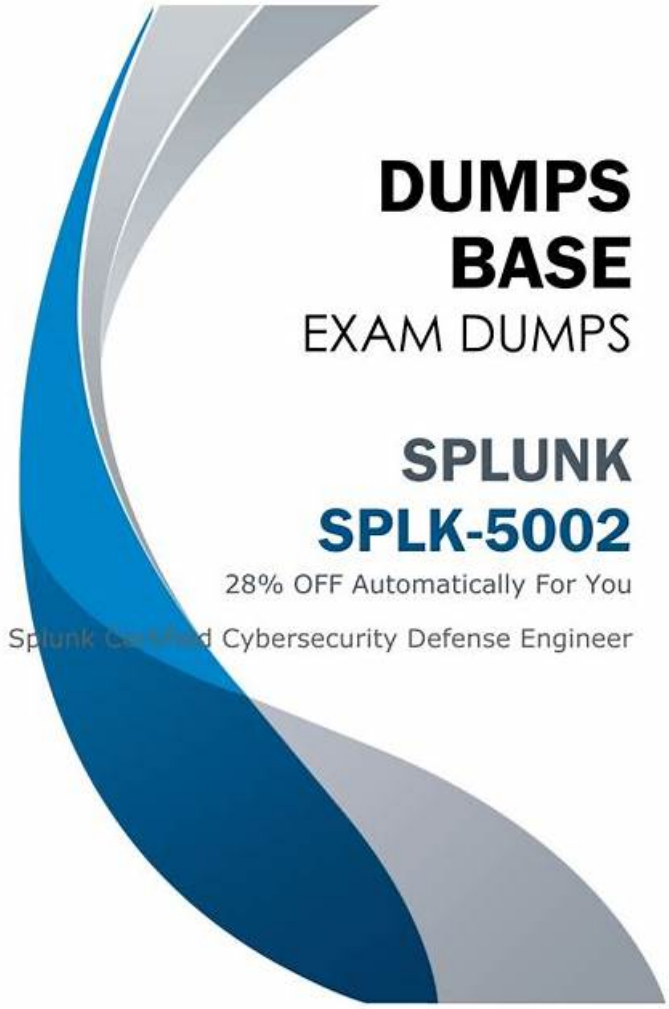
Splunk SPLK-5002 Dumps PDF, Useful SPLK-5002 Dumps



BTW, DOWNLOAD part of FreeCram SPLK-5002 dumps from Cloud Storage: https://drive.google.com/open?id=1iALY5bDouI37ZqnujX0HFpx9Q4x4uKUE

Using an updated Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) exam dumps is necessary to get success on the first attempt. So, it is very important to choose a Splunk SPLK-5002 exam prep material that helps you to practice actual Splunk SPLK-5002 Questions. FreeCram provides you with that product which not only helps you to memorize real Splunk SPLK-5002 questions but also allows you to practice your learning.

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	• 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 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	• 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.

SPLK-5002 Dumps PDF - Realistic Splunk Splunk Certified Cybersecurity Defense Engineer Dumps PDF

Candidates who become Splunk SPLK-5002 certified demonstrate their worth in the Splunk field. The Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) certification is proof of their competence and skills. This is a highly sought-after skill in large Splunk companies and makes a career easier for the candidate. To become certified, you must pass the Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) certification exam. For this task, you need high-quality and accurate Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) exam dumps. We have seen that candidates who study with outdated Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) practice material don't get success and lose their resources.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q42-Q47):

NEW QUESTION # 42
Which features of Splunk are crucial for tuning correlation searches?(Choosethree)

- A. Reviewing notable event outcomes
- B. Optimizing search queries
- C. Enabling event sampling
- D. Disabling field extractions
- E. Using thresholds and conditions

Answer: A,B,E

Explanation:
Correlation searches are a key component of Splunk Enterprise Security (ES) that help detect and alert on security threats by analyzing machine data across various sources. Proper tuning of these searches is essential to reduce false positives, improve performance, and enhance the accuracy of security detections in a Security Operations Center (SOC).
Crucial Features for Tuning Correlation Searches
#1. Using Thresholds and Conditions (A)
Thresholds help control the sensitivity of correlation searches by defining when a condition is met.
Setting appropriate conditions ensures that only relevant events trigger notable events or alerts, reducing noise.
Example:
Instead of alerting on any failed login attempt, a threshold of 5 failed logins within 10 minutes can be set to identify actual brute-force attempts.

