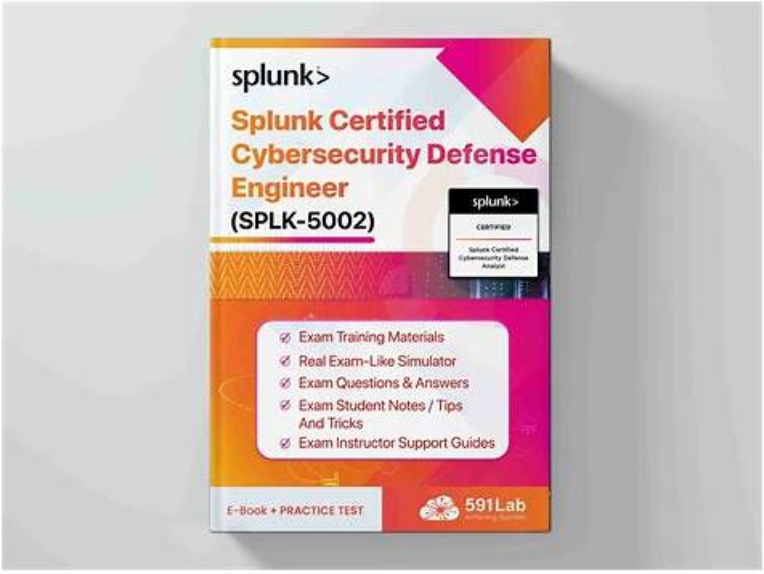
Real Splunk SPLK-5002 Exam Question Samples For Free



BTW, DOWNLOAD part of Prep4SureReview SPLK-5002 dumps from Cloud Storage: https://drive.google.com/open?id=1-LpKj70D-Kl845KOX0xpcJfV0dUsMroJ

With every Splunk SPLK-5002 practice test attempt, you will see yourself improve gradually, and on Splunk SPLK-5002 exam day, you will be able to finish the Splunk Certified Cybersecurity Defense Engineer SPLK-5002 exam as far as possible and space enough time to do an entire check for careless mistakes. Download the full version of Prep4SureReview SPLK-5002 PDF Questions and practice tests and start your professional journey. We ensure you can pass the Splunk Certified Cybersecurity Defense Engineer SPLK-5002 exam on the first attempt.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 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.
Topic 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.
Topic 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.
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.

>> SPLK-5002 Valid Exam Papers <<

Valid SPLK-5002 Test Practice | SPLK-5002 Exam Certification

We are a team of certified professionals with lots of experience in editing SPLK-5002 exam questions. Every candidate should have more than 11 years' education experience in this filed of SPLK-5002 study guide. We have rather a large influence over quite a quantity of candidates. We are more than more popular by our high passing rate and high quality of our SPLK-5002 Study Guide. Our education team of professionals will give you the best of what you deserve. If you are headache about your SPLK-5002 certification exams, our SPLK-5002 training materials will be your best select.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q43-Q48):

NEW QUESTION # 43
What is the role of aggregation policies in correlation searches?

- A. To index events from multiple sources
- B. To normalize event fields for dashboards
- C. To automate responses to critical events
- D. To group related notable events for analysis

Answer: D

Explanation:
Aggregation policies in Splunk Enterprise Security (ES) are used to group related notable events, reducing alert fatigue and improving incident analysis.
Role of Aggregation Policies in Correlation Searches:
Group Related Notable Events (A)
Helps SOC analysts see a single consolidated event instead of multiple isolated alerts.
Uses common attributes like user, asset, or attack type to aggregate events.
Improves Incident Response Efficiency
Reduces the number of duplicate alerts, helping analysts focus on high-priority threats.

NEW QUESTION # 44
When generating documentation for a security program, what key element should be included?

- A. Financial cost breakdown
- B. Vendor contract details
- C. Standard operating procedures (SOPs)
- D. Organizational hierarchy chart

Answer: C

Explanation:
Key Elements of Security Program Documentation
A security program's documentation ensures consistency, compliance, and efficiency in cybersecurity operations.
#Why Include Standard Operating Procedures (SOPs)?
Defines step-by-step processesfor security tasks.
Ensures security teams followstandardized workflowsfor handling incidents, vulnerabilities, and monitoring.
Supportscompliance with regulationslikeNIST, ISO 27001, and CIS controls.
Example:

SOP forincident responseoutlines how analysts escalate security threats.
#Incorrect Answers:
A: Vendor contract details# Vendor agreements are important butnot core to a security program's documentation.
B: Organizational hierarchy chart# Useful for internal structure butnot essential for security documentation.
D: Financial cost breakdown# Related to budgeting, not security operations.
#Additional Resources:
NIST Security Documentation Framework
Splunk Security Operations Guide

NEW QUESTION # 45
A company's Splunk setup processes logs from multiple sources with inconsistent field naming conventions.
Howshould the engineer ensure uniformity across data for better analysis?

