

# 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 in 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 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 3**

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 4**

Which of the following will show all artifacts that have the term results in a filePath CEF value?

- A. `.../rest/artifact?_filter_cef_filePath_icontain="results"`
- B. `...rest/artifacts/filePath="%results%"`
- C. `.../result/artifacts/cef/filePath= "%results%"`
- D. `.../result/artifact?_query_cef_filepath_icontains="results"`

**Answer:** A

**Explanation:**

The correct answer is A because the `_filter` parameter is used to filter the results based on a field value, and the `icontains` operator is used to perform a case-insensitive substring match. The `filePath` field is part of the Common Event Format (CEF) standard, and the `cef_` prefix is used to access CEF fields in the REST API. The answer B is incorrect because it uses the wrong syntax for the REST API. The answer C is incorrect because it uses the wrong endpoint (result instead of artifact) and the wrong syntax for the REST API. The answer D is incorrect because it uses the wrong syntax for the REST API and the wrong spelling for the `icontains` operator. Reference: Splunk SOAR REST API Guide, page 18.

To query and display all artifacts that contain the term "results" in a filePath CEF (Common Event Format) value, using the REST API endpoint with a filter parameter is effective. The filter `_filter_cef_filePath_icontain="results"` is applied to search within the artifact data for filePath fields that contain the term "results", disregarding case sensitivity. This method allows users to precisely locate and work with artifacts that meet specific criteria, aiding in the investigation and analysis processes within Splunk SOAR.

**NEW QUESTION 5**

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 `sudo 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 6**

Severity can be set during ingestion and later changed manually. What other mechanism can change the severity of 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 7**

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 8**

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 9**

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 10**

Which of the following describes the use of labels in Phantom?

- A. Labels determine the service level agreement (SLA) for a container.
- B. Labels control the default severity, ownership, and sensitivity for the container.
- C. Labels control which apps are allowed to execute actions on the container.
- D. Labels determine which playbook(s) are executed when a container is created.

**Answer:** D

**Explanation:**

In Splunk Phantom, labels are used to categorize containers and trigger specific automated responses. When a container is created, labels can be assigned to it based on the nature of the event, type of incident, or other criteria. These labels are then matched against playbooks, which have label conditions defined within them. When the conditions are met, the corresponding playbooks are automatically executed. Labels do not directly control service level agreements, default severity, ownership, sensitivity, or app execution permissions.

**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 15**

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 16**

Which of the following is a step when configuring event forwarding from Splunk to Phantom?

- A. Map CIM to CEF fields.
- B. Create a Splunk alert that uses the `event_forward.py` script to send events to Phantom.
- C. Map CEF to CIM fields.
- D. Create a saved search that generates the JSON for the new container on Phantom.

**Answer:** B

**Explanation:**

A step when configuring event forwarding from Splunk to Phantom is to create a Splunk alert that uses the event\_forward.py script to send events to Phantom. This script will convert the Splunk events to CEF format and send them to Phantom as containers. The other options are not valid steps for event forwarding. See Forwarding events from Splunk to Phantom for more details.

Configuring event forwarding from Splunk to Phantom typically involves creating a Splunk alert that leverages a script (like event\_forward.py) to automatically send triggered event data to Phantom. This setup enables Splunk to act as a detection mechanism that, upon identifying notable events based on predefined criteria, forwards these events to Phantom for further orchestration, automation, and response actions. This integration streamlines the process of incident management by connecting Splunk's powerful data analysis capabilities with Phantom's orchestration and automation framework.

**NEW QUESTION 21**

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 23**

What is the simplest way to pass data between playbooks?

- A. Action results
- B. File system
- C. Artifacts
- D. KV Store

**Answer:** A

**Explanation:**

Passing data between playbooks in Splunk Phantom is most efficiently done through action results. Playbooks are composed of actions, which are individual steps that perform operations. When an action is executed, it generates results, which can include data like IP addresses, usernames, or any other relevant information. These results can be passed to subsequent playbooks as input, allowing for a seamless flow of information and enabling complex automation sequences. Other methods, like using the file system, artifacts, or KV Store, are less direct and can be more complex to implement for this purpose.

