Explore the Benefits and Splunk SPLK-2003 Exam Preparation Strategies

BTW, DOWNLOAD part of ValidTorrent SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1vk0iFKLA5UzooN1kmUPXaIqkqXb9YjHN

Nowadays the competition in the job market is fiercer than any time in the past. If you want to find a good job， you must own good competences and skillful major knowledge. So owning the SPLK-2003 certification is necessary for you because we will provide the best study materials to you. Our SPLK-2003 Exam Torrent is of high quality and efficient, and it can help you pass the test successfully.

Splunk SPLK-2003 exam is a certification exam designed for individuals who want to become certified Splunk Phantom administrators. Splunk Phantom is a security orchestration, automation, and response (SOAR) platform that allows organizations to automate and streamline their security operations. The SPLK-2003 Exam Tests knowledge and skills related to the administration and configuration of the Splunk Phantom platform.

>> Relevant SPLK-2003 Answers <<

Exam SPLK-2003 Book - Dumps SPLK-2003 Vce

If you purchase our SPLK-2003 preparation questions, it will be very easy for you to easily and efficiently find the exam focus. More importantly, if you take our products into consideration, our SPLK-2003 study materials will bring a good academic outcome for you. At the same time, we believe that our SPLK-2003 training quiz will be very useful for you to have high quality learning time during your learning process. Your success is 100% guaranteed with our SPLK-2003 learning guide!

Splunk Phantom Certified Admin Sample Questions (Q40-Q45):

NEW QUESTION # 40
Which of the following items cannot be modified once entered into SOAR?

- A. A comment.
- B. A note.
- C. A container.
- D. An artifact.

Answer: D

NEW QUESTION # 41
Seventy can be set during ingestion and later changed manually. What other mechanism can change the severity or a container?

- A. Actions
- B. Playbooks
- C. Notes
- D. Service level agreement (SLA) expiration

Answer: A

NEW QUESTION # 42
Without customizing container status within SOAR, what are the three types of status for a container?

- A. Low, Medium, High
- B. New, Open, Resolved
- C. Low, Medium, Critical
- D. New, In Progress, Closed

Answer: D

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 # 43
Why does SOAR use wildcards within artifact data paths?

- A. To make decision execution in playbooks run faster.
- B. To make data access in playbooks easier.
- C. To make playbooks filter out nulls.
- D. To make playbooks more specific.

Answer: B

Explanation:
Wildcards are used within artifact data paths in Splunk SOAR playbooks to simplify the process of accessing data. They allow playbooks to reference dynamic or variable data structures without needing to specify exact paths, which can vary between artifacts. This flexibility makes it easier to write playbooks that work across different events and scenarios, without hard-coding data paths.
SOAR uses wildcards within artifact data paths to make data access in playbooks easier. A data path is a way of specifying the location of a piece of data within an artifact. For example, artifact.cef.sourceAddress is a data path that refers to the source address field of the artifact. A wildcard is a special character that can match any value or subfield within a data path. For example, artifact.*.cef.sourceAddress is a data path that uses a wildcard to match any field name before the cef subfield. This allows the playbook to access the source address data regardless of the field name, which can vary depending on the app or source that generated the artifact.

NEW QUESTION # 44
How is a Django filter query performed?

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

Answer: C

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.

NEW QUESTION # 45
.....