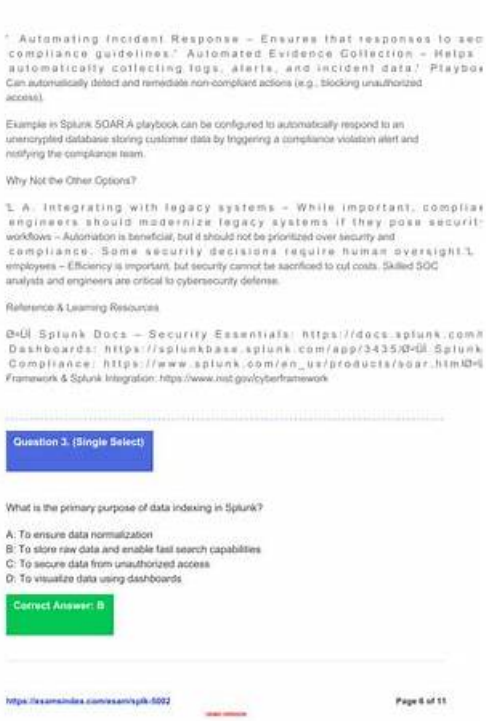
SPLK-5002 valid vce collection & SPLK-5002 latest training dumps


' Automating Incident Response – Ensures that responses to sec
compliance guidelines.' Automated Evidence Collection – Helps
automatically collecting logs, alerts, and incident data.' Playbo
Can automatically detect and remediate non-compliant actions (e.g., blocking unauthorized
access).

Example in Splunk SOAR:A playbook can be configured to automatically respond to an
unencrypted database storing customer data by triggering a compliance violation alert and
notifying the compliance team.

Why Not the Other Options?

'L A. Integrating with legacy systems – While important, compliar
engineers should modernize legacy systems if they pose securit
workflows – Automation is beneficial, but it should not be prioritized over security and
compliance. Some security decisions require human oversight'L
employees – Efficiency is important, but security cannot be sacrificed to cut costs. Skilled SOC
analysts and engineers are critical to cybersecurity defense.

Reference & Learning Resources

@=Ûl Splunk Docs – Security Essentials: https://docs.splunk.com
Dashboards: https://splunkbase.splunk.com/app/3435/@=Ûl Splunk
Compliance: https://www.splunk.com/en_us/products/soar.html@=
Framework & Splunk Integration: https://www.nist.gov/cyberframework

Question 3: (Single Select)

What is the primary purpose of data indexing in Splunk?

A: To ensure data normalization
B: To store raw data and enable fast search capabilities
C: To secure data from unauthorized access
D: To visualize data using dashboards

Correct Answer: B

https://examsindex.com/exam/splk-5002 Page 6 of 11

2026 Latest TestsDumps SPLK-5002 PDF Dumps and SPLK-5002 Exam Engine Free Share: https://drive.google.com/open?id=1WKpY1PHzKjVEq5oSjMv466U4UIx2NOXg

The TestsDumps guarantees their customers that if they have prepared with Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) practice test, they can pass the Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) certification easily. If the applicants fail to do it, they can claim their payment back according to the terms and conditions. Many candidates have prepared from the actual Splunk SPLK-5002 Practice Questions and rated them as the best to study for the examination and pass it in a single try with the best score. The Splunk SPLK-5002 practice material of TestsDumps came into existence after consultation with many professionals and getting their positive reviews.

Knowledge is defined as intangible asset that can offer valuable reward in future, so never give up on it and our SPLK-5002 exam preparation can offer enough knowledge to cope with the exam effectively. To satisfy the needs of exam candidates, our experts wrote our SPLK-5002 practice materials with perfect arrangement and scientific compilation of messages, so you do not need to study other SPLK-5002 training questions to find the perfect one anymore.

