# Splunk SPLK-5002 Dumps Free, Valid SPLK-5002 Exam Format


P.S. Free & New SPLK-5002 dumps are available on Google Drive shared by ExamCost: https://drive.google.com/open?id=1Vj-DR2AKalzESH2__GUC53RoztzVmITFe

The study materials from our company can help you get your certification easily, we believe that you have been unable to hold yourself back to understand our Splunk Certified Cybersecurity Defense Engineer guide torrent, if you use our study materials, it will be very easy for you to save a lot of time. In order to meet the needs of all customers, Our SPLK-5002 study torrent has a long-distance aid function. If you feel confused about our SPLK-5002 test torrent when you use our products, do not hesitate and send a remote assistance invitation to us for help, we are willing to provide remote assistance for you in the shortest time.

In order to meet the needs of all customers that pass their exam and get related certification, the experts of our company have designed the updating system for all customers. Our SPLK-5002 exam question will be constantly updated every day. The IT experts of our company will be responsible for checking whether our SPLK-5002 exam prep is updated or not. Once our SPLK-5002 test questions are updated, our system will send the message to our customers immediately. If you use our SPLK-5002 Exam Prep, you will have the opportunity to enjoy our updating system. You will get the newest information about your exam in the shortest time. You do not need to worry about that you will miss the important information, more importantly, the updating system is free for you, so hurry to buy our SPLK-5002 exam question, you will find it is a best choice for you.

**>> Splunk SPLK-5002 Dumps Free <<**

## High-quality Splunk SPLK-5002 Dumps Free Technically Researched by Splunk First-Grade Trainers

ExamCost is an experienced website with great reputation which offering Splunk dumps torrent and professional explanations. Our SPLK-5002 test questions are created by our IT elites who pay great attention to the IT exam certification so we can ensure you the authority and reliability of our SPLK-5002 Practice Test.

## 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 | • 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 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 | • 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. |

## Splunk Certified Cybersecurity Defense Engineer Sample Questions (Q42-Q47):

**NEW QUESTION # 42**
What are the benefits of maintaining a detection lifecycle?(Choosetwo)

- A. Ensuring detections remain relevant to evolving threats
- B. Scaling the Splunk deployment effectively
- C. Automating the deployment of new detection logic
- D. Detecting and eliminating outdated searches

**Answer: A,D**

Explanation:
Why Maintain a Detection Lifecycle?
Adetection lifecycleensures that security alerts, correlation searches, and automation playbooks arecontinuously refinedto maintainaccuracy, efficiency, and relevanceagainst modern threats.
#1. Detecting and Eliminating Outdated Searches (Answer A)#Removes unnecessary or redundant correlation searchesthat may slow down performance.#Prevents false positivescaused by outdated detection logic.
#Example:A Splunk ES search for anold malware variantmay no longer be effective # it should be updated to detectnew techniques used by attackers.
#2. Ensuring Detections Remain Relevant to Evolving Threats (Answer C)#Regular updatesensure thatnew MITRE ATT&CK techniquesand threat indicators are included.#Example:If attackers start usingLiving-off- the-Land (LotL) techniques, security teams mustupdate detection rules to identify suspicious PowerShell activity.
Why Not the Other Options?
#B. Scaling the Splunk deployment effectively- Lifecycle management improvesdetection accuracy, notinfrastructure scalability.#D. Automating the deployment of new detection logic- Automation helps, but lifecycle management isabout reviewing and updating detections, not just deployment.
References & Learning Resources
#Detection Management in Splunk ES: https://docs.splunk.com/Documentation/ES#Updating Threat Detections Using MITRE ATT&CK in Splunk: https://attack.mitre.org/resources#Best Practices for SOC Detection Engineering: https://splunkbase.splunk.com

**NEW QUESTION # 43**
What are critical elements of an effective incident report?(Choosethree)

- A. Recommendations for future prevention

- B. Names of all employees involved
- C. Financial implications of the incident
- D. Timeline of events
- E. Steps taken to resolve the issue

**Answer: A,D,E**

Explanation:
Critical Elements of an Effective Incident Report
An incident reportdocuments security breaches, outlines response actions, and provides prevention strategies.
#1. Timeline of Events (A)
Provides achronological sequenceof the incident.
Helps analystsreconstruct attacksand understand attack vectors.
Example:
08:30 AM- Suspicious login detected.
08:45 AM- SOC investigation begins.
09:10 AM- Endpoint isolated.
#2. Steps Taken to Resolve the Issue (C)
Documentscontainment, eradication, and recovery efforts.
Ensures teamsfollow response procedures correctly.
Example:
Blocked malicious IPs, revoked compromised credentials, and restored affected systems.
#3. Recommendations for Future Prevention (E)
Suggestssecurity improvementsto prevent future attacks.
Example:
Enhance SIEM correlation rules, enforce multi-factor authentication, or update firewall rules.
#Incorrect Answers:
B: Financial implications of the incident# Important for executives,not crucial for an incident report.
D: Names of all employees involved# Avoidsexposing individualsand focuses on security processes.
#Additional Resources:
Splunk Incident Response Documentation
NIST Computer Security Incident Handling Guide

**NEW QUESTION # 44**
Which report type is most suitable for monitoring the success of a phishing campaign detection program?

