Splunk Phantom Certified Admin pdf test & SPLK-2003 test dumps

P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by TorrentVCE: https://drive.google.com/open?id=1rDOn_x67nW_jfi4TbfIgbpJVcIv6WAIR

With the cumulative effort over the past years, our SPLK-2003 study guide has made great progress with passing rate up to 98 to 100 percent among the market. A lot of professional experts concentrate to making our SPLK-2003preparation materials by compiling the content so they have gained reputation in the market for their proficiency and dedication. About some esoteric points, they illustrate with examples for you on the SPLK-2003 Exam Braindumps.

To become certified, candidates must pass the SPLK-2003 Exam with a score of at least 70%. SPLK-2003 exam consists of 60 multiple-choice questions and has a time limit of 90 minutes. The questions are designed to test the candidate's knowledge of the Phantom platform and their ability to apply that knowledge to real-world scenarios.

The Splunk SPLK-2003 exam is designed for individuals who have a basic understanding of Splunk Phantom. Having experience with scripting languages and a basic understanding of networking, cybersecurity, and incident response is recommended. Given the popularity and demand for SOAR solutions, the certification also benefits those who wish to specialize in the niche area of SOAR technology.

>> Valid Braindumps SPLK-2003 Files <<

SPLK-2003 Exam Demo - SPLK-2003 Examcollection Dumps

In order to provide the best SPLK-2003 test training guide for all people, our company already established the integrate quality

manage system, before sell serve and promise after sale. If you buy the SPLK-2003 preparation materials from our company, we can make sure that you will have the right to enjoy the 24 hours full-time online service on our SPLK-2003 Exam Questions. In order to help the customers solve the problem at any moment, our server staff will be online all the time give you the suggestions on SPLK-2003 study guide.

The SPLK-2003 certification exam is a proctored exam that consists of 60 multiple-choice questions. Candidates have two hours to complete the exam and must achieve a score of 70% or higher to pass. SPLK-2003 Exam is available in English and Japanese and can be taken at any Pearson VUE testing center worldwide.

Splunk Phantom Certified Admin Sample Questions (Q27-Q32):

NEW QUESTION # 27
Which of the following accurately describes the Files tab on the Investigate page?

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

Answer: B

Explanation:
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. Reference, page 23.

NEW QUESTION # 28
Which app allows a user to run Splunk queries from within Phantom?

- A. Splunk App for Phantom Reporting.
- B. Splunk App for Phantom?
- C. Phantom App for Splunk.
- D. The Integrated Splunk/Phantom app.

Answer: B

Explanation:
The Splunk App for Phantom allows users to run Splunk queries directly from within the Phantom platform. This app facilitates the integration between Splunk and Phantom, enabling users to post data to Splunk as events, update notable events, run SPL (Search Processing Language) queries, and pull events from Splunk into Phantom. By configuring the asset settings and ingest settings in the configured asset, users can leverage the full capabilities of Splunk within the Phantom environment.

NEW QUESTION # 29
Which of the following can the format block be used for?

- A. To generate arrays for input into other functions.
- B. To create text strings that merge state text with dynamic values for input or output.
- C. To generate string parameters for automated action blocks.
- D. To generate HTML or CSS content for output in email messages, user prompts, or comments.

Answer: B

Explanation:
The format block in Splunk SOAR is utilized to construct text strings by merging static text with dynamic values, which can then be used for both input to other playbook blocks and output for reports, emails, or other forms of communication. This capability is

essential for customizing messages, commands, or data processing tasks within a playbook, allowing for the dynamic insertion of variable data into predefined text templates.
This feature enhances the playbook's ability to present information clearly and to execute actions that require specific parameter formats.

NEW QUESTION # 30
Why is it good playbook design to create smaller and more focused playbooks? (select all that apply)

- A. To avoid duplication of code across multiple playbooks.
- B. Reduce large complex playbooks which become difficult to maintain.
- C. Reduces amount of playbook data stored in each repo.
- D. Encourages code reuse in a more compartmentalized form.