**NEW QUESTION 24**

When is using decision blocks most useful?

- A. When selecting one (or zero) possible paths in the playbook.
- B. When processing different data in parallel.
- C. When evaluating complex, multi-value results or artifacts.
- D. When modifying downstream data hi one or more paths in the playbook.

**Answer:** A

**Explanation:**

Decision blocks are most useful when selecting one (or zero) possible paths in the playbook. Decision blocks allow the user to define one or more conditions based on action results, artifacts, or custom expressions, and execute the corresponding path if the condition is met. If none of the conditions are met, the playbook execution ends. Decision blocks are not used for processing different data in parallel, evaluating complex, multi-value results or artifacts, or modifying downstream data in one or more paths in the playbook. Decision blocks within Splunk Phantom playbooks are used to control the flow of execution based on certain criteria. They are most useful when you need to select one or potentially no paths for the playbook to follow, based on the evaluation of specified conditions. This is akin to an if-else or switch-case logic in programming where depending on the conditions met, a particular path is chosen for further actions. Decision blocks evaluate the data and direct the playbook to different paths accordingly, making them a fundamental component for creating dynamic and responsive automation workflows.

**NEW QUESTION 27**

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 30**

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 35**

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 38**

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 41**

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 44**

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 45**

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 in<sup>1</sup>. 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 data<sup>2</sup>.
- 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 in<sup>3</sup>.
- 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 event<sup>1</sup>.

**NEW QUESTION 46**

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

- A. New, Open, Resolved
- B. Low, Medium, High
- C. New, In Progress, Closed
- D. Low, Medium, Critical

**Answer:** C

**Explanation:**

In Splunk SOAR, without any customization, the three default statuses for a container are New, In Progress, and Closed. These statuses are designed to reflect the lifecycle of an incident or event within the platform, from its initial detection and logging (New), through the investigation and response stages (In Progress), to its final resolution and closure (Closed). These statuses help in organizing and prioritizing incidents, tracking their progress, and ensuring a structured workflow. Options A, B, and D do not accurately represent the default container statuses within SOAR, making option C the correct answer. Containers are the top-level data structure that SOAR playbook APIs operate on. Containers can have different statuses that indicate their state and progress in the SOAR workflow. Without customizing container status within SOAR, the three types of status for a container are:

- New: The container has been created but not yet assigned or investigated.
- In Progress: The container has been assigned and is being investigated or automated.
- Closed: The container has been resolved or dismissed and no further action is required. Therefore, option C is the correct answer, as it lists the three types of status for a container without customizing container status within SOAR. Option A is incorrect, because Resolved is not a type of status for a container without customizing container status within SOAR, but rather a custom status that can be defined by an administrator. Option B is incorrect, because Low, Medium, and High are not types of status for a container, but rather types of severity that indicate the urgency or impact of a container. Option D is incorrect, for the same reason as option B.

1: Web search results from `search_web(query="Splunk SOAR Automation Developer container status")`

**NEW QUESTION 48**

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 documentation<sup>1</sup>, 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 52**

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 53**

Which of the following can be edited or deleted in the Investigation page?

- A. Action results
- B. Comments
- C. Approval records
- D. Artifact values

**Answer:** B

**Explanation:**

On the Investigation page in Splunk SOAR, users have the ability to edit or delete comments associated with an event or a container. Comments are generally used for collaboration and to provide additional context to an investigation. While action results, approval records, and artifact values are typically not editable or deletable to maintain the integrity of the investigative data, comments are more flexible and can be managed by users to reflect the current state of the investigation.

Investigation page allows you to view and edit various information and data related to an event or a case. One of the things that you can edit or delete in the Investigation page is the comments that you or other users have added to the activity feed. Comments are a way of communicating and collaborating with other users during the investigation process. You can edit or delete your own comments by clicking on the three-dot menu icon next to the comment and selecting the appropriate option. You can also reply to other users' comments by clicking on the reply icon. Therefore, option B is the correct answer, as it is the only option that can be edited or deleted in the Investigation page. Option A is incorrect, because action results are the outputs of the actions or playbooks that have been run on



the event or case, and they cannot be edited or deleted in the Investigation page. Option C is incorrect, because approval records are the logs of the approval requests and responses that have been made for certain actions or playbooks, and they cannot be edited or deleted in the Investigation page. Option D is incorrect, because artifact values are the data that has been collected or generated by the event or case, and they cannot be edited or deleted in the Investigation page.

