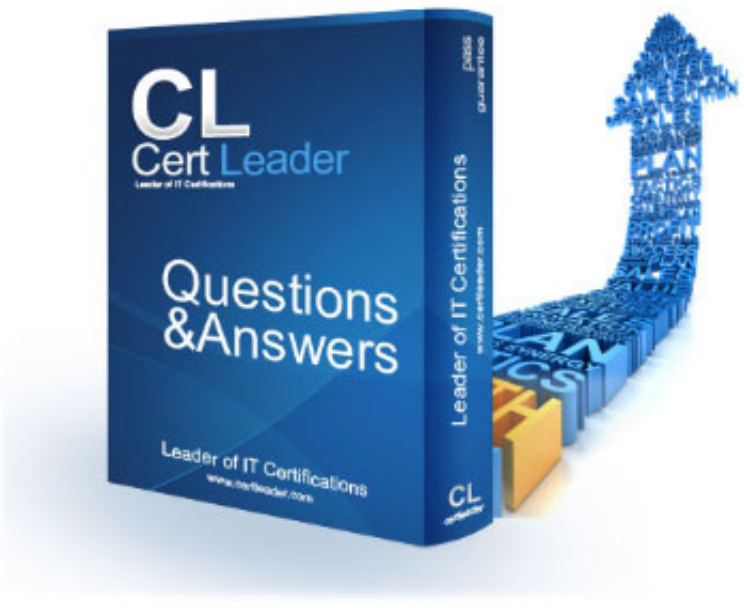
SPLK-2003 Dumps

Splunk Phantom Certified Admin

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



NEW QUESTION 1
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 2
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 3
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 4
Under Asset Ingestion Settings, how many labels must be applied when configuring an asset?

A. Labels are not configured under Asset Ingestion Settings.
B. One.
C. One or more.
D. Zero or more.

Answer: D

Explanation:
Under Asset Ingestion Settings in Splunk SOAR, when configuring an asset, the number of labels that must be applied can be zero or more. Labels are optional and are used to categorize data and control access. They are not a requirement under Asset Ingestion Settings, but they can be used to enhance organization and filtering if chosen.

NEW QUESTION 5
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 6
Which app allows a user to send Splunk Enterprise Security notable events to Phantom?

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

Answer: C

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

NEW QUESTION 7
Is it possible to import external Python libraries such as the time module?

A. No.
B. No, but this can be changed by setting the proper permissions.
C. Yes, in the global block.
D. Ye
E. from a drop-down menu.

Answer: C

Explanation:
In Splunk SOAR, it is possible to import external Python libraries, such as the time module, within the scope of a playbook's global code block. The global block allows users to define custom Python code, including imports of standard Python libraries that are included in the Phantom platform's Python environment. This capability enables the extension of playbooks' functionality with additional Python logic, making playbooks more powerful and versatile in their operations.

NEW QUESTION 8
Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

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

Answer: D

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

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

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

Answer: C

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

NEW QUESTION 10
An active playbook can be configured to operate on all containers that share which attribute?

A. Artifact
B. Label
C. Tag
D. Severity

Answer: B

Explanation:
The correct answer is B because an active playbook can be configured to operate on all containers that share a label. A label is a user-defined attribute that can be applied to containers to group them by a common characteristic, such as source, type, severity, etc. Labels can be used to filter containers and trigger active playbooks based on the label value. See Splunk SOAR Documentation for more details.
In Splunk SOAR, labels are used to categorize containers (such as incidents or events) based on their characteristics or the type of security issue they represent. An active playbook can be configured to trigger on all containers that share a specific label, enabling targeted automation based on the nature of the incident. This functionality allows for efficient and relevant playbook execution, ensuring that the automated response is tailored to the specific requirements of the container's category. Labels serve as a powerful organizational tool within SOAR, guiding the automated response framework to act on incidents that meet predefined criteria, thus streamlining the security operations process.

NEW QUESTION 12
What is the main purpose of using a customized workbook?

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

Answer: B

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

NEW QUESTION 17
Configuring SOAR search to use an external Splunk server provides which of the following benefits?

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

Answer: A

Explanation:
Configuring Splunk SOAR to use an external Splunk server provides several benefits, one of which is the ability to run more complex reports on SOAR activities. Splunk's powerful search and reporting capabilities allow for deeper analysis and more sophisticated reporting on the data generated by SOAR activities, beyond what is possible with the built- in SOAR search engine.

NEW QUESTION 19
Why is it good playbook design to create smaller and more focused playbooks? (select all that apply)

A. Reduces amount of playbook data stored in each repo.

B. Reduce large complex playbooks which become difficult to maintain.
C. Encourages code reuse in a more compartmentalized form.
D. To avoid duplication of code across multiple playbooks.

