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.leads4pass.com/splk-2003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

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 2

Which app allows a user to send Splunk Enterprise Security notable events to Phantom?

A. Any of the integrated Splunk/Phantom Apps

B. Splunk App for Phantom Reporting.

C. Splunk App for Phantom.

D. Phantom App for Splunk.

Correct Answer: C

The Splunk App for Phantom is designed to facilitate the integration between Splunk Enterprise Security and Splunk SOAR (Phantom), enabling the seamless forwarding of notable events from Splunk to Phantom. This app allows users to leverage the analytical and data processing capabilities of Splunk ES and utilize Phantom for automated orchestration and response. The app typically includes mechanisms for specifying which notable events to send to Phantom, formatting the data appropriately, and ensuring secure communication between the two platforms. This integration is crucial for organizations looking to combine the strengths of Splunk\\'s SIEM capabilities with Phantom\\'s automation and orchestration features to enhance their security operations.

QUESTION 3

Some of the playbooks on the SOAR server should only be executed by members of the admin role. How can this rule be applied?

A. Make sure the Execute Playbook capability is removed from all roles except admin.

B. Place restricted playbooks in a second source repository that has restricted access.

C. Add a filter block to all restricted playbooks that filters for runRole = "Admin".

D. Add a tag with restricted access to the restricted playbooks.

Correct Answer: A

To restrict playbook execution to members of the admin role within Splunk SOAR, the \\'Execute Playbook\\' capability must be managed appropriately. This is done by ensuring that this capability is removed from all other roles except the admin role. Role-based access control (RBAC) in Splunk SOAR allows for granular permissions, which means you can configure which roles have the ability to execute playbooks, and by restricting this capability, you can control which users are able to initiate playbook runs.

QUESTION 4

After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

A. The new object ID.

B. The new object name.

C. The full CEF name.

D. The PostGres UUID.

Correct Answer: A

The correct answer is A because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is the new object ID. The object ID is a unique identifier for each object in Phantom, such as a container, an artifact, an action, or a playbook. The object ID can be used to retrieve, update, or delete the object using the Phantom REST API. The answer B is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the new object name, which is a human-readable name for the object. The object name can be used to search for the object using the Phantom web interface. The answer C is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the full CEF name, which is a standard format for event data. The full CEF name can be used to access the CEF fields of an artifact using the Phantom REST API. The answer D is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the PostGres UUID, which is a unique identifier for each row in a PostGres database. The PostGres UUID is not exposed to the Phantom REST API. Reference: Splunk SOAR REST API Guide, page 17. When a POST request is made to a Phantom REST endpoint to create a new object, such as an event, artifact, or container, the typical response includes the ID of the newly created object. This ID is a unique identifier that can be used to reference the object within the system for future operations, such as updating, querying, or deleting the object. The response does not usually include the full name or other specific details of the object, as the ID is the most important piece of information needed immediately after creation for reference purposes.

QUESTION 5

Which Phantom API command is used to create a custom list?

A. phantom.add_list()

B. phantom.create_list()

C. phantom.include_list()

D. phantom.new_list()

Correct Answer: B

The Phantom API command to create a custom list is phantom.create_list(). This command takes a list name and an optional description as parameters and returns a list ID if successful. The other commands are not valid Phantom API commands. phantom.add_list() is a Python function that can be used in custom code blocks to add data to an existing list. To create a custom list in Splunk Phantom, the appropriate API command used is phantom.create_list(). This function allows for the creation of a new list that can be used to store data such as IP addresses, file hashes, or any other information that you want to track or reference across multiple playbooks or within different parts of the Phantom platform. The custom list is a flexible data structure that can be leveraged for various use cases within Phantom, including data enrichment, persistent storage of information, and cross-playbook data sharing.

QUESTION 6

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 7

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.

QUESTION 8

Which of the following are the default ports that must be configured on Splunk to allow connections from SOAR?

A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)

B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)

C. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)

D. SplunkWeb (8469), SplunkD (8702), HTTP Collector (8864)

Correct Answer: C

For Splunk SOAR to connect with Splunk Enterprise, certain default ports must be configured to facilitate communication between the two platforms. Typically, SplunkWeb, which serves the Splunk Enterprise web interface, uses port 8000. SplunkD, the Splunk daemon that handles most of the back-end services, listens on port 8089. The HTTP Event Collector (HEC), which allows HTTP clients to send data to Splunk, typically uses port 8088. These ports are essential for the integration, allowing SOAR to send data to Splunk for indexing, searching, and visualization. Options A, B, and D list incorrect port configurations for this purpose, making option C the correct answer based on standard Splunk configurations. These are the default ports used by Splunk SOAR (On-premises) to communicate with the embedded Splunk Enterprise instance. SplunkWeb is the web interface for Splunk Enterprise, SplunkD is the management port for Splunk Enterprise, and HTTP Collector is the port for receiving data from HTTP Event Collector (HEC). The other options are either incorrect or not default ports. For example, option B has the SplunkWeb and SplunkD ports reversed, and option D has arbitrary port numbers that are not used by Splunk by default.

