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.certbus.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

Which of the following supported approaches enables Phantom to run on a Windows server?

A. Install the Phantom RPM in a GNU Cygwin implementation.

B. Run the Phantom OVA as a cloud instance.

C. Install the Phantom RPM file in Windows Subsystem for Linux (WSL).

D. Run the Phantom OVA as a virtual machine.

Correct Answer: D

Splunk SOAR (formerly Phantom) does not natively run on Windows servers as it is primarily designed for Linux environments. However, it can be deployed on a Windows server through virtualization. By running the Phantom OVA (Open Virtualization Appliance) as a virtual machine, users can utilize virtualization platforms like VMware or VirtualBox on a Windows server to host the Phantom environment. This approach allows for the deployment of Phantom in a Windows-centric infrastructure by leveraging virtualization technology to encapsulate the Phantom application within a supported Linux environment provided by the OVA.

QUESTION 2

What users are included in a new installation of SOAR?

A. The admin and automation users are included by default.

B. The admin, power, and user users are included by default.

C. Only the admin user is included by default.

D. No users are included by default.

Correct Answer: A

The admin and automation users are included by default. Comprehensive and References of

QUESTION 3

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 4

Configuring SOAR search to use an external Splunk server provides which of the following benefits?

A. The ability to run more complex reports on SOAR activities.

B. The ability to ingest Splunk notable events into SOAR.

C. The ability to automate Splunk searches within SOAR.

D. The ability to display results as Splunk dashboards within SOAR.

Correct Answer: A

Configuring Splunk SOAR to use an external Splunk server provides several benefits, one of which is the ability to run more complex reports on SOAR activities. Splunk\\'s powerful search and reporting capabilities allow for deeper analysis and more sophisticated reporting on the data generated by SOAR activities, beyond what is possible with the built- in SOAR search engine.

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

Without customizing container status within Phantom, what are the three types of status for a container?

A. New, In Progress, Closed

B. Low, Medium, High

C. Mew, Open, Resolved

D. Low, Medium, Critical

Correct Answer: A

Within Splunk SOAR, containers (which represent incidents, cases, or events) have a lifecycle that is tracked through their status. The default statuses available without any customization are "New", "In Progress", and "Closed". These statuses help in organizing and managing the incident response process, allowing users to easily track the progress of investigations and responses from initial detection through to resolution.

QUESTION 7

If no data matches any filter conditions, what is the next block run by the playbook?

A. The end block.

B. The start block.

C. The filter block.

D. The next block.

Correct Answer: A

In Splunk SOAR (formerly Phantom), when a playbook is running and it encounters a filter block, if no data matches the filter conditions specified, the playbook will proceed to the end block. The end block signifies the completion of the playbook\\'s execution path that was contingent on the filter conditions being met. If the filter conditions are not met, and there are no alternative paths specified, the playbook recognizes this as the logical conclusion of that particular execution flow.

QUESTION 8

When working with complex data paths, which operator is used to access a sub-element inside another element?

A. !(pipe)

B. *(asterisk)

C. :(colon)

D. .(dot)

Correct Answer: D

When working with complex data paths in Splunk SOAR, particularly within playbooks, the dot (.) operator is used to access sub-elements within a larger data structure. This operator allows for the navigation through nested data, such as

dictionaries or objects within JSON responses, enabling playbook actions and decision blocks to reference specific pieces of data within the artifacts or action results. This capability is crucial for extracting and manipulating relevant information from complex data sets during incident analysis and response automation.

QUESTION 9

What is the main purpose of using a customized workbook?

A. Workbooks automatically implement a customized processing of events using Python code.

B. Workbooks guide user activity and coordination during event analysis and case operations.

C. Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.

D. Workbooks may not be customized; only default workbooks are permitted within Phantom.

Correct Answer: B

The main purpose of using a customized workbook is to guide user activity and coordination during event analysis and case operations. Workbooks can be customized to include different phases, tasks, and instructions for the users. The other options are not valid purposes of using a customized workbook. See Workbooks for more information. Customized workbooks in Splunk SOAR are designed to guide users through the process of analyzing events and managing cases. They provide a structured framework for documenting investigations, tracking progress, and ensuring that all necessary steps are followed during incident response and case management. This helps in coordinating team efforts, maintaining consistency in response activities, and ensuring that all aspects of an incident are thoroughly investigated and resolved. Workbooks can be customized to fit the specific processes and procedures of an organization, making them a versatile tool for managing security operations.

QUESTION 10

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 11

Which of the following is a best practice for use of the global block?

A. Execute code at the beginning of each run of the playbook.

B. Declare outputs which will be selectable within playbook blocks.

C. Import packages which will be used within the playbook.

D. Execute custom code after each run of the playbook.

Correct Answer: C

The global block within a Splunk SOAR playbook is primarily used to import external packages or define global variables that will be utilized across various parts of the playbook. This block sets the stage for the playbook by ensuring that all necessary libraries, modules, or predefined variables are available for use in subsequent actions, decision blocks, or custom code segments within the playbook. This practice promotes code reuse and efficiency, enabling more sophisticated and powerful playbook designs by leveraging external functionalities.

QUESTION 12

Which of the following is a reason to create a new role in SOAR?

A. To define a set of users who have access to a special label.

B. To define a set of users who have access to a restricted app.

C. To define a set of users who have access to an event\\'s reports.

D. To define a set of users who have access to a sensitive tag.

Correct Answer: A

Creating a new role in Splunk SOAR is often done to define a set of users who have specific access rights, such as access to a special label. Labels in SOAR can be used to categorize data and control access. By assigning a role with access to a particular label, administrators can ensure that only a specific group of users can view or interact with containers, events, or artifacts that have been tagged with that label, thus maintaining control over sensitive data or operations.

QUESTION 13

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 14

Which of the following is the complete list of the types of backups that are supported by Phantom?

A. Full backups.

B. Full, delta, and incremental backups.

C. Full and incremental backups.

D. Full and delta backups.

Correct Answer: C

Splunk Phantom supports different types of backups to safeguard data. Full backups create a complete copy of the current state of the system, while incremental backups only save the changes made since the last backup. This approach allows for efficient use of storage space and faster backups after the initial full backup. Delta backups, which would save changes since the last full or incremental backup, are not a standard part of Phantom\\'s backup capabilities according to available documentation. Therefore, the complete list of backups supported by Phantom would be Full and Incremental backups.

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.