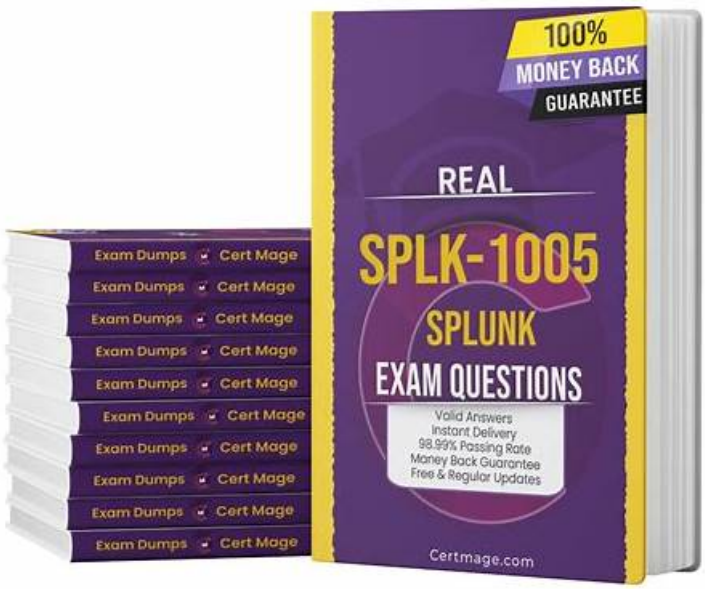
Free PDF Quiz 2026 Splunk SPLK-5002–High Pass-Rate Reliable Dumps Files



DOWNLOAD the newest SurePassExams SPLK-5002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1SdXkFwyQK_I37DXobKblUKARA3Uzv8d0

If you want to pass the SPLK-5002 exam and get the related certification in the shortest time, choosing the SPLK-5002 training materials from our company will be in the best interests of all people. We can make sure that it will be very easy for you to pass your SPLK-5002 exam and get the related certification in the shortest time that beyond your imagination. You can know the instructions on the SPLK-5002 Certification Training materials from our web. And you can also free download the demo of our SPLK-5002 exam questions to check before your payment.

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	• 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	• 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.

Authoritative Reliable SPLK-5002 Dumps Files | 100% Free SPLK-5002 Test Pdf

Living in such a world where competitiveness is a necessity that can distinguish you from others, every one of us is trying our best to improve ourselves in every way. It has been widely recognized that the SPLK-5002 exam can better equip us with a newly gained personal skill, which is crucial to individual self-improvement in today's computer era. With the certified advantage admitted by the test SPLK-5002 Certification, you will have the competitive edge to get a favorable job in the global market. Here our SPLK-5002 exam preparation materials are tailor-designed for you to pass the SPLK-5002 exam.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q96-Q101):

NEW QUESTION # 96
A security analyst needs to update the SOP for handling phishing incidents.
What should they prioritize?

- A. Reporting incidents to the executive board immediately
- B. Ensuring all reports are manually verified by analysts
- C. Automating the isolation of suspected phishing emails
- D. Documenting steps for user awareness training

Answer: D

Explanation:
Updating the SOP for Handling Phishing Incidents
AStandard Operating Procedure (SOP)should focus onprevention, detection, and response.
#1. Documenting Steps for User Awareness Training (C)
Training employeeshelps prevent phishing incidents.
Example:
Teach users toidentify phishing emails and report them via a Splunk SOAR playbook.
#Incorrect Answers:
A: Ensuring all reports are manually verified by analysts#Automation(via SOAR) should be used forinitial triage.
B: Automating the isolation of suspected phishing emails# Automation is useful, butuser education prevents incidents.
D: Reporting incidents to the executive board immediately#Only major security breachesshould beescalated to executives.
#Additional Resources:
NIST Incident Response Guide
Splunk Phishing Detection Playbooks

NEW QUESTION # 97
Based on a recent red team exercise, an organization is highly concerned about pass the hash attacks especially including tools like Empire. Which Eventcode associated to PowerShell Script Block Logging would be used to detect this activity?

