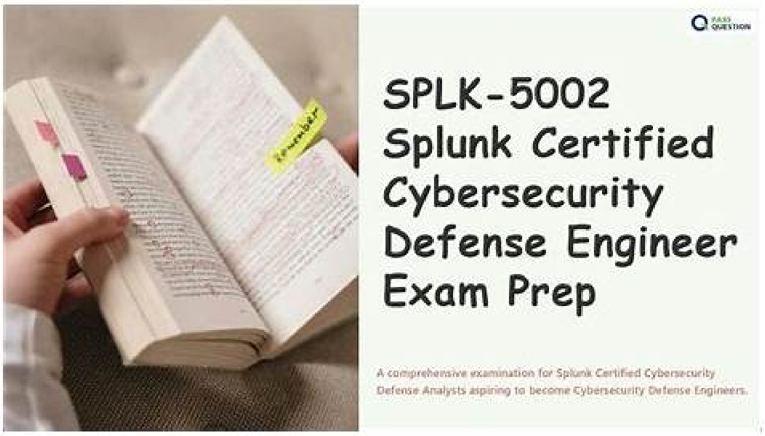
Exam SPLK-5002 Bible - SPLK-5002 Exam Quick Prep


PASS QUESTION
SPLK-5002
Splunk Certified
Cybersecurity
Defense Engineer
Exam Prep
A comprehensive examination for Splunk Certified Cybersecurity Defense Analysts aspiring to become Cybersecurity Defense Engineers.

What's more, part of that PassReview SPLK-5002 dumps now are free: https://drive.google.com/open?id=1qlaBf4nemimlFw7WPo8K2FSwOGGWITgu

It is quite clear that let the facts speak for themselves is more convincing than any word, therefore, we have prepared free demo in this website for our customers to have a taste of the SPLK-5002 test torrent compiled by our company. You will understand the reason why we are so confident to say that the SPLK-5002 exam torrent compiled by our company is the top-notch SPLK-5002 Exam Torrent for you to prepare for the exam. Just like the old saying goes:" Facts are stronger than arguments." You can choose to download our free demo at any time as you like, you are always welcome to have a try, and we trust that our SPLK-5002 exam materials will never let you down.

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	• 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	• 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.

>> Exam SPLK-5002 Bible <<

Pass Guaranteed SPLK-5002 - Useful Exam Splunk Certified Cybersecurity Defense Engineer Bible

We can provide you with efficient online services during the whole day, no matter what kind of problems or consultants about our SPLK-5002 quiz torrent; we will spare no effort to help you overcome them sooner or later. First of all, we have professional staff with dedication to check and update out SPLK-5002 Exam Torrent materials on a daily basis, so that you can get the latest information from our SPLK-5002 exam torrent at any time. Besides our after-sales service engineers will be always online to give remote guidance and assistance for you on SPLK-5002 study questions if necessary.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q45-Q50):

NEW QUESTION # 45
What does the following search do?

- A. Displays a list of processes and their parent processes.
- B. Displays a count of processes created by the same user.
- C. Displays a count of processes created by the same child process.
- D. Displays a list of newly created processes and the user that created them.

Answer: A

Explanation:
The search filters on EventCode=4688 (Windows event for process creation) and then uses stats count, values(process) by parent_process_name. This produces a list of processes (child processes) along with their parent processes, showing how many times each parent process created child processes.

NEW QUESTION # 46
A compliance audit reveals gaps in the tracking of privileged account activities.
Howcan the team address this issue?

- A. Automate report generation for privileged accounts
- B. Use summary indexes to delete old data
- C. Exclude privileged accounts from reporting
- D. Focus only on low-priority account activity

Answer: A

Explanation:
Privileged accounts pose ahigh security risk, and tracking their activity iscritical for compliance(e.g.,PCI DSS, NIST, ISO 27001, SOC 2).
#1. Automate Report Generation for Privileged Accounts (A)
Ensurescontinuous monitoringofadmin/root accounts.
Helpsdetect misuse or unauthorized access.
Example:
Splunk Enterprise Security (ES)can generate scheduled reports on:
Failed login attempts by privileged users.
Actions performed using admin credentials.
#Incorrect Answers:
B: Use summary indexes to delete old data# Summary indexes improve performance butdo not help track privileged accounts.
C: Focus only on low-priority account activity# Privileged accountsshould always be high-priority.
D: Exclude privileged accounts from reporting# This wouldviolate compliance requirements.
#Additional Resources:
Splunk Security Monitoring for Privileged Accounts
NIST Access Control Guide

NEW QUESTION # 47

What framework in Enterprise Security allows engineers to build detections using known malicious IOCs comparing them to event logs to find suspicious behavior?

- A. OSINT Framework
- B. Threat Intelligence Framework
- C. Incident Management Framework
- D. Asset & Intelligence Framework

Answer: B

Explanation:
The Threat Intelligence Framework in Splunk Enterprise Security enables engineers to build detections using known malicious IOCs (such as IPs, domains, or file hashes) and compare them against event logs. This framework automates IOC correlation to identify suspicious behavior.

