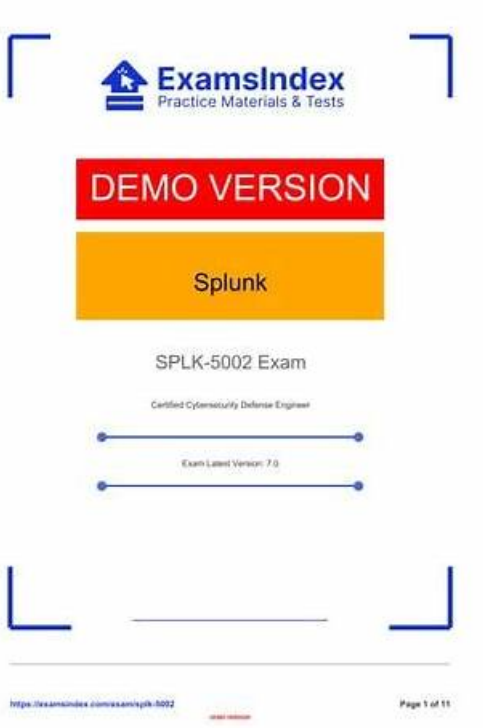
# SPLK-5002 Examsfragen & SPLK-5002 Exam




P.S. Kostenlose 2026 Splunk SPLK-5002 Prüfungsfragen sind auf Google Drive freigegeben von ZertFragen verfügbar: https://drive.google.com/open?id=1qVmvdNNFLQ4CFPUdv5HOQTLLZG7x6bL2

Die neuesten Schulungsunterlagen zur Splunk SPLK-5002 (Splunk Certified Cybersecurity Defense Engineer) Zertifizierungsprüfung von ZertFragen sind von den Expertenteams bearbeitet, die vielen beim Verwirklichen ihres Traums verhelfen. In der konkurrenzfähigen Gesellschaft muss man die Fachleute seine eigenen Kenntinisse und Technikniveau unter Beweis stellen, um seine Position zu verstärken. Durch die Splunk SPLK-5002 Zertifizierungsprüfung kann man seine Fähigkeiten beweisen. Mit dem Splunk SPLK-5002 Zertifikat werden große Veränderungen in Ihrer Arbeit stattfinden. Ihr Gehalt wird erhöht und Sie werden sicher befördert.

## 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 | • 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 3 | • 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 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. |



## bestehen Sie SPLK-5002 Ihre Prüfung mit unserem Prep SPLK-5002 Ausbildung Material & kostenloser Dowload Torrent

Unser ZertFragen ist international ganz berühmt. Die Anwendbarkeit von den Schulungsunterlagen ist sehr groß. Sie werden von den IT-Experten nach ihren Kenntnissen und Erfahrungen bearbeitet. Die Feedbacks von den Kandidaten haben sich gezeigt, dass unsere Prüdukte eher von guter Qualität sind. Wenn Sie einer der IT-Kandidaten sind, sollen Sie die Schulungsunterlagen zur Splunk SPLK-5002 Zertifizierungsprüfung von ZertFragen ohne Zweifel wählen.

## Splunk Certified Cybersecurity Defense Engineer SPLK-5002 Prüfungsfragen mit Lösungen (Q39-Q44):

**39. Frage**
A corporate laptop was disconnected from the internet Friday at 5PM local time. While offline, the user unknowingly opened a malicious file. The laptop came back online the following Monday morning, 9AM local time. The current detection has a 15 minute lookback period. How can the detection be tuned to account for this scenario?

- A. Increase the info_max_time to account for the weekend.
- B. Leverage an event time configuration within the detection.
- C. Increase the info_min_time to account for the weekend.
- D. Leverage an index time configuration within the detection.

**Antwort: B**

Begründung:
To catch events that occurred while the laptop was offline and only indexed later, the detection should leverage event time rather than index time. Event time ensures detections are based on when the activity actually happened, not when the logs were ingested, preventing missed findings after delayed ingestion.

**40. Frage**
What is the primary purpose of data indexing in Splunk?

- A. To store raw data and enable fast search capabilities
- B. To visualize data using dashboards

- C. To ensure data normalization
- D. To secure data from unauthorized access

**Antwort: A**

Begründung:
Understanding Data Indexing in Splunk
In Splunk Enterprise Security (ES) and Splunk SOAR, data indexing is a fundamental process that enables efficient storage, retrieval, and searching of data.
#Why is Data Indexing Important?
Stores raw machine data (logs, events, metrics) in a structured manner.
Enables fast searching through optimized data storage techniques.
Uses an indexer to process, compress, and store data efficiently.
Why the Correct Answer is B?
Splunk indexes data to store it efficiently while ensuring fast retrieval for searches, correlation searches, and analytics.
It assigns metadata to indexed events, allowing SOC analysts to quickly filter and search logs.
#Incorrect Answers & Explanations
A: To ensure data normalization # Splunk normalizes data using Common Information Model (CIM), not indexing.
C: To secure data from unauthorized access # Splunk uses RBAC (Role-Based Access Control) and encryption for security, not indexing.
D: To visualize data using dashboards # Dashboards use indexed data for visualization, but indexing itself is focused on data storage and retrieval.
#Additional Resources:
Splunk Data Indexing Documentation
Splunk Architecture & Indexing Guide

**41. Frage**
An EDR tool was recently purchased and needs to be integrated into existing Splunk SOAR playbooks. Which actions are typically associated with this type of asset?

