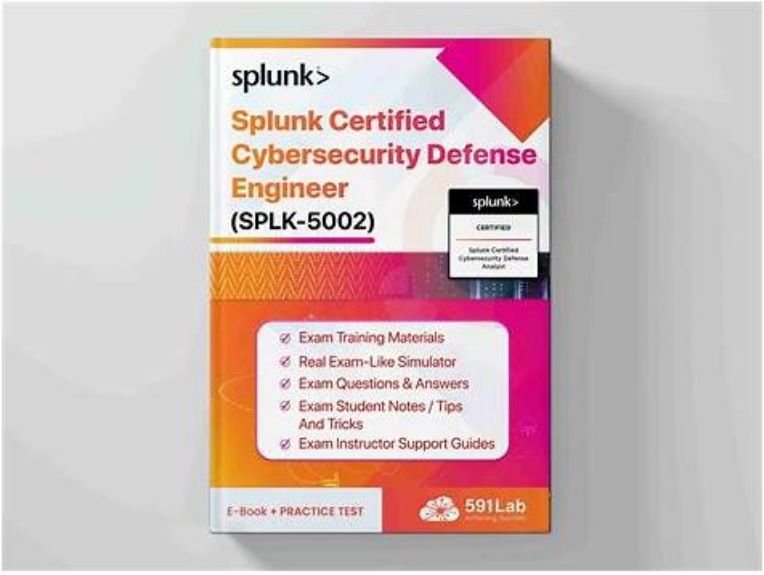
100% Pass 2026 Updated SPLK-5002: Exam Sample Splunk Certified Cybersecurity Defense Engineer Questions



What's more, part of that BraindumpQuiz SPLK-5002 dumps now are free: https://drive.google.com/open?id=1wAVqktj1WMBRAgdpcn6udmZG5tSzTXvQ

Splunk Certified Cybersecurity Defense Engineer Exam Questions save your study time and help you prepare in less duration. We have hundreds of most probable questions which have a chance to appear in the real Splunk Certified Cybersecurity Defense Engineer exam. The Splunk SPLK-5002 exam questions are affordable and 365 days free updated, and you can use them without any guidance. However, in case of any trouble, our support team is always available to sort out the problems. We will provide you with the information covered in the current test and incorporate materials that originate from Splunk SPLK-5002 Exam Dumps.

Our test bank includes all the possible questions and answers which may appear in the real exam and the quintessence and summary of the exam papers in the past. We strive to use the simplest language to make the learners understand our SPLK-5002 study materials and the most intuitive method to express the complicated and obscure concepts. For the learners to fully understand our SPLK-5002 Study Materials, we add the instances, simulation and diagrams to explain the contents which are very hard to understand. So after you use our SPLK-5002 study materials you will feel that our SPLK-5002 study materials' name matches with the reality.

>> Exam Sample SPLK-5002 Questions <<

Latest Exam Sample SPLK-5002 Questions Offer You The Best Valid Exam Duration | Splunk Splunk Certified Cybersecurity Defense Engineer

If you have the certificate, you can enjoy many advantages: you can enter a big enterprise and double your salary and buy things you want. SPLK-5002 learning materials will offer you such a chance to you. With skilled professionals to compile the SPLK-5002 exam materials of us, we will give you the high-quality study guide materials. In addition, we offer you free update for one year, that is to say, in the following year, you can obtain the latest version for SPLK-5002 Exam Materials once they updates. We have service stuff to answer any of your confusions.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details

Topic 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.
Topic 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.
Topic 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.
Topic 4	• 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 5	• 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.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q71-Q76):

NEW QUESTION # 71
What document can be helpful in understanding the prioritization of risk when comparing entities in an organization?

- A. Application architecture diagrams
- B. Infrastructure architecture diagrams
- C. Business Continuity or Disaster Recovery plan
- D. A hierarchical organization chart

Answer: C

Explanation:
A Business Continuity or Disaster Recovery (BC/DR) plan identifies critical business processes, systems, and dependencies. It helps in understanding the prioritization of risk across entities in the organization, ensuring that the most business-critical assets are given higher priority in risk- based alerting and response.

NEW QUESTION # 72
A Splunk administrator needs to integrate a third-party vulnerability management tool to automate remediation workflows. What is the most efficient first step?

