ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

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:

Q Log Management & Retention – Stores and correlates security logs for auditability and forensic investigation.

Q Real-time Monitoring & Alerts – Detects suspicious activity and alerts SOC teams.

Q Prebuilt Compliance Dashboards – Comes with out-of-the-box dashboards for PCI-DSS, GDPR, HIPAA, NIST 800-53, and other frameworks.

Q 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:

Q Automating Incident Response – Ensures that responses to security threats follow predefined compliance guidelines.

Q Automated Evidence Collection – Helps in audit documentation by automatically collecting logs, alerts, and incident data.

Q 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?

X A. Integrating with legacy systems – While important, compliance is a higher priority. Security engineers should modernize legacy systems if they pose security risks.

X C. Automating all workflows – Automation is beneficial, but it should not be prioritized over security and compliance. Some security decisions require human oversight.

X 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

Q 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.

Q 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.

Q 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

X 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.

X 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 3se the "Test Connectivity" Feature - Ensures that APIs and integrations work.
2 Qimulate an Incident - Manually trigger an alert similar to a real attack (e.g., phishing email or failed admin login).
3 Qeview the Execution Path - Check each step in the playbook debugger to verify correct actions.
4 3nalyze Logs & Alerts - Validate that Splunk ES logs, security alerts, and remediation steps are correct.
5 Qine-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 Qnhancing 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 Qrioritizing 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?
8. 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 QDefine Privileged Accounts & Groups - Identify high-risk users (Admin, HR, Finance, CISO).

2 CZAssign Risk Scores — Apply higher scores to actions involving privileged users.

3 Qnable 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 riskbased 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

Question: 6

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

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.

Q 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.

X Incorrect Answers & Explanations

A . To ensure data normalization → Splunk normalizes data using Common Information Model (CIM), not indexing.

C . To secure data from unauthorized access → Splunk uses RBAC (Role-Based Access Control) and encryption for security, not indexing.

D . To visualize data using dashboards → Dashboards use indexed data for visualization, but indexing itself is focused on data storage and retrieval.

Additional Resources:

Splunk Data Indexing Documentation

Splunk Architecture & Indexing Guide

Question: 7

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

Answer: A, D C

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

1 Qesting 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.

2 Qerifying 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.

3 (^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.

Incorrect Answers & Explanations

B . Monitoring data ingestion rates → Data ingestion is crucial for Splunk Enterprise, but not a core integration validation step for SOAR.

E . Increasing indexer capacity → This is related to Splunk Enterprise data indexing, not Splunk SOAR integration validation.

Additional Resources:

Splunk SOAR Administration Guide

Splunk SOAR Playbook Validation

Splunk SOAR API Integrations

Question: 8

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

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.
Reference:
Splunk ES Documentation on Notable Event Enrichment
Correlation Search Best Practices
Using Lookups for Data Enrichment

Question: 9

What is the primary purpose of correlation searches in Splunk?

A. To extract and index raw data
B. To identify patterns and relationships between multiple data sources
C. To create dashboards for real-time monitoring
D. To store pre-aggregated search results

Answer: B

Explanation:

Correlation searches in Splunk Enterprise Security (ES) are a critical component of Security Operations Center (SOC) workflows, designed to detect threats by analyzing security data from multiple sources.
Primary Purpose of Correlation Searches:

Identify threats and anomalies: They detect patterns and suspicious activity by correlating logs, alerts, and events from different sources.

Automate security monitoring: By continuously running searches on ingested data, correlation searches help reduce manual efforts for SOC analysts.

Generate notable events: When a correlation search identifies a security risk, it creates a notable event in Splunk ES for investigation.

Trigger security automation: In combination with Splunk SOAR, correlation searches can initiate automated response actions, such as isolating endpoints or blocking malicious IPs.

Since correlation searches analyze relationships and patterns across multiple data sources to detect security threats, the correct answer is B. To identify patterns and relationships between multiple data sources.

Reference:

Splunk ES Correlation Searches Overview

Best Practices for Correlation Searches

Splunk ES Use Cases and Notable Events

Question: 10

Which practices strengthen the development of Standard Operating Procedures (SOPs)? (Choose three)

A. Regular updates based on feedback
B. Focusing solely on high-risk scenarios
C. Collaborating with cross-functional teams
D. Including detailed step-by-step instructions
E. Excluding historical incident data

Answer: A, C, D

Explanation:

Why Are These Practices Essential for SOP Development?

Standard Operating Procedures (SOPs) are crucial for ensuring consistent, repeatable, and effective security operations in a Security Operations Center (SOC). Strengthening SOP development ensures efficiency, clarity, and adaptability in responding to incidents.

1 (^Regular Updates Based on Feedback (Answer A)

Security threats evolve, and SOPs must be updated based on real-world incidents, analyst feedback, and lessons learned.

Example: A new ransomware variant is detected; the SOP is updated to include a specific containment playbook in Splunk SOAR.

2 Qollaborating with Cross-Functional Teams (Answer C)

Effective SOPs require input from SOC analysts, threat hunters, IT, compliance teams, and DevSecOps.

Ensures that all relevant security and business perspectives are covered.

Example: A SOC team collaborates with DevOps to ensure that a cloud security response SOP aligns with AWS security controls.

3 Qincluding Detailed Step-by-Step Instructions (Answer D)

SOPs should provide clear, actionable, and standardized steps for security analysts.

Example: A Splunk ES incident response SOP should include:

How to investigate a security alert using correlation searches.

How to escalate incidents based on risk levels.

How to trigger a Splunk SOAR playbook for automated remediation.

Why Not the Other Options?

B. Focusing solely on high-risk scenarios – All security events matter, not just high-risk ones. Low- level alerts can be early indicators of larger threats.

E. Excluding historical incident data – Past incidents provide valuable lessons to improve SOPs and incident response workflows.

Reference & Learning Resources

Best Practices for SOPs in Cybersecurity: https://www.nist.gov/cybersecurity-framework

Splunk SOAR Playbook SOP Development: https://docs.splunk.com/Documentation/SOAR

Incident Response SOPs with Splunk: https://splunkbase.splunk.com

Question: 11

A Splunk administrator needs to integrate a third-party vulnerability management tool to automate remediation workflows.

What is the most efficient first step?

A. Set up a manual alerting system for vulnerabilities
B. Use REST APIs to integrate the third-party tool with Splunk SOAR
C. Write a correlation search for each vulnerability type
D. Configure custom dashboards to monitor vulnerabilities

Answer: B

Explanation:

Why Use REST APIs for Integration?

When integrating a third-party vulnerability management tool (e.g., Tenable, Qualys, Rapid7) with Splunk SOAR, using REST APIs is the most efficient and scalable approach.

Why REST APIs?

APIs enable direct communication between Splunk SOAR and the third-party tool.

Allows automated ingestion of vulnerability data into Splunk.

Supports automated remediation workflows (e.g., patch deployment, firewall rule updates).

Reduces manual work by allowing Splunk SOAR to pull real-time data from the vulnerability tool.

