Exam Questions SPLK-2003

Splunk Phantom Certified Admin

https://www.2passeasy.com/dumps/SPLK-2003/

NEW QUESTION 1
How can the debug log for a playbook execution be viewed?

A. On the Investigation page, select Debug Log from the playbook's action menu in the Recent Activity panel.
B. Click Expand Scope m the debug window.
C. In Administration > System Health > Playbook Run History, select the playbook execution entry, then select Log.
D. Open the playbook in the Visual Playbook Editor, and select Debug Logs in Settings.

Answer: A

Explanation:
Debug logs are essential for troubleshooting and understanding the execution flow of a playbook in Splunk Phantom. The debug log for a playbook execution can be viewed by navigating to the Investigation page of a specific event or container. Within the Recent Activity panel, there is an action menu associated with each playbook run. Selecting "Debug Log" from this menu will display the detailed execution log, showing each action taken, the results of those actions, and any errors or messages generated during the playbook run.

NEW QUESTION 2
What metrics can be seen from the System Health Display? (select all that apply)

A. Playbook Usage
B. Memory Usage
C. Disk Usage
D. Load Average

Answer: BCD

Explanation:
System Health Display is a dashboard that shows the status and performance of the SOAR processes and components, such as the automation service, the playbook daemon, the DECIDED process, and the REST API. Some of the metrics that can be seen from the System Health Display are:
•Memory Usage: The percentage of memory used by the system and the processes.
•Disk Usage: The percentage of disk space used by the system and the processes.
•Load Average: The average number of processes in the run queue or waiting for disk I/O over a period of time.
Therefore, options B, C, and D are the correct answers, as they are the metrics that can be seen from the System Health Display. Option A is incorrect, because Playbook Usage is not a metric that can be seen from the System Health Display, but rather a metric that can be seen from the Playbook Usage dashboard, which shows the number of playbooks and actions run over a period of time.
1: Web search results from search_web(query="Splunk SOAR Automation Developer System Health Display")
The System Health Display in Splunk SOAR provides several metrics to help monitor and manage the health of the system. These typically include:
•B: Memory Usage - This metric shows the amount of memory being used by the SOAR platform, which is important for ensuring that the system does not exceed available resources.
•C: Disk Usage - This metric indicates the amount of storage space being utilized, which is crucial for maintaining adequate storage resources and for planning capacity.
•D: Load Average - This metric provides an indication of the overall load on the system over a period of time, which helps in understanding the system's performance and in identifying potential bottlenecks or issues.
Playbook Usage is generally not a metric displayed on the System Health page; instead, it's more related to the usage analytics of playbooks rather than system health metrics.

NEW QUESTION 3
Why does SOAR use wildcards within artifact data paths?

A. To make playbooks more specific.
B. To make playbooks filter out nulls.
C. To make data access in playbooks easier.
D. To make decision execution in playbooks run faster.

Answer: C

Explanation:
Wildcards are used within artifact data paths in Splunk SOAR playbooks to simplify the process of accessing data. They allow playbooks to reference dynamic or variable data structures without needing to specify exact paths, which can vary between artifacts. This flexibility makes it easier to write playbooks that work across different events and scenarios, without hard-coding data paths.
SOAR uses wildcards within artifact data paths to make data access in playbooks easier. A data path is a way of specifying the location of a piece of data within an artifact. For example, artifact.cef.sourceAddress is a data path that refers to the source address field of the artifact. A wildcard is a special character that can match any value or subfield within a data path. For example, artifact.*.cef.sourceAddress is a data path that uses a wildcard to match any field name before the cef subfield. This allows the playbook to access the source address data regardless of the field name, which can vary depending on the app or source that generated the artifact. Therefore, option C is the correct answer, as it explains why SOAR uses wildcards within artifact data paths. Option A is incorrect, because wildcards do not make playbooks more specific, but more flexible and adaptable. Option B is incorrect, because wildcards do not make playbooks filter out nulls, but match any value or subfield. Option D is incorrect, because wildcards do not make decision execution in playbooks run faster, but make data access in playbooks easier.
1: Understanding datapaths in Administer Splunk SOAR (Cloud)

NEW QUESTION 4
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.

NEW QUESTION 5
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. Ye
E. from a drop-down menu.

Answer: C

Explanation:
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.

NEW QUESTION 6
A user has written a playbook that calls three other playbooks, one after the other. The user notices that the second playbook starts executing before the first one completes. What is the cause of this behavior?

A. Incorrect Join configuration on the second playbook.
B. The first playbook is performing poorly.
C. The steep option for the second playbook is not set to a long enough interval.
D. Synchronous execution has not been configured.

