Valid SPLK-5002 Exam Cost - Exam SPLK-5002 Consultant

What's more, part of that Free4Dump SPLK-5002 dumps now are free: https://drive.google.com/open?id=1LFvGJqfJN0XcXrIRxPDnaglnmODJ0op_

Many exam candidates feel hampered by the shortage of effective SPLK-5002 practice materials, and the thick books and similar materials causing burden for you. Serving as indispensable choices on your way of achieving success especially during this exam, more than 98 percent of candidates pass the exam with our SPLK-5002 practice materials and all of former candidates made measurable advance and improvement. All SPLK-5002 practice materials fall within the scope of this exam for your information. The content is written promptly and helpfully because we hired the most processional experts in this area to compile the Splunk Certified Cybersecurity Defense Engineer practice materials.

If you are searching for an easy and rewarding study content to get through the SPLK-5002 Exam, you are at the right place to get success. Our SPLK-5002 exam questions can help you pass the exam and achieve the according certification with ease. If you study with our SPLK-5002 Practice Guide for 20 to 30 hours, then you will be bound to pass the exam with confidence. And the price for our SPLK-5002 training engine is quite favourable. What are you waiting for? Just come and buy it!

>> Valid SPLK-5002 Exam Cost <<

Exam Splunk SPLK-5002 Consultant - New Study SPLK-5002 Questions

It is carefully edited and reviewed by our experts. The design of the content conforms to the examination outline. Through the practice of our SPLK-5002 study materials, you can grasp the intention of the examination organization accurately. The number of its test questions is several times of the traditional problem set, which basically covers all the knowledge points to be mastered in the exam. You only need to review according to the content of our SPLK-5002 Study Materials, no need to refer to other materials. With the help of our SPLK-5002 study materials, your preparation process will be relaxed and pleasant.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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	• 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.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q18-Q23):

NEW QUESTION # 18
Which Splunk feature enables integration with third-party tools for automated response actions?

- A. Data model acceleration
- B. Event sampling
- C. Summary indexing
- D. Workflow actions

Answer: D

Explanation:
Security teams use Splunk Enterprise Security (ES) and Splunk SOAR to integrate with firewalls, endpoint security, and SIEM tools for automated threat response.
#Workflow Actions (B) - Key Integration Feature
Allows analysts to trigger automated actions directly from Splunk searches and dashboards.
Can integrate with SOAR playbooks, ticketing systems (e.g., ServiceNow), or firewalls to take action.
Example:
Block an IP on a firewall from a Splunk dashboard.
Trigger a SOAR playbook for automated threat containment.
#Incorrect Answers:
A: Data Model Acceleration # Speeds up searches, but doesn't handle integrations.
C: Summary Indexing # Stores summarized data for reporting, not automation.
D: Event Sampling # Reduces search load, but doesn't trigger automated actions.
#Additional Resources:
Splunk Workflow Actions Documentation
Automating Response with Splunk SOAR

NEW QUESTION # 19
Which components are necessary to develop a SOAR playbook in Splunk?(Choosethree)

- A. Actionable steps or tasks
- B. Manual approval processes
- C. Threat intelligence feeds
- D. Defined workflows

- E. Integration with external tools

Answer: A,D,E

Explanation:
Splunk SOAR (Security Orchestration, Automation, and Response) playbooks automate security processes, reducing response times.
#1. Defined Workflows (A)
A structured flowchart of actions for handling security events.
Ensures that the playbook follows a logical sequence (e.g., detect # enrich # contain # remediate).
Example:
If a phishing email is detected, the workflow includes:
Extract email artifacts (e.g., sender, links).
Check indicators against threat intelligence feeds.
Quarantine the email if it is malicious.
#2. Actionable Steps or Tasks (C)
Each playbook contains specific, automated steps that execute responses.
Examples:
Extracting indicators from logs.
Blocking malicious IPs in firewalls.
Isolating compromised endpoints.
#3. Integration with External Tools (E)
Playbooks must connect with SIEM, EDR, firewalls, threat intelligence platforms, and ticketing systems.
Uses APIs and connectors to integrate with tools like:
Splunk ES
Palo Alto Networks
Microsoft Defender
ServiceNow
#Incorrect Answers:
B: Threat intelligence feeds # These enrich playbooks but are not mandatory components of playbook development.
D: Manual approval processes # Playbooks are designed for automation, not manual approvals.
#Additional Resources:
Splunk SOAR Playbook Documentation
Best Practices for Developing SOAR Playbooks

NEW QUESTION # 20
A company wants to implement risk-based detection for privileged account activities.
Whatshould they configure first?

