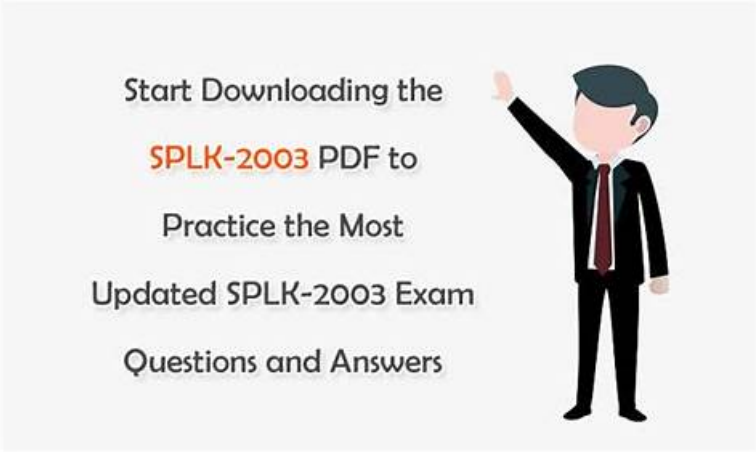
SPLK-2003 Exam, SPLK-2003 Fragenkatalog



BONUS!!! Laden Sie die vollständige Version der ZertFragen SPLK-2003 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1xHG9ukR8kWFwPkC8jafwcUTeLTZmvjka

Mit der Ankunft der Flut des Informationszeitalters im 21. Jahrhundert müssen die Menschen ihre Kenntnisse verbessern, um sich dem Zeitalter anzupassen. Aber das ist noch nicht genügend. In der IT-Branche ist Splunk SPLK-2003 Zertifizierungsprüfung ganz notwendig. Aber diese Prüfung ist ganz schwierig. Sie können auch internationale Anerkennung und Akzeptanz erhalten, eine glänzende Zukunft haben und ein hohes Gehalt beziehen. ZertFragen verfügt über die weltweit zuverlässigsten IT-Schulungsmaterialien und mit ihm können Sie Ihre wunderbare Pläne realisieren. We garantieren Ihnen 100%, die Prüfung zu bestehen. Bewerber, die an der Splunk SPLK-2003 Zertifizierungsprüfung teilnehmen, warum zögern Sie noch. Schnell, bitte!

Um sich auf die SPLK-2003-Prüfung vorzubereiten, sollten Kandidaten Erfahrung mit Splunk Phantom in einer realen Umgebung haben. Sie sollten auch mit den Grundlagen von Skript und Programmierung sowie mit Netzwerk- und Sicherheitskonzepten vertraut sein. Splunk bietet eine Reihe von Schulungskursen an, um den Kandidaten dabei zu helfen, sich auf die Prüfung vorzubereiten, einschließlich Online-Kursen, virtuellem Ausbildungsausbildungen und Schulungen vor Ort. Kandidaten finden auch eine Fülle von Ressourcen und Studienmaterialien online, einschließlich Praxisprüfungen, Lernleitfäden und Foren, in denen sie Fragen stellen und Rat von anderen Fachleuten erhalten können.

>> SPLK-2003 Exam <<

Die seit kurzem aktuellsten Splunk Phantom Certified Admin Prüfungsunterlagen, 100% Garantie für Ihen Erfolg in der Splunk SPLK-2003 Prüfungen!

Die Welt verändert sich. Daher müssen mit den Veränderungen Schritt halten. Wir ZertFragen beachten immer die vielfältige Veränderungen der Splunk SPLK-2003 Prüfung. Wir haben schon zahlreiche Prüfungsaufgaben der Splunk SPLK-2003 Prüfung von mehreren Jahren geforscht. Jetzt können wir Ihnen die wertvolle Prüfungsunterlagen der Splunk SPLK-2003 bieten. Nach Ihrem Kauf geben Ihnen rechtzeitigen Bescheid über die Aktualisierungsinformationen der Splunk SPLK-2003. Dieser Dienst ist kostenlos, weil die Gebühren für die Unterlagen bezahlen, haben Sie schon alle auf Splunk SPLK-2003 bezügliche Hilfen gekauft.

Die Splunk SPLK-2003 Prüfung ist darauf ausgelegt, die Kompetenz einer Person in der Administration von Splunk Phantom zu testen, einer umfassenden Plattform für Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR). Diese Zertifizierung richtet sich an IT-Profis, die für die Verwaltung und Wartung von Splunk Phantom in ihren jeweiligen Organisationen verantwortlich sind. Durch das Bestehen dieser Prüfung können Kandidaten ihre Expertise in der Implementierung, Konfiguration und Fehlerbehebung von Splunk Phantom demonstrieren.