Steps to Integrate a Third-Party Vulnerability Tool with Splunk SOAR Using REST API:

1 ClObtain API Credentials — Get API keys or authentication tokens from the vulnerability management tool.

2 Qonfigure REST API Integration - Use Splunk SOAR's built-in API connectors or create a custom REST API call.

3 Qhgest Vulnerability Data into Splunk - Map API responses to Splunk ES correlation searches.

4 (^Automate Remediation Playbooks - Build Splunk SOAR playbooks to:

Automatically open tickets for critical vulnerabilities.

Trigger patches or firewall rules for high-risk vulnerabilities.

Notify SOC analysts when a high-risk vulnerability is detected on a critical asset.

Example Use Case in Splunk SOAR:

Scenario: The company uses Tenable.io for vulnerability management.

Splunk SOAR connects to Tenable's API and pulls vulnerability scan results.

If a critical vulnerability is found on a production server, Splunk SOAR:

Automatically creates a ServiceNow ticket for remediation.

Triggers a patching script to fix the vulnerability.

Updates Splunk ES dashboards for tracking.

Why Not the Other Options?

A. Set up a manual alerting system for vulnerabilities – Manual alerting is inefficient and doesn't scale well.

C. Write a correlation search for each vulnerability type – This would create too many rules; API integration allows real-time updates from the vulnerability tool.

D. Configure custom dashboards to monitor vulnerabilities – Dashboards provide visibility but don't automate remediation.

Reference & Learning Resources

Splunk SOAR API Integration Guide: https://docs.splunk.com/Documentation/SOAR

Integrating Tenable, Qualys, Rapid7 with Splunk: https://splunkbase.splunk.com

REST API Automation in Splunk SOAR: https://www.splunk.com/en_us/products/soar.html

Question: 12

Which sourcetype configurations affect data ingestion? (Choose three)

A. Event breaking rules
B. Timestamp extraction
C. Data retention policies
D. Line merging rules

Answer: A, B, D

Explanation:

The sourcetype in Splunk defines how incoming machine data is interpreted, structured, and stored. Proper sourcetype configurations ensure accurate event parsing, indexing, and searching.

Q 1. Event Breaking Rules (A)

Determines how Splunk splits raw logs into individual events.

If misconfigured, a single event may be broken into multiple fragments or multiple log lines may be combined incorrectly.

Controlled using LINE_BREAKER and BREAK_ONLY_BEFORE settings.

Q 2. Timestamp Extraction (B)

Extracts and assigns timestamps to events during ingestion.

Incorrect timestamp configuration leads to misplaced events in time-based searches.

Uses TIME_PREFIX, MAX_TIMESTAMP_LOOKAHEAD, and TIME_FORMAT settings.

Q 3. Line Merging Rules (D)

Controls whether multiline events should be combined into a single event.

Useful for logs like stack traces or multi-line syslog messages.

Uses SHOULD_LINEMERGE and LINE_BREAKER settings.

X Incorrect Answer:

C . Data Retention Policies →

Affects storage and deletion, not data ingestion itself.

Additional Resources:

Splunk Sourcetype Configuration Guide

Event Breaking and Line Merging

Question: 13

What is a key feature of effective security reports for stakeholders?

A. High-level summaries with actionable insights
B. Detailed event logs for every incident
C. Exclusively technical details for IT teams
D. Excluding compliance-related metrics

Answer: A

Explanation:

Security reports provide stakeholders (executives, compliance officers, and security teams) with insights into security posture, risks, and recommendations.

Q Key Features of Effective Security Reports

High-Level Summaries

Stakeholders don't need raw logs but require summary-level insights on threats and trends.

Actionable Insights

Reports should provide clear recommendations on mitigating risks.

Visual Dashboards & Metrics

Charts, KPIs, and trends enhance understanding for non-technical stakeholders.

X Incorrect Answers:

B . Detailed event logs for every incident → Logs are useful for analysts, not executives.

C . Exclusively technical details for IT teams → Reports should balance technical & business insights.

D . Excluding compliance-related metrics → Compliance is critical in security reporting.

Additional Resources:

Splunk Security Reporting Best Practices

Creating Executive Security Reports

Question: 14

Which Splunk feature enables integration with third-party tools for automated response actions?

A. Data model acceleration
B. Workflow actions
C. Summary indexing
D. Event sampling

Answer: B

Explanation:

Security teams use Splunk Enterprise Security (ES) and Splunk SOAR to integrate with firewalls, endpoint security, and SIEM tools for automated threat response.

Q Workflow Actions (B) - Key Integration Feature

Allows analysts to trigger automated actions directly from Splunk searches and dashboards.

Can integrate with SOAR playbooks, ticketing systems (e.g., ServiceNow), or firewalls to take action.

Example:

Block an IP on a firewall from a Splunk dashboard.

Trigger a SOAR playbook for automated threat containment.

X Incorrect Answers:

A . Data Model Acceleration → Speeds up searches, but doesn't handle integrations.

C . Summary Indexing → Stores summarized data for reporting, not automation.

D . Event Sampling → Reduces search load, but doesn't trigger automated actions.

Additional Resources:

Splunk Workflow Actions Documentation Automating Response with Splunk SOAR

Question: 15

Which action improves the effectiveness of notable events in Enterprise Security?

A. Applying suppression rules for false positives
B. Disabling scheduled searches
C. Using only raw log data in searches
D. Limiting the search scope to one index

Answer: A

Explanation:

Notable events in Splunk Enterprise Security (ES) are triggered by correlation searches, which generate alerts when suspicious activity is detected. However, if too many false positives occur, analysts waste time investigating non-issues, reducing SOC efficiency.

How to Improve Notable Events Effectiveness:

Apply suppression rules to filter out known false positives and reduce alert fatigue.

Refine correlation searches by adjusting thresholds and tuning event detection logic.

Leverage risk-based alerting (RBA) to prioritize high-risk events.

Use adaptive response actions to enrich events dynamically.

By suppressing false positives, SOC analysts focus on real threats, making notable events more actionable. Thus, the correct answer is A. Applying suppression rules for false positives.

Reference:

Managing Notable Events in Splunk ES

Best Practices for Tuning Correlation Searches

Using Suppression in Splunk ES

Question: 16

Which actions can optimize case management in Splunk? (Choose two)

A. Standardizing ticket creation workflows
B. Increasing the indexing frequency
C. Integrating Splunk with ITSM tools
D. Reducing the number of search heads

Answer: AC

Explanation:

Effective case management in Splunk Enterprise Security (ES) helps streamline incident tracking, investigation, and resolution.
How to Optimize Case Management:

Standardizing ticket creation workflows (A)
Ensures consistency in how incidents are reported and tracked.
Reduces manual errors and improves collaboration between SOC teams.
Integrating Splunk with ITSM tools (C)
Automates the process of creating and updating tickets in ServiceNow, Jira, or Remedy.
Enables better tracking of incidents and response actions.
Incorrect Answers:

X B. Increasing the indexing frequency – This improves data availability but does not directly optimize case management.

