Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin

NEW QUESTION 1
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.

Answer: A

Explanation:
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.

NEW QUESTION 2
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 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

Answer: D

Explanation:
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.

NEW QUESTION 4
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)

Answer: D

Explanation:
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.

NEW QUESTION 5
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 6
A user selects the New option under Sources on the menu. What will be displayed?

A. A list of new assets.
B. The New Data Ingestion wizard.
C. A list of new data sources.
D. A list of new events.

Answer: B

Explanation:
Selecting the New option under Sources in the Splunk SOAR menu typically initiates the New Data Ingestion wizard. This wizard guides users through the process of configuring new data sources for ingestion into the SOAR platform. It is designed to streamline the setup of various data inputs, such as event logs, threat intelligence feeds, or notifications from other security tools, ensuring that SOAR can receive and process relevant security data efficiently. This feature is crucial for expanding SOAR's monitoring and response capabilities by integrating diverse data sources. Options A, C, and D do not accurately describe what is displayed when the New option under Sources is selected, making option B the correct choice.
New Data Ingestion wizard allows you to create a new data source for Splunk SOAR (On- premises) by selecting the type of data, the ingestion method, and the configuration options. The other options are incorrect because they do not match the description of the New option under Sources on the menu. For example, option A refers to a list of new assets, which is not related to data ingestion. Option C refers to a list of new data sources, which is not what the New option does. Option D refers to a list of new events, which is not the same as creating a new data source.

NEW QUESTION 7
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

NEW QUESTION 8
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 9
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.

Answer: A

Explanation:
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.

NEW QUESTION 10
Why is it good playbook design to create smaller and more focused playbooks? (select all that apply)

A. Reduces amount of playbook data stored in each repo.
B. Reduce large complex playbooks which become difficult to maintain.
C. Encourages code reuse in a more compartmentalized form.
D. To avoid duplication of code across multiple playbooks.

Answer: BCD

Explanation:
Creating smaller and more focused playbooks in Splunk SOAR is considered good design practice for several reasons:
•B: It reduces complexity, making playbooks easier to maintain. Large, complex playbooks can become unwieldy and difficult to troubleshoot or update.
•C: Encourages code reuse, as smaller playbooks can be designed to handle specific tasks that can be reused across different scenarios.
•D: Avoids duplication of code, as common functionalities can be centralized within specific playbooks, rather than having the same code replicated across multiple playbooks.
This approach has several benefits, such as:
•Reducing large complex playbooks which become difficult to maintain. Smaller playbooks are easier to read, debug, and update1.
•Encouraging code reuse in a more compartmentalized form. Smaller playbooks can be used as building blocks for multiple scenarios, reducing the need to write duplicate code12.
•Improving performance and scalability. Smaller playbooks can run faster and consume less resources than larger playbooks2.
The other options are not valid reasons for creating smaller and more focused playbooks. Reducing the amount of playbook data stored in each repo is not a significant benefit, as the playbook data is not very large compared to other types of data in Splunk SOAR. Avoiding duplication of code across multiple playbooks is a consequence of code reuse, not a separate goal.

NEW QUESTION 10
How is a Django filter query performed?

A. By adding parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo".
B. phantom/rest/search/app/contains/"sumo"
C. Browse to the Django Filter Query Editor in the Administration panel.
D. Install the SOAR Django App first, then configure the search query in the App editor.

Answer: A

Explanation:
Django filter queries in Splunk SOAR are performed by appending filter parameters directly to the REST API URL. This allows users to refine their search and retrieve specific data. For example, to filter containers by tags containing the word "sumo", the following URL structure would be used: https://<PHANTOM_URL>/rest/container?_filter_tags_contains="sumo". This format enables users to construct dynamic queries that can filter results based on specified criteria within the Django framework used by Splunk SOAR.
The correct way to perform a Django filter query in Splunk SOAR is to add parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains=“sumo”. This will return a list of containers that have the tag “sumo” in them. You can use various operators and fields to filter the results according to your needs. For more details, see Query for Data and Use filters in your Splunk SOAR (Cloud) playbook to specify a subset of artifacts before further processing. The other options are either incorrect or irrelevant for this question. For example:
•phantom/rest/search/app/contains/“sumo” is not a valid URL for a Django filter query. It will return an error message saying “Invalid endpoint”.
•There is no Django Filter Query Editor in the Administration panel of Splunk SOAR. You can use the REST API Tester to test your queries, but not to edit them.
•There is no SOAR Django App that needs to be installed or configured for performing Django filter queries. Splunk SOAR uses the Django framework internally, but you do not need to install or use any additional apps for this purpose.

NEW QUESTION 13
How can an individual asset action be manually started?

A. With the > action button in the analyst queue page.
B. By executing a playbook in the Playbooks section.
C. With the > action button in the Investigation page.
D. With the > asset button in the asset configuration section.

