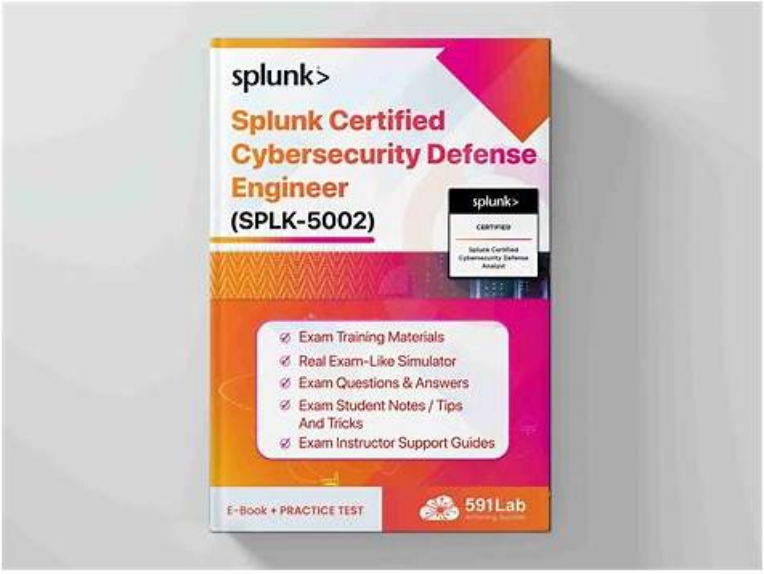
Latest SPLK-5002 Exam Fee, Reliable SPLK-5002 Exam Camp



P.S. Free 2026 Splunk SPLK-5002 dumps are available on Google Drive shared by ExamsReviews: https://drive.google.com/open?id=1VRZznDg4bb9Re5EXTHWfdiIV_22cPYdp

Our desktop Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) practice exam software allows you to see your progress report at the end of each attempt. In this way, you find your mistakes and overcome them before the final take. Our desktop software is customizable so you can change the duration and Splunk questions of SPLK-5002 Practice Tests according to your learning requirements. Since this software requires installation on Windows computers, you can take the Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) practice exam offline.

We boost the expert team to specialize in the research and production of the SPLK-5002 guide questions and professional personnel to be responsible for the update of the study materials. We keep a close watch at the change of the popular trend among the industry and the latest social views so as to keep pace with the times and provide the clients with the newest SPLK-5002 Study Materials resources. And clients are our gods and the clients' satisfaction with our SPLK-5002 guide material is the biggest resource of our happiness. So why you still hesitated? Go and buy our SPLK-5002 guide questions now.

>> Latest SPLK-5002 Exam Fee <<

Excellent Splunk SPLK-5002 Practice Material's 3 formats

The Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) exam dumps are real and updated SPLK-5002 exam questions that are verified by subject matter experts. They work closely and check all SPLK-5002 exam dumps one by one. They maintain and ensure the top standard of ExamsReviews SPLK-5002 Exam Questions all the time. The SPLK-5002 practice test is being offered in three different formats. These SPLK-5002 exam questions formats are PDF dumps files, web-based practice test software, and desktop practice test software.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 (Q33-Q38):

NEW QUESTION # 33
A new playbook needs to be developed for automated phishing analysis and response.
Configured in SOAR are integrations with Splunk Enterprise Security and actions from assets that pull in user-reported emails, perform automated threat analysis, add blocks on the proxy, and an EDR vendor to take various actions. Which would be the best workflow for the new playbook?

- A. 1. Ingest the email from the mail vendor
  2. Detonate email in the automated threat analysis system and collect verdict, looking for malicious indicators
  3. Search the mail system for all users that received the email
  4. Block all URLs and processes with the proxy and EDR solutions
- B. 1. Submit the email from Splunk Enterprise Security
  2. Search the mail system for all users that received the email
  3. Review results from the automated threat analysis
  4. Block any malicious URLs and processes with the proxy and EDR solutions
- C. 1. Ingest the email from the mail vendor
  2. Detonate email in the automated threat analysis system and collect verdict, looking for malicious indicators
  3. Search the mail system for all users that received the email
  4. Block any malicious URLs and processes with the proxy and EDR solutions
- D. 1. Submit the user reported email from Splunk Enterprise Security
  2. Search the mail system for all users that received the email
  3. Review results from the automated threat analysis
  4. Block any malicious URLs and processes with the proxy and EDR solutions

Answer: C

Explanation:
The best workflow for automated phishing analysis and response is:
1. Ingest the email from the mail vendor - acquire the reported email for analysis.
2. Detonate the email in the automated threat analysis system and collect verdict - determine if the email is malicious and extract indicators.
3. Search the mail system for all users that received the email - identify impacted users.
4. Block any malicious URLs and processes with the proxy and EDR solutions - take targeted remediation based on verified malicious indicators.

NEW QUESTION # 34
Which of the following is not a type of metadata that can be returned by the metadata command?

- A. hosts
- B. assets
- C. sources
- D. sourcetypes

Answer: B

Explanation:
The metadata command in Splunk can return information about sourcetypes, hosts, and sources, but it does not return data about assets. Assets are managed separately in Enterprise Security's asset and identity framework, not through the metadata command.

NEW QUESTION # 35
Which action improves the effectiveness of notable events in Enterprise Security?

- A. Limiting the search scope to one index
- B. Disabling scheduled searches
- C. Using only raw log data in searches
- D. Applying suppression rules for false positives

Answer: D

NEW QUESTION # 36
What methods can improve Splunk's indexing performance?(Choosetwo)

- A. Optimize event breaking rules.
- B. Use universal forwarders for data ingestion.
- C. Create multiple search heads.
- D. Enable indexer clustering.

Answer: A,D

Explanation:
Improving Splunk's indexing performance is crucial for handling large volumes of data efficiently while maintaining fast search speeds and optimized storage utilization.
Methods to Improve Indexing Performance:
Enable Indexer Clustering (A)
Distributes indexing load across multiple indexers.
Ensures high availability and fault tolerance by replicating indexed data.
Optimize Event Breaking Rules (D)
Defines clear event boundaries to reduce processing overhead.
Uses correctLINE_BREAKERandTRUNCATEsettings to improve parsing speed.

NEW QUESTION # 37
A Splunk administrator needs to integrate a third-party vulnerability management tool to automate remediation workflows. What is the most efficient first step?

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

Answer: A

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 # 38
.....

In order to meet the different need from our customers, the experts and professors from our company designed three different versions of our SPLK-5002 exam questions for our customers to choose, including the PDF version, the online version and the software version. Though the content of the SPLK-5002 Study Materials is the same, but the displays are totally different to make sure that our customers can study our SPLK-5002 learning guide at any time and condition.

bookmarksden.com, zaynabbccu907802.vigilwiki.com, jimbnnd219956.wikilentillas.com, darrenahth411759.blogunteer.com, deborahwwqf469514.therainblog.com, lancegrxe875525.blogvivi.com, Disposable vapes

DOWNLOAD the newest ExamsReviews SPLK-5002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1VRZznDg4bb9Re5EXTHWfdiIV_22cPYdp