SPLK-2003 Lernhilfe & SPLK-2003 Antworten

2026 Die neuesten ZertSoft SPLK-2003 PDF-Versionen Prüfungsfragen und SPLK-2003 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=1hT4Cu-8H88HUhfrhvbJNqiKxCNM11QqU

In unserem ZertSoft gibt es viele IT-Fachleute, die Splunk SPLK-2003 Zertifizierungsantworten bearbeiten, deren Hit-Rate 100% beträgt. Ohne Zweifel gibt es auch viele ähnliche Websites, die Ihnen vielleicht auch Lernhilfe und Online-Service bieten. Aber wir sind ihnen in vielen Aspekten voraus. Die Gründe dafür liegen darin, dass wir Splunk SPLK-2003 Prüfungsfragen und Antworten mit hoher Hit-Rate bieten, die sich regelmäßig aktualisieren. So können die an der Splunk SPLK-2003 Zertifizierungsprüfung teilnehmenden Prüflinge unbesorgt bestehen. Wir, ZertSoft, versprechen Ihnen, dass Sie die Splunk SPLK-2003 ZertifizierungsPrüfung 100% bestehen können.

Die Prüfung besteht aus 60 Multiple-Choice-Fragen und wird online durchgeführt. Die Kandidaten haben 90 Minuten Zeit, um die Prüfung abzuschließen, und eine Bestehensnote von 70% oder höher ist erforderlich, um die Zertifizierung zu erlangen. Die Prüfung deckt eine Reihe von Themen ab, darunter Phantom-Architektur und -Komponenten, Installation und Konfiguration, Playbook-Entwicklung, Automatisierung und Orchestrierung sowie Integrationen mit anderen Sicherheitstools.

>> SPLK-2003 Lernhilfe <<

SPLK-2003 Der beste Partner bei Ihrer Vorbereitung der Splunk Phantom Certified Admin

In dieser Gesellschaft, wo es zahlreiche Talent gibt, muss man immer noch seine Kenntnisse verbessern. Und der Bedarf an den spitzen IT-Fachleuten nimmt weiter zu. In der internationalen Gesellschaft ist es auch so. So wollen viele Leute die Splunk SPLK-2003 Zertifizierungsprüfung bestehen. Aber es ist nicht so leicht. Jedoch ist sehr wahrscheinlich, dass Sie gute Schulungsunnterlagen wählen und die Prüfung somit bestehen können. Unsere Schulungsunterlagen zur Splunk SPLK-2003 Zertifizierungsprüfung von ZertSoft befähigen Sie, diese Zertifizierung zu bestehen. Die Schulungsunterlagen von ZertSoft hat von vielen Kandidaten überprüft. Sie sind in der internationalen Gesellschaft immer Vorläufer. Wenn Sie die Splunk SPLK-2003 Zertifizierungsprüfung bestehen wollen, schicken doch die Schulungsunterlagen zur Splunk SPLK-2003 Zertifizierungsprüfung in den Warenkorb.

Die SPLK-2003-Prüfung besteht aus 60 Multiple-Choice-Fragen und dauert 90 Minuten. Die Prüfung umfasst eine Reihe von Themen, darunter Phantom-Plattformarchitektur, Automatisierungsworkflows, Ereignismanagement, Playbook-Design und Incident-Response-Management. Um die Prüfung zu bestehen, müssen die Kandidaten eine Mindestpunktzahl von 70% erreichen.

Splunk Phantom Certified Admin SPLK-2003 Prüfungsfragen mit Lösungen (Q30-Q35):

30. Frage
Some of the playbooks on the Phantom server should only be executed by members of the admin role. How can this rule be applied?

- A. Add a filter block to al restricted playbooks that Titters for runRole - "Admin".
- B. Place restricted playbooks in a second source repository that has restricted access.
- C. Add a tag with restricted access to the restricted playbooks.
- D. Make sure the Execute Playbook capability is removed from al roles except admin.

Antwort: D

Begründung:
The correct answer is C because the best way to restrict the execution of playbooks to members of the admin role is to make sure the Execute Playbook capability is removed from all roles except admin. The Execute Playbook capability is a permission that allows a user to run any playbook on any container. By default, all roles have this capability, but it can be removed or added in the Phantom UI by going to Administration > User Management > Roles. Removing this capability from all roles except admin will ensure that only admin users can execute playbooks. See Splunk SOAR Documentation for more details. To ensure that only members of the admin role can execute specific playbooks on the Phantom server, the most effective approach is to manage role-based access controls (RBAC) directly. By configuring the system to remove the
"Execute Playbook" capability from all roles except for the admin role, you can enforce this rule. This method leverages Phantom's built-in RBAC mechanisms to restrict playbook execution privileges. It is a straightforward and secure way to ensure that only users with the necessary administrative privileges can initiate the execution of sensitive or critical playbooks, thus maintaining operational security and control.

31. Frage
Which of the following actions will store a compressed, secure version of an email attachment with suspected malware for future analysis?

- A. Use the Files tab on the Investigation page to upload the attachment.
- B. Add a link to the file in a new artifact.
- C. Use the Upload action of the Secure Store app to store the file in the database.
- D. Copy/paste the attachment into a note.

