Splunk.SPLK-2003.v2024-05-20.q77

Exam Code:	SPLK-2003
Exam Name:	Splunk Phantom Certified Admin
Certification Provider:	Splunk
Free Question Number:	77
Version:	v2024-05-20
# of views:	2015
# of Questions views:	770
https://www.freepdfdumps.com/Splunk.SPLK-2003.v2024-05-20.q77.html	

NEW QUESTION: 1
What metrics can be seen from the System Health Display? (select all that apply)
A. Playbook Usage
B. Memory Usage
C. Disk Usage
D. Load Average
Answer: B,C,D (LEAVE A REPLY)
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. Some of the metrics that can be seen from the System Health Display are:
*Memory Usage: The percentage of memory used by the system and the processes.
*Disk Usage: The percentage of disk space used by the system and the processes.
*Load Average: The average number of processes in the run queue or waiting for disk I/O over a period of time.
Therefore, options B, C, and D are the correct answers, as they are the metrics that can be seen from the System Health Display. Option A is incorrect, because Playbook Usage is not a metric that can be seen from the System Health Display, but rather a metric that can be seen from the Playbook Usage dashboard, which shows the number of playbooks and actions run over a period of time.
1: Web search results from search_web(query="Splunk SOAR Automation Developer System Health Display") The System Health Display in Splunk SOAR provides several metrics to help monitor and manage the health of the system. These typically include:
*B: Memory Usage - This metric shows the amount of memory being used by the SOAR platform, which is important for ensuring that the system does not exceed available resources.

*C: Disk Usage - This metric indicates the amount of storage space being utilized, which is crucial for maintaining adequate storage resources and for planning capacity.
*D: Load Average - This metric provides an indication of the overall load on the system over a period of time, which helps in understanding the system's performance and in identifying potential bottlenecks or issues.
Playbook Usage is generally not a metric displayed on the System Health page; instead, it's more related to the usage analytics of playbooks rather than system health metrics.

NEW QUESTION: 2
What is the default embedded search engine used by Phantom?
A. Embedded Splunk search engine.
B. Embedded Phantom search engine.
C. Embedded Elastic search engine.
D. Embedded Django search engine.
Answer: (SHOW ANSWER)
Explanation
The default embedded search engine used by Phantom is the Embedded Elastic search engine. This engine provides fast and scalable search capabilities for Phantom data. The other options are not valid search engines for Phantom. See [Search engine configuration] for more information.

NEW QUESTION: 3
When is using decision blocks most useful?
A. When modifying downstream data hi one or more paths in the playbook.
B. When processing different data in parallel.
C. When selecting one (or zero) possible paths in the playbook.
D. When evaluating complex, multi-value results or artifacts.
Answer: (SHOW ANSWER)

NEW QUESTION: 4
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 playbook debugger's scope is set to new.
B. The playbook debugger's scope is set to all.
C. The playbook is using an incorrect container.
D. The container has artifacts not parameters.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
How is it possible to evaluate user prompt results?
A. Set action_result.summary. status to required.

B. Set the user prompt to reinvoke if it times out.
C. Set action_result. summary. response to required.
D. Add a decision Mode
Answer: D (LEAVE A REPLY)
Explanation
A user can evaluate user prompt results by adding a decision block after the user prompt action block. The decision block can use the action_result.summary.response parameter to check the user's input and branch the playbook execution accordingly. Setting the action_result.summary.status or action_result.summary.response to required does not affect the evaluation of user prompt results. Setting the user prompt to reinvoke if it times out does not evaluate the user prompt results, but only repeats the prompt. Reference, page 16.

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: (SHOW ANSWER)
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.

NEW QUESTION: 7
When is using decision blocks most useful?
A. When selecting one (or zero) possible paths in the playbook.
B. When processing different data in parallel.
C. When evaluating complex, multi-value results or artifacts.
D. When modifying downstream data hi one or more paths in the playbook.
Answer: A (LEAVE A REPLY)
Explanation

Decision blocks are most useful when selecting one (or zero) possible paths in the playbook. Decision blocks allow the user to define one or more conditions based on action results, artifacts, or custom expressions, and execute the corresponding path if the condition is met. If none of the conditions are met, the playbook execution ends. Decision blocks are not used for processing different data in parallel, evaluating complex, multi-value results or artifacts, or modifying downstream data in one or more paths in the playbook. Reference, page 15.

