Splunk SPLK-2003 Exam | Valid SPLK-2003 Exam Duration - Offer you Valid SPLK-2003 Pass Guarantee

P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by Dumpkiller: https://drive.google.com/open?id=1pUF9Vn9Q4ZyNZfJNDrlzjJ_YYaIf0IXJ

The industry experts hired by SPLK-2003 exam materials are those who have been engaged in the research of SPLK-2003 exam for many years. They have a keen sense of smell in the direction of the exam. Therefore, they can make accurate predictions on the exam questions. Therefore, our study materials specifically introduce a mock examination function. With SPLK-2003 exam materials, you can not only feel the real exam environment, but also experience the difficulty of the exam. You can test your true level through simulated exams. At the same time, after repeated practice of SPLK-2003 study braindumps, I believe that you will feel familiar with these questions during the exam and you will feel that taking the exam is as easy as doing exercises in peace.

Splunk SPLK-2003: Splunk Phantom Certified Admin Exam is one of the most sought-after certifications in the IT industry today. It is designed for professionals who want to prove their expertise in Splunk Phantom and its administration. Splunk Phantom Certified Admin certification validates the skills required to manage and maintain the Splunk Phantom platform, automate tasks, create playbooks, integrate with other systems, and troubleshoot issues.

>> Valid SPLK-2003 Exam Duration <<

SPLK-2003 Pass Guarantee | Latest SPLK-2003 Braindumps Files

Can you imagine that you only need to review twenty hours to successfully obtain the Splunk certification? Can you imagine that you don't have to stay up late to learn and get your boss's favor? With SPLK-2003 study materials, passing exams is no longer a dream. If you are an office worker, SPLK-2003 Study Materials can help you make better use of the scattered time to review. Just a mobile phone can let you do questions at any time.

Splunk Phantom Certified Admin Sample Questions (Q74-Q79):

NEW QUESTION # 74
Within the 12A2 design methodology, which of the following most accurately describes the last step?

- A. List of the outputs of the playbook design.
- B. List of the data needed to run the playbook.
- C. List of the apps used by the playbook.
- D. List of the actions of the playbook design.

Answer: A

Explanation:
The last step of the 12A2 design methodology is to list the outputs of the playbook design. The outputs are the expected results or outcomes of the playbook execution, such as sending an email, creating a ticket, blocking an IP, etc. The outputs should be aligned with the objectives and goals of the playbook.
The 12A2 design methodology in the context of Splunk SOAR (formerly Phantom) refers to a structured approach to developing playbooks. The last step in this methodology focuses on defining the outputs of the playbook design. This step is crucial as it outlines what the expected results or actions the playbook should achieve upon its completion. These outputs can vary widely, from sending notifications, creating tickets, updating statuses, to generating reports.
Defining the outputs is essential for understanding the playbook's impact on the security operation workflows and how it contributes to resolving security incidents or automating tasks.

NEW QUESTION # 75
How is a Django filter query performed?

- A. Browse to the Django Filter Query Editor in the Administration panel.
- B. phantom/rest/search/app/contains/"sumo"
- C. By adding parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo".
- D. Install the SOAR Django App first, then configure the search query in the App editor.

Answer: C

Explanation:
Django filter queries in Splunk SOAR are performed by appending filter parameters directly to the REST API URL. This allows users to refine their search and retrieve specific data. For example, to filter containers by tags containing the word "sumo", the following URL structure would be used: https://<PHANTOM_URL>
/rest/container?_filter_tags_contains="sumo". This format enables users to construct dynamic queries that can filter results based on specified criteria within the Django framework used by Splunk SOAR.
The correct way to perform a Django filter query in Splunk SOAR is to add parameters to the URL similar to the following: phantom/rest/container?_filter_tags_contains="sumo". This will return a list of containers that have the tag "sumo" in them. You can use various operators and fields to filter the results according to your needs. For more details, see Query for Data and Use filters in your Splunk SOAR (Cloud) playbook to specify a subset of artifacts before further processing. The other options are either incorrect or irrelevant for this question. For example:
*phantom/rest/search/app/contains/"sumo" is not a valid URL for a Django filter query. It will return an error message saying "Invalid endpoint".
*There is no Django Filter Query Editor in the Administration panel of Splunk SOAR. You can use the REST API Tester to test your queries, but not to edit them.
*There is no SOAR Django App that needs to be installed or configured for performing Django filter queries.
Splunk SOAR uses the Django framework internally, but you do not need to install or use any additional apps for this purpose.

