

SPLK-2003 Dumps

Splunk Phantom Certified Admin

<https://www.certleader.com/SPLK-2003-dumps.html>



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

The SOAR server has been configured to use an external Splunk search head for search and searching on SOAR works; however, the search results don't include content that was being returned by search before configuring external search. Which of the following could be the problem?

- A. The existing content indexes on the SOAR server need to be re-indexed to migrate them to Splunk.
- B. The user configured on the SOAR side with Phantomsearch capability is not enabled on Splunk.
- C. The remote Splunk search head is currently offline.
- D. Content that existed before configuring external search must be backed up on SOAR and restored on the Splunk search head.

Answer: B

Explanation:

If, after configuring an external Splunk search head for search in SOAR, the search results do not include content that was previously returned, one possible issue could be that the user account configured on the SOAR side does not have the required permissions (such as the 'phantomsearch' capability) enabled on the Splunk side. This capability is necessary for the SOAR server to execute searches and retrieve results from the Splunk search head.

NEW QUESTION 5

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 6

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 icontain 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 7

Which app allows a user to send Splunk Enterprise Security notable events to Phantom?

- A. Any of the integrated Splunk/Phantom Apps
- B. Splunk App for Phantom Reporting.
- C. Splunk App for Phantom.
- D. Phantom App for Splunk.

Answer: C

Explanation:

The Splunk App for Phantom is designed to facilitate the integration between Splunk Enterprise Security and Splunk SOAR (Phantom), enabling the seamless forwarding of notable events from Splunk to Phantom. This app allows users to leverage the analytical and data processing capabilities of Splunk ES and utilize Phantom for automated orchestration and response. The app typically includes mechanisms for specifying which notable events to send to Phantom, formatting the data appropriately, and ensuring secure communication between the two platforms. This integration is crucial for organizations looking to combine the strengths of Splunk's SIEM capabilities with Phantom's automation and orchestration features to enhance their security operations.

NEW QUESTION 8

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 9

Sevnty can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

- A. Notes
- B. Actions
- C. Service level agreement (SLA) expiration
- D. Playbooks

Answer: D

Explanation:

The severity of a container in Splunk Phantom can be set manually or automatically during the ingestion process. In addition to these methods, playbooks can also change the severity of a container. Playbooks are automated workflows that define a series of actions based on certain triggers and conditions. Within a playbook, actions can be defined to adjust the severity level of a container depending on the analysis of the event data, the outcome of actions taken, or other contextual factors. This dynamic adjustment allows for a more accurate and responsive incident prioritization as new information becomes available during the investigation process.

NEW QUESTION 10

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

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

Answer: A

Explanation:

To restrict playbook execution to members of the admin role within Splunk SOAR, the 'Execute Playbook' capability must be managed appropriately. This is done by ensuring that this capability is removed from all other roles except the admin role. Role-based access control (RBAC) in Splunk SOAR allows for granular permissions, which means you can configure which roles have the ability to execute playbooks, and by restricting this capability, you can control which users are able to initiate playbook runs.

NEW QUESTION 10

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

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

Answer: A

Explanation:

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

NEW QUESTION 13

Which of the following actions will store a compressed, secure version of an email attachment with suspected malware for future analysis?

- A. Copy/paste the attachment into a note.
- B. Add a link to the file in a new artifact.
- C. Use the Files tab on the Investigation page to upload the attachment.
- D. Use the Upload action of the Secure Store app to store the file in the database.

Answer: D

Explanation:

To securely store a compressed version of an email attachment suspected of containing malware for future analysis, the most effective approach within Splunk SOAR is to use the Upload action of the Secure Store app. This app is specifically designed to handle sensitive or potentially dangerous files by securely storing them within the SOAR database, allowing for controlled access and analysis at a later time. This method ensures that the file is not only safely contained but also available for future forensic or investigative purposes without risking exposure to the malware. Options A, B, and C do not provide the same level of security and functionality for handling suspected malware files, making option D the most appropriate choice.

