SPLK-2003 Q&As

Splunk SOAR Certified Automation Developer

Pass Splunk SPLK-2003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/splk-2003.html

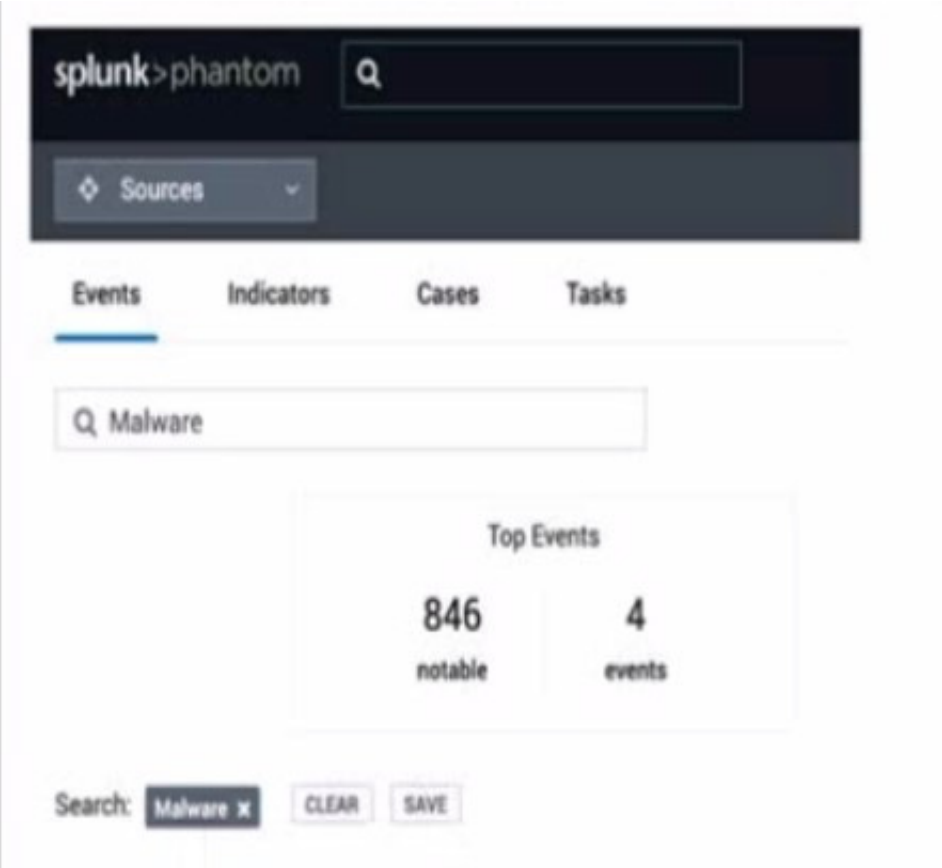
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

In this image, which container fields are searched for the text "Malware"?



A. Event Name and Artifact Names.

B. Event Name, Notes, Comments.

C. Event Name or ID.

Correct Answer: C

In the image provided, the search functionality within Splunk\\'s Phantom Security Orchestration, Automation, and Response (SOAR) platform is shown. When you enter a search term like "Malware" in the search bar, Splunk Phantom will typically search through the container fields that are most relevant to identifying and categorizing events. Containers in Phantom are used to group related events, indicators, cases, and tasks. They contain various fields that can be searched through, such as the Event Name or ID, which are primary identifiers for a container. This search does not extend to fields such as Notes or Comments, which are ancillary text entries linked to an event or container. Artifact Names are part of the container\\'s data structure but are not the primary search target in this context unless specifically configured to be included in the search scope.

QUESTION 2

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.

Correct Answer: B

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.

QUESTION 3

Which of the following actions will store a compressed, secure version of an email attachment with suspected malware for future analysis?

A. Copy/paste the attachment into a note.

B. Add a link to the file in a new artifact.

C. Use the Files tab on the Investigation page to upload the attachment.

D. Use the Upload action of the Secure Store app to store the file in the database.

Correct Answer: D

To securely store a compressed version of an email attachment suspected of containing malware for future analysis, the most effective approach within Splunk SOAR is to use the Upload action of the Secure Store app. This app is specifically designed to handle sensitive or potentially dangerous files by securely storing them within the SOAR database, allowing for controlled access and analysis at a later time. This method ensures that the file is not only safely contained but also available for future forensic or investigative purposes without risking exposure to the malware. Options A, B, and C do not provide the same level of security and functionality for handling suspected malware files, making option D the most appropriate choice.

Secure Store app is a SOAR app that allows you to store files securely in the SOAR database. The Secure Store app provides two actions: Upload and Download. The Upload action takes a file as an input and stores it in the SOAR database in a compressed and encrypted format. The Download action takes a file ID as an input and retrieves the file from the SOAR database and decrypts it. The Secure Store app can be used to store files that contain sensitive or malicious data, such as email attachments with suspected malware, for future analysis. Therefore, option D is the correct answer, as it states the action that will store a compressed, secure version of an email attachment with suspected malware for future analysis. Option A is incorrect, because copying and pasting the attachment into a note will not store the file securely, but rather expose the file content to anyone who can view the note. Option B is incorrect, because adding a link to the file in a new artifact will not store the file securely, but rather create a reference to the file location, which may not be accessible or reliable. Option C is incorrect, because using the Files tab on the Investigation page to upload the attachment will not store the file securely, but rather store the file in the SOAR file system, which may not be encrypted or compressed. Web search results from search_web(query="Splunk SOAR Automation

Developer store email attachment with suspected malware")

QUESTION 4

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.

Correct Answer: A

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.., 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. Web search results from search_web(query="Splunk SOAR Automation Developer input parameter to an action")

QUESTION 5

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)

Correct Answer: D

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.