DumpsMaterials's Splunk SPLK-2003 Practice Test Software (Web-Based and Desktop)

2025 Latest DumpsMaterials SPLK-2003 PDF Dumps and SPLK-2003 Exam Engine Free Share: https://drive.google.com/open?id=1-K1OCQnREmrr8HCPj-GaPX5MdG5HAeQf

DumpsMaterials is an excellent IT certification examination information website. In DumpsMaterials you can find exam tips and materials about Splunk certification SPLK-2003 exam. You can also free download part of examination questions and answers about Splunk SPLK-2003 in DumpsMaterials. DumpsMaterials will timely provide you free updates about Splunk SPLK-2003 exam materials. Besides, the exam materials we sold are to provide the answers. Our IT experts team will continue to take advantage of professional experience to come up with accurate and detailed exam practice questions to help you pass the exam. In short, we will provide you with everything you need about Splunk Certification SPLK-2003 Exam.

Whether you are good at learning or not, passing the exam can be a very simple and enjoyable matter together with our SPLK-2003 practice engine. As a professional multinational company, we fully take into account the needs of each user when developing our SPLK-2003 Exam Braindumps. For example, in order to make every customer can purchase at ease, our SPLK-2003 preparation quiz will provide users with three different versions for free trial, corresponding to the three official versions.

>> SPLK-2003 Valid Braindumps Ppt <<

Maximize Your Success with DumpsMaterials Customizable SPLK-2003 Splunk Phantom Certified Admin Practice Test

If you want to pass the SPLK-2003 exam, our SPLK-2003 practice questions are elemental exam material you cannot miss. It is proved by our loyal customers that our passing rate of SPLK-2003 practice materials has reached up to 98 to 100 percent up to now. Besides, free updates of SPLK-2003 Exam Torrent will be sent to your mailbox freely for one year, hope you can have a great experience during usage of our SPLK-2003 practice materials.

Splunk SPLK-2003: Splunk Phantom Certified Admin exam is designed for professionals who want to demonstrate their expertise in administering and managing the Splunk Phantom platform. SPLK-2003 exam is intended for individuals who have experience in managing and automating security operations using Splunk Phantom.

Splunk SPLK-2003 certification exam consists of multiple-choice questions that cover various aspects of Splunk Phantom administration. SPLK-2003 exam is designed to test the candidate's understanding of Splunk Phantom's architecture, deployment, configuration, and management. SPLK-2003 exam also covers topics related to Splunk Phantom's integrations with other technologies, such as security information and event management (SIEM) systems and security orchestration, automation and response (SOAR) solutions.

To prepare for the SPLK-2003 Exam, candidates should have a strong understanding of security operations and incident response processes. They should also be familiar with Splunk Phantom's architecture, features, and capabilities. Splunk offers a range of training courses and resources to help candidates prepare for the exam, including the Phantom Certified Admin Course and the Phantom Fundamentals eLearning course. Additionally, candidates can benefit from hands-on experience working with the platform and participating in Splunk's online community to learn from other users and experts. Obtaining the Splunk Phantom Certified Admin certification can help IT professionals advance their careers in security operations and demonstrate their expertise in using advanced

automation and orchestration tools to improve their organization's security posture.

Splunk Phantom Certified Admin Sample Questions (Q44-Q49):

NEW QUESTION # 44
Which of the following are the default ports that must be configured on Splunk to allow connections from SOAR?

- A. SplunkWeb (8088), SplunkD (8089), HTTP Collector (8000)
- B. SplunkWeb (8089), SplunkD (8088), HTTP Collector (8000)
- C. SplunkWeb (8000), SplunkD (8089), HTTP Collector (8088)
- D. SplunkWeb (8469), SplunkD (8702), HTTP Collector (8864)

Answer: C

Explanation:
For Splunk SOAR to connect with Splunk Enterprise, certain default ports must be configured to facilitate communication between the two platforms. Typically, SplunkWeb, which serves the Splunk Enterprise web interface, uses port 8000. SplunkD, the Splunk daemon that handles most of the back-end services, listens on port 8089. The HTTP Event Collector (HEC), which allows HTTP clients to send data to Splunk, typically uses port 8088. These ports are essential for the integration, allowing SOAR to send data to Splunk for indexing, searching, and visualization. Options A, B, and D list incorrect port configurations for this purpose, making option C the correct answer based on standard Splunk configurations.
These are the default ports used by Splunk SOAR (On-premises) to communicate with the embedded Splunk Enterprise instance. SplunkWeb is the web interface for Splunk Enterprise, SplunkD is the management port for Splunk Enterprise, and HTTP Collector is the port for receiving data from HTTP Event Collector (HEC).
The other options are either incorrect or not default ports. For example, option B has the SplunkWeb and SplunkD ports reversed, and option D has arbitrary port numbers that are not used by Splunk by default.

NEW QUESTION # 45
What are the differences between cases and events?

- A. Cases: only include high-level incident artifacts.
  Events: only include low-level incident artifacts.
- B. Cases: contain a collection of containers.
  Events: contain potential threats.
- C. Case: potential threats.
  Events: identified as a specific kind of problem and need a structured approach.
- D. Cases: incidents with a known violation and a plan for correction.
  Events: occurrences in the system that may require a response.

Answer: D

Explanation:
Explanation
Cases and events are two types of containers in Phantom. Cases are incidents with a known violation and a plan for correction, such as a malware infection, a phishing attack, or a data breach. Events are occurrences in the system that may require a response, such as an alert, a log entry, or an email. Cases and events can contain both high-level and low-level incident artifacts, such as IP addresses, URLs, files, or users. Cases do not contain a collection of containers, but rather a collection of artifacts, tasks, notes, and comments. Events are not necessarily potential threats, but rather indicators of potential threats. Reference, page 9.