Answer: C

Explanation:
An individual asset action can be manually started with the > action button in the Investigation page. This allows the user to select an asset and an action to perform on it. The other options are not valid ways to start an asset action manually. See Performing asset actions for more information. Individual asset actions in Splunk SOAR can be manually initiated from the Investigation page of a container. The "> action" button on this page allows users to execute specific actions associated with assets directly, enabling on- the-fly operations on artifacts or indicators within a container. This feature is particularly useful for ad-hoc analysis and actions, allowing analysts to respond to or investigate specific aspects of an incident without the need for a full playbook.

NEW QUESTION 15
When the Splunk App for SOAR Export executes a Splunk search, which activities are completed?

A. CEF fields are mapped to CIM flelds and a container is created on the SOAR server.
B. CIM fields are mapped to CEF fields and a container is created on the SOAR server.
C. CEF fields are mapped to CIM and a container is created on the Splunk server.
D. CIM fields are mapped to CEF and a container is created on the Splunk server.

Answer: B

Explanation:
When the Splunk App for SOAR Export executes a Splunk search, it typically involves mapping Common Information Model (CIM) fields from Splunk to the Common Event Format (CEF) used by SOAR, after which a container is created on the SOAR server to house the related artifacts and information. This process allows for the integration of data between Splunk, which uses CIM for data normalization, and Splunk SOAR, which uses CEF as its data format for incidents and events.
Splunk App for SOAR Export is responsible for sending data from your Splunk Enterprise or Splunk Cloud instances to Splunk SOAR. The Splunk App for SOAR Export acts as a translation service between the Splunk platform and Splunk SOAR by performing the following tasks:
•Mapping fields from Splunk platform alerts, such as saved searches and data models, to CEF fields.
•Translating CIM fields from Splunk Enterprise Security (ES) notable events to CEF fields.
•Forwarding events in CEF format to Splunk SOAR, which are stored as artifacts. Therefore, option B is the correct answer, as it states the activities that are completed when the Splunk App for SOAR Export executes a Splunk search. Option A is incorrect, because CEF fields are not mapped to CIM fields, but the other way around. Option C is incorrect, because a container is not created on the Splunk server, but on the SOAR server. Option D is incorrect, because a container is not created on the Splunk server, but on the SOAR server.
1: Web search results from search_web(query="Splunk SOAR Automation Developer Splunk App for SOAR Export")

NEW QUESTION 20
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. Synchronous execution has not been configured.
B. The first playbook is performing poorly.
C. The sleep option for the second playbook is not set to a long enough interval.
D. Incorrect join configuration on the second playbook.

Answer: A

Explanation:
In Splunk SOAR, playbooks can execute actions either synchronously (waiting for one action to complete before starting the next) or asynchronously (allowing actions to run concurrently). If a playbook starts executing before the previous one has completed, it indicates that synchronous execution has not been properly configured between these playbooks. This is crucial when the output of one playbook is a dependency for the subsequent playbook. Options B, C, and D do not directly address the observed behavior of concurrent playbook execution, making option A the most accurate explanation for why the second playbook starts before the completion of the first.
synchronous execution is a feature of the SOAR automation engine that allows you to control the order of execution of playbook blocks. Synchronous execution ensures that a playbook block waits for the completion of the previous block before starting its execution. Synchronous execution can be enabled or disabled for each playbook block in the playbook editor, by toggling the Synchronous Execution switch in the block settings. Therefore, option A is the correct answer, as it states the cause of the behavior where the second playbook starts executing before the first one completes. Option B is incorrect, because the first playbook performing poorly is not the cause of the behavior, but rather a possible consequence of the behavior. Option C is incorrect, because the sleep option for the second playbook is not the cause of the behavior, but rather a workaround that can be used to delay the execution of the second playbook. Option D is incorrect, because the join configuration on the second playbook is not the cause of the behavior, but rather a way of merging multiple paths of execution into one.
1: Web search results from search_web(query="Splunk SOAR Automation Developer synchronous execution")

NEW QUESTION 24
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 29
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.

Answer: A

Explanation:
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.

NEW QUESTION 30
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 31
Which of the following expressions will output debug information to the debug window in the Visual Playbook Editor?

A. phantom.debug()
B. phantom.exception()
C. phantom.print ()
D. phantom.assert()

Answer: A

Explanation:
The phantom.debug() function is used within Splunk SOAR playbooks to output debug information to the debug window in the Visual Playbook Editor. This function is instrumental in troubleshooting and developing playbooks, as it allows developers to print out variables, messages, or any relevant information that can help in understanding the flow of the playbook, the data being processed, and any issues that might arise during execution. This debugging tool is essential for ensuring that playbooks are functioning as intended and for diagnosing any problems that may occur.

NEW QUESTION 34
When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible?