Antwort: C

Begründung:
To securely store a compressed version of an email attachment suspected of containing malware for future analysis, the most effective approach within Splunk SOAR is to use the Upload action of the Secure Store app. This app is specifically designed to handle sensitive or potentially dangerous files by securely storing them within the SOAR database, allowing for controlled access and analysis at a later time. This method ensures that the file is not only safely contained but also available for future forensic or investigative purposes without risking exposure to the malware. Options A, B, and C do not provide the same level of security and functionality for handling suspected malware files, making option D the most appropriate choice.
Secure Store app is a SOAR app that allows you to store files securely in the SOAR database. The Secure Store app provides two actions: Upload and Download. The Upload action takes a file as an input and stores it in the SOAR database in a compressed and encrypted format. The Download action takes a file ID as an input and retrieves the file from the SOAR database and decrypts it. The Secure Store app can be used to store files that contain sensitive or malicious data, such as email attachments with suspected malware, for future analysis. Therefore, option D is the correct answer, as it states the action that will store a compressed, secure version of an email attachment with suspected malware for future analysis. Option A is incorrect, because copying and pasting the attachment into a note will not store the file securely, but rather expose the file content to anyone who can view the note. Option B is incorrect, because adding a link to the file in a new artifact will not store the file securely, but rather create a reference to the file location, which may not be accessible or reliable. Option C is incorrect, because using the Files tab on the Investigation page to upload the attachment will not store the file securely, but rather store the file in the SOAR file system, which may not be encrypted or compressed.

32. Frage

Phantom supports multiple user authentication methods such as LDAP and SAML2. What other user authentication method is supported?

- A. SAML3
- B. Biometrics
- C. OpenID
- D. PIV/CAC

Antwort: D

Begründung:
Splunk SOAR supports multiple user authentication methods to ensure secure access to the platform. Apart from LDAP (Lightweight Directory Access Protocol) and SAML2 (Security Assertion Markup Language 2.0), SOAR also supports PIV (Personal Identity Verification) and CAC (Common Access Card) as authentication methods. These are particularly used in government and military organizations for secure and authenticated access to systems, providing a high level of security through physical tokens or cards that contain encrypted user credentials.

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

Antwort: D

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.

34. Frage
On the Splunk search head, when configuring the app to search SOAR searchable content, what are the two requirements to complete the app setup?

- A. User accounts and syslog.
- B. User accounts and an HTTP Event Collector token.
- C. User accounts and REST API.
- D. User accounts and universal forwarder.

Antwort: C

35. Frage
.....

SPLK-2003 Antworten: https://www.zertsoft.com/SPLK-2003-pruefungsfragen.html

- Neueste Splunk Phantom Certified Admin Prüfung pdf - SPLK-2003 Prüfung Torrent Suchen Sie einfach auf 《 www.echtefrage.top 》 nach kostenloser Download von { SPLK-2003 } SPLK-2003 Kostenlos Downloden
- SPLK-2003 Fragen - Antworten - SPLK-2003 Studienführer - SPLK-2003 Prüfungsvorbereitung Öffnen Sie ➤ www.itzert.com geben Sie ➠ SPLK-2003 ein und erhalten Sie den kostenlosen Download SPLK-2003 Zertifizierungsfragen
- SPLK-2003 Testengine SPLK-2003 Schulungsangebot SPLK-2003 Prüfungsfragen " www.zertpruefung.ch " ist die beste Webseite um den kostenlosen Download von 「 SPLK-2003 」 zu erhalten SPLK-2003 Fragenpool
- SPLK-2003 German SPLK-2003 Praxisprüfung SPLK-2003 Online Prüfung Öffnen Sie die Webseite www.itzert.com und suchen Sie nach kostenloser Download von ➡ SPLK-2003 SPLK-2003 Testengine
- SPLK-2003 Online Prüfung SPLK-2003 Kostenlos Downloden SPLK-2003 Online Prüfung Erhalten Sie den kostenlosen Download von ⇛ SPLK-2003 ⇚ mühelos über ⇛ www.zertsoft.com ⇚ SPLK-2003 Prüfungsfragen
- Die seit kurzem aktuellsten Splunk SPLK-2003 Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der Prüfungen! URL kopieren ☀ www.itzert.com ☀ Öffnen und suchen Sie { SPLK-2003 } Kostenloser Download SPLK-2003 German
- SPLK-2003 Praxisprüfung SPLK-2003 Fragenpool SPLK-2003 German Suchen Sie auf der Webseite { www.itzert.com } nach 「 SPLK-2003 」 und laden Sie es kostenlos herunter SPLK-2003 Prüfungsmaterialien
- SPLK-2003 Schulungsangebot SPLK-2003 Simulationsfragen SPLK-2003 Zertifizierungsfragen Suchen Sie einfach auf ➤ www.itzert.com nach kostenloser Download von ➡ SPLK-2003 SPLK-2003 Echte Fragen
- 100% Garantie SPLK-2003 Prüfungserfolg URL kopieren ➡ www.it-pruefung.com Öffnen und suchen Sie ➤ SPLK-2003 Kostenloser Download SPLK-2003 Prüfungsfragen
- Seit Neuem aktualisierte SPLK-2003 Examfragen für Splunk SPLK-2003 Prüfung Suchen Sie einfach auf ➤ www.itzert.com nach kostenloser Download von ➤ SPLK-2003 SPLK-2003 Echte Fragen
- Das neueste SPLK-2003, nützliche und praktische SPLK-2003 pass4sure Trainingsmaterial URL kopieren ▶ www.zertpruefung.ch ◀ Öffnen und suchen Sie [SPLK-2003] Kostenloser Download SPLK-2003 Echte Fragen
- 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, 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, 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, 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, wjhsd.instructure.com, Disposable vapes

P.S. Kostenlose und neue SPLK-2003 Prüfungsfragen sind auf Google Drive freigegeben von ZertSoft verfügbar: https://drive.google.com/open?id=1hT4Cu-8H88HUhfrhvbJNqiKxCNM1lQqU