New SPLK-5002 Braindumps Free, Exam SPLK-5002 Testking

P.S. Free 2026 Splunk SPLK-5002 dumps are available on Google Drive shared by PracticeTorrent: https://drive.google.com/open?id=1Ll4_l34vkrv0cZ2wrMzXHk4RJFHdrqLR

If you are still in colleges, it is a good chance to learn the knowledge of the SPLK-5002 study engine because you have much time. At present, many office workers are keen on learning our SPLK-5002 guide materials even if they are busy with their work. So you should never give up yourself as long as there has chances. In short, what you have learned on our SPLK-5002 study engine will benefit your career development.

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	• 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	• 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	• 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.

>> New SPLK-5002 Braindumps Free <<

Exam SPLK-5002 Testking - Pass SPLK-5002 Rate

If you want to pass your exam and get your certification, we can make sure that our Cybersecurity Defense Analyst guide questions will be your ideal choice. Our company will provide you with professional team, high quality service and reasonable price. In order to help customers solve problems, our company always insist on putting them first and providing valued service. We deeply believe that our SPLK-5002 question torrent will help you pass the exam and get your certification successfully in a short time. Maybe you cannot wait to understand our SPLK-5002 Guide questions; we can promise that our products have a higher quality when compared with other study materials. At the moment I am willing to show our SPLK-5002 guide torrents to you, and I can make a bet that you will be fond of our products if you understand it.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q116-Q121):

NEW QUESTION # 116
What are the main steps of the Splunk data pipeline?(Choosethree)

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

Answer: A,C,D

Explanation:
The Splunk Data Pipeline consists of multiple stages that process incoming data from ingestion to visualization.
Main Steps of the Splunk Data Pipeline:
Input Phase (C)
Splunk collects raw data from logs, applications, network traffic, and endpoints.
Supports various data sources like syslog, APIs, cloud services, and agents (e.g., Universal Forwarders).
Parsing (D)
Splunk breaks incoming data into events and extracts metadata fields.
Removes duplicates, formats timestamps, and applies transformations.
Indexing (A)
Stores parsed events into indexes for efficient searching.
Supports data retention policies, compression, and search optimization.

NEW QUESTION # 117
Which of the following is a methodology to help prevent malicious lateral movement?

- A. Lockheed Martin Cyber Kill Chain
- B. Breakglass
- C. Zero Trust
- D. MITRE ATT&CK

Answer: C

Explanation:
Zero Trust is a security methodology that helps prevent malicious lateral movement by enforcing the principle of "never trust, always verify." It restricts access based on continuous verification, least privilege, and microsegmentation, making it harder for attackers to move laterally within the network.

NEW QUESTION # 118

What is the primary purpose of correlation searches in Splunk?

- A. To identify patterns and relationships between multiple data sources
- B. To store pre-aggregated search results
- C. To create dashboards for real-time monitoring
- D. To extract and index raw data

Answer: A

Explanation:
Correlation searches in Splunk Enterprise Security (ES) are a critical component of Security Operations Center (SOC) workflows, designed to detect threats by analyzing security data from multiple sources.
Primary Purpose of Correlation Searches:
Identify threats and anomalies: They detect patterns and suspicious activity by correlating logs, alerts, and events from different sources.
Automate security monitoring: By continuously running searches on ingested data, correlationsearches help reduce manual efforts for SOC analysts.
Generate notable events: When a correlation search identifies a security risk, it creates a notable event in Splunk ES for investigation.
Trigger security automation: In combination with Splunk SOAR, correlation searches can initiate automated response actions, such as isolating endpoints or blocking malicious IPs.
Since correlation searches analyze relationships and patterns across multiple data sources to detect security threats, the correct answer is B. To identify patterns and relationships between multiple data sources.
References:
Splunk ES Correlation Searches Overview
Best Practices for Correlation Searches
Splunk ES Use Cases and Notable Events

NEW QUESTION # 119
What is the main purpose of incorporating threat intelligence into a security program?

- A. To proactively identify and mitigate potential threats
- B. To automate response workflows
- C. To generate incident reports for stakeholders
- D. To archive historical events for compliance

Answer: A

Explanation:
Why Use Threat Intelligence in Security Programs?
Threat intelligence providesreal-time data on known threats, helping SOC teamsidentify, detect, and mitigate security risks proactively.
#Key Benefits of Threat Intelligence:#Early Threat Detection- Identifiesknown attack patterns(IP addresses, domains, hashes).#Proactive Defense- Blocks threatsbefore they impact systems.#Better Incident Response- Speeds uptriage and forensic analysis.#Contextualized Alerts- Reduces false positives bycorrelating security events with known threats.
#Example Use Case in Splunk ES:#Scenario:The SOC team ingeststhreat intelligence feeds(e.g., from MITRE ATT&CK, VirusTotal).#Splunk Enterprise Security (ES)correlates security eventswith knownmalicious IPs or domains.#If an internal system communicates with aknown C2 server, the SOC teamautomatically receives an alertandblocks the IPusing Splunk SOAR.
Why Not the Other Options?
#A. To automate response workflows- While automation is beneficial,threat intelligence is primarily for proactive identification.#C. To generate incident reports for stakeholders- Reports are abyproduct, but not themain goalof threat intelligence.#D. To archive historical events for compliance- Threat intelligence isreal- time and proactive, whereas compliance focuses onrecord-keeping.
References & Learning Resources
#Splunk ES Threat Intelligence Guide: https://docs.splunk.com/Documentation/ES#MITRE ATT&CK Integration with Splunk: https://attack.mitre.org/resources#Threat Intelligence Best Practices in SOC: https://splunkbase.splunk.com

NEW QUESTION # 120
Which Splunk configuration ensures events are parsed and indexed only once for optimal storage?

- A. Universal forwarder
- B. Index time transformations
- C. Search head clustering
- D. Summary indexing

Answer: B

Explanation:
Why Use Index-Time Transformations for One-Time Parsing & Indexing?
Splunk parses and indexes data once during ingestion to ensure efficient storage and search performance.
Index-time transformations ensure that logs are:
#Parsed, transformed, and stored efficiently before indexing.#Normalized before indexing, so the SOC team doesn't need to clean up fields later.#Processed once, ensuring optimal storage utilization.
#Example of Index-Time Transformation in Splunk:#Scenario: The SOC team needs to mask sensitive data in security logs before storing them in Splunk.#Solution: Use anINDEXED_EXTRACTIONSrule to:
Redact confidential fields (e.g., obfuscate Social Security Numbers in logs).
Rename fields for consistency before indexing.

NEW QUESTION # 121
.....

Nowadays the knowledge capabilities and mental labor are more valuable than the manual labor because knowledge can create more wealth than the mental labor. If you boost professional knowledge capabilities in some area you are bound to create a lot of values and can get a good job with high income. Passing the test of SPLK-5002 Certification can help you achieve that, and our SPLK-5002 training materials are the best study materials for you to prepare for the SPLK-5002 test. Our SPLK-5002 guide materials combine the key information to help the clients both solidify the foundation and advance with the times.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, topnotch.ng, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.taowang.com, Disposable vapes

P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by PracticeTorrent: https://drive.google.com/open?id=1LI4_l34vkrv0cZ2wrMzXHk4RJFHdrqLR