Exam Questions SPLK-2003

Splunk Phantom Certified Admin

https://www.2passeasy.com/dumps/SPLK-2003/

NEW QUESTION 1
How can the debug log for a playbook execution be viewed?

A. On the Investigation page, select Debug Log from the playbook's action menu in the Recent Activity panel.
B. Click Expand Scope m the debug window.
C. In Administration > System Health > Playbook Run History, select the playbook execution entry, then select Log.
D. Open the playbook in the Visual Playbook Editor, and select Debug Logs in Settings.

Answer: A

Explanation:
Debug logs are essential for troubleshooting and understanding the execution flow of a playbook in Splunk Phantom. The debug log for a playbook execution can be viewed by navigating to the Investigation page of a specific event or container. Within the Recent Activity panel, there is an action menu associated with each playbook run. Selecting "Debug Log" from this menu will display the detailed execution log, showing each action taken, the results of those actions, and any errors or messages generated during the playbook run.

NEW QUESTION 2
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 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
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 5
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 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
Which app allows a user to run Splunk queries from within Phantom?

A. Splunk App for Phantom?
B. The Integrated Splunk/Phantom app.
C. Phantom App for Splunk.
D. Splunk App for Phantom Reporting.

Answer: C

Explanation:
The Phantom App for Splunk allows a user to run Splunk queries from within Phantom. This app provides actions such as run query, ingest events, and save search, which enable the user to interact with Splunk from Phantom playbooks or the Phantom UI. The other apps are not relevant for this use case. The Splunk App for Phantom is used to send data from Splunk to Phantom. The Integrated Splunk/Phantom app is a deprecated app that was replaced by the Splunk App for Phantom. The Splunk App for Phantom Reporting is used to generate reports on Phantom activity from Splunk. The Phantom App for Splunk is the application that enables Splunk users to run Splunk queries from within the Splunk Phantom platform. This app integrates Splunk's data and search capabilities into Phantom's security automation and orchestration framework, allowing users to perform actions such as running searches, creating events, and updating records in Splunk directly from Phantom.

NEW QUESTION 8
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 9

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 10
What is the main purpose of using a customized workbook?

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

Answer: B

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

NEW QUESTION 10
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 14
How is a Django filter query performed?

A. By adding parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo".
B. phantom/rest/search/app/contains/"sumo"
C. Browse to the Django Filter Query Editor in the Administration panel.
D. Install the SOAR Django App first, then configure the search query in the App editor.

Answer: A

Explanation:
Django filter queries in Splunk SOAR are performed by appending filter parameters directly to the REST API URL. This allows users to refine their search and retrieve specific data. For example, to filter containers by tags containing the word "sumo", the following URL structure would be used:
https://<PHANTOM_URL>/rest/container?_filter_tags_contains="sumo". This format enables users to construct dynamic queries that can filter results based on specified criteria within the Django framework used by Splunk SOAR.
The correct way to perform a Django filter query in Splunk SOAR is to add parameters to the URL similar to the following:
phantom/rest/container?_filter_tags_contains="sumo". This will return a list of containers that have the tag "sumo" in them. You can use various operators and fields to filter the results according to your needs. For more details, see Query for Data and Use filters in your Splunk SOAR (Cloud) playbook to specify a subset of artifacts before further processing. The other options are either incorrect or irrelevant for this question. For example:
•phantom/rest/search/app/contains/"sumo" is not a valid URL for a Django filter query. It will return an error message saying "Invalid endpoint".
•There is no Django Filter Query Editor in the Administration panel of Splunk SOAR. You can use the REST API Tester to test your queries, but not to edit them.
•There is no SOAR Django App that needs to be installed or configured for performing Django filter queries. Splunk SOAR uses the Django framework internally, but you do not need to install or use any additional apps for this purpose.

NEW QUESTION 18
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 20
Which of the following is a reason to create a new role in SOAR?

A. To define a set of users who have access to a special label.
B. To define a set of users who have access to a restricted app.
C. To define a set of users who have access to an event's reports.
D. To define a set of users who have access to a sensitive tag.

Answer: A

Explanation:
Creating a new role in Splunk SOAR is often done to define a set of users who have specific access rights, such as access to a special label. Labels in SOAR can be used to categorize data and control access. By assigning a role with access to a particular label, administrators can ensure that only a specific group of users can view or interact with containers, events, or artifacts that have been tagged with that label, thus maintaining control over sensitive data or operations.

NEW QUESTION 22
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 27
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 32
After enabling multi-tenancy, which of the Mowing is the first configuration step?

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

Answer: D

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

NEW QUESTION 34
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 35
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 36
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 37

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 38

Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?

A. Non-Human
B. Automation
C. Automation Engineer
D. Service Account

Answer: A

Explanation:
In Splunk SOAR, the 'Non-Human' role is appropriate for accounts that are used exclusively to execute automated tasks. This role is designed for service accounts that interact with the SOAR platform programmatically rather than through a human user. It ensures that the account has the necessary permissions to perform automated actions while restricting access that would be unnecessary or inappropriate for a non-human entity.

NEW QUESTION 43

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 44

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 49

What are indicators?

A. Action result items that determine the flow of execution in a playbook.
B. Action results that may appear in multiple containers.

C. Artifact values that can appear in multiple containers.
D. Artifact values with special security significance.

Answer: D

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

NEW QUESTION 53
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 54
What does a user need to do to have a container with an event from Splunk use context- aware actions designed for notable events?

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

Answer: C

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

NEW QUESTION 58
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 61
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-2003 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-2003 Product From:

https://www.2passeasy.com/dumps/SPLK-2003/

Money Back Guarantee

SPLK-2003 Practice Exam Features:

* SPLK-2003 Questions and Answers Updated Frequently

* SPLK-2003 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-2003 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-2003 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year