X D. Reducing the number of search heads – This might degrade search performance rather than optimize case handling.
Reference:
Splunk ES Case Management
Integrating Splunk with ServiceNow
Automating Ticket Creation in Splunk

Question: 17

Which REST API actions can Splunk perform to optimize automation workflows? (Choose two)

A. POST for creating new data entries
B. DELETE for archiving historical data
C. GET for retrieving search results
D. PUT for updating index configurations

Answer: A, C

Explanation:

The Splunk REST API allows programmatic access to Splunk's features, helping automate security workflows in a Security Operations Center (SOC).
Key REST API Actions for Automation:
POST for creating new data entries (A)
Used to send logs, alerts, or notable events to Splunk.
Essential for integrating external security tools with Splunk.
GET for retrieving search results (C)
Fetches logs, alerts, and notable event details programmatically.
Helps automate security monitoring and incident response.
Incorrect Answers:

X B. DELETE for archiving historical data – DELETE is rarely used in Splunk as it does not archive data; instead, retention policies handle old data.

X D. PUT for updating index configurations – While PUT can modify configurations, it is not a core automation function in SOC workflows.
Reference:

Splunk REST API Documentation
Using Splunk API for Automation
Best Practices for Automating Security Workflows

Question: 18

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

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?
Q Maps event fields to a standardized schema
Q Supports prebuilt Splunk apps like Enterprise Security (ES)
Q 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?
X A. Extract fields from raw events – CIM does not extract fields; it maps existing fields into a standardized format.
X C. Compress data during indexing – CIM is about data normalization, not compression.
X 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: 19

A company's Splunk setup processes logs from multiple sources with inconsistent field naming conventions.
How should the engineer ensure uniformity across data for better analysis?

A. Create field extraction rules at search time.
B. Use data model acceleration for real-time searches.
C. Apply Common Information Model (CIM) data models for normalization.
D. Configure index-time data transformations.

Answer: C

Explanation:

Why Use CIM for Field Normalization?

When processing logs from multiple sources with inconsistent field names, the best way to ensure uniformity is to use Splunk's Common Information Model (CIM).

Key Benefits of CIM for Normalization:

Ensures that different field names (e.g., src_ip, ip_src, source_address) are mapped to a common schema.
Allows security teams to run a single search query across multiple sources without manual mapping.
Enables correlation searches in Splunk Enterprise Security (ES) for better threat detection.
Example Scenario in a SOC:

Problem: The SOC team needs to correlate firewall logs, cloud logs, and endpoint logs for failed logins.

Q Without CIM: Each log source uses a different field name for failed logins, requiring multiple search queries.

Q With CIM: All failed login events map to the same standardized field (e.g., action="failure"), allowing one unified search query.

Why Not the Other Options?

X A. Create field extraction rules at search time – Helps with parsing data but doesn't standardize field names across sources.

X B. Use data model acceleration for real-time searches – Accelerates searches but doesn't fix inconsistent field naming.

X D. Configure index-time data transformations – Changes fields at indexing but is less flexible than CIM's search-time normalization.

Reference & Learning Resources
Splunk CIM for Normalization: https://docs.splunk.com/Documentation/CIM
Splunk ES CIM Field Mappings: https://splunkbase.splunk.com/app/263
Best Practices for Log Normalization: https://www.splunk.com/en_us/blog/tips-and-tricks

Question: 20

Which Splunk configuration ensures events are parsed and indexed only once for optimal storage?

A. Summary indexing
B. Universal forwarder
C. Index time transformations
D. Search head clustering

Answer: C

Explanation:

Why Use Index-Time Transformations for One-Time Parsing & Indexing?

Splunk parses and indexes data once during ingestion to ensure efficient storage and search performance. Index-time transformations ensure that logs are:

Q Parsed, transformed, and stored efficiently before indexing.

Q Normalized before indexing, so the SOC team doesn't need to clean up fields later.

Q Processed once, ensuring optimal storage utilization.

Example of Index-Time Transformation in Splunk:

Scenario: The SOC team needs to mask sensitive data in security logs before storing them in Splunk.

Q Solution: Use an INDEXED_EXTRACTIONS rule to:

Redact confidential fields (e.g., obfuscate Social Security Numbers in logs).

Rename fields for consistency before indexing.

Question: 21

Which elements are critical for documenting security processes? (Choose two)

A. Detailed event logs
B. Visual workflow diagrams
C. Incident response playbooks
D. Customer satisfaction surveys

Answer: B, C

Explanation:

Effective documentation ensures that security teams can standardize response procedures, reduce incident response time, and improve compliance.

Q 1. Visual Workflow Diagrams (B)

Helps map out security processes in an easy-to-understand format.

Useful for SOC analysts, engineers, and auditors to understand incident escalation procedures.

Example:

Incident flow diagrams showing escalation from Tier 1 SOC analysts → Threat hunters → Incident response teams.

Q 2. Incident Response Playbooks (C)

Defines step-by-step response actions for security incidents.

Standardizes how teams should detect, analyze, contain, and remediate threats.

Example:

A SOAR playbook for handling phishing emails (e.g., extract indicators, check sandbox results, quarantine email).

X Incorrect Answers:

A . Detailed event logs → Logs are essential for investigations but do not constitute process documentation.

D . Customer satisfaction surveys → Not relevant to security process documentation.

Additional Resources:

NIST Cybersecurity Framework - Incident Response

Splunk SOAR Playbook Documentation

Question: 22

What is a key advantage of using SOAR playbooks in Splunk?

A. Manually running searches across multiple indexes
B. Automating repetitive security tasks and processes
C. Improving dashboard visualization capabilities
D. Enhancing data retention policies

Answer: B

Explanation:

Splunk SOAR (Security Orchestration, Automation, and Response) playbooks help SOC teams automate, orchestrate, and respond to threats faster.

Q Key Benefits of SOAR Playbooks

Automates Repetitive Tasks

Reduces manual workload for SOC analysts.

Automates tasks like enriching alerts, blocking IPs, and generating reports.

Orchestrates Multiple Security Tools

Integrates with firewalls, EDR, SIEMs, threat intelligence feeds.

Example: A playbook can automatically enrich an IP address by querying VirusTotal, Splunk, and SIEM logs.

Accelerates Incident Response

Reduces Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

Example: A playbook can automatically quarantine compromised endpoints in CrowdStrike after an alert.

X Incorrect Answers:

A . Manually running searches across multiple indexes → SOAR playbooks are about automation, not manual searches.

C . Improving dashboard visualization capabilities → Dashboards are part of SIEM (Splunk ES), not SOAR playbooks.

D . Enhancing data retention policies → Retention is a Splunk Indexing feature, not SOAR-related.

Additional Resources:

Splunk SOAR Playbook Guide

Automating Threat Response with SOAR

Question: 23

What elements are critical for developing meaningful security metrics? (Choose three)

A. Relevance to business objectives
B. Regular data validation
C. Visual representation through dashboards
D. Avoiding integration with third-party tools
E. Consistent definitions for key terms

Answer: A, B, E

Explanation:

Key Elements of Meaningful Security Metrics

Security metrics should align with business goals, be validated regularly, and have standardized definitions to ensure reliability.

Q 1. Relevance to Business Objectives (A)

Security metrics should tie directly to business risks and priorities.

Example:

A financial institution might track fraud detection rates instead of generic malware alerts.

Q 2. Regular Data Validation (B)

Ensures data accuracy by removing false positives, duplicates, and errors.

Example:

Validating phishing alert effectiveness by cross-checking with user-reported emails.

Q 3. Consistent Definitions for Key Terms (E)

Standardized definitions prevent misinterpretation of security metrics.

