HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **SPLK-2003**

Title : Splunk SOAR Certified Automation Developer Exam

Version : DEMO

1.Configuring Phantom search to use an external Splunk server provides which of the following benefits?
A. The ability to run more complex reports on Phantom activities.
B. The ability to ingest Splunk notable events into Phantom.
C. The ability to automate Splunk searches within Phantom.
D. The ability to display results as Splunk dashboards within Phantom.
Answer: C
Explanation:
The correct answer is C because configuring Phantom search to use an external Splunk server allows you to automate Splunk searches within Phantom using the run query action. This action can be used to run any Splunk search command on the external Splunk server and return the results to Phantom. You can also use the format results action to parse the results and use them in other blocks. See Splunk SOAR Documentation for more details.
Configuring Phantom (now known as Splunk SOAR) to use an external Splunk server enhances the automation capabilities within Phantom by allowing the execution of Splunk searches as part of the automation and orchestration processes. This integration facilitates the automation of tasks that involve querying data from Splunk, thereby streamlining security operations and incident response workflows. Splunk SOAR's ability to integrate with over 300 third-party tools, including Splunk, supports a wide range of automatable actions, thus enabling a more efficient and effective security operations center (SOC) by reducing the time to respond to threats and by making repetitive tasks more manageable https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation-features.html

2.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.
Answer: C
Explanation:
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.

3.Which of the following are the steps required to complete a full backup of a Splunk Phantom deployment' Assume the commands are executed from /opt/phantom/bin and that no other backups have been made.

A. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup.pyc --backup.
B. On the command line enter: sudo phenv python ibackup.pyc --backup —backup-type full, then sudo phenv python ibackup.pyc --setup.
C. Within the UI: Select from the main menu Administration > System Health > Backup.
D. Within the UI: Select from the main menu Administration > Product Settings > Backup.
Answer: B
Explanation:
The correct answer is B because the steps required to complete a full backup of a Splunk Phantom deployment are to first run the --backup --backup-type full command and then run the -- setup command. The --backup command creates a backup file in the /opt/phantom/backup directory. The --backup-type full option specifies that the backup file includes all the data and configuration files of the Phantom server. The --setup command creates a configuration file that contains the encryption key and other information needed to restore the backup file. See Splunk SOAR Certified Automation Developer Track for more details.
Performing a full backup of a Splunk Phantom deployment involves using the command-line interface, primarily because Phantom's architecture and data management processes are designed to be managed at the server level for comprehensive backup and recovery. The correct sequence involves initiating a full backup first using the --backup --backup-type full option to ensure all configurations, data, and necessary components are included in the backup. Following the completion of the backup, the --setup option might be used to configure or verify the backup settings, although typically, the setup would precede backup operations in practical scenarios. This process ensures that all aspects of the Phantom deployment are preserved, including configurations, playbooks, cases, and other data, which is crucial for disaster recovery and system migration.

4.An active playbook can be configured to operate on all containers that share which attribute?
A. Artifact
B. Label
C. Tag
D. Severity
Answer: B
Explanation:
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.

5.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.
Answer: C
Explanation:
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.