- A. Configure index-time data transformations.
- B. Apply Common Information Model (CIM) data models for normalization.
- C. Create field extraction rules at search time.
- D. Use data model acceleration for real-time searches.

Answer: B

Explanation:
Why Use CIM for Field Normalization?
When processing logs from multiple sources with inconsistent field names, the best way to ensure uniformity is to use Splunk's Common Information Model (CIM).
#Key Benefits of CIM for Normalization:
Ensures that different field names (e.g., src_ip, ip_src, source_address) are mapped to a common schema.
Allows security teams to run a single search query across multiple sources without manual mapping.
Enables correlation searches in Splunk Enterprise Security (ES) for better threat detection.
Example Scenario in a SOC:
#Problem: The SOC team needs to correlate firewall logs, cloud logs, and endpoint logs for failed logins.
#Without CIM: Each log source uses a different field name for failed logins, requiring multiple search queries.
#With CIM: All failed login events map to the same standardized field (e.g., action="failure"), allowing one unified search query.
Why Not the Other Options?
#A. Create field extraction rules at search time - Helps with parsing data but doesn't standardize field names across sources.#B. Use data model acceleration for real-time searches - Accelerates searches but doesn't fix inconsistent field naming.#D. Configure index-time data transformations - Changes fields at indexing but is less flexible than CIM's search-time normalization.
References & Learning Resources
#Splunk CIM for Normalization: https://docs.splunk.com/Documentation/CIM#Splunk ES CIM Field Mappings: https://splunkbase.splunk.com/app/263#Best Practices for Log Normalization: https://www.splunk.com/en_us/blog/tips-and-tricks

NEW QUESTION # 46
What feature allows you to extract additional fields from events at search time?

- A. Search-time field extraction
- B. Index-time field extraction
- C. Event parsing
- D. Data modeling

Answer: A

Explanation:
Splunk allows dynamic field extraction to enhance data analysis without modifying raw indexed data.
Search-Time Field Extraction:
Extracts fields on-demand when running searches.
Uses Splunk's Field Extraction Engine (rex,spath, or automatic field discovery).
Minimizes indexing overhead by keeping the raw data unchanged.

NEW QUESTION # 47
A security engineer is tasked with improving threat intelligence sharing within the company.
Whatis the most effective first step?

- A. Use threat intelligence only for executive reporting.
- B. Implement a real-time threat feed integration.
- C. Share raw threat data with all employees.
- D. Restrict access to external threat intelligence sources.

Answer: B

Explanation:
Improving Threat Intelligence Sharing in an Organization
Threat intelligence enhances cybersecurity by providing real-time insights into emerging threats.
#1. Implement a Real-Time Threat Feed Integration (A)
Enables real-time ingestion of threat indicators (IOCs, IPs, hashes, domains).
Helps automate threat detection and blocking.
Example:
Integrating STIX/TAXII, Splunk Threat Intelligence Framework, or a SOAR platform for live threat updates.
#Incorrect Answers:
B: Restrict access to external threat intelligence sources # Sharing intelligence enhances security, not restricting it.
C: Share raw threat data with all employees # Raw intelligence needs analysis and context before distribution.
D: Use threat intelligence only for executive reporting # SOC analysts, incident responders, and IT teams need actionable intelligence.
#Additional Resources:
Splunk Threat Intelligence Framework
How to Integrate STIX/TAXII in Splunk

NEW QUESTION # 48
.....

Format

- SPLK-5002 Valid Exam Papers - Splunk Splunk Certified Cybersecurity Defense Engineer - Trustable Valid SPLK-5002 Test Practice □ Easily obtain ➤ SPLK-5002 □ for free download through ▹ www.pdfvce.com ◃ □SPLK-5002 Reliable Test Syllabus
- SPLK-5002 Authorized Test Dumps □ SPLK-5002 Reliable Braindumps Files □ SPLK-5002 Latest Exam Format □ □ Go to website （ www.practicevce.com ） open and search for ➡ SPLK-5002 □□□ to download for free □ □Authentic SPLK-5002 Exam Hub
- www.stes.tyc.edu.tw, szw0.com, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.mochome.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, kumu.io, Disposable vapes

BTW, DOWNLOAD part of Prep4SureReview SPLK-5002 dumps from Cloud Storage: https://drive.google.com/open?id=1-LpKj70D-Kl845KOX0xpcJfV0dUsMroJ