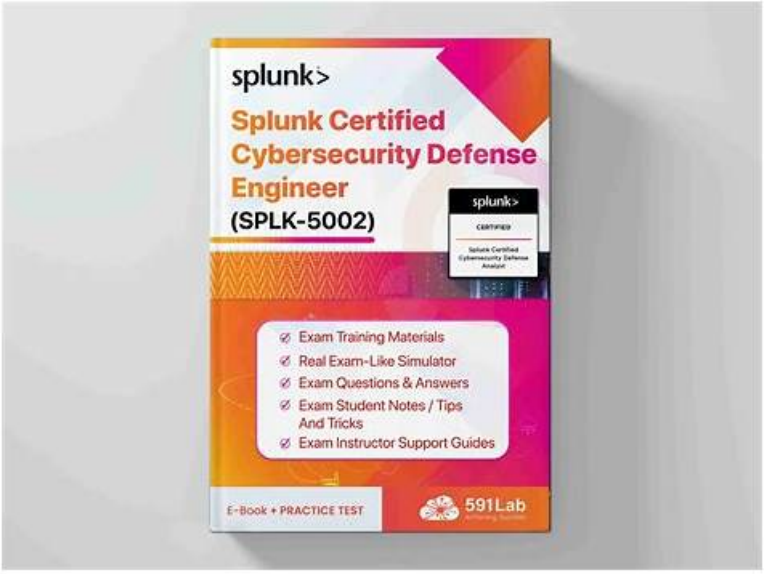
Pass Guaranteed SPLK-5002 - Accurate Splunk Certified Cybersecurity Defense Engineer Latest Study Guide



BONUS!!! Download part of itPass4sure SPLK-5002 dumps for free: https://drive.google.com/open?id=1hjOwFIdrrmcydrND0adMErJRZqLC8alN

The objective of Splunk SPLK-5002 is to assist candidates in preparing for the Splunk SPLK-5002 certification test by equipping them with the actual SPLK-5002 questions PDF and SPLK-5002 practice exams to attempt the SPLK-5002 Exam successfully. The Splunk SPLK-5002 practice material comes in three formats, desktop SPLK-5002 practice test software, web-based SPLK-5002 practice exam, and SPLK-5002 Dumps PDF that cover all exam topics.

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	• 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	• 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	• 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	• 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.

>> SPLK-5002 Latest Study Guide <<

Pass Guaranteed Splunk - SPLK-5002 - Splunk Certified Cybersecurity Defense Engineer Newest Latest Study Guide

The software is designed for use on a Windows computer. This software helps hopefuls improve their performance on subsequent attempts by recording and analyzing Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) exam results. Like the actual Splunk SPLK-5002 Certification Exam, Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) practice exam software has a certain number of questions and allocated time to answer.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q33-Q38):

NEW QUESTION # 33
What are essential steps in developing threat intelligence for a security program?(Choosethree)

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

Answer: A,B,D

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 # 34
Which type of correlation search reviews the events in the risk index and uses an aggregation of events impacting a single risk object to generate risk notables?

- A. Risk Incident Notable
- B. Risk Category
- C. Risk Rule
- D. Risk Incident Rule

Answer: D

Explanation:
A Risk Incident Rule correlation search reviews the events stored in the risk index and aggregates them by risk object (such as a user or asset). When the combined risk score crosses a defined threshold, it generates a risk notable in Enterprise Security.

NEW QUESTION # 35

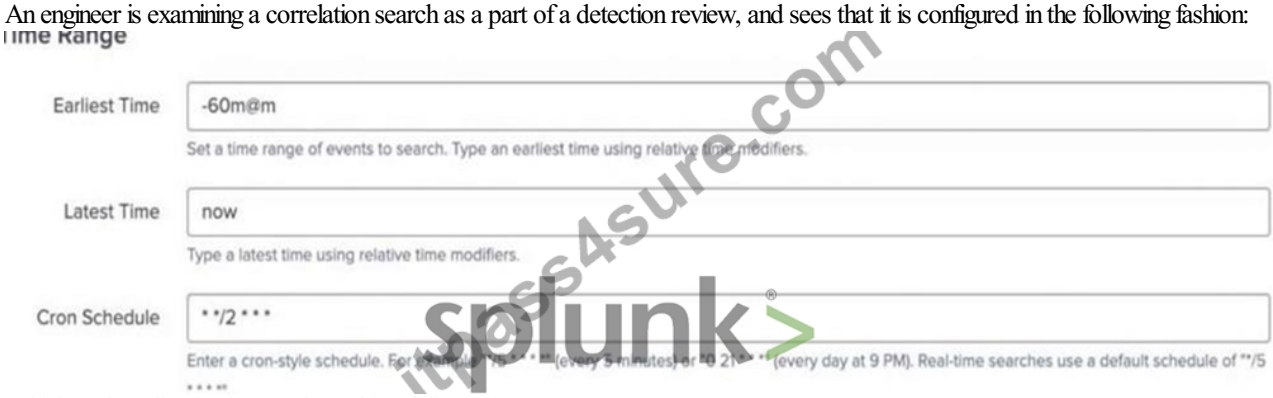
Which of the following macro values will exclude all of the company networks if it is called from the following search?
index=firewall sourcetype=pan:traffic NOT "company_networks"

- A. (src_ip=151.157.30.0/24 AND src_ip=26.06.18.0/24)
- B. (src_ip IN (151.157.30.0/24, 26.06.18.0/24))
- C. NOT (src_ip=151.157.30.0/24 AND src_ip=26.06.18.0/24)
- D. NOT (src_ip IN (151.157.30.0/24, 26.06.18.0/24))

Answer: D

Explanation:
To exclude all company networks from the search, the macro should negate the source IPs using NOT (src_ip IN (...)). This ensures that any traffic originating from the specified company networks is filtered out of the results.

