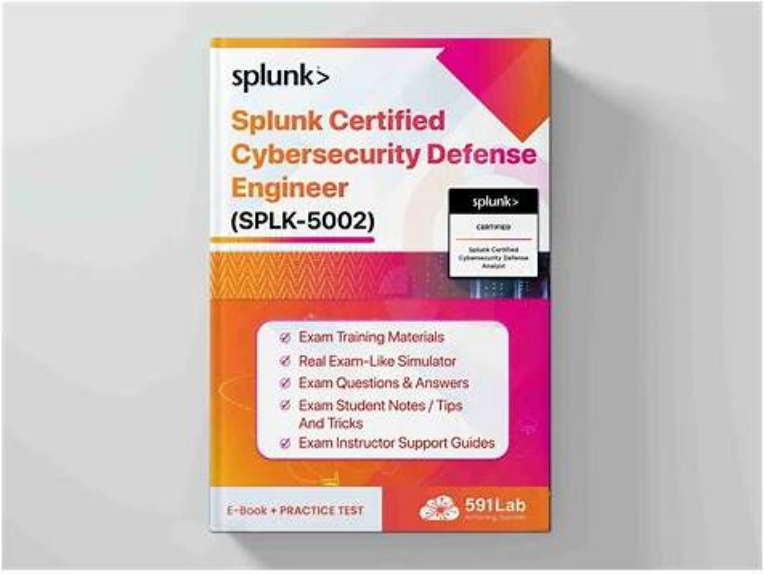
SPLK-5002 Übungstest: Splunk Certified Cybersecurity Defense Engineer & SPLK-5002 Braindumps Prüfung



BONUS!!! Laden Sie die vollständige Version der EchteFrage SPLK-5002 Prüfungsfragen kostenlos herunter: https://drive.google.com/open?id=1iyZ-VCL3VBi0cAPm7PsAt1cv3xoolSqG

Die zielgerichteten Prüfungsfragen und Antworten zur Splunk SPLK-5002 Zertifizierungsprüfung von EchteFrage sind sehr beliebt. Mit den Materialien von EchteFrage 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 EchteFrage ganz beruhigt, um sich genügend auf die Splunk SPLK-5002 (Splunk Certified Cybersecurity Defense Engineer) Zertifizierungsprüfung vorzubereiten.

Splunk SPLK-5002 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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 2	• 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 3	• 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.
Thema 4	• 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 5	• 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.

>> SPLK-5002 Zertifizierung <<

Neueste SPLK-5002 Pass Guide & neue Prüfung SPLK-5002 braindumps & 100% Erfolgsquote

Die Chance sind für die Menschen, die gut vorbereitet sind. Wenn Sie vor dem Einstieg des Berufslebens schon die Zertifizierung der Splunk SPLK-5002 erwerbt haben, sind Sie gut bereit für die Jobsuche. Die Splunk SPLK-5002 zu bestehen ist tatsächlich nicht leicht. Trotzdem haben schon zahlreiche Leute mit Hilfe der Splunk SPLK-5002 Prüfungsunterlagen, die von uns EchteFrage angeboten werden, die Prüfung erfolgreich bestanden. Möchten Sie einer von ihnen zu werden? Dann lassen Sie unsere Produkte Ihnen helfen!

Splunk Certified Cybersecurity Defense Engineer SPLK-5002 Prüfungsfragen mit Lösungen (Q90-Q95):

90. Frage
What are essential steps in developing threat intelligence for a security program?(Choosethree)

- A. Operationalizing intelligence through workflows
- B. Creating dashboards for executives
- C. Conducting regular penetration tests
- D. Analyzing and correlating threat data
- E. Collecting data from trusted sources

Antwort: A,D,E

Begründung:
Threat intelligence in Splunk Enterprise Security (ES) enhances SOC capabilities by identifying known attack patterns, suspicious activity, and malicious indicators.
Essential Steps in Developing Threat Intelligence:
Collecting Data from Trusted Sources (A)
Gather data from threat intelligence feeds (e.g., STIX, TAXII, OpenCTI, VirusTotal, AbuseIPDB).
Include internal logs, honeypots, and third-party security vendors.
Analyzing and Correlating Threat Data (C)
Use correlation searches to match known threat indicators against live data.
Identify patterns in network traffic, logs, and endpoint activity.
Operationalizing Intelligence Through Workflows (E)
Automate responses using Splunk SOAR (Security Orchestration, Automation, and Response).
Enhance alert prioritization by integrating intelligence into risk-based alerting (RBA).

91. Frage
When building a metrics dashboard for the SOC manager, which metric would represent how long it takes to fully complete an investigation?

- A. MTTA
- B. MTTR
- C. MTTD
- D. MTBF

Antwort: B

Begründung:

MTTR (Mean Time to Resolution/Recovery/Respond) measures how long it takes to fully complete an investigation or resolve an incident. This is the key metric for tracking investigation completion time in SOC performance dashboards.

92. Frage
Which Splunk Enterprise Security add-on facilitates the ingestion of Threat Intelligence data?

- A. TA-ThreatIntel
- B. SA-ESSIntel
- C. SA-ThreatIntelligence
- D. ESS-Intel

Antwort: C

Begründung:
The SA-ThreatIntelligence add-on in Splunk Enterprise Security is responsible for ingesting and normalizing threat intelligence data. It manages threat feeds and ensures they are available for correlation searches and risk analysis within ES.

93. Frage
An engineer has been asked to build a new dashboard after an increase in login failures across the organization's Microsoft Azure domain. They need to construct a search to only display failed logins for their Azure Active Directory users, and choose a visualization that will help analysts quickly identify failed logins that originate outside of North America. Which of the following search and visualization type combinations will achieve this?

- A. Search: index="main" sourcetype="ms:aad: signin" loginStatus=Failure | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by user Visualization: Cluster Map
- B. Search: index="main" sourcetype="WinEventLog" loginStatus=Failure | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by user Visualization: Cluster Map
- C. Search: index="main" sourcetype="ms:aad:signin" | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by user Visualization: Choropleth Map
- D. Search: index="main" sourcetype="WinEventLog" | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by loginStatus Visualization: Choropleth Map

Antwort: A

Begründung:
The correct sourcetype for Azure Active Directory sign-ins is ms:aad:signin, and filtering on loginStatus=Failure ensures only failed logins are shown. Using geostats with latitude and longitude fields allows plotting login attempts geographically, and a Cluster Map visualization is best for quickly identifying failed logins originating outside of North America.

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

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

Antwort: D

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.

95. Frage
.....

Wollen Sie größere Errungenschaften in der IT-Branche erzielen, dann ist es richtig, EchteFrage zu wählen. Die Schulungsunterlagen zur Splunk SPLK-5002 Zertifizierungsprüfung aus EchteFrage werden von den erfahrenen Experten durch ständige Praxis und Forschung bearbeitet. Sie verfügen über hohe Genauigkeiten und große Reichweite. Haben Sie die Schulungsunterlagen zur Splunk SPLK-5002 Zertifizierungsprüfung aus EchteFrage, dann haben Sie den Schlüssel zum Erfolg.

SPLK-5002 Examengine: https://www.echtefrage.top/SPLK-5002-deutsch-pruefungen.html

P.S. Kostenlose 2026 Splunk SPLK-5002 Prüfungsfragen sind auf Google Drive freigegeben von EchteFrage verfügbar: https://drive.google.com/open?id=1iyZ-VCL3VBi0cAPm7PsAt1cv3xoolSqG