- A. Set up a manual alerting system for vulnerabilities
- B. Configure custom dashboards to monitor vulnerabilities
- C. Write a correlation search for each vulnerability type
- D. Use REST APIs to integrate the third-party tool with Splunk SOAR

Answer: D

Explanation:
Why Use REST APIs for Integration?
When integrating a third-party vulnerability management tool (e.g., Tenable, Qualys, Rapid7) with Splunk SOAR, using REST APIs

is the most efficient and scalable approach.
Why REST APIs?
APIs enable direct communication between Splunk SOAR and the third-party tool.
Allows automated ingestion of vulnerability data into Splunk.
Supports automated remediation workflows (e.g., patch deployment, firewall rule updates).
Reduces manual work by allowing Splunk SOAR to pull real-time data from the vulnerability tool.
Steps to Integrate a Third-Party Vulnerability Tool with Splunk SOAR Using REST API:
1. Obtain API Credentials - Get API keys or authentication tokens from the vulnerability management tool.
2. Configure REST API Integration - Use Splunk SOAR's built-in API connectors or create a custom REST API call.
3. Ingest Vulnerability Data into Splunk - Map API responses to Splunk ES correlation searches.
4. Automate Remediation Playbooks - Build Splunk SOAR playbooks to:
Automatically open tickets for critical vulnerabilities.
Trigger patches or firewall rules for high-risk vulnerabilities.
Notify SOC analysts when a high-risk vulnerability is detected on a critical asset.
Example Use Case in Splunk SOAR:
Scenario: The company uses Tenable.io for vulnerability management.
Splunk SOAR connects to Tenable's API and pulls vulnerability scan results.
If a critical vulnerability is found on a production server, Splunk SOAR:
Automatically creates a ServiceNow ticket for remediation.
Triggers a patching script to fix the vulnerability.
Updates Splunk ES dashboards for tracking.

NEW QUESTION # 73
Which of the following detections would use a high count of events with Windows Event Code 4740 grouped by a user to determine suspicious behavior?

- A. Detect Excessive AWS Security Scanning
- B. Detect Excessive User Account Lockouts
- C. Detect Excessive Network Connections
- D. Detect Excessive User Logins

Answer: B

Explanation:
Windows Event Code 4740 indicates that a user account has been locked out. A high count of these events grouped by user would therefore map to the detection "Detect Excessive User Account Lockouts", signaling possible brute-force or malicious login attempts.

NEW QUESTION # 74
What field is used by default to direct data into CIM data model datasets?

- A. sourcetype
- B. tag
- C. dataset
- D. source

Answer: B

Explanation:
By default, data is directed into CIM (Common Information Model) data model datasets using the tag field. Tags applied to events determine which datasets the events populate, enabling normalization and alignment with CIM.

NEW QUESTION # 75
What should a security engineer prioritize when building a new security process?

- A. Reducing the overall number of employees required
- B. Integrating it with legacy systems

- C. Ensuring it aligns with compliance requirements
- D. Automating all workflows within the process

Answer: C

Explanation:
When aSecurity Engineeris building a new security process, theirtop priorityshould be ensuring that the process aligns withcompliance requirements. This is crucial because compliance dictates the legal, regulatory, and industry standards that organizations must follow to protect sensitive data and maintain trust.
Why Compliance is the Top Priority?
Legal and Regulatory Obligations- Many industries are required to follow compliance standards such asGDPR, HIPAA, PCI-DSS, NIST, ISO 27001, and SOX. Non-compliance can lead toheavy fines and legal actions.
Data Protection & Privacy- Compliance ensures that sensitive information is handled securely, preventingdata breachesandunauthorized access.
Risk Reduction- Following compliance standards helps mitigate cybersecurity risks byimplementing security best practicessuch as encryption, access controls, and logging.
Business Reputation & Trust- Organizations that comply with standards buildcustomer confidence and industry credibility.
Audit Readiness- Security teams must ensure that logs, incidents, and processes align with compliance frameworks topass internal/external auditseasily.
How Does Splunk Enterprise Security (ES) Help with Compliance?
Splunk ES is aSecurity Information and Event Management (SIEM)tool that helps organizations meet compliance requirements by:
#Log Management & Retention- Stores and correlates security logs forauditability and forensic investigation.
#Real-time Monitoring & Alerts- Detects suspicious activity andalerts SOC teams.#Prebuilt Compliance Dashboards- Comes with out-of-the-box dashboards forPCI-DSS, GDPR, HIPAA, NIST 800-53, and other frameworks.#Automated Reporting- Generates reports that can be used forcompliance audits.
Example in Splunk ES:A security engineer can createcorrelation searches and risk-based alerting (RBA)to monitor and enforce compliance policies.
How Does Splunk SOAR Help Automate Compliance-Driven Security Processes?
Splunk SOAR (Security Orchestration, Automation, and Response) enhances compliance processes by:
#Automating Incident Response- Ensures that responses to security threats followpredefined compliance guidelines.#Automated Evidence Collection- Helps inaudit documentationby automatically collecting logs, alerts, and incident data.#Playbooks for Compliance Violations- Can automaticallydetect and remediatenon- compliant actions (e.g., blocking unauthorized access).
Example in Splunk SOAR:Aplaybookcan be configured to automaticallyrespond to an unencrypted database storing customer databy triggering a compliance violation alert and notifying the compliance team.
Why Not the Other Options?
#A. Integrating with legacy systems- While important,compliance is a higher priority. Security engineers shouldmodernizelegacy systems if they pose security risks.#C. Automating all workflows- Automation is beneficial, but it should not be prioritizedover security and compliance. Some security decisions requirehuman oversight.#D. Reducing the number of employees- Efficiency is important, butsecurity cannot be sacrificedto cut costs. Skilled SOC analysts and engineers arecritical to cybersecurity defense.
References & Learning Resources
#Splunk Docs - Security Essentials: https://docs.splunk.com/#Splunk ES Compliance Dashboards: https://splunkbase.splunk.com/app/3435/#Splunk SOAR Playbooks for Compliance: https://www.splunk.com/en_us/products/soar.html#NIST Cybersecurity Framework & Splunk Integration: https://www.nist.gov/cyberframework

NEW QUESTION # 76
.....