>> SPLK-5002 Latest Test Simulations <<

Free PDF 2026 Splunk Reliable SPLK-5002: Splunk Certified Cybersecurity Defense Engineer Latest Test Simulations

If you want to choose passing Splunk certification SPLK-5002 exam to make yourself have a more stable position in today's competitive IT area and the professional ability become more powerful, you must have a strong expertise. And passing Splunk certification SPLK-5002 exam is not very simple. Perhaps passing Splunk Certification SPLK-5002 Exam is a stepping stone to promote yourself in the IT area, but it doesn't need to spend a lot of time and effort to review the relevant knowledge, you can choose to use our TestsDumps product, a training tool prepared for the IT certification exams.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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.
Topic 3	• 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.
Topic 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.
Topic 5	• 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.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q63-Q68):

NEW QUESTION # 63
A company wants to implement risk-based detection for privileged account activities. What should they configure first?

- A. Correlation searches with low thresholds
- B. Event sampling for raw data
- C. Asset and identity information for privileged accounts
- D. Automated dashboards for all accounts

Answer: C

Explanation:
Why Configure Asset & Identity Information for Privileged Accounts First?
Risk-based detection focuses on identifying and prioritizing threats based on the severity of their impact. For privileged accounts (admins, domain controllers, finance users), understanding who they are, what they access, and how they behave is critical.
Key Steps for Risk-Based Detection in Splunk ES:
1. Define Privileged Accounts & Groups - Identify high-risk users (Admin, HR, Finance, CISO).
2. Assign Risk Scores - Apply higher scores to actions involving privileged users.
3. Enable Identity & Asset Correlation - Link users to assets for better detection.
4. Monitor for Anomalies - Detect abnormal login patterns, excessive file access, or unusual privilege escalation.

NEW QUESTION # 64
The SOC manager has a desire to measure mean time to acknowledge findings (notable events) in order to meet a desired service level objective. Which two fields can be used to measure this metric?

- A. Status, Owner
- B. User, Status
- C. Severity, Owner
- D. Urgency, Status

Answer: A

Explanation:
Mean Time to Acknowledge (MTTA) can be measured using the Status and Owner fields. Status indicates when a notable event moves from a new or unacknowledged state, and Owner identifies which analyst acknowledged the event, allowing calculation of the time taken to respond.

NEW QUESTION # 65
A cyber defense engineer plays a role in maintaining a secure SOAR Cloud configuration. Which network security statement is correct about SOAR Cloud?

- A. The Automation Broker initiates an outbound SSL connection to Splunk Cloud, and also initiates an outbound connection to the managed endpoints.
- B. The Automation Broker initiates an outbound SSL connection to Splunk Cloud, and the managed endpoint initiates an outbound connection to the Automation Broker.
- C. Splunk Cloud initiates an outbound SSL connection to both the Automation Broker and managed endpoints.
- D. The Automation Broker initiates an inbound SSL connection to Splunk Cloud, and also initiates an outbound connection to the managed endpoints.

Answer: A

Explanation:
In Splunk SOAR Cloud, the Automation Broker is responsible for maintaining connectivity. It initiates an outbound SSL connection to Splunk Cloud (so no inbound firewall rules are needed) and also makes outbound connections to the managed endpoints to execute playbook actions securely.

NEW QUESTION # 66
What key elements should an audit report include?(Choosetwo)

- A. Analysis of past incidents
- B. Compliance metrics
- C. List of unprocessed log data
- D. Asset inventory details

Answer: A,B

Explanation:
An audit report provides an overview of security operations, compliance adherence, and past incidents, helping organizations ensure regulatory compliance and improve security posture.
Key Elements of an Audit Report:
Analysis of Past Incidents (A)
Includes details on security breaches, alerts, and investigations.
Helps identify recurring threats and security gaps.
Compliance Metrics (C)
Evaluates adherence to regulatory frameworks (e.g., NIST, ISO 27001, PCI-DSS, GDPR).
Measures risk scores, policy violations, and control effectiveness.

NEW QUESTION # 67
Utilizing a Standard Operating Procedure (SOP) is an effective way to ensure that analysts are responding to generated findings in a consistent and analytical manner. Where is the best place within the Notable Adaptive Response Action to include a link to an SOP?

- A. Useful Links
- B. Recommended Actions
- C. Next Steps
- D. Description

Answer: A

Explanation:
The best place to include a link to a Standard Operating Procedure (SOP) within the Notable Adaptive Response Action is Useful Links. This section is designed to provide analysts with quick access to external resources such as SOPs, documentation, or playbooks, ensuring consistent and guided responses.

