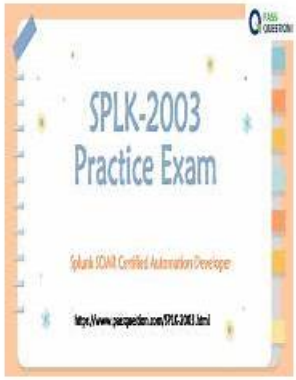
Pdf Demo SPLK-2003 Download, Exam SPLK-2003 Passing Score



P.S. Free 2025 Splunk SPLK-2003 dumps are available on Google Drive shared by Exams-boost: https://drive.google.com/open?id=14IpzYYVVpdpyR_4kgXaYPBXOtubmDgfj

The world is changing rapidly and the requirements to the employees are higher than ever before. If you want to find an ideal job and earn a high income you must boost good working abilities and profound major knowledge. Passing SPLK-2003 certification can help you realize your dreams. If you buy our product, we will provide you with the best Splunk SOAR Certified Automation Developer study materials and it can help you obtain SPLK-2003certification. Our product is of high quality and our service is perfect.

The Splunk Phantom Certified Admin certification program is designed to provide IT professionals with a recognized credential that validates their knowledge and skills in the area of security automation and orchestration. Certified professionals will be able to demonstrate their ability to effectively use the Phantom platform to automate security tasks, improve incident response times, and enhance the overall security posture of their organization.

Splunk SPLK-2003 certification exam is designed to test the skills and knowledge of individuals who wish to become certified as a Splunk Phantom Certified Admin. Splunk Phantom Certified Admin certification is intended for professionals who are responsible for deploying, configuring, and managing the Splunk Phantom platform, which is used for security automation and orchestration. SPLK-2003 Exam covers a range of topics, including architecture and deployment, user and role management, automation and orchestration, and integration with third-party tools.

>> Pdf Demo SPLK-2003 Download <<

Exam SPLK-2003 Passing Score & Sample SPLK-2003 Questions Answers

Before the clients decide to buy our SPLK-2003 test guide they can firstly be familiar with our products. The clients can understand the detailed information about our products by visiting the pages of our products on our company's website. Firstly you could know the price and the version of our SPLK-2003 study question, the quantity of the questions and the answers. Secondly you could look at the free demos of our SPLK-2003 learning prep to see if the questions and the answers are valuable. And our pass rate of SPLK-2003 exam questions is more than 98%.

Splunk Phantom Certified Admin Sample Questions (Q97-Q102):

NEW QUESTION # 97
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 # 98
When writing a custom function that uses regex to extract the domain name from a URL, a user wants to create a new artifact for the extracted domain. Which of the following Python API calls will create a new artifact?

- A. phantom.add_artifact ()
- B. phantom. update ()
- C. phantom.new_artifact ()
- D. phantom.create_artifact ()

Answer: D

Explanation:
In the Splunk SOAR platform, when writing a custom function in Python to handle data such as extracting a domain name from a URL, you can create a new artifact using the Python API call phantom.create_artifact(). This function allows you to specify the details of the new artifact, such as the type, CEF (Common Event Format) data, container it belongs to, and other relevant information necessary to create an artifact within the system.

NEW QUESTION # 99
Without customizing container status within SOAR, what are the three types of status for a container?

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

Answer: B

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.

NEW QUESTION # 100
Which of the following can be configured in the ROI Settings?

- A. Analyst hours per month.
- B. Number of full time employees (FTEs).
- C. Annual analyst salary.
- D. Time lost.

Answer: A

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 # 101
Playbooks typically handle which types of data?

- A. Container data, Artifact data, Result data, Threat data
- B. Container data, Artifact CEF data, Result data, List data
- C. Container data, Artifact CEF data, Result data. Threat data
- D. Container CEF data, Artifact data, Result data, List data

Answer: B

Explanation:
Playbooks in Splunk SOAR are designed to handle various types of data to automate responses to security incidents. The correct types of data handled by playbooks include:
* Container Data: Containers are used to group related data for an incident or event. Playbooks can access this information to perform actions and make decisions.
* Artifact CEF Data: Artifacts hold detailed information about the event or incident, including CEF (Common Event Format) data. Playbooks often process this CEF data for various actions.
* Result Data: This refers to the data generated from actions executed by the playbook, such as results from API calls, integrations, or automated responses.

* List Data: Lists in Splunk SOAR are collections of reusable data (such as IP blocklists, whitelists, etc.) that playbooks can access to check values or make decisions based on external lists.
The inclusion of List data instead of Threat data distinguishes this option from others, as lists are more directly used by playbooks during execution, whereas threat data is a broader category that is often processed but not always directly handled by playbooks.
References:
* Splunk SOAR Documentation: Playbook Data Handling.
* Splunk SOAR Best Practices: Automating with Playbooks.

NEW QUESTION # 102
.....

The latest Splunk Phantom Certified Admin SPLK-2003 exam and exam study guide is reliable, Splunk Phantom Certified Admin SPLK-2003 with reasonable exam price and guaranteed questions answers. Splunk offers actual Splunk Phantom Certified Admin to sure your success in SPLK-2003 Exam. Don't worry, this Splunk Phantom Certified Admin SPLK-2003 test price is benefit and content is 365 days updates!