Splunk SPLK-5002 Latest Braindumps Sheet | Reliable SPLK-5002 Test Pass4sure

What's more, part of that RealValidExam SPLK-5002 dumps now are free: https://drive.google.com/open?id=1ob_2RqLwEFqy_peYiWwvQUk3vCEjTVoB

To ensure that the SPLK-5002 dumps PDF format remains up to date, the Splunk SPLK-5002 questions in it are regularly revised to reflect any modifications to the SPLK-5002 exam content. This commitment to staying current and aligned with the SPLK-5002 Exam Topics ensures that candidates receive the Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) updated questions.

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	• 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 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	• 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 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.

Trustworthy SPLK-5002 Latest Braindumps Sheet & Leader in Qualification Exams & Accurate Reliable SPLK-5002 Test Pass4sure

Now, the test syllabus of the SPLK-5002 exam is changing every year. More and more people choose to prepare the exam to improve their ability. So the SPLK-5002 exam becomes more difficult than before. For our experts, they are capable of seizing the tendency of the real exam. The questions and answers of our SPLK-5002 Guide materials will change every year according to the examination outlines. And we always keep them to be the latest and accurate.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q48-Q53):

NEW QUESTION # 48
What are essential steps in developing threat intelligence for a security program?(Choosethree)

- A. Collecting data from trusted sources
- B. Operationalizing intelligence through workflows
- C. Creating dashboards for executives
- D. Conducting regular penetration tests
- E. Analyzing and correlating threat data

Answer: A,B,E

Explanation:
Threat intelligence in Splunk Enterprise Security (ES) enhances SOC capabilities by identifying known attack patterns, suspicious activity, and malicious indicators.
Essential Steps in Developing Threat Intelligence:
Collecting Data from Trusted Sources (A)
Gather data from threat intelligence feeds (e.g., STIX, TAXII, OpenCTI, VirusTotal, AbuseIPDB).
Include internal logs, honeypots, and third-party security vendors.

Analyzing and Correlating Threat Data (C)
Use correlation searches to match known threat indicators against live data.
Identify patterns in network traffic, logs, and endpoint activity.
Operationalizing Intelligence Through Workflows (E)
Automate responses using Splunk SOAR (Security Orchestration, Automation, and Response).
Enhance alert prioritization by integrating intelligence into risk-based alerting (RBA).

NEW QUESTION # 49
What are the benefits of incorporating asset and identity information into correlation searches?(Choosetwo)

- A. Reducing the volume of raw data indexed
- B. Prioritizing incidents based on asset value
- C. Accelerating data ingestion rates
- D. Enhancing the context of detections

Answer: B,D

Explanation:
Why is Asset and Identity Information Important in Correlation Searches?
Correlation searches in Splunk Enterprise Security (ES) analyze security events to detect anomalies, threats, and suspicious behaviors. Adding asset and identity information significantly improves security detection and response by:
1##Enhancing the Context of Detections - (Answer A)
Helps analysts understand the impact of an event by associating security alerts with specific assets and users.
Example: If a failed login attempt happens on a critical server, it's more serious than one on a guest user account.
2##Prioritizing Incidents Based on Asset Value - (Answer C)
High-value assets (CEO's laptop, production databases) need higher priority investigations.
Example: If malware is detected on a critical finance server, the SOC team prioritizes it over a low-impact system.
Why Not the Other Options?
#B. Reducing the volume of raw data indexed - Asset and identity enrichment adds more metadata;it doesn't reduce indexed data.#D. Accelerating data ingestion rates - Adding asset identity doesn't speed up ingestion; it actually introduces more processing.
References & Learning Resources
#Splunk ES Asset & Identity Framework: https://docs.splunk.com/Documentation/ES/latest/Admin/Assetsandidentitymanagement#Correlation Searches in Splunk ES: https://docs.splunk.com/Documentation/ES/latest/Admin/Correlationsearches

NEW QUESTION # 50
What methods can improve dashboard usability for security program analytics?(Choosethree)

- A. Avoiding performance optimization
- B. Limiting the number of panels on the dashboard
- C. Standardizing color coding for alerts
- D. Using drill-down options for detailed views
- E. Adding context-sensitive filters

Answer: C,D,E

Explanation:
Methods to Improve Dashboard Usability in Security Analytics
A well-designed Splunk security dashboard helps SOC teams quickly identify, analyze, and respond to security threats.
#1. Using Drill-Down Options for Detailed Views (A)
Allows analysts to click on high-level metrics and drill down into event details.
Helps teams pivot from summary statistics to specific security logs.
Example:
Clicking on a failed login trend chart reveals specific failed login attempts per user.
#2. Standardizing Color Coding for Alerts (B)
Consistent color usage enhances readability and priority identification.
Example:
Red # Critical incidents
Yellow # Medium-risk alerts

Green # Resolved issues
#3. Adding Context-Sensitive Filters (D)
Filters allow users to focus on specific security events without running new searches.
Example:
A dropdown filter for "Event Severity" lets analysts view only high-risk events.
#Incorrect Answers:
C: Limiting the number of panels on the dashboard # Dashboards should be optimized, not restricted.
E: Avoiding performance optimization # Performance tuning is essential for responsive dashboards.
#Additional Resources:
Splunk Dashboard Design Best Practices
Optimizing Security Dashboards in Splunk

NEW QUESTION # 51
What is the main purpose of incorporating threat intelligence into a security program?

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

Answer: B

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 # 52
An engineer observes a high volume of false positives generated by a correlation search.
Whatsteps should they take to reduce noise without missing critical detections?

- A. Increase the frequency of the correlation search.
- B. Add suppression rules and refine thresholds.
- C. Limit the search to a single index.
- D. Disable the correlation search temporarily.

Answer: B

Explanation:
How to Reduce False Positives in Correlation Searches?
High false positives can overwhelm SOC teams, causing alert fatigue and missed real threats. The best solution is to fine-tune suppression rules and refine thresholds.
#How Suppression Rules & Threshold Tuning Help:#Suppression Rules: Prevent repeated false positives from low-risk recurring events (e.g., normal system scans).#Threshold Refinement: Adjust sensitivity to focus on true threats (e.g., changing a login failure alert from 3 to 10 failed attempts).

#Example in Splunk ES:#Scenario: A correlation search generates too many alerts for failed logins.#Fix: SOC analysts refine detection thresholds:
Suppress alerts if failed logins occur within a short timeframe but are followed by a successful login.
Only trigger an alert if failed logins exceed 10 attempts within 5 minutes.
Why Not the Other Options?
#A. Increase the frequency of the correlation search - Increases search load without reducing false positives.
#C. Disable the correlation search temporarily - Leads to blind spots in detection.#D. Limit the search to a single index - May exclude critical security logs from detection.
References & Learning Resources
#Splunk ES Correlation Search Optimization Guide: https://docs.splunk.com/Documentation/ES#Reducing False Positives in SOC Workflows: https://splunkbase.splunk.com#Fine-Tuning Security Alerts in Splunk: https://www.splunk.com/en_us/blog/security

NEW QUESTION # 53
......

Splunk is one of the international top companies in the world providing wide products line which is applicable for most families and companies, and even closely related to people's daily life. Passing exam with SPLK-5002 valid exam lab questions will be a key to success; will be new boost and will be important for candidates' career path. Splunk offers all kinds of certifications, SPLK-5002 valid exam lab questions will be a good choice.

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, pct.edu.pk, Disposable vapes

BONUS!!! Download part of RealValidExam SPLK-5002 dumps for free: https://drive.google.com/open?id=1ob_2RqLwEFqy_peYiWwvQUk3vCEjTVoB