SPLK-2003 Pdf Files & New SPLK-2003 Test Prep

BONUS!!! Download part of ActualCollection SPLK-2003 dumps for free: https://drive.google.com/open?id=1bBvZppvcC9zO5hJcKVGd5NHgJBi6hVGx

These Splunk SPLK-2003 exam questions give you an idea about the final Splunk SPLK-2003 exam questions formats, exam question structures, and best possible answers, and you will also enhance your exam time management skills. Finally, at the end of Splunk SPLK-2003 Exam Practice test you will be ready to pass the final Splunk SPLK-2003 exam easily. Best of luck in Splunk Splunk exam and professional career!!!

Passing the SPLK-2003 certification exam demonstrates that the candidate has the necessary knowledge and skills to effectively manage and support Splunk Phantom deployments. It also indicates that the candidate understands how to use Splunk Phantom to streamline incident response, automate repetitive tasks, and integrate with other security tools.

Splunk SPLK-2003 exam is designed for IT professionals who want to become certified Splunk Phantom administrators. SPLK-2003 Exam Tests the candidate's knowledge of the Splunk Phantom platform and their ability to configure and manage it effectively. It covers a range of topics, including the architecture of the platform, installation and configuration, automation and orchestration, and advanced features such as custom actions and integrations.

>> SPLK-2003 Pdf Files <<

New Splunk SPLK-2003 Test Prep - SPLK-2003 Authorized Exam Dumps

There are totally three versions of SPLK-2003 practice materials which are the most suitable versions for you: PDF, Software and APP online versions. We promise ourselves and exam candidates to make these Splunk Phantom Certified Admin SPLK-2003 Learning Materials top notch. So if you are in a dark space, our Splunk SPLK-2003 exam questions can inspire you make great improvements.

Splunk Phantom platform is a powerful tool for automating IT processes and securing your organization's digital assets. By becoming a certified Splunk Phantom admin, you will gain the skills and knowledge necessary to leverage the full potential of this platform. Splunk Phantom Certified Admin certification is recognized globally and demonstrates to employers that you have the expertise to manage and automate complex IT processes using the Splunk Phantom platform.

Splunk Phantom Certified Admin Sample Questions (Q81-Q86):

NEW QUESTION # 81
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 # 82
After a playbook has run, where are the results stored?

- A. Container
- B. Log file
- C. Splunk Index
- D. Case

Answer: A

Explanation:
The correct answer is C because after a playbook has run, the results are stored in the container that triggered the playbook. The container is a data object that represents an event or a case in Phantom. The container contains information such as the name, the description, the severity, the status, the owner, and the labels of the event or case. The container also contains the artifacts, the action results, the comments, the notes, and the phases and tasks associated with the event or case. The answer A is incorrect because after a playbook has run, the results are not stored in a Splunk index, which is a data structure that stores events from various data sources in Splunk. The Splunk index is not directly accessible by Phantom, but can be queried by Phantom using the Splunk app. The answer B is incorrect because after a playbook has run, the results are not stored in a case, which is a type of container that represents a security incident in Phantom. The case is a subset of the container, and not all containers are cases. The answer D is incorrect because after a playbook has run, the results are not stored in a log file, which is a file that records the activities or events that occur in a system or a process. The log file is not a data object in Phantom, but can be a data source for Phantom.
Reference: Splunk SOAR User Guide, page 19. In Splunk Phantom, after a playbook has been executed, the results of the actions within that playbook are stored in the container associated with the event. A container is a data structure that encapsulates all relevant information and data for an incident or event within Phantom, including action results, artifacts, notes, and more. The container allows users to see a consolidated view of all the data and activity related to a particular event. These results are not stored in the Splunk Index, a separate case, or a log file as their primary storage but may be sent to a Splunk index for further analysis.

NEW QUESTION # 83
Splunk user account(s) with which roles must be created to configure SOAR with an external Splunk Enterprise instance?

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

Answer: D

NEW QUESTION # 84
Which of the following describes the use of labels m 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 determine which playbook(s) are executed when a container is created.
- D. Labels control the default seventy, ownership, and sensitivity for the container.

Answer: C

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 # 85
What users are included in a new installation of SOAR?

- A. The admin and automation users are included by default.
- B. Only the admin user is included by default.
- C. No users are included by default.
- D. The admin, power, and user users are included by default.

Answer: A

Explanation:
In a new installation of Splunk SOAR, two default user accounts are typically created: admin and automation. The admin account is intended for system administration tasks, providing full access to all features and settings within the SOAR platform. The automation user is a special account used for automated processes and scripts that interact with the SOAR platform, often without requiring direct human intervention. This user has specific permissions that can be tailored for automated tasks.

NEW QUESTION # 86
......

- 100% Pass 2026 SPLK-2003: Splunk Phantom Certified Admin Perfect Pdf Files □ Copy URL “ www.practicevce.com ” open and search for ➤ SPLK-2003 □ to download for free □Test SPLK-2003 Valid
- Accurate SPLK-2003 Study Material □ Customizable SPLK-2003 Exam Mode □ SPLK-2003 Valid Exam Answers □ Go to website 《 www.pdfvce.com 》 open and search for ➠ SPLK-2003 □ to download for free □Certification SPLK-2003 Test Questions
- 100% Pass 2026 SPLK-2003: Splunk Phantom Certified Admin Perfect Pdf Files □ Open ➠ www.pdfdumps.com □ and search for □ SPLK-2003 □ to download exam materials for free □Customizable SPLK-2003 Exam Mode
- SPLK-2003 Reliable Exam Question □ SPLK-2003 Valid Exam Answers □ Certification SPLK-2003 Test Questions □ Search for 《 SPLK-2003 》 and download it for free immediately on [www.pdfvce.com] □Customizable SPLK-2003 Exam Mode
- SPLK-2003 Pdf Files - 100% Pass 2026 SPLK-2003: First-grade New Splunk Phantom Certified Admin Test Prep □ Search for □ SPLK-2003 □ and download it for free immediately on ➽ www.prep4sures.top □ □Valid SPLK-2003 Test Question
- Customizable SPLK-2003 Exam Mode □ SPLK-2003 New Practice Questions □ Dumps SPLK-2003 Questions □ Open website （ www.pdfvce.com ） and search for 【 SPLK-2003 】 for free download □Reliable SPLK-2003 Test Question
- Quick Tips for Exam Success using Splunk SPLK-2003 Questions □ Easily obtain free download of ▶ SPLK-2003 ◀ by searching on ➡ www.testkingpass.com □□□ □Certification SPLK-2003 Test Questions
- p.me-page.com, myportal.utt.edu.tt, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, Disposable vapes

DOWNLOAD the newest ActualCollection SPLK-2003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1bBvZppvcC9zO5hJcKVGd5NHgJBi6hVGx