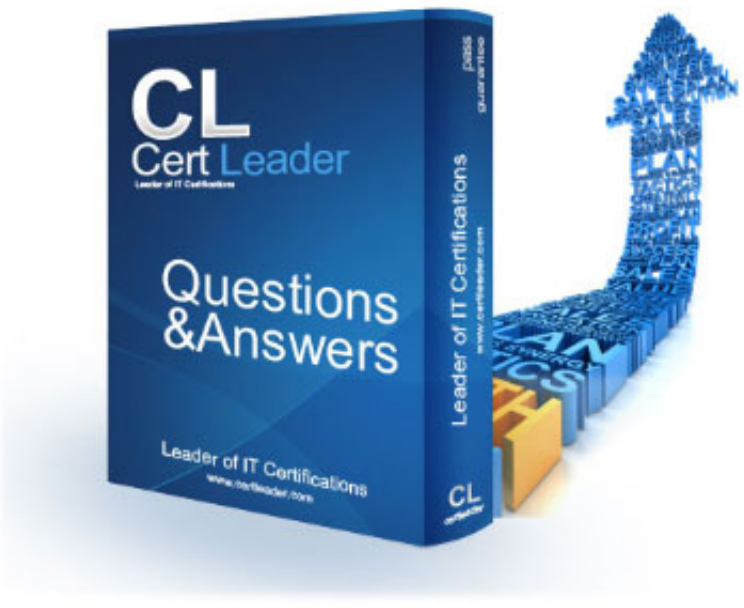
SPLK-2003 Dumps

Splunk Phantom Certified Admin

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

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. 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
Which of the following is the complete list of the types of backups that are supported by Phantom?

A. Full backups.
B. Full, delta, and incremental backups.
C. Full and incremental backups.
D. Full and delta backups.

Answer: C

Explanation:
Splunk Phantom supports different types of backups to safeguard data. Full backups create a complete copy of the current state of the system, while incremental backups only save the changes made since the last backup. This approach allows for efficient use of storage space and faster backups after the initial full backup. Delta backups, which would save changes since the last full or incremental backup, are not a standard part of Phantom's backup capabilities according to available documentation. Therefore, the complete list of backups supported by Phantom would be Full and Incremental backups.

NEW QUESTION 3
The SOAR server has been configured to use an external Splunk search head for search and searching on SOAR works; however, the search results don't include content that was being returned by search before configuring external search. Which of the following could be the problem?

A. The existing content indexes on the SOAR server need to be re-indexed to migrate them to Splunk.
B. The user configured on the SOAR side with Phantomsearch capability is not enabled on Splunk.
C. The remote Splunk search head is currently offline.
D. Content that existed before configuring external search must be backed up on SOAR and restored on the Splunk search head.

Answer: B

Explanation:
If, after configuring an external Splunk search head for search in SOAR, the search results do not include content that was previously returned, one possible issue could be that the user account configured on the SOAR side does not have the required permissions (such as the 'phantomsearch' capability) enabled on the Splunk side. This capability is necessary for the SOAR server to execute searches and retrieve results from the Splunk search head.

NEW QUESTION 4
How can a child playbook access the parent playbook's action results?

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

Answer: C

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

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

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

Answer: B

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

NEW QUESTION 7
Some of the playbooks on the SOAR server should only be executed by members of the admin role. How can this rule be applied?

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

Answer: A

Explanation:
To restrict playbook execution to members of the admin role within Splunk SOAR, the 'Execute Playbook' capability must be managed appropriately. This is done by ensuring that this capability is removed from all other roles except the admin role. Role-based access control (RBAC) in Splunk SOAR allows for granular permissions, which means you can configure which roles have the ability to execute playbooks, and by restricting this capability, you can control which users are able to initiate playbook runs.

