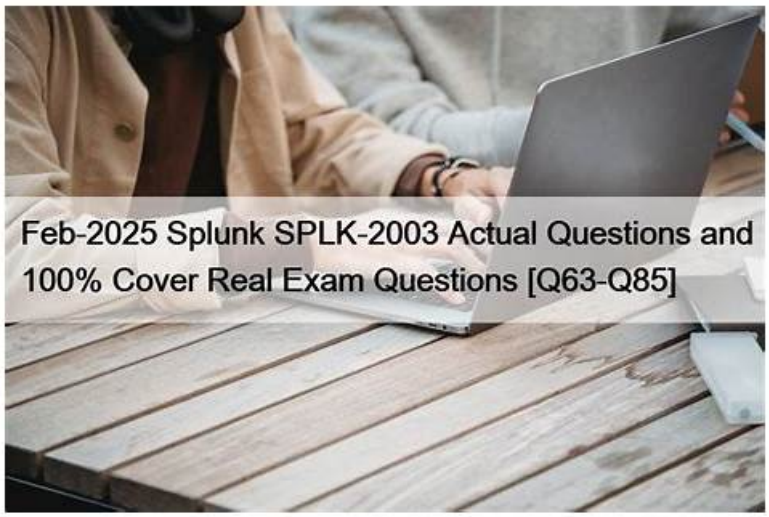
SPLK-2003 Actual Test Answers - Useful SPLK-2003 Dumps



What's more, part of that ValidVCE SPLK-2003 dumps now are free: https://drive.google.com/open?id=13sBM-x-dibV5tCRmsXsxhaYa90dqtAOX

As the old saying goes, practice is the only standard to testify truth. In other word, it has been a matter of common sense that pass rate of the SPLK-2003 study materials is the most important standard to testify whether it is useful and effective for people to achieve their goal. We believe that you must have paid more attention to the pass rate of the SPLK-2003 study materials. If you focus on the study materials from our company, you will find that the pass rate of our products is higher than other study materials in the market, yes, we have a 99% pass rate, which means if you take our the SPLK-2003 Study Materials into consideration, it is very possible for you to pass your exam and get the related certification.

Splunk SPLK-2003 exam consists of 60 multiple-choice questions and must be completed within 90 minutes. Candidates must achieve a passing score of 70% or higher to earn the Splunk Phantom Certified Admin certification. SPLK-2003 exam covers a range of topics, including Phantom architecture, installation and configuration, workflow management, playbook creation and configuration, and integration with other security tools. Successful candidates will be able to demonstrate their ability to use Splunk Phantom to automate security operations workflows, streamline incident response, and improve overall security posture. The Splunk SPLK-2003 Certification is an excellent way for security professionals to validate their skills and expertise in Splunk Phantom and advance their careers in the security automation and orchestration field.

To prepare for the SPLK-2003 exam, candidates are recommended to take the Splunk Phantom Certified Admin course. This course covers all the topics that are included in the certification exam and provides hands-on experience in administering the Splunk Phantom platform. Candidates can also access a range of study materials, including practice exams and online forums, to help them prepare for the exam.

>> SPLK-2003 Actual Test Answers <<

Easy to use Formats of ValidVCE Splunk SPLK-2003 Practice Exam Material

You can use this Splunk SPLK-2003 version on any operating system, and this software is accessible through any browser like Opera, Safari, Chrome, Firefox, and IE. You can easily assess yourself with the help of our SPLK-2003 practice software, as it records all your previous results for future use.

Splunk SPLK-2003 (Splunk Phantom Certified Admin) Exam is an essential certification for professionals who want to demonstrate their proficiency in the administration of Splunk Phantom. Splunk Phantom Certified Admin certification exam covers various topics such as playbook management, automation workflows, and integration with other security tools. Passing the exam will provide candidates with an opportunity to enhance their career prospects and showcase their skills in the field of cybersecurity.

Splunk Phantom Certified Admin Sample Questions (Q59-Q64):

NEW QUESTION # 59
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

- A. Map CIM to CEF fields.
- B. Map CEF to CIM fields.
- C. Create a saved search that generates the JSON for the new container on Phantom.
- D. Create a Splunk alert that uses the event_forward.py script to send events to Phantom.

