Vendor: Splunk

Exam Code:SPLK-2003

Exam Name: Splunk SOAR Certified Automation Developer

Version: Demo

QUESTION 1

When assigning an input parameter to an action while building a playbook, a user notices the artifact value they are looking for does not appear in the auto-populated list.

How is it possible to enter the unlisted artifact value?

A. Type the CEF datapath in manually.

B. Delete and recreate the artifact.

C. Edit the artifact to enable the List as Parameter option for the CEF value.

D. Edit the container to allow CEF parameters.

Correct Answer: A

When building a playbook in Splunk SOAR, if the desired artifact value does not appear in the auto-populated list of input parameters for an action, users have the option to manually enter the Common Event Format (CEF) datapath for that value. This allows for greater flexibility and customization in playbook design, ensuring that specific data points can be targeted even if they\\'re not immediately visible in the interface. This manual entry of CEF datapaths allows users to directly reference the necessary data within artifacts, bypassing limitations of the auto-populated list. Options B, C, and D suggest alternative methods that are not typically used for this purpose, making option A the correct and most direct approach to entering an unlisted artifact value in a playbook action. When assigning an input parameter to an action while building a playbook, a user can use the auto-populated list of artifact values that match the expected data type for the parameter. The auto-populated list is based on the contains parameter of the action inputs and outputs, which enables contextual actions in the SOAR user interface. However, the auto-populated list may not include all the possible artifact values that can be used as parameters, especially if the artifact values are nested or have uncommon data types. In that case, the user can type the CEF datapath in manually, using the syntax artifact.., where field is the name of the artifact field, such as cef, and key is the name of the subfield within the artifact field, such as sourceAddress. Typing the CEF datapath in manually allows the user to enter the unlisted artifact value as an input parameter to the action. Therefore, option A is the correct answer, as it states how it is possible to enter the unlisted artifact value. Option B is incorrect, because deleting and recreating the artifact is not a way to enter the unlisted artifact value, but rather a way to lose the existing artifact data. Option C is incorrect, because editing the artifact to enable the List as Parameter option for the CEF value is not a way to enter the unlisted artifact value, but rather a way to make the artifact value appear in the auto-populated list. Option D is incorrect, because editing the container to allow CEF parameters is not a way to enter the unlisted artifact value, but rather a way to modify the container properties, which are not related to the action parameters. Web search results from search_web(query="Splunk SOAR Automation Developer input parameter to an action")

QUESTION 2

What values can be applied when creating Custom CEF field?

A. Name

B. Name, Data Type

C. Name, Value

D. Name, Data Type, Severity

Correct Answer: B

Custom CEF fields can be created with a name and a data type. The name must be unique and the data type must be one of the following: string, int, float, bool, or list. The severity is not a valid option for custom CEF fields. See Creating custom CEF fields for more details. When creating Custom Common Event Format (CEF) fields in Splunk SOAR (formerly Phantom), the essential values you need to specify are the "Name" of the field and the "Data Type." The "Name" is the identifier for the field, while the "Data Type" specifies the kind of data the field will hold, such as string, integer, IP address, etc. This combination allows for the structured and accurate representation of data within SOAR, ensuring that custom fields are compatible with the platform\\'s data processing and analysis mechanisms.

QUESTION 3

After enabling multi-tenancy, which of the Mowing is the first configuration step?

A. Select the associated tenant artifacts.

B. Change the tenant permissions.

C. Set default tenant base address.

D. Configure the default tenant.

Correct Answer: D

Upon enabling multi-tenancy in Splunk SOAR, the first step in configuration typically involves setting up the default tenant. This foundational step is critical as it establishes the primary operating environment under which subsequent tenants can be created and managed. The default tenant serves as the template for permissions, settings, and configurations that might be inherited or customized by additional tenants. Proper configuration of the default tenant ensures a stable and consistent framework for multi- tenancy operations, allowing for segregated environments within the same SOAR instance, each tailored to specific operational needs or organizational units.

QUESTION 4

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 5

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 6

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 7

Within the 12A2 design methodology, which of the following most accurately describes the last step?

A. List of the apps used by the playbook.

B. List of the actions of the playbook design.

C. List of the outputs of the playbook design.

D. List of the data needed to run the playbook.

Correct Answer: C

The correct answer is C because the last step of the 12A2 design methodology is to list the outputs of the playbook design. The outputs are the expected results or outcomes of the playbook execution, such as sending an email, creating a ticket, blocking an IP, etc. The outputs should be aligned with the objectives and goals of the playbook. See Splunk SOAR Certified Automation Developer for more details. The 12A2 design methodology in the context of Splunk SOAR (formerly Phantom) refers to a structured approach to developing playbooks. The last step in this methodology focuses on defining the outputs of the playbook design. This step is crucial as it outlines what the expected results or actions the playbook should achieve upon its completion. These outputs can vary widely, from sending notifications, creating tickets, updating statuses, to generating reports. Defining the outputs is essential for understanding the playbook\\'s impact on the security operation workflows and how it contributes to resolving security incidents or automating tasks.

QUESTION 8

How is it possible to evaluate user prompt results?

A. Set action_result.summary. status to required.

B. Set the user prompt to reinvoke if it times out.

C. Set action_result. summary. response to required.

D. Add a decision Mode

Correct Answer: C

In Splunk Phantom, user prompts are actions that require human input. To evaluate the results of a user prompt, you can set the response requirement in the action result summary. By setting action_result.summary.response to required, the playbook ensures that it captures the user\\'s input and can act upon it. This is critical in scenarios where subsequent actions depend on the choices made by the user in response to a prompt. Without setting this, the playbook would not have a defined way to handle the user response, which might lead to incorrect or unexpected playbook behavior.

QUESTION 9

Which of the following can be configured in the ROl Settings?

A. Analyst hours per month.

B. Time lost.

C. Number of full time employees (FTEs).

D. Annual analyst salary.

Correct Answer: D

In the ROI (Return on Investment) Settings within Splunk SOAR, one of the configurable parameters is the annual analyst salary. This setting is used to help quantify the cost savings and efficiency gains achieved through the use of SOAR in an organization\\'s security operations. By factoring in the cost of analyst labor, organizations can better assess the financial impact of automating and streamlining security processes with SOAR, contributing to a comprehensive understanding of the solution\\'s value.

QUESTION 10

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 11

What is enabled if the Logging option for a playbook\\'s settings is enabled?

A. More detailed logging information Is available m the Investigation page.

B. All modifications to the playbook will be written to the audit log.

C. More detailed information is available in the debug window.

D. The playbook will write detailed execution information into the spawn.log.

Correct Answer: C

Enabling the Logging option for a playbook\\'s settings in Splunk SOAR enhances the level of detail provided in the debug window when the playbook is executed. This feature is particularly useful for development and troubleshooting purposes, as it allows playbook authors and analysts to see more granular information about how each action within the playbook operates, including inputs, outputs, and any errors or warnings. This detailed logging aids in identifying issues, understanding the playbook\\'s flow, and optimizing performance.

QUESTION 12

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