Answer: D

Explanation:
The correct answer is D because synchronous execution has not been configured. Synchronous execution is a feature that allows you to control the order of execution of playbook blocks. By default, Phantom executes playbook blocks asynchronously, meaning that it does not wait for one block to finish before starting the next one. This can cause problems when you have dependencies between blocks or when you call other playbooks. To enable synchronous execution, you need to use the sync action in the run playbook block and specify the name of the next block to run after the called playbook completes. See Splunk SOAR Documentation for more details. In Splunk SOAR, playbooks can be executed either synchronously or asynchronously. Synchronous execution ensures that a playbook waits for a called playbook to complete before proceeding to the next step. If the second playbook starts executing before the first one completes, it indicates that synchronous execution was not configured for the playbooks. Without synchronous execution, playbooks will execute independently of each other's completion status, leading to potential overlaps in execution. This behavior can be controlled by properly configuring the playbook execution settings to ensure that dependent playbooks complete their tasks in the desired order.

NEW QUESTION 7
Which of the following accurately describes the Files tab on the Investigate page?

A. A user can upload the output from a detonate action to the the files tab for further investigation.
B. Files tab items and artifacts are the only data sources that can populate active cases.
C. Files tab items cannot be added to investigation
D. Instead, add them to action blocks.
E. Phantom memory requirements remain static, regardless of Files tab usage.

Answer: A

Explanation:
The Files tab on the Investigate page allows the user to upload, download, and view files related to an investigation. A user can upload the output from a detonate action to the Files tab for further investigation, such as analyzing the file metadata, content, or hash. Files tab items and artifacts are not the only data sources that can populate active cases, as cases can also include events, tasks, notes, and comments. Files tab items can be added to investigations by using the add file action block or the Add File button on the Files tab. Phantom memory requirements may increase depending on the Files tab usage, as files are stored in the Phantom database.
The Files tab on the Investigate page in Splunk Phantom is an area where users can manage and analyze files related to an investigation. Users can upload files, such as outputs from a 'detonate file' action which analyzes potentially malicious files in a sandbox environment. The files tab allows users to store and further investigate these outputs, which can include reports, logs, or any other file types that have been generated or are relevant to the investigation. The Files tab is an integral part of the investigation process, providing easy access to file data for analysis and correlation with other incident data.

NEW QUESTION 8
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.

NEW 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.

Answer: B

Explanation:
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.

NEW QUESTION 10
Which is the primary system requirement that should be increased with heavy usage of the file vault?

A. Amount of memory.
B. Number of processors.
C. Amount of storage.
D. Bandwidth of network.

Answer: C

Explanation:
The primary system requirement that should be increased with heavy usage of the file vault is the amount of storage. The file vault is a secure repository for storing files on Phantom. The more files are stored, the more storage space is needed. The other options are not directly related to the file vault usage. See [File vault] for more information. Heavy usage of the file vault in Splunk SOAR necessitates an increase in the amount of storage available. The file vault is used to securely store files associated with cases, such as malware samples, logs, and other artifacts relevant to an investigation. As the volume of files and the size of stored data grow, ensuring sufficient storage capacity becomes critical to maintain performance and ensure that all necessary data is retained for analysis and evidence.

NEW QUESTION 10
After a playbook has run, where are the results stored?

A. Splunk Index
B. Case
C. Container
D. Log file

Answer: C

Explanation:
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a data object in Phantom, but can be a data source for Phantom. Reference: Splunk SOAR User Guide, page 19. In Splunk Phantom, after a playbook has been executed, the results of the actions within that playbook are stored in the container associated with the event. A container is a data structure that encapsulates all relevant information and data for an incident or event within Phantom, including action results, artifacts, notes, and more. The container allows users to see a consolidated view of all the data and activity related to a particular event. These results are not stored in the Splunk Index, a separate case, or a log file as their primary storage but may be sent to a Splunk index for further analysis.

NEW QUESTION 11
In addition to full backups. Phantom supports what other backup type using backup?

A. Snapshot
B. Incremental
C. Partial
D. Differential

Answer: B

Explanation:
Splunk Phantom supports incremental backups in addition to full backups. An incremental backup is a type of backup that only copies the data that has changed since the last backup (whether that was a full backup or another incremental backup). This method is more storage-efficient than a full backup because it does not repeatedly back up the same data, reducing the amount of storage required and speeding up the backup process. Differential backups, which record the changes since the last full backup, and partial backups, which allow the selection of specific data to back up, are not standard backup types offered by Splunk Phantom according to its documentation.

