SPLK-5002 Exam Dumps Demo, Exam SPLK-5002 Learning

P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by GetValidTest: https://drive.google.com/open?id=15DpOPloVgDYYLTl7BqSj3tkm6F5ijOkD

You may have been learning and trying to get the SPLK-5002 certification hard, and good result is naturally become our evaluation to one of the important indices for one level. You need to use our SPLK-5002 exam questions to testify the knowledge so that you can get the SPLK-5002 Test Prep to obtain the qualification certificate to show your all aspects of the comprehensive abilities, and the SPLK-5002 exam guide can help you in a very short period of time to prove yourself perfectly and efficiently.

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	• 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	• 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 5	• 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.

>> SPLK-5002 Exam Dumps Demo <<

Pass Guaranteed Quiz 2026 Splunk SPLK-5002 Fantastic Exam Dumps Demo

If you are lack of skills in the preparation of getting the certification, our SPLK-5002 study materials are the best choice for you. Many people have successfully realized economic freedom after getting the SPLK-5002 certificate and changing a high salary job. So you need to act from now, come to join us and struggle together. Our SPLK-5002 Study Materials will help you change into social elite and you will never feel dispointed.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q19-Q24):

NEW QUESTION # 19
An engineer has been asked to build a new dashboard after an increase in login failures across the organization's Microsoft Azure domain. They need to construct a search to only display failed logins for their Azure Active Directory users, and choose a visualization that will help analysts quickly identify failed logins that originate outside of North America. Which of the following search and visualization type combinations will achieve this?

- A. Search: index="main" sourcetype="WinEventLog" | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by loginStatus Visualization: Choropleth Map
- B. Search: index="main" sourcetype="ms:aad: signin" loginStatus=Failure | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by user Visualization: Cluster Map
- C. Search: index="main" sourcetype="ms:aad:signin" | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by user Visualization: Choropleth Map
- D. Search: index="main" sourcetype="WinEventLog" loginStatus=Failure | geostats latfield=geoCoordinates.latitude longfield=geoCoordinates.longitude count by user Visualization: Cluster Map

Answer: B

Explanation:
The correct sourcetype for Azure Active Directory sign-ins is ms:aad:signin, and filtering on loginStatus=Failure ensures only failed logins are shown. Using geostats with latitude and longitude fields allows plotting login attempts geographically, and a Cluster Map visualization is best for quickly identifying failed logins originating outside of North America.

NEW QUESTION # 20
Which Enterprise Security components provide enrichment to the Risk Framework?

- A. Risk Object, Notable Framework, Data Models
- B. Assets & Identities Framework, Risk Factoring, Annotations
- C. Risk Object, Threat Intelligence, Data models
- D. Assets & Identities Framework, Threat Intelligence, Notes

Answer: B

Explanation:
The Risk Framework in Enterprise Security is enriched by the Assets & Identities Framework (providing contextual information about users and systems), Risk Factoring (applying multipliers to adjust risk scoring), and Annotations (such as MITRE ATT&CK mappings). These components work together to provide meaningful, prioritized risk findings.

NEW QUESTION # 21
Which actions enhance the accuracy of Splunk dashboards?(Choosetwo)

- A. Performing regular data validation
- B. Using accelerated data models
- C. Disabling drill-down features
- D. Avoiding token-based filters

Answer: A,B

Explanation:

How to Improve Dashboard Accuracy in Splunk?
#1. Using Accelerated Data Models (Answer A)#Increases search speedand ensuresdashboards load faster.
#Provides pre-processed structured dataforreal-time analysis.#Example:ASOC dashboard tracking failed loginsuses an accelerated authentication data model forfaster rendering.
#2. Performing Regular Data Validation (Answer C)#Ensures that the indexed data is accurate and complete.
#Prevents misleading dashboardscaused by incomplete logs or incorrect field extractions.#Example:If afirewall log source stops sending data, regular validation detects missing logsbefore analysts rely on incorrect dashboards.
Why Not the Other Options?
#B. Avoiding token-based filters- Tokensimprovedashboard flexibility; avoiding themreduces usability.#D. Disabling drill-down features- Drill-downsenhance insightsby allowing analysts to investigate details easily.
References & Learning Resources
#Splunk Dashboard Performance Optimization: https://docs.splunk.com/Documentation/Splunk/latest/Viz/Dashboards#Using Data Models for Fast and Accurate Dashboards: https://splunkbase.splunk.com#Regular Data Validation for SOC Dashboards: https://www.splunk.com/en_us/blog/security

NEW QUESTION # 22
What is a key feature of effective security reports for stakeholders?

- A. High-level summaries with actionable insights
- B. Detailed event logs for every incident
- C. Excluding compliance-related metrics
- D. Exclusively technical details for IT teams

Answer: A

Explanation:
Security reports provide stakeholders (executives, compliance officers, and security teams) with insights into security posture, risks, and recommendations.
#Key Features of Effective Security Reports
High-Level Summaries
Stakeholders don't need raw logs but require summary-level insights on threats and trends.
Actionable Insights
Reports should provide clear recommendations on mitigating risks.
Visual Dashboards & Metrics
Charts, KPIs, and trends enhance understanding for non-technical stakeholders.
#Incorrect Answers:
B: Detailed event logs for every incident # Logs are useful for analysts, not executives.
C: Exclusively technical details for IT teams # Reports should balance technical & business insights.
D: Excluding compliance-related metrics # Compliance is critical in security reporting.
#Additional Resources:
Splunk Security Reporting Best Practices
Creating Executive Security Reports

NEW QUESTION # 23
A SOC's Incident Response Standard Operating Procedure (SOP) calls for any phishing emails containing files to be detonated in Splunk Attack Analyzer for evaluation. Which of the following can an engineer implement to gain efficiency through automation?