1: Start with Investigation in Splunk SOAR (Cloud)

#### NEW QUESTION 54

Which of the following can be configured in the ROI 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 59

Which of the following is an advantage of using the Visual Playbook Editor?

- A. Eliminates any need to use Python code.
- B. The Visual Playbook Editor is the only way to generate user prompts.
- C. Supports Python or Javascript.
- D. Easier playbook maintenance.

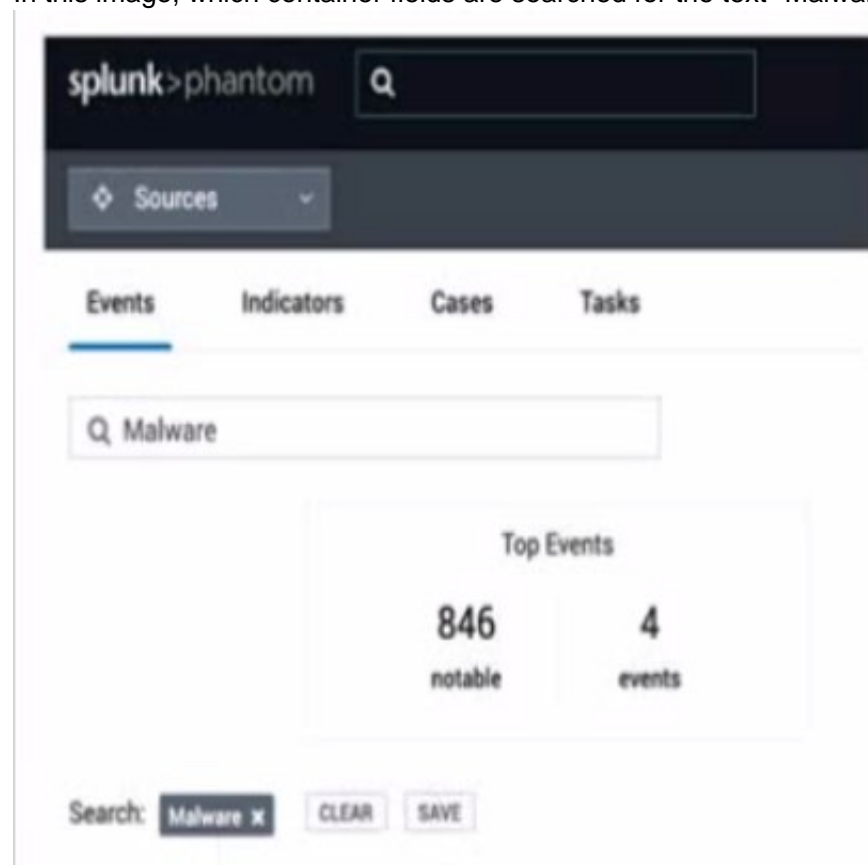
**Answer:** D

#### Explanation:

Visual Playbook Editor is a feature of Splunk SOAR that allows you to create, edit, and implement automated playbooks using visual building blocks and execution flow lanes, without having to write code. The Visual Playbook Editor automatically generates the code for you, which you can view and edit in the Code Editor if needed. The Visual Playbook Editor also supports Python and Javascript as scripting languages for custom code blocks. One of the advantages of using the Visual Playbook Editor is that it makes playbook maintenance easier, as you can quickly modify, test, and debug your playbooks using the graphical interface. Therefore, option D is the correct answer, as it states an advantage of using the Visual Playbook Editor. Option A is incorrect, because using the Visual Playbook Editor does not eliminate the need to use Python code, but rather simplifies the process of creating and editing code. You can still add custom Python code to your playbooks using the custom function block or the Code Editor. Option B is incorrect, because the Visual Playbook Editor is not the only way to generate user prompts, but rather one of the ways. You can also generate user prompts using the classic playbook editor or the Code Editor. Option C is incorrect, because supporting Python or Javascript is not an advantage of using the Visual Playbook Editor, but rather a feature of Splunk SOAR in general. You can use Python or Javascript in any of the playbook editors, not just the Visual Playbook Editor. 1: Web search results from search\_web(query="Splunk SOAR Automation Developer Visual Playbook Editor")