NEW QUESTION: 8
Within the 12A2 design methodology, which of the following most accurately describes the last step?
A. List of the outputs of the playbook design.
B. List of the data needed to run the playbook.
C. List of the apps used by the playbook.
D. List of the actions of the playbook design.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 9
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 (LEAVE A REPLY)
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.

NEW QUESTION: 10
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 (LEAVE A REPLY)
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.

NEW QUESTION: 11
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 (LEAVE A REPLY)
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: 12
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 8080 and TCP 8191.
C. Splunk Cloud is not supported.
D. TCP 80 and TCP 443.

Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which app allows a user to run Splunk queries from within Phantom?
A. Splunk App for Phantom?
B. The Integrated Splunk/Phantom app.
C. Phantom App for Splunk.
D. Splunk App for Phantom Reporting.
Answer: C (LEAVE A REPLY)
Explanation
The Phantom App for Splunk allows a user to run Splunk queries from within Phantom. This app provides actions such as run query, ingest events, and save search, which enable the user to interact with Splunk from Phantom playbooks or the Phantom UI. The other apps are not relevant for this use case. The Splunk App for Phantom is used to send data from Splunk to Phantom. The Integrated Splunk/Phantom app is a deprecated app that was replaced by the Splunk App for Phantom. The Splunk App for Phantom Reporting is used to generate reports on Phantom activity from Splunk. Reference, page 1.

NEW QUESTION: 14
Which of the following accurately describes the Files tab on the Investigate page?
A. A user can upload the output from a detonate action to the the files tab for further investigation.
B. Files tab items and artifacts are the only data sources that can populate active cases.
C. Files tab items cannot be added to investigations. Instead, add them to action blocks.
D. Phantom memory requirements remain static, regardless of Files tab usage.
Answer: A (LEAVE A REPLY)
The Files tab on the Investigate page allows the user to upload, download, and view files related to an investigation. A user can upload the output from a detonate action to the Files tab for further investigation, such as analyzing the file metadata, content, or hash. Files tab items and artifacts are not the only data sources that can populate active cases, as cases can also include events, tasks, notes, and comments. Files tab items can be added to investigations by using the add file action block or the Add File button on the Files tab. Phantom memory requirements may increase depending on the Files tab usage, as files are stored in the Phantom database.
The Files tab on the Investigate page in Splunk Phantom is an area where users can manage and analyze files related to an investigation. Users can upload files, such as outputs from a 'detonate file' action which analyzes potentially malicious files in a sandbox environment. The files tab allows users to store and further investigate these outputs, which can include reports, logs, or any other file types that have been generated or are relevant to the investigation. The Files tab is an integral part of the investigation process, providing easy access to file data for analysis and correlation with other incident data.

NEW QUESTION: 15
What is the simplest way to pass data between playbooks?
A. Action results
B. File system
C. Artifacts
D. KV Store
Answer: (SHOW ANSWER)
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: 16
Which is the primary system requirement that should be increased with heavy usage of the file vault?
A. Number of processors.
B. Amount of memory.
C. Bandwidth of network.
D. Amount of storage.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 17
On a multi-tenant Phantom server, what is the default tenant's ID?
A. Default
B. 1
C. 0
D. *

Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
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 (LEAVE A REPLY)
Explanation
The correct answer is B because Phantom supports PIV/CAC as another user authentication method besides LDAP and SAML2. PIV/CAC stands for Personal Identity Verification (PIV) or Common Access Card (CAC) and is a smart card that can be used to authenticate users to Phantom. SAML3 is not a valid authentication method. Biometrics and OpenID are not supported by Phantom. See Splunk SOAR Documentation for more details.

NEW QUESTION: 19
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 (LEAVE A REPLY)
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: 20
What is the simplest way to pass data between playbooks?
A. Action results
B. Artifacts
C. KV Store
D. File system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
Which is the primary system requirement that should be increased with heavy usage of the file vault?
A. Amount of memory.
B. Number of processors.
C. Amount of storage.
D. Bandwidth of network.
Answer: C (LEAVE A REPLY)
Explanation
The primary system requirement that should be increased with heavy usage of the file vault is the amount of storage. The file vault is a secure repository for storing files on Phantom. The more files are stored, the more storage space is needed. The other options are not directly related to the file vault usage. See [File vault] for more information.