NEW QUESTION # 76
Which of the following are the steps required to complete a full backup of a Splunk Phantom deployment' Assume the commands are executed from /opt/phantom/bin and that no other backups have been made.

- A. On the command line enter: sudo phenv python ibackup.pyc --backup -backup-type full, then sudo phenv python ibackup.pyc --setup.
- B. Within the UI: Select from the main menu Administration > System Health > Backup.
- C. Within the UI: Select from the main menu Administration > Product Settings > Backup.
- D. On the command line enter: rode sudo python ibackup.pyc --setup, then audo phenv python ibackup.pyc --backup.

Answer: A

Explanation:
The correct answer is B because the steps required to complete a full backup of a Splunk Phantom deployment are to first run the --backup --backup-type full command and then run the --setup command.
The --backup command creates a backup file in the /opt/phantom/backup directory. The --backup-type full option specifies that the backup file includes all the data and configuration files of the Phantom server.
The --setup command creates a configuration file that contains the encryption key and other information needed to restore the backup file. See Splunk SOAR Certified Automation Developer Track for more details.
Performing a full backup of a Splunk Phantom deployment involves using the command-line interface, primarily because Phantom's architecture and data management processes are designed to be managed at the server level for comprehensive backup and recovery. The correct sequence involves initiating a full backup first using the --backup --backup-type full option to ensure all configurations, data, and necessary components are included in the backup. Following the completion of the backup, the --setup option might be used to configure or verify the backup settings, although typically, the setup would precede backup operations in practical scenarios. This process ensures that all aspects of the Phantom deployment are preserved, including configurations, playbooks, cases, and other data, which is crucial for disaster recovery and system migration.

NEW QUESTION # 77
Which of the following is a step when configuring event forwarding from Splunk to Phantom?

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

Answer: A

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.
See Forwarding events from Splunk to Phantom for more details.
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 # 78
What is enabled if the Logging option for a playbook's settings is enabled?

- A. The playbook will write detailed execution information into the spawn.log.
- B. More detailed logging information Is available m the Investigation page.
- C. More detailed information is available in the debug window.
- D. All modifications to the playbook will be written to the audit log.

Answer: B

Explanation:
In Splunk SOAR (formerly known as Phantom), enabling the Logging option for a playbook's settings primarily affects how logging information is displayed on the Investigation page. When this option is enabled, more detailed logging information is made available on the Investigation page, which can be crucial for troubleshooting and understanding the execution flow of the playbook. This detailed information can include execution steps, actions taken, and conditional logic paths followed during the playbook run.

