Splunk SPLK-5002 Practice Questions

Shared by Parrish on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What feature allows you to extract additional fields from events at search time?

Options:

A- Index-time field extraction
B- Event parsing
C- Search-time field extraction
D- Data modeling

Answer:

C

Explanation:

Splunk allows dynamic field extraction to enhance data analysis without modifying raw indexed data.

Search-Time Field Extraction:

Extracts fields on-demand when running searches.

Uses Splunk's Field Extraction Engine (rex, spath, or automatic field discovery).

Minimizes indexing overhead by keeping the raw data unchanged.

Incorrect Answers: A. Index-time field extraction -- Happens during indexing and cannot be changed later. B. Event parsing -- Splunk parses events before indexing, not at search time. D. Data modeling -- Data models enhance searches but do not perform field extraction.

Search-Time vs. Index-Time Extraction

Using rex and spath for Field Extraction

Question 2

Question Type: MultipleChoice

A security analyst wants to validate whether a newly deployed SOAR playbook is performing as expected.

What steps should they take?

Options:

A- Test the playbook using simulated incidents
B- Monitor the playbook's actions in real-time environments
C- Automate all tasks within the playbook immediately
D- Compare the playbook to existing incident response workflows

Answer:

A

Explanation:

A SOAR (Security Orchestration, Automation, and Response) playbook is a set of automated actions designed to respond to security incidents. Before deploying it in a live environment, a security analyst must ensure that it operates correctly, minimizes false positives, and doesn't disrupt business operations.

Key Reasons for Using Simulated Incidents:

Ensures that the playbook executes correctly and follows the expected workflow.

Identifies false positives or incorrect actions before deployment.

Tests integrations with other security tools (SIEM, firewalls, endpoint security).

Provides a controlled testing environment without affecting production.

How to Test a Playbook in Splunk SOAR?

1 Use the 'Test Connectivity' Feature -- Ensures that APIs and integrations work. 2 Simulate an Incident -- Manually trigger an alert similar to a real attack (e.g., phishing email or failed admin login). 3 Review the Execution Path -- Check each step in the playbook debugger to verify correct actions. 4 Analyze Logs & Alerts -- Validate that Splunk ES logs, security alerts, and remediation steps are correct. 5 Fine-tune Based on Results -- Modify the playbook logic to reduce unnecessary alerts or excessive automation.

Why Not the Other Options?

B. Monitor the playbook's actions in real-time environments -- Risky without prior validation. It can cause disruptions if the playbook misfires. C. Automate all tasks immediately -- Not best practice. Gradual deployment ensures better security control and monitoring. D. Compare with

existing workflows -- Good practice, but it does not validate the playbook's real execution.

Reference & Learning Resources

Splunk SOAR Documentation: https://docs.splunk.com/Documentation/SOAR Testing Playbooks in Splunk SOAR: https://www.splunk.com/en_us/products/soar.html SOAR Playbook Debugging Best Practices: https://splunkbase.splunk.com

Question 3

Question Type: MultipleChoice

What is the purpose of leveraging REST APIs in a Splunk automation workflow?

Options:

A- To configure storage retention policies
B- To integrate Splunk with external applications and automate interactions
C- To compress data before indexing
D- To generate predefined reports

Answer:

B

Explanation:

Splunk's REST API allows external applications and security tools to automate workflows, integrate with Splunk, and retrieve/search data programmatically.

Why Use REST APIs in Splunk Automation?

Automates interactions between Splunk and other security tools.

Enables real-time data ingestion, enrichment, and response actions.

Used in Splunk SOAR playbooks for automated threat response.

Example:

A security event detected in Splunk ES triggers a Splunk SOAR playbook via REST API to:

Retrieve threat intelligence from VirusTotal.

Block the malicious IP in Palo Alto firewall.

Create an incident ticket in ServiceNow.

Incorrect Answers:

A . To configure storage retention policies Storage is managed via Splunk indexing, not REST APIs.

C . To compress data before indexing Splunk does not use REST APIs for data compression.

D . To generate predefined reports Reports are generated using Splunk's search and reporting functionality, not APIs.

Additional Resources:

Splunk REST API Documentation

Automating Workflows with Splunk API

Question 4

Question Type: MultipleChoice

Which methodology prioritizes risks by evaluating both their likelihood and impact?

Options:

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

Answer:

B

Explanation:

Understanding Risk-Based Prioritization

Risk-based prioritization is a methodology that evaluates both the likelihood and impact of risks to determine which threats require immediate action.

Why Risk-Based Prioritization?

Focuses on high-impact and high-likelihood risks first.

Helps SOC teams manage alerts effectively and avoid alert fatigue.

Used in SIEM solutions (Splunk ES) and Risk-Based Alerting (RBA).

Example in Splunk Enterprise Security (ES):

A failed login attempt from an internal employee might be low risk (low impact, low likelihood).