Secure Store app is a SOAR app that allows you to store files securely in the SOAR database. The Secure Store app provides two actions: Upload and Download. The Upload action takes a file as an input and stores it in the SOAR database in a compressed and encrypted format. The Download action takes a file ID as an input and retrieves the file from the SOAR database and decrypts it. The Secure Store app can be used to store files that contain sensitive or malicious data, such as email attachments with suspected malware, for future analysis. Therefore, option D is the correct answer, as it states the action that will store a compressed, secure version of an email attachment with suspected malware for future analysis. Option A is incorrect, because copying and pasting the attachment into a note will not store the file securely, but rather expose the file content to anyone who can view the note. Option B is incorrect, because adding a link to the file in a new artifact will not store the file securely, but rather create a reference to the file location, which may not be accessible or reliable. Option C is incorrect, because using the Files tab on the Investigation page to upload the attachment will not store the file securely, but rather store the file in the SOAR file system, which may not be encrypted or compressed.

1: Web search results from search_web(query="Splunk SOAR Automation Developer store email attachment with suspected malware")

NEW QUESTION 16

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

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

Answer: A

Explanation:

The Files tab on the Investigate page allows the user to upload, download, and view files related to an investigation. A user can upload the output from a detonate action to the Files tab for further investigation, such as analyzing the file metadata, content, or hash. Files tab items and artifacts are not the only data sources that can populate active cases, as cases can also include events, tasks, notes, and comments. Files tab items can be added to investigations by using the add file action block or the Add File button on the Files tab. Phantom memory requirements may increase depending on the Files tab usage, as files are stored in the

Phantom database.

The Files tab on the Investigate page in Splunk Phantom is an area where users can manage and analyze files related to an investigation. Users can upload files, such as outputs from a 'detonate file' action which analyzes potentially malicious files in a sandbox environment. The files tab allows users to store and further investigate these outputs, which can include reports, logs, or any other file types that have been generated or are relevant to the investigation. The Files tab is an integral part of the investigation process, providing easy access to file data for analysis and correlation with other incident data.

NEW QUESTION 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 18

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

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

Answer: BCD

Explanation:

Creating smaller and more focused playbooks in Splunk SOAR is considered good design practice for several reasons:

- B: It reduces complexity, making playbooks easier to maintain. Large, complex playbooks can become unwieldy and difficult to troubleshoot or update.
- C: Encourages code reuse, as smaller playbooks can be designed to handle specific tasks that can be reused across different scenarios.
- D: Avoids duplication of code, as common functionalities can be centralized within specific playbooks, rather than having the same code replicated across multiple playbooks.

This approach has several benefits, such as:

- Reducing large complex playbooks which become difficult to maintain. Smaller playbooks are easier to read, debug, and update¹.
- Encouraging code reuse in a more compartmentalized form. Smaller playbooks can be used as building blocks for multiple scenarios, reducing the need to write duplicate code¹².
- Improving performance and scalability. Smaller playbooks can run faster and consume less resources than larger playbooks².

The other options are not valid reasons for creating smaller and more focused playbooks. Reducing the amount of playbook data stored in each repo is not a significant benefit, as the playbook data is not very large compared to other types of data in Splunk SOAR. Avoiding duplication of code across multiple playbooks is a consequence of code reuse, not a separate goal.

NEW QUESTION 19

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

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

Answer: A

Explanation:

Within Splunk SOAR, containers (which represent incidents, cases, or events) have a lifecycle that is tracked through their status. The default statuses available without any customization are "New", "In Progress", and "Closed". These statuses help in organizing and managing the incident response process, allowing users to easily track the progress of investigations and responses from initial detection through to resolution.

NEW QUESTION 22

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 25

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 29

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 33

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

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

Answer: B

Explanation:

In Splunk SOAR, the Investigation page is where users can delve into the details of containers, artifacts, and actions. It provides a comprehensive view of the incident or event under investigation, including the JSON data associated with containers. This JSON data represents the structured information about the container, including its attributes, artifacts, and actions taken within the playbook. Options A, C, and D do not typically provide a direct view of the container's JSON data, making option B the correct answer for where a user can view this information within SOAR.