NEW QUESTION 8
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 9
After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

A. The new object ID.
B. The new object name.
C. The full CEF name.
D. The PostGres UUID.

Answer: A

Explanation:
The correct answer is A because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is the new object ID. The object ID is a unique identifier for each object in Phantom, such as a container, an artifact, an action, or a playbook. The object ID can be used to retrieve, update, or delete the object using the Phantom REST API. The answer B is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the new object name, which is a human-readable name for the object. The object name can be used to search for the object using the Phantom web interface. The answer C is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the full CEF name, which is a standard format for event data. The full CEF name can be used to access the CEF fields of an artifact using the Phantom REST API. The answer D is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the PostGres UUID, which is a unique identifier for each row in a PostGres database. The PostGres UUID is not exposed to the Phantom REST API. Reference: Splunk SOAR REST API Guide, page 17. When a POST request is made to a Phantom REST endpoint to create a new object, such as an event, artifact, or container, the typical response includes the ID of the newly created object. This ID is a unique identifier that can be used to reference the object within the system for future operations, such as updating, querying, or deleting the object. The response does not usually include the full name or other specific details of the object, as the ID is the most important piece of information needed immediately after creation for reference purposes.

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

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

Answer: C

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

NEW QUESTION 10
A user selects the New option under Sources on the menu. What will be displayed?

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

Answer: B

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

NEW QUESTION 11
Configuring Phantom search to use an external Splunk server provides which of the following benefits?

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

Answer: C

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

https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation- features.html

NEW QUESTION 15
Which of the following describes the use of labels m Phantom?

A. Labels determine the service level agreement (SLA) for a container.
B. Labels control the default seventy, ownership, and sensitivity for the container.
C. Labels control which apps are allowed to execute actions on the container.
D. Labels determine which playbook(s) are executed when a container is created.

Answer: D

Explanation:
In Splunk Phantom, labels are used to categorize containers and trigger specific automated responses. When a container is created, labels can be assigned to it based on the nature of the event, type of incident, or other criteria. These labels are then matched against playbooks, which have label conditions defined within them. When the conditions are met, the corresponding playbooks are automatically executed. Labels do not directly control service level agreements, default severity, ownership, sensitivity, or app execution permissions.

NEW QUESTION 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 22
What are the components of the I2A2 design methodology?

A. Inputs, Interactions, Actions, Apps
B. Inputs, Interactions, Actions, Artifacts
C. Inputs, Interactions, Apps, Artifacts
D. Inputs, Interactions, Actions, Assets

Answer: B

Explanation:
I2A2 design methodology is a framework for designing playbooks that consists of four components:
•Inputs: The data that is required for the playbook to run, such as artifacts, parameters, or custom fields.
•Interactions: The blocks that allow the playbook to communicate with users or other systems, such as prompts, comments, or emails.
•Actions: The blocks that execute the core logic of the playbook, such as app actions, filters, decisions, or utilities.
•Artifacts: The data that is generated or modified by the playbook, such as new artifacts, container fields, or notes.
The I2A2 design methodology helps you to plan, structure, and test your playbooks in a modular and efficient way. Therefore, option B is the correct answer, as it lists the correct components of the I2A2 design methodology. Option A is incorrect, because apps are not a component of the I2A2 design methodology, but a source of actions that can be used in the playbook. Option C is incorrect, for the same reason as option A. Option D is incorrect, because assets are not a component of the I2A2 design methodology, but a configuration of app credentials that can be used in the playbook.
1: Use a playbook design methodology in Administer Splunk SOAR (Cloud)
The I2A2 design methodology is an approach used in Splunk SOAR to structure and design playbooks. The acronym stands for Inputs, Interactions, Actions, and Artifacts. This methodology guides the creation of playbooks by focusing on these four key components, ensuring that all necessary aspects of an automated response are considered and effectively implemented within the platform.

NEW QUESTION 27
What is the simplest way to pass data between playbooks?

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

Answer: A

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

NEW QUESTION 30
During a second test of a playbook, a user receives an error that states: 'an empty parameters list was passed to phantom.act()." What does this indicate?

