Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin

NEW QUESTION 1
What is the default log level for system health debug logs?

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

Answer: A

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

NEW QUESTION 2
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 3
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 4
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 5
Which two playbook blocks can discern which path in the playbook to take next?

A. Prompt and decision blocks.
B. Decision and action blocks.

C. Filter and decision blocks.
D. Filter and prompt blocks.

Answer: C

Explanation:
In Splunk SOAR playbooks, filter and decision blocks are used to discern which path in the playbook to take next. Filter blocks evaluate data against specified criteria and direct the flow based on whether the data matches the filter. Decision blocks use logical conditions to determine the path that the playbook execution should follow. Together, they enable the playbook to dynamically respond to different situations and data inputs.

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 of the following are the steps required to complete a full backup of a Splunk Phantom deployment' Assume the commands are executed from /opt/phantom/bin and that no other backups have been made.

A. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup.pyc --backup.
B. On the command line enter: sudo phenv python ibackup.pyc --backup —backup-type full, then sudo phenv python ibackup.pyc --setup.
C. Within the UI: Select from the main menu Administration > System Health > Backup.
D. Within the UI: Select from the main menu Administration > Product Settings > Backup.

Answer: B

Explanation:
The correct answer is B because the steps required to complete a full backup of a Splunk Phantom deployment are to first run the --backup --backup-type full command and then run the --setup command. The --backup command creates a backup file in the /opt/phantom/backup directory. The --backup-type full option specifies that the backup file includes all the data and configuration files of the Phantom server.
The --setup command creates a configuration file that contains the encryption key and other information needed to restore the backup file. See Splunk SOAR Certified Automation Developer Track for more details.
Performing a full backup of a Splunk Phantom deployment involves using the command-line interface, primarily because Phantom's architecture and data management processes are designed to be managed at the server level for comprehensive backup and recovery. The correct sequence involves initiating a full backup first using the --backup --backup- type full option to ensure all configurations, data, and necessary components are included in the backup. Following the completion of the backup, the --setup option might be used to configure or verify the backup settings, although typically, the setup would precede backup operations in practical scenarios. This process ensures that all aspects of the Phantom deployment are preserved, including configurations, playbooks, cases, and other data, which is crucial for disaster recovery and system migration.

NEW QUESTION 8
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 9
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 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 10
How is it possible to evaluate user prompt results?

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

Answer: C

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

NEW QUESTION 12
A user has written a playbook that calls three other playbooks, one after the other. The user notices that the second playbook starts executing before the first one completes. What is the cause of this behavior?

A. Incorrect Join configuration on the second playbook.
B. The first playbook is performing poorly.
C. The steep option for the second playbook is not set to a long enough interval.
D. Synchronous execution has not been configured.

Answer: D

Explanation:
The correct answer is D because synchronous execution has not been configured. Synchronous execution is a feature that allows you to control the order of execution of playbook blocks. By default, Phantom executes playbook blocks asynchronously, meaning that it does not wait for one block to finish before starting the next one. This can cause problems when you have dependencies between blocks or when you call other playbooks. To enable synchronous execution, you need to use the sync action in the run playbook block and specify the name of the next block to run after the called playbook completes. See Splunk SOAR Documentation for more details. In Splunk SOAR, playbooks can be executed either synchronously or asynchronously. Synchronous execution ensures that a playbook waits for a called playbook to complete before proceeding to the next step. If the second playbook starts executing before the first one completes, it indicates that synchronous execution was not configured for the playbooks. Without synchronous execution, playbooks will execute independently of each other's completion status, leading to potential overlaps in execution. This behavior can be controlled by properly configuring the playbook execution settings to ensure that dependent playbooks complete their tasks in the desired order.

