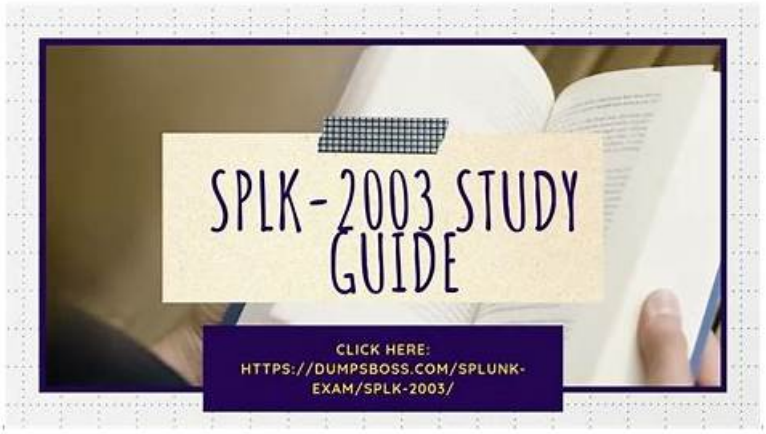
SPLK-2003 Latest Test Simulations - SPLK-2003 Study Guide



BTW, DOWNLOAD part of Actual4test SPLK-2003 dumps from Cloud Storage: https://drive.google.com/open?id=1SHCQcUN7jVscV4pXVyDivz_lL4UQGKDK

As we all know, examination is a difficult problem for most students, but getting the test SPLK-2003 certification and obtaining the relevant certificate is of great significance to the workers. Fortunately, however, you don't have to worry about this kind of problem anymore because you can find the best solution- SPLK-2003 practice materials. With our technology and ancillary facilities of the continuous investment and research, our company's future is a bright, the SPLK-2003 study tools have many advantages, and the pass rate of our SPLK-2003 exam questions is as high as 99% to 100%.

The Splunk Phantom Certified Admin certification exam consists of 60 multiple-choice questions that need to be completed within 90 minutes. The passing score for the exam is 70%. SPLK-2003 exam is available in English, Japanese, and Simplified Chinese. SPLK-2003 Exam Fee is $200 USD, and it can be taken online from anywhere in the world. Splunk Phantom Certified Admin certification is valid for two years, after which the candidate needs to retake the exam to maintain their certification status.

>> SPLK-2003 Latest Test Simulations <<

Splunk SPLK-2003 Study Guide, New SPLK-2003 Study Notes

Our top priority is to help every customer in cracking the Splunk Phantom Certified Admin (SPLK-2003) test. Therefore, we have created these formats so that every applicant can prepare successfully for the Splunk Phantom Certified Admin (SPLK-2003) exam on the first attempt. We are aware that the cost for the registration of the Splunk SPLK-2003 examination is not what everyone can pay. After paying the hefty Splunk Phantom Certified Admin (SPLK-2003) test registration fee, applicants usually run on a tight budget. This is why Actual4test provides you with the Splunk Phantom Certified Admin (SPLK-2003) real questions with up to 1 year of free updates.

Splunk SPLK-2003 Exam is a valuable certification for individuals who work with Splunk Phantom. SPLK-2003 exam tests the knowledge and skills of candidates in administering and maintaining Splunk Phantom in complex environments. Splunk Phantom Certified Admin certification provides a competitive advantage in the job market and validates the expertise of individuals in security orchestration, automation, and response.

Splunk Phantom platform is a security automation and orchestration solution that enables organizations to automate repetitive tasks, respond to security incidents quickly, and improve their overall security posture. The platform is designed to help security teams work more efficiently and effectively by automating manual tasks, integrating with other security tools, and enabling collaboration across teams.

Splunk Phantom Certified Admin Sample Questions (Q11-Q16):

NEW QUESTION # 11
Which of the following describes the use of labels m Phantom?

- A. Labels determine the service level agreement (SLA) for a container.

- B. Labels determine which playbook(s) are executed when a container is created.
- C. Labels control which apps are allowed to execute actions on the container.
- D. Labels control the default seventy, ownership, and sensitivity for the container.

Answer: B

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 # 12
How is it possible to evaluate user prompt results?

- A. Set the user prompt to reinvoke if it times out.
- B. Add a decision Mode
- C. Set action_result.summary. status to required.
- D. Set action_result. summary. response to required.

Answer: D

Explanation:
In Splunk Phantom, user prompts are actions that require human input. To evaluate the results of a user prompt, you can set the response requirement in the action result summary. By setting action_result.summary.response to required, the playbook ensures that it captures the user's input and can act upon it. This is critical in scenarios where subsequent actions depend on the choices made by the user in response to a prompt. Without setting this, the playbook would not have a defined way to handle the user response, which might lead to incorrect or unexpected playbook behavior.

NEW QUESTION # 13
Which of the following queries would return all artifacts that contain a SHA1 file hash?

- A. https://<PHANTOM_URL>/rest/artifact?_filter_cef_Shal_contains=""
- B. https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_insull=False
- C. https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_insull=false
- D. https://<PHANTOM_URL>/rest/artifact?_filter_shal__insull=False

Answer: B

Explanation:
To retrieve all artifacts containing a SHA1 file hash via the Splunk SOAR REST API, the appropriate query would filter for artifacts where the 'cef_sha1' field is not null, indicating that a SHA1 hash is present. The correct REST API call should use the filter parameter _filter_cef_shal__isnull=False (assuming 'shal' is a typo and it should be 'sha1'). This query parameter is used to filter out artifacts that do not have a SHA1 hash, thus returning only those that do.

NEW QUESTION # 14
What is the primary objective of using the I2A2 playbook design methodology?

- A. To create simple, reusable, modular playbooks.
- B. To create playbooks that customers will not edit.
- C. To create detailed playbooks.
- D. To meet customer requirements using a single playbook.

Answer: A

NEW QUESTION # 15
Which of the following queries would return all artifacts that contain a SHA1 file hash?

- A. https://<PHANTOM_URL>/rest/artifact?_filter_cef_Shal_contains=""
- B. https://<PHANTOM_URL>/rest/artifact?_filter_cef_shal_insull=False
- C. https://<PHANTOM_URL>/rest/artifact?_filter_cef_md5_insull=false
- D. https://<PHANTOM_URL>/rest/artifact?_filter_shal__insull=False

Answer: A

Explanation:
To return all artifacts that contain a SHA1 file hash using the Splunk SOAR REST API, the correct query would use the _filter_cef_Shal_contains parameter. This parameter filters the artifacts to only those that contain a value in the SHA1 field within the Common Event Format (CEF) data structure. The contains operator is used to match any artifacts that have a SHA1 hash present.

NEW QUESTION # 16
.....