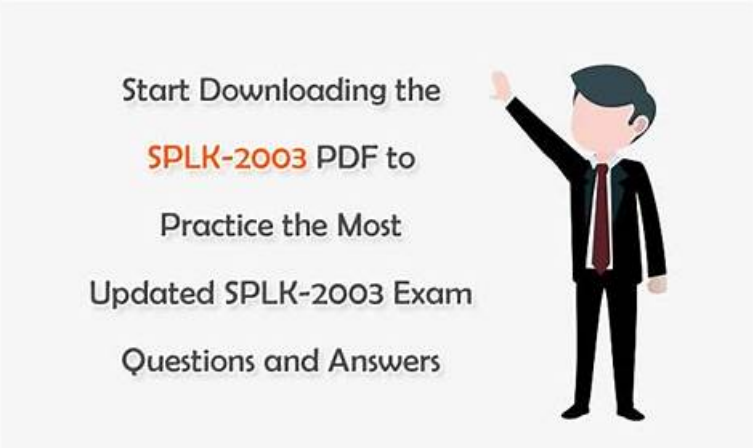
SPLK-2003 Ausbildungsressourcen - SPLK-2003 Prüfungsfrage



Übrigens, Sie können die vollständige Version der Pass4Test SPLK-2003 Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1i7Brld-rBbstR-Z-NFmg_T_a8VneNBxZ

Unsere Splunk SPLK-2003 Prüfungsunterlage (Splunk Phantom Certified Admin) enthalten alle echten, originalen und richtigen Fragen und Antworten. Die Abdeckungsrate unserer Splunk SPLK-2003 Unterlagen (Fragen und Antworten) (Splunk Phantom Certified Admin) ist normalerweise mehr als 98%.

Die SPLK-2003 Zertifizierung ist ideal für Fachleute, die mit Splunk Phantom arbeiten und ihre Fähigkeiten und Kenntnisse validieren möchten. Sie ist auch relevant für IT-Profis, die ihr Skillset erweitern und Splunk Phantom in ihre bestehende Infrastruktur integrieren möchten. Die Zertifizierung demonstriert ein Verständnis für bewährte Verfahren zur Nutzung dieser Plattform und bietet Fachleuten einen Wettbewerbsvorteil auf dem Arbeitsmarkt.

Zur Vorbereitung auf die Splunk SPLK-2003-Prüfung können Kandidaten den Splunk Phantom Certified Admin-Kurs besuchen, der alle Themen abdeckt, die relevant für die Prüfung sind. Dieser Kurs ist online verfügbar und beinhaltet praktische Übungen und Simulationen, die den Kandidaten helfen, ihre Fähigkeiten und ihr Wissen zu entwickeln. Kandidaten können auch auf verschiedene Ressourcen zugreifen, wie offizielle Splunk-Dokumentationen, Whitepapers und Foren, um ihr Lernen zu ergänzen.

>> SPLK-2003 Ausbildungsressourcen <<

Splunk SPLK-2003 Prüfungsfrage & SPLK-2003 Fragen Und Antworten

Es ist unnötig für Sie, viel Zeit an einer SPLK-2003 Zertifizierungsprüfung zu verwenden. Wenn Sie es schwierig für die Vorbereitung der Splunk SPLK-2003 Prüfung finden und viel Zeit verschwenden müssen, sollen Sie am Besten Pass4Test SPLK-2003 Dumps als Ihr Lerngerät benutzen, weil es kann viel Zeit für Sie sparen. Und es ist wichtiger, dass sie Ihnen versprechen, die Splunk SPLK-2003 Prüfung zu bestehen. Und es gibt keine anderen Unterlagen in dem Markt. Sie können viele andere interessante Dinge machen, statt die Splunk SPLK-2003 Prüfungen vorzubereiten. So, klicken Sie Pass4Test Webseite und Informieren Sie sich. Sie werden bereuen, diese Chance zu verlieren.

Splunk SPLK-2003, auch bekannt als die Splunk Phantom Certified Admin-Prüfung, ist für IT-Fachleute ausgelegt, die ihr Know-how für die Verwendung von Splunk Phantom zur Automatisierung und Orchestrierung von Aufgaben im Security Operations Center (SOC) der Organisation validieren möchten. Diese Zertifizierung zeigt, dass eine Person über die Fähigkeiten und das Wissen verfügt, um Splunk Phantom zu verwalten, zu konfigurieren und zu beheben, eine Sicherheitsautomatisierung und Orchestrierungsplattform, mit der SOC -Teams auf Cyber -Bedrohungen effizienter und effektiver reagieren können.

Splunk Phantom Certified Admin SPLK-2003 Prüfungsfragen mit Lösungen (Q114-Q119):

114. Frage
What is the default embedded search engine used by Phantom?

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

Antwort: B

Begründung:
Splunk SOAR (formerly Phantom) utilizes its own embedded search engine for querying and analyzing data within the platform. This search engine is specifically designed to cater to the unique data structures and use cases of security automation and orchestration, including searching through containers, artifacts, actions, and more. While Splunk SOAR can integrate with external Splunk instances for enhanced data analysis and search capabilities, the platform's primary, out-of-the-box search functionality is provided by its embedded Phantom search engine.

115. Frage
In a playbook, more than one Action block can be active at one time. What is this called?

- A. Juggle Processing
- B. Parallel Processing
- C. Serial Processing
- D. Multithreaded Processing

Antwort: B

Begründung:
In Splunk SOAR, when a playbook is designed such that more than one Action block is active at the same time, it is referred to as 'Parallel Processing'. This allows for multiple actions to be executed concurrently, which can significantly speed up the execution of a playbook as it does not have to wait for one action to complete before starting another. Parallel processing enables more efficient use of resources and time, particularly in complex playbooks that perform numerous actions.

