Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin

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
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()

Answer: B

Explanation:
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.

NEW QUESTION 3
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.

Answer: C

Explanation:
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.

NEW QUESTION 4
How can a child playbook access the parent playbook's action results?

A. Child playbooks can access parent playbook data while the parent Is still running.
B. By setting scope to ALL when starting the child.
C. When configuring the playbook block in the parent, add the desired results in the Scope parameter.
D. The parent can create an artifact with the data needed by the did.

Answer: C

Explanation:
In Splunk Phantom, child playbooks can access the action results of a parent playbook through the use of the Scope parameter. When a parent playbook calls a child playbook, it can pass certain data along by setting the Scope parameter to include the desired action results. This parameter is configured within the playbook block that initiates the child playbook. By specifying the appropriate scope, the parent playbook effectively determines what data the child playbook will have access to, allowing for a more modular and organized flow of information between playbooks.

NEW QUESTION 5
After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

A. The new object ID.
B. The new object name.
C. The full CEF name.
D. The PostGres UUID.

Answer: A

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

NEW QUESTION 6
How is it possible to evaluate user prompt results?

A. Set action_result.summar
B. status to required.
C. Set the user prompt to reinvoke if it times out.
D. Set action_resul
E. summar
F. response to required.
G. Add a decision Mode

Answer: C

Explanation:
In Splunk Phantom, user prompts are actions that require human input. To evaluate the results of a user prompt, you can set the response requirement in the action result summary. By setting action_result.summary.response to required, the playbook ensures that it captures the user's input and can act upon it. This is critical in scenarios where subsequent actions depend on the choices made by the user in response to a prompt. Without setting this, the playbook would not have a defined way to handle the user response, which might lead to incorrect or unexpected playbook behavior.

NEW QUESTION 7
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 8
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 9
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 10
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
A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit which of the following data to pass forward to the next block?

A. Null IP addresses
B. Non-null IP addresses
C. Non-null destinationAddresses
D. Null values

Answer: B

Explanation:
A filter block with only one condition configured which states: artifact.*.cef.sourceAddress !- , would permit only non-null IP addresses to pass forward to the next block. The !- operator means “is not null”. The other options are not valid because they either include null values or other fields than sourceAddress. See Filter block for more details. A filter block in Splunk SOAR that is configured with the condition artifact.*.cef.sourceAddress != (assuming the intention was to use "!=" to denote 'not equal to') is designed to allow data that has non-null sourceAddress values to pass through to subsequent blocks. This means that any artifact data within the container that includes a sourceAddress field with a defined value (i.e., an actual IP address) will be permitted to move forward in the playbook. The filter effectively screens out any artifacts that do not have a source address specified, focusing the playbook's actions on those artifacts that contain valid IP address information in the sourceAddress field.

NEW QUESTION 14
What is the default embedded search engine used by SOAR?

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

Answer: B

Explanation:
the default embedded search engine used by SOAR is the SOAR search engine, which is powered by the PostgreSQL database built-in to Splunk SOAR (Cloud). A Splunk SOAR (Cloud) Administrator can configure options for search from the Home menu, in Search Settings under Administration Settings. The SOAR search engine has been modified to accept the * wildcard and supports various operators and filters. For search syntax and examples, see Search within Splunk SOAR (Cloud)2.
Option A is incorrect, because the embedded Splunk search engine was used in earlier releases of Splunk SOAR (Cloud), but not in the current version. Option C is incorrect, because Django is a web framework, not a search engine. Option D is incorrect, because Elastic is a separate search engine that is not embedded in Splunk SOAR (Cloud).
1: Configure search in Splunk SOAR (Cloud) 2: Search within Splunk SOAR (Cloud)
Splunk SOAR utilizes its own embedded search engine by default, which is tailored to its security orchestration and automation framework. While Splunk SOAR can integrate with other search engines, like the Embedded Splunk search engine, for advanced capabilities and log analytics, its default setup comes with an embedded search engine optimized for

the typical data and search patterns encountered within the SOAR platform.

NEW QUESTION 15
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 17
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 18
During a second test of a playbook, a user receives an error that states: 'an empty parameters list was passed to phantom.act()." What does this indicate?