Example:

Clearly defining MTTD (Mean Time to Detect) vs. MTTR (Mean Time to Respond).

X Incorrect Answers:

C . Visual representation through dashboards → Dashboards help, but data quality matters more.

D f. Avoiding integration with third-party tools → Integrations with SIEM, SOAR, EDR, and firewalls are crucial for effective metrics.

Additional Resources:

NIST Security Metrics Framework

Splunk

Question: 24

Which REST API method is used to retrieve data from a Splunk index?

A. POST

B. GET

C. PUT

D. DELETE

Answer: B

Explanation:

The GET method in the Splunk REST API is used to retrieve data from a Splunk index. It allows users and automated scripts to fetch logs, alerts, or query results programmatically.

Key Points About GET in Splunk API:

Used for searching and retrieving logs from indexes.

Can be used to get search results, job status, and Splunk configuration details.

Common API endpoints include:

/services/search/jobs/{search_id}/results – Retrieves results of a completed search.

/services/search/jobs/export – Exports search results in real-time.

Incorrect Answers:

X A. POST – Used for submitting new search jobs or sending data to Splunk.

X C. PUT – Used for modifying existing Splunk configurations, not retrieving data.

X D. DELETE – Used to remove Splunk objects like reports or alerts, not for retrieval.

Reference:

Splunk REST API - GET Method
How to Use Splunk API for Search Queries

Question: 25

What is the primary function of a Lean Six Sigma methodology in a security program?

A. Automating detection workflows
B. Optimizing processes for efficiency and effectiveness
C. Monitoring the performance of detection searches
D. Enhancing user activity logs

Answer: B

Explanation:

Lean Six Sigma (LSS) is a process improvement methodology used to enhance operational efficiency by reducing waste, eliminating errors, and improving consistency.
Primary Function of Lean Six Sigma in a Security Program:
Improves security operations efficiency by optimizing alert handling, threat hunting, and incident response workflows.
Reduces unnecessary steps in SOC processes, eliminating redundancies in threat detection and response.
Enhances decision-making by using data-driven analysis to improve security metrics and Key Performance Indicators (KPIs).
Incorrect Answers:
X A. Automating detection workflows – Lean Six Sigma focuses on process improvement, not automation.
X C. Monitoring the performance of detection searches – While Lean Six Sigma enhances efficiency,
it does not specifically monitor search performance.
X D. Enhancing user activity logs – This is related to logging and auditing, not Lean Six Sigma. Reference:
Lean Six Sigma in Cybersecurity
Using Six Sigma to Improve SOC Processes

Question: 26

What Splunk process ensures that duplicate data is not indexed?

A. Data deduplication
B. Metadata tagging
C. Indexer clustering
D. Event parsing

Answer: D

Explanation:

Splunk prevents duplicate data from being indexed through event parsing, which occurs during the data ingestion process.

How Event Parsing Prevents Duplicate Data:

Splunk's indexer parses incoming data and assigns unique timestamps, metadata, and event IDs to prevent reindexing duplicate logs.

CRC Checks (Cyclic Redundancy Checks) are applied to avoid duplicate event ingestion.

Index-time filtering and transformation rules help detect and drop repeated data before indexing.

Incorrect Answers:

X A. Data deduplication – While deduplication removes duplicates in searches, it does not prevent duplicate indexing.

X B. Metadata tagging – Tags help with categorization but do not control duplication.

X C. Indexer clustering – Clustering improves redundancy and availability but does not prevent duplicates.

Reference:

Splunk Data Parsing Process

Splunk Indexing and Data Handling

Question: 27

A cybersecurity engineer notices a delay in retrieving indexed data during a security incident investigation. The Splunk environment has multiple indexers but only one search head.

Which approach can resolve this issue?

A. Increase search head memory allocation.

B. Optimize search queries to use tstats instead of raw searches.

C. Configure a search head cluster to distribute search queries.

D. Implement accelerated data models for faster querying.

Answer: B

Explanation:

Why Use tstats for Faster Searches?

When a cybersecurity engineer experiences delays in retrieving indexed data, the best way to improve search performance is to use tstats instead of raw searches.

What is tstats?

tstats is a high-performance command that queries data from indexed fields only, rather than scanning raw events. This makes searches significantly faster and more efficient.

Why is This the Best Approach?

tstats searches are 10-100x faster than raw event searches.

It leverages metadata and indexed fields, reducing search load.

It minimizes memory and CPU usage on the search head and indexers.

Example Use Case:

Scenario: The SOC team is investigating failed logins across multiple indexers.

Q Using a raw search:

index=security sourcetype=auth_logs action=failed | stats count by user

Problem: This query scans millions of raw events, causing slow performance.

Q Optimized using tstats:

| tstats count where index=security sourcetype=auth_logs action=failed by user

Q Advantage: Faster results without scanning raw events.

Why Not the Other Options?

X A. Increase search head memory allocation – May help, but inefficient queries will still slow down searches.

X C. Configure a search head cluster – A single search head isn't necessarily the problem; improving search performance is more effective.

X D. Implement accelerated data models – Useful for prebuilt dashboards, but won't improve ad- hoc searches.

Question: 28

How can you ensure that a specific sourcetype is assigned during data ingestion?

A. Use props.conf to specify the sourcetype.
B. Define the sourcetype in the search head.
C. Configure the sourcetype in the deployment server.
D. Use REST API calls to tag sourcetypes dynamically.

Answer: A

Explanation:

Why Use props.conf to Assign Sourcetypes?

In Splunk, sourcetypes define the format and structure of incoming data. Assigning the correct sourcetype ensures that logs are parsed, indexed, and searchable correctly.

How Does props.conf Help?

props.conf allows manual sourcetype assignment based on source or host.

Ensures that logs are indexed with the correct parsing rules (timestamps, fields, etc.).

Example Configuration in props.conf: ini

CopyEdit

[source::/var/log/auth.log]

sourcetype = auth_logs

Q This forces all logs from /var/log/auth.log to be assigned sourcetype=auth_logs.

Why Not the Other Options?

X B. Define the sourcetype in the search head – Sourcetypes are assigned at ingestion time, not at search time.

X C. Configure the sourcetype in the deployment server – The deployment server manages configurations, but props.conf is what actually assigns sourcetypes.

X D. Use REST API calls to tag sourcetypes dynamically – REST APIs help modify configurations, but they don't assign sourcetypes directly during ingestion.

Reference & Learning Resources

Splunk props.conf Documentation:

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf

Best Practices for Sourcetype Management: https://www.splunk.com/en_us/blog/tips-and-tricks

Splunk Data Parsing Guide: https://splunkbase.splunk.com

Question: 29

What is the main purpose of incorporating threat intelligence into a security program?

A. To automate response workflows
B. To proactively identify and mitigate potential threats
C. To generate incident reports for stakeholders

D. To archive historical events for compliance

Answer: B

Explanation:

Why Use Threat Intelligence in Security Programs?

Threat intelligence provides real-time data on known threats, helping SOC teams identify, detect, and mitigate security risks proactively.

Key Benefits of Threat Intelligence:

Q Early Threat Detection – Identifies known attack patterns (IP addresses, domains, hashes).