NEW QUESTION # 68
.....

Many customers may doubt the quality of our SPLK-5002 learning quiz since they haven't tried them. But our SPLK-5002 training engine is reliable. What you have learnt on our SPLK-5002 exam materials are going through special selection. The core knowledge of the real exam is significant. With our guidance, you will be confident to take part in the SPLK-5002 Exam. Our SPLK-5002 study materials will be your good assistant. Put your ideas into practice.

Answers SPLK-5002 Real Questions: https://www.testsdumps.com/SPLK-5002_real-exam-dumps.html

- Splunk SPLK-5002 Exam Dumps in PDF Format □ Copy URL 【 www.exam4labs.com 】 open and search for ➤ SPLK-5002 □ to download for free □SPLK-5002 Certification Dumps
- Test SPLK-5002 Simulator □ Dumps SPLK-5002 Vce □ SPLK-5002 Top Exam Dumps □ Search for 「 SPLK-5002 」 on ➽ www.pdfvce.com □ immediately to obtain a free download □SPLK-5002 Latest Test Questions
- Splunk SPLK-5002 Exam Dumps in PDF Format □ 《 www.testkingpass.com 》 is best website to obtain 《 SPLK-5002 》 for free download □SPLK-5002 Top Exam Dumps
- Testing SPLK-5002 Center □ Key SPLK-5002 Concepts □ SPLK-5002 Top Exam Dumps □ Search for ✔ SPLK-5002 □✔□ and download it for free immediately on ➠ www.pdfvce.com □ □SPLK-5002 Valuable Feedback
- Splunk SPLK-5002 Exam Dumps in PDF Format □ Easily obtain free download of （ SPLK-5002 ） by searching on [www.practicevce.com] □SPLK-5002 Valuable Feedback
- SPLK-5002 Latest Test Simulations | Professional Splunk Certified Cybersecurity Defense Engineer 100% Free Answers Real Questions ☺ Go to website ➡ www.pdfvce.com □□□ open and search for □ SPLK-5002 □ to download for free □ □New SPLK-5002 Dumps Free
- Test SPLK-5002 Simulator □ Test SPLK-5002 Simulator □ Test SPLK-5002 Simulator ✴ Easily obtain □ SPLK-5002 □ for free download through ➤ www.exam4labs.com □ □SPLK-5002 Latest Test Questions
- Free PDF Quiz Reliable Splunk - SPLK-5002 Latest Test Simulations □ Open ➥ www.pdfvce.com □ enter ⇛ SPLK-5002 ⇚ and obtain a free download □Test SPLK-5002 Simulator
- Test SPLK-5002 Simulator □ SPLK-5002 New Soft Simulations □ Free SPLK-5002 Brain Dumps □ Enter （ www.examcollectionpass.com ） and search for ➽ SPLK-5002 □ to download for free □Dumps SPLK-5002 Vce
- Study Guide SPLK-5002 Pdf □ Free SPLK-5002 Brain Dumps □ Dumps SPLK-5002 Vce □ Open ☀ www.pdfvce.com □☀□ enter ➠ SPLK-5002 □ and obtain a free download □SPLK-5002 Complete Exam Dumps
- New SPLK-5002 Exam Prep □ SPLK-5002 Latest Exam Format □ Study Guide SPLK-5002 Pdf □ Easily obtain free download of { SPLK-5002 } by searching on ➤ www.prep4sures.top □ □SPLK-5002 Exam Certification Cost
- barbarajkmw894051.blogtov.com, esocialmall.com, socialislife.com, zoyaxtaa048492.blogaritma.com, iwanttobookmark.com, minaytgj134106.idblogmaker.com, iowa-bookmarks.com, jasperbywc265085.onzeblog.com, harleyolic102074.blogsidea.com, learn.csisafety.com.au, Disposable vapes

P.S. Free 2026 Splunk SPLK-5002 dumps are available on Google Drive shared by TestsDumps: https://drive.google.com/open?id=1WKpY1PHzKjVEq5oSjMv466U4UIx2NOXg