NEW QUESTION # 48
Which practices improve the effectiveness of security reporting?(Choosethree)

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

Answer: A,B,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 # 49
MITRE D3FEND is designed to compliment MITRE's list of adversarial tactics, techniques, and common knowledge (ATT&CK). Which tactics are associated with MITRE D3FEND in order to detect, deny, and disrupt adversarial efforts?

- A. Harden, Detect, Exclude, Deceive, Eradicate
- B. Harden, Detect, Exclude, Define, Eradicate
- C. Harden, Detect, Isolate, Deceive, Evict
- D. Harden, Detect, Isolate, Disrupt, Evict

Answer: C

Explanation:
MITRE D3FEND provides defensive tactics that complement MITRE ATT&CK. The associated tactics are Harden, Detect, Isolate, Deceive, and Evict, which map to defensive measures organizations can use to counter adversarial behaviors.

NEW QUESTION # 50
......

We offer you free update for one year for SPLK-5002 study guide, namely, in the following year, you can obtain the latest version for free. And the latest version for SPLK-5002 exam dumps will be sent to your email automatically. In addition, SPLK-5002 exam materials are high quality, since we have experienced experts to compile and verify them, therefore the quality and accuracy can be guaranteed, so you can use them at ease. We have online and offline chat service, and if you have any questions about SPLK-5002 Exam Dumps, you can consult us, and we will give you reply as quickly as possible.

SPLK-5002 Exam Quick Prep: https://www.passreview.com/SPLK-5002_exam-braindumps.html

- SPLK-5002 Test Guide - Splunk Certified Cybersecurity Defense Engineer Study Question -amp; SPLK-5002 Exam Questions □ Search for ➥ SPLK-5002 □ and obtain a free download on ► www.prep4away.com ◄ □SPLK-5002 Exam Test
- Practical Exam SPLK-5002 Bible | Amazing Pass Rate For SPLK-5002: Splunk Certified Cybersecurity Defense Engineer | Effective SPLK-5002 Exam Quick Prep □ Open website ➡ www.pdfvce.com □□□ and search for " SPLK-5002 " for free download □SPLK-5002 Study Plan
- Dumps SPLK-5002 Collection □ SPLK-5002 Reliable Test Bootcamp □ Real SPLK-5002 Torrent □ Search for " SPLK-5002 " on ⇛ www.troytecdumps.com ⇚ immediately to obtain a free download □Actual SPLK-5002 Test Answers
- 2026 Realistic SPLK-5002: Exam Splunk Certified Cybersecurity Defense Engineer Bible 100% Pass Quiz □ Easily obtain ➡ SPLK-5002 □□□ for free download through ▷ www.pdfvce.com ◁ □SPLK-5002 Study Plan
- New SPLK-5002 Test Sims □ Free SPLK-5002 Test Questions □ SPLK-5002 Study Plan □ Download ☀ SPLK-5002 □☀□ for free by simply entering ➠ www.examcollectionpass.com □ website □SPLK-5002 Test Quiz
- Valid SPLK-5002 Test Cram □ Valid SPLK-5002 Test Cram □ New SPLK-5002 Cram Materials □ Open □ www.pdfvce.com □ enter ✔ SPLK-5002 □✔□ and obtain a free download □Actual SPLK-5002 Test Answers
- Latest SPLK-5002 Exam Duration □ Latest SPLK-5002 Exam Duration □ Valid Braindumps SPLK-5002 Files □ The page for free download of ✔ SPLK-5002 □✔□ on ➡ www.prep4sures.top □□□ will open immediately □SPLK-5002 Dump File
- New SPLK-5002 Cram Materials □ New SPLK-5002 Cram Materials □ Actual SPLK-5002 Test Answers □ Open ⇛ www.pdfvce.com ⇚ enter { SPLK-5002 } and obtain a free download □SPLK-5002 Study Plan
- Key Features of Splunk SPLK-5002 PDF Questions By www.exam4labs.com □ Search for □ SPLK-5002 □ and obtain a free download on ➤ www.exam4labs.com □ □SPLK-5002 Dump File
- 2026 Valid 100% Free SPLK-5002 – 100% Free Exam Bible | SPLK-5002 Exam Quick Prep □ Open □ www.pdfvce.com □ enter [SPLK-5002] and obtain a free download □New SPLK-5002 Exam Pattern
- Practical Exam SPLK-5002 Bible | Amazing Pass Rate For SPLK-5002: Splunk Certified Cybersecurity Defense Engineer | Effective SPLK-5002 Exam Quick Prep □ ✔ www.practicevce.com □✔□ is best website to obtain □ SPLK-5002 □ for free download □Dumps SPLK-5002 Collection
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, gettr.com, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by PassReview: https://drive.google.com/open?id=1qlaBf4nemimlFw7WPo8K2FSwOGGWITgu