SPLK-2003 Valid Test Online | Reliable SPLK-2003 Dumps Files

BONUS!!! Download part of FreeCram SPLK-2003 dumps for free: https://drive.google.com/open?id=1OncAjL5J1iyaoDAk3Iwl9jVGy9Q77Zdf

If you are preparing for the Splunk Phantom Certified Admin (SPLK-2003) exam dumps our SPLK-2003 Questions help you to get high scores in your Splunk SPLK-2003 exam. Test your knowledge of the Splunk Phantom Certified Admin exam dumps with FreeCram Splunk SPLK-2003 Practice Questions. The software is designed to help with SPLK-2003 exam dumps preparation.

Splunk Phantom Certified Admin Exam is a great way to demonstrate your expertise in Splunk Phantom and its administration. It is a valuable credential that can help you advance your career in the IT industry. Splunk Phantom Certified Admin certification also provides access to a community of certified professionals, where you can share knowledge, collaborate on projects, and network with peers.

>> SPLK-2003 Valid Test Online <<

Pass Guaranteed Splunk SPLK-2003 Marvelous Valid Test Online

Compared with those uninformed exam candidates who do not have effective preparing guide like our SPLK-2003 study braindumps, you have already won than them. Among wide array of choices, our products are absolutely perfect. Besides, from economic perspective, our SPLK-2003 Real Questions are priced reasonably so we made a balance between delivering satisfaction to customers and doing our own jobs. So in this critical moment, our SPLK-2003 prep guide will make you satisfied.

Splunk Phantom Certified Admin Sample Questions (Q84-Q89):

NEW QUESTION # 84
Which of the following is a best practice for use of the global block?

- A. Import packages which will be used within the playbook.
- B. Declare outputs which will be selectable within playbook blocks.
- C. Execute code at the beginning of each run of the playbook.
- D. Execute custom code after each run of the playbook.

Answer: A

Explanation:
Explanation
The correct answer is C because the global block can be used to import packages that will be used within the playbook. This can be useful for importing external libraries or custom modules that provide additional functionality or logic for the playbook. The answer A is incorrect because the global block cannot be used to execute code at the beginning of each run of the playbook, as the global block is only executed once when the playbook is loaded. The answer B is incorrect because the global block cannot be used to declare outputs that will be selectable within playbook blocks, as the outputs are declared in the individual blocks that produce them. The answer D is incorrect because the global block cannot be used to execute custom code after each run of the playbook, as the global block is only executed once when the playbook is loaded. Reference: Splunk SOAR Playbook Development Guide, page 34.

NEW QUESTION # 85
Which of the following accurately describes the Files tab on the Investigate page?

- A. Files tab items cannot be added to investigations. Instead, add them to action blocks.
- B. Phantom memory requirements remain static, regardless of Files tab usage.
- C. Files tab items and artifacts are the only data sources that can populate active cases.
- D. A user can upload the output from a detonate action to the the files tab for further investigation.

Answer: D

Explanation:
The Files tab on the Investigate page allows the user to upload, download, and view files related to an investigation. A user can upload the output from a detonate action to the Files tab for further investigation, such as analyzing the file metadata, content, or hash. Files tab items and artifacts are not the only data sources that can populate active cases, as cases can also include events, tasks, notes, and comments. Files tab items can be added to investigations by using the add file action block or the Add File button on the Files tab.
Phantom memory requirements may increase depending on the Files tab usage, as files are stored in the Phantom database.
The Files tab on the Investigate page in Splunk Phantom is an area where users can manage and analyze files related to an investigation. Users can upload files, such as outputs from a 'detonate file' action which analyzes potentially malicious files in a sandbox environment. The files tab allows users to store and further investigate these outputs, which can include reports, logs, or any other file types that have been generated or are relevant to the investigation. The Files tab is an integral part of the investigation process, providing easy access to file data for analysis and correlation with other incident data.

NEW QUESTION # 86
Splunk user account(s) with which roles must be created to configure SOAR with an external Splunk Enterprise instance?

- A. admin, user
- B. phantomsearch, phantomdelete
- C. superuser, administrator
- D. phantomcreate, phantomedit

Answer: B

NEW QUESTION # 87
On the Splunk search head, when configuring the app to search SOAR searchable content, what are the two requirements to complete the app setup?

- A. User accounts and an HTTP Event Collector token.
- B. User accounts and syslog.
- C. User accounts and universal forwarder.
- D. User accounts and REST API.

Answer: A

Explanation:
When configuring the Splunk app on the search head to search SOAR (Splunk's Security Orchestration, Automation, and Response) searchable content, two key components are required:
* User Accounts: The user accounts are necessary to authenticate and authorize users who are accessing SOAR data through the Splunk app. These accounts manage permissions and access levels to ensure the proper users can search and interact with the data coming from SOAR.
* HTTP Event Collector (HEC) Token: The HEC token is crucial because it allows the Splunk app to receive data from Splunk SOAR. SOAR sends events and other data to the Splunk platform via HEC.
This token is used for secure communication and authentication between Splunk and SOAR. The token must be configured in the Splunk app to allow it to collect and search SOAR data seamlessly.
Other options like syslog, REST API, or a universal forwarder are commonly used methods for ingesting data into Splunk but are not specific requirements for setting up the Splunk app to search SOAR content. The HTTP Event Collector is the primary method for this setup, along with the correct user accounts.

References:
* Splunk Documentation on HTTP Event Collector and SOAR Integration.
* Splunk SOAR App Setup Guide for Splunk Search Head Configuration.

NEW QUESTION # 88
A new project requires event data from SOAR to be sent to an external system via REST. All events with the label notable that are in new status should be sent. Which of the following REST Django expressions will select the correct events?

- A.
- B.
- C.
- D.

Answer: C

Explanation:
The correct REST Django expression to retrieve events with the label "notable" that are in the "new" status is using the container endpoint, as containers are used to store events and associated data in Splunk SOAR. The expression correctly filters the events by label (_filter_label="notable") and status (_filter_status="new"), ensuring only notable events that are still in the "new" status are selected.
A and D reference the wrong endpoints (event and notable respectively), which do not align with the container-based model used in Splunk SOAR for storing and filtering events.
B is incorrect due to the use of _filter_name instead of _filter_label, which is not a valid filter in this context.
References:
Splunk SOAR Documentation: REST API Endpoints.
Splunk SOAR Developer Guide: Using Django REST for Filtering.

NEW QUESTION # 89
.....

- SPLK-2003 Trustworthy Exam Torrent □ Test SPLK-2003 Sample Online □ SPLK-2003 Test Dumps Free ✔ Search for ➥ SPLK-2003 □ and easily obtain a free download on "www.pdfvce.com" □SPLK-2003 Real Exam
- 2026 Unparalleled SPLK-2003 Valid Test Online Help You Pass SPLK-2003 Easily □ Search for （ SPLK-2003 ） and obtain a free download on ➡ www.validtorrent.com □□□ □Dumps SPLK-2003 Download
- www.stes.tyc.edu.tw, 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, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of FreeCram SPLK-2003 dumps for free: https://drive.google.com/open?id=1OncAjL5J1iyaoDAk3Iwl9jVGy9Q77Zdf