NEW QUESTION 15
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 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 20
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 21
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

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

Answer: B

Explanation:
A step when configuring event forwarding from Splunk to Phantom is to create a Splunk alert that uses the event_forward.py script to send events to Phantom. This script will convert the Splunk events to CEF format and send them to Phantom as containers. The other options are not valid steps for event forwarding. See Forwarding events from Splunk to Phantom for more details.
Configuring event forwarding from Splunk to Phantom typically involves creating a Splunk alert that leverages a script (like event_forward.py) to automatically send triggered event data to Phantom. This setup enables Splunk to act as a detection mechanism that, upon identifying notable events based on predefined criteria, forwards these events to Phantom for further orchestration, automation, and response actions. This integration streamlines the process of incident management by connecting Splunk's powerful data analysis capabilities with Phantom's orchestration and automation framework.

NEW QUESTION 26
What is the simplest way to pass data between playbooks?

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

Answer: A

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

NEW QUESTION 31
During a second test of a playbook, a user receives an error that states: 'an empty parameters list was passed to phantom.act()." What does this indicate?

A. The container has artifacts not parameters.
B. The playbook is using an incorrect container.
C. The playbook debugger's scope is set to new.
D. The playbook debugger's scope is set to all.

Answer: A

Explanation:
The error message "an empty parameters list was passed to phantom.act()" typically indicates that the action being called by the playbook does not have the required parameters to execute. This can happen if the playbook expects certain data to be present in the container's artifacts but finds none. Artifacts in Splunk SOAR (Phantom) are data elements associated with a container (such as an event or alert) that playbooks can act upon. If a playbook action is designed to use data from artifacts as parameters and those artifacts are missing or do not contain the expected data, the playbook cannot execute the action properly, leading to this error.

NEW QUESTION 33
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 37
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 40
When assigning an input parameter to an action while building a playbook, a user notices the artifact value they are looking for does not appear in the auto-populated list.
How is it possible to enter the unlisted artifact value?

A. Type the CEF datapath in manually.
B. Delete and recreate the artifact.
C. Edit the artifact to enable the List as Parameter option for the CEF value.
D. Edit the container to allow CEF parameters.

Answer: A

Explanation:
When building a playbook in Splunk SOAR, if the desired artifact value does not appear in the auto-populated list of input parameters for an action, users have the option to manually enter the Common Event Format (CEF) datapath for that value. This allows for greater flexibility and customization in playbook design, ensuring that specific data points can be targeted even if they're not immediately visible in the interface. This manual entry of CEF datapaths allows users to directly reference the necessary data within artifacts, bypassing limitations of the auto-populated list. Options B, C, and D suggest alternative methods that are not typically used for this purpose, making option A the correct and most direct approach to entering an unlisted artifact value in a playbook action.
When assigning an input parameter to an action while building a playbook, a user can use the auto-populated list of artifact values that match the expected data type for the parameter. The auto-populated list is based on the contains parameter of the action inputs and outputs, which enables contextual actions in the SOAR user interface. However, the auto-populated list may not include all the possible artifact values that can be used as parameters, especially if the artifact values are nested or have uncommon data types. In that case, the user can type the CEF datapath in manually, using the syntax artifact.<field>.<key>, where field is the name of the artifact field, such as cef, and key is the name of the subfield within the artifact field, such as sourceAddress. Typing the CEF datapath in manually allows the user to enter the unlisted artifact value as an input parameter to the action. Therefore, option A is the correct answer, as it states how it is possible to enter the unlisted artifact value. Option B is incorrect, because deleting and recreating the artifact is not a way to enter the unlisted artifact value, but rather a way to lose the existing artifact data. Option C is incorrect, because editing the artifact to enable the List as Parameter option for the CEF value is not a way to enter the unlisted artifact value, but rather a way to make the artifact value appear in the auto-populated list. Option D is incorrect, because editing the container to allow CEF parameters is not a way to enter the unlisted artifact value, but rather a way to modify the container properties, which are not related to the action parameters.
1: Web search results from search_web(query="Splunk SOAR Automation Developer input parameter to an action")

NEW QUESTION 41
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 44
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 49
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 50
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 53
A user wants to get the playbook results for a single artifact. Which steps will accomplish the?

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

Answer: A

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

NEW QUESTION 54
After enabling multi-tenancy, which of the Mowing is the first configuration step?

