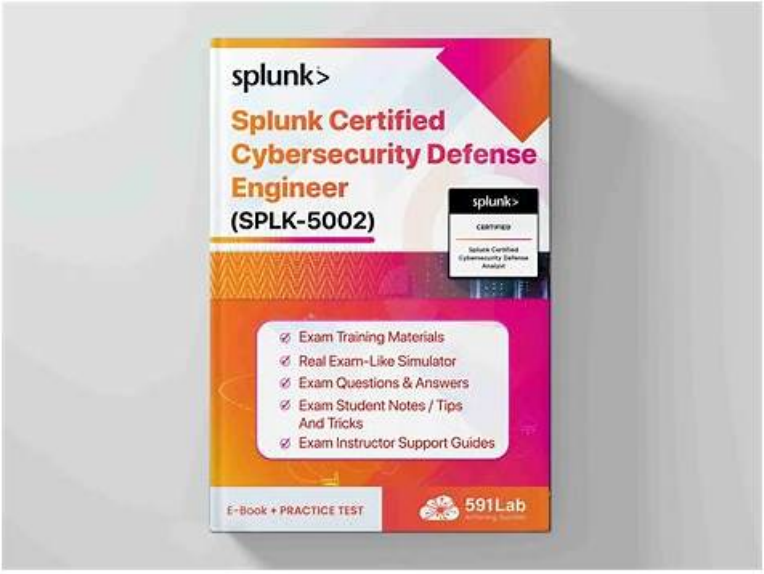
Quiz 2026 Reliable Splunk SPLK-5002: Real Splunk Certified Cybersecurity Defense Engineer Exam Answers



P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by DumpsMaterials: https://drive.google.com/open?id=185NA84smfCRNvu2B3nSumzJGRyr4vyb-

Generally speaking, preparing for the SPLK-5002 exam is a very hard and even some suffering process. Because time is limited, sometimes we have to spare time to do other things to review the exam content, which makes the preparation process full of pressure and anxiety. But from the point of view of customers, our SPLK-5002 Study Materials will not let you suffer from this. As mentioned above, our SPLK-5002 study materials have been carefully written, each topic is the essence of the content. Only should you spend about 20 - 30 hours to study SPLK-5002 study materials carefully can you take the exam.

DumpsMaterials Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) PDF exam questions file is portable and accessible on laptops, tablets, and smartphones. This pdf contains test questions compiled by experts. Answers to these pdf questions are correct and cover each section of the examination. You can even use this format of Splunk Certified Cybersecurity Defense Engineer questions without restrictions of place and time. This Splunk SPLK-5002 Pdf Format is printable to read real questions manually. We update our pdf questions collection regularly to match the updates of the Splunk SPLK-5002 real exam.

>> Real SPLK-5002 Exam Answers <<

Pass Guaranteed Quiz High-quality SPLK-5002 - Real Splunk Certified Cybersecurity Defense Engineer Exam Answers

Our SPLK-5002 exam guide has high quality of service. We provide 24-hour online service on the SPLK-5002 training engine. If you have any questions in the course of using the bank, you can contact us by email. We will provide you with excellent after-sales service with the utmost patience and attitude. And we will give you detailed solutions to any problems that arise during the course of using the SPLK-5002 learning braindumps. And our SPLK-5002 study materials welcome your supervision and criticism.

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	• 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 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	• 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 5	• 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.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q72-Q77):

NEW QUESTION # 72
When creating a new playbook to be called directly from Mission Control or Enterprise Security, which type of playbook must be used?

- A. Input
- B. Automation
- C. Process
- D. Response

Answer: D

Explanation:
A Response playbook must be used when creating a new playbook that can be called directly from Mission Control or Enterprise Security. Response playbooks are designed to run in these contexts to standardize and automate incident response actions.

NEW QUESTION # 73
What document can be helpful in understanding the prioritization of risk when comparing entities in an organization?

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

Answer: D

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 # 74
A Splunk administrator needs to integrate a third-party vulnerability management tool to automate remediation workflows.
Whatis the most efficient first step?

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

Answer: C

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.
Why Not the Other Options?
#A. Set up a manual alerting system for vulnerabilities - Manual alerting is inefficient and doesn't scale well.
#C. Write a correlation search for each vulnerability type - This would create too many rules; API integration allows real-time updates from the vulnerability tool.#D. Configure custom dashboards to monitor vulnerabilities - Dashboards provide visibility but don't automate remediation.
References & Learning Resources
#Splunk SOAR API Integration Guide: https://docs.splunk.com/Documentation/SOAR#Integrating Tenable, Qualys, Rapid7 with Splunk: https://splunkbase.splunk.com#REST API Automation in Splunk SOAR:
https://www.splunk.com/en_us/products/soar.html

NEW QUESTION # 75
The SOC notices over the course of an investigation there are numerous logs like the following:
14-Apr-2024 20:16:49.083 client 15.111.116.918*18345 UDP: query:
reallybad.c2.com IN A response: SERVFAIL +E
What detection should be created to alert on this behavior for the future?

- A. Excessive Network Failures
- B. Excessive DNS Failures
- C. Excessive Authentication Failures
- D. Excessive Endpoint Failures

Answer: B

Explanation:
The log shows repeated DNS query failures (SERVFAIL) to a suspicious domain (reallybad.c2.com). The correct detection to create is Excessive DNS Failures, which alerts on abnormal patterns of failed DNS lookups that may indicate command-and-control or malware activity.

NEW QUESTION # 76

What are key elements of a well-constructed notable event?(Choosethree)

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

Answer: B,C,D

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 # 77
.....

- SPLK-5002 Training Online 囤 Reliable SPLK-5002 Real Exam □ SPLK-5002 Latest Test Braindumps □ Copy URL ⇛ www.pdfvce.com ⇚ open and search for ☀ SPLK-5002 □☀□ to download for free □New SPLK-5002 Dumps Ppt
- SPLK-5002 Latest Practice Materials □ SPLK-5002 New Braindumps Sheet □ SPLK-5002 Study Demo □ Open （ www.examdiscuss.com ） and search for ⇛ SPLK-5002 ⇚ to download exam materials for free □SPLK-5002 Latest Test Braindumps
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, 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, schoolido.lu, 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, 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, Disposable vapes

BTW, DOWNLOAD part of DumpsMaterials SPLK-5002 dumps from Cloud Storage: https://drive.google.com/open?id=185NA84smfCRNvu2B3nSumzJGRyr4vyb-