A. The container has artifacts not parameters.

B. The playbook is using an incorrect container.
C. The playbook debugger's scope is set to new.
D. The playbook debugger's scope is set to all.

Answer: A

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

NEW QUESTION 33
When 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

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. Decision blocks within Splunk Phantom playbooks are used to control the flow of execution based on certain criteria. They are most useful when you need to select one or potentially no paths for the playbook to follow, based on the evaluation of specified conditions. This is akin to an if-else or switch-case logic in programming where depending on the conditions met, a particular path is chosen for further actions. Decision blocks evaluate the data and direct the playbook to different paths accordingly, making them a fundamental component for creating dynamic and responsive automation workflows.

NEW QUESTION 36
In addition to full backups. Phantom supports what other backup type using backup?

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

Answer: B

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

NEW QUESTION 37
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 42
Which of the following are the default ports that must be configured on Splunk to allow connections from Phantom?

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

Answer: D

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

NEW QUESTION 46
When assigning an input parameter to an action while building a playbook, a user notices the artifact value they are looking for does not appear in the auto-populated list.
How is it possible to enter the unlisted artifact value?

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

Answer: A

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

NEW QUESTION 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

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 54
Which of the following expressions will output debug information to the debug window in the Visual Playbook Editor?

A. phantom.debug()
B. phantom.exception()
C. phantom.print ()
D. phantom.assert()

Answer: A

Explanation:
The phantom.debug() function is used within Splunk SOAR playbooks to output debug information to the debug window in the Visual Playbook Editor. This function is instrumental in troubleshooting and developing playbooks, as it allows developers to print out variables, messages, or any relevant information that can help in understanding the flow of the playbook, the data being processed, and any issues that might arise during execution. This debugging tool is essential for ensuring that playbooks are functioning as intended and for diagnosing any problems that may occur.

NEW QUESTION 58
Where in SOAR can a user view the JSON data for a container?

A. In the analyst queue.
B. On the Investigation page.
C. In the data ingestion display.
D. In the audit log.

Answer: B

Explanation:
In Splunk SOAR, the Investigation page is where users can delve into the details of containers, artifacts, and actions. It provides a comprehensive view of the incident or event under investigation, including the JSON data associated with containers. This JSON data represents the structured information about the container, including its attributes, artifacts, and actions taken within the playbook. Options A, C, and D do not typically provide a direct view of the container's JSON data, making option B the correct answer for where a user can view this information within SOAR.
A container is the top-level data structure that SOAR playbook APIs operate on. Every container is a structured JSON object which can nest more arbitrary JSON objects, that represent artifacts. A container is the top-level object against which automation is run. To view the JSON data for a container, you need to navigate to the Investigation page, which shows the details of a container, such as its name, label, owner, status, severity, and artifacts. On the Investigation page, you can click on the JSON tab, which displays the JSON representation of the container and its artifacts. Therefore, option B is the correct answer, as it states where in SOAR a user can view the JSON data for a container. Option A is incorrect, because the analyst queue is not where a user can view the JSON data for a container, but rather where a user can view the list of containers assigned to them or their team. Option C is incorrect, because the data ingestion display is not where a user can view the JSON data for a container, but rather where a user can view the status and configuration of the data sources that ingest data into SOAR. Option D is incorrect, because the audit log is not where a user can view the JSON data for a container, but rather where a user can view the history of actions performed on the SOAR system, such as creating, updating, or deleting objects.
1: Understanding containers in Splunk SOAR (Cloud)

NEW QUESTION 62
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 64
A customer wants to design a modular and reusable set of playbooks that all communicate with each other. Which of the following is a best practice for data sharing across playbooks?

A. Use the py-postgresq1 module to directly save the data in the Postgres database.
B. Cal the child playbooks getter function.
C. Create artifacts using one playbook and collect those artifacts in another playbook.
D. Use the Handle method to pass data directly between playbooks.