Q Proactive Defense – Blocks threats before they impact systems.

Q Better Incident Response – Speeds up triage and forensic analysis.

Q Contextualized Alerts – Reduces false positives by correlating security events with known threats.

Example Use Case in Splunk ES:

Scenario: The SOC team ingests threat intelligence feeds (e.g., from MITRE ATT&CK, VirusTotal).

Q Splunk Enterprise Security (ES) correlates security events with known malicious IPs or domains.

Q If an internal system communicates with a known C2 server, the SOC team automatically receives an alert and blocks the IP using Splunk SOAR.

Why Not the Other Options?

X A. To automate response workflows – While automation is beneficial, threat intelligence is primarily for proactive identification.

X C. To generate incident reports for stakeholders – Reports are a byproduct, but not the main goal of threat intelligence.

X D. To archive historical events for compliance – Threat intelligence is real-time and proactive, whereas compliance focuses on record-keeping.

Reference & Learning Resources

Splunk ES Threat Intelligence Guide: https://docs.splunk.com/Documentation/ES

MITRE ATT&CK Integration with Splunk: https://attack.mitre.org/resources

Threat Intelligence Best Practices in SOC: https://splunkbase.splunk.com

Question: 30

What are the key components of Splunk's indexing process? (Choose three)

A. Parsing
B. Searching
C. Indexing
D. Alerting
E. Input phase

Answer: A, C, E

Explanation:

Key Components of Splunk's Indexing Process

Splunk's indexing process consists of multiple stages that ingest, process, and store data efficiently for search and analysis.

Q 1. Input Phase (E)

Collects data from sources (e.g., syslogs, cloud services, network devices).

Defines where the data comes from and applies pre-processing rules.

Example:

A firewall log is ingested from a syslog server into Splunk.

Q 2. Parsing (A)

Breaks raw data into individual events.

Applies rules for timestamp extraction, line breaking, and event formatting.

Example:

A multiline log file is parsed so that each log entry is a separate event.

Q 3. Indexing (C)

Stores parsed data in indexes to enable fast searching.

Assigns metadata like host, source, and sourcetype.

Example:

An index=firewall_logs contains all firewall-related events.

X Incorrect Answers:

B . Searching → Searching happens after indexing, not during the indexing process.

D . Alerting → Alerting is part of SIEM and detection, not indexing.

Additional Resources:

Splunk Indexing Process Documentation

Splunk Data Processing Pipeline

Question: 31

How can you ensure efficient detection tuning? (Choose three)

A. Perform regular reviews of false positives.
B. Use detailed asset and identity information.
C. Disable correlation searches for low-priority threats.
D. Automate threshold adjustments.

Answer: A, B, D

Explanation:

Ensuring Efficient Detection Tuning in Splunk Enterprise Security

Detection tuning is essential to minimize false positives and improve security visibility.

Q 1. Perform Regular Reviews of False Positives (A)

Reviewing false positives helps refine detection logic.

Analysts should analyze past alerts and adjust correlation rules.

Example:

Tuning a failed login correlation search to exclude known legitimate admin accounts.

Q 2. Use Detailed Asset and Identity Information (B)

Enriches detections with asset and user context.

Helps differentiate high-risk vs. low-risk security events.

Example:

A login from an executive's laptop is higher risk than from a test server.

Q 3. Automate Threshold Adjustments (D)

Dynamic thresholds adjust based on activity baselines.

Reduces false positives while maintaining security coverage.

Example:

A brute-force detection rule dynamically adjusts its alerting threshold based on normal user behavior.

X Incorrect Answer:

C . Disable correlation searches for low-priority threats → Instead of disabling, adjust the rule sensitivity or lower alert severity.

Additional Resources:

Splunk Security Essentials: Detection Tuning Guide

Tuning Correlation Searches in Splunk ES

Question: 32

Which configurations are required for data normalization in Splunk? (Choose two)

A. props.conf
B. transforms.conf
C. savedsearches.conf
D. authorize.conf
E. eventtypes.conf

Answer: A, B

Explanation:

Configurations Required for Data Normalization in Splunk

Data normalization ensures consistent field naming and event structuring, especially for Splunk Common Information Model (CIM) compliance.

Q 1. props.conf (A)

Defines how data is parsed and indexed.

Controls field extractions, event breaking, and timestamp recognition.

Example:

Assigns custom sourcetypes and defines regex-based field extraction.

Q 2. transforms.conf (B)

Used for data transformation, lookup table mapping, and field aliasing.

Example:

Normalizes firewall logs by renaming src_ip → src to align with CIM.

X Incorrect Answers:

C . savedsearches.conf → Defines scheduled searches, not data normalization.

D . authorize.conf → Manages user permissions, not data normalization.

E . eventtypes.conf → Groups events into categories but doesn't modify data structure.

Additional Resources:

Splunk Data Normalization Guide

Understanding props.conf and transforms.conf

Question: 33

What methods improve risk and detection prioritization? (Choose three)

A. Assigning risk scores to assets and events
B. Using predefined alert templates
C. Incorporating business context into decisions
D. Automating detection tuning
E. Enforcing strict search head resource limits

Answer: A, C, D

Explanation:

Risk and detection prioritization in Splunk Enterprise Security (ES) helps SOC analysts focus on the most critical threats. By assigning risk scores, integrating business context, and automating detection tuning, organizations can prioritize security incidents efficiently.

Methods to Improve Risk and Detection Prioritization:

Assigning Risk Scores to Assets and Events (A)

Uses Risk-Based Alerting (RBA) to prioritize high-risk activities based on behavior and history.

Helps SOC teams focus on true threats instead of isolated events.

Incorporating Business Context into Decisions (C)

Adds context from asset criticality, user roles, and business impact.

Ensures alerts are ranked based on their potential business impact.

Automating Detection Tuning (D)

Uses machine learning and adaptive response actions to reduce false positives.

Dynamically adjusts alert thresholds based on evolving threat patterns.

Incorrect Answers:

X B. Using predefined alert templates – Static templates don't dynamically prioritize risk.

X E. Enforcing strict search head resource limits – This impacts system performance but does not directly improve detection prioritization.

Reference:

Splunk Risk-Based Alerting (RBA) Documentation

Best Practices for Prioritizing Security Alerts

Using Machine Learning for Threat Detection

Question: 34

What are the main steps of the Splunk data pipeline? (Choose three)

A. Indexing
B. Visualization
C. Input phase
D. Parsing
E. Alerting

Answer: A, C, D

Explanation:

The Splunk Data Pipeline consists of multiple stages that process incoming data from ingestion to visualization.

Main Steps of the Splunk Data Pipeline:

Input Phase (C)

Splunk collects raw data from logs, applications, network traffic, and endpoints.

Supports various data sources like syslog, APIs, cloud services, and agents (e.g., Universal Forwarders).

Parsing (D)

Splunk breaks incoming data into events and extracts metadata fields.

Removes duplicates, formats timestamps, and applies transformations.

Indexing (A)

Stores parsed events into indexes for efficient searching.

Supports data retention policies, compression, and search optimization.

Incorrect Answers:

X B. Visualization – Happens later in dashboards, but not part of the data pipeline itself.

X E. Alerting – Occurs after the data pipeline processes and analyzes events.

