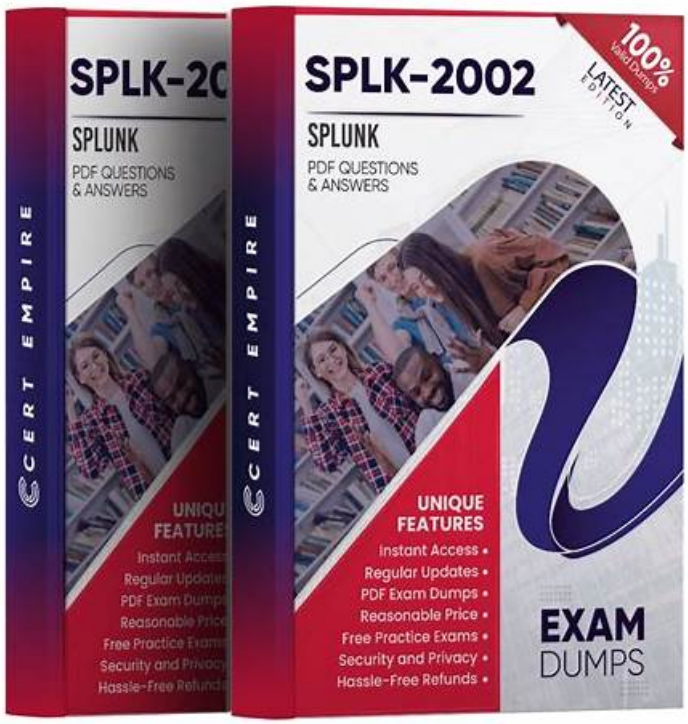
Splunk SPLK-5002 Real Dump, SPLK-5002 Free Learning Cram



P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by PassTestking: https://drive.google.com/open?id=1dIihg3M8LwWrCQz5Xa0RMmTKoxriGJyu

Our company is professional brand. There are a lot of experts and professors in the field in our company. All the experts in our company are devoting all of their time to design the best SPLK-5002 SPLK-5002 study materials for all people. In order to ensure quality of the products, a lot of experts keep themselves working day and night. We believe that our study materials will have the ability to help all people pass their SPLK-5002 Exam and get the related exam in the near future.

Splunk SPLK-5002 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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	• 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 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 guide & SPLK-5002 Real dumps & SPLK-5002 free file

Our company always put the quality of the SPLK-5002 practice materials on top priority. In the past ten years, we have made many efforts to perfect our SPLK-5002 study materials. Our SPLK-5002 study questions cannot tolerate any small mistake. All staff has made great dedication to developing the SPLK-5002 Exam simulation. Our professional experts are devoting themselves on the compiling and updating the exam materials and our services are ready to guide you 24/7 when you have any question.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q93-Q98):

NEW QUESTION # 93
What are benefits of aligning security processes with common methodologies like NIST or MITRE ATT&CK?(Choosetwo)

- A. Enhancing organizational compliance
- B. Ensuring standardized threat responses
- C. Improving incident response metrics
- D. Accelerating data ingestion rates

Answer: A,B

Explanation:
Aligning security processes with frameworks likeNIST Cybersecurity Framework (CSF)orMITRE ATT&CKprovides astructured approach to threat detection and response.
Benefits of Using Common Security Methodologies:
Enhancing Organizational Compliance (A)
Helps organizationsmeet regulatory requirements(e.g., NIST, ISO 27001, GDPR).
Ensuresconsistent security controlsare implemented.
Ensuring Standardized Threat Responses (C)
MITRE ATT&CK providesa common language for adversary techniques.
ImprovesSOC workflows by aligning detection and response strategies.

NEW QUESTION # 94
Which methodology prioritizes risks by evaluating both their likelihood and impact?

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

Answer: B

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 # 95
Engineers are commonly asked to turn data sources like EDR alerts into risk events. Doing so requires a dynamic mapping of the signatures in the rule to MITRE ATT&CK. Which of the following fields could be used to dynamically set the MITRE ATT&CK technique ID for the EDR alerts?

- A. mitre_attack.tactic_id
- B. annotations.mitre_attack.tactic_id
- C. mitre_attack.mitre_technique_id
- D. annotations.mitre_attack.mitre_technique_id

Answer: D

Explanation:
Risk-based alerting expects MITRE ATT&CK mappings to be provided through the annotations namespace. The correct dynamic field for specifying the ATT&CK technique ID is annotations.mitre_attack.mitre_technique_id, which Splunk uses when generating risk events.

