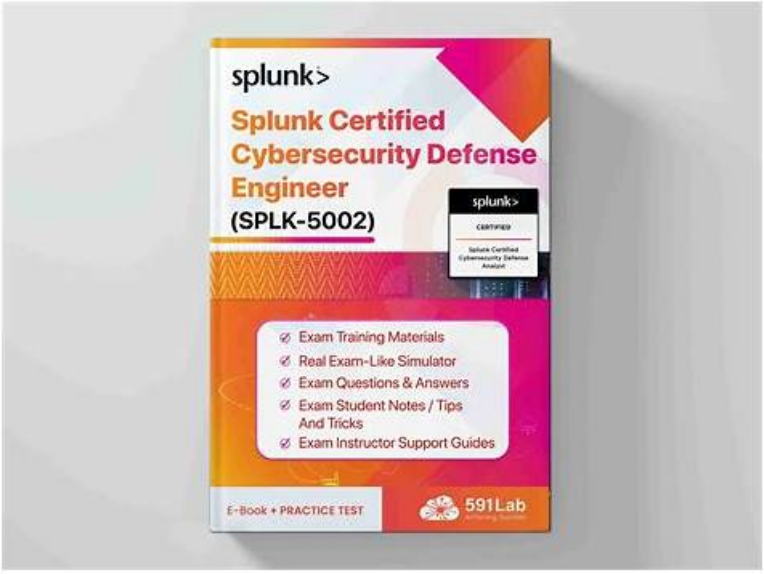
# Want to Know Your Readiness for Splunk SPLK-5002 Exam? Take Our Online Practice Test




P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by Real4Prep: https://drive.google.com/open?id=1r7cZatOF3OQ8vqwt41nFDbM8PB-apb8f

Real4Prep provides updated and valid Splunk SPLK-5002 Exam Questions because we are aware of the absolute importance of updates, keeping in mind the dynamic Splunk SPLK-5002 Exam Syllabus. We provide you update checks for 365 days after purchase for absolutely no cost.

## Splunk SPLK-5002 Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • 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 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 | • 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 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. |

# Valid Exam SPLK-5002 Book - Valid Braindumps SPLK-5002 Pdf

It never needs an internet connection. Splunk Splunk Certified Cybersecurity Defense Engineer practice exam software has several mock exams, designed just like the real exam. Splunk SPLK-5002 Practice Exam software contains all the important questions which have a greater chance of appearing in the final exam. Real4Prep always tries to ensure that you are provided with the most updated Splunk Certified Cybersecurity Defense Engineer Exam Questions to pass the exam on the first attempt.

## Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q77-Q82):

**NEW QUESTION # 77**
What methods enhance risk-based detection in Splunk?(Choosetwo)

- A. Using summary indexing for raw events
- B. Limiting the number of correlation searches
- C. Defining accurate risk modifiers
- D. Enriching risk objects with contextual data

**Answer: C,D**

Explanation:
Risk-based detection in Splunk prioritizes alerts based on behavior, threat intelligence, and business impact.
Enhancing risk scores and enriching contextual data ensures that SOC teams focus on the most critical threats.
Methods to Enhance Risk-Based Detection:
Defining Accurate Risk Modifiers (A)
Adjusts risk scores dynamically based on asset value, user behavior, and historical activity.
Ensures that low-priority noise doesn't overwhelm SOC analysts.
Enriching Risk Objects with Contextual Data (D)
Adds threat intelligence feeds, asset criticality, and user behavior data to alerts.
Improves incident triage and correlation of multiple low-level events into significant threats.

**NEW QUESTION # 78**
Which practices improve the effectiveness of security reporting?(Choosethree)

- A. Including unrelated historical data for context
- B. Customizing reports for different audiences
- C. Providing actionable recommendations
- D. Automating report generation
- E. Using dynamic filters for better analysis

**Answer: B,C,D**

Explanation:
Effective security reporting helps SOC teams, executives, and compliance officers make informed decisions.
#1. Automating Report Generation (A)
Saves time by scheduling reports for regular distribution.
Reduces manual effort and ensures timely insights.
Example:
A weekly phishing attack report sent to SOC analysts.
#2. Customizing Reports for Different Audiences (B)
Technical reports for SOC teams include detailed event logs.
Executive summaries provide risk assessments and trends.
Example:
SOC analysts see incident logs, while executives get a risk summary.
#3. Providing Actionable Recommendations (D)
Reports should not just show data but suggest actions.

Example:
If failed login attempts increase, recommend MFA enforcement.
#Incorrect Answers:
C: Including unrelated historical data for context # Reports should be concise and relevant.
E: Using dynamic filters for better analysis # Useful in dashboards, but not a primary factor in reporting effectiveness.
#Additional Resources:
Splunk Security Reporting Guide
Best Practices for Security Metrics

**NEW QUESTION # 79**
Which features of Splunk are crucial for tuning correlation searches?(Choosethree)

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

**Answer: A,B,C**

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 # 80**
Which of the following is a reason to utilize ES risk framework as a part of detection building?

