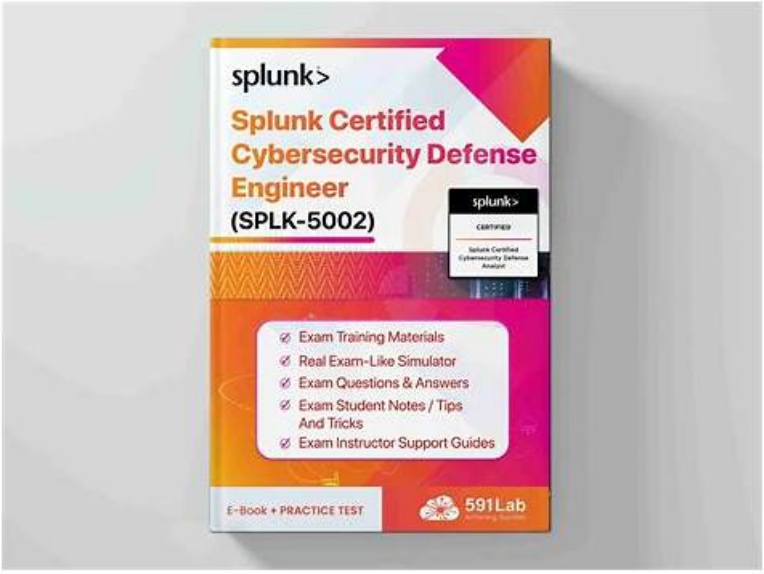
Splunk SPLK-5002 Testing Engine, SPLK-5002 Fragen Und Antworten



P.S. Kostenlose 2026 Splunk SPLK-5002 Prüfungsfragen sind auf Google Drive freigegeben von DeutschPrüfung verfügbar: https://drive.google.com/open?id=1CRzDOdKsaYHDOaOkXGi1xU726S03xbQE

Sind Sie einer von den vielen? Machen Sie sich noch Sorgen wegen den zahlreichen Kurse und Materialien zur Splunk SPLK-5002 Zertifizierungsprüfung? DeutschPrüfung ist Ihnen eine weise Wahl, denn wir Ihnen die umfassendesten Prüfungsmaterialien bieten, die Fragen und Antworten und ausführliche Erklärungen beinhalten. Alle diesen werden Ihnen helfen, die Fachkenntnisse zu beherrschen. Wir sind selbstsicher, dass Sie die Splunk SPLK-5002 Zertifizierungsprüfung bestehen. Das ist unser Versprechen an den Kunden.

Die zielgerichteten Prüfungsfragen und Antworten zur Splunk SPLK-5002 Zertifizierungsprüfung von DeutschPrüfung sind sehr beliebt. Mit den Materialien von DeutschPrüfung können Sie nicht nur neue Kenntnisse und Erfahrungen gewinnen, sondern sich auch genügend auf die Prüfung vorbereiten. Obwohl die Splunk SPLK-5002 Zertifizierungsprüfung schwer ist, würden Sie mehr Selbewusstsein für die Prüfung haben, nachdem Sie diese Fragenkataloge gekauft haben. Wählen Sie die effizienten Fragenkataloge von DeutschPrüfung ganz beruhigt, um sich genügend auf die Splunk SPLK-5002 (Splunk Certified Cybersecurity Defense Engineer) Zertifizierungsprüfung vorzubereiten.

>> Splunk SPLK-5002 Testing Engine <<

SPLK-5002 Fragen Und Antworten & SPLK-5002 Fragen Antworten

Sind Sie IT-Fachmann? Wollen Sie Erfolg? Dann kaufen Sie die Schulungsunterlagen zur Splunk SPLK-5002 Zertifizierungsprüfung von DeutschPrüfung. Sie werden von der Praxis prüft. Sie werden Ihnen helfen, die Splunk SPLK-5002 Zertifizierungsprüfung zu bestehen. Ihre Berufsaussichten werden sich sicher verbessern. Sie werden ein hohes Gehalt beziehen. Sie können eine Karriere in der internationalen Gesellschaft machen. Wenn Sie spitze technischen Fähigkeiten haben, sollen Sie sich keine Sorgen machen. Die Schulungsunterlagen zur Splunk SPLK-5002 Zertifizierungsprüfung von DeutschPrüfung werden Ihren Traum verwirklichen. Wir werden mit Ihnen durch dick und dünn gehen und die Herausforderung mit Ihnen zusammen nehmen.

Splunk SPLK-5002 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Automation and Efficiency: This section assesses Automation Engineers and SOAR Specialists in streamlining security operations. It covers developing automation for SOPs, optimizing case management workflows, utilizing REST APIs, designing SOAR playbooks for response automation, and evaluating integrations between Splunk Enterprise Security and SOAR tools.