A. The container has artifacts not parameters.
B. The playbook is using an incorrect container.
C. The playbook debugger's scope is set to new.
D. The playbook debugger's scope is set to all.

Answer: A

Explanation:
The error message "an empty parameters list was passed to phantom.act()" typically indicates that the action being called by the playbook does not have the required parameters to execute. This can happen if the playbook expects certain data to be present in the container's artifacts but finds none. Artifacts in Splunk SOAR (Phantom) are data elements associated with a container (such as an event or alert) that playbooks can act upon. If a playbook action is designed to use data from artifacts as parameters and those artifacts are missing or do not contain the expected data, the playbook cannot execute the action properly, leading to this error.

NEW QUESTION 22
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 24
On a multi-tenant Phantom server, what is the default tenant's ID?

A. Default
B. 1
C. *

Answer: C

Explanation:
The correct answer is C because the default tenant's ID is 1. The tenant ID is a unique identifier for each tenant on a multi-tenant Phantom server. The default tenant is the tenant that is created when Phantom is installed and contains all the existing data and assets. The default tenant's ID is always 1 and cannot be changed. Other tenants have IDs that are assigned sequentially starting from 2. See Splunk SOAR Documentation for more details. In a multi-tenant Splunk SOAR environment, the default tenant is typically assigned an ID of 1. This ID is system-generated and is used to uniquely identify the default tenant within the SOAR database and system configurations. The default tenant serves as the primary operational environment before any additional tenants are configured, and its ID is crucial for database operations, API calls, and internal reference within the SOAR platform. Understanding and correctly using tenant IDs is essential for managing resources, permissions, and data access in a multi-tenant SOAR setup.

NEW QUESTION 28
When assigning an input parameter to an action while building a playbook, a user notices the artifact value they are looking for does not appear in the auto-populated list.
How is it possible to enter the unlisted artifact value?

A. Type the CEF datapath in manually.
B. Delete and recreate the artifact.
C. Edit the artifact to enable the List as Parameter option for the CEF value.
D. Edit the container to allow CEF parameters.

Answer: A

Explanation:
When building a playbook in Splunk SOAR, if the desired artifact value does not appear in the auto-populated list of input parameters for an action, users have the option to manually enter the Common Event Format (CEF) datapath for that value. This allows for greater flexibility and customization in playbook design, ensuring that specific data points can be targeted even if they're not immediately visible in the interface. This manual entry of CEF datapaths allows users to directly reference the necessary data within artifacts, bypassing limitations of the auto-populated list. Options B, C, and D suggest alternative methods that are not typically used for this purpose, making option A the correct and most direct approach to entering an unlisted artifact value in a playbook action.
When assigning an input parameter to an action while building a playbook, a user can use the auto-populated list of artifact values that match the expected data type for the parameter. The auto-populated list is based on the contains parameter of the action inputs and outputs, which enables contextual actions in the SOAR user interface. However, the auto-populated list may not include all the possible artifact values that can be used as parameters, especially if the artifact values are nested or have uncommon data types. In that case, the user can type the CEF datapath in manually, using the syntax artifact.<field>.<key>, where field is the name of the artifact field, such as cef, and key is the name of the subfield within the artifact field, such as sourceAddress. Typing the CEF datapath in manually allows the user to enter the unlisted artifact value as an input parameter to the action. Therefore, option A is the correct answer, as it states how it is possible to enter the unlisted artifact value. Option B is incorrect, because deleting and recreating the artifact is not a way to enter the unlisted artifact value, but rather a way to lose the existing artifact data. Option C is incorrect, because editing the artifact to enable the List as Parameter option for the CEF value is not a way to enter the unlisted artifact value, but rather a way to make the artifact value appear in the auto-populated list. Option D is incorrect, because editing the container to allow CEF parameters is not a way to enter the unlisted artifact value, but rather a way to modify the container properties, which are not related to the action parameters.
1: Web search results from search_web(query="Splunk SOAR Automation Developer input parameter to an action")

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 34
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 35
Which of the following can the format block be used for?

A. To generate arrays for input into other functions.
B. To generate HTML or CSS content for output in email messages, user prompts, or comments.
C. To generate string parameters for automated action blocks.
D. To create text strings that merge state text with dynamic values for input or output.