NEW QUESTION # 96
What are key elements of a well-constructed notable event?(Choosethree)

- A. Proper categorization
- B. Meaningful descriptions
- C. Relevant field extractions
- D. Minimal use of contextual data

Answer: A,B,C

Explanation:
A notable event in Splunk Enterprise Security (ES) represents a significant security detection that requires investigation.
#Key Elements of a Good Notable Event:#Meaningful Descriptions (Answer A) Helps analysts understand the event at a glance.
Example: Instead of "Possible attack detected," use "Multiple failed admin logins from foreign IP address".
#Proper Categorization (Answer C)
Ensures events are classified correctly (e.g., Brute Force, Insider Threat, Malware Activity).
Example: A malicious file download alert should be categorized as "Malware Infection", not just "General Alert".
#Relevant Field Extractions (Answer D)
Ensures that critical details (IP, user, timestamp) are present for SOC analysis.
Example: If an alert reports failed logins, extracted fields should include username, source IP, and login method.
Why Not the Other Options?
#B. Minimal use of contextual data - More context helps SOC analysts investigate faster.
References & Learning Resources
#Building Effective Notable Events in Splunk ES: https://docs.splunk.com/Documentation/ES#SOC Best Practices for Security Alerts: https://splunkbase.splunk.com#How to Categorize Security Alerts Properly: https://www.splunk.com/en_us/blog/security

NEW QUESTION # 97
A Splunk administrator needs to integrate a third-party vulnerability management tool to automate remediation workflows. What is the most efficient first step?

- A. Set up a manual alerting system for vulnerabilities
- B. Configure custom dashboards to monitor vulnerabilities
- C. Write a correlation search for each vulnerability type
- D. Use REST APIs to integrate the third-party tool with Splunk SOAR

Answer: D

Explanation:
Why Use REST APIs for Integration?
When integrating a third-party vulnerability management tool (e.g., Tenable, Qualys, Rapid7) with Splunk SOAR, using REST APIs is the most efficient and scalable approach.
Why REST APIs?
APIs enable direct communication between Splunk SOAR and the third-party tool.
Allows automated ingestion of vulnerability data into Splunk.
Supports automated remediation workflows (e.g., patch deployment, firewall rule updates).
Reduces manual work by allowing Splunk SOAR to pull real-time data from the vulnerability tool.
Steps to Integrate a Third-Party Vulnerability Tool with Splunk SOAR Using REST API:
1. Obtain API Credentials - Get API keys or authentication tokens from the vulnerability management tool.
2. Configure REST API Integration - Use Splunk SOAR's built-in API connectors or create a custom REST API call.
3. Ingest Vulnerability Data into Splunk - Map API responses to Splunk ES correlation searches.
4. Automate Remediation Playbooks - Build Splunk SOAR playbooks to:
Automatically open tickets for critical vulnerabilities.
Trigger patches or firewall rules for high-risk vulnerabilities.
Notify SOC analysts when a high-risk vulnerability is detected on a critical asset.
Example Use Case in Splunk SOAR:
Scenario: The company uses Tenable.io for vulnerability management.
Splunk SOAR connects to Tenable's API and pulls vulnerability scan results.
If a critical vulnerability is found on a production server, Splunk SOAR:
Automatically creates a ServiceNow ticket for remediation.
Triggers a patching script to fix the vulnerability.
Updates Splunk ES dashboards for tracking.

NEW QUESTION # 98
.....

- SPLK-5002 Actual Exam - SPLK-5002 Exam Guide - SPLK-5002 Practice Exam □ Search for □ SPLK-5002 □ and download it for free on ➡ www.pdfdumps.com □□□ website □Study SPLK-5002 Center
- SPLK-5002 Practice Exams Free □ Study SPLK-5002 Center □ SPLK-5002 Certification Materials □ Download ➡ SPLK-5002 □□□ for free by simply searching on ➡ www.pdfvce.com □□□ □SPLK-5002 Reliable Exam Sims
- Vce SPLK-5002 Exam □ Test SPLK-5002 Questions Pdf □ SPLK-5002 Practice Exams Free □ Download □ SPLK-5002 □ for free by simply entering ⇛ www.testkingpass.com ⇚ website □Examcollection SPLK-5002 Dumps
- Valid SPLK-5002 Test Preparation □ SPLK-5002 Certification Materials □ Exam SPLK-5002 Format □ Download 【 SPLK-5002 】 for free by simply entering 【 www.pdfvce.com 】 website □Valid SPLK-5002 Test Practice
- Tips to Crack Splunk SPLK-5002 Exam Easily □ { www.vce4dumps.com } is best website to obtain ⇛ SPLK-5002 ⇚ for free download □Sample SPLK-5002 Exam
- myportal.utt.edu.tt, www.divephotoguide.com, www.aliyihou.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, wjhsd.instructure.com, 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.1pge.cc, Disposable vapes

What's more, part of that PassTestking SPLK-5002 dumps now are free: https://drive.google.com/open?id=1dIihg3M8LwWrCQz5Xa0RMmTKoxriGJyu