ExamsIndex
Practice Materials & Tests

DEMO VERSION

Splunk

SPLK-5002 Exam

Certified Cybersecurity Defense Engineer

Exam Latest Version: 7.0

Question 1. (Multi Select)

Which features of Splunk are crucial for tuning correlation searches? (Choose three)

A: Using thresholds and conditions
B: Reviewing notable event outcomes
C: Enabling event sampling
D: Disabling field extractions
E: Optimizing search queries

Correct Answer: A, B, E

Explanation:

Correlation searches are a key component of Splunk Enterprise Security (ES) that help detect and alert on security threats by analyzing machine data across various sources. Proper tuning of these searches is essential to reduce false positives, improve performance, and enhance the accuracy of security detections in a Security Operations Center (SOC).

Crucial Features for Tuning Correlation Searches

' 1. Using Thresholds and Conditions (A)

Thresholds help control the sensitivity of correlation searches by defining when a condition is met.

Setting appropriate conditions ensures that only relevant events trigger notable events or alerts, reducing noise.

Example:

Instead of alerting on any failed login attempt, a threshold of 5 failed logins within 10 minutes can be set to identify actual brute-force attempts.

' 2. Reviewing Notable Event Outcomes (B)

Notable events are generated by correlation searches, and reviewing them is critical for fine-tuning.

Analysts in the SOC should frequently review false positives, duplicates, and low-priority alerts

to refine rules.

Example:

If a correlation search is generating excessive alerts for normal user activity, analysts can modify it to exclude known safe behaviors.

' 3. Optimizing Search Queries (E)

Efficient Splunk Search Processing Language (SPL) queries are crucial to improving search performance.

Best practices include:

Using index-time fields instead of extracting fields at search time.

Avoiding wildcards and unnecessary joins in searches.

Using tstats instead of regular searches to improve efficiency.

Example:

Using:

| tstats count where index=firewall by src_ip

instead of:

index=firewall | stats count by src_ip

can significantly improve performance.

Incorrect Answers & Explanation

'L C. Enabling Event Sampling

Event sampling helps analyze a subset of events to improve testing but does not directly impact correlation search tuning in production.

In a SOC environment, tuning needs to be based on actual real-time event volumes, not just sampled data.

'L D. Disabling Field Extractions

Field extractions are essential for correlation searches because they help identify and analyze security-related fields (e.g., user, src_ip, dest_ip).

Disabling them would limit the visibility of important security event attributes, making detections less effective.

Additional Resources for Learning

Ø=ÜÌ Splunk Documentation & Learning Paths:

Splunk ES Correlation Search Documentation

Best Practices for Writing SPL

Splunk Security Essentials - Use Cases

SOC Analysts Guide for Correlation Search Tuning

Ø=ÜÌ Courses & Certifications:

Splunk Enterprise Security Certified Admin

Splunk Core Certified Power User

Splunk SOAR Certified Automation Specialist

Question 2. (Single Select)

What should a security engineer prioritize when building a new security process?

A: Integrating it with legacy systems
B: Ensuring it aligns with compliance requirements
C: Automating all workflows within the process
D: Reducing the overall number of employees required

Correct Answer: B

Explanation:

When a Security Engineer is building a new security process, their top priority should be ensuring that the process aligns with compliance requirements. This is crucial because compliance dictates the legal, regulatory, and industry standards that organizations must follow to protect sensitive data and maintain trust.

Why Compliance is the Top Priority?

Legal and Regulatory Obligations – Many industries are required to follow compliance standards such as GDPR, HIPAA, PCI-DSS, NIST, ISO 27001, and SOX. Non-compliance can lead to heavy fines and legal actions.

Data Protection & Privacy – Compliance ensures that sensitive information is handled securely, preventing data breaches and unauthorized access.

Risk Reduction – Following compliance standards helps mitigate cybersecurity risks by implementing security best practices such as encryption, access controls, and logging.

Business Reputation & Trust – Organizations that comply with standards build customer confidence and industry credibility.

Audit Readiness – Security teams must ensure that logs, incidents, and processes align with compliance frameworks to pass internal/external audits easily.

How Does Splunk Enterprise Security (ES) Help with Compliance?

Splunk ES is a Security Information and Event Management (SIEM) tool that helps organizations meet compliance requirements by:

' Log Management & Retention – Stores and correlates security l investigation.' Real-time Monitoring & Alerts – Detects suspiciou teams.' Prebuilt Compliance Dashboards – Comes with out-of-the PCI-DSS, GDPR, HIPAA, NIST 800-53, and other frameworks.' Au Generates reports that can be used for compliance audits.

Example in Splunk ES:A security engineer can create correlation searches and risk-based alerting (RBA) to monitor and enforce compliance policies.

How Does Splunk SOAR Help Automate Compliance-Driven Security Processes?

Splunk SOAR (Security Orchestration, Automation, and Response) enhances compliance processes by:

' Automating Incident Response – Ensures that responses to sec
compliance guidelines.' Automated Evidence Collection – Helps i
automatically collecting logs, alerts, and incident data.' Playboo
Can automatically detect and remediate non-compliant actions (e.g., blocking unauthorized access).

Example in Splunk SOAR:A playbook can be configured to automatically respond to an unencrypted database storing customer data by triggering a compliance violation alert and notifying the compliance team.