- A. Weekly incident trend reports
- B. Risk score-based summary reports
- C. SLA compliance reports
- D. Real-time notable event dashboards

**Answer: D**

Explanation:
Why Use Real-Time Notable Event Dashboards for Phishing Detection?
Phishing campaigns require real-time monitoring to detect threats as they emerge and respond quickly.
#Why "Real-Time Notable Event Dashboards" is the Best Choice? (Answer B)#Shows live security alerts for phishing detections.#Enables SOC analysts to take immediate action (e.g., blocking malicious domains, disabling compromised accounts).#Uses correlation searches in Splunk Enterprise Security (ES) to detect phishing indicators.
#Example in Splunk:#Scenario: A company runs a phishing awareness campaign.#Real-time dashboards track:
How many employees clicked on phishing links.
How many users reported phishing emails.
Any suspicious activity (e.g., account takeovers).
Why Not the Other Options?
#A. Weekly incident trend reports - Helpful for analysis but not fast enough for phishing detection.#C. Risk score-based summary reports - Risk scores are useful but not designed for real-time phishing detection.#D.
SLA compliance reports - SLA reports measure performance but don't help actively detect phishing attacks.
References & Learning Resources
#Splunk ES Notable Events & Phishing Detection: https://docs.splunk.com/Documentation/ES#Real-Time Security Monitoring with Splunk: https://splunkbase.splunk.com#SOC Dashboards for Phishing Campaigns:

https://www.splunk.com/en_us/blog/tips-and-tricks

**NEW QUESTION # 45**
What is the main purpose of Splunk's Common Information Model (CIM)?

- A. To create accelerated reports
- B. To normalize data for correlation and searches
- C. To extract fields from raw events
- D. To compress data during indexing

**Answer: B**

Explanation:
What is the Splunk Common Information Model (CIM)?
Splunk's Common Information Model (CIM) is a standardized way to normalize and map event data from different sources to a common field format. It helps with:
Consistent searches across diverse log sources
Faster correlation of security events
Better compatibility with prebuilt dashboards, alerts, and reports
Why is Data Normalization Important?
Security teams analyze data from firewalls, IDS/IPS, endpoint logs, authentication logs, and cloud logs.
These sources have different field names (e.g., "src_ip" vs. "source_address").
CIM ensures a standardized format, so correlation searches work seamlessly across different log sources.
How CIM Works in Splunk?
#Maps event fields to a standardized schema#Supports prebuilt Splunk apps like Enterprise Security (ES)
#Helps SOC teams quickly detect security threats
#Example Use Case:
A security analyst wants to detect failed admin logins across multiple authentication systems.
Without CIM, different logs might use:
user_login_failed
auth_failure
login_error
With CIM, all these fields map to the same normalized schema, enabling one unified search query.
Why Not the Other Options?
#A. Extract fields from raw events - CIM does not extract fields; it maps existing fields into a standardized format.#C. Compress data during indexing - CIM is about data normalization, not compression.#D. Create accelerated reports - While CIM supports acceleration, its main function is standardizing log formats.
References & Learning Resources
#Splunk CIM Documentation: https://docs.splunk.com/Documentation/CIM#How Splunk CIM Helps with Security Analytics: https://www.splunk.com/en_us/solutions/common-information-model.html#Splunk Enterprise Security & CIM Integration: https://splunkbase.splunk.com/app/263

**NEW QUESTION # 46**
Which Splunk feature helps to standardize data for better search accuracy and detection logic?

- A. Normalization Rules
- B. Data Models
- C. Field Extraction
- D. Event Correlation

**Answer: B**

Explanation:
Why Use "Data Models" for Standardized Search Accuracy and Detection Logic?
SplunkData Modelsprovide astructured, normalized representationof raw logs, improving:
#Search consistency across different log sources#Detection logic by ensuring standardized field names#Faster and more efficient querieswith data model acceleration
#Example in Splunk Enterprise Security:#Scenario:A SOC team monitors login failures acrossmultiple authentication systems.#Without Data Models:Different logs usesrc_ip, source_ip, or ip_address, making searches complex.#With Data

Models:All fieldsmap to a standard format, enablingconsistent detection logic.
Why Not the Other Options?
#A. Field Extraction- Extracts fields from raw events butdoes not standardize field names across sources.#C. Event Correlation- Detects relationships between logsbut doesn't normalize data for search accuracy.#D. Normalization Rules- A general term; Splunkuses CIM & Data Models for normalization.
References & Learning Resources
#Splunk Data Models Documentation: https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutdatamodels#Using CIM & Data Models for Security Analytics: https://splunkbase.splunk.com/app/263#How Data Models Improve Search Performance: https://www.splunk.com/en_us/blog/tips-and-

**NEW QUESTION # 47**
.....

Using ExamCost's SPLK-5002 test certification training materials to pass SPLK-5002 certification exam is easy. Our SPLK-5002 test certification training materials is made up of senior IT specialist team through their own exploration and continuous practice and research. Our ExamCost's SPLK-5002 test certification training materials can help you in your first attempt to pass SPLK-5002 exam easily.