New SPLK-5002 Exam Preparation - SPLK-5002 Reliable Test Testking

BONUS!!! Download part of PremiumVCEDump SPLK-5002 dumps for free: https://drive.google.com/open?id=1AJTwXc9cE0NHFIQhyd2cVydaS5bqeZgz

For SPLK-5002 test dumps, we give you free demo for you to try, so that you can have a deeper understanding of what you are going to buy. The pass rate is 98%, and we also pass guarantee and money back guarantee if you fail to pass it. SPLK-5002 test dumps of us contain questions and answers, and it will help you to have an adequate practice. Besides we have free update for one year for you, therefore you can get the latest version in the following year if you buying SPLK-5002 Exam Dumps of us. Buying them, and you will benefit from them in the next year.

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	• 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	• 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.

>> New SPLK-5002 Exam Preparation <<

100% Pass 2026 Splunk The Best SPLK-5002: New Splunk Certified Cybersecurity Defense Engineer Exam Preparation

It is heartening to announce that all PremiumVCEDump users will be allowed to capitalize on a free Splunk SPLK-5002 exam questions demo of all three formats of the Splunk SPLK-5002 practice test. It will make them scrutinize how our formats work and what we offer them, for example, the form and pattern of Splunk SPLK-5002 Exam Dumps, and their relevant and updated answers. It is convenient for our consumers to check PremiumVCEDump Splunk SPLK-5002 exam questions free of charge before purchasing the Splunk Certified Cybersecurity Defense Engineer practice exam.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q52-Q57):

NEW QUESTION # 52
What is a key feature of effective security reports for stakeholders?

- A. Excluding compliance-related metrics
- B. Detailed event logs for every incident
- C. High-level summaries with actionable insights
- D. Exclusively technical details for IT teams

Answer: C

Explanation:
Security reports provide stakeholders (executives, compliance officers, and security teams) with insights into security posture, risks, and recommendations.
Key Features of Effective Security Reports
High-Level Summaries
Stakeholders don't need raw logs but require summary-level insights on threats and trends.
Actionable Insights
Reports should provide clear recommendations on mitigating risks.
Visual Dashboards & Metrics
Charts, KPIs, and trends enhance understanding for non-technical stakeholders.

NEW QUESTION # 53
When setting Common Information Model (CIM) accelerations, which parameter should be defined to set how far back in time (specified as a relative time string) the Splunk platform creates its column stores?

- A. Summary range
- B. Backfill range
- C. Max summarization search time
- D. Accelerate until maximum time

Answer: A

Explanation:
The Summary range parameter in CIM accelerations defines how far back in time (using a relative time string) the Splunk platform creates its column stores. This determines the historical coverage of accelerated data available for searches and dashboards.

NEW QUESTION # 54
Which action improves the effectiveness of notable events in Enterprise Security?

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

Answer: B

Explanation:
Notable events in Splunk Enterprise Security (ES) are triggered by correlation searches, which generate alerts when suspicious activity is detected. However, if too many false positives occur, analysts waste time investigating non-issues, reducing SOC efficiency.
How to Improve Notable Events Effectiveness:
Apply suppression rules to filter out known false positives and reduce alert fatigue.
Refine correlation searches by adjusting thresholds and tuning event detection logic.
Leverage risk-based alerting (RBA) to prioritize high-risk events.
Use adaptive response actions to enrich events dynamically.
By suppressing false positives, SOC analysts focus on real threats, making notable events more actionable. Thus, the correct answer is A. Applying suppression rules for false positives.

NEW QUESTION # 55
During an incident, a correlation search generates several notable events related to failed logins. The engineer notices the events are from test accounts.
Whatshould be done to address this?

- A. Suppress all notable events temporarily.
- B. Apply filtering to exclude test accounts from the search results.
- C. Lower the search threshold for failed logins.
- D. Disable the correlation search for test accounts.

Answer: B

Explanation:
When a correlation search in Splunk Enterprise Security (ES) generates excessive notable events due to test accounts, the best approach is to filter out test accounts while keeping legitimate detections active.
#1. Apply Filtering to Exclude Test Accounts (B)
Modifies the correlation search to exclude known test accounts.
Reduces false positives while keeping real threats visible.
Example:
Update the search to exclude test accounts:
index=auth_logs NOT user IN ("test_user1", "test_user2")
#Incorrect Answers:
A: Disable the correlation search for test accounts # This removes visibility into all failed logins, including those that may indicate real threats.
C: Lower the search threshold for failed logins # Would increase false positives, making it harder for SOC teams to focus on real attacks.
D: Suppress all notable events temporarily # Suppression hides all alerts, potentially missing real security incidents.
#Additional Resources:
Splunk ES: Managing Correlation Searches
Reducing False Positives in SIEM

NEW QUESTION # 56
When developing security metrics, why would a Key Performance Indicator (KPI) that focuses on total perimeter firewall blocks be an ineffective metric?

- A. Perimeter firewalls should be measured on both the number of connections that they permit as well as the number they block.

- B. The metric is too high level, it should be broken down by the type of block. For example, blocks of remote systems that have repeated failed connections to services that do not exist.
- C. Perimeter firewalls are exposed on the internet directly and thus subject to automated scanners and attack tools.
- D. This a Key Result Indicator, not a KPI. It is a metric that is measuring the results of the perimeter firewall's actions, not the performance of the firewall.

Answer: C

Explanation:
A KPI based on total perimeter firewall blocks is ineffective because perimeter firewalls are constantly exposed to the internet and subject to automated scans and attack tools, which can generate very high block counts. This inflates the metric with noise, making it a poor indicator of actual security performance or risk reduction.

NEW QUESTION # 57
.....

The format name of Channel Partner Program SPLK-5002 practice test questions is Splunk PDF Questions file, desktop practice test software, and web-based practice test software. Choose the nay type of Channel Partner Program Splunk Certified Cybersecurity Defense Engineer SPLK-5002 Practice Exam Questions that fit your Splunk SPLK-5002 exam preparation requirement and budget and start preparation without wasting further time.