Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin

NEW QUESTION 1
How can the debug log for a playbook execution be viewed?

A. On the Investigation page, select Debug Log from the playbook's action menu in the Recent Activity panel.
B. Click Expand Scope m the debug window.
C. In Administration > System Health > Playbook Run History, select the playbook execution entry, then select Log.
D. Open the playbook in the Visual Playbook Editor, and select Debug Logs in Settings.

Answer: A

Explanation:
Debug logs are essential for troubleshooting and understanding the execution flow of a playbook in Splunk Phantom. The debug log for a playbook execution can be viewed by navigating to the Investigation page of a specific event or container. Within the Recent Activity panel, there is an action menu associated with each playbook run. Selecting "Debug Log" from this menu will display the detailed execution log, showing each action taken, the results of those actions, and any errors or messages generated during the playbook run.

NEW QUESTION 2
How can a child playbook access the parent playbook's action results?

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

Answer: C

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

NEW QUESTION 3
Why does SOAR use wildcards within artifact data paths?

A. To make playbooks more specific.
B. To make playbooks filter out nulls.
C. To make data access in playbooks easier.
D. To make decision execution in playbooks run faster.

Answer: C

Explanation:
Wildcards are used within artifact data paths in Splunk SOAR playbooks to simplify the process of accessing data. They allow playbooks to reference dynamic or variable data structures without needing to specify exact paths, which can vary between artifacts. This flexibility makes it easier to write playbooks that work across different events and scenarios, without hard-coding data paths.
SOAR uses wildcards within artifact data paths to make data access in playbooks easier. A data path is a way of specifying the location of a piece of data within an artifact. For example, artifact.cef.sourceAddress is a data path that refers to the source address field of the artifact. A wildcard is a special character that can match any value or subfield within a data path. For example, artifact.*.cef.sourceAddress is a data path that uses a wildcard to match any field name before the cef subfield. This allows the playbook to access the source address data regardless of the field name, which can vary depending on the app or source that generated the artifact. Therefore, option C is the correct answer, as it explains why SOAR uses wildcards within artifact data paths. Option A is incorrect, because wildcards do not make playbooks more specific, but more flexible and adaptable. Option B is incorrect, because wildcards do not make playbooks filter out nulls, but match any value or subfield. Option D is incorrect, because wildcards do not make decision execution in playbooks run faster, but make data access in playbooks easier.
1: Understanding datapaths in Administer Splunk SOAR (Cloud)

NEW QUESTION 4
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 5
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 6
Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

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

Answer: D

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

NEW QUESTION 7
When working with complex data paths, which operator is used to access a sub-element inside another element?

A. !(pipe)
B. *(asterisk)
C. :(colon)
D. .(dot)

Answer: D

Explanation:
When working with complex data paths in Splunk SOAR, particularly within playbooks, the dot (.) operator is used to access sub-elements within a larger data structure. This operator allows for the navigation through nested data, such as dictionaries or objects within JSON responses, enabling playbook actions and decision blocks to reference specific pieces of data within the artifacts or action results. This capability is crucial for extracting and manipulating relevant information from complex data sets during incident analysis and response automation.

NEW QUESTION 8
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 9
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 10
Configuring Phantom search to use an external Splunk server provides which of the following benefits?

A. The ability to run more complex reports on Phantom activities.
B. The ability to ingest Splunk notable events into Phantom.
C. The ability to automate Splunk searches within Phantom.
D. The ability to display results as Splunk dashboards within Phantom.

Answer: C

Explanation:
The correct answer is C because configuring Phantom search to use an external Splunk server allows you to automate Splunk searches within Phantom using the run query action. This action can be used to run any Splunk search command on the external Splunk server and return the results to Phantom. You can also use the format results action to parse the results and use them in other blocks. See Splunk SOAR Documentation for more details.
Configuring Phantom (now known as Splunk SOAR) to use an external Splunk server enhances the automation capabilities within Phantom by allowing the execution of Splunk searches as part of the automation and orchestration processes. This integration facilitates the automation of tasks that involve querying data from Splunk, thereby streamlining security operations and incident response workflows. Splunk SOAR's ability to integrate with over 300 third-party tools, including Splunk, supports a wide range of automatable actions, thus enabling a more efficient and effective security operations center (SOC) by reducing the time to respond to threats and by making repetitive tasks more manageable
https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation- features.html

NEW QUESTION 10
What is the main purpose of using a customized workbook?

