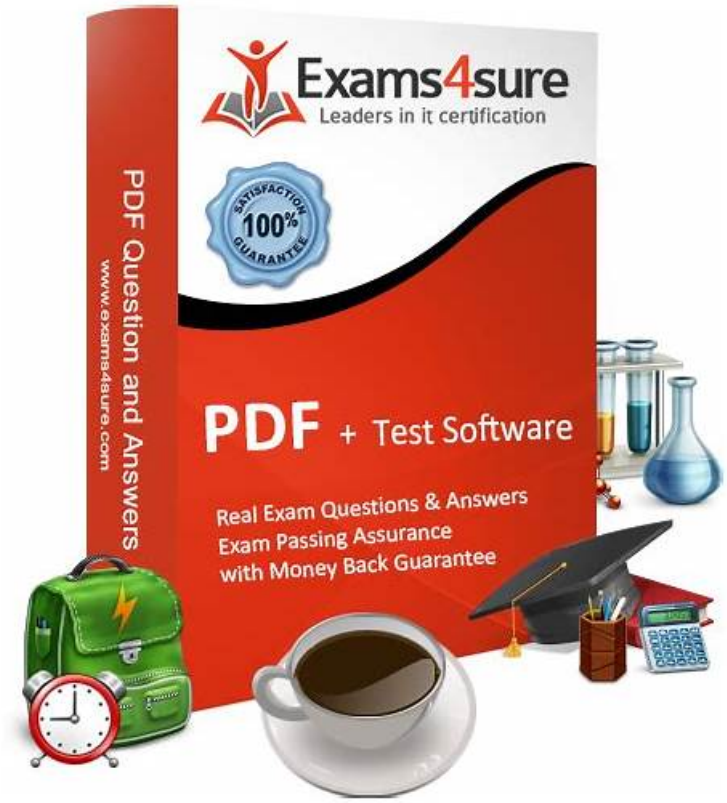
SPLK-5002 Test Answers | SPLK-5002 Latest Braindumps Book



BONUS!!! Download part of FreeDumps SPLK-5002 dumps for free: https://drive.google.com/open?id=1CHd68Un9DtdBfEYKBiZ4ZQBpLn4t6d_U

Our company have the higher class operation system than other companies, so we can assure you that you can start to prepare for the SPLK-5002 exam with our study materials in the shortest time. In addition, if you decide to buy SPLK-5002 exam materials from our company, we can make sure that your benefits will far exceed the costs of you. The rate of return will be very obvious for you. We sincerely reassure all people on the SPLK-5002 Test Question from our company and enjoy the benefits that our study materials bring. We believe that our study materials will have the ability to help all people pass their SPLK-5002 exam and get the related exam in the near future.

The operating system of SPLK-5002 exam practice has won the appreciation of many users around the world. Within five to ten minutes after your payment is successful, our operating system will send a link to SPLK-5002 Training Materials to your email address. After our SPLK-5002 study guide update, our operating system will also send you a timely message to ensure that you will not miss a single message.

>> SPLK-5002 Test Answers <<

100% Pass SPLK-5002 - Splunk Certified Cybersecurity Defense Engineer – High-quality Test Answers

Learning and understanding Splunk SPLK-5002 Exam Questions is not enough to pass the SPLK-5002 exam. Regular tests and self-evaluation are essential. The online SPLK-5002 practice test engine makes it easy for candidates to self-evaluate anytime. The results will boost your confidence and highlight any areas that need more attention. Educationists and experts highly acknowledge this tool created by FreeDumps.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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	• 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 5	• 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.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q89-Q94):

NEW QUESTION # 89
A cybersecurity engineer notices a delay in retrieving indexed data during a security incident investigation.
The Splunk environment has multiple indexers but only one search head.
Which approach can resolve this issue?

- A. Implement accelerated data models for faster querying.
- B. Increase search head memory allocation.
- C. Optimize search queries to use tstats instead of raw searches.
- D. Configure a search head cluster to distribute search queries.

Answer: C

Explanation:
Why Usetstatsfor Faster Searches?
When a cybersecurity engineer experiences delays in retrieving indexed data, the best way to improve search performance is to usetstatsinstead of raw searches.
#What iststats?tstatsis a high-performance command that queries data from indexed fields only, rather than scanning raw events. This makes searches significantly faster and more efficient.
#Why is This the Best Approach?
tstatssearches are 10-100x faster than raw event searches.
It leverages metadata and indexed fields, reducing search load.
It minimizes memory and CPU usage on the search head and indexers.
#Example Use Case:#Scenario: The SOC team is investigating failed logins across multiple indexers.#Using a raw search:
index=security sourcetype=auth_logs action=failed | stats count by user
#Problem: This query scans millions of raw events, causing slow performance.
#Optimized usingtstats:
| tstats count where index=security sourcetype=auth_logs action=failed by user
#Advantage: Faster results without scanning raw events.
Why Not the Other Options?