NEW QUESTION # 46
If two or more conditions apply to data in a filter block, which path is followed in the playbook?

- A. All matching paths will be followed, but the first path to reach the end block will terminate the playbook.
- B. Only the first matching condition will activate its path.
- C. Only the last matching condition will activate its path.
- D. All paths with matching conditions are followed in parallel.

Answer: D

NEW QUESTION # 47
After a playbook has run, where are the results stored?

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

Answer: D

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 # 48
Two action blocks, geolocate_ip 1 and file_reputation_2, are connected to a decision block. Which of the following is a correct configuration for making a decision on the action results from one of the given blocks?

- A.


- B.


- C.


- D.


Answer: C

Explanation:
In the given decision block, you are trying to evaluate the results of two action blocks: geolocate_ip_1 and file_reputation_2. The correct configuration for making a decision based on the result of geolocate_ip_1 is by checking the country_iso_code field from the action result and setting the evaluation option to != (not equal), with no specific value provided in the "Select Value" box. This essentially checks whether a valid country ISO code exists in the action result and proceeds if it's not empty or different from a specific value. This is a common check when working with geolocation results to see if a response has been returned.
Other options (B, C, and D) include response codes or list comparisons, which do not align with the decision structure mentioned, which needs to operate based on a country_iso_code field.
References:
* Splunk SOAR Playbook Development Guide.

* Splunk SOAR Documentation on Decision Blocks and Action Result Evaluation.

NEW QUESTION # 49

.....

With constantly updated Splunk pdf files providing the most relevant questions and correct answers, you can find a way out in your industry by getting the SPLK-2003 certification. Our SPLK-2003 test engine is very intelligence and can help you experienced the interactive study. In addition, you will get the scores after each SPLK-2003 Practice Test, which can make you know about the weakness and strengthen about the SPLK-2003 real test , then you can study purposefully.

Pdf SPLK-2003 Braindumps: https://www.dumpsmaterials.com/SPLK-2003-real-torrent.html

- Free PDF Quiz Authoritative SPLK-2003 - Splunk Phantom Certified Admin Valid Braindumps Ppt □ Open website ➥ www.real4dumps.com □ and search for 《 SPLK-2003 》 for free download □Valid SPLK-2003 Test Voucher
- Free PDF Quiz Authoritative SPLK-2003 - Splunk Phantom Certified Admin Valid Braindumps Ppt □ Easily obtain free download of 「 SPLK-2003 」 by searching on ➥ www.pdfvce.com □ □SPLK-2003 Valid Test Prep
- Guaranteed SPLK-2003 Success □ SPLK-2003 Valid Exam Test □ SPLK-2003 Real Dump □ Easily obtain ▸ SPLK-2003 ◂ for free download through ☀ www.examsreviews.com □☀□ □SPLK-2003 Reliable Test Simulator
- Valid Braindumps SPLK-2003 Ppt ☀ SPLK-2003 Exam Cram Questions □ SPLK-2003 Latest Test Report □ Search for ⇛ SPLK-2003 ⇚ and download exam materials for free through 【 www.pdfvce.com 】 □SPLK-2003 Reliable Exam Topics
- SPLK-2003 Valid Braindumps Ppt - Splunk Splunk Phantom Certified Admin Realistic Valid Braindumps Ppt Pass Guaranteed □ Search for □ SPLK-2003 □ on [www.passcollection.com] immediately to obtain a free download □ □Valid SPLK-2003 Test Voucher
- SPLK-2003 Exam Cram Questions □ SPLK-2003 Test Questions □ New SPLK-2003 Exam Preparation □ Search for ⇛ SPLK-2003 ⇚ and download it for free immediately on [www.pdfvce.com] ☃Valid SPLK-2003 Test Prep
- Guaranteed SPLK-2003 Success □ SPLK-2003 Real Dump □ SPLK-2003 Test Questions □ Open website □ www.lead1pass.com □ and search for [SPLK-2003] for free download □Valid SPLK-2003 Test Prep
- Pass Guaranteed Quiz 2025 Splunk SPLK-2003: Splunk Phantom Certified Admin Useful Valid Braindumps Ppt □ Search for [SPLK-2003] and download it for free on 【 www.pdfvce.com 】 website □Valid Braindumps SPLK-2003 Ppt
- SPLK-2003 Valid Braindumps Ppt - Splunk Splunk Phantom Certified Admin Realistic Valid Braindumps Ppt Pass Guaranteed □ Immediately open ➠ www.lead1pass.com □ and search for " SPLK-2003 " to obtain a free download □SPLK-2003 Latest Test Answers
- Pass Guaranteed Quiz SPLK-2003 - Splunk Phantom Certified Admin Valid Braindumps Ppt □ Enter ▹ www.pdfvce.com ◃ and search for 【 SPLK-2003 】 to download for free □SPLK-2003 Valid Exam Test
- SPLK-2003 Valid Exam Test □ Dumps SPLK-2003 Reviews □ SPLK-2003 Reliable Exam Topics □ The page for free download of ✔ SPLK-2003 □✔□ on ➤ www.torrentvalid.com □ will open immediately □SPLK-2003 Latest Test Report
- shortcourses.russellcollege.edu.au, www.pcsq28.com, belajarformula.com, gxfk.fktime.com, mikemil988.mybuzzblog.com, app.360hcskills.com, academy.businesskul.com, frearn.com, benward394.webdesign96.com, mikemil988.blog4youth.com

DOWNLOAD the newest DumpsMaterials SPLK-2003 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1-K1OCQnREmrr8HCPj-GaPX5MdG5HAeQf