Multiple failed logins from a foreign country with a known bad reputation could be high risk (high impact, high likelihood).

Incorrect Answers:

A . Threat modeling Identifies potential threats but doesn't prioritize risks dynamically.

C . Incident lifecycle management Focuses on handling security incidents, not risk evaluation.

D . Statistical anomaly detection Detects unusual activity but doesn't prioritize based on impact.

Additional Resources:

Splunk Risk-Based Alerting (RBA) Guide

NIST Risk Assessment Framework

Question 5

Question Type: MultipleChoice

What is the main purpose of Splunk's Common Information Model (CIM)?

Options:

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

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.

Reference & 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

Question 6

Question Type: MultipleChoice

What are the benefits of maintaining a detection lifecycle? (Select two)

Options:

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

Answer:

A, C

Explanation:

Why Maintain a Detection Lifecycle?

A detection lifecycle ensures that security alerts, correlation searches, and automation playbooks are continuously refined to maintain accuracy, efficiency, and relevance against modern threats.

1. Detecting and Eliminating Outdated Searches (Answer A) Removes unnecessary or redundant correlation searches that may slow down performance. Prevents false positives caused by outdated detection logic. Example: A Splunk ES search for an old malware variant may no longer be effective it should be updated to detect new techniques used by attackers.

2. Ensuring Detections Remain Relevant to Evolving Threats (Answer C) Regular updates ensure that new MITRE ATT&CK techniques and threat indicators are included. Example: If attackers start using Living-off-the-Land (LotL) techniques, security teams must update detection rules to identify suspicious PowerShell activity.

Why Not the Other Options?

B. Scaling the Splunk deployment effectively -- Lifecycle management improves detection accuracy, not infrastructure scalability. D. Automating the deployment of new detection logic --

Automation helps, but lifecycle management is about reviewing and updating detections, not just deployment.

Reference & 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

Question 7

Question Type: MultipleChoice

An organization uses MITRE ATT&CK to enhance its threat detection capabilities.

How should this methodology be incorporated?

Options:

A- Develop custom detection rules based on attack techniques.
B- Use it only for reporting after incidents.
C- Rely solely on vendor-provided threat intelligence.
D- Deploy it as a replacement for current detection systems.

Answer:

A

Explanation:

MITRE ATT&CK is a threat intelligence framework that helps security teams map attack techniques to detection rules.

1. Develop Custom Detection Rules Based on Attack Techniques (A)

Maps Splunk correlation searches to MITRE ATT&CK techniques to detect adversary behaviors.

Example:

To detect T1078 (Valid Accounts):

index=auth_logs action=failed | stats count by user, src_ip

If an account logs in from anomalous locations, trigger an alert.

Incorrect Answers:

B . Use it only for reporting after incidents MITRE ATT&CK should be used proactively for threat detection.

C . Rely solely on vendor-provided threat intelligence Custom rules tailored to an organization's threat landscape are more effective.

D . Deploy it as a replacement for current detection systems MITRE ATT&CK complements existing SIEM/EDR tools, not replaces them.

Additional Resources:

MITRE ATT&CK & Splunk

Using MITRE ATT&CK in SIEMs

Question 8

Question Type: MultipleChoice

A Splunk administrator is tasked with creating a weekly security report for executives.

What elements should they focus on?

Options:

A- High-level summaries and actionable insights
B- Detailed logs of every notable event
C- Excluding compliance metrics to simplify reports
D- Avoiding visuals to focus on raw data

Answer:

A

Explanation:

Why Focus on High-Level Summaries & Actionable Insights?

Executive security reports should provide concise, strategic insights that help leadership teams make informed decisions.

Key Elements for an Executive-Level Report: Summarized Security Incidents -- Focus on major

threats and trends. Actionable Recommendations -- Include mitigation steps for ongoing risks. Visual Dashboards -- Use charts and graphs for easy interpretation. Compliance & Risk Metrics -- Highlight compliance status (e.g., PCI-DSS, NIST).

Example in Splunk: Scenario: A CISO requests a weekly security report. Best Report Format:

Threat Summary: 'Detected 15 phishing attacks this week.'

Key Risks: 'Increase in brute-force login attempts.'

Recommended Actions: 'Enhance MFA enforcement & user awareness training.'

Why Not the Other Options?

B. Detailed logs of every notable event -- Too technical; executives need summaries, not raw logs. C. Excluding compliance metrics to simplify reports -- Compliance is critical for risk assessment. D. Avoiding visuals to focus on raw data -- Visuals improve clarity; raw data is too complex for executives.

Reference & Learning Resources

Splunk Security Reporting Best Practices: https://www.splunk.com/en_us/blog/security Creating Effective Executive Dashboards in Splunk: https://splunkbase.splunk.com Cybersecurity Metrics & Reporting for Leadership Teams: https://www.nist.gov/cyberframework