A. Select the associated tenant artifacts.
B. Change the tenant permissions.
C. Set default tenant base address.
D. Configure the default tenant.

Answer: D

Explanation:
Upon enabling multi-tenancy in Splunk SOAR, the first step in configuration typically involves setting up the default tenant. This foundational step is critical as it establishes the primary operating environment under which subsequent tenants can be created and managed. The default tenant serves as the template for permissions, settings, and configurations that might be inherited or customized by additional tenants. Proper configuration of the default tenant ensures a stable and consistent framework for multi- tenancy operations, allowing for segregated environments within the same SOAR instance, each tailored to specific operational needs or organizational units.

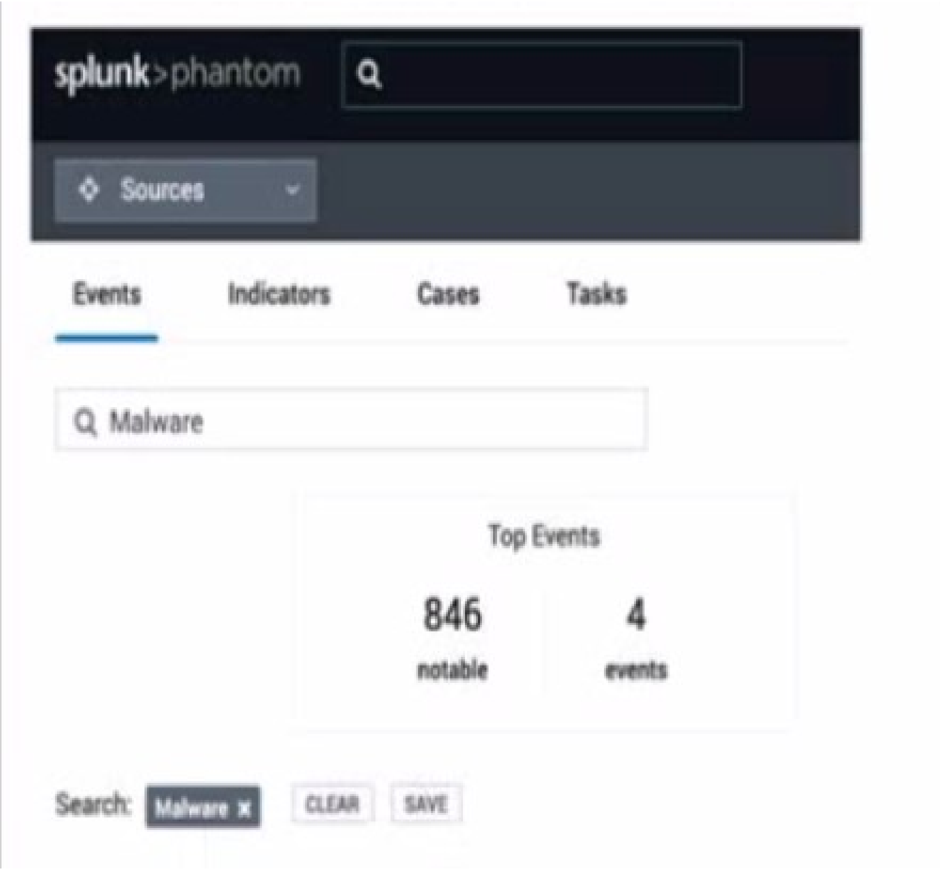
NEW QUESTION 57
Which of the following applies to filter blocks?

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 59
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 60
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 62
Which of the following can be done with the System Health Display?

A. Create a temporary, edited version of a process and test the results.
B. Partially rewind processes, which is useful for debugging.
C. View a single column of status for SOAR processe
D. For metrics, click Details.
E. Reset DECIDED to reset playbook environments back to at-start conditions.