NEW QUESTION: 22
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 (LEAVE A REPLY)
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: 23
Which Phantom API command is used to create a custom list?
A. phantom.add_list()
B. phantom.create_list()
C. phantom.include_list()
D. phantom.new_list()
Answer: (SHOW ANSWER)
Explanation
The Phantom API command to create a custom list is phantom.create_list(). This command takes a list name and an optional description as parameters and returns a list ID if successful. The other commands are not valid Phantom API commands. phantom.add_list() is a Python function that can be used in custom code blocks to add data to an existing list. Reference, page 5.

NEW QUESTION: 24
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 (LEAVE A REPLY)
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: 25
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 (LEAVE A REPLY)
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: 26
Which of the following are examples of things commonly done with the Phantom REST APP
A. Use Django queries; use Docker to create a container and add artifacts to it; remove temporary lists.
B. Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists.
C. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.

D. Use Django queries; use curl to create a container and add artifacts to it; add action blocks.
Answer: (SHOW ANSWER)

NEW QUESTION: 27
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: (SHOW ANSWER)
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.

NEW QUESTION: 28
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. Synchronous execution has not been configured.
B. The first playbook is performing poorly.
C. The sleep option for the second playbook is not set to a long enough interval.
D. Incorrect join configuration on the second playbook.
Answer: A (LEAVE A REPLY)
In Splunk SOAR, playbooks can execute actions either synchronously (waiting for one action to complete before starting the next) or asynchronously (allowing actions to run concurrently). If a playbook starts executing before the previous one has completed, it indicates that synchronous execution has not been properly configured between these playbooks. This is crucial when the output of one playbook is a dependency for the subsequent playbook. Options B, C, and D do not directly address the observed behavior of concurrent playbook execution, making option A the most accurate explanation for why the second playbook starts before the completion of the first.
synchronous execution is a feature of the SOAR automation engine that allows you to control the order of execution of playbook blocks. Synchronous execution ensures that a playbook block waits for the completion of the previous block before starting its execution. Synchronous execution can be enabled or disabled for each playbook block in the playbook editor, by toggling the Synchronous Execution switch in the block settings. Therefore, option A is the correct answer, as it states the cause of the behavior where the second playbook starts executing before the first one completes. Option B is incorrect, because the first playbook performing poorly is not the cause of the behavior, but rather a

possible consequence of the behavior. Option C is incorrect, because the sleep option for the second playbook is not the cause of the behavior, but rather a workaround that can be used to delay the execution of the second playbook. Option D is incorrect, because the join configuration on the second playbook is not the cause of the behavior, but rather a way of merging multiple paths of execution into one.
1: Web search results from search_web(query="Splunk SOAR Automation Developer synchronous execution")

NEW QUESTION: 29
Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?
A. Add a tag with restricted access to the restricted playbooks.
B. Place restricted playbooks in a second source repository that has restricted access.
C. Add a filter block to al restricted playbooks that Titters for runRole - "Admin".
D. Make sure the Execute Playbook capability is removed from al roles except admin.
Answer: (SHOW ANSWER)

NEW QUESTION: 30
How can more than one user perform tasks in a workbook?
A. Any user in a role with write access to the case's workbook can be assigned to tasks.
B. Add the required users to the authorized list for the container.
C. Any user with a role that has Perform Task enabled can execute tasks for workbooks.
D. The container owner can assign any authorized user to any task in a workbook.
Answer: C (LEAVE A REPLY)
In Splunk SOAR, tasks within workbooks can be performed by any user whose role has the 'Perform Task' capability enabled. This capability is assigned within the role configuration and allows users with the appropriate permissions to execute tasks. It is not limited to users with write access or the container owner; rather, it is based on the specific permissions granted to the role with which the user is associated.