Why Not the Other Options?

'L A. Integrating with legacy systems – While important, compliar
engineers should modernize legacy systems if they pose security
workflows – Automation is beneficial, but it should not be prioritized over security and
compliance. Some security decisions require human oversight.'L
employees – Efficiency is important, but security cannot be sacrificed to cut costs. Skilled SOC analysts and engineers are critical to cybersecurity defense.

Reference & Learning Resources

Ø=ÜÌ Splunk Docs – Security Essentials: https://docs.splunk.com/Ø
Dashboards: https://splunkbase.splunk.com/app/3435/Ø=ÜÌ Splunk
Compliance: https://www.splunk.com/en_us/products/soar.html Ø=Ü
Framework & Splunk Integration: https://www.nist.gov/cyberframework

---

Question 3. (Single Select)

What is the primary purpose of data indexing in Splunk?

A: To ensure data normalization
B: To store raw data and enable fast search capabilities
C: To secure data from unauthorized access
D: To visualize data using dashboards

Correct Answer: B

Explanation:

Understanding Data Indexing in Splunk

In Splunk Enterprise Security (ES) and Splunk SOAR, data indexing is a fundamental process that enables efficient storage, retrieval, and searching of data.

' Why is Data Indexing Important?

Stores raw machine data (logs, events, metrics) in a structured manner.

Enables fast searching through optimized data storage techniques.

Uses an indexer to process, compress, and store data efficiently.

Why the Correct Answer is B?

Splunk indexes data to store it efficiently while ensuring fast retrieval for searches, correlation searches, and analytics.

It assigns metadata to indexed events, allowing SOC analysts to quickly filter and search logs.

'L Incorrect Answers & Explanations

A. To ensure data normalization!' Splunk normalizes data using (CIM), not indexing.

C. To secure data from unauthorized access!' Splunk uses RBAC and encryption for security, not indexing.

D. To visualize data using dashboards!' Dashboards use indexe indexing itself is focused on data storage and retrieval.

Ø=ÜÌ Additional Resources:

Splunk Data Indexing Documentation

Splunk Architecture & Indexing Guide

Question 4. (Multi Select)

Which features are crucial for validating integrations in Splunk SOAR? (Choose three)

A: Testing API connectivity
B: Monitoring data ingestion rates
C: Verifying authentication methods
D: Evaluating automated action performance
E: Increasing indexer capacity

Correct Answer: A, C, D

Explanation:

Validating Integrations in Splunk SOAR

Splunk SOAR (Security Orchestration, Automation, and Response) integrates with various security tools to automate security workflows. Proper validation of integrations ensures that playbooks, threat intelligence feeds, and incident response actions function as expected.

' Key Features for Validating Integrations

1þ ã Testing API Connectivity (A)

Ensures Splunk SOAR can communicate with external security tools (firewalls, EDR, SIEM, etc.).

Uses API testing tools like Postman or Splunk SOAR's built-in Test Connectivity feature.

2þ ã Verifying Authentication Methods (C)

Confirms that integrations use the correct authentication type (OAuth, API Key, Username/Password, etc.).

Prevents failed automations due to expired or incorrect credentials.

3þ ã Evaluating Automated Action Performance (D)

Monitors how well automated security actions (e.g., blocking IPs, isolating endpoints) perform.

Helps optimize playbook execution time and response accuracy.

'L Incorrect Answers & Explanations

B . Monitoring data ingestion rates !’ Data ingestion is crucial fo
core integration validation step for SOAR.

E . Increasing indexer capacity !’ This is related to Splunk Enter
SOAR integration validation.

Ø=ÜÌ Additional Resources:

Splunk SOAR Administration Guide

Splunk SOAR Playbook Validation

Splunk SOAR API Integrations

Question 5. (Single Select)

How can you incorporate additional context into notable events generated by correlation searches?

A: By adding enriched fields during search execution
B: By using the dedup command in SPL
C: By configuring additional indexers
D: By optimizing the search head memory

Correct Answer: A

Explanation:

In Splunk Enterprise Security (ES), notable events are generated by correlation searches, which are predefined searches designed to detect security incidents by analyzing logs and alerts from multiple data sources. Adding additional context to these notable events enhances their value for analysts and improves the efficiency of incident response.

To incorporate additional context, you can:

Use lookup tables to enrich data with information such as asset details, threat intelligence, and user identity.

Leverage KV Store or external enrichment sources like CMDB (Configuration Management Database) and identity management solutions.

Apply Splunk macros or eval commands to transform and enhance event data dynamically.

Use Adaptive Response Actions in Splunk ES to pull additional information into a notable event.

The correct answer is A. By adding enriched fields during search execution, because enrichment occurs dynamically during search execution, ensuring that additional fields (such as geolocation, asset owner, and risk score) are included in the notable event.

Splunk ES Documentation on Notable Event Enrichment

Correlation Search Best Practices

Using Lookups for Data Enrichment

ExamsIndex

Demo PDF Complete

Your SPLK-5002 Demo (5 Questions)

Get the Complete Version

Full Questions with Detailed Explanations

Interactive Web-Based Exams Available

To get 30% off, use Coupon Code: NEWYEAR30

https://examsindex.com/exam/splk-5002