Answer: D

Explanation:
A step when configuring event forwarding from Splunk to Phantom is to create a Splunk alert that uses the event_forward.py script to send events to Phantom. This script will convert the Splunk events to CEF format and send them to Phantom as containers. The other options are not valid steps for event forwarding.
Configuring event forwarding from Splunk to Phantom typically involves creating a Splunk alert that leverages a script (like event_forward.py) to automatically send triggered event data to Phantom. This setup enables Splunk to act as a detection mechanism that, upon identifying notable events based on predefined criteria, forwards these events to Phantom for further orchestration, automation, and response actions. This integration streamlines the process of incident management by connecting Splunk's powerful data analysis capabilities with Phantom's orchestration and automation framework.

NEW QUESTION # 60
What are indicators?

- A. Action result items that determine the flow of execution in a playbook.
- B. Artifact values with special security significance.
- C. Action results that may appear in multiple containers.
- D. Artifact values that can appear in multiple containers.

Answer: B

Explanation:
Indicators within the context of Splunk SOAR refer to artifact values that have special security significance.
These are typically derived from the data within artifacts and are identified as having particular importance in the analysis and investigation of security incidents. Indicators might include items such as IP addresses, domain names, file hashes, or other data points that can be used to detect, correlate, and respond to security threats. Recognizing and managing indicators effectively is key to leveraging SOAR for enhanced threat intelligence, incident response, and security operations efficiency.

NEW QUESTION # 61
Which of the following can be configured in the ROI Settings?

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

Answer: D

Explanation:
The ROI (Return on Investment) Settings within Splunk SOAR are designed to help organizations assess the value derived from their use of the platform, particularly in terms of resource allocation and efficiency gains. The setting mentioned in the question, "Number of full time employees (FTEs)," relates directly to measuring this efficiency.
Answer "C" is correct because configuring the number of full-time employees (FTEs) in the ROI settings allows an organization to input and monitor how many personnel are dedicated to security operations managed through SOAR. This setting is crucial for calculating the labor cost associated with incident response and routine security tasks. By understanding the number of FTEs involved, organizations can better assess the labor cost savings provided by automation and orchestration in SOAR. This data helps in quantifying the operational efficiency and the overall impact of SOAR on resource optimization.
In contrast, other options like "Analyst hours per month," "Time lost," and "Annual analyst salary" might seem relevant but are not

directly configurable within the ROI settings of Splunk SOAR.
These aspects could be indirectly calculated or estimated based on the number of FTEs and other operational metrics but are not directly input as settings in the system.
This use of FTEs in ROI calculations is often discussed in materials related to cybersecurity efficiency metrics and SOAR platform utilization. Official Splunk documentation and best practices guides typically provide insights into how to set up and interpret ROI settings, highlighting the importance of accurate configuration for meaningful analytics.

NEW QUESTION # 62
Splunk user account(s) with which roles must be created to configure Phantom with an external Splunk Enterprise instance?

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

Answer: B

Explanation:
When configuring Splunk Phantom to integrate with an external Splunk Enterprise instance, it is typically required to have user accounts with sufficient privileges to access data and perform necessary actions. The roles of "superuser" and "administrator" in Splunk provide the broad set of permissions needed for such integration, enabling comprehensive access to data, management capabilities, and the execution of searches or actions that Phantom may require as part of its automated playbooks or investigations.

NEW QUESTION # 63
What is the default embedded search engine used by Phantom?

- A. Embedded Phantom search engine.
- B. Embedded Splunk search engine.
- C. Embedded Elastic search engine.
- D. Embedded Django search engine.

