SPLK-2003$^{Q\&As}$

Splunk SOAR Certified Automation Developer

QUESTION 1

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 2

Which of the following queries would return all artifacts that contain a SHA1 file hash?

A. https:///rest/artifact?_filter_cef_md5_insull=false

B. https:///rest/artifact?_filter_cef_Shal_contains=""

C. https:///rest/artifact?_filter_cef_shal_insull=False

D. https:///rest/artifact?_filter_shal__insull=False

Correct Answer: C

To retrieve all artifacts containing a SHA1 file hash via the Splunk SOAR REST API, the appropriate query would filter for artifacts where the \\'cef_sha1\\' field is not null, indicating that a SHA1 hash is present. The correct REST API call should use the filter parameter _filter_cef_shal__isnull=False (assuming \\'shal\\' is a typo and it should be \\'sha1\\'). This query parameter is used to filter out artifacts that do not have a SHA1 hash, thus returning only those that do.

QUESTION 3

In a playbook, more than one Action block can be active at one time. What is this called?

A. Serial Processing

B. Parallel Processing

C. Multithreaded Processing

D. Juggle Processing

Correct Answer: B

In Splunk SOAR, when a playbook is designed such that more than one Action block is active at the same time, it is referred to as \\'Parallel Processing\\'. This allows for multiple actions to be executed concurrently, which can significantly speed up the execution of a playbook as it does not have to wait for one action to complete before starting another. Parallel processing enables more efficient use of resources and time, particularly in complex playbooks that perform numerous actions.

QUESTION 4

Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

A. Notes

B. Actions

C. Service level agreement (SLA) expiration

D. Playbooks

Correct Answer: D

The severity of a container in Splunk Phantom can be set manually or automatically during the ingestion process. In addition to these methods, playbooks can also change the severity of a container. Playbooks are automated workflows that define a series of actions based on certain triggers and conditions. Within a playbook, actions can be defined to adjust the severity level of a container depending on the analysis of the event data, the outcome of actions taken, or other contextual factors. This dynamic adjustment allows for a more accurate and responsive incident prioritization as new information becomes available during the investigation process.

QUESTION 5

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.