Answer: A,B,D

Explanation:
Creating smaller and more focused playbooks in Splunk SOAR is considered good design practice for several reasons:
*B: It reduces complexity, making playbooks easier to maintain. Large, complex playbooks can become unwieldy and difficult to troubleshoot or update.
*C: Encourages code reuse, as smaller playbooks can be designed to handle specific tasks that can be reused across different scenarios.
*D: Avoids duplication of code, as common functionalities can be centralized within specific playbooks, rather than having the same code replicated across multiple playbooks.
This approach has several benefits, such as:
*Reducing large complex playbooks which become difficult to maintain. Smaller playbooks are easier to read, debug, and update1.
*Encouraging code reuse in a more compartmentalized form. Smaller playbooks can be used as building blocks for multiple scenarios, reducing the need to write duplicate code12.
*Improving performance and scalability. Smaller playbooks can run faster and consume less resources than larger playbooks2.
The other options are not valid reasons for creating smaller and more focused playbooks. Reducing the amount of playbook data stored in each repo is not a significant benefit, as the playbook data is not very large compared to other types of data in Splunk SOAR. Avoiding duplication of code across multiple playbooks is a consequence of code reuse, not a separate goal.

NEW QUESTION # 31
On a multi-tenant Phantom server, what is the default tenant's ID?

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

Answer: C

Explanation:
The correct answer is C because 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. See Splunk SOAR Documentation for more details. 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 # 32
.....

- Valid SPLK-2003 Exam Sims □ Exam SPLK-2003 Online □ Exam SPLK-2003 Online □ Copy URL ⇛ www.prep4away.com ⇚ open and search for ▸ SPLK-2003 ◂ to download for free □SPLK-2003 Test Certification Cost
- Splunk SPLK-2003 Exam | Valid Braindumps SPLK-2003 Files - 100% Pass Rate Offer of SPLK-2003 Exam Demo □ Easily obtain free download of ➡ SPLK-2003 □□□ by searching on ➽ www.pdfvce.com □ □Latest SPLK-2003 Dumps Questions
- SPLK-2003 Valid Test Pdf ♣ SPLK-2003 Latest Exam Practice □ SPLK-2003 Valid Mock Exam □ Open ▹ www.examdiscuss.com ◃ and search for 「 SPLK-2003 」 to download exam materials for free □SPLK-2003 Actual Exam Dumps
- SPLK-2003 Exam Simulator □ SPLK-2003 Simulation Questions □ SPLK-2003 Accurate Answers □ Open ➤ www.pdfvce.com □ enter " SPLK-2003 " and obtain a free download □SPLK-2003 Actual Exam Dumps
- SPLK-2003 Exam Assessment □ Reliable SPLK-2003 Guide Files □ Latest SPLK-2003 Dumps Questions □ Enter ▹ www.troytecdumps.com ◃ and search for ➡ SPLK-2003 □□□ to download for free □SPLK-2003 Exam Simulator
- Test SPLK-2003 Testking □ Exam SPLK-2003 Online □ Sample SPLK-2003 Questions Answers □ Go to website ➥ www.pdfvce.com □ open and search for [SPLK-2003] to download for free □SPLK-2003 Test Certification Cost
- Track Your Progress with Splunk SPLK-2003 Practice Test □ Search for 《 SPLK-2003 》 and easily obtain a free download on 《 www.testkingpass.com 》 □SPLK-2003 Valid Mock Exam
- Free Updates For Splunk SPLK-2003 PDF Questions □ Download □ SPLK-2003 □ for free by simply searching on ➠ www.pdfvce.com □ □SPLK-2003 Valid Mock Exam
- Free Updates For Splunk SPLK-2003 PDF Questions □ ▹ www.prep4away.com ◃ is best website to obtain { SPLK-2003 } for free download □SPLK-2003 Exam Simulator
- Valid SPLK-2003 Exam Sims □ Vce SPLK-2003 Download □ Test SPLK-2003 Testking □ Copy URL ⇛ www.pdfvce.com ⇚ open and search for " SPLK-2003 " to download for free □SPLK-2003 Accurate Answers
- Test SPLK-2003 Testking □ SPLK-2003 Accurate Answers □ SPLK-2003 Simulation Questions □ Easily obtain free download of ☀ SPLK-2003 □☀□ by searching on ➡ www.vce4dumps.com □□□ □Free SPLK-2003 Practice
- 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, myportal.utt.edu.tt, pct.edu.pk, www.stes.tyc.edu.tw, study.stcs.edu.np, Disposable vapes

DOWNLOAD the newest TorrentVCE SPLK-2003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1rDOn_x67nW_jfi4TbfIgbpJVcIv6WAIR