QUESTION 9

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 10

Which of the following are examples of things commonly done with the Phantom REST APP

A. Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists.

B. Use Django queries; use Docker to create a container and add artifacts to it; remove temporary lists.

C. Use Django queries; use curl to create a container and add artifacts to it; add action blocks.

D. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.

Correct Answer: C

The Phantom REST API, often interacted with through the Phantom REST APP, is a powerful tool for automating and integrating Splunk SOAR with other systems. Common uses of the Phantom REST APP include using Django queries to interact with the SOAR database, using curl commands to programmatically create containers and add artifacts to them, and configuring action blocks within playbooks for automated actions. This flexibility allows for a wide range of automation and integration possibilities, enhancing the SOAR platform\\'s capability to respond to security incidents and manage data.

QUESTION 11

What is the default log level for system health debug logs?

A. INFO

B. WARN

C. ERROR

D. DEBUG

Correct Answer: A

The default log level for system health debug logs in Splunk SOAR is typically set to INFO. This log level provides a balance between verbosity and relevance, offering insights into the operational status of the system without the detailed granularity of DEBUG or the limited scope of WARN and ERROR levels.

The default log level for system health debug logs is INFO. This means that only informational messages and higher severity messages (such as WARN, ERROR, or CRITICAL) are written to the log files. You can adjust the logging level for each daemon running in Splunk SOAR to help debug or troubleshoot issues. For more details, see Configure the logging levels for Splunk SOAR (On-premises) daemons.

QUESTION 12

Which of the following applies to filter blocks?

A. Can select which blocks have access to container data.

B. Can select assets by tenant, approver, or app.

C. Can be used to select data for use by other blocks.

D. Can select containers by seventy or status.

Correct Answer: C

The correct answer is C because filter blocks can be used to select data for use by other blocks. Filter blocks can filter data from the container, artifacts, or custom lists based on various criteria, such as field name, value, operator, etc. Filter blocks can also join data from multiple sources using the join action. The output of the filter block can be used as input for other blocks, such as decision, format, prompt, etc. See Splunk SOAR Documentation for more details. Filter blocks within Splunk SOAR playbooks are designed to sift through data and select specific pieces of information based on defined criteria. These blocks are crucial for narrowing down the data that subsequent blocks in a playbook will act upon. By applying filters, a playbook can focus on relevant data, thereby enhancing efficiency and ensuring that actions are taken based on precise, contextually relevant information. This capability is essential for tailoring the playbook\\'s actions to the specific needs of the incident or workflow, enabling more targeted and effective automation strategies. Filters do not directly select blocks for container data access, choose assets by various administrative criteria, or select containers by attributes like severity or status; their primary function is to refine data within the playbook\\'s operational context.

QUESTION 13

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 14

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.

QUESTION 15

How can the DECIDED process be restarted?

A. By restarting the playbook daemon.

B. On the System Health page.

C. In Administration > Server Settings.

D. By restarting the automation service.

Correct Answer: D

DECIDED process is a core component of the SOAR automation engine that handles the execution of playbooks and actions. The DECIDED process can be restarted by restarting the automation service, which can be done from the command line using the service phantom restart command2. Restarting the automation service also restarts the playbook daemon, which is another core component of the SOAR automation engine that handles the loading and unloading of playbooks3. Therefore, option D is the correct answer, as it restarts both the DECIDED process and the playbook daemon. Option A is incorrect, because restarting the playbook daemon alone does not restart the DECIDED process. Option B is incorrect, because the System Health page does not provide an option to restart the DECIDED process or the automation service. Option C is incorrect, because the Administration > Server Settings page does not provide an option to restart the DECIDED process or the automation service.

In Splunk SOAR, if the DECIDED process, which is responsible for playbook execution, needs to be restarted, this can typically be done by restarting the automation (or phantom) service. This service manages the automation processes, including playbook execution. Restarting it can reset the DECIDED process, resolving issues related to playbook execution or process hangs.