Answer: C

Explanation:
The correct answer is C because creating artifacts using one playbook and collecting those artifacts in another playbook is a best practice for data sharing across playbooks. Artifacts are data objects that are associated with a container and can be used to store information such as IP addresses, URLs, file hashes, etc. Artifacts can be created using the add artifact action in any playbook block and can be collected using the get artifacts action in the filter block. Artifacts can also be used to trigger active playbooks based on their label or type. See Splunk SOAR Documentation for more details.
In the context of Splunk SOAR, one of the best practices for data sharing across playbooks is to create artifacts in one playbook and use another playbook to collect and utilize those artifacts. Artifacts in Splunk SOAR are structured data related to security incidents (containers) that playbooks can act upon. By creating artifacts in one playbook, you can effectively pass data and context to subsequent playbooks, allowing for modular, reusable, and interconnected playbook designs. This approach promotes efficiency, reduces redundancy, and enhances the playbook's ability to handle complex workflows.

NEW QUESTION 67
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: D

Explanation:
In the ROI (Return on Investment) Settings within Splunk SOAR, one of the configurable parameters is the annual analyst salary. This setting is used to help quantify the cost savings and efficiency gains achieved through the use of SOAR in an organization's security operations. By factoring in the cost of analyst labor, organizations can better assess the financial impact of automating and streamlining security processes with SOAR, contributing to a comprehensive understanding of the solution's value.

NEW QUESTION 69
Which of the following applies to filter blocks?

A. Can select which blocks have access to container data.
B. Can select assets by tenant, approver, or app.
C. Can be used to select data for use by other blocks.
D. Can select containers by seventy or status.

Answer: C

Explanation:
The correct answer is C because filter blocks can be used to select data for use by other blocks. Filter blocks can filter data from the container, artifacts, or custom lists based on various criteria, such as field name, value, operator, etc. Filter blocks can also join data from multiple sources using the join action. The output of the filter block can be used as input for other blocks, such as decision, format, prompt, etc. See Splunk SOAR Documentation for more details.
Filter blocks within Splunk SOAR playbooks are designed to sift through data and select specific pieces of information based on defined criteria. These blocks are crucial for narrowing down the data that subsequent blocks in a playbook will act upon. By applying filters, a playbook can focus on relevant data, thereby enhancing efficiency and ensuring that actions are taken based on precise, contextually relevant information. This capability is essential for tailoring the playbook's actions to the specific needs of the incident or workflow, enabling more targeted and effective automation strategies. Filters do not directly select blocks for container data access, choose assets by various administrative criteria, or select containers by attributes like severity or status; their primary function is to refine data within the playbook's operational context.

NEW QUESTION 70
What values can be applied when creating Custom CEF field?

A. Name
B. Name, Data Type
C. Name, Value
D. Name, Data Type, Severity

Answer: B

Explanation:
Custom CEF fields can be created with a name and a data type. The name must be unique and the data type must be one of the following: string, int, float, bool, or list. The severity is not a valid option for custom CEF fields. See Creating custom CEF fields for more details. When creating Custom Common Event Format (CEF) fields in Splunk SOAR (formerly Phantom), the essential values you need to specify are the "Name" of the field and the "Data Type." The "Name" is the identifier for the field, while the "Data Type" specifies the kind of data the field will hold, such as string, integer, IP address, etc. This combination allows for the structured and accurate representation of data within SOAR, ensuring that custom fields are compatible with the platform's data processing and analysis mechanisms.

NEW QUESTION 75
Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

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

Answer: C

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

NEW QUESTION 80
How can the DECIDED process be restarted?

