Free PDF Quiz SPLK-2003 - Splunk Phantom Certified Admin Updated Books PDF

P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by VCEDumps: https://drive.google.com/open?id=1GESo0tOZVg48OS9OxdlOeGcCJfNeEkAx

The great reputation of our SPLK-2003 study materials has earned the title "the model study material for the test certification" for us. Our assiduous pursuit for high quality of our products creates our top-ranking SPLK-2003 study materials and constantly increasing sales volume. Our company has forged a group of professional experts with the excelsior craftsmanship and a mature service system. The quality of our SPLK-2003 Study Materials is high because our experts team organizes and compiles them according to the real exam's needs and has extracted the essence of all of the information about the test.

Obtaining the Splunk Phantom Certified Admin certification can lead to better career opportunities and higher salaries. As IT organizations continue to adopt SOAR solutions, the demand for professionals with Splunk Phantom skills will increase. A Splunk Phantom admin can expect to earn an average salary of $115,000 per year, according to Glassdoor.

>> SPLK-2003 Books PDF <<

Advantages Of These Splunk SPLK-2003 Exam Questions Formats

In order to meet the demand of all customers and protect your machines network security, our company can promise that our SPLK-2003 study materials have adopted technological and other necessary measures to ensure the security of personal information they collect, and prevent information leaks, damage or loss. In addition, the SPLK-2003 Study Materials system from our company can help all customers ward off network intrusion and attacks prevent information leakage, protect user machines network security.

The SPLK-2003 exam consists of 73 multiple-choice questions that evaluate a candidate's proficiency in the following areas: configuring and deploying Splunk Phantom, managing assets and playbooks, creating and managing incidents, and implementing automation in workflows. SPLK-2003 Exam Duration is two hours, and it can be taken online or in-person.

Splunk Phantom Certified Admin Sample Questions (Q14-Q19):

NEW QUESTION # 14
Which of the following roles is appropriate for a Splunk SOAR account that will only be used to execute automated tasks?

- A. Service Account
- B. Automation
- C. Automation Engineer
- D. Non-Human

Answer: D

Explanation:
In Splunk SOAR, the 'Non-Human' role is appropriate for accounts that are used exclusively to execute automated tasks. This role is designed for service accounts that interact with the SOAR platform programmatically rather than through a human user. It ensures that the account has the necessary permissions to perform automated actions while restricting access that would be unnecessary or

inappropriate for a non-human entity.

NEW QUESTION # 15
When working with complex datapaths, which operator is used to access a sub-element inside another element?

- A. : (colon)
- B. * (asterisk)
- C. . (dot)
- D. | (pipe)

Answer: C

Explanation:
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.

NEW QUESTION # 16
What is the simplest way to pass data between playbooks?

- A. File system
- B. Artifacts
- C. Action results
- D. KV Store

Answer: B

Explanation:
The simplest way to pass data between playbooks in Splunk SOAR is through the use of artifacts.
Artifacts are objects that can store data and are associated with containers. When multiple playbooks work on a single container, they can access and manipulate the same set of artifacts, allowing for seamless data transfer between playbooks. This method is straightforward and does not require additional setup or management of external storage systems, making it the most direct and efficient way to pass data within the Splunk SOAR environment.

NEW QUESTION # 17
What is the simplest way to pass data between playbooks?

- A. File system
- B. Artifacts
- C. Action results
- D. KV Store

Answer: B

Explanation:
Explanation
The correct answer is C because artifacts are the simplest way to pass data between playbooks. Artifacts are data objects that are associated with a container and can be created, updated, or deleted by playbooks. Artifacts can be used to store and share information such as indicators, evidence, or action results between playbooks.
The answer A is incorrect because action results are not a way to pass data between playbooks, but a way to receive data from an action within a playbook. The answer B is incorrect because the file system is not a way to pass data between playbooks, but a way to store and access files on the Phantom server or a remote host.
The answer D is incorrect because the KV Store is not a way to pass data between playbooks, but a way to store and retrieve key-value pairs on the Phantom server. Reference: Splunk SOAR Playbook Development Guide, page 30.

NEW QUESTION # 18
Some of the playbooks on the SOAR server should only be executed by members of the admin role. How can this rule be applied?

- A. Add a tag with restricted access to the restricted playbooks.
- B. Add a filter block to all restricted playbooks that filters for runRole = "Admin".
- C. Make sure the Execute Playbook capability is removed from all roles except admin.
- D. Place restricted playbooks in a second source repository that has restricted access.

Answer: C

Explanation:
To restrict playbook execution to members of the admin role within Splunk SOAR, the 'Execute Playbook' capability must be managed appropriately. This is done by ensuring that this capability is removed from all other roles except the admin role. Role-based access control (RBAC) in Splunk SOAR allows for granular permissions, which means you can configure which roles have the ability to execute playbooks, and by restricting this capability, you can control which users are able to initiate playbook runs.

NEW QUESTION # 19
.....