#### NEW QUESTION 62

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 63**

What values can be applied when creating Custom CEF field?

- A. Name
- B. Name, Data Type
- C. Name, Value
- D. Name, Data Type, Severity

**Answer: B**

**Explanation:**

Custom CEF fields can be created with a name and a data type. The name must be unique and the data type must be one of the following: string, int, float, bool, or list. The severity is not a valid option for custom CEF fields. See Creating custom CEF fields for more details. When creating Custom Common Event Format (CEF) fields in Splunk SOAR (formerly Phantom), the essential values you need to specify are the "Name" of the field and the "Data Type." The "Name" is the identifier for the field, while the "Data Type" specifies the kind of data the field will hold, such as string, integer, IP address, etc. This combination allows for the structured and accurate representation of data within SOAR, ensuring that custom fields are compatible with the platform's data processing and analysis mechanisms.

**NEW QUESTION 66**

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 67**

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

- A. `https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_issnull=false`
- B. `https://<PHANTOM_URL>/rest/artifact?_filter_cef_Sha1_contains=""`
- C. `https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_issnull=False`
- D. `https://<PHANTOM_URL>/rest/artifact?_filter_shal_issnull=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_issnull=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 69**

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 70

What do assets provide for app functionality?

- A. Assets provide location, credentials, and other parameters needed to run actions.
- B. Assets provide hostnames, passwords, and other artifacts needed to run actions.
- C. Assets provide Python code, REST API, and other capabilities needed to run actions.
- D. Assets provide firewall, network, and data sources needed to run actions.

**Answer:** A

#### Explanation:

The correct answer is A because assets provide location, credentials, and other parameters needed to run actions. Assets are configurations that define how Phantom connects to external systems or devices, such as firewalls, endpoints, or threat intelligence sources. Assets specify the app, the IP address or hostname, the username and password, and any other settings required to run actions on the target system or device. The answer B is incorrect because assets do not provide hostnames, passwords, and other artifacts needed to run actions, which are data objects that can be created or retrieved by playbooks. The answer C is incorrect because assets do not provide Python code, REST API, and other capabilities needed to run actions, which are provided by apps. The answer D is incorrect because assets do not provide firewall, network, and data sources needed to run actions, which are external systems or devices that can be connected to by assets. Reference: Splunk SOAR Admin Guide, page 45. Assets in Splunk Phantom are configurations that contain the necessary information for apps to connect to external systems and services. This information can include IP addresses, domain names, credentials like usernames and passwords, and other necessary parameters such as API keys or tokens. These parameters enable the apps to perform actions like running queries, executing commands, or gathering data. Assets do not provide the actual Python code, REST API capabilities, or network infrastructure; they are the bridge between the apps and the external systems with the configuration data needed for successful communication and action execution

#### NEW QUESTION 75

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 78

When analyzing events, a working on a case, significant items can be marked as evidence. Where can all of a case's evidence items be viewed together?

- A. Workbook page Evidence tab.
- B. Evidence report.
- C. Investigation page Evidence tab.
- D. At the bottom of the Investigation page widget panel.

**Answer:** C

#### Explanation:

In Splunk SOAR, when working on a case and analyzing events, items marked as significant evidence are aggregated for review. These evidence items can be collectively viewed on the Investigation page under the Evidence tab. This centralized view allows analysts to easily access and review all marked evidence related to a case, facilitating a streamlined analysis process and ensuring that key information is readily available for investigation and decision-making.

#### NEW QUESTION 80

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 84

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 85

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 89

.....



## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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](#)**