A. By restarting the playbook daemon.

B. On the System Health page.
C. In Administration > Server Settings.
D. By restarting the automation service.

Answer: D

Explanation:
DECIDED process is a core component of the SOAR automation engine that handles the execution of playbooks and actions. The DECIDED process can be restarted by restarting the automation service, which can be done from the command line using the service phantom restart command2. Restarting the automation service also restarts the playbook daemon, which is another core component of the SOAR automation engine that handles the loading and unloading of playbooks3. Therefore, option D is the correct answer, as it restarts both the DECIDED process and the playbook daemon. Option A is incorrect, because restarting the playbook daemon alone does not restart the DECIDED process. Option B is incorrect, because the System Health page does not provide an option to restart the DECIDED process or the automation service. Option C is incorrect, because the Administration > Server Settings page does not provide an option to restart the DECIDED process or the automation service.
In Splunk SOAR, if the DECIDED process, which is responsible for playbook execution, needs to be restarted, this can typically be done by restarting the automation (or phantom) service. This service manages the automation processes, including playbook execution.
Restarting it can reset the DECIDED process, resolving issues related to playbook execution or process hangs.

NEW QUESTION 82
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 85
What do assets provide for app functionality?

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

Answer: A

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

NEW QUESTION 86
What are the differences between cases and events?

A. Case: potential threats.Events: identified as a specific kind of problem and need a structured approach.
B. Cases: only include high-level incident artifacts.Events: only include low-level incident artifacts.
C. Cases: contain a collection of container
D. Events: contain potential threats.
E. Cases: incidents with a known violation and a plan for correctio
F. Events: occurrences in the system that may require a response.

Answer: D

Explanation:
Cases and events are two types of containers in Phantom. Cases are incidents with a known violation and a plan for correction, such as a malware infection, a

phishing attack, or a data breach. Events are occurrences in the system that may require a response, such as an alert, a log entry, or an email. Cases and events can contain both high-level and low-level incident artifacts, such as IP addresses, URLs, files, or users. Cases do not contain a collection of containers, but rather a collection of artifacts, tasks, notes, and comments. Events are not necessarily potential threats, but rather indicators of potential threats. In the context of Splunk Phantom, cases and events serve different purposes. Cases are structured to manage and respond to incidents with known violations and typically have a plan for correction. They often involve a coordinated response and may include various artifacts, notes, tasks, and evidence that need to be managed collectively. Events, on the other hand, are occurrences or alerts within the system that may require a response. They can be considered as individual pieces of information or incidents that may be part of a larger case. Events are the building blocks that can be aggregated into cases if they are related and require a consolidated approach to incident response and investigation.

NEW QUESTION 90
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

Explanation:
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 93
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 95
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 Docker to create a container and add artifacts to it; remove temporary lists.
C. Use Django queries; use curl to create a container and add artifacts to it; add action blocks.
D. Use SQL queries; use curl to create a container and add artifacts to it; remove temporary lists.

Answer: C

Explanation:
The Phantom REST API, often interacted with through the Phantom REST APP, is a powerful tool for automating and integrating Splunk SOAR with other systems. Common uses of the Phantom REST APP include using Django queries to interact with the SOAR database, using curl commands to programmatically create containers and add artifacts to them, and configuring action blocks within playbooks for automated actions. This flexibility allows for a wide range of automation and integration possibilities, enhancing the SOAR platform's capability to respond to security incidents and manage data.

NEW QUESTION 96
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 100
A user wants to use their Splunk Cloud instance as the external Splunk instance for Phantom. What ports need to be opened on the Splunk Cloud instance to facilitate this? Assume default ports are in use.

A. TCP 8088 and TCP 8099.

B. TCP 80 and TCP 443.
C. Splunk Cloud is not supported.
D. TCP 8080 and TCP 8191.

Answer: B

Explanation:
To integrate Splunk Phantom with a Splunk Cloud instance, network communication over certain ports is necessary. The default ports for web traffic are TCP 80 for HTTP and TCP 443 for HTTPS. Since Splunk Cloud instances are accessed over the internet, ensuring that these ports are open is essential for Phantom to communicate with Splunk Cloud for various operations, such as running searches, sending data, and receiving results. It is important to note that TCP 8088 is typically used by Splunk's HTTP Event Collector (HEC), which may also be relevant depending on the integration specifics.

