

SPLK-2003 Prüfungs & SPLK-2003 Online Test



Die Feedbacks von den IT-Fachleuten, die Splunk SPLK-2003 Zertifizierungsprüfung erfolgreich bestanden haben, haben bewiesen, dass ihren Erfolg Fast2test beizumessen ist. Die Fragen und Antworten zur Splunk SPLK-2003 Zertifizierungsprüfung haben ihnen sehr geholfen. Dabei erspart Fast2test ihnen auch viele wertvolle Zeit und Energie. Sie haben die Splunk SPLK-2003 Zertifizierungsprüfung ganz mühlos beim ersten Versuch bestanden. So ist Fast2test eine zuverlässige Website. Wenn Sie Fast2test wählen, sind Sie der nächste erfolgreiche IT-Fachmann. Fast2test würde Ihren Traum verwirklichen.

Die Splunk SPLK-2003-Prüfung ist für IT-Profis konzipiert, die zertifizierte Administratoren der Splunk Phantom-Plattform werden möchten. Splunk Phantom ist eine Sicherheits-Orchestrierungs-, Automatisierungs- und Reaktionslösung (SOAR), die Organisationen dabei hilft, ihre Sicherheitsoperationen zu optimieren und ihre Incident-Response-Kapazitäten zu verbessern. Die Prüfung umfasst eine Vielzahl von Themen, darunter Installation und Konfiguration, Benutzerverwaltung, Workflow-Design, Automatisierung und Integration mit anderen Sicherheitstools. Das Bestehen der SPLK-2003-Prüfung demonstriert das Wissen und die Fähigkeiten eines Kandidaten im Umgang mit Splunk Phantom zur Automatisierung und Orchestrierung von Sicherheitstasks, was es Organisationen ermöglicht, schneller und effektiver auf Sicherheitsvorfälle zu reagieren.

Die Splunk Phantom-Plattform ist eine fortschrittliche Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR), die Unternehmen hilft, ihre Sicherheitsvorgänge zu automatisieren. Es wurde entwickelt, um den Prozess der Identifizierung und Reaktion auf Cybersicherheitsbedrohungen zu optimieren. Die Plattform ist sehr anpassbar und kann auf die spezifischen Bedürfnisse verschiedener Organisationen zugeschnitten werden. Die SPLK-2003-Prüfung stellt sicher, dass die Kandidaten die Plattform gründlich verstehen und sie effektiv verwalten können.

Die Splunk SPLK-2003 (Splunk Phantom Certified Admin) Zertifizierungsprüfung ist eine wertvolle Zertifizierung für Fachkräfte, die mit der Splunk Phantom Plattform arbeiten. Sie validiert das Wissen und die Fähigkeiten, die erforderlich sind, um die Plattform effektiv zu verwalten und zu nutzen, und bietet einen Wettbewerbsvorteil auf dem Arbeitsmarkt. Kandidaten, die die Prüfung bestehen, zeigen ihre Fähigkeit, Probleme zu beheben, Benutzer und Ressourcen zu verwalten und Phantom mit anderen Tools und Plattformen zu integrieren, was sie in der Branche sehr gefragt macht.

>> SPLK-2003 Prüfungs <<

SPLK-2003 Online Test & SPLK-2003 Zertifizierungsfragen

Die Examfragen zur Splunk SPLK-2003 Zertifizierungsprüfung von Fast2test ist von den IT-Experten verifiziert und überprüft. Die Fragen und Antworten zur Splunk SPLK-2003 Zertifizierungsprüfung sind die von der Praxis überprüfte Software und die Schulungsinstrumente. In Fast2test werden Sie die besten Zertifizierungsmaterialien finden, die originale Fragen und Antworten enthalten. Unsere Materialien bieten Ihnen die Chance, die echten Übungen zu machen. Endlich werden Sie Ihr Ziel, nämlich die Splunk SPLK-2003 Zertifizierungsprüfung zu bestehen, erreichen.

Splunk Phantom Certified Admin SPLK-2003 Prüfungsfragen mit Lösungen (Q78-Q83):

78. Frage

Which Phantom VPE Nock S used to add information to custom lists?

- A. Filter blocks
- B. Decision blocks

- C. Action blocks
- **D. API blocks**

Antwort: D

79. Frage

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

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

Antwort: A

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.

80. Frage

Which of the following is accurate?

- **A. Phantom.debug() outputs to the VPE debugger display.**
- B. System.Out.Prinln() outputs to the VPE debugger display.
- C. Phantom.debug() is the same as phantom.error() except it prints in red text.
- D. Users can output debug info using the print() or print "" syntax.

Antwort: A

81. Frage

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

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

Antwort: D

Begründung:

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.

82. Frage

Which of the following cannot be marked as evidence in a container?

- Antwort: D**

.....

- [illegible]