NEW QUESTION 13
Which of the following are the default ports that must be configured on Splunk to allow connections from Phantom?

A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)
C. SplunkWeb (8421), SplunkD (8061), HTTP Collector (8798)
D. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)

Answer: D

Explanation:
The correct answer is D because the default ports that must be configured on Splunk to allow connections from Phantom are SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088). SplunkWeb is the port used to access the Splunk web interface. SplunkD is the port used to communicate with the Splunk server. HTTP Collector is the port used to send data to Splunk using the HTTP Event Collector (HEC). These ports must be configured on Splunk and Phantom to enable the integration between the two products. See Splunk SOAR Documentation for more details.
To allow connections from Splunk Phantom to Splunk, certain default ports need to be open and properly configured. The default ports include SplunkWeb (8000) for web access, SplunkD (8089) for Splunk's management port, and the HTTP Event Collector (HEC) on port 8088, which is used for ingesting data into Splunk. These ports are essential for the communication between Splunk Phantom and Splunk, facilitating data exchange, search capabilities, and the integration of various functionalities between the two platforms.

NEW QUESTION 16
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.

Answer: C

Explanation:
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.

NEW QUESTION 21
Which of the following is an asset ingestion setting in SOAR?

A. Polling Interval
B. Tag
C. File format
D. Operating system

Answer: A

Explanation:
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.
1: Configure ingest settings for a Splunk SOAR (On-premises) asset

NEW QUESTION 25
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.

Answer: A

Explanation:
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.

NEW QUESTION 29
Which Phantom VPE Nock S used to add information to custom lists?

A. Action blocks
B. Filter blocks
C. API blocks
D. Decision blocks

Answer: C

Explanation:
Filter blocks are used to add information to custom lists in Phantom VPE. Filter blocks allow the user to specify a list name and a filter expression to select the data to be added to the list. Action blocks are used to execute app actions, API blocks are used to make REST API calls, and decision blocks are used to evaluate conditions and branch the playbook execution. In the Phantom Visual Playbook Editor (VPE), an API block is used to interact with various external APIs, including custom lists within Phantom. Custom lists are key-value stores that can be used to maintain state, aggregate data, or track information across multiple playbook runs. API blocks allow the playbook to make GET, POST, PUT, and DELETE requests to these lists, facilitating the addition, retrieval, update, or removal of information. This makes API blocks a versatile tool in managing custom list data within playbooks.

NEW QUESTION 33
Where in SOAR can a user view the JSON data for a container?

A. In the analyst queue.
B. On the Investigation page.
C. In the data ingestion display.
D. In the audit log.

Answer: B

Explanation:
In Splunk SOAR, the Investigation page is where users can delve into the details of containers, artifacts, and actions. It provides a comprehensive view of the incident or event under investigation, including the JSON data associated with containers. This JSON data represents the structured information about the container, including its attributes, artifacts, and actions taken within the playbook. Options A, C, and D do not typically provide a direct view of the container's JSON data, making option B the correct answer for where a user can view this information within SOAR.
A container is the top-level data structure that SOAR playbook APIs operate on. Every container is a structured JSON object which can nest more arbitrary JSON objects, that represent artifacts. A container is the top-level object against which automation is run. To view the JSON data for a container, you need to navigate to the Investigation page, which shows the details of a container, such as its name, label, owner, status, severity, and artifacts. On the Investigation page, you can click on the JSON tab, which displays the JSON representation of the container and its artifacts. Therefore, option B is the correct answer, as it states where in SOAR a user can view the JSON data for a container. Option A is incorrect, because the analyst queue is not where a user can view the JSON data for a container, but rather where a user can view the list of containers assigned to them or their team. Option C is incorrect, because the data ingestion display is not where a user can view the JSON data for a container, but rather where a user can view the status and configuration of the data sources that ingest data into SOAR. Option D is incorrect, because the audit log is not where a user can view the JSON data for a container, but rather where a user can view the history of actions performed on the SOAR system, such as creating, updating, or deleting objects.
1: Understanding containers in Splunk SOAR (Cloud)

NEW QUESTION 36
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.