NEW QUESTION 103
Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?

A. superuser, administrator
B. phantomcreat
C. phantomedit
D. phantomsearch, phantomdelete
E. admin,user

Answer: A

Explanation:
When configuring Splunk Phantom to integrate with an external Splunk Enterprise instance, it is typically required to have user accounts with sufficient privileges to access data and perform necessary actions. The roles of "superuser" and "administrator" in Splunk provide the broad set of permissions needed for such integration, enabling comprehensive access to data, management capabilities, and the execution of searches or actions that Phantom may require as part of its automated playbooks or investigations.

NEW QUESTION 108
Which of the following can be configured in the ROI Settings?

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

Answer: C

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

NEW QUESTION 113
Where can the Splunk App for SOAR Export be downloaded from?

A. GitHub and Splunkbase.
B. SOAR Community and GitHub.
C. Splunkbase and SOAR Community.
D. Splunk Answers and Splunkbase.

Answer: C

Explanation:
The Splunk App for SOAR Export can typically be downloaded from Splunkbase, which is Splunk's marketplace for apps and add-ons. Additionally, it can often be found within the SOAR Community site, where users can share and access apps, playbooks, and other resources created for the Splunk SOAR ecosystem. These platforms provide trusted sources for downloading the app, ensuring compatibility and support.
Splunk App for SOAR Export can be downloaded from two sources: Splunkbase and SOAR Community. Splunkbase is the official repository of Splunk apps and add-ons, where you can find the latest version of the Splunk App for SOAR Export, along with its documentation, release notes, and ratings2. SOAR Community is the online forum for Splunk SOAR users and developers, where you can find the Splunk App for SOAR Export, along with other useful resources, such as FAQs, tips, and best practices3. Therefore, option C is the correct answer, as it lists the two sources where the Splunk App for SOAR Export can be downloaded from. Option A is incorrect, because GitHub is not a source where the Splunk App for SOAR Export can be downloaded from, but rather a platform for hosting and managing code repositories. Option B is incorrect, for the same reason as option A. Option D is incorrect, because Splunk Answers is not a source where the Splunk App for SOAR Export can be downloaded from, but rather a platform for asking and answering questions about Splunk products and services.
1: Web search results from search_web(query="Splunk SOAR Automation Developer Splunk App for SOAR Export") 2: Splunk App for SOAR Export | Splunkbase
3: SOAR Community - Splunk App for SOAR Export

NEW QUESTION 118
Which of the following are the default ports that must be configured on Splunk to allow connections from SOAR?

A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)
C. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)
D. SplunkWeb (8469), SplunkD (8702), HTTP Collector (8864)

Answer: C

Explanation:
For Splunk SOAR to connect with Splunk Enterprise, certain default ports must be configured to facilitate communication between the two platforms. Typically, SplunkWeb, which serves the Splunk Enterprise web interface, uses port 8000. SplunkD, the Splunk daemon that handles most of the back-end services, listens on port 8089. The HTTP Event Collector (HEC), which allows HTTP clients to send data to Splunk, typically uses port 8088. These ports are essential for the integration, allowing SOAR to send data to Splunk for indexing, searching, and visualization. Options A, B, and D list incorrect port configurations for this purpose, making option C the correct answer based on standard Splunk configurations.
These are the default ports used by Splunk SOAR (On-premises) to communicate with the embedded Splunk Enterprise instance. SplunkWeb is the web interface for Splunk Enterprise, SplunkD is the management port for Splunk Enterprise, and HTTP Collector is the port for receiving data from HTTP Event Collector (HEC). The other options are either incorrect or not default ports. For example, option B has the SplunkWeb and SplunkD ports reversed, and option D has arbitrary port numbers that are not used by Splunk by default.

NEW QUESTION 119
.....

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