NEW QUESTION: 31
Which of the following are the default ports that must be configured on Splunk to allow connections from Phantom?
A. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)
B. SplunkWeb (8421), SplunkD (8061), HTTP Collector (8798)
C. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
D. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32
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 (LEAVE A REPLY)
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: 33
Which of the following can be configured in the ROI Settings?
A. Analyst hours per month.
B. Time lost.
C. Number of full time employees (FTEs).
D. Annual analyst salary.
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because the number of full time employees (FTEs) is one of the settings that can be configured in the Return on Investment (ROI) Settings page. This setting is used to calculate the ROI metrics based on the number of analysts in the organization. The answer A is incorrect because the analyst hours per month is not a configurable setting, but a calculated metric based on the FTEs and the average hours per month. The answer B is incorrect because the time lost is not a configurable setting, but a calculated metric based on the number of incidents and the average time lost per incident. The answer D is incorrect because the annual analyst salary is not a configurable setting, but a calculated metric based on the FTEs and the average salary per analyst. Reference: Splunk SOAR Admin Guide, page 131.

NEW QUESTION: 34

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: (SHOW ANSWER)
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.

NEW QUESTION: 35
Configuring Phantom search to use an external Splunk server provides which of the following benefits?
A. The ability to ingest Splunk notable events into Phantom.
B. The ability to automate Splunk searches within Phantom.
C. The ability to display results as Splunk dashboards within Phantom.
D. The ability to run more complex reports on Phantom activities.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
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: (SHOW ANSWER)
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.

NEW QUESTION: 37
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 (LEAVE A REPLY)
Explanation
The correct answer is A because the phantom.debug() function is used to output debug information to the debug window in the Visual Playbook Editor. This function can be useful for troubleshooting and testing playbooks. The answer B is incorrect because the phantom.exception() function is used to output exception information to the debug window in the Visual Playbook Editor. This function can be useful for handling errors and exceptions in playbooks. The answer C is incorrect because the phantom.print() function is used to output information to the standard output stream in the Phantom server. This function can be useful for logging and auditing purposes. The answer D is incorrect because the phantom.assert() function is used to check if a condition is true or false and raise an exception if it is false. This function can be useful for validating inputs and outputs in playbooks. Reference: Splunk SOAR Playbook Development Guide, page 22.

NEW QUESTION: 38
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 (LEAVE A REPLY)
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: 39
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: A (LEAVE A REPLY)
Explanation
The Logging option for a playbook's settings enables more detailed logging information to be available in the Investigation page. This can help with debugging and troubleshooting the playbook execution. The other options are not related to the Logging option. See Playbook settings for more information.

NEW QUESTION: 40
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 (LEAVE A REPLY)
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: 41
After a successful POST to a Phantom REST endpoint to create a new object what result is returned?
A. The new object name.
B. The PostGres UUID.
C. The new object ID.
D. The full CEF name.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
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: (SHOW ANSWER)
Explanation
The correct answer is A because the image shows the search interface of the Splunk SOAR product, where the user can search for events and artifacts based on various criteria. The image shows that the user has entered the text "Malware" in the search bar, which means that the search will look for events and artifacts that have the term "Malware" in their name. The answer B is incorrect because the search interface does not search for notes or comments, which are separate entities in the Splunk SOAR product. The answer C is incorrect because the search interface does not search for event ID, which is a unique identifier for each event. Reference: Splunk SOAR User Guide, page 21.

NEW QUESTION: 43
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 (LEAVE A REPLY)
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: 44
Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?
A. Playbooks
B. Notes
C. Service level agreement (SLA) expiration
D. Actions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
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: (SHOW ANSWER)
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: 46
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: (SHOW ANSWER)
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: 47
How can a child playbook access the parent playbook's action results?
A. When configuring the playbook block in the parent, add the desired results in the Scope parameter.
B. Child playbooks can access parent playbook data while the parent Is still running.
C. By setting scope to ALL when starting the child.
D. The parent can create an artifact with the data needed by the did.
Answer: (SHOW ANSWER)

NEW QUESTION: 48
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: (SHOW ANSWER)

NEW QUESTION: 49
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 (LEAVE A REPLY)
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: 50
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 (LEAVE A REPLY)
Explanation
The correct answer is D because the dot (.) operator is used to access a sub-element inside another element when working with complex datapaths. For example, if the datapath is container['artifacts'][0]['cef']['sourceAddress'], the dot operator is used to access the sourceAddress sub-element inside the cef element. The answer A is incorrect because the pipe (!) operator is used to chain multiple filters or functions when working with complex datapaths. For example, if the datapath is container['artifacts'][0]['cef']['sourceAddress']! startswith('10.'), the pipe operator is used to apply the startswith function to the sourceAddress element. The answer B is incorrect because the asterisk (*) operator is used to iterate over all the elements of an array when working with complex datapaths. For example, if the datapath is container['artifacts'][*]['cef']['sourceAddress'], the asterisk operator is used to access the sourceAddress element of all the artifacts in the container. The answer C is incorrect because the colon (:) operator is used to specify a range of elements in an array when working with complex datapaths. For example, if the datapath is

container['artifacts'][0:5]['cef']['sourceAddress'], the colon operator is used to access the sourceAddress element of the first five artifacts in the container. Reference: Splunk SOAR Playbook Development Guide, page 28.