Answer: A

Explanation:
The admin and automation users are included by default. Comprehensive Explanation and References of Correct Answer:: According to the Splunk SOAR (On-premises) default credentials, script options, and sample configuration files documentation1, the default credentials on a new installation of Splunk SOAR (On-premises) are:
Web Interface Username: soar_local_admin password: password
On Splunk SOAR (On-premises) deployments which have been upgraded from earlier releases the user account admin becomes a normal user account with the Administrator role.
The automation user is a special user account that is used by Splunk SOAR (On-premises) to run actions and playbooks. It has the Automation role, which grants it full access to all objects and data in Splunk SOAR (On-premises).
The other options are incorrect because they either omit the automation user or include users that are not created by default. For example, option B includes the power and user users, which are not part of the default installation. Option C only includes the admin user, which ignores the automation user. Option D claims that

no users are included by default, which is false.
In a new installation of Splunk SOAR, two default user accounts are typically created: admin and automation. The admin account is intended for system administration tasks, providing full access to all features and settings within the SOAR platform. The automation user is a special account used for automated processes and scripts that interact with the SOAR platform, often without requiring direct human intervention. This user has specific permissions that can be tailored for automated tasks. Options B, C, and D do not accurately represent the default user accounts included in a new SOAR installation, making option A the correct answer.

NEW QUESTION 40
A user wants to get the playbook results for a single artifact. Which steps will accomplish the?

A. Use the contextual menu from the artifact and select run playbook.
B. Use the run playbook dialog and set the scope to the artifact.
C. Create a new container including Just the artifact in question.
D. Use the contextual menu from the artifact and select the actions.

Answer: A

Explanation:
To get playbook results for a single artifact, a user can utilize the contextual menu option directly from the artifact itself. This method allows for targeted execution of a playbook on just that artifact, facilitating a focused analysis or action based on the data within that specific artifact. This approach is particularly useful when a user needs to drill down into the details of an individual piece of evidence or data point within a larger incident or case, allowing for granular control and execution of playbooks in the Splunk SOAR environment.

NEW QUESTION 44
A customer wants to design a modular and reusable set of playbooks that all communicate with each other. Which of the following is a best practice for data sharing across playbooks?

A. Use the py-postgresq1 module to directly save the data in the Postgres database.
B. Cal the child playbooks getter function.
C. Create artifacts using one playbook and collect those artifacts in another playbook.
D. Use the Handle method to pass data directly between playbooks.

Answer: C

Explanation:
The correct answer is C because creating artifacts using one playbook and collecting those artifacts in another playbook is a best practice for data sharing across playbooks. Artifacts are data objects that are associated with a container and can be used to store information such as IP addresses, URLs, file hashes, etc. Artifacts can be created using the add artifact action in any playbook block and can be collected using the get artifacts action in the filter block. Artifacts can also be used to trigger active playbooks based on their label or type. See Splunk SOAR Documentation for more details.
In the context of Splunk SOAR, one of the best practices for data sharing across playbooks is to create artifacts in one playbook and use another playbook to collect and utilize those artifacts. Artifacts in Splunk SOAR are structured data related to security incidents (containers) that playbooks can act upon. By creating artifacts in one playbook, you can effectively pass data and context to subsequent playbooks, allowing for modular, reusable, and interconnected playbook designs. This approach promotes efficiency, reduces redundancy, and enhances the playbook's ability to handle complex workflows.

NEW QUESTION 46
Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

A. Add a filter block to al restricted playbooks that Titters for runRole - "Admin".
B. Add a tag with restricted access to the restricted playbooks.
C. Make sure the Execute Playbook capability is removed from al roles except admin.
D. Place restricted playbooks in a second source repository that has restricted access.

Answer: C

Explanation:
The correct answer is C because the best way to restrict the execution of playbooks to members of the admin role is to make sure the Execute Playbook capability is removed from all roles except admin. The Execute Playbook capability is a permission that allows a user to run any playbook on any container. By default, all roles have this capability, but it can be removed or added in the Phantom UI by going to Administration > User Management > Roles. Removing this capability from all roles except admin will ensure that only admin users can execute playbooks. See Splunk SOAR Documentation for more details. To ensure that only members of the admin role can execute specific playbooks on the Phantom server, the most effective approach is to manage role-based access controls (RBAC) directly. By configuring the system to remove the "Execute Playbook" capability from all roles except for the admin role, you can enforce this rule. This method leverages Phantom's built-in RBAC mechanisms to restrict playbook execution privileges. It is a straightforward and secure way to ensure that only users with the necessary administrative privileges can initiate the execution of sensitive or critical playbooks, thus maintaining operational security and control.

NEW QUESTION 50
When writing a custom function that uses regex to extract the domain name from a URL, a user wants to create a new artifact for the extracted domain. Which of the following Python API calls will create a new artifact?

A. phantom.new_artifact ()
B. phanto
C. update ()
D. phantom.create_artifact ()
E. phantom.add_artifact ()

Answer: C

Explanation:
In the Splunk SOAR platform, when writing a custom function in Python to handle data such as extracting a domain name from a URL, you can create a new artifact using the Python API call phantom.create_artifact(). This function allows you to specify the details of the new artifact, such as the type, CEF (Common

Event Format) data, container it belongs to, and other relevant information necessary to create an artifact within the system.

