

Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin



NEW QUESTION 1

What is the default log level for system health debug logs?

- A. INFO
- B. WARN
- C. ERROR
- D. DEBUG

Answer: A

Explanation:

The default log level for system health debug logs in Splunk SOAR is typically set to INFO. This log level provides a balance between verbosity and relevance, offering insights into the operational status of the system without the detailed granularity of DEBUG or the limited scope of WARN and ERROR levels. The default log level for system health debug logs is INFO. This means that only informational messages and higher severity messages (such as WARN, ERROR, or CRITICAL) are written to the log files. You can adjust the logging level for each daemon running in Splunk SOAR to help debug or troubleshoot issues. For more details, see Configure the logging levels for Splunk SOAR (On-premises) daemons.

NEW QUESTION 2

What is enabled if the Logging option for a playbook's settings is enabled?

- A. More detailed logging information is available in the Investigation page.
- B. All modifications to the playbook will be written to the audit log.
- C. More detailed information is available in the debug window.
- D. The playbook will write detailed execution information into the spawn.log.

Answer: C

Explanation:

Enabling the Logging option for a playbook's settings in Splunk SOAR enhances the level of detail provided in the debug window when the playbook is executed. This feature is particularly useful for development and troubleshooting purposes, as it allows playbook authors and analysts to see more granular information about how each action within the playbook operates, including inputs, outputs, and any errors or warnings. This detailed logging aids in identifying issues, understanding the playbook's flow, and optimizing performance.

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 child.

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

Under Asset Ingestion Settings, how many labels must be applied when configuring an asset?

- A. Labels are not configured under Asset Ingestion Settings.
- B. One.
- C. One or more.
- D. Zero or more.

Answer: D

Explanation:

Under Asset Ingestion Settings in Splunk SOAR, when configuring an asset, the number of labels that must be applied can be zero or more. Labels are optional and are used to categorize data and control access. They are not a requirement under Asset Ingestion Settings, but they can be used to enhance organization and filtering if chosen.

NEW QUESTION 6

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 7

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 8

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 9

Is it possible to import external Python libraries such as the time module?

- A. No.
- B. No, but this can be changed by setting the proper permissions.
- C. Yes, in the global block.
- D. Ye
- E. from a drop-down menu.

Answer: C

Explanation:

In Splunk SOAR, it is possible to import external Python libraries, such as the time module, within the scope of a playbook's global code block. The global block allows users to define custom Python code, including imports of standard Python libraries that are included in the Phantom platform's Python environment. This capability enables the extension of playbooks' functionality with additional Python logic, making playbooks more powerful and versatile in their operations.

NEW QUESTION 10

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 10

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 13

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 17

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 21

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 25

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 29

What are the components of the I2A2 design methodology?

- A. Inputs, Interactions, Actions, Apps
- B. Inputs, Interactions, Actions, Artifacts
- C. Inputs, Interactions, Apps, Artifacts
- D. Inputs, Interactions, Actions, Assets

Answer: B

Explanation:

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. Therefore, option B is the correct answer, as it lists the correct components of the I2A2 design methodology. Option A is incorrect, because apps are not a component of the I2A2 design methodology, but a source of actions that can be used in the playbook. Option C is incorrect, for the same reason as option A. Option D is incorrect, because assets are not a component of the I2A2 design methodology, but a configuration of app credentials that can be used in the playbook.

1: Use a playbook design methodology in Administer Splunk SOAR (Cloud)

The I2A2 design methodology is an approach used in Splunk SOAR to structure and design playbooks. The acronym stands for Inputs, Interactions, Actions, and Artifacts. This methodology guides the creation of playbooks by focusing on these four key components, ensuring that all necessary aspects of an automated response are considered and effectively implemented within the platform.

NEW QUESTION 33

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"](https://<PHANTOM_URL>/rest/container?_filter_tags_contains=). 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 36

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 40

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 45

Which of the following is a best practice for use of the global block?

- A. Execute code at the beginning of each run of the playbook.
- B. Declare outputs which will be selectable within playbook blocks.
- C. Import packages which will be used within the playbook.
- D. Execute custom code after each run of the playbook.

Answer: C

Explanation:

The global block within a Splunk SOAR playbook is primarily used to import external packages or define global variables that will be utilized across various parts of the playbook. This block sets the stage for the playbook by ensuring that all necessary libraries, modules, or predefined variables are available for use in subsequent actions, decision blocks, or custom code segments within the playbook. This practice promotes code reuse and efficiency, enabling more sophisticated and powerful playbook designs by leveraging external functionalities.

NEW QUESTION 46

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

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

Answer: A

Explanation:

The asset ingestion setting 'Polling Interval' within Splunk SOAR determines how frequently the SOAR platform will poll an asset to ingest data. This setting is crucial for assets that are configured to pull in data from external sources at regular intervals. Adjusting the polling interval allows administrators to balance the need for timely data against network and system resource considerations.