- A. Use a SOAR playbook to submit the email to PhishTank, which will automatically handle the Splunk Attack Analyzer submission, and make this information available to an assigned analyst.
- B. Automatically assign findings containing the tag "phishing" to analysts to speed up the start of data collection steps and reduce the time to disposition for the finding.
- C. Use a SOAR playbook to handle the Splunk Attack Analyzer submission and data collection steps, and make this information available to an assigned analyst.
- D. Automatically send all findings containing the tag "phishing" to create an email notification for the SOC.

Answer: C

Explanation:
The most efficient approach is to use a SOAR playbook to automatically handle the Splunk Attack Analyzer submission and data

collection steps, then present the results to the assigned analyst.
This reduces manual effort, accelerates phishing investigation workflows, and aligns directly with the SOC's SOP.

NEW QUESTION # 24
.....

GetValidTest will provide you with a standard, classified, and authentic study material for all the IT candidates. Our experts are trying their best to supply you with the high quality SPLK-5002 training pdf which contains the important knowledge required by the actual test. The high quality and valid SPLK-5002 study torrent will make you more confidence in the real test. Additionally, you will get the updated Splunk vce dumps within one year after payment. With the updated SPLK-5002 study material, you can successfully pass at first try.

Exam SPLK-5002 Learning: https://www.getvalidtest.com/SPLK-5002-exam.html

- Free PDF 2026 Trustable Splunk SPLK-5002: Splunk Certified Cybersecurity Defense Engineer Exam Dumps Demo □ Download ☀ SPLK-5002 □☀□ for free by simply entering ⇛ www.prepawaypdf.com ⇚ website □Valid SPLK-5002 Test Voucher
- Pass SPLK-5002 Exam with the Best Accurate SPLK-5002 Exam Dumps Demo by Pdfvce □ Search on 《 www.pdfvce.com 》 for 【 SPLK-5002 】 to obtain exam materials for free download □SPLK-5002 Reliable Braindumps Book
- Splunk SPLK-5002 Exam | SPLK-5002 Exam Dumps Demo - 100% Pass Rate Offer of Exam SPLK-5002 Learning □ Search for 「 SPLK-5002 」 and download it for free immediately on ➤ www.practicevce.com □ □SPLK-5002 Latest Exam Cost
- Splunk SPLK-5002 Exam Dumps Demo: Splunk Certified Cybersecurity Defense Engineer - Pdfvce Pass Guaranteed □ Search for [SPLK-5002] and download it for free on [www.pdfvce.com] website □Preparation SPLK-5002 Store
- SPLK-5002 Reliable Braindumps Book □ SPLK-5002 Reliable Test Questions □ SPLK-5002 Pdf Torrent □ □ www.prep4away.com □ is best website to obtain ➠ SPLK-5002 □ for free download □SPLK-5002 Test Valid
- Pass Guaranteed Efficient Splunk - SPLK-5002 Exam Dumps Demo □ Download 「 SPLK-5002 」 for free by simply searching on ▸ www.pdfvce.com ◂ □SPLK-5002 Latest Exam Cost
- Pass Guaranteed Efficient Splunk - SPLK-5002 Exam Dumps Demo □ Search for ⇛ SPLK-5002 ⇚ and download it for free on □ www.examdiscuss.com □ website □Valid SPLK-5002 Test Voucher
- Pass SPLK-5002 Exam with the Best Accurate SPLK-5002 Exam Dumps Demo by Pdfvce □ Search for ➥ SPLK-5002 □ on □ www.pdfvce.com □ immediately to obtain a free download □SPLK-5002 Reliable Braindumps Book
- Splunk SPLK-5002 Exam Dumps Demo: Splunk Certified Cybersecurity Defense Engineer - www.troytecdumps.com Ensure you a High Passing Rate □ Easily obtain " SPLK-5002 " for free download through ➠ www.troytecdumps.com □ □ □SPLK-5002 Valid Mock Test
- SPLK-5002 Exam Dumps Demo | Sound for Splunk Certified Cybersecurity Defense Engineer □ Download 「 SPLK-5002 」 for free by simply entering 《 www.pdfvce.com 》 website □Valid SPLK-5002 Test Voucher
- Splunk SPLK-5002 Exam Dumps Demo: Splunk Certified Cybersecurity Defense Engineer - www.pdfdumps.com Ensure you a High Passing Rate □ Enter ➡ www.pdfdumps.com □□□ and search for 【 SPLK-5002 】 to download for free □SPLK-5002 Latest Exam Cost
- www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, bbs.agenew.cn, 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, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that GetValidTest SPLK-5002 dumps now are free: https://drive.google.com/open?id=15DpOPloVgDYYLTl7BqSj3tkm6F5ijOkD