Answer: BCD

Explanation:
Creating smaller and more focused playbooks in Splunk SOAR is considered good design practice for several reasons:
•B: It reduces complexity, making playbooks easier to maintain. Large, complex playbooks can become unwieldy and difficult to troubleshoot or update.
•C: Encourages code reuse, as smaller playbooks can be designed to handle specific tasks that can be reused across different scenarios.
•D: Avoids duplication of code, as common functionalities can be centralized within specific playbooks, rather than having the same code replicated across multiple playbooks.
This approach has several benefits, such as:
•Reducing large complex playbooks which become difficult to maintain. Smaller playbooks are easier to read, debug, and update1.
•Encouraging code reuse in a more compartmentalized form. Smaller playbooks can be used as building blocks for multiple scenarios, reducing the need to write duplicate code12.
•Improving performance and scalability. Smaller playbooks can run faster and consume less resources than larger playbooks2.
The other options are not valid reasons for creating smaller and more focused playbooks. Reducing the amount of playbook data stored in each repo is not a significant benefit, as the playbook data is not very large compared to other types of data in Splunk SOAR. Avoiding duplication of code across multiple playbooks is a consequence of code reuse, not a separate goal.

NEW QUESTION 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

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

NEW QUESTION 23
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

Explanation:
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 28
Which of the following is an asset ingestion setting in SOAR?

A. Polling Interval
B. Tag
C. File format
D. Operating system

Answer: A

Explanation:
The asset ingestion setting 'Polling Interval' within Splunk SOAR determines how frequently the SOAR platform will poll an asset to ingest data. This setting is crucial for assets that are configured to pull in data from external sources at regular intervals. Adjusting the polling interval allows administrators to balance the need for timely data against network and system resource considerations.
An asset ingestion setting is a configuration option that allows you to specify how often SOAR should poll an asset for new data. Data ingestion settings are

available for assets such as QRadar, Splunk, and IMAP. To configure ingestion settings for an asset, you need to navigate to the Asset Configuration page, select the Ingest Settings tab, and edit the Polling Interval field. The Polling Interval is the number of seconds between each poll request that SOAR sends to the asset. Therefore, option A is the correct answer, as it is the only option that is an asset ingestion setting in SOAR. Option B is incorrect, because Tag is not an asset ingestion setting, but a way of labeling an asset for easier identification and filtering. Option C is incorrect, because File format is not an asset ingestion setting, but a way of specifying the format of the data that is ingested from an asset. Option D is incorrect, because Operating system is not an asset ingestion setting, but a way of identifying the type of system that an asset runs on.
1: Configure ingest settings for a Splunk SOAR (On-premises) asset

NEW QUESTION 29
When configuring a Splunk asset for SOAR to connect to a Splunk Cloud instance, the user discovers that they need to be able to run two different on_poll searches. How is this possible?

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

Answer: C

Explanation:
In Splunk SOAR, if a user needs to run two different on_poll searches for a Splunk Cloud instance, the way to achieve this is to configure a second Splunk asset specifically for the second query. Each asset can be configured with its own on_poll search, allowing multiple searches to be run at their respective intervals. This method provides flexibility and ensures that each search can be managed and configured individually.
The correct way to run two different on_poll searches from a Splunk Cloud instance to Splunk SOAR is to configure a second Splunk asset with the second query. Each Splunk asset in Splunk SOAR can only have one query for the on_poll event, which defines which events to pull in and when to pull them in1. Therefore, if you need to run two different queries, you need to create two separate Splunk assets and configure them with the respective queries. The other options are either not possible or not effective for this purpose. For example:
•Installing a second Splunk app in Splunk SOAR will not help, as the app is just a container for the actions and assets, not the source of the data2.
•Configuring the second query in the Splunk App for SOAR Export will not work, as this app is used to forward events from the Splunk platform to Splunk SOAR, not to pull them in3.
•Entering the two queries in the asset as comma separated values will not work, as the asset will only accept one valid query for the on_poll event1.

NEW QUESTION 32
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 34
Without customizing container status within SOAR, what are the three types of status for a container?

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

Answer: C

Explanation:
In Splunk SOAR, without any customization, the three default statuses for a container are New, In Progress, and Closed. These statuses are designed to reflect the lifecycle of an incident or event within the platform, from its initial detection and logging (New), through the investigation and response stages (In Progress), to its final resolution and closure (Closed). These statuses help in organizing and prioritizing incidents, tracking their progress, and ensuring a structured workflow. Options A, B, and D do not accurately represent the default container statuses within SOAR, making option C the correct answer. containers are the top-level data structure that SOAR playbook APIs operate on. Containers can have different statuses that indicate their state and progress in the SOAR workflow. Without customizing container status within SOAR, the three types of status for a container are:
•New: The container has been created but not yet assigned or investigated.
•In Progress: The container has been assigned and is being investigated or automated.
•Closed: The container has been resolved or dismissed and no further action is required. Therefore, option C is the correct answer, as it lists the three types of status for a container without customizing container status within SOAR. Option A is incorrect, because Resolved is not a type of status for a container without customizing container status within SOAR, but rather a custom status that can be defined by an administrator. Option B is incorrect, because Low, Medium, and High are not types of status for a container, but rather types of severity that indicate the urgency or impact of a container. Option D is incorrect, for the same reason as option B.
1: Web search results from search_web(query="Splunk SOAR Automation Developer container status")