An asset ingestion setting is a configuration option that allows you to specify how often SOAR should poll an asset for new data. Data ingestion settings are available for assets such as QRadar, Splunk, and IMAP. To configure ingestion settings for an asset, you need to navigate to the Asset Configuration page, select the Ingest Settings tab, and edit the Polling Interval field. The Polling Interval is the number of seconds between each poll request that SOAR sends to the asset. Therefore, option A is the correct answer, as it is the only option that is an asset ingestion setting in SOAR. Option B is incorrect, because Tag is not an asset

ingestion setting, but a way of labeling an asset for easier identification and filtering. Option C is incorrect, because File format is not an asset ingestion setting, but a way of specifying the format of the data that is ingested from an asset. Option D is incorrect, because Operating system is not an asset ingestion setting, but a way of identifying the type of system that an asset runs on.

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

NEW QUESTION 50

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 55

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

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

Answer: A

Explanation:

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

NEW QUESTION 56

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

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

Answer: C

Explanation:

In Splunk SOAR, if a user needs to run two different `on_poll` searches for a Splunk Cloud instance, the way to achieve this is to configure a second Splunk asset specifically for the second query. Each asset can be configured with its own `on_poll` search, allowing multiple searches to be run at their respective intervals. This method provides flexibility and ensures that each search can be managed and configured individually.

The correct way to run two different `on_poll` searches from a Splunk Cloud instance to Splunk SOAR is to configure a second Splunk asset with the second query. Each Splunk asset in Splunk SOAR can only have one query for the `on_poll` event, which defines which events to pull in and when to pull them in¹. Therefore, if you need to run two different queries, you need to create two separate Splunk assets and configure them with the respective queries. The other options are either not possible or not effective for this purpose. For example:

- Installing a second Splunk app in Splunk SOAR will not help, as the app is just a container for the actions and assets, not the source of the data².
- Configuring the second query in the Splunk App for SOAR Export will not work, as this app is used to forward events from the Splunk platform to Splunk SOAR, not to pull them in³.
- Entering the two queries in the asset as comma separated values will not work, as the asset will only accept one valid query for the `on_poll` event¹.

NEW QUESTION 58

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 59

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 63

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

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

Answer: A

Explanation:

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

NEW QUESTION 64

Which of the following applies to filter blocks?

- A. Can select which blocks have access to container data.
- B. Can select assets by tenant, approver, or app.
- C. Can be used to select data for use by other blocks.
- D. Can select containers by severity or status.

Answer: C

Explanation:

The correct answer is C because filter blocks can be used to select data for use by other blocks. Filter blocks can filter data from the container, artifacts, or custom lists based on various criteria, such as field name, value, operator, etc. Filter blocks can also join data from multiple sources using the join action. The output of the filter block can be used as input for other blocks, such as decision, format, prompt, etc. See Splunk SOAR Documentation for more details.

Filter blocks within Splunk SOAR playbooks are designed to sift through data and select specific pieces of information based on defined criteria. These blocks are crucial for narrowing down the data that subsequent blocks in a playbook will act upon. By applying filters, a playbook can focus on relevant data, thereby enhancing efficiency and ensuring that actions are taken based on precise, contextually relevant information. This capability is essential for tailoring the playbook's actions to the specific needs of the incident or workflow, enabling more targeted and effective automation strategies. Filters do not directly select blocks for container data access, choose assets by various administrative criteria, or select containers by attributes like severity or status; their primary function is to refine data within the playbook's operational context.

NEW QUESTION 69

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.