- A. Block hash, reset user password, quarantine device, get indicator
- B. Block hash, block process, quarantine device, get indicator
- C. Block device, remove email, detonate URL, get indicator
- D. Block URL, block subdomain, quarantine device, get indicator, detonate URL

**Antwort: B**

Begründung:
EDR platforms commonly support host-level actions such as blocking malicious hashes, stopping or blocking processes, quarantining infected endpoints, and retrieving indicators for investigation.

**42. Frage**
Which Splunk feature enables integration with third-party tools for automated response actions?

- A. Event sampling
- B. Workflow actions
- C. Data model acceleration
- D. Summary indexing

**Antwort: B**

Begründung:
Security teams use Splunk Enterprise Security (ES) and Splunk SOAR to integrate with firewalls, endpoint security, and SIEM tools for automated threat response.
#Workflow Actions (B) - Key Integration Feature
Allows analysts to trigger automated actions directly from Splunk searches and dashboards.
Can integrate with SOAR playbooks, ticketing systems (e.g., ServiceNow), or firewalls to take action.
Example:
Block an IP on a firewall from a Splunk dashboard.

Trigger a SOAR playbook for automated threat containment.
#Incorrect Answers:
A: Data Model Acceleration # Speeds up searches, but doesn't handle integrations.
C: Summary Indexing # Stores summarized data for reporting, not automation.
D: Event Sampling # Reduces search load, but doesn't trigger automated actions.
#Additional Resources:
Splunk Workflow Actions Documentation
Automating Response with Splunk SOAR

**43. Frage**
During a high-priority incident, a user queries an index but sees incomplete results.
Whatis the most likely issue?

- A. Buckets in the warm state are inaccessible.
- B. The search head configuration is outdated.
- C. Indexers have reached their queue capacity.
- D. Data normalization was not applied.

**Antwort: C**

Begründung:
If a user queries an index during a high-priority incident but sees incomplete results, it is likely that the indexers are overloaded, causing queue bottlenecks.
Why Indexer Queue Capacity Issues Cause Incomplete Results:
When indexing queues fill up, incoming data cannot be processed efficiently.
Search results may be incomplete or delayed if events are still in the indexing queue and not fully written to disk.
Heavy search loads during incidents can also increase pressure on indexers.
How to Fix It:
Monitor indexing queues via the Monitoring Console (indexing>indexing performance).
Checkmetrics.logon indexers formax_queue_size_exceededwarnings.
Increase indexer capacity or optimize search scheduling to reduce load.

**44. Frage**
.....

Manchmal bedeutet ein kleinem Schritt ein großem Fortschritt des Lebens. Die Splunk SPLK-5002 Prüfung scheit nur ein kleinem Test zu sein, aber der Vorteil der Prüfungszertifizierung der Splunk SPLK-5002 für Ihr Arbeitsleben darf nicht übersehen werden. Diese internationale Zertifikat beweist Ihre ausgezeichnete IT-Fähigkeit. Neben Splunk SPLK-5002 sind auch andere Zertifizierungsprüfung sehr wichtig, deren neueste Unterlagen können Sie auch auf unserer Webseite finden.

Lerntipps

- SPLK-5002 Vorbereitung □ SPLK-5002 Zertifizierungsprüfung □ SPLK-5002 Schulungsunterlagen □ URL kopieren ☀ www.itzert.com □☀□ Öffnen und suchen Sie [ SPLK-5002 ] Kostenloser Download □SPLK-5002 Ausbildungsressourcen
- SPLK-5002 Quizfragen Und Antworten □ SPLK-5002 Quizfragen Und Antworten □ SPLK-5002 Prüfungsübungen □ Suchen Sie auf ➽ www.zertpruefung.ch □ nach kostenlosem Download von ➡ SPLK-5002 □□□ □SPLK-5002 Lerntipps
- SPLK-5002 Online Prüfung □ SPLK-5002 Vorbereitung □ SPLK-5002 Ausbildungsressourcen □ Öffnen Sie die Website ➠ www.itzert.com □ Suchen Sie ⇛ SPLK-5002 ⇚ Kostenloser Download □SPLK-5002 Testengine
- SPLK-5002 echter Test - SPLK-5002 sicherlich-zu-bestehen - SPLK-5002 Testguide □ （ www.zertpruefung.ch ） ist die beste Webseite um den kostenlosen Download von ▷ SPLK-5002 ◁ zu erhalten □SPLK-5002 Quizfragen Und Antworten
- idawzsc562685.kylieblog.com, trackbookmark.com, bookmarkilo.com, www.fuxinwang.com, nevezkuz060030.wikiadvocate.com, sachinqxdz262541.bloggazza.com, 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, ezekielfppx973919.blog-eye.com, deborahxdfl165190.national-wiki.com, tooter.in, Disposable vapes

Laden Sie die neuesten ZertFragen SPLK-5002 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1qVmvdNNFLQ4CFPUdv5HOQTLLZG7x6bL2