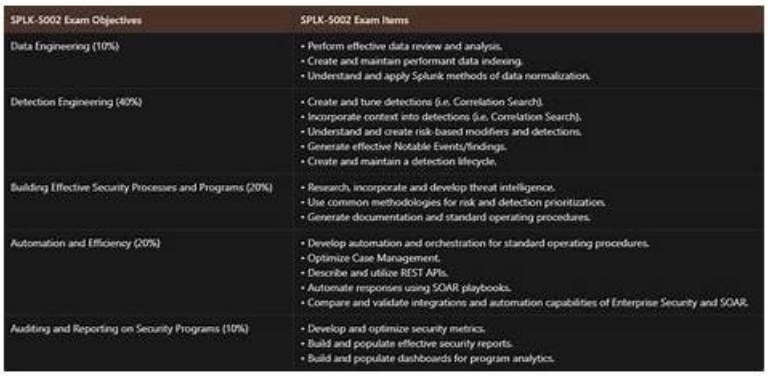
SPLK-5002 Reliable Cram Materials, SPLK-5002 Exam Materials



SPLK-5002 Exam Objectives	SPLK-5002 Exam Items
Data Engineering (10%)	• Perform effective data review and analysis. • Create and maintain performant data indexing. • Understand and apply Splunk methods of data normalization.
Detection Engineering (40%)	• Create and tune detections (i.e. Correlation Search). • Incorporate context into detections (i.e. Correlation Search). • Understand and create risk-based modifiers and detections. • Generate effective Notable Events/findings. • Create and maintain a detection lifecycle.
Building Effective Security Processes and Programs (20%)	• Research, incorporate and develop threat intelligence. • Use common methodologies for risk and detection prioritization. • Generate documentation and standard operating procedures.
Automation and Efficiency (20%)	• Develop automation and orchestration for standard operating procedures. • Optimize Case Management. • Describe and utilize REST APIs. • Automate responses using SOAR playbooks. • Compare and validate integrations and automation capabilities of Enterprise Security and SOAR.
Auditing and Reporting on Security Programs (10%)	• Develop and optimize security metrics. • Build and populate effective security reports. • Build and populate dashboards for program analytics.

What's more, part of that Exam-Killer SPLK-5002 dumps now are free: https://drive.google.com/open?id=1g8dfX5AjisqWHcUNQucGe-pDRTtxgj8e

A lot of applicants have studied with Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) practice material and passed the SPLK-5002 exam on the first try with their hard work and consistency. The Exam-Killer assures the customers that they will pass the SPLK-5002 Exam on the first try by studying from SPLK-5002 exam material and if they fail to do it so they can claim their money back (terms and conditions apply). Buy It Now!

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	• 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 4	• 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 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 Reliable Cram Materials <<

SPLK-5002 Exam Materials | Reliable SPLK-5002 Braindumps Ebook

The privacy protection of users is an eternal issue in the internet age. Many illegal websites will sell users' privacy to third parties, resulting in many buyers are reluctant to believe strange websites. But you don't need to worry about it at all when buying our SPLK-5002 learning engine: SPLK-5002. We assure you that we will never sell users' information because it is damaging our own reputation. In addition, when you buy our SPLK-5002 simulating exam, our website will use professional technology to encrypt the privacy of every user to prevent hackers from stealing. We believe that business can last only if we fully consider it for our customers, so we will never do anything that will damage our reputation. Hope you can give our SPLK-5002 exam questions full trust, we will not disappoint you.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q62-Q67):

NEW QUESTION # 62
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=4168
- B. EventCode=4126
- C. EventCode=4624
- D. EventCode=4104

Answer: D

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 # 63
In order to perform a complete data assessment, an engineer's role within Splunk must have which of the following?

- A. Access to Knowledge Objects.
- B. The capability to edit macros.
- C. The capability to create Correlation Searches.
- D. Access to applicable indexes.

Answer: D

Explanation:
To perform a complete data assessment in Splunk, an engineer must have access to applicable indexes. Without index access, the engineer cannot review ingested data, validate mappings, or evaluate coverage for detections and reporting.

NEW QUESTION # 64
What are key elements of a well-constructed notable event?(Choosethree)

- A. Proper categorization
- B. Relevant field extractions
- C. Meaningful descriptions
- D. Minimal use of contextual data

Answer: A,B,C

Explanation:
A notable event in Splunk Enterprise Security (ES) represents a significant security detection that requires investigation.
#Key Elements of a Good Notable Event:#Meaningful Descriptions (Answer A) Helps analysts understand the event at a glance.
Example: Instead of "Possible attack detected," use "Multiple failed admin logins from foreign IP address".
#Proper Categorization (Answer C)
Ensures events are classified correctly (e.g., Brute Force, Insider Threat, Malware Activity).
Example: A malicious file download alert should be categorized as "Malware Infection", not just "General Alert".
#Relevant Field Extractions (Answer D)

Ensures that critical details (IP, user, timestamp) are present for SOC analysis.
Example: If an alert reports failed logins, extracted fields should include username, source IP, and login method.
Why Not the Other Options?
#B. Minimal use of contextual data - More context helps SOC analysts investigate faster.
References & Learning Resources
#Building Effective Notable Events in Splunk ES: https://docs.splunk.com/Documentation/ES#SOC Best Practices for Security Alerts: https://splunkbase.splunk.com#How to Categorize Security Alerts Properly: https://www.splunk.com/en_us/blog/security

NEW QUESTION # 65
Which actions help to monitor and troubleshoot indexing issues?(Choosethree)

- A. Review internal logs such as splunkd.log.
- B. Monitor queues in the Monitoring Console.
- C. Use btool to check configurations.
- D. Enable distributed search in Splunk Web.

Answer: A,B,C

Explanation:
Indexing issues can cause search performance problems, data loss, and delays in security event processing.
#1. Use btool to Check Configurations (A)
Helps validate Splunk configurations related to indexing.
Example:
Checkindexes.confsettings:
splunk btool indexes list --debug
#2. Monitor Queues in the Monitoring Console (B)
Identifies indexing bottlenecks such as blocked queues, dropped events, or indexing lag.
Example:
Navigate to: Settings # Monitoring Console # Indexing Performance.
#3. Review Internal Logs Such as splunkd.log (C)
Thesplunkd.logfile contains indexing errors, disk failures, and queue overflows.
Example:
Use Splunk to search internal logs:
D: Enable distributed search in Splunk Web # Distributed search improves scalability, but does not troubleshoot indexing problems.
#Additional Resources:
Splunk Indexing Performance Guide
Using btool for Debugging

NEW QUESTION # 66
Which of the following identifies elements of the Detection Development Lifecyle (DDLC)?

- A. Research, Design, Deploy, Validate
- B. Research, Develop, Document, Test, Deploy
- C. Design, Develop, Deploy, Monitor, Maintain
- D. Design, Develop, Test, Deploy

Answer: C

Explanation:
The Detection Development Lifecycle (DDLC) includes the stages Design, Develop, Deploy, Monitor, and Maintain. This structured process ensures detections are thoughtfully built, effectively deployed, and continuously refined for accuracy and relevance.

NEW QUESTION # 67
.....

we devote a lot of efforts to compile the SPLK-5002 study materials. Even if you unfortunately fail in the test we won't let you suffer the loss of the money and energy and we will return your money back at the first moment. After you pass the SPLK-5002 test you will enjoy the benefits the certificate brings to you such as you will be promoted by your boss in a short time and your wage will surpass your colleagues.