Answer: D

Explanation:
The format block in Splunk SOAR is utilized to construct text strings by merging static text with dynamic values, which can then be used for both input to other playbook blocks and output for reports, emails, or other forms of communication. This capability is essential for customizing messages, commands, or data processing tasks within a playbook, allowing for the dynamic insertion of variable data into predefined text templates. This feature enhances the playbook's ability to present information clearly and to execute actions that require specific parameter formats.

NEW QUESTION 36
What is the primary objective of using the I2A2 playbook design methodology?

A. To create detailed playbooks.
B. To create playbooks that customers will not edit.
C. To meet customer requirements using a single playbook.
D. To create simple, reusable, modular playbooks.

Answer: D

Explanation:
The primary objective of using the I2A2 playbook design methodology in Splunk SOAR is to create playbooks that are simple, reusable, and modular. This design philosophy emphasizes the creation of playbooks that can be easily understood and maintained, encourages the reuse of playbook components in different scenarios, and fosters the development of playbooks that can be modularly connected or used independently as needed.
I2A2 design methodology is a framework for designing playbooks that consists of four components:
•Inputs: The data that is required for the playbook to run, such as artifacts, parameters, or custom fields.
•Interactions: The blocks that allow the playbook to communicate with users or other systems, such as prompts, comments, or emails.
•Actions: The blocks that execute the core logic of the playbook, such as app actions, filters, decisions, or utilities.
•Artifacts: The data that is generated or modified by the playbook, such as new artifacts, container fields, or notes.
The I2A2 design methodology helps you to plan, structure, and test your playbooks in a modular and efficient way. The primary objective of using the I2A2 design methodology is to create simple, reusable, modular playbooks that can be easily maintained, shared, and customized. Therefore, option D is the correct answer, as it states the primary objective of using the I2A2 design methodology. Option A is incorrect, because creating detailed playbooks is not the primary objective of using the I2A2 design methodology, but rather a possible outcome of following the framework. Option B is incorrect, because creating playbooks that customers will not edit is not the primary objective of using the I2A2 design methodology, but rather a potential risk of not following the framework. Option C is incorrect, because meeting customer requirements using a single playbook is not the primary objective of using the I2A2 design methodology, but rather a challenge that can be overcome by using the framework.
1: Use a playbook design methodology in Administer Splunk SOAR (Cloud).

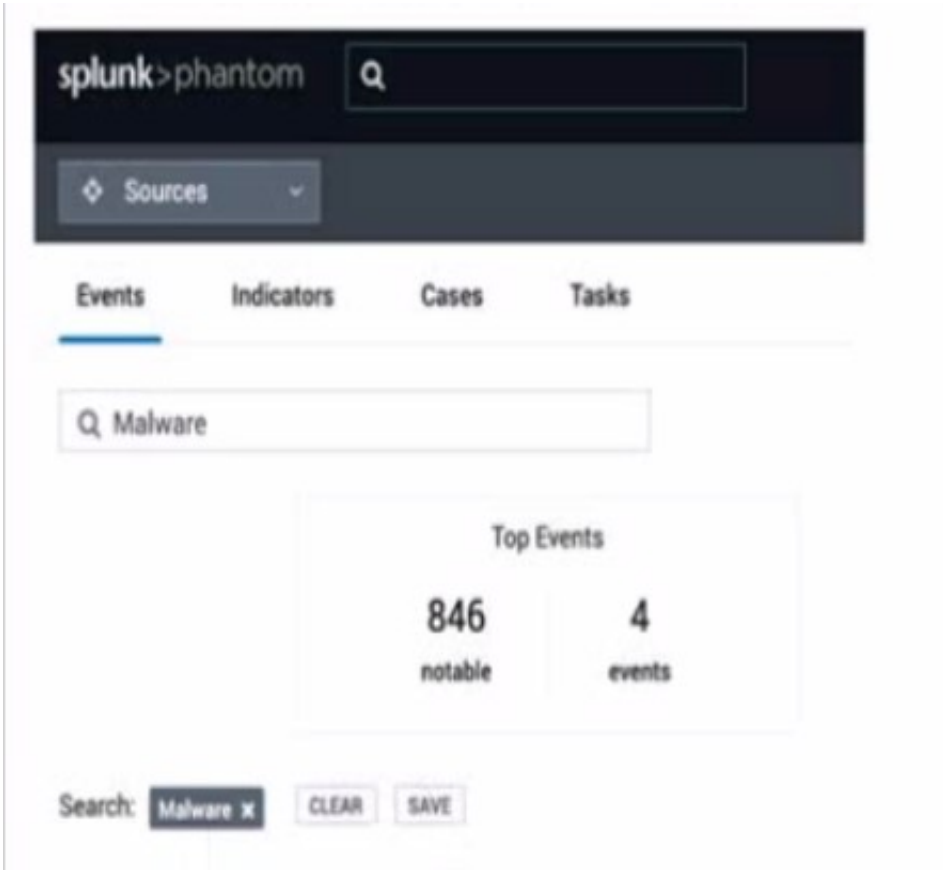
NEW QUESTION 39
After enabling multi-tenancy, which of the Mowing is the first configuration step?