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

Answer: C

Explanation:
In Splunk SOAR, if a user needs to run two different on_poll searches for a Splunk Cloud instance, the way to achieve this is to configure a second Splunk asset specifically for the second query. Each asset can be configured with its own on_poll search, allowing multiple searches to be run at their respective intervals. This method provides flexibility and ensures that each search can be managed and configured individually.
The correct way to run two different on_poll searches from a Splunk Cloud instance to Splunk SOAR is to configure a second Splunk asset with the second query. Each Splunk asset in Splunk SOAR can only have one query for the on_poll event, which defines which events to pull in and when to pull them in1. Therefore, if you need to run two different queries, you need to create two separate Splunk assets and configure them with the respective queries. The other options are either not possible or not effective for this purpose. For example:
•Installing a second Splunk app in Splunk SOAR will not help, as the app is just a container for the actions and assets, not the source of the data2.
•Configuring the second query in the Splunk App for SOAR Export will not work, as this app is used to forward events from the Splunk platform to Splunk SOAR, not to pull them in3.
•Entering the two queries in the asset as comma separated values will not work, as the asset will only accept one valid query for the on_poll event1.

NEW QUESTION 37
What is the default embedded search engine used by Phantom?

A. Embedded Splunk search engine.
B. Embedded Phantom search engine.
C. Embedded Elastic search engine.
D. Embedded Django search engine.

Answer: B

Explanation:
Splunk SOAR (formerly Phantom) utilizes its own embedded search engine for querying and analyzing data within the platform. This search engine is specifically designed to cater to the unique data structures and use cases of security automation and orchestration, including searching through containers, artifacts, actions,

and more. While Splunk SOAR can integrate with external Splunk instances for enhanced data analysis and search capabilities, the platform's primary, out-of-the-box search functionality is provided
by its embedded Phantom search engine.

NEW QUESTION 41
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.

Answer: D

Explanation:
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.

NEW QUESTION 45
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 47
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.

Answer: D

Explanation:
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.

NEW QUESTION 51
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 54
Which of the following queries would return all artifacts that contain a SHA1 file hash?

A. https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_insull=false
B. https://<PHANTOM_URL>/rest/artifact?_filter_cef_Shal_contains=""
C. https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_insull=False
D. https://<PHANTOM_URL>/rest/artifact?_filter_shal insull=False

Answer: C

Explanation:
To retrieve all artifacts containing a SHA1 file hash via the Splunk SOAR REST API, the appropriate query would filter for artifacts where the 'cef_sha1' field is not null, indicating that a SHA1 hash is present. The correct REST API call should use the filter parameter _filter_cef_shal isnull=False (assuming 'shal' is a typo and it should be 'sha1'). This query parameter is used to filter out artifacts that do not have a SHA1 hash, thus returning only those that do.

NEW QUESTION 58
What are the differences between cases and events?

A. Case: potential threats.Events: identified as a specific kind of problem and need a structured approach.
B. Cases: only include high-level incident artifacts.Events: only include low-level incident artifacts.
C. Cases: contain a collection of container
D. Events: contain potential threats.
E. Cases: incidents with a known violation and a plan for correctio
F. Events: occurrences in the system that may require a response.

Answer: D

Explanation:
Cases and events are two types of containers in Phantom. Cases are incidents with a known violation and a plan for correction, such as a malware infection, a phishing attack, or a data breach. Events are occurrences in the system that may require a response, such as an alert, a log entry, or an email. Cases and events can contain both high-level and low-level incident artifacts, such as IP addresses, URLs, files, or users. Cases do not contain a collection of containers, but rather a collection of artifacts, tasks, notes, and comments. Events are not necessarily potential threats, but rather indicators of potential threats. In the context of Splunk Phantom, cases and events serve different purposes. Cases are structured to manage and respond to incidents with known violations and typically have a plan for correction. They often involve a coordinated response and may include various artifacts, notes, tasks, and evidence that need to be managed collectively. Events, on the other hand, are occurrences or alerts within the system that may require a response. They can be considered as individual pieces of information or incidents that may be part of a larger case. Events are the building blocks that can be aggregated into cases if they are related and require a consolidated approach to incident response and investigation.

NEW QUESTION 59
Phantom supports multiple user authentication methods such as LDAP and SAML2. What other user authentication method is supported?

A. SAML3
B. PIV/CAC
C. Biometrics
D. OpenID

Answer: B

Explanation:
Splunk SOAR supports multiple user authentication methods to ensure secure access to the platform. Apart from LDAP (Lightweight Directory Access Protocol) and SAML2 (Security Assertion Markup Language 2.0), SOAR also supports PIV (Personal Identity Verification) and CAC (Common Access Card) as authentication methods. These are particularly used in government and military organizations for secure and authenticated access to systems, providing a high level of security through physical tokens or cards that contain encrypted user credentials.

NEW QUESTION 61
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 65
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.

Answer: D

Explanation:
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.

NEW QUESTION 70
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 72
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

Answer: B

Explanation:
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.

NEW QUESTION 73
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-2003 Practice Test Here