- A. Asset and identity information for privileged accounts
- B. Event sampling for raw data
- C. Correlation searches with low thresholds
- D. Automated dashboards for all accounts

Answer: A

Explanation:
Why Configure Asset & Identity Information for Privileged Accounts First?
Risk-based detection focuses on identifying and prioritizing threats based on the severity of their impact. For privileged accounts (admins, domain controllers, finance users), understanding who they are, what they access, and how they behave is critical.
#Key Steps for Risk-Based Detection in Splunk ES:1##Define Privileged Accounts & Groups - Identify high- risk users (Admin, HR, Finance, CISO).2##Assign Risk Scores - Apply higher scores to actions involving privileged users.3##Enable Identity & Asset Correlation - Link users to assets for better detection.
4##Monitor for Anomalies - Detect abnormal login patterns, excessive file access, or unusual privilege escalation.
#Example in Splunk ES:
A domain admin logs in from an unusual location # Trigger high-risk alert A finance director downloads sensitive payroll data at midnight # Escalate for investigation Why Not the Other Options?
#B. Correlation searches with low thresholds - May generate excessive false positives, overwhelming the SOC.#C. Event sampling for raw data - Doesn't provide context for risk-based detection.#D. Automated dashboards for all accounts - Useful for visibility, but not the first step for risk-based security.

References & Learning Resources
#Splunk ES Risk-Based Alerting (RBA): https://www.splunk.com/en_us/blog/security/risk-based-alerting.
html#Privileged Account Monitoring in Splunk: https://docs.splunk.com/Documentation/ES/latest/User
/RiskBasedAlerting#Implementing Privileged Access Security (PAM) with Splunk: https://splunkbase.splunk.
com

NEW QUESTION # 21
Which methodology prioritizes risks by evaluating both their likelihood and impact?

- A. Incident lifecycle management
- B. Statistical anomaly detection
- C. Risk-based prioritization
- D. Threat modeling

Answer: C

Explanation:
Understanding Risk-Based Prioritization
Risk-based prioritization is a methodology that evaluatesboth the likelihood and impact of risksto determine which threats require immediate action.
#Why Risk-Based Prioritization?
Focuses onhigh-impact and high-likelihoodrisks first.
HelpsSOC teams manage alerts effectivelyand avoid alert fatigue.
Used inSIEM solutions (Splunk ES) and Risk-Based Alerting (RBA).
Example in Splunk Enterprise Security (ES):
Afailed login attemptfrom aninternal employeemight below risk(low impact, low likelihood).
Multiple failed loginsfrom aforeign countrywith a knownbad reputationcould behigh risk(high impact, high likelihood).
#Incorrect Answers:
A: Threat modeling# Identifies potential threats but doesn'tprioritize risks dynamically.
C: Incident lifecycle management# Focuses on handling security incidents, notrisk evaluation.
D: Statistical anomaly detection# Detects unusual activity but doesn'tprioritize based on impact.
#Additional Resources:
Splunk Risk-Based Alerting (RBA) Guide
NIST Risk Assessment Framework

NEW QUESTION # 22
Which features of Splunk are crucial for tuning correlation searches?(Choosethree)

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

Answer: B,D,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 # 23
.....

The Splunk Certified Cybersecurity Defense Engineer certification exam is a valuable asset for beginners and seasonal professionals. If you want to improve your career prospects then SPLK-5002 certification is a step in the right direction. Whether you're just starting your career or looking to advance your career, the SPLK-5002 Certification Exam is the right choice. With the SPLK-5002 certification you can gain a range of career benefits which include credibility, marketability, validation of skills, and access to new job opportunities.

Easily obtain free download of " SPLK-5002 " by searching on ➥ www.pdfvce.com □ □SPLK-5002 Reliable Exam Blueprint

- Download The Latest Valid SPLK-5002 Exam Cost Right Now □ Search for ➤ SPLK-5002 □ and easily obtain a free download on ➡ www.real4dumps.com □□□ □SPLK-5002 Reliable Exam Blueprint
- Valid SPLK-5002 Exam Cost – Free Download Exam Consultant for SPLK-5002: Splunk Certified Cybersecurity Defense Engineer □ Go to website □ www.pdfvce.com □ open and search for ➤ SPLK-5002 □ to download for free □SPLK-5002 Questions Answers
- Exam Cram SPLK-5002 Pdf □ Study SPLK-5002 Group □ SPLK-5002 Practice Test Pdf □ Search for ▹ SPLK-5002 ◃ and download exam materials for free through 【 www.dumps4pdf.com 】 □Books SPLK-5002 PDF
- Splunk SPLK-5002 Exam | Valid SPLK-5002 Exam Cost - 100% Pass Rate Offer of Exam SPLK-5002 Consultant □ Open ➥ www.pdfvce.com □ and search for ➥ SPLK-5002 □ to download exam materials for free □SPLK-5002 Valid Braindumps Files
- Preparation SPLK-5002 Store ✔ New SPLK-5002 Test Registration □ Reliable SPLK-5002 Exam Braindumps □ Open " www.actual4labs.com " and search for ➤ SPLK-5002 □ to download exam materials for free □SPLK-5002 Practice Exam
- 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, myportal.utt.edu.tt, nogorweb.com, elearning.eauqardho.edu.so, study.stcs.edu.np, mikemil988.shoutmyblog.com, www.stes.tyc.edu.tw, www.multifed.com, profzulu.com, mikemil988.blogrenanda.com, tedcole945.blogginaway.com, Disposable vapes

What's more, part of that Free4Dump SPLK-5002 dumps now are free: https://drive.google.com/open?id=1LFvGJqfJN0XcXrIRxPDnaglnmODJ0op_