- A. EventCode=4126
- B. EventCode=4168

- C. EventCode=4104
- D. EventCode=4624

Answer: C

Explanation:
EventCode=4104 is associated with PowerShell Script Block Logging, which records the full content of executed PowerShell scripts. This is critical for detecting malicious frameworks like Empire that rely on PowerShell for pass-the-hash and other attack techniques.

NEW QUESTION # 98
Which of the following cURL commands would allow an engineer to effectively disable the REST API endpoint they've been utilizing for testing a detection named TestSearchDevelopment?

- A. Splunk endpoints cannot be disabled.
- B. curl -k -u admin:pass
  https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/ -X DELETE
- C. curl -k -u admin:pass
  https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable
  -X PUT
- D. curl -k -u admin:pass
  https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable
  -X POST

Answer: D

Explanation:
To disable a saved search (detection) via the Splunk REST API, the correct syntax is a POST request to the .../disable endpoint. Thus, the proper cURL command is curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/saved/searches/TestSearchDevelopment/disable
-X POST

NEW QUESTION # 99
Which Enterprise Security components provide enrichment to the Risk Framework?

- A. Assets & Identities Framework, Threat Intelligence, Notes
- B. Risk Object, Notable Framework, Data Models
- C. Assets & Identities Framework, Risk Factoring, Annotations
- D. Risk Object, Threat Intelligence, Data models

Answer: C

Explanation:
The Risk Framework in Enterprise Security is enriched by the Assets & Identities Framework (providing contextual information about users and systems), Risk Factoring (applying multipliers to adjust risk scoring), and Annotations (such as MITRE ATT&CK mappings). These components work together to provide meaningful, prioritized risk findings.

NEW QUESTION # 100
Which sourcetype configurations affect data ingestion?(Choosethree)

- A. Event breaking rules
- B. Data retention policies
- C. Line merging rules
- D. Timestamp extraction

Answer: A,C,D

Explanation:

The sourcetype in Splunk defines how incoming machine data is interpreted, structured, and stored. Proper sourcetype configurations ensure accurate event parsing, indexing, and searching.
#1. Event Breaking Rules (A)
Determines how Splunk splits raw logs into individual events.
If misconfigured, a single event may be broken into multiple fragments or multiple log lines may be combined incorrectly.
Controlled using LINE_BREAKER and BREAK_ONLY_BEFORE settings.
#2. Timestamp Extraction (B)
Extracts and assigns timestamps to events during ingestion.
Incorrect timestamp configuration leads to misplaced events in time-based searches.
Uses TIME_PREFIX, MAX_TIMESTAMP_LOOKAHEAD, and TIME_FORMAT settings.
#3. Line Merging Rules (D)
Controls whether multiline events should be combined into a single event.
Useful for logs like stack traces or multi-line syslog messages.
Uses SHOULD_LINEMERGE and LINE_BREAKER settings.
C: Data Retention Policies #
Affects storage and deletion, not data ingestion itself.
#Additional Resources:
Splunk Sourcetype Configuration Guide
Event Breaking and Line Merging

NEW QUESTION # 101
.....

Having a good command of professional knowledge for customers related to this SPLK-5002 exam is of superior condition. However, that is not certain and sure enough to successfully pass this exam. You need efficiency and exam skills as well. Actually, a great majority of exam candidates feel abstracted at this point, wondering which one is the perfect practice material they are looking for. To make things clear, we will instruct you on the traits of our SPLK-5002 real materials one by one. Here we recommend our SPLK-5002 guide question for your reference.

P.S. Free 2026 Splunk SPLK-5002 dumps are available on Google Drive shared by SurePassExams: https://drive.google.com/open?id=1SdXkFwyQK_I37DXobKblUKARA3Uzv8d0