Splunk

Exam Questions SPLK-2003

Splunk Phantom Certified Admin

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
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 3
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 4
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 5
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 6
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 7
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

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

Answer: B

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

NEW QUESTION 8
What is the default embedded search engine used by SOAR?

A. Embedded Splunk search engine.
B. Embedded SOAR search engine.
C. Embedded Django search engine.
D. Embedded Elastic search engine.

Answer: B

Explanation:
the default embedded search engine used by SOAR is the SOAR search engine, which is powered by the PostgreSQL database built-in to Splunk SOAR (Cloud). A Splunk SOAR (Cloud) Administrator can configure options for search from the Home menu, in Search Settings under Administration Settings. The SOAR search engine has been modified to accept the * wildcard and supports various operators and filters. For search syntax and examples, see Search within Splunk SOAR (Cloud)2.
Option A is incorrect, because the embedded Splunk search engine was used in earlier releases of Splunk SOAR (Cloud), but not in the current version. Option C is incorrect, because Django is a web framework, not a search engine. Option D is incorrect, because Elastic is a separate search engine that is not embedded in Splunk SOAR (Cloud).
1: Configure search in Splunk SOAR (Cloud) 2: Search within Splunk SOAR (Cloud)

Splunk SOAR utilizes its own embedded search engine by default, which is tailored to its security orchestration and automation framework. While Splunk SOAR can integrate with other search engines, like the Embedded Splunk search engine, for advanced capabilities and log analytics, its default setup comes with an embedded search engine optimized for
the typical data and search patterns encountered within the SOAR platform.

NEW QUESTION 9
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 10
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 10
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 15
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 20
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 21
Which of the following can the format block be used for?

A. To generate arrays for input into other functions.
B. To generate HTML or CSS content for output in email messages, user prompts, or comments.
C. To generate string parameters for automated action blocks.
D. To create text strings that merge state text with dynamic values for input or output.

Answer: D

Explanation:
The format block in Splunk SOAR is utilized to construct text strings by merging static text with dynamic values, which can then be used for both input to other playbook blocks and output for reports, emails, or other forms of communication. This capability is essential for customizing messages, commands, or data processing tasks within a playbook, allowing for the dynamic insertion of variable data into predefined text templates. This feature enhances the playbook's ability to present information clearly and to execute actions that require specific parameter formats.

NEW QUESTION 22
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 23
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 25
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 29
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 34
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 38
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 42
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-2003 Practice Exam Features:

* SPLK-2003 Questions and Answers Updated Frequently

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

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

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