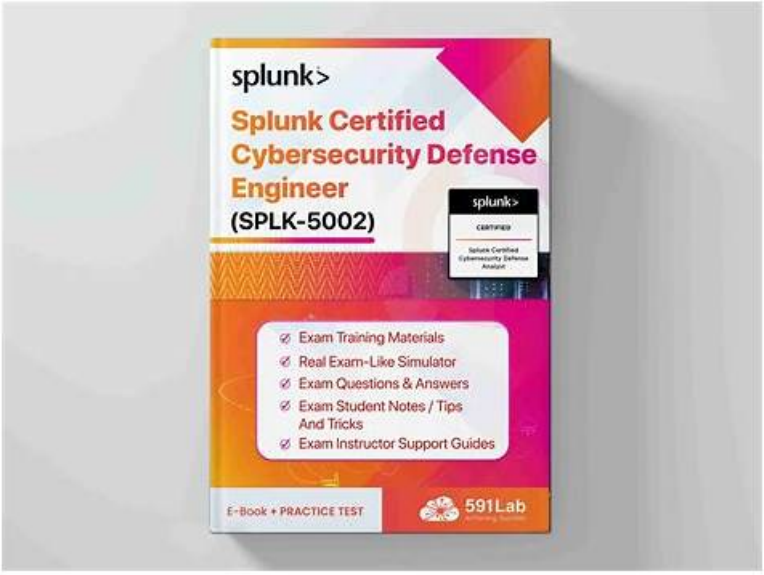
HOT SPLK-5002 Discount - Splunk Splunk Certified Cybersecurity Defense Engineer - Latest SPLK-5002 Valid Study Guide



DOWNLOAD the newest Dumpcollection SPLK-5002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1zVOFAxaaj7nUpB5DqCP5ZyZxcFBGSI_J

If you are one of such frustrated candidates, don't get panic. Dumpcollection declares its services in providing the real SPLK-5002 PDF Questions. It ensures that you would qualify for the Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) certification exam on the maiden strive with brilliant grades. Dumpcollection has formulated the Splunk Certified Cybersecurity Defense Engineer (SPLK-5002) product in three versions. You will find their specifications below to understand them better.

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	• 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	• 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	• 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 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.

SPLK-5002 Discount | Professional SPLK-5002: Splunk Certified Cybersecurity Defense Engineer 100% Pass

Our SPLK-5002 exam materials are flexible and changeable, and the servide provide by our company is quite specific. Our SPLK-5002 test questions have been following the pace of digitalization, constantly refurbishing, and adding new things. I hope you can feel the SPLK-5002 exam prep sincerely serve customers. We also attach great importance to the opinions of our customers. As long as you make reasonable recommendations for our SPLK-5002 test material, we will give you free updates to the system's benefits. We have always advocated customer first. If you use our learning materials to achieve your goals, we will be honored. SPLK-5002 exam prep look forward to meeting you.

Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q43-Q48):

NEW QUESTION # 43
A cyber defense engineer plays a role in maintaining a secure SOAR Cloud configuration. Which network security statement is correct about SOAR Cloud?

- A. Splunk Cloud initiates an outbound SSL connection to both the Automation Broker and managed endpoints.
- B. The Automation Broker initiates an inbound SSL connection to Splunk Cloud, and also initiates an outbound connection to the managed endpoints.
- C. The Automation Broker initiates an outbound SSL connection to Splunk Cloud, and the managed endpoint initiates an outbound connection to the Automation Broker.
- D. The Automation Broker initiates an outbound SSL connection to Splunk Cloud, and also initiates an outbound connection to the managed endpoints.

Answer: D

Explanation:
In Splunk SOAR Cloud, the Automation Broker is responsible for maintaining connectivity. It initiates an outbound SSL connection to Splunk Cloud (so no inbound firewall rules are needed) and also makes outbound connections to the managed endpoints to execute playbook actions securely.

NEW QUESTION # 44
The SOC Manager requested a better method to standardize the list of tasks that analysts follow when they evaluate events or cases. Which Splunk SOAR feature allows the creation of SOPs based on criteria like the type of event or attack vector?

- A. Cases
- B. Incidents
- C. Events
- D. Workbooks

Answer: D

Explanation:
Workbooks in Splunk SOAR allow SOC managers to standardize analyst workflows by defining SOPs (Standard Operating Procedures) as structured task lists. These can be applied automatically based on event type or attack vector, ensuring consistency in investigations.

NEW QUESTION # 45
In Enterprise Security, what is the name of the threat intelligence lookup pertaining to files?

- A. file_hash
- B. user_intel
- C. file_intel
- D. user_hash

Answer: C

Explanation:
In Splunk Enterprise Security, the file_intel lookup is used for threat intelligence related to files, such as file hashes or suspicious file indicators. This lookup allows correlation searches and risk scoring to incorporate known malicious file information.

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

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

Answer: B

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
A company wants to implement risk-based detection for privileged account activities. What should they configure first?

- A. Correlation searches with low thresholds
- B. Automated dashboards for all accounts
- C. Event sampling for raw data
- D. Asset and identity information for privileged accounts

Answer: D

Explanation:
Why Configure Asset & Identity Information for Privileged Accounts First?
Risk-based detection focuses on identifying and prioritizing threats based on the severity of their impact. For privileged accounts (admins, domain controllers, finance users), understanding who they are, what they access, and how they behave is critical.
Key Steps for Risk-Based Detection in Splunk ES:
1. Define Privileged Accounts & Groups - Identify high-risk users (Admin, HR, Finance, CISO).

2. Assign Risk Scores - Apply higher scores to actions involving privileged users.
3. Enable Identity & Asset Correlation - Link users to assets for better detection.
4. Monitor for Anomalies - Detect abnormal login patterns, excessive file access, or unusual privilege escalation.

NEW QUESTION # 48
.....

The Splunk SPLK-5002 certification verifies that you have a basic understanding of Splunk Certified Cybersecurity Defense Engineer concepts and virtualization. Success in the SPLK-5002 exam of the Splunk SPLK-5002 certificate also proves your knowledge of basic troubleshooting concepts and data center technology. When you earn the SPLK-5002 Certification you will get reliable exam guide materials.

P.S. Free 2026 Splunk SPLK-5002 dumps are available on Google Drive shared by Dumpcollection: https://drive.google.com/open?id=1zVOFAxaaj7nUpB5DqCP5ZyZxcFBGSI_J