116. Frage
After a successful POST to a Phantom REST endpoint to create a new object what result is returned?

- A. The PostGres UUID.
- B. The new object ID.
- C. The new object name.
- D. The full CEF name.

Antwort: B

Begründung:
The correct answer is A because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is the new object ID. The object ID is a unique identifier for each object in Phantom, such as a container, an artifact, an action, or a playbook. The object ID can be used to retrieve, update, or delete the object using the Phantom REST API. The answer B is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the new object name, which is a human-readable name for the object. The object name can be used to search for the object using the Phantom web interface. The answer C is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the full CEF name, which is a standard format for event data. The full CEF name can be used to access the CEF fields of an artifact using the Phantom REST API. The answer D is incorrect because after a successful POST to a Phantom REST endpoint to create a new object, the result returned is not the PostGres UUID, which is a unique identifier for each row in a PostGres database. The PostGres UUID is not exposed to the Phantom REST API. Reference: Splunk SOAR REST API Guide, page
17. When a POST request is made to a Phantom REST endpoint to create a new object, such as an event, artifact, or container, the typical response includes the ID of the newly created object. This ID is a unique identifier that can be used to reference the object within the system for future operations, such as updating, querying, or deleting the object. The response does not usually include the full name or other specific details of the object, as the ID is the most important piece of information needed immediately after creation for reference purposes.

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

Antwort: C

Begründung:
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.

118. Frage
Which of the following views provides a holistic view of an incident - providing event metadata, Service Level Agreement status, Severity, sensitivity of an event, and other detailed event info?

- A. Technical
- B. Executive
- C. Analyst
- D. Investigation

Antwort: D

Begründung:
The Investigation view in Splunk SOAR provides a comprehensive and holistic view of an incident. This view includes vital details such as event metadata, Service Level Agreement (SLA) status, severity, sensitivity of the event, and other relevant information. It allows analysts to track and manage incidents effectively by presenting a clear picture of all aspects of the investigation process. This view is designed to help users take timely actions based on critical data points, making it a pivotal feature for incident response teams.
Other views like Executive or Analyst may focus on specific reporting or technical details, but the Investigation view provides the most complete perspective on the incident and its progress.
References:
* Splunk SOAR Documentation: Investigation View Overview.
* Splunk SOAR Incident Response Best Practices.

119. Frage
.....

www.itzert.com ⇐ geben Sie □ SPLK-2003 □ ein und erhalten Sie den kostenlosen Download □SPLK-2003 Prüfungs-Guide

- SPLK-2003 PDF Demo □ SPLK-2003 PDF Testsoftware □ SPLK-2003 Testing Engine □ Geben Sie ➽ www.zertpruefung.ch □ ein und suchen Sie nach kostenloser Download von ☀ SPLK-2003 □☀□ □SPLK-2003 Testing Engine
- SPLK-2003 Dumps Deutsch □ SPLK-2003 Prüfungs-Guide □ SPLK-2003 Prüfung □ Öffnen Sie die Website ➡ www.itzert.com □□□ Suchen Sie 「 SPLK-2003 」 Kostenloser Download □SPLK-2003 PDF Demo
- Sie können so einfach wie möglich - SPLK-2003 bestehen! □ Suchen Sie auf ✔ www.echtefrage.top □✔□ nach ➡ SPLK-2003 □□□ und erhalten Sie den kostenlosen Download mühelos □SPLK-2003 PDF Demo
- SPLK-2003 Trainingsunterlagen □ SPLK-2003 Dumps Deutsch □ SPLK-2003 Quizfragen Und Antworten □ Öffnen Sie die Webseite { www.itzert.com } und suchen Sie nach kostenloser Download von ▹ SPLK-2003 ◃ □SPLK-2003 Antworten
- SPLK-2003 Prüfungs-Guide □ SPLK-2003 Testing Engine □ SPLK-2003 Prüfungsfrage □ Öffnen Sie die Website 【 www.echtefrage.top 】 Suchen Sie [SPLK-2003] Kostenloser Download □SPLK-2003 Testing Engine
- SPLK-2003: Splunk Phantom Certified Admin Dumps - PassGuide SPLK-2003 Examen □ Öffnen Sie die Webseite ▹ www.itzert.com ◃ und suchen Sie nach kostenloser Download von 「 SPLK-2003 」 🈵SPLK-2003 Unterlage
- SPLK-2003 Prüfungsfrage □ SPLK-2003 Antworten 🈵 SPLK-2003 Antworten □ URL kopieren ➡ www.deutschpruefung.com □□□ Öffnen und suchen Sie [SPLK-2003] Kostenloser Download □SPLK-2003 Deutsch Prüfung
- SPLK-2003 Übungsmaterialien □ SPLK-2003 Übungsmaterialien □ SPLK-2003 Unterlage □ Suchen Sie auf der Webseite ⇛ www.itzert.com ⇚ nach 《 SPLK-2003 》 und laden Sie es kostenlos herunter □SPLK-2003 Probesfragen
- SPLK-2003 Testing Engine □ SPLK-2003 Unterlage □ SPLK-2003 Zertifikatsdemo □ Öffnen Sie die Webseite " www.zertpruefung.ch " und suchen Sie nach kostenloser Download von ✔ SPLK-2003 □✔□ □SPLK-2003 Prüfungsfrage
- www.stes.tyc.edu.tw, study.stcs.edu.np, www.stes.tyc.edu.tw, 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, shortcourses.russellcollege.edu.au, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, pct.edu.pk, Disposable vapes

BONUS!!! Laden Sie die vollständige Version der Pass4Test SPLK-2003 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1i7Brld-rBbstR-Z-NFmg_T_a8VneNBxZ