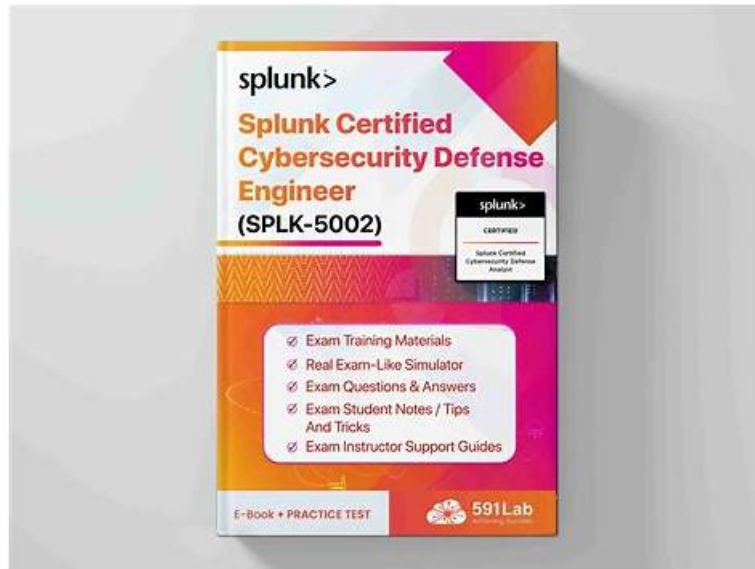


# HOT SPLK-5002 Discount - Splunk Splunk Certified Cybersecurity Defense Engineer - Latest SPLK-5002 Valid Study Guide



DOWNLOAD the newest Dumpcollection SPLK-5002 PDF dumps from Cloud Storage for free: [https://drive.google.com/open?id=1zVOFAxaaaj7nUpB5DqCP5ZyZxcFBGSI\\_J](https://drive.google.com/open?id=1zVOFAxaaaj7nUpB5DqCP5ZyZxcFBGSI_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	<ul style="list-style-type: none"> <li>• <b>Detection Engineering:</b> 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.</li> </ul>
Topic 2	<ul style="list-style-type: none"> <li>• <b>Data Engineering:</b> 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.</li> </ul>
Topic 3	<ul style="list-style-type: none"> <li>• <b>Auditing and Reporting on Security Programs:</b> 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.</li> </ul>
Topic 4	<ul style="list-style-type: none"> <li>• <b>Building Effective Security Processes and Programs:</b> 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.</li> </ul>

Topic 5	<ul style="list-style-type: none"> <li>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.</li> </ul>
---------	---

>> SPLK-5002 Discount <<

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

Our SPLK-5002 exam materials are flexible and changeable, and the service 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. How can 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 a high security risk, and tracking their activity is critical for compliance (e.g., PCI DSS, NIST, ISO 27001, SOC 2).

#1. Automate Report Generation for Privileged Accounts (A)

Ensures continuous monitoring of admin/root accounts.

Helps detect 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 but do not help track privileged accounts.

C: Focus only on low-priority account activity# Privileged accounts should always be high-priority.

D: Exclude privileged accounts from reporting# This would violate 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.

**SPLK-5002 Valid Study Guide:** [https://www.dumpcollection.com/SPLK-5002\\_braindumps.html](https://www.dumpcollection.com/SPLK-5002_braindumps.html)

- Free SPLK-5002 Download  Valid SPLK-5002 Exam Materials  Free SPLK-5002 Download  Search for « SPLK-5002 » and download exam materials for free through  [www.prep4away.com](http://www.prep4away.com)   SPLK-5002 Valid Study Materials
- Valid SPLK-5002 Exam Materials  Test SPLK-5002 Preparation  SPLK-5002 Valid Test Review  Enter ➔ [www.pdfvce.com](http://www.pdfvce.com)  and search for “SPLK-5002” to download for free  Valid SPLK-5002 Exam Materials
- Test SPLK-5002 Guide Online  Valid SPLK-5002 Exam Labs  SPLK-5002 Training Online  Search for ➔ SPLK-5002  and download it for free immediately on [ [www.prepawayexam.com](http://www.prepawayexam.com) ]  SPLK-5002 Exam Cram Questions
- High Pass-Rate SPLK-5002 Discount Help You to Get Acquainted with Real SPLK-5002 Exam Simulation  Search for “SPLK-5002” and easily obtain a free download on ✓ [www.pdfvce.com](http://www.pdfvce.com)  ✓   SPLK-5002 Reliable Test Guide
- 100% Pass Quiz 2026 Professional Splunk SPLK-5002 Discount  Easily obtain [ SPLK-5002 ] for free download through 【 [www.prep4sures.top](http://www.prep4sures.top) 】  Test SPLK-5002 Preparation
- Studying Splunk SPLK-5002 Exam is Easy with Our The Best SPLK-5002 Discount: Splunk Certified Cybersecurity Defense Engineer  Open ( [www.pdfvce.com](http://www.pdfvce.com) ) enter ✓ SPLK-5002  ✓  and obtain a free download  Valid SPLK-5002 Exam Labs
- Free PDF Quiz Useful SPLK-5002 - Splunk Certified Cybersecurity Defense Engineer Discount  Open ⇒ [www.pass4test.com](http://www.pass4test.com) ⇐ and search for ⇒ SPLK-5002 ⇐ to download exam materials for free  SPLK-5002 Reliable Test Cram
- SPLK-5002 Actual Test Answers  SPLK-5002 Exam Cram Questions  SPLK-5002 Valid Study Materials  Download ⇒ SPLK-5002 ⇐ for free by simply searching on [ [www.pdfvce.com](http://www.pdfvce.com) ]  SPLK-5002 Reliable Test Guide
- Web-Based Splunk SPLK-5002 Practice Exam  Search for ➔ SPLK-5002  and download it for free on  [www.validtorrent.com](http://www.validtorrent.com)  website  SPLK-5002 Exam Cram Questions
- Test SPLK-5002 Guide Online  SPLK-5002 Reliable Test Guide  Relevant SPLK-5002 Answers  Easily obtain free download of ➔ SPLK-5002  by searching on ▶ [www.pdfvce.com](http://www.pdfvce.com) ◀  Relevant SPLK-5002 Answers
- 100% Pass Quiz High-quality SPLK-5002 - Splunk Certified Cybersecurity Defense Engineer Discount  Download ✓ SPLK-5002  ✓  for free by simply searching on [ [www.practicevce.com](http://www.practicevce.com) ]  Test SPLK-5002 Preparation
- [cormacpij379216.bloggazza.com](http://cormacpij379216.bloggazza.com), [murraymiry419439.59bloggers.com](http://murraymiry419439.59bloggers.com), [olivebookmarks.com](http://olivebookmarks.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [ihannadiqz782401.blogtov.com](http://ihannadiqz782401.blogtov.com), [hannaixil140385.yomoblog.com](http://hannaixil140385.yomoblog.com), [allbookmarking.com](http://allbookmarking.com), [philipmiec361069.wannawiki.com](http://philipmiec361069.wannawiki.com), [gregoryytr137863.tnpwiki.com](http://gregoryytr137863.tnpwiki.com), [luluhkky372989.activablog.com](http://luluhkky372989.activablog.com), Disposable vapes

P.S. Free 2026 Splunk SPLK-5002 dumps are available on Google Drive shared by Dumpcollection:  
[https://drive.google.com/open?id=1zVOFAxaaj7nUpB5DqCP5ZyZxcFBGSI\\_J](https://drive.google.com/open?id=1zVOFAxaaj7nUpB5DqCP5ZyZxcFBGSI_J)