NEW QUESTION 51
To limit the impact of custom code on the VPE, where should the custom code be placed?

A. A custom container or a separate KV store.
B. A separate code repository.
C. A custom function block.
D. A separate container.

Answer: C

Explanation:
To limit the impact of custom code on the Visual Playbook Editor (VPE) in Splunk SOAR, custom code should be placed within a custom function block. Custom function blocks are designed to encapsulate code within a playbook, allowing users to input their own Python code and execute it as part of the playbook run. By confining custom code to these blocks, it maintains the VPE's performance and stability by isolating the custom code from the core functions of the playbook.
A custom function block is a way of adding custom Python code to your playbook, which can expand the functionality and processing of your playbook logic. Custom functions can also interact with the REST API in a customizable way. You can share custom functions across your team and across multiple playbooks to increase collaboration and efficiency. To create custom functions, you must have Edit Code permissions, which can be configured by an Administrator in Administration > User Management > Roles and Permissions. Therefore, option C is the correct answer, as it is the recommended way of placing custom code on the VPE, which limits the impact of custom code on the VPE performance and security. Option A is incorrect, because a custom container or a separate KV store are not valid ways of placing custom code on the VPE, but rather ways of storing data or artifacts. Option B is incorrect, because a separate code repository is not a way of placing custom code on the VPE, but rather a way of managing and versioning your code outside of Splunk SOAR. Option D is incorrect, because a separate container is not a way of placing custom code on the VPE, but rather a way of creating a new event or case.
1: Add custom code to your Splunk SOAR (Cloud) playbook with the custom function block using the classic playbook editor

NEW QUESTION 55
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.

Answer: C

Explanation:
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.

NEW QUESTION 56
When configuring a Splunk asset for Phantom to connect to a SplunkC loud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible

A. Enter the two queries in the asset as comma separated values.
B. Configure the second query in the Phantom app for Splunk.
C. Install a second Splunk app and configure the query in the second app.
D. Configure a second Splunk asset with the second query.

Answer: D

Explanation:
In scenarios where there's a need to run different on_poll searches for a Splunk Cloud instance from Splunk SOAR, configuring a second Splunk asset for the additional query is a practical solution. Splunk SOAR's architecture allows for multiple assets of the same type to be configured with distinct settings. By setting up a second Splunk asset specifically for the second on_poll search query, users can maintain separate configurations and ensure that each query is executed in its intended context without interference. This approach provides flexibility in managing different data collection or monitoring needs within the same SOAR environment.

NEW QUESTION 57
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.

Answer: D

Explanation:
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.

NEW QUESTION 60
Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?

A. superuser, administrator
B. phantomcreat
C. phantomedit
D. phantomsearch, phantomdelete
E. admin,user

Answer: A

Explanation:
When configuring Splunk Phantom to integrate with an external Splunk Enterprise instance, it is typically required to have user accounts with sufficient privileges to access data and perform necessary actions. The roles of "superuser" and "administrator" in Splunk provide the broad set of permissions needed for such integration, enabling comprehensive access to data, management capabilities, and the execution of searches or actions that Phantom may require as part of its automated playbooks or investigations.

NEW QUESTION 63
What does a user need to do to have a container with an event from Splunk use context- aware actions designed for notable events?

A. Include the notable event's event_id field and set the artifacts label to aplunk notable event id.
B. Rename the event_id field from the notable event to splunkNotableEventId.
C. Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.
D. Add a custom field to the container named event_id and set the custom field's data type to splunk notable event id.

Answer: C

Explanation:
For a container in Splunk SOAR to utilize context-aware actions designed for notable events from Splunk, it is crucial to ensure that the notable event's unique identifier (event_id) is included in the search results pulled into SOAR. Moreover, by adding a Common Event Format (CEF) definition for the event_id field within Phantom, and setting its data type to something that denotes it as a Splunk notable event ID, SOAR can recognize and appropriately handle these identifiers. This setup facilitates the correct mapping and processing of notable event data within SOAR, enabling the execution of context-aware actions that are specifically tailored to the characteristics of Splunk notable events.

NEW QUESTION 67
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-2003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-2003 Product From:

https://www.2passeasy.com/dumps/SPLK-2003/

Money Back Guarantee

SPLK-2003 Practice Exam Features:

* SPLK-2003 Questions and Answers Updated Frequently

* SPLK-2003 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-2003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-2003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year