A container is the top-level data structure that SOAR playbook APIs operate on. Every container is a structured JSON object which can nest more arbitrary JSON objects, that represent artifacts. A container is the top-level object against which automation is run. To view the JSON data for a container, you need to navigate to the Investigation page, which shows the details of a container, such as its name, label, owner, status, severity, and artifacts. On the Investigation page, you can click on the JSON tab, which displays the JSON representation of the container and its artifacts. Therefore, option B is the correct answer, as it states where in SOAR a user can view the JSON data for a container. Option A is incorrect, because the analyst queue is not where a user can view the JSON data for a container, but rather where a user can view the list of containers assigned to them or their team. Option C is incorrect, because the data ingestion display is not where a user can view the JSON data for a container, but rather where a user can view the status and configuration of the data sources that ingest data into SOAR. Option D is incorrect, because the audit log is not where a user can view the JSON data for a container, but rather where a user can view the history of actions performed on the SOAR system, such as creating, updating, or deleting objects.

1: Understanding containers in Splunk SOAR (Cloud)

NEW QUESTION 37

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 42

What users are included in a new installation of SOAR?

- A. The admin and automation users are included by default.
- B. The admin, power, and user users are included by default.
- C. Only the admin user is included by default.
- D. No users are included by default.

Answer: A

Explanation:

The admin and automation users are included by default. Comprehensive Explanation and References of Correct Answer:: According to the Splunk SOAR (On-premises) default credentials, script options, and sample configuration files documentation¹, the default credentials on a new installation of Splunk SOAR (On-premises) are:

Web Interface Username: `soar_local_admin` password: `password`

On Splunk SOAR (On-premises) deployments which have been upgraded from earlier releases the user account admin becomes a normal user account with the Administrator role.

The automation user is a special user account that is used by Splunk SOAR (On-premises) to run actions and playbooks. It has the Automation role, which grants it full access to all objects and data in Splunk SOAR (On-premises).

The other options are incorrect because they either omit the automation user or include users that are not created by default. For example, option B includes the power and user users, which are not part of the default installation. Option C only includes the admin user, which ignores the automation user. Option D claims that no users are included by default, which is false.

In a new installation of Splunk SOAR, two default user accounts are typically created: admin and automation. The admin account is intended for system administration tasks, providing full access to all features and settings within the SOAR platform. The automation user is a special account used for automated processes and scripts that interact with the SOAR platform, often without requiring direct human intervention. This user has specific permissions that can be tailored for automated tasks. Options B, C, and D do not accurately represent the default user accounts included in a new SOAR installation, making option A the correct answer.

NEW QUESTION 45

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 46

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

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

Answer: C

Explanation:

The correct answer is C because creating artifacts using one playbook and collecting those artifacts in another playbook is a best practice for data sharing across playbooks. Artifacts are data objects that are associated with a container and can be used to store information such as IP addresses, URLs, file hashes, etc. Artifacts can be created using the add artifact action in any playbook block and can be collected using the get artifacts action in the filter block. Artifacts can also be used to trigger active playbooks based on their label or type. See Splunk SOAR Documentation for more details.

In the context of Splunk SOAR, one of the best practices for data sharing across playbooks is to create artifacts in one playbook and use another playbook to collect and utilize those artifacts. Artifacts in Splunk SOAR are structured data related to security incidents (containers) that playbooks can act upon. By creating artifacts in one playbook, you can effectively pass data and context to subsequent playbooks, allowing for modular, reusable, and interconnected playbook designs. This approach promotes efficiency, reduces redundancy, and enhances the playbook's ability to handle complex workflows.