A. Select the associated tenant artifacts.
B. Change the tenant permissions.
C. Set default tenant base address.
D. Configure the default tenant.

Answer: D

Explanation:
Upon enabling multi-tenancy in Splunk SOAR, the first step in configuration typically involves setting up the default tenant. This foundational step is critical as it establishes the primary operating environment under which subsequent tenants can be created and managed. The default tenant serves as the template for permissions, settings, and configurations that might be inherited or customized by additional tenants. Proper configuration of the default tenant ensures a stable and consistent framework for multi- tenancy operations, allowing for segregated environments within the same SOAR instance, each tailored to specific operational needs or organizational units.

NEW QUESTION 43
In this image, which container fields are searched for the text "Malware"?



A. Event Name and Artifact Names.
B. Event Name, Notes, Comments.
C. Event Name or ID.

Answer: C

Explanation:
In the image provided, the search functionality within Splunk's Phantom Security Orchestration, Automation, and Response (SOAR) platform is shown. When you enter a search term like "Malware" in the search bar, Splunk Phantom will typically search through the container fields that are most relevant to identifying and categorizing events. Containers in Phantom are used to group related events, indicators, cases, and tasks. They contain various fields that can be searched through, such as the Event Name or ID, which are primary identifiers for a container. This search does not extend to fields such as Notes or Comments, which are ancillary text entries linked to an event or container. Artifact Names are part of the container's data structure but are not the primary search target in this context unless specifically configured to be included in the search scope.

NEW QUESTION 47
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.

NEW QUESTION 48
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 52
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 56
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 58
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 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 66
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 71
Where can the Splunk App for SOAR Export be downloaded from?

A. GitHub and Splunkbase.
B. SOAR Community and GitHub.
C. Splunkbase and SOAR Community.
D. Splunk Answers and Splunkbase.

Answer: C

Explanation:
The Splunk App for SOAR Export can typically be downloaded from Splunkbase, which is Splunk's marketplace for apps and add-ons. Additionally, it can often be found within the SOAR Community site, where users can share and access apps, playbooks, and other resources created for the Splunk SOAR ecosystem. These platforms provide trusted sources for downloading the app, ensuring compatibility and support.
Splunk App for SOAR Export can be downloaded from two sources: Splunkbase and SOAR Community. Splunkbase is the official repository of Splunk apps and add-ons, where you can find the latest version of the Splunk App for SOAR Export, along with its documentation, release notes, and ratings2. SOAR Community is the online forum for Splunk SOAR users and developers, where you can find the Splunk App for SOAR Export, along with other useful resources, such as FAQs, tips, and best practices3. Therefore, option C is the correct answer, as it lists the two sources where the Splunk App for SOAR Export can be downloaded from.
Option A is incorrect, because GitHub is not a source where the Splunk App for SOAR Export can be downloaded from, but rather a platform for hosting and managing code repositories. Option B is incorrect, for the same reason as option A. Option D is incorrect, because Splunk Answers is not a source where the Splunk App for SOAR Export can be downloaded from, but rather a platform for asking and answering questions about Splunk products and services.
1: Web search results from search_web(query="Splunk SOAR Automation Developer Splunk App for SOAR Export") 2: Splunk App for SOAR Export | Splunkbase
3: SOAR Community - Splunk App for SOAR Export

NEW QUESTION 76
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 79
.....

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