- A. Help accelerate the run time of detections, allowing a faster mean time to detection.
- B. Simplify SOAR automation and remediation, lowering the mean time to recover.
- C. Create a feedback loop into threat intelligence to identify potential insider threats.
- D. Help prioritize security findings based on their potential business impact.

**Answer: D**

Explanation:
The ES (Enterprise Security) risk framework is designed to assign risk scores to events and entities, allowing security teams to prioritize security findings based on potential business impact.
This ensures that the most critical risks are addressed first, improving overall response effectiveness.

**NEW QUESTION # 81**
Which methodology prioritizes risks by evaluating both their likelihood and impact?

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

**Answer: D**

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 # 82**
.....

The Internet is increasingly becoming a platform for us to work and learn, while many products are unreasonable in web design, and too much information is not properly classified. It's disorganized. Our SPLK-5002 exam materials draw lessons from the experience

of failure, will all kinds of qualification examination has carried on the classification of clear layout, at the same time the user when they entered the SPLK-5002 Study Dumps page in the test module classification of clear, convenient to use a very short time to find what they want to study, which began the next exercise. This saves the user time and makes our SPLK-5002 study dumps clear and clear, which satisfies the needs of more users, which is why our products stand out among many similar products.

**Valid Exam SPLK-5002 Book**: https://www.real4prep.com/SPLK-5002-exam.html

- Latest Updated Splunk SPLK-5002 Reliable Test Sims - SPLK-5002 Valid Exam Splunk Certified Cybersecurity Defense Engineer Book □ Search for 《 SPLK-5002 》 and obtain a free download on □ www.dumpsmaterials.com □ □ □SPLK-5002 Passing Score Feedback
- 100% SPLK-5002 Correct Answers □ SPLK-5002 Book Pdf ✔□ New SPLK-5002 Dumps Ppt □ Search for □ SPLK-5002 □ on 【 www.pdfvce.com 】 immediately to obtain a free download □SPLK-5002 Latest Exam Vce
- Well-Prepared SPLK-5002 Reliable Test Sims - Efficient Valid Exam SPLK-5002 Book Ensure You a High Passing Rate □ Search for （ SPLK-5002 ） and download it for free immediately on ➥ www.examcollectionpass.com □ □Valid SPLK-5002 Exam Cram
- Test Certification SPLK-5002 Cost □ SPLK-5002 Premium Files □ Test Certification SPLK-5002 Cost □ Open website [ www.pdfvce.com ] and search for ▹ SPLK-5002 ◃ for free download □SPLK-5002 Test Free
- Splunk SPLK-5002 exam practice questions and answers □ Go to website ▹ www.prep4sures.top ◃ open and search for " SPLK-5002 " to download for free □SPLK-5002 Passing Score Feedback
- Well-Prepared SPLK-5002 Reliable Test Sims - Efficient Valid Exam SPLK-5002 Book Ensure You a High Passing Rate □ Easily obtain ➠ SPLK-5002 □ for free download through ▸ www.pdfvce.com ◂ □New SPLK-5002 Test Question
- SPLK-5002 Book Pdf □ SPLK-5002 Test Free □ VCE SPLK-5002 Dumps □ Download □ SPLK-5002 □ for free by simply searching on [ www.examcollectionpass.com ] □SPLK-5002 Passing Score Feedback
- Splunk SPLK-5002 exam practice questions and answers ☯ Immediately open ⇛ www.pdfvce.com ⇚ and search for ➥ SPLK-5002 □ to obtain a free download □SPLK-5002 Premium Files
- Latest Updated Splunk SPLK-5002 Reliable Test Sims - SPLK-5002 Valid Exam Splunk Certified Cybersecurity Defense Engineer Book □ Open website 《 www.vceengine.com 》 and search for □ SPLK-5002 □ for free download □New SPLK-5002 Dumps Ppt
- Splunk SPLK-5002 exam practice questions and answers □ Search for ▹ SPLK-5002 ◃ and easily obtain a free download on ⏭ www.pdfvce.com □ □SPLK-5002 Valid Test Labs
- SPLK-5002 Valid Study Notes ☑ SPLK-5002 Premium Files ⤴ SPLK-5002 Test Price □ Search for ➥ SPLK-5002 □ □ and download exam materials for free through （ www.examdiscuss.com ） □SPLK-5002 Test Price
- royalbookmarking.com, blancheqgfw022679.webdesign96.com, junaidlwmq398195.goabroadblog.com, bookmarkinglog.com, www.stes.tyc.edu.tw, myauzou120851.techionblog.com, deborahxwau970765.smblogsites.com, ammaroanq876076.wikiusnews.com, bookmarkinginfo.com, bookmarkproduct.com, Disposable vapes

BONUS!!! Download part of Real4Prep SPLK-5002 dumps for free: https://drive.google.com/open?id=1r7cZatOF3OQ8vqwt41nFDbM8PB-apb8f