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

QUESTION 1

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

A. No.

B. No, but this can be changed by setting the proper permissions.

C. Yes, in the global block.

D. Yes. from a drop-down menu.

Correct Answer: C

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

QUESTION 2

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

Correct Answer: A

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.

QUESTION 3

Which of the following can be edited or deleted in the Investigation page?

A. Action results

B. Comments

C. Approval records

D. Artifact values

Correct Answer: B

On the Investigation page in Splunk SOAR, users have the ability to edit or delete comments associated with an event or a container. Comments are generally used for collaboration and to provide additional context to an investigation. While action results, approval records, and artifact values are typically not editable or deletable to maintain the integrity of the investigative data, comments are more flexible and can be managed by users to reflect the current state of the investigation.

Investigation page allows you to view and edit various information and data related to an event or a case. One of the things that you can edit or delete in the Investigation page is the comments that you or other users have added to the activity feed. Comments are a way of communicating and collaborating with other users during the investigation process. You can edit or delete your own comments by clicking on the three-dot menu icon next to the comment and selecting the appropriate option. You can also reply to other users\\' comments by clicking on the reply icon. Therefore, option B is the correct answer, as it is the only option that can be edited or deleted in the Investigation page. Option A is incorrect, because action results are the outputs of the actions or playbooks that have been run on the event or case, and they cannot be edited or deleted in the Investigation page. Option C is incorrect, because approval records are the logs of the approval requests and responses that have been made for certain actions or playbooks, and they cannot be edited or deleted in the Investigation page. Option D is incorrect, because artifact values are the data that has been collected or generated by the event or case, and they cannot be edited or deleted in the Investigation page.

1: Start with Investigation in Splunk SOAR (Cloud)

QUESTION 4

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.

Correct Answer: A

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.

QUESTION 5

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)

Correct Answer: D

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.