NEW QUESTION # 36
An engineer is examining a correlation search as a part of a detection review, and sees that it is configured in the following fashion:



Which of the following is true about this configuration?

- A. There could be missing findings as the search frequency and time range are improperly configured.
- B. The risk modifiers should be adjusted for an hour of data.
- C. The search will run as prescribed without issue every 30 minutes.
- D. There could be missing data as the search schedule is not ingesting data properly.

Answer: A

Explanation:
The correlation search is scheduled to run every 2 minutes (*/2 * * * *) but is querying a 60-minute window (earliest = -60m@m). This large mismatch between the time range and the execution frequency is considered an improper configuration for ES correlation searches.
Such a configuration can lead to inconsistent detection behavior, including missed or duplicate findings, because the search continually reprocesses a very large window using a very short execution interval.

NEW QUESTION # 37
What document can be helpful in understanding the prioritization of risk when comparing entities in an organization?

- A. Application architecture diagrams
- B. A hierarchical organization chart
- C. Business Continuity or Disaster Recovery plan
- D. Infrastructure architecture diagrams

Answer: C

Explanation:
A Business Continuity or Disaster Recovery (BC/DR) plan identifies critical business processes, systems, and dependencies. It helps in understanding the prioritization of risk across entities in the organization, ensuring that the most business-critical assets are given higher priority in risk- based alerting and response.

NEW QUESTION # 38

.....

It is a virtual certainty that our SPLK-5002 actual exam is high efficient with passing rate up to 98 percent and so on. We made it by persistence, patient and enthusiastic as well as responsibility. Moreover, about some tricky problems of SPLK-5002 Exam Materials you do not to be anxious and choose to take a detour, our experts left notes for your reference. So our SPLK-5002 practice materials are beyond the contrivance of all of you.

SPLK-5002 Exam Topic: https://www.itpass4sure.com/SPLK-5002-practice-exam.html

- SPLK-5002 Learning Materials: Splunk Certified Cybersecurity Defense Engineer - SPLK-5002 Actual Lab Questions □ Open □ www.prep4sures.top □ and search for [SPLK-5002] to download exam materials for free □SPLK-5002 Key Concepts
- SPLK-5002 Test Book □ Valid SPLK-5002 Study Notes □ SPLK-5002 Valid Dumps □ Search for ⇛ SPLK-5002 ⇚ and easily obtain a free download on （ www.pdfvce.com ） □SPLK-5002 Discount
- SPLK-5002 Download Fee □ SPLK-5002 Actual Dump □ SPLK-5002 Discount ✌ Search on { www.testkingpass.com } for ☀ SPLK-5002 □☀□ to obtain exam materials for free download □SPLK-5002 New APP Simulations
- SPLK-5002 Real Exam Questions □ Latest SPLK-5002 Braindumps Files □ Valid SPLK-5002 Study Notes □ Search for ⇛ SPLK-5002 ⇚ and download it for free on ▸ www.pdfvce.com ◂ website □SPLK-5002 Certificate Exam
- Certified SPLK-5002 Questions ➡□ Latest SPLK-5002 Braindumps Files ↗ SPLK-5002 Valid Dumps Sheet □ Go to website □ www.practicevce.com □ open and search for ▹ SPLK-5002 ◃ to download for free □SPLK-5002 New APP Simulations
- SPLK-5002 Learning Materials: Splunk Certified Cybersecurity Defense Engineer - SPLK-5002 Actual Lab Questions □ Copy URL ☀ www.pdfvce.com □☀□ open and search for ✔ SPLK-5002 □✔□ to download for free □SPLK-5002 Discount
- Practice SPLK-5002 Test Engine □ Valid Dumps SPLK-5002 Files □ SPLK-5002 Download Fee □ Search for 【 SPLK-5002 】 and download it for free immediately on ➥ www.pdfdumps.com □ □Latest SPLK-5002 Braindumps Files
- The Key to Success: Proper Planning and the Right Splunk SPLK-5002 Exam Questions □ Search for " SPLK-5002 " and easily obtain a free download on ➡ www.pdfvce.com □□□ □Certified SPLK-5002 Questions
- 2026 SPLK-5002 Latest Study Guide | Useful Splunk Certified Cybersecurity Defense Engineer 100% Free Exam Topic □ Go to website 「 www.testkingpass.com 」 open and search for ▹ SPLK-5002 ◃ to download for free □Mock SPLK-5002 Exam
- SPLK-5002 Certificate Exam □ SPLK-5002 Actual Dump □ SPLK-5002 Real Exam Questions □ Easily obtain □ SPLK-5002 □ for free download through ➠ www.pdfvce.com □ □Latest SPLK-5002 Braindumps Files
- 100% Pass Quiz SPLK-5002 - Splunk Certified Cybersecurity Defense Engineer Latest Latest Study Guide □ Search for 《 SPLK-5002 》 and easily obtain a free download on □ www.practicevce.com □ □SPLK-5002 Certificate Exam
- murrayitxr717866.get-blogging.com, myaiwhi244823.governor-wiki.com, bookmarkinglog.com, programi.healthandmore.rs, followbookmarks.com, hassanyeco674815.activablog.com, thesocialdelight.com, jakubipil047007.ourabilitywiki.com, bookmarkswing.com, eduduct.com, Disposable vapes

P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by itPass4sure: https://drive.google.com/open?id=1hjOwFIdrrmcydrND0adMErJRZqLC8alN