Answer: C

Explanation:
System Health Display is a dashboard that shows the status and performance of the SOAR processes and components, such as the automation service, the playbook daemon, the DECIDED process, and the REST API. One of the things that can be done with the System Health Display is to reset DECIDED, which is a core component of the SOAR automation engine that handles the execution of playbooks and actions. Resetting DECIDED can be useful for troubleshooting or debugging purposes, as it resets the playbook environments back to at-start conditions, meaning that any changes made by the playbooks are discarded and the playbooks are reloaded. To reset DECIDED, you need to click on the Reset DECIDED button on the System Health Display dashboard. Therefore, option D is the correct answer, as it is the only option that can be done with the System Health Display. Option A is incorrect, because creating a temporary, edited version of a process and testing the results is not something that can be done with the System Health Display, but rather with the Debugging dashboard, which allows you to modify and run a process in a sandbox environment. Option B is incorrect, because partially rewinding processes, which is useful for debugging, is not something that can be done with the System Health Display, but rather with the Rewind feature, which allows you to go back to a previous state of a process and resume the execution from there. Option C is incorrect, because viewing a single column of status for SOAR processes is not something that can be done with the System

Health Display, but rather with the Status Display dashboard, which shows a simplified view of the SOAR processes and their status.
1: Web search results from search_web(query="Splunk SOAR Automation Developer System Health Display")

NEW QUESTION 64
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 do assets provide for app functionality?

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

Answer: A

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

NEW QUESTION 72
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 77
When configuring a Splunk asset for Phantom to connect to a SplunkC loud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible

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

Answer: D

Explanation:
In scenarios where there's a need to run different on_poll searches for a Splunk Cloud instance from Splunk SOAR, configuring a second Splunk asset for the additional query is a practical solution. Splunk SOAR's architecture allows for multiple assets of the same type to be configured with distinct settings. By setting up

a second Splunk asset specifically for the second on_poll search query, users can maintain separate configurations and ensure that each query is executed in its intended context without interference. This approach provides flexibility in managing different data collection or monitoring needs within the same SOAR environment.

NEW QUESTION 82
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 85
What are indicators?

A. Action result items that determine the flow of execution in a playbook.
B. Action results that may appear in multiple containers.
C. Artifact values that can appear in multiple containers.
D. Artifact values with special security significance.

Answer: D

Explanation:
Indicators within the context of Splunk SOAR refer to artifact values that have special security significance. These are typically derived from the data within artifacts and are identified as having particular importance in the analysis and investigation of security incidents. Indicators might include items such as IP addresses, domain names, file hashes, or other data points that can be used to detect, correlate, and respond to security threats. Recognizing and managing indicators effectively is key to leveraging SOAR for enhanced threat intelligence, incident response, and security operations efficiency.

NEW QUESTION 86
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 87
Which of the following can be configured in the ROI Settings?

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

Answer: C

Explanation:
ROI Settings dashboard allows you to configure the parameters used to estimate the data displayed in the Automation ROI Summary dashboard. One of the settings that can be configured is the FTE Gained, which is the number of full time employees (FTEs) that are freed up by automation. To calculate this value, Splunk SOAR divides the number of actions run by automation by the number of expected actions an analyst would take, based on minutes per action and analyst hours per day. Therefore, option A is the correct answer, as it is one of the settings that can be configured in the ROI Settings dashboard. Option B is incorrect, because time lost is not a setting that can be configured in the ROI Settings dashboard, but a metric that is calculated by Splunk SOAR based on the difference between the analyst minutes per action and the actual minutes per action. Option C is incorrect, because analyst hours per month is not a setting that can be configured in the ROI Settings dashboard, but a value that is derived from the analyst hours per day setting. Option D is incorrect, because annual analyst salary is a setting that can be configured in the ROI Settings dashboard, but not the one that is asked in the question.
1: Configure the ROI Settings dashboard in Administer Splunk SOAR (On-premises)
ROI (Return on Investment) Settings within Splunk SOAR are used to estimate the efficiency and financial impact of the SOAR platform. One of the configurable parameters in these settings is the 'Analyst hours per month'. This parameter helps in calculating the time saved through automation, which in turn can be translated into cost savings and efficiency gains. It reflects the direct contribution of the SOAR platform to operational productivity.

NEW QUESTION 88
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 90
......

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

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-2003 Practice Test Here