NEW QUESTION: 51
Which of the following is an asset ingestion setting in SOAR?
A. Polling Interval
B. Tag
C. File format
D. Operating system
Answer: A (LEAVE A REPLY)
The asset ingestion setting 'Polling Interval' within Splunk SOAR determines how frequently the SOAR platform will poll an asset to ingest data. This setting is crucial for assets that are configured to pull in data from external sources at regular intervals. Adjusting the polling interval allows administrators to balance the need for timely data against network and system resource considerations.
An asset ingestion setting is a configuration option that allows you to specify how often SOAR should poll an asset for new data. Data ingestion settings are available for assets such as QRadar, Splunk, and IMAP. To configure ingestion settings for an asset, you need to navigate to the Asset Configuration page, select the Ingest Settings tab, and edit the Polling Interval field. The Polling Interval is the number of seconds between each poll request that SOAR sends to the asset. Therefore, option A is the correct answer, as it is the only option that is an asset ingestion setting in SOAR. Option B is incorrect, because Tag is not an asset ingestion setting, but a way of labeling an asset for easier identification and filtering. Option C is incorrect, because File format is not an asset ingestion setting, but a way of specifying the format of the data that is ingested from an asset. Option D is incorrect, because Operating system is not an asset ingestion setting, but a way of identifying the type of system that an asset runs on.
1: Configure ingest settings for a Splunk SOAR (On-premises) asset

NEW QUESTION: 52
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: (SHOW ANSWER)
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: 53
Within the 12A2 design methodology, which of the following most accurately describes the last step?
A. List of the apps used by the playbook.
B. List of the actions of the playbook design.
C. List of the outputs of the playbook design.
D. List of the data needed to run the playbook.
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because the last step of the 12A2 design methodology is to list the outputs of the playbook design. The outputs are the expected results or outcomes of the playbook execution, such as sending an email, creating a ticket, blocking an IP, etc. The outputs should be aligned with the objectives and goals of the playbook. See Splunk SOAR Certified Automation Developer for more details.

NEW QUESTION: 54
What is the default embedded search engine used by SOAR?
A. Embedded Splunk search engine.
B. Embedded SOAR search engine.
C. Embedded Django search engine.
D. Embedded Elastic search engine.
Answer: B (LEAVE A REPLY)
the default embedded search engine used by SOAR is the SOAR search engine, which is powered by the PostgreSQL database built-in to Splunk SOAR (Cloud). A Splunk SOAR (Cloud) Administrator can configure options for search from the Home menu, in Search Settings under Administration Settings. The SOAR search engine has been modified to accept the * wildcard and supports various operators and filters. For search syntax and examples, see Search within Splunk SOAR (Cloud)2.
Option A is incorrect, because the embedded Splunk search engine was used in earlier releases of Splunk SOAR (Cloud), but not in the current version. Option C is incorrect, because Django is a web framework, not a search engine. Option D is incorrect, because Elastic is a separate search engine that is not embedded in Splunk SOAR (Cloud).
1: Configure search in Splunk SOAR (Cloud) 2: Search within Splunk SOAR (Cloud)
Splunk SOAR utilizes its own embedded search engine by default, which is tailored to its security orchestration and automation framework. While Splunk SOAR can integrate with other search engines, like the Embedded Splunk search engine, for advanced capabilities

and log analytics, its default setup comes with an embedded search engine optimized for the typical data and search patterns encountered within the SOAR platform.