A. Workbooks automatically implement a customized processing of events using Python code.
B. Workbooks guide user activity and coordination during event analysis and case operations.
C. Workbooks apply service level agreements (SLAs) to containers and monitor completion status on the ROI dashboard.
D. Workbooks may not be customized; only default workbooks are permitted within Phantom.

Answer: B

Explanation:
The main purpose of using a customized workbook is to guide user activity and coordination during event analysis and case operations. Workbooks can be customized to include different phases, tasks, and instructions for the users. The other options are not valid purposes of using a customized workbook. See Workbooks for more information.
Customized workbooks in Splunk SOAR are designed to guide users through the process of analyzing events and managing cases. They provide a structured framework for documenting investigations, tracking progress, and ensuring that all necessary steps are followed during incident response and case management. This helps in coordinating team efforts, maintaining consistency in response activities, and ensuring that all aspects of an incident are thoroughly investigated and resolved. Workbooks can be customized to fit the specific processes and procedures of an organization, making them a versatile tool for managing security operations.

NEW QUESTION 13
A filter block with only one condition configured which states: artifact.*.cef .sourceAddress !- , would permit which of the following data to pass forward to the next block?

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

Answer: B

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

NEW QUESTION 17
Which is the primary system requirement that should be increased with heavy usage of the file vault?

A. Amount of memory.
B. Number of processors.
C. Amount of storage.
D. Bandwidth of network.

Answer: C

Explanation:
The primary system requirement that should be increased with heavy usage of the file vault is the amount of storage. The file vault is a secure repository for

storing files on Phantom. The more files are stored, the more storage space is needed. The other options are not directly related to the file vault usage. See [File vault] for more information. Heavy usage of the file vault in Splunk SOAR necessitates an increase in the amount of storage available. The file vault is used to securely store files associated with cases, such as malware samples, logs, and other artifacts relevant to an investigation. As the volume of files and the size of stored data grow, ensuring sufficient storage capacity becomes critical to maintain performance and ensure that all necessary data is retained for analysis and evidence.

NEW QUESTION 21
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 26
When the Splunk App for SOAR Export executes a Splunk search, which activities are completed?

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

Answer: B

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

NEW QUESTION 27
After a playbook has run, where are the results stored?

A. Splunk Index
B. Case
C. Container
D. Log file

Answer: C

Explanation:
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a data object in Phantom, but can be a data source for Phantom. Reference: Splunk SOAR User Guide, page 19. In Splunk Phantom, after a playbook has been executed, the results of the actions within that playbook are stored in the container associated with the event. A container is a data structure that encapsulates all relevant information and data for an incident or event within Phantom, including action results, artifacts, notes, and more. The container allows users to see a consolidated view of all the data and activity related to a particular event. These results are not stored in the Splunk Index, a separate case, or a log file as their primary storage but may be sent to a Splunk index for further analysis.

NEW QUESTION 28
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 33
Which Phantom VPE Nock S used to add information to custom lists?

A. Action blocks
B. Filter blocks
C. API blocks
D. Decision blocks

Answer: C

Explanation:
Filter blocks are used to add information to custom lists in Phantom VPE. Filter blocks allow the user to specify a list name and a filter expression to select the data to be added to the list. Action blocks are used to execute app actions, API blocks are used to make REST API calls, and decision blocks are used to evaluate conditions and branch the playbook execution. In the Phantom Visual Playbook Editor (VPE), an API block is used to interact with various external APIs, including custom lists within Phantom. Custom lists are key-value stores that can be used to maintain state, aggregate data, or track information across multiple playbook runs. API blocks allow the playbook to make GET, POST, PUT, and DELETE requests to these lists, facilitating the addition, retrieval, update, or removal of information. This makes API blocks a versatile tool in managing custom list data within playbooks.

NEW QUESTION 35
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 36
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 41

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.

