to security threats. Recognizing and managing indicators effectively is key to leveraging SOAR for enhanced threat intelligence, incident response, and security operations efficiency.