Free PDF Quiz 2026 Reliable SPLK-2003: Splunk Phantom Certified Admin Valid Study Notes

BTW, DOWNLOAD part of PracticeDump SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1qBKjzIBrWhdQvMeASS3MVTnlda4gdsBB

What is more difficult is not only passing the Financials in Splunk Phantom Certified Admin (SPLK-2003) certification exam, but the acute anxiety and the excessive burden also make the candidate nervous to qualify for the Splunk Phantom Certified Admin (SPLK-2003) certification. If you are going through the same tough challenge, do not worry because PracticeDump is here to assist you.

Splunk SPLK-2003 (Splunk Phantom Certified Admin) Certification Exam is designed to test the knowledge and skills of professionals who are interested in becoming certified as an administrator in the Splunk Phantom platform. Splunk Phantom Certified Admin certification is recognized globally and is highly regarded in the IT industry. SPLK-2003 Exam is divided into multiple sections, and candidates are expected to demonstrate their proficiency in each section to obtain the certification.

>> SPLK-2003 Valid Study Notes <<

SPLK-2003 Preparation Materials and Study Guide: Splunk Phantom Certified Admin - PracticeDump

After you purchase our SPLK-2003 exam guide is you can download the test bank you have bought immediately. You only need 20-30 hours to learn and prepare for the exam, because it is enough for you to grasp all content of our study materials, and the passing rate is very high and about 98%-100%. Our laTest SPLK-2003 Quiz torrent provides 3 versions and you can choose the most suitable one for you to learn. All in all, there are many merits of our SPLK-2003 quiz prep.

The SPLK-2003 certification exam is aimed at IT professionals who are responsible for managing Splunk Phantom in an enterprise environment. This includes security analysts, incident response teams, and IT administrators. Splunk Phantom Certified Admin certification is also useful for consultants and professionals who work with clients to implement and manage Splunk Phantom. The SPLK-2003 Certification is a valuable credential that demonstrates a candidate's expertise in Splunk Phantom administration and can help to advance their career in the field of security operations and incident response.

Splunk Phantom Certified Admin Sample Questions (Q64-Q69):

NEW QUESTION # 64
On a multi-tenant Phantom server, what is the default tenant's ID?

- A. 0
- B. *
- C. Default
- D. 1

Answer: D

Explanation:

The default tenant's ID is 1. The tenant ID is a unique identifier for each tenant on a multi-tenant Phantom server. The default tenant is the tenant that is created when Phantom is installed and contains all the existing data and assets. The default tenant's ID is always 1 and cannot be changed. Other tenants have IDs that are assigned sequentially starting from 2.
In a multi-tenant Splunk SOAR environment, the default tenant is typically assigned an ID of 1.
This ID is system-generated and is used to uniquely identify the default tenant within the SOAR database and system configurations. The default tenant serves as the primary operational environment before any additional tenants are configured, and its ID is crucial for database operations, API calls, and internal reference within the SOAR platform. Understanding and correctly using tenant IDs is essential for managing resources, permissions, and data access in a multi-tenant SOAR setup.

NEW QUESTION # 65
Which of the following describes the use of labels in Phantom?

- A. Labels control which apps are allowed to execute actions on the container.
- B. Labels determine the service level agreement (SLA) for a container.
- C. Labels control the default seventy, ownership, and sensitivity for the container.
- D. Labels determine which playbook(s) are executed when a container is created.

Answer: D

Explanation:
In Splunk Phantom, labels are used to categorize containers and trigger specific automated responses. When a container is created, labels can be assigned to it based on the nature of the event, type of incident, or other criteria. These labels are then matched against playbooks, which have label conditions defined within them.
When the conditions are met, the corresponding playbooks are automatically executed. Labels do not directly control service level agreements, default severity, ownership, sensitivity, or app execution permissions.

NEW QUESTION # 66
To limit the impact of custom code on the VPE, where should the custom code be placed?

- A. A separate container.
- B. A custom container or a separate KV store.
- C. A custom function block.
- D. A separate code repository.

Answer: C

Explanation:
To limit the impact of custom code on the Visual Playbook Editor (VPE) in Splunk SOAR, custom code should be placed within a custom function block. Custom function blocks are designed to encapsulate code within a playbook, allowing users to input their own Python code and execute it as part of the playbook run.
By confining custom code to these blocks, it maintains the VPE's performance and stability by isolating the custom code from the core functions of the playbook.
A custom function block is a way of adding custom Python code to your playbook, which can expand the functionality and processing of your playbook logic. Custom functions can also interact with the REST API in a customizable way. You can share custom functions across your team and across multiple playbooks to increase collaboration and efficiency. To create custom functions, you must have Edit Code permissions, which can be configured by an Administrator in Administration > User Management > Roles and Permissions. Therefore, option C is the correct answer, as it is the recommended way of placing custom code on the VPE, which limits the impact of custom code on the VPE performance and security. Option A is incorrect, because a custom container or a separate KV store are not valid ways of placing custom code on the VPE, but rather ways of storing data or artifacts. Option B is incorrect, because a separate code repository is not a way of placing custom code on the VPE, but rather a way of managing and versioning your code outside of Splunk SOAR. Option D is incorrect, because a separate container is not a way of placing custom code on the VPE, but rather a way of creating a new event or case.
1: Add custom code to your Splunk SOAR (Cloud) playbook with the custom function block using the classic playbook editor

NEW QUESTION # 67
Which of the following will show all artifacts that have the term results in a filePath CEF value?

- A. ...rest/artifacts/filePath="%results%"
- B. .../rest/artifact?_filter_cef_filePath_icontain="results"
- C. .../result/artifacts/cef/filePath= '%results%"
- D. .../result/artifact?_query_cef_filepath_icontains="results

Answer: B

Explanation:
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.

NEW QUESTION # 68
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. Make sure the Execute Playbook capability is removed from all roles except admin.
- B. Add a tag with restricted access to the restricted playbooks.
- C. Add a filter block to all restricted playbooks that filters for runRole = "Admin".
- D. Place restricted playbooks in a second source repository that has restricted access.

Answer: A

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 # 69
.....

- SPLK-2003 Valid Dumps Files □ SPLK-2003 Accurate Test □ Latest SPLK-2003 Dumps Free □ Immediately open ✔ www.pdfvce.com □✔□ and search for { SPLK-2003 } to obtain a free download □Pass4sure SPLK-2003 Study Materials
- Newest SPLK-2003 Valid Study Notes Offer You The Best New Braindumps Pdf | Splunk Splunk Phantom Certified Admin □ Search for ➤ SPLK-2003 □ on { www.prep4away.com } immediately to obtain a free download □Reliable SPLK-2003 Test Preparation
- Free PDF High-quality SPLK-2003 - Splunk Phantom Certified Admin Valid Study Notes □ Search for 《 SPLK-2003 》 and easily obtain a free download on ☀ www.pdfvce.com □☀□ □New SPLK-2003 Exam Duration
- SPLK-2003 Test Price □ New SPLK-2003 Exam Question □ SPLK-2003 Exam Certification □ Download （ SPLK-2003 ） for free by simply entering □ www.exam4labs.com □ website □Free SPLK-2003 Sample
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, iatdacademy.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, k12.instructure.com, www.fanart-central.net, bbs.t-firefly.com, bbs.t-firefly.com, emanubrain.com, Disposable vapes

BTW, DOWNLOAD part of PracticeDump SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1qBKjzIBrWhdQvMeASS3MVTnlda4gdsBB