NEW QUESTION: 55
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. Configure the second query in the Phantom app for Splunk.
B. Enter the two queries in the asset as comma separated values.
C. Configure a second Splunk asset with the second query.
D. Install a second Splunk app and configure the query in the second app.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
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 (LEAVE A REPLY)
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: 57
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: (SHOW ANSWER)
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: 58
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 (LEAVE A REPLY)
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: 59
Which of the following are examples of things commonly done with the Phantom REST APP
A. Use Django queries; use curl to create a container and add artifacts to it; remove temporary lists.
B. Use Django queries; use curl to create a container and add artifacts to it; add action blocks.
C. Use Django queries; use Docker to create a container and add artifacts to it; remove temporary lists.
D. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.
Answer: (SHOW ANSWER)

Explanation
The correct answer is A because using Django queries, using curl to create a container and add artifacts to it, and removing temporary lists are examples of things commonly done with the Phantom REST APP. The Phantom REST APP is a built-in app that allows you to interact with the Phantom server using REST API calls. You can use the run query action to execute Django queries on the Phantom database and return the results as JSON. You can use the curl command to send HTTP requests to the Phantom server and perform various operations, such as creating containers, adding artifacts, running playbooks, etc. You can use the remove list action to delete temporary lists that are no longer needed. See Splunk SOAR Documentation for more details.

NEW QUESTION: 60
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 (LEAVE A REPLY)
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.

NEW QUESTION: 61
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: C (LEAVE A REPLY)
Explanation
The correct answer is C because indicators are artifact values that can appear in multiple containers.
Indicators are a special type of artifacts that are used to store information that is relevant for threat intelligence, such as IP addresses, URLs, file hashes, etc. Indicators can be created using the add indicator action in any playbook block and can be collected using the get indicators action in the filter block. Indicators can also be used to trigger active playbooks based on their label or type. See Splunk SOAR Documentation for more details.

NEW QUESTION: 62
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: (SHOW ANSWER)
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: 63
Configuring Phantom search to use an external Splunk server provides which of the following benefits?
A. The ability to run more complex reports on Phantom activities.
B. The ability to ingest Splunk notable events into Phantom.
C. The ability to automate Splunk searches within Phantom.
D. The ability to display results as Splunk dashboards within Phantom.
Answer: (SHOW ANSWER)
Explanation
The correct answer is C because configuring Phantom search to use an external Splunk server allows you to automate Splunk searches within Phantom using the run query action. This action can be used to run any Splunk search command on the external Splunk server and return the results to Phantom. You can also use the format results action to parse the results and use them in other blocks. See Splunk SOAR Documentation for more details.

NEW QUESTION: 64
In addition to full backups. Phantom supports what other backup type using backup?
A. Incremental
B. Differential
C. Snapshot
D. Partial
Answer: (SHOW ANSWER)

NEW QUESTION: 65
Within the 12A2 design methodology, which of the following most accurately describes the last step?
A. List of the apps used by the playbook.
B. List of the actions of the playbook design.
C. List of the outputs of the playbook design.
D. List of the data needed to run the playbook.
Answer: (SHOW ANSWER)
The correct answer is C because the last step of the 12A2 design methodology is to list the outputs of the playbook design. The outputs are the expected results or outcomes of the playbook execution, such as sending an email, creating a ticket, blocking an IP, etc. The outputs should be aligned with the objectives and goals of the playbook. See Splunk SOAR Certified Automation Developer for more details.
The 12A2 design methodology in the context of Splunk SOAR (formerly Phantom) refers to a structured approach to developing playbooks. The last step in this methodology focuses on defining the outputs of the playbook design. This step is crucial as it outlines what the expected results or actions the playbook should achieve upon its completion. These outputs can vary widely, from sending notifications, creating tickets, updating statuses, to generating reports. Defining the outputs is essential for understanding the playbook's impact on the security operation workflows and how it contributes to resolving security incidents or automating tasks.

NEW QUESTION: 66
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. Yes. from a drop-down menu.
Answer: C (LEAVE A REPLY)
Explanation
External Python libraries can be imported in the global block of a playbook. The global block is executed once when the playbook is loaded and can be used to define global

variables and import modules. The time module is one of the standard Python modules that can be imported in the global block. See Global block for more details.