Reference:

Splunk Data Processing Pipeline Overview

How Splunk Parses and Indexes Data

Question: 35

What methods enhance risk-based detection in Splunk? (Choose two)

A. Defining accurate risk modifiers

B. Limiting the number of correlation searches

C. Using summary indexing for raw events

D. Enriching risk objects with contextual data

Answer: A, D

Explanation:

Risk-based detection in Splunk prioritizes alerts based on behavior, threat intelligence, and business impact. Enhancing risk scores and enriching contextual data ensures that SOC teams focus on the most critical threats.

Methods to Enhance Risk-Based Detection:

Defining Accurate Risk Modifiers (A)

Adjusts risk scores dynamically based on asset value, user behavior, and historical activity.

Ensures that low-priority noise doesn't overwhelm SOC analysts.

Enriching Risk Objects with Contextual Data (D)

Adds threat intelligence feeds, asset criticality, and user behavior data to alerts.

Improves incident triage and correlation of multiple low-level events into significant threats. Incorrect Answers:

X B. Limiting the number of correlation searches – Reducing correlation searches may lead to missed threats.

X C. Using summary indexing for raw events – Summary indexing improves performance but does not enhance risk-based detection.

Reference:

Splunk Risk-Based Alerting Guide

Threat Intelligence in Splunk ES

Question: 36

Which of the following actions improve data indexing performance in Splunk? (Choose two)

A. Indexing data with detailed metadata
B. Configuring index time field extractions
C. Using lightweight forwarders for data ingestion
D. Increasing the number of indexers in a distributed environment

Answer: B, D

Explanation:

How to Improve Data Indexing Performance in Splunk?

Optimizing indexing performance is critical for ensuring faster search speeds, better storage efficiency, and reduced latency in a Splunk deployment.

Why is "Configuring Index-Time Field Extractions" Important? (Answer B)

Extracting fields at index time reduces the need for search-time processing, making searches faster. Example: If security logs contain IP addresses, usernames, or error codes, configuring index-time extraction ensures that these fields are already available during searches.

Why "Increasing the Number of Indexers in a Distributed Environment" Helps? (Answer D)

Adding more indexers distributes the data load, improving overall indexing speed and search performance.

Example: In a large SOC environment, more indexers allow for faster log ingestion from multiple sources (firewalls, IDS, cloud services).

Why Not the Other Options?

X A. Indexing data with detailed metadata – Adding too much metadata increases indexing overhead and slows down performance.

X C. Using lightweight forwarders for data ingestion – Lightweight forwarders only forward raw data and don't enhance indexing performance.

Reference & Learning Resources

Splunk Indexing Performance Guide:
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Howindexingworks

Best Practices for Splunk Indexing Optimization: https://splunkbase.splunk.com

Distributed Splunk Architecture for Large-Scale Environments:
https://www.splunk.com/en_us/blog/tips-and-tricks

Question: 37

Which report type is most suitable for monitoring the success of a phishing campaign detection program?

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

Answer: B

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)

Q Shows live security alerts for phishing detections.

Q Enables SOC analysts to take immediate action (e.g., blocking malicious domains, disabling compromised accounts).

Q Uses correlation searches in Splunk Enterprise Security (ES) to detect phishing indicators.

Example in Splunk:

Scenario: A company runs a phishing awareness campaign.

Q 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?

X A. Weekly incident trend reports – Helpful for analysis but not fast enough for phishing detection.

X C. Risk score-based summary reports – Risk scores are useful but not designed for real-time phishing detection.

X D. SLA compliance reports – SLA reports measure performance but don't help actively detect phishing attacks.

Reference & 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

Question: 38

What is the role of event timestamping during Splunk's data indexing?

A. Assigning data to a specific source type
B. Tagging events for correlation searches
C. Synchronizing event data with system time
D. Ensuring events are organized chronologically

Answer: D

Explanation:

Why is Event Timestamping Important in Splunk?

Event timestamps help maintain the correct sequence of logs, ensuring that data is accurately analyzed and correlated over time.

Why "Ensuring Events Are Organized Chronologically" is the Best Answer? (Answer D)

Q Prevents event misalignment – Ensures logs appear in the correct order.

Q Enables accurate correlation searches – Helps SOC analysts trace attack timelines.

Q Improves incident investigation accuracy – Ensures that event sequences are correctly reconstructed.

Example in Splunk:

Scenario: A security analyst investigates a brute-force attack across multiple logs.

Q Without correct timestamps, login failures might appear out of order, making analysis difficult.

Q With proper event timestamping, logs line up correctly, allowing SOC analysts to detect the exact attack timeline.

Why Not the Other Options?

X A. Assigning data to a specific sourcetype – Sourcetypes classify logs but don't affect timestamps.

X B. Tagging events for correlation searches – Correlation uses timestamps but timestamping itself isn't about tagging.

X C. Synchronizing event data with system time – System time matters, but event timestamping is about chronological ordering.

Reference & Learning Resources

Splunk Event Timestamping Guide:

https://docs.splunk.com/Documentation/Splunk/latest/Data/HowSplunkextractstimestamps

Best Practices for Log Time Management in Splunk: https://www.splunk.com/en_us/blog/tips-and- tricks

SOC Investigations & Log Timestamping: https://splunkbase.splunk.com

Question: 39

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

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.

Q 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).

X 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: 40

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

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.

Q 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.

X 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: 41

Which components are necessary to develop a SOAR playbook in Splunk? (Choose three)

A. Defined workflows
B. Threat intelligence feeds
C. Actionable steps or tasks
D. Manual approval processes
E. Integration with external tools

Answer: A, C, E

Explanation:

Splunk SOAR (Security Orchestration, Automation, and Response) playbooks automate security processes, reducing response times.

Q 1. Defined Workflows (A)

A structured flowchart of actions for handling security events.

Ensures that the playbook follows a logical sequence (e.g., detect → enrich → contain → remediate). Example:
If a phishing email is detected, the workflow includes:
Extract email artifacts (e.g., sender, links).
Check indicators against threat intelligence feeds.
Quarantine the email if it is malicious.
Q 2. Actionable Steps or Tasks (C)
Each playbook contains specific, automated steps that execute responses.
Examples:
Extracting indicators from logs.
Blocking malicious IPs in firewalls.
Isolating compromised endpoints.
Q 3. Integration with External Tools (E)
Playbooks must connect with SIEM, EDR, firewalls, threat intelligence platforms, and ticketing systems.
Uses APIs and connectors to integrate with tools like:
Splunk ES
Palo Alto Networks
Microsoft Defender
ServiceNow
X Incorrect Answers:
B . Threat intelligence feeds → These enrich playbooks but are not mandatory components of playbook development.
D . Manual approval processes → Playbooks are designed for automation, not manual approvals. Additional Resources:
Splunk SOAR Playbook Documentation
Best Practices for Developing SOAR Playbooks

Question: 42

What Splunk feature is most effective for managing the lifecycle of a detection?