#2. Reviewing Notable Event Outcomes (B)
Notable events are generated by correlation searches, and reviewing them is critical for fine-tuning.
Analysts in the SOC should frequently review false positives, duplicates, and low-priority alerts to refine rules.
Example:
If a correlation search is generating excessive alerts for normal user activity, analysts can modify it to exclude known safe behaviors.
#3. Optimizing Search Queries (E)
Efficient Splunk Search Processing Language (SPL) queries are crucial to improving search performance.
Best practices include:
Using index-time fields instead of extracting fields at search time.
Avoiding wildcards and unnecessary joins in searches.
Using tstats instead of regular searches to improve efficiency.
Example:
Using:
| tstats count where index=firewall by src_ip
instead of:
index=firewall | stats count by src_ip
can significantly improve performance.
Incorrect Answers & Explanation
#C. Enabling Event Sampling
Event sampling helps analyze a subset of events to improve testing but does not directly impact correlation search tuning in production.
In a SOC environment, tuning needs to be based on actual real-time event volumes, not just sampled data.
#D. Disabling Field Extractions
Field extractions are essential for correlation searches because they help identify and analyze security-related fields (e.g.,user,src_ip,dest_ip).
Disabling them would limit the visibility of important security event attributes, making detections less effective.
Additional Resources for Learning
#Splunk Documentation & Learning Paths:
Splunk ES Correlation Search Documentation
Best Practices for Writing SPL
Splunk Security Essentials - Use Cases
SOC Analysts Guide for Correlation Search Tuning
#Courses & Certifications:
Splunk Enterprise Security Certified Admin
Splunk Core Certified Power User
Splunk SOAR Certified Automation Specialist

NEW QUESTION # 43
Which Splunk configuration ensures events are parsed and indexed only once for optimal storage?

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

Answer: C

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 # 44
What is the role of aggregation policies in correlation searches?

- A. To automate responses to critical events
- B. To index events from multiple sources
- C. To normalize event fields for dashboards
- D. To group related notable events for analysis

Answer: D

Explanation:
Aggregation policies in Splunk Enterprise Security (ES) are used to group related notable events, reducing alert fatigue and improving incident analysis.
Role of Aggregation Policies in Correlation Searches:
Group Related Notable Events (A)
Helps SOC analysts see a single consolidated event instead of multiple isolated alerts.
Uses common attributes like user, asset, or attack type to aggregate events.
Improves Incident Response Efficiency
Reduces the number of duplicate alerts, helping analysts focus on high-priority threats.

NEW QUESTION # 45
What is a key advantage of using SOAR playbooks in Splunk?

- A. Enhancing data retention policies
- B. Manually running searches across multiple indexes
- C. Improving dashboard visualization capabilities
- D. Automating repetitive security tasks and processes

Answer: D

Explanation:
Splunk SOAR (Security Orchestration, Automation, and Response) playbooks help SOC teams automate, orchestrate, and respond to threats faster.
#Key Benefits of SOAR Playbooks
Automates Repetitive Tasks
Reduces manual workload for SOC analysts.
Automates tasks like enriching alerts, blocking IPs, and generating reports.
Orchestrates Multiple Security Tools
Integrates with firewalls, EDR, SIEMs, threat intelligence feeds.
Example: A playbook can automatically enrich an IP address by querying VirusTotal, Splunk, and SIEM logs.
Accelerates Incident Response
Reduces Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).
Example: A playbook can automatically quarantine compromised endpoints in CrowdStrike after an alert.
#Incorrect Answers:
A: Manually running searches across multiple indexes # SOAR playbooks are about automation, not manual searches.
C: Improving dashboard visualization capabilities # Dashboards are part of SIEM (Splunk ES), not SOAR playbooks.
D: Enhancing data retention policies # Retention is a Splunk Indexing feature, not SOAR-related.
#Additional Resources:
Splunk SOAR Playbook Guide
Automating Threat Response with SOAR

NEW QUESTION # 46
How can Splunk engineers monitor indexing performance effectively?(Choosetwo)

- A. Enable detailed event logging for indexers.
- B. Track indexer queue size and throughput.
- C. Use the Monitoring Console.
- D. Create correlation searches on indexed data.

Answer: B,C

Explanation:
Monitoring indexing performance in Splunk is crucial for ensuring efficient data ingestion, search performance, and resource utilization.
Methods to Monitor Indexing Performance Effectively:
Use the Monitoring Console (A)
Provides real-time visibility into indexing performance.
Displays resource utilization, indexing rate, queue health, and disk usage.
Track Indexer Queue Size and Throughput (D)
Monitoring queue sizes prevents indexing bottlenecks.
Ensures data is processed efficiently without delays.

NEW QUESTION # 47
.....

The Splunk SPLK-5002 Certification is a valuable credential in the modern world. The Splunk SPLK-5002 certification exam offers a great opportunity for beginners and experienced professionals to validate their skills and knowledge level. With the one certification Splunk Certified Cybersecurity Defense Engineer exam you can upgrade your expertise and knowledge.