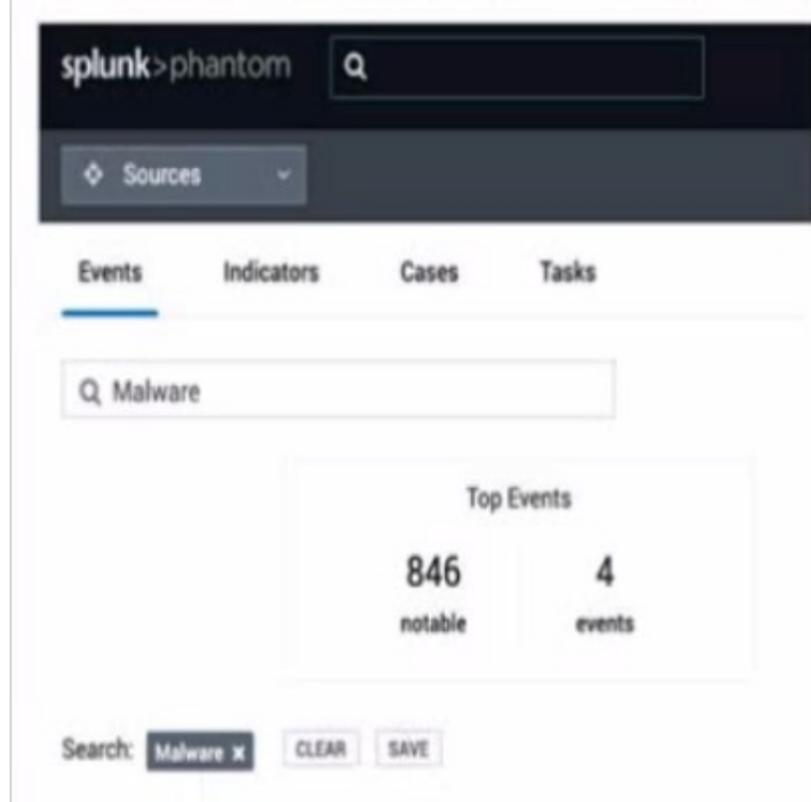
Answer: D

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 74

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 77

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 82

How can the DECIDED process be restarted?

- A. By restarting the playbook daemon.
- B. On the System Health page.
- C. In Administration > Server Settings.

D. By restarting the automation service.

Answer: D

Explanation:

DECIDED process is a core component of the SOAR automation engine that handles the execution of playbooks and actions. The DECIDED process can be restarted by restarting the automation service, which can be done from the command line using the service phantom restart command². Restarting the automation service also restarts the playbook daemon, which is another core component of the SOAR automation engine that handles the loading and unloading of playbooks³. Therefore, option D is the correct answer, as it restarts both the DECIDED process and the playbook daemon. Option A is incorrect, because restarting the playbook daemon alone does not restart the DECIDED process. Option B is incorrect, because the System Health page does not provide an option to restart the DECIDED process or the automation service. Option C is incorrect, because the Administration > Server Settings page does not provide an option to restart the DECIDED process or the automation service.

In Splunk SOAR, if the DECIDED process, which is responsible for playbook execution, needs to be restarted, this can typically be done by restarting the automation (or phantom) service. This service manages the automation processes, including playbook execution. Restarting it can reset the DECIDED process, resolving issues related to playbook execution or process hangs.

NEW QUESTION 86

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_shal_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 87

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 92

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 93

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

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

Answer: B

Explanation:

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

NEW QUESTION 96

Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?

- A. Non-Human
- B. Automation
- C. Automation Engineer
- D. Service Account

Answer: A

Explanation:

In Splunk SOAR, the 'Non-Human' role is appropriate for accounts that are used exclusively to execute automated tasks. This role is designed for service accounts that interact with the SOAR platform programmatically rather than through a human user. It ensures that the account has the necessary permissions to perform automated actions while restricting access that would be unnecessary or inappropriate for a non-human entity.

NEW QUESTION 99

How can more than one user perform tasks in a workbook?

- A. Any user in a role with write access to the case's workbook can be assigned to tasks.
- B. Add the required users to the authorized list for the container.
- C. Any user with a role that has Perform Task enabled can execute tasks for workbooks.
- D. The container owner can assign any authorized user to any task in a workbook.

Answer: C

Explanation:

In Splunk SOAR, tasks within workbooks can be performed by any user whose role has the 'Perform Task' capability enabled. This capability is assigned within the role configuration and allows users with the appropriate permissions to execute tasks. It is not limited to users with write access or the container owner; rather, it is based on the specific permissions granted to the role with which the user is associated.

NEW QUESTION 104

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 108

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 109

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 112

Which of the following can be configured in the ROI Settings?

- A. Number of full time employees (FTEs).
- B. Time lost.
- C. Analyst hours per month.
- D. Annual analyst salary.

Answer: C

Explanation:

ROI Settings dashboard allows you to configure the parameters used to estimate the data displayed in the Automation ROI Summary dashboard. One of the settings that can be configured is the FTE Gained, which is the number of full time employees (FTEs) that are freed up by automation. To calculate this value, Splunk SOAR divides the number of actions run by automation by the number of expected actions an analyst would take, based on minutes per action and analyst hours per day. Therefore, option A is the correct answer, as it is one of the settings that can be configured in the ROI Settings dashboard. Option B is incorrect, because time lost is not a setting that can be configured in the ROI Settings dashboard, but a metric that is calculated by Splunk SOAR based on the difference between the analyst minutes per action and the actual minutes per action. Option C is incorrect, because analyst hours per month is not a setting that can be configured in the ROI Settings dashboard, but a value that is derived from the analyst hours per day setting. Option D is incorrect, because annual analyst salary is a setting that can be configured in the ROI Settings dashboard, but not the one that is asked in the question.

1: Configure the ROI Settings dashboard in Administer Splunk SOAR (On-premises)

ROI (Return on Investment) Settings within Splunk SOAR are used to estimate the efficiency and financial impact of the SOAR platform. One of the configurable parameters in these settings is the 'Analyst hours per month'. This parameter helps in calculating the time saved through automation, which in turn can be translated into cost savings and efficiency gains. It reflects the direct contribution of the SOAR platform to operational productivity.

NEW QUESTION 114

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 117

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 122

.....

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](#)