It's important to note that enabling logging does not affect the audit logs or the debug window directly, nor does it write execution details to the spawn.log. Instead, it enhances the visibility and granularity of logs displayed on the specific Investigation page related to the playbook's execution.
References:
Splunk Documentation and SOAR User Guides typically outline the impacts of enabling various settings within the playbook configurations, explaining how these settings affect the operation and logging within the system. For specific references, consulting the latest Splunk SOAR documentation would provide the most accurate and detailed guidance.
Enabling the Logging option for a playbook's settings in Splunk SOAR indeed affects the level of detail provided on the Investigation page. Here's a comprehensive explanation of its impact:
Investigation Page Logging:
The Investigation page serves as a centralized location for reviewing all activities related to an incident or event within Splunk SOAR.
When the Logging option is enabled, it enhances the level of detail available on this page, providing a granular view of the playbook's execution.
This includes detailed information about each action's execution, such as parameters used, results obtained, and any conditional logic that was evaluated.
Benefits of Detailed Logging:
Troubleshooting: It becomes easier to diagnose issues within a playbook when you can see a detailed log of its execution.
Incident Analysis: Analysts can better understand the sequence of events and the decisions made by the playbook during an incident.
Playbook Optimization: Developers can use the detailed logs to refine and improve the playbook's logic and performance.
Non-Impacted Areas:
The audit log, which tracks changes to the playbook itself, is not affected by the Logging option.
The debug window, used for real-time debugging during playbook development, also remains unaffected.
The spawn.log file, which contains internal operational logs for the Splunk SOAR platform, does not receive detailed execution information from playbooks.
Best Practices:
Enable detailed logging during the development and testing phases of a playbook to ensure thorough analysis and debugging.
Consider the potential impact on storage and performance when enabling detailed logging in a production environment.
References:
For the most accurate and up-to-date guidance on playbook settings and their effects, I recommend consulting the latest Splunk SOAR documentation and user guides. These resources provide in-depth information on configuring playbooks and understanding the implications of various settings within the Splunk SOAR platform.
In summary, the Logging option is a powerful feature that enhances the visibility of playbook operations on the Investigation page, aiding in incident analysis and ensuring that playbooks are functioning correctly. It is an essential tool for security teams to effectively manage and respond to incidents within their environment.

NEW QUESTION # 79

......

Different from the common question bank on the market, SPLK-2003 exam guide is a scientific and efficient learning system that is recognized by many industry experts. In normal times, you may take months or even a year to review a professional exam, but with SPLK-2003 exam guide you only need to spend 20-30 hours to review before the exam. And with SPLK-2003 learning question, you will no longer need any other review materials, because our study materials already contain all the important test sites. At the same time, SPLK-2003 test prep helps you to master the knowledge in the course of the practice.

SPLK-2003 Pass Guarantee: https://www.dumpkiller.com/SPLK-2003_braindumps.html

- SPLK-2003 Exam Online □ SPLK-2003 Accurate Answers □ Exam SPLK-2003 Topic □ Download { SPLK-2003 } for free by simply entering [www.prepawayete.com] website □Reliable SPLK-2003 Test Pattern
- SPLK-2003 Latest Exam Papers □ SPLK-2003 Exam Online □ SPLK-2003 Trustworthy Exam Content □ The page for free download of { SPLK-2003 } on { www.pdfvce.com } will open immediately □SPLK-2003 Exam Fee
- Pass Guaranteed SPLK-2003 - Splunk Phantom Certified Admin –Reliable Valid Exam Duration 📰 Enter ☀ www.examcollectionpass.com □☀□ and search for 【 SPLK-2003 】 to download for free □Reliable SPLK-2003 Test Pattern
- 2026 Valid SPLK-2003 Exam Duration 100% Pass | Valid Splunk Phantom Certified Admin Pass Guarantee Pass for sure □ Search for ▹ SPLK-2003 ◃ and download exam materials for free through ⇛ www.pdfvce.com ⇚ □Latest SPLK-2003 Version
- Pass Guaranteed Quiz Splunk - High Pass-Rate Valid SPLK-2003 Exam Duration □ Easily obtain { SPLK-2003 } for free download through ➠ www.examcollectionpass.com □ □SPLK-2003 Exam Fee
- nativemediastudios.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, www.stes.tyc.edu.tw, cssoxfordgrammar.site, www.stes.tyc.edu.tw, wanderlog.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New SPLK-2003 dumps are available on Google Drive shared by Dumpkiller: https://drive.google.com/open?id=1pUF9Vn9Q4ZyNZfJNDrlzjJ_YYaIf0IXJ