Answer: B

Explanation:
The default embedded search engine used by Splunk SOAR (formerly known as Phantom) is the embedded Splunk search engine.
Here's a detailed explanation:
Embedded Splunk Search Engine:
Splunk SOAR uses an embedded, preconfigured version of Splunk Enterprise as its native search engine.
This integration allows for powerful searching capabilities within Splunk SOAR, leveraging Splunk's robust search and indexing features.
Search Configuration:
While the embedded Splunk search engine is the default, organizations have the option to configure Splunk SOAR to use a different Splunk Enterprise deployment or an external Elasticsearch instance.
This flexibility allows organizations to tailor their search infrastructure to their specific needs and existing environments.
Search Capabilities:
The embedded Splunk search engine enables users to perform complex searches, analyze data, and generate reports directly within the Splunk SOAR platform.
It supports the full range of Splunk's search processing language (SPL) commands, functions, and visualizations.
References:
Splunk SOAR Documentation: Configure search in Splunk Phantom1.
Splunk SOAR Documentation: Configure search in Splunk SOAR (On-premises)2.
In summary, the embedded Splunk search engine is the default search engine in Splunk SOAR, providing a seamless and powerful search experience for users within the platform.

NEW QUESTION # 64
.....

Useful SPLK-2003 Dumps: https://www.validvce.com/SPLK-2003-exam-collection.html

- 100% Pass Fantastic SPLK-2003 - Splunk Phantom Certified Admin Actual Test Answers □ Download ▹ SPLK-2003 ◃ for free by simply searching on { www.troytecdumps.com } □SPLK-2003 Exam Simulator
- Pass Guaranteed Quiz SPLK-2003 - Splunk Phantom Certified Admin –The Best Actual Test Answers □ Immediately open ➤ www.pdfvce.com □ and search for { SPLK-2003 } to obtain a free download □Latest SPLK-2003 Dumps Files
- Free PDF Quiz 2026 Pass-Sure Splunk SPLK-2003 Actual Test Answers □ Enter 《 www.dumpsmaterials.com 》 and search for ☀ SPLK-2003 □☀□ to download for free □Latest SPLK-2003 Dumps Files
- SPLK-2003 Training Tools □ Certification SPLK-2003 Training □ SPLK-2003 Exam Review □ Search for 《 SPLK-2003 》 and download it for free on ➡ www.pdfvce.com □□□ website □SPLK-2003 Practice Mock
- Exam SPLK-2003 Collection Pdf □ Reliable SPLK-2003 Practice Questions Ⓜ SPLK-2003 Practice Mock □ Search for ▹ SPLK-2003 ◃ and download it for free immediately on { www.validtorrent.com } □Dumps SPLK-2003 Collection
- 100% Pass Fantastic SPLK-2003 - Splunk Phantom Certified Admin Actual Test Answers □ Open website □ www.pdfvce.com □ and search for 《 SPLK-2003 》 for free download □Test SPLK-2003 Sample Questions
- Latest SPLK-2003 Exam Materials □ SPLK-2003 Latest Guide Files □ SPLK-2003 Practice Mock □ Search for □ SPLK-2003 □ and download exam materials for free through 「 www.practicevce.com 」 □Reliable SPLK-2003 Practice Questions
- SPLK-2003 Accurate Test □ SPLK-2003 Latest Guide Files □ Latest SPLK-2003 Exam Materials □ Search on ✔ www.pdfvce.com □✔□ for （ SPLK-2003 ） to obtain exam materials for free download ⤴SPLK-2003 New Study Notes
- Dumps SPLK-2003 Collection □ Reliable SPLK-2003 Practice Questions □ Certification SPLK-2003 Training □ Enter ➡ www.torrentvce.com □□□ and search for □ SPLK-2003 □ to download for free □SPLK-2003 Reliable Torrent
- Pass Guaranteed Quiz SPLK-2003 - Splunk Phantom Certified Admin –The Best Actual Test Answers □ The page for free download of □ SPLK-2003 □ on [www.pdfvce.com] will open immediately □SPLK-2003 Practice Exam Online
- SPLK-2003 Exam Cram Questions □ SPLK-2003 Exam Cram Questions □ SPLK-2003 Exam Simulator □ Search for ✔ SPLK-2003 □✔□ and download exam materials for free through ▸ www.dumpsquestion.com ◂ □SPLK-2003 Training Tools
- 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, bicyclebuysell.com, 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, Disposable vapes

DOWNLOAD the newest ValidVCE SPLK-2003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=13sBM-x-dibV5tCRmsXsxhaYa90dqtAOX