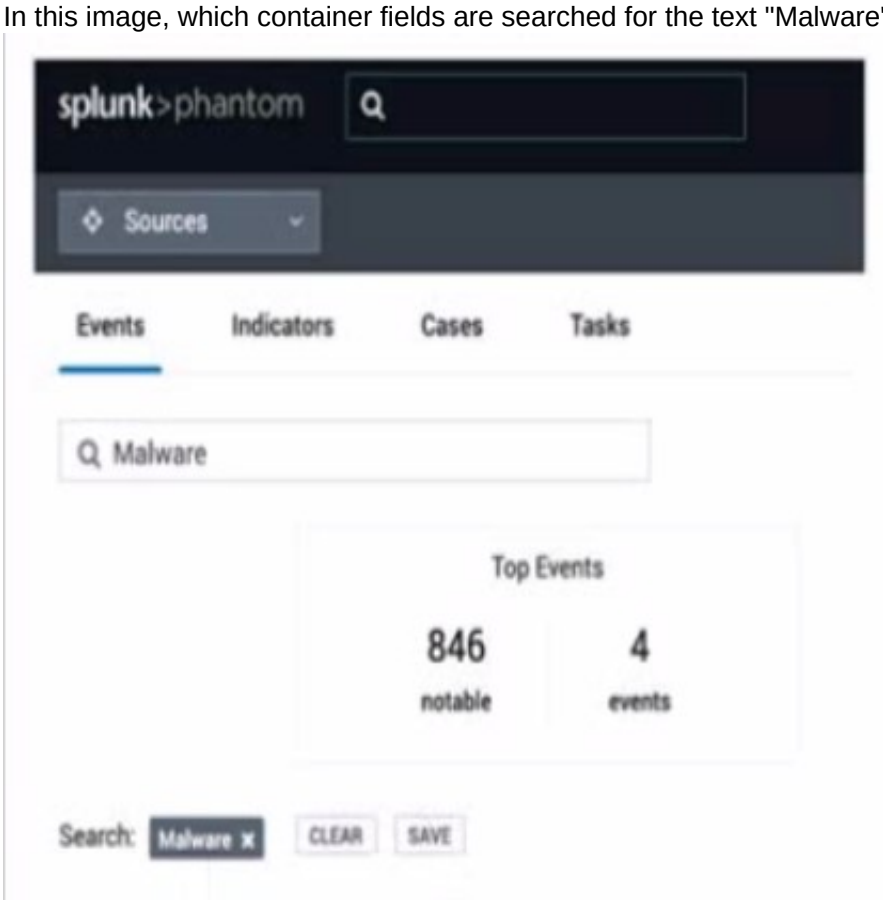
NEW QUESTION 43
Which of the following can be edited or deleted in the Investigation page?

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 47
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 50
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 55
Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

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

Answer: C

Explanation:
The correct answer is C because the best way to restrict the execution of playbooks to members of the admin role is to make sure the Execute Playbook capability is removed from all roles except admin. The Execute Playbook capability is a permission that allows a user to run any playbook on any container. By default, all roles have this capability, but it can be removed or added in the Phantom UI by going to Administration > User Management > Roles. Removing this capability from all roles except admin will ensure that only admin users can execute playbooks. See Splunk SOAR Documentation for more details. To ensure that only members of the admin role can execute specific playbooks on the Phantom server, the most effective approach is to manage role-based access controls (RBAC) directly. By configuring the system to remove the "Execute Playbook" capability from all roles except for the admin role, you can enforce this rule. This method leverages Phantom's built-in RBAC mechanisms to restrict playbook execution privileges. It is a straightforward and secure way to ensure that only users with the necessary administrative privileges can initiate the execution of sensitive or critical playbooks, thus maintaining operational security and control.

NEW QUESTION 60
Within the 12A2 design methodology, which of the following most accurately describes the last step?

A. List of the apps used by the playbook.
B. List of the actions of the playbook design.
C. List of the outputs of the playbook design.
D. List of the data needed to run the playbook.

Answer: C

Explanation:
The correct answer is C because the last step of the 12A2 design methodology is to list the outputs of the playbook design. The outputs are the expected results or outcomes of the playbook execution, such as sending an email, creating a ticket, blocking an IP, etc. The outputs should be aligned with the objectives and goals of the playbook. See Splunk SOAR Certified Automation Developer for more details.
The 12A2 design methodology in the context of Splunk SOAR (formerly Phantom) refers to a structured approach to developing playbooks. The last step in this methodology focuses on defining the outputs of the playbook design. This step is crucial as it outlines what the expected results or actions the playbook should achieve upon its completion. These outputs can vary widely, from sending notifications, creating tickets, updating statuses, to generating reports. Defining the outputs is essential for understanding the playbook's impact on the security operation workflows and how it contributes to resolving security incidents or automating tasks.

NEW QUESTION 62
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 66
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 68
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 69
When analyzing events, a working on a case, significant items can be marked as evidence. Where can ail 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 70
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 72
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 76
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

SPLK-2003 Practice Exam Features:

* SPLK-2003 Questions and Answers Updated Frequently

* SPLK-2003 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-2003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-2003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year