NEW QUESTION: 67
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: (SHOW ANSWER)
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: 68
When writing a custom function that uses regex to extract the domain name from a URL, a user wants to create a new artifact for the extracted domain. Which of the following Python API calls will create a new artifact?
A. phantom.new_artifact ()
B. phantom. update ()
C. phantom.create_artifact ()
D. phantom.add_artifact ()
Answer: (SHOW ANSWER)

In the Splunk SOAR platform, when writing a custom function in Python to handle data such as extracting a domain name from a URL, you can create a new artifact using the Python API call phantom.create_artifact().
This function allows you to specify the details of the new artifact, such as the type, CEF (Common Event Format) data, container it belongs to, and other relevant information necessary to create an artifact within the system.

NEW QUESTION: 69
How can the debug log for a playbook execution be viewed?
A. Open the playbook in the Visual Playbook Editor, and select Debug Logs in Settings.
B. On the Investigation page, select Debug Log from the playbook's action menu in the Recent Activity panel.
C. In Administration > System Health > Playbook Run History, select the playbook execution entry, then select Log.
D. Click Expand Scope m the debug window.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
In this image, which container fields are searched for the text "Malware"?

A. Event Name or ID.
B. Event Name and Artifact Names.

C. Event Name, Notes, Comments.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
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 (LEAVE A REPLY)
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: 72
After a playbook has run, where are the results stored?
A. Splunk Index
B. Case
C. Container
D. Log file
Answer: C (LEAVE A REPLY)
Explanation
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a

data object in Phantom, but can be a data source for Phantom. Reference: Splunk SOAR User Guide, page 19.

NEW QUESTION: 73
Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?
A. Add a filter block to al restricted playbooks that Titters for runRole - "Admin".
B. Add a tag with restricted access to the restricted playbooks.
C. Make sure the Execute Playbook capability is removed from al roles except admin.
D. Place restricted playbooks in a second source repository that has restricted access.
Answer: C (LEAVE A REPLY)
The correct answer is C because the best way to restrict the execution of playbooks to members of the admin role is to make sure the Execute Playbook capability is removed from all roles except admin. The Execute Playbook capability is a permission that allows a user to run any playbook on any container. By default, all roles have this capability, but it can be removed or added in the Phantom UI by going to Administration > User Management > Roles. Removing this capability from all roles except admin will ensure that only admin users can execute playbooks. See Splunk SOAR Documentation for more details. To ensure that only members of the admin role can execute specific playbooks on the Phantom server, the most effective approach is to manage role-based access controls (RBAC) directly. By configuring the system to remove the "Execute Playbook" capability from all roles except for the admin role, you can enforce this rule. This method leverages Phantom's built-in RBAC mechanisms to restrict playbook execution privileges. It is a straightforward and secure way to ensure that only users with the necessary administrative privileges can initiate the execution of sensitive or critical playbooks, thus maintaining operational security and control.

NEW QUESTION: 74
Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?
A. Non-Human
B. Automation
C. Automation Engineer
D. Service Account
Answer: (SHOW ANSWER)
In Splunk SOAR, the 'Non-Human' role is appropriate for accounts that are used exclusively to execute automated tasks. This role is designed for service accounts that interact with the SOAR platform programmatically rather than through a human user. It ensures that the account has the necessary permissions to perform automated actions while restricting access that would be unnecessary or inappropriate for a non-human entity.

NEW QUESTION: 75
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: A (LEAVE A REPLY)
Explanation
A user who wants to use their Splunk Cloud instance as the external Splunk instance for Phantom needs to open TCP 8088 and TCP 8099 ports on the Splunk Cloud instance. TCP 8088 is used for the HTTP Event Collector (HEC) service, which allows Phantom to send data to Splunk Cloud. TCP 8099 is used for the Splunk REST API service, which allows Phantom to query data from Splunk Cloud. The other port combinations are not valid for this scenario. Splunk Cloud is supported as an external Splunk instance for Phantom. Reference, page 6.

NEW QUESTION: 76
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. Synchronous execution has not been configured.
B. The steep option for the second playbook is not set to a long enough interval.
C. Incorrect Join configuration on the second playbook.
D. The first playbook is performing poorly.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 77
What are the differences between cases and events?
A. Cases: only include high-level incident artifacts.

Events: only include low-level incident artifacts.
B. Case: potential threats.
Events: identified as a specific kind of problem and need a structured approach.
C. Cases: incidents with a known violation and a plan for correction.
Events: occurrences in the system that may require a response.
D. Cases: contain a collection of containers.
Events: contain potential threats.
Answer: B (LEAVE A REPLY)