Thema 2	• Building Effective Security Processes and Programs: This section targets Security Program Managers and Compliance Officers, focusing on operationalizing security workflows. It involves researching and integrating threat intelligence, applying risk and detection prioritization methodologies, and developing documentation or standard operating procedures (SOPs) to maintain robust security practices.
Thema 3	• Data Engineering: This section of the exam measures the skills of Security Analysts and Cybersecurity Engineers and covers foundational data management tasks. It includes performing data review and analysis, creating and maintaining efficient data indexing, and applying Splunk methods for data normalization to ensure structured and usable datasets for security operations.
Thema 4	• Auditing and Reporting on Security Programs: This section tests Auditors and Security Architects on validating and communicating program effectiveness. It includes designing security metrics, generating compliance reports, and building dashboards to visualize program performance and vulnerabilities for stakeholders.
Thema 5	• Detection Engineering: This section evaluates the expertise of Threat Hunters and SOC Engineers in developing and refining security detections. Topics include creating and tuning correlation searches, integrating contextual data into detections, applying risk-based modifiers, generating actionable Notable Events, and managing the lifecycle of detection rules to adapt to evolving threats.

Splunk Certified Cybersecurity Defense Engineer SPLK-5002 Prüfungsfragen mit Lösungen (Q16-Q21):

16. Frage
When creating a new playbook to be called directly from Mission Control or Enterprise Security, which type of playbook must be used?

- A. Input
- B. Automation
- C. Response
- D. Process

Antwort: C

Begründung:
A Response playbook must be used when creating a new playbook that can be called directly from Mission Control or Enterprise Security. Response playbooks are designed to run in these contexts to standardize and automate incident response actions.

17. Frage
The following SPL is designed to report on a certain SOC metric. Which metric is the most likely topic for this report?

- A. Mean time to Triage
- B. Dwell Time
- C. Mean time to Resolve
- D. Mean time to Respond

Antwort: A

Begründung:
The SPL calculates the time difference between create_time and triage_time for notable events.

This directly measures how long it takes analysts to triage an alert after it is created, which is the definition of Mean Time to Triage (MTTT).

18. Frage
When creating a detection, how might an engineer ensure that all possible contextual fields about a given asset and identity are added to a risk event?

- A. Call an adaptive response action for Active Directory using | ldapsearch for a real-time update.
- B. Use | lookup identities.csv to call all available identity information in the detection output.
- C. Include the standard CIM fields (e.g. user, src, src_user, etc.) in the detection output.
- D. Use | lookup assets.csv to call all available asset information in the detection output.

Antwort: C

Begründung:
To ensure all possible contextual fields about an asset and identity are included in a risk event, the engineer should include the standard CIM fields (such as user, src, src_user, etc.) in the detection output. These fields are recognized by the Assets & Identities framework and automatically enrich risk events with relevant context.

19. Frage
A compliance audit reveals gaps in the tracking of privileged account activities.
Howcan the team address this issue?

- A. Use summary indexes to delete old data
- B. Exclude privileged accounts from reporting
- C. Focus only on low-priority account activity
- D. Automate report generation for privileged accounts

Antwort: D

Begründung:
Privileged accounts pose ahigh security risk, and tracking their activity iscritical for compliance(e.g.,PCI DSS, NIST, ISO 27001, SOC 2).
#1. Automate Report Generation for Privileged Accounts (A)
Ensurescontinuous monitoringofadmin/root accounts.
Helpsdetect misuse or unauthorized access.
Example:
Splunk Enterprise Security (ES)can generate scheduled reports on:
Failed login attempts by privileged users.
Actions performed using admin credentials.
#Incorrect Answers:
B: Use summary indexes to delete old data# Summary indexes improve performance butdo not help track privileged accounts.
C: Focus only on low-priority account activity# Privileged accountsshould always be high-priority.
D: Exclude privileged accounts from reporting# This wouldviolate compliance requirements.
#Additional Resources:
Splunk Security Monitoring for Privileged Accounts
NIST Access Control Guide

20. Frage
Which REST API method is used to retrieve data from a Splunk index?

- A. POST
- B. DELETE
- C. PUT
- D. GET

Antwort: D

Begründung:
The GET method in the Splunk REST API is used to retrieve data from a Splunk index. It allows users and automated scripts to fetch logs, alerts, or query results programmatically.
Key Points About GET in Splunk API:
Used for searching and retrieving logs from indexes.
Can be used to get search results, job status, and Splunk configuration details.
Common API endpoints include:
/services/search/jobs/{search_id}/results- Retrieves results of a completed search.
/services/search/jobs/export- Exports search results in real-time.

21. Frage
.....

Mit der Ankunft der Informationsepoche im 21. Jahrhunderts wird das Splunk SPLK-5002 Zertifikat auch unerlässlich in der IT-Branche. Ob Sie ein Anfänger oder ein Pendler sind, können Sie Ihre erwünschte Ergebnisse nur mit Häflte der Bemühungen von anderen erzeilen, denn es gibt bei DeutschPrüfung für Sie maßgeschneidete Fragenkataloge zur Splunk SPLK-5002 Zertifizierungsprüfung. DeutschPrüfung wird Ihnen begleiten, für den Traum zu kämpfen. Worauf warten Sie noch?