We own three versions of the SPLK-5002 exam torrent for you to choose. They conclude PDF version, PC version and APP online version. You can choose the most convenient version of the SPLK-5002 quiz torrent. The three versions of the SPLK-5002 test prep boost different strengths and you can find the most appropriate choice. For example, the PDF version is convenient for download and printing and is easy and convenient for review and learning. It can be printed into papers and is convenient to make notes. You can learn the SPLK-5002 Test Prep at any time or place and repeatedly practice. The version has no limit for the amount of the persons and times. The PC version of SPLK-5002 quiz torrent is suitable for the computer with Windows system. It can simulate real operation exam atmosphere and simulate exams.

Valid SPLK-5002 Exam Duration: https://www.braindumpquiz.com/SPLK-5002-exam-material.html

- High Quality SPLK-5002 Prep Guide Dump is Most Valid SPLK-5002 Certification Materials □ Immediately open ➠ www.prepawaypdf.com □ and search for □ SPLK-5002 □ to obtain a free download □Latest SPLK-5002 Test

Question

- SPLK-5002 Practice Test □ Customizable SPLK-5002 Exam Mode □ Reliable SPLK-5002 Test Pass4sure □ Search for ➽ SPLK-5002 □ and obtain a free download on ▸ www.pdfvce.com ◂ □VCE SPLK-5002 Exam Simulator
- SPLK-5002 Practice Test □ SPLK-5002 Latest Exam Cram □ Valid SPLK-5002 Exam Answers □ Open website [www.examcollectionpass.com] and search for ➥ SPLK-5002 □ for free download □Vce SPLK-5002 Test Simulator
- Reliable Exam Sample SPLK-5002 Questions – Fast Download Valid Exam Duration for SPLK-5002 □ Enter 「 www.pdfvce.com 」 and search for " SPLK-5002 " to download for free □Customizable SPLK-5002 Exam Mode
- Splunk Certified Cybersecurity Defense Engineer Exam Dumps Get Success With Minimal Effort □ Search on { www.troytecdumps.com } for ✔ SPLK-5002 □✔□ to obtain exam materials for free download □SPLK-5002 New Real Test
- High Quality SPLK-5002 Prep Guide Dump is Most Valid SPLK-5002 Certification Materials □ Search for ☀ SPLK-5002 □☀□ and obtain a free download on □ www.pdfvce.com □ □VCE SPLK-5002 Exam Simulator
- Easy To Use and Compatible www.pdfdumps.com Splunk SPLK-5002 Questions Formats □ Enter ➠ www.pdfdumps.com □ and search for □ SPLK-5002 □ to download for free □Latest SPLK-5002 Test Question
- High Quality SPLK-5002 Prep Guide Dump is Most Valid SPLK-5002 Certification Materials □ Enter ➥ www.pdfvce.com □ and search for 【 SPLK-5002 】 to download for free □Reliable SPLK-5002 Test Dumps
- VCE SPLK-5002 Exam Simulator □ Latest SPLK-5002 Test Question □ SPLK-5002 Exam Sims □ Open website { www.pass4test.com } and search for { SPLK-5002 } for free download □Vce SPLK-5002 Test Simulator
- Latest SPLK-5002 Test Question □ SPLK-5002 Valid Test Topics □ Latest SPLK-5002 Dumps Pdf □ The page for free download of ➥ SPLK-5002 □ on ➤ www.pdfvce.com □ will open immediately □SPLK-5002 Exam Topics
- Trusting Effective Exam Sample SPLK-5002 Questions Is The First Step to Pass Splunk Certified Cybersecurity Defense Engineer □ Open " www.prepawaypdf.com " and search for { SPLK-5002 } to download exam materials for free □ □VCE SPLK-5002 Exam Simulator
- enrollbookmarks.com, safiyampwe744072.mdkblog.com, bookmarkfavors.com, victortcir628099.blognody.com, idatjdh232082.digitollblog.com, quay.io, lulukhpa952641.theobloggers.com, sahilpxhu198287.jasperwiki.com, my-social-box.com, keirannzni599843.blogsumer.com, Disposable vapes

DOWNLOAD the newest BraindumpQuiz SPLK-5002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1wAVqktj1WMBRAgdpcn6udmZG5tSzTXvQ