A. Data model acceleration
B. Content management in Enterprise Security
C. Metrics indexing
D. Summary indexing

Answer: B

Explanation:

Why Use "Content Management in Enterprise Security" for Detection Lifecycle Management?
The detection lifecycle refers to the process of creating, managing, tuning, and deprecating security detections over time. In Splunk Enterprise Security (ES), Content Management helps security teams: Q Create, update, and retire correlation searches and security content
Q Manage use case coverage for different threat categories
Q Tune detection rules to reduce false positives
Q Track changes in detection rules for better governance
Example in Splunk ES:

Scenario: A company updates its threat detection strategy based on new attack techniques.

Q SOC analysts use Content Management in ES to:

Review existing correlation searches

Modify detection logic to adapt to new attack patterns

Archive outdated detections and enable new MITRE ATT&CK techniques

Why Not the Other Options?

X A. Data model acceleration – Improves search performance but does not manage detection lifecycles.

X C. Metrics indexing – Used for time-series data (e.g., system performance monitoring), not for managing detections.

X D. Summary indexing – Stores precomputed search results but does not control detection content.

Reference & Learning Resources

Splunk ES Content Management Documentation: https://docs.splunk.com/Documentation/ES

Best Practices for Security Content Management in Splunk ES: https://www.splunk.com/en_us/blog/security

MITRE ATT&CK Integration with Splunk: https://attack.mitre.org/resources

Question: 43

Which Splunk feature helps to standardize data for better search accuracy and detection logic?

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

Answer: B

Explanation:

Why Use "Data Models" for Standardized Search Accuracy and Detection Logic?

Splunk Data Models provide a structured, normalized representation of raw logs, improving:

Q Search consistency across different log sources

Q Detection logic by ensuring standardized field names

Q Faster and more efficient queries with data model acceleration

Example in Splunk Enterprise Security:

Scenario: A SOC team monitors login failures across multiple authentication systems.

Q Without Data Models: Different logs use src_ip, source_ip, or ip_address, making searches complex.

Q With Data Models: All fields map to a standard format, enabling consistent detection logic.

Why Not the Other Options?

X A. Field Extraction – Extracts fields from raw events but does not standardize field names across sources.

X C. Event Correlation – Detects relationships between logs but doesn't normalize data for search accuracy.

X D. Normalization Rules – A general term; Splunk uses CIM & Data Models for normalization.

Reference & 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-

Question: 44

A Splunk administrator is tasked with creating a weekly security report for executives.
What elements should they focus on?

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:

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

Example in Splunk:

Scenario: A CISO requests a weekly security report.
Q 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?

X B. Detailed logs of every notable event – Too technical; executives need summaries, not raw logs.
X C. Excluding compliance metrics to simplify reports – Compliance is critical for risk assessment.
X 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

Question: 45

When generating documentation for a security program, what key element should be included?

A. Vendor contract details
B. Organizational hierarchy chart
C. Standard operating procedures (SOPs)

D. Financial cost breakdown

Answer: C

Explanation:

Key Elements of Security Program Documentation

A security program's documentation ensures consistency, compliance, and efficiency in cybersecurity operations.

Q Why Include Standard Operating Procedures (SOPs)?

Defines step-by-step processes for security tasks.

Ensures security teams follow standardized workflows for handling incidents, vulnerabilities, and monitoring.

Supports compliance with regulations like NIST, ISO 27001, and CIS controls.

Example:

SOP for incident response outlines how analysts escalate security threats.

X Incorrect Answers:

A . Vendor contract details → Vendor agreements are important but not core to a security program's documentation.

B . Organizational hierarchy chart → Useful for internal structure but not essential for security documentation.

D . Financial cost breakdown → Related to budgeting, not security operations. Additional Resources:

NIST Security Documentation Framework

Splunk Security Operations Guide

Question: 46

What are critical elements of an effective incident report? (Choose three)

A. Timeline of events
B. Financial implications of the incident
C. Steps taken to resolve the issue
D. Names of all employees involved
E. Recommendations for future prevention

Answer: A, C, E

Explanation:

Critical Elements of an Effective Incident Report

An incident report documents security breaches, outlines response actions, and provides prevention strategies.

Q 1. Timeline of Events (A)

Provides a chronological sequence of the incident.

Helps analysts reconstruct attacks and understand attack vectors.

Example:

08:30 AM – Suspicious login detected.

08:45 AM – SOC investigation begins.

09:10 AM – Endpoint isolated.

Q 2. Steps Taken to Resolve the Issue (C)

Documents containment, eradication, and recovery efforts.

Ensures teams follow response procedures correctly.

Example:

Blocked malicious IPs, revoked compromised credentials, and restored affected systems.

Q 3. Recommendations for Future Prevention (E)

Suggests security improvements to prevent future attacks.

Example:

Enhance SIEM correlation rules, enforce multi-factor authentication, or update firewall rules.

X Incorrect Answers:

B . Financial implications of the incident → Important for executives, not crucial for an incident report.

D . Names of all employees involved → Avoids exposing individuals and focuses on security processes.

Additional Resources:

Splunk Incident Response Documentation

NIST Computer Security Incident Handling Guide

Question: 47

What is the primary function of summary indexing in Splunk reporting?

A. Storing unprocessed log data
B. Creating pre-aggregated data for faster reporting
C. Normalizing raw data for analysis
D. Enhancing the accuracy of alerts

Answer: B

Explanation:

Primary Function of Summary Indexing in Splunk Reporting

Summary indexing allows pre-aggregation of data to improve performance and speed up reports.

Q Why Use Summary Indexing?

Reduces processing time by storing computed results instead of raw data.

Helps SOC teams generate reports faster and optimize search performance.

Example:

Instead of searching millions of firewall logs in real-time, a summary index stores daily aggregated counts of blocked IPs.

X Incorrect Answers:

A . Storing unprocessed log data → Raw logs are stored in primary indexes, not summary indexes.

C . Normalizing raw data for analysis → Normalization is handled by CIM and data models.

D . Enhancing the accuracy of alerts → Summary indexing improves reporting performance, not alert accuracy.

Additional Resources:

Splunk Summary Indexing Guide

Optimizing SIEM Reports in Splunk

Question: 48

How can Splunk engineers monitor indexing performance effectively? (Choose two)

A. Use the Monitoring Console.
B. Create correlation searches on indexed data.
C. Enable detailed event logging for indexers.
D. Track indexer queue size and throughput.

Answer: A, D

Explanation:

Monitoring indexing performance in Splunk is crucial for ensuring efficient data ingestion, search performance, and resource utilization.

Methods to Monitor Indexing Performance Effectively:

Use the Monitoring Console (A)

Provides real-time visibility into indexing performance.

Displays resource utilization, indexing rate, queue health, and disk usage.

Track Indexer Queue Size and Throughput (D)

Monitoring queue sizes prevents indexing bottlenecks.

Ensures data is processed efficiently without delays.

Incorrect Answers:

X B. Create correlation searches on indexed data – Correlation searches focus on security events, not indexing performance.

X C. Enable detailed event logging for indexers – Increases log volume but does not directly help monitor indexing performance.

Reference:

Splunk Monitoring Console Overview

Best Practices for Monitoring Splunk Indexing Performance

Question: 49

What are benefits of aligning security processes with common methodologies like NIST or MITRE ATT&CK? (Choose two)

A. Enhancing organizational compliance
B. Accelerating data ingestion rates
C. Ensuring standardized threat responses
D. Improving incident response metrics

Answer: A, C

Explanation:

Aligning security processes with frameworks like NIST Cybersecurity Framework (CSF) or MITRE ATT&CK provides a structured approach to threat detection and response.