Splunk Phantom Certified Admin SPLK-2003 Prüfungsfragen mit Lösungen (Q84-Q89):

84. Frage
Which of the following will show all artifacts that have the term results in a filePath CEF value?

- A. .../rest/artifact?_filter_cef_filePath_icontain="results"
- B. .../result/artifact?_query_cef_filepath_icontains="results
- C. .../result/artifacts/cef/filePath= '%results%"
- D. ...rest/artifacts/filePath="%results%"

Antwort: A

Begründung:
Explanation
The correct answer is A because the _filter parameter is used to filter the results based on a field value, and the icontain operator is used to perform a case-insensitive substring match. The filePath field is part of the Common Event Format (CEF) standard, and the cef_ prefix is used to access CEF fields in the REST API. The answer B is incorrect because it uses the wrong syntax for the REST API. The answer C is incorrect because it uses the wrong endpoint (result instead of artifact) and the wrong syntax for the REST API. The answer D is incorrect because it uses the wrong syntax for the REST API and the wrong spelling for the icontains operator.
Reference: Splunk SOAR REST API Guide, page 18.

85. Frage
What are indicators?

- A. Action result items that determine the flow of execution in a playbook.
- B. Action results that may appear in multiple containers.
- C. Artifact values with special security significance.
- D. Artifact values that can appear in multiple containers.

Antwort: D

Begründung:
Indicators in Splunk SOAR (formerly Phantom) are crucial elements used to detect and respond to security incidents. Let's break down what indicators are and their significance:
Definition of Indicators:
Indicators are data points or patterns that suggest the presence of malicious activity or potential security threats.
They can be anything from IP addresses, domain names, file hashes, URLs, email addresses, or other observable artifacts.
Indicators help security teams identify and correlate events across different sources to understand the scope and impact of an incident.
Types of Indicators:
Observable Indicators: These are directly observable artifacts, such as IP addresses, domain names, or file hashes.
Behavioral Indicators: These describe patterns of behavior, such as failed login attempts, lateral movement, or suspicious network traffic.
Contextual Indicators: These provide additional context around an event, such as the user account associated with an action or the time of occurrence.
Use Cases for Indicators:
Threat Detection: Security analysts create rules or playbooks that trigger based on specific indicators. For example, an indicator like a known malicious IP address can trigger an alert.
Incident Response: During an incident, indicators help identify affected systems, track lateral movement, and prioritize response efforts.
Threat Intelligence Sharing: Organizations share indicators with each other to improve collective security posture.
Multiple Containers:
Indicators can appear in multiple containers (playbooks, actions, etc.) within Splunk SOAR.
For example, an IP address associated with a suspicious domain might appear in both a threat intelligence playbook and an incident response playbook.
Artifact Values vs. Indicators:
While artifact values are related, they are not the same as indicators.
Artifact values represent specific data extracted from an artifact (e.g., extracting an IP address from an email header).
Indicators encompass a broader range of data points and are used for detection and correlation.
References:
Splunk SOAR Documentation: Indicators
Splunk SOAR Community: Understanding Indicators

86. 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. Copy/paste the attachment into a note.
- C. Add a link to the file in a new artifact.
- D. Use the Upload action of the Secure Store app to store the file in the database.

Antwort: D

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.

87. Frage
An active playbook can be configured to operate on all containers that share which attribute?

- A. Tag
- B. Artifact
- C. Label
- D. Severity

Antwort: C

Begründung:
An active playbook can be configured to operate on all containers that share a label. A label is a user-defined attribute that can be applied to containers to group them by a common characteristic, such as source, type, severity, etc. Labels can be used to filter containers and trigger active playbooks based on the label value.
In Splunk SOAR, labels are used to categorize containers (such as incidents or events) based on their characteristics or the type of security issue they represent. An active playbook can be configured to trigger on all containers that share a specific label, enabling targeted automation based on the nature of the incident. This functionality allows for efficient and relevant playbook execution, ensuring that the automated response is tailored to the specific requirements of the container's category. Labels serve as a powerful organizational tool within SOAR, guiding the automated response framework to act on incidents that meet predefined criteria, thus streamlining the security operations process.

88. Frage
Which of the following supported approaches enables Phantom to run on a Windows server?

- A. Install the Phantom RPM in a GNU Cygwin implementation.
- B. Run the Phantom OVA as a virtual machine.
- C. Run the Phantom OVA as a cloud instance.
- D. Install the Phantom RPM file in Windows Subsystem for Linux (WSL).

Antwort: B

Begründung:
Splunk SOAR (formerly Phantom) does not natively run on Windows servers as it is primarily designed for Linux environments. However, it can be deployed on a Windows server through virtualization. By running the Phantom OVA (Open Virtualization Appliance) as a virtual machine, users can utilize virtualization platforms like VMware or VirtualBox on a Windows server to host the Phantom environment. This approach allows for the deployment of Phantom in a Windows-centric infrastructure by leveraging virtualization technology to encapsulate the Phantom application within a supported Linux environment provided by the OVA.

89. Frage
......