Splunk

SPLK-5002 Exam

Splunk Certified Cybersecurity Defense Engineer

Questions & Answers
Demo

Version: 5.0

Question: 1

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

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 logs for auditability and forensic investigation.
✅ Real-time Monitoring & Alerts – Detects suspicious activity and alerts SOC teams.

✅ Prebuilt Compliance Dashboards – Comes with out-of-the-box dashboards for PCI-DSS, GDPR, HIPAA, NIST 800-53, and other frameworks.
✅ Automated Reporting – 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 security threats follow predefined compliance guidelines.
✅ Automated Evidence Collection – Helps in audit documentation by automatically collecting logs, alerts, and incident data.
✅ Playbooks for Compliance Violations – 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?
❌ A. Integrating with legacy systems – While important, compliance is a higher priority. Security engineers should modernize legacy systems if they pose security risks.
❌ C. Automating all workflows – Automation is beneficial, but it should not be prioritized over security and compliance. Some security decisions require human oversight.
❌ D. Reducing the number of 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
Splunk Docs – Security Essentials: https://docs.splunk.com/
Splunk ES Compliance Dashboards: https://splunkbase.splunk.com/app/3435/
Splunk SOAR Playbooks for Compliance: https://www.splunk.com/en_us/products/soar.html
NIST Cybersecurity Framework & Splunk Integration: https://www.nist.gov/cyberframework

Question: 2

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

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

❌ 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.

❌ 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

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
Courses & Certifications:
Splunk Enterprise Security Certified Admin
Splunk Core Certified Power User
Splunk SOAR Certified Automation Specialist

Question: 3

A security analyst wants to validate whether a newly deployed SOAR playbook is performing as expected.
What steps should they take?

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: 4

What are the benefits of incorporating asset and identity information into correlation searches? (Choose two)

A. Enhancing the context of detections
B. Reducing the volume of raw data indexed
C. Prioritizing incidents based on asset value
D. Accelerating data ingestion rates

Answer: A, C

Explanation:

Why is Asset and Identity Information Important in Correlation Searches?
Correlation searches in Splunk Enterprise Security (ES) analyze security events to detect anomalies, threats, and suspicious behaviors. Adding asset and identity information significantly improves security detection and response by:
1 ☐ Enhancing the Context of Detections – (Answer A)
Helps analysts understand the impact of an event by associating security alerts with specific assets and users.
Example: If a failed login attempt happens on a critical server, it's more serious than one on a guest user account.
2 ☐ Prioritizing Incidents Based on Asset Value – (Answer C)
High-value assets (CEO's laptop, production databases) need higher priority investigations.
Example: If malware is detected on a critical finance server, the SOC team prioritizes it over a low-impact system.
Why Not the Other Options?
✕ B. Reducing the volume of raw data indexed – Asset and identity enrichment adds more metadata; it doesn't reduce indexed data.
✕ D. Accelerating data ingestion rates – Adding asset identity doesn't speed up ingestion; it actually introduces more processing.

Reference & Learning Resources
Splunk ES Asset & Identity Framework:
https://docs.splunk.com/Documentation/ES/latest/Admin/Assetsandidentitymanagement
Correlation Searches in Splunk ES:
https://docs.splunk.com/Documentation/ES/latest/Admin/Correlationsearches

Question: 5

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

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

Answer: A

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.
Example in Splunk ES:
A domain admin logs in from an unusual location → Trigger high-risk alert
A finance director downloads sensitive payroll data at midnight → Escalate for investigation
Why Not the Other Options?
✕ B. Correlation searches with low thresholds – May generate excessive false positives, overwhelming the SOC.
✕ C. Event sampling for raw data – Doesn't provide context for risk-based detection.
✕ D. Automated dashboards for all accounts – Useful for visibility, but not the first step for risk-based security.

Reference & Learning Resources
Splunk ES Risk-Based Alerting (RBA): https://www.splunk.com/en_us/blog/security/risk-based-alerting.html
Privileged Account Monitoring in Splunk: https://docs.splunk.com/Documentation/ES/latest/User/RiskBasedAlerting
Implementing Privileged Access Security (PAM) with Splunk: https://splunkbase.splunk.com