Benefits of Using Common Security Methodologies:

Enhancing Organizational Compliance (A)

Helps organizations meet regulatory requirements (e.g., NIST, ISO 27001, GDPR).

Ensures consistent security controls are implemented.

Ensuring Standardized Threat Responses (C)

MITRE ATT&CK provides a common language for adversary techniques.

Improves SOC workflows by aligning detection and response strategies.

Incorrect Answers:

X B. Accelerating data ingestion rates – Frameworks focus on security processes, not data ingestion speed.

X D. Improving incident response metrics – While methodologies help in structuring responses, the improvement of metrics is an indirect benefit.

Reference:

NIST Cybersecurity Framework

MITRE ATT&CK Overview

How Splunk Uses MITRE ATT&CK

Question: 50

A company wants to create a dashboard that displays normalized event data from various sources. What approach should they use?

A. Implement a data model using CIM.
B. Apply search-time field extractions.
C. Use SPL queries to manually extract fields.
D. Configure a summary index.

Answer: A

Explanation:

When organizations need to normalize event data from various sources, using Common Information Model (CIM) in Splunk is the best approach.

Why Use CIM for Normalized Event Data?

Standardizes Data Across Different Log Sources

CIM ensures consistent field names and formats across varied log types.

Makes searches, reports, and dashboards easier to manage.

Enables Faster and More Efficient Searches

Uses Data Models to accelerate search queries.

Reduces the need for custom field extractions.

Incorrect Answers:

X B. Apply search-time field extractions – This helps with raw data parsing but does not normalize data across sources.

X C. Use SPL queries to manually extract fields – This is a temporary fix and does not provide scalable normalization.

X D. Configure a summary index – Helps with performance but does not ensure event normalization.

Reference:

Splunk Common Information Model (CIM) Documentation

Best Practices for Implementing CIM

Question: 51

What methods improve the efficiency of Splunk's automation capabilities? (Choose three)

A. Using modular inputs
B. Optimizing correlation search queries
C. Leveraging saved search acceleration
D. Implementing low-latency indexing
E. Employing prebuilt SOAR playbooks

Answer: A, B, E

Explanation:

How to Improve Splunk's Automation Efficiency?

Splunk's automation capabilities rely on efficient data ingestion, optimized searches, and automated response workflows. The following methods help improve Splunk's automation:

1. Using Modular Inputs (Answer A)

Modular inputs allow Splunk to ingest third-party data efficiently (e.g., APIs, cloud services, or security tools).

Benefit: Improves automation by enabling real-time data collection for security workflows.

Example: Using a modular input to ingest threat intelligence feeds and trigger automatic responses.

2. Optimizing Correlation Search Queries (Answer B)

Well-optimized correlation searches reduce query time and false positives.

Benefit: Faster detections → Triggers automated actions in SOAR with minimal delay.

Example: Using tstats instead of raw searches for efficient event detection.

3. Employing Prebuilt SOAR Playbooks (Answer E)

SOAR playbooks automate security responses based on predefined workflows.

Benefit: Reduces manual effort in phishing response, malware containment, etc.

Example: Automating phishing email analysis using a SOAR playbook that extracts attachments, checks URLs, and blocks malicious senders.

Why Not the Other Options?

X C. Leveraging saved search acceleration – Helps with dashboard performance, but doesn't directly improve automation.

X D. Implementing low-latency indexing – Reduces indexing lag but is not a core automation feature.

Reference & Learning Resources

Splunk SOAR Automation Guide: https://docs.splunk.com/Documentation/SOAR

Optimizing Correlation Searches in Splunk ES: https://docs.splunk.com/Documentation/ES

Prebuilt SOAR Playbooks for Security Automation: https://splunkbase.splunk.com

Question: 52

A security team notices delays in responding to phishing emails due to manual investigation processes.

How can Splunk SOAR improve this workflow?

A. By prioritizing phishing cases manually

B. By automating email triage and analysis with playbooks

C. By assigning cases to analysts in real-time

D. By increasing the indexing frequency of email logs

Answer: B

Explanation:

How Splunk SOAR Improves Phishing Response?

Phishing attacks require fast detection and response. Manual investigation delays can be eliminated using Splunk SOAR automation.

Why Use Playbooks for Automated Email Triage? (Answer B)

Extracts email headers and attachments for analysis

Checks links & attachments against threat intelligence feeds

Automatically quarantines or deletes malicious emails

Q Escalates high-risk cases to SOC analysts

Example Playbook Workflow in Splunk SOAR:

Scenario: A suspicious email is reported.

Splunk SOAR playbook automatically:

Extracts sender details & checks against threat intelligence

Analyzes URLs & attachments using VirusTotal/Sandboxing

Tags the email as "Malicious" or "Safe"

Quarantines the email & alerts SOC analysts

Why Not the Other Options?

A. Prioritizing phishing cases manually – Still requires manual effort, leading to delays.

C. Assigning cases to analysts in real-time – Doesn't solve the issue of slow manual investigations.

D. Increasing the indexing frequency of email logs – Helps with log retrieval but doesn't automate phishing response.

Reference & Learning Resources

Splunk SOAR Phishing Playbook Guide: https://docs.splunk.com/Documentation/SOAR

Phishing Detection Automation in Splunk: https://splunkbase.splunk.com

Email Threat Intelligence with SOAR: https://www.splunk.com/en_us/blog/security

Question: 53

What are the essential components of risk-based detections in Splunk?

A. Risk modifiers, risk objects, and risk scores
B. Summary indexing, tags, and event types
C. Alerts, notifications, and priority levels
D. Source types, correlation searches, and asset groups

Answer: A

Explanation:

What Are Risk-Based Detections in Splunk?

Risk-based detections in Splunk Enterprise Security (ES) assign risk scores to security events based on threat severity and asset criticality.

Key Components of Risk-Based Detections:

1 Qisk Modifiers - Adjusts risk scores based on event type (e.g., failed logins, malware detections).
2 Qisk Objects - Entities associated with security events (e.g., users, IPs, devices).
3 Qisk Scores - Numerical values indicating the severity of a risk.

Example in Splunk Enterprise Security:

Scenario: A high-privilege account (Admin) fails multiple logins from an unusual location.

Splunk ES applies risk-based detection:

Failed logins add +10 risk points

Login from a suspicious country adds +15 points

Total risk score exceeds 25 → Triggers an alert

Why Not the Other Options?

B. Summary indexing, tags, and event types – Summary indexing stores precomputed data, but doesn't drive risk-based detection.

C. Alerts, notifications, and priority levels – Important, but risk-based detection is based on scoring, not just alerts.

D. Source types, correlation searches, and asset groups – Helps in data organization, but not specific to risk-based detections.

Reference & Learning Resources

Splunk ES Risk-Based Alerting Guide: https://docs.splunk.com/Documentation/ES

Risk-Based Detections & Scoring in Splunk: https://www.splunk.com/en_us/blog/security/risk-based-alerting.html

Best Practices for Risk Scoring in SOC Operations: https://splunkbase.splunk.com

Question: 54

A