Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin

NEW QUESTION 1
What is enabled if the Logging option for a playbook's settings is enabled?

A. More detailed logging information Is available m 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 2
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 3
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 4
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 5
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 6
How is it possible to evaluate user prompt results?

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

Answer: C

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

NEW QUESTION 7
A user selects the New option under Sources on the menu. What will be displayed?

A. A list of new assets.
B. The New Data Ingestion wizard.
C. A list of new data sources.
D. A list of new events.

Answer: B

Explanation:
Selecting the New option under Sources in the Splunk SOAR menu typically initiates the New Data Ingestion wizard. This wizard guides users through the process of configuring new data sources for ingestion into the SOAR platform. It is designed to streamline the setup of various data inputs, such as event logs, threat intelligence feeds, or notifications from other security tools, ensuring that SOAR can receive and process relevant security data efficiently. This feature is crucial for expanding SOAR's monitoring and response capabilities by integrating diverse data sources. Options A, C, and D do not accurately describe what is displayed when the New option under Sources is selected, making option B the correct choice.
New Data Ingestion wizard allows you to create a new data source for Splunk SOAR (On- premises) by selecting the type of data, the ingestion method, and the configuration options. The other options are incorrect because they do not match the description of the New option under Sources on the menu. For example, option A refers to a list of new assets, which is not related to data ingestion. Option C refers to a list of new data sources, which is not what the New option does. Option D refers to a list of new events, which is not the same as creating a new data source.

NEW QUESTION 8
Which of the following describes the use of labels m Phantom?

A. Labels determine the service level agreement (SLA) for a container.
B. Labels control the default seventy, 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 9
What is the main purpose of using a customized workbook?

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

Answer: B

Explanation:
The main purpose of using a customized workbook is to guide user activity and coordination during event analysis and case operations. Workbooks can be customized to include different phases, tasks, and instructions for the users. The other options are not valid purposes of using a customized workbook. See Workbooks for more information.

Customized workbooks in Splunk SOAR are designed to guide users through the process of analyzing events and managing cases. They provide a structured framework for documenting investigations, tracking progress, and ensuring that all necessary steps are followed during incident response and case management. This helps in coordinating team efforts, maintaining consistency in response activities, and ensuring that all aspects of an incident are thoroughly investigated and resolved. Workbooks can be customized to fit the specific processes and procedures of an organization, making them a versatile tool for managing security operations.

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

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

Answer: B

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

NEW QUESTION 10
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 14
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 18
How can an individual asset action be manually started?

A. With the > action button in the analyst queue page.
B. By executing a playbook in the Playbooks section.
C. With the > action button in the Investigation page.
D. With the > asset button in the asset configuration section.

Answer: C

Explanation:
An individual asset action can be manually started with the > action button in the Investigation page. This allows the user to select an asset and an action to perform on it. The other options are not valid ways to start an asset action manually. See Performing asset actions for more information. Individual asset actions in

Splunk SOAR can be manually initiated from the Investigation page of a container. The "> action" button on this page allows users to execute specific actions associated with assets directly, enabling on- the-fly operations on artifacts or indicators within a container. This feature is particularly useful for ad-hoc analysis and actions, allowing analysts to respond to or investigate specific aspects of an incident without the need for a full playbook.

NEW QUESTION 19
In addition to full backups. Phantom supports what other backup type using backup?

A. Snapshot
B. Incremental
C. Partial
D. Differential

Answer: B

Explanation:
Splunk Phantom supports incremental backups in addition to full backups. An incremental backup is a type of backup that only copies the data that has changed since the last backup (whether that was a full backup or another incremental backup). This method is more storage-efficient than a full backup because it does not repeatedly back up the same data, reducing the amount of storage required and speeding up the backup process. Differential backups, which record the changes since the last full backup, and partial backups, which allow the selection of specific data to back up, are not standard backup types offered by Splunk Phantom according to its documentation.

NEW QUESTION 21
Which of the following are the default ports that must be configured on Splunk to allow connections from Phantom?

A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)
C. SplunkWeb (8421), SplunkD (8061), HTTP Collector (8798)
D. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)

Answer: D

Explanation:
The correct answer is D because the default ports that must be configured on Splunk to allow connections from Phantom are SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088). SplunkWeb is the port used to access the Splunk web interface. SplunkD is the port used to communicate with the Splunk server. HTTP Collector is the port used to send data to Splunk using the HTTP Event Collector (HEC). These ports must be configured on Splunk and Phantom to enable the integration between the two products. See Splunk SOAR Documentation for more details.
To allow connections from Splunk Phantom to Splunk, certain default ports need to be open and properly configured. The default ports include SplunkWeb (8000) for web access, SplunkD (8089) for Splunk's management port, and the HTTP Event Collector (HEC) on port 8088, which is used for ingesting data into Splunk. These ports are essential for the communication between Splunk Phantom and Splunk, facilitating data exchange, search capabilities, and the integration of various functionalities between the two platforms.

NEW QUESTION 24
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 26
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 31
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 34
What is the primary objective of using the I2A2 playbook design methodology?

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

Answer: D

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

NEW QUESTION 36
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 41
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 seventy 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 45
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 49
Which of the following queries would return all artifacts that contain a SHA1 file hash?

A. https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_insull=false
B. https://<PHANTOM_URL>/rest/artifact?_filter_cef_Shal_contains=""
C. https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_insull=False
D. https://<PHANTOM_URL>/rest/artifact?_filter_shal insull=False

Answer: C

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

NEW QUESTION 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 58
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 60
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 63
What does a user need to do to have a container with an event from Splunk use context- aware actions designed for notable events?

A. Include the notable event's event_id field and set the artifacts label to aplunk notable event id.
B. Rename the event_id field from the notable event to splunkNotableEventId.
C. Include the event_id field in the search results and add a CEF definition to Phantom for event_id, datatype splunk notable event id.
D. Add a custom field to the container named event_id and set the custom field's data type to splunk notable event id.

Answer: C

Explanation:
For a container in Splunk SOAR to utilize context-aware actions designed for notable events from Splunk, it is crucial to ensure that the notable event's unique identifier (event_id) is included in the search results pulled into SOAR. Moreover, by adding a Common Event Format (CEF) definition for the event_id field within Phantom, and setting its data type to something that denotes it as a Splunk notable event ID, SOAR can recognize and appropriately handle these identifiers. This setup facilitates the correct mapping and processing of notable event data within SOAR, enabling the execution of context-aware actions that are specifically tailored to the characteristics of Splunk notable events.

NEW QUESTION 64
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 66
.....

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