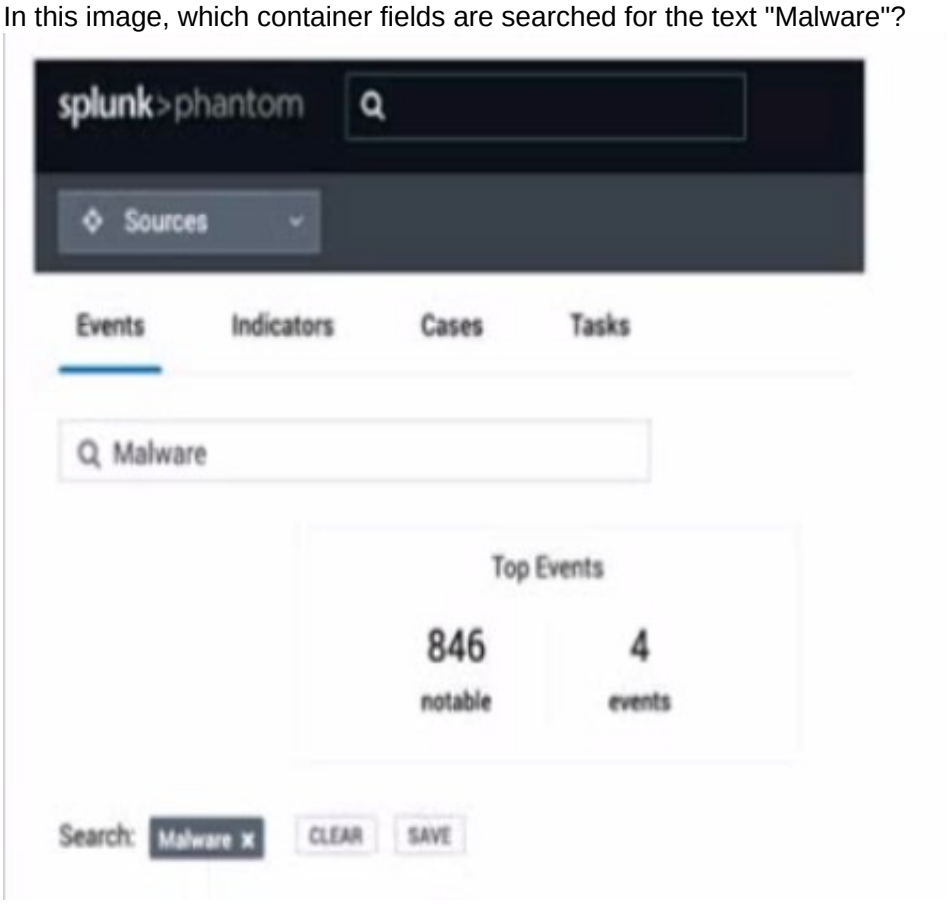
NEW QUESTION 37
What users are included in a new installation of SOAR?

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

Answer: A

Explanation:
The admin and automation users are included by default. Comprehensive Explanation and References of Correct Answer:: According to the Splunk SOAR (On-premises) default credentials, script options, and sample configuration files documentation1, the default credentials on a new installation of Splunk SOAR (On-premises) are:
Web Interface Username: soar_local_admin password: password
On Splunk SOAR (On-premises) deployments which have been upgraded from earlier releases the user account admin becomes a normal user account with the Administrator role.
The automation user is a special user account that is used by Splunk SOAR (On-premises) to run actions and playbooks. It has the Automation role, which grants it full access to all objects and data in Splunk SOAR (On-premises).
The other options are incorrect because they either omit the automation user or include users that are not created by default. For example, option B includes the power and user users, which are not part of the default installation. Option C only includes the admin user, which ignores the automation user. Option D claims that no users are included by default, which is false.
In a new installation of Splunk SOAR, two default user accounts are typically created: admin and automation. The admin account is intended for system administration tasks, providing full access to all features and settings within the SOAR platform. The automation user is a special account used for automated processes and scripts that interact with the SOAR platform, often without requiring direct human intervention. This user has specific permissions that can be tailored for automated tasks. Options B, C, and D do not accurately represent the default user accounts included in a new SOAR installation, making option A the correct answer.

NEW QUESTION 38
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 42
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 43
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. phanto
C. update ()
D. phantom.create_artifact ()
E. phantom.add_artifact ()

Answer: C

Explanation:
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 47
Phantom supports multiple user authentication methods such as LDAP and SAML2. What other user authentication method is supported?

A. SAML3
B. PIV/CAC
C. Biometrics
D. OpenID

Answer: B

Explanation:
Splunk SOAR supports multiple user authentication methods to ensure secure access to the platform. Apart from LDAP (Lightweight Directory Access Protocol) and SAML2 (Security Assertion Markup Language 2.0), SOAR also supports PIV (Personal Identity Verification) and CAC (Common Access Card) as authentication methods. These are particularly used in government and military organizations for secure and authenticated access to systems, providing a high level of security through physical tokens or cards that contain encrypted user credentials.

NEW QUESTION 49
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 52
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 56
Which of the following supported approaches enables Phantom to run on a Windows server?

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

Answer: D

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

NEW QUESTION 61
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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