#A. Increase search head memory allocation - May help, but inefficient queries will still slow down searches.
#C. Configure a search head cluster - A single search head isn't necessarily the problem; improvingsearch performance is more effective.#D. Implement accelerated data models - Useful for prebuilt dashboards, but won't improve ad-hoc searches.

NEW QUESTION # 90
Which Enterprise Security components provide enrichment to the Risk Framework?

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

Answer: D

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 # 91
What are the key components of Splunk's indexing process?(Choosethree)

- A. Indexing
- B. Input phase
- C. Alerting
- D. Parsing
- E. Searching

Answer: A,B,D

Explanation:
Key Components of Splunk's Indexing Process
Splunk's indexing process consists of multiple stages that ingest, process, and store data efficiently for search and analysis.
#1. Input Phase (E)
Collects data from sources (e.g., syslogs, cloud services, network devices).
Defines where the data comes from and applies pre-processing rules.
Example:
A firewall log is ingested from a syslog server into Splunk.
#2. Parsing (A)
Breaks raw data into individual events.
Applies rules for timestamp extraction, line breaking, and event formatting.
Example:
A multiline log file is parsed so that each log entry is a separate event.
#3. Indexing (C)
Stores parsed data in indexes to enable fast searching.
Assigns metadata like host, source, and sourcetype.
Example:
An index=firewall_logs contains all firewall-related events.
#Incorrect Answers:
B: Searching # Searching happens after indexing, not during the indexing process.
D: Alerting # Alerting is part of SIEM and detection, not indexing.
#Additional Resources:
Splunk Indexing Process Documentation
Splunk Data Processing Pipeline

NEW QUESTION # 92
Below is an example of a sysmon process create log. Which EventCode would be associated to this log entry?

- A. EventCode=4
- B. EventCode=3
- C. EventCode=1
- D. EventCode=2

Answer: C

Explanation:
In Sysmon, EventCode=1 corresponds to a Process Create event. The log provided shows details of a new process creation (powershell.exe) including ProcessGuid, ProcessId, CommandLine, ParentProcessId, and ParentImage, which are all fields specific to a Process Create event.

NEW QUESTION # 93
What provides consistency for data mapping applied to data model and saved search exports between Splunk Enterprise Security and Splunk SOAR?

- A. Global field mappings
- B. Global field aliases
- C. Field aliases
- D. Field labels

Answer: A

Explanation:
Global field mappings provide consistency for how data is mapped when exporting from Splunk Enterprise Security to Splunk SOAR. They ensure that fields align correctly across both platforms, allowing seamless integration and accurate automation or reporting.

NEW QUESTION # 94
.....

We have authoritative production team made up by thousands of experts helping you get hang of our SPLK-5002 study question and enjoy the high quality study experience. We will update the content of SPLK-5002 test guide from time to time according to recent changes of examination outline and current policies. Besides, our SPLK-5002 Exam Questions can help you optimize your learning method by simplifying obscure concepts so that you can master better. One more to mention, with our SPLK-5002 test guide, there is no doubt that you can cut down your preparing time in 20-30 hours of practice before you take the exam.

- Latest SPLK-5002 Exam Materials □ SPLK-5002 Exam Study Guide □ Latest Braindumps SPLK-5002 Book □ Open （ www.pdfvce.com ） enter ➠ SPLK-5002 □ and obtain a free download □VCE SPLK-5002 Dumps
- 100% Pass Quiz Splunk - High Hit-Rate SPLK-5002 - Splunk Certified Cybersecurity Defense Engineer Test Answers □ Search for ➥ SPLK-5002 □ and download it for free immediately on ▸ www.testkingpass.com ◂ □SPLK-5002 Valid Test Cost
- www.stes.tyc.edu.tw, www.jygame8.com, www.stes.tyc.edu.tw, jeanytmg914353.gynoblog.com, wildbookmarks.com, andrewnlua163103.blogoxo.com, finnianyqub773255.topbloghub.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, laylaxwly084557.newsbloger.com, Disposable vapes

BTW, DOWNLOAD part of FreeDumps SPLK-5002 dumps from Cloud Storage: https://drive.google.com/open?id=1CHd68Un9DtdBfEYKBiZ4ZQBpLn4t6d_U