NEW QUESTION 49

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 50

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

- A. `https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_isnull=false`
- B. `https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_contains=""`
- C. `https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_isnull=False`
- D. `https://<PHANTOM_URL>/rest/artifact?_filter_shal_isnull=False`

Answer: C

Explanation:

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

NEW QUESTION 51

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

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

Answer: C

Explanation:

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

1: Add custom code to your Splunk SOAR (Cloud) playbook with the custom function block using the classic playbook editor

NEW QUESTION 53

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 56

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 60

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 61

A user wants to use their Splunk Cloud instance as the external Splunk instance for Phantom. What ports need to be opened on the Splunk Cloud instance to facilitate this? Assume default ports are in use.

- A. TCP 8088 and TCP 8099.
- B. TCP 80 and TCP 443.
- C. Splunk Cloud is not supported.
- D. TCP 8080 and TCP 8191.

Answer: B

Explanation:

To integrate Splunk Phantom with a Splunk Cloud instance, network communication over certain ports is necessary. The default ports for web traffic are TCP 80 for HTTP and TCP 443 for HTTPS. Since Splunk Cloud instances are accessed over the internet, ensuring that these ports are open is essential for Phantom to communicate with Splunk Cloud for various operations, such as running searches, sending data, and receiving results. It is important to note that TCP 8088 is typically used by Splunk's HTTP Event Collector (HEC), which may also be relevant depending on the integration specifics.

NEW QUESTION 65

Which of the following supported approaches enables Phantom to run on a Windows server?

- A. Install the Phantom RPM in a GNU Cygwin implementation.
- B. Run the Phantom OVA as a cloud instance.
- C. Install the Phantom RPM file in Windows Subsystem for Linux (WSL).
- D. Run the Phantom OVA as a virtual machine.

Answer: D

Explanation:

Splunk SOAR (formerly Phantom) does not natively run on Windows servers as it is primarily designed for Linux environments. However, it can be deployed on a Windows server through virtualization. By running the Phantom OVA (Open Virtualization Appliance) as a virtual machine, users can utilize virtualization platforms like VMware or VirtualBox on a Windows server to host the Phantom environment. This approach allows for the deployment of Phantom in a Windows-centric infrastructure by leveraging virtualization technology to encapsulate the Phantom application within a supported Linux environment provided by the OVA.

NEW QUESTION 68

Which of the following are the default ports that must be configured on Splunk to allow connections from SOAR?

- A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
- B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)
- C. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)

D. SplunkWeb (8469), SplunkD (8702), HTTP Collector (8864)

Answer: C

Explanation:

For Splunk SOAR to connect with Splunk Enterprise, certain default ports must be configured to facilitate communication between the two platforms. Typically, SplunkWeb, which serves the Splunk Enterprise web interface, uses port 8000. SplunkD, the Splunk daemon that handles most of the back-end services, listens on port 8089. The HTTP Event Collector (HEC), which allows HTTP clients to send data to Splunk, typically uses port 8088. These ports are essential for the integration, allowing SOAR to send data to Splunk for indexing, searching, and visualization. Options A, B, and D list incorrect port configurations for this purpose, making option C the correct answer based on standard Splunk configurations.

These are the default ports used by Splunk SOAR (On-premises) to communicate with the embedded Splunk Enterprise instance. SplunkWeb is the web interface for Splunk Enterprise, SplunkD is the management port for Splunk Enterprise, and HTTP Collector is the port for receiving data from HTTP Event Collector (HEC). The other options are either incorrect or not default ports. For example, option B has the SplunkWeb and SplunkD ports reversed, and option D has arbitrary port numbers that are not used by Splunk by default.

NEW QUESTION 70

In a playbook, more than one Action block can be active at one time. What is this called?

- A. Serial Processing
- B. Parallel Processing
- C. Multithreaded Processing
- D. Juggle Processing

Answer: B

Explanation:

In Splunk SOAR, when a playbook is designed such that more than one Action block is active at the same time, it is referred to as 'Parallel Processing'. This allows for multiple actions to be executed concurrently, which can significantly speed up the execution of a playbook as it does not have to wait for one action to complete before starting another. Parallel processing enables more efficient use of resources and time, particularly in complex playbooks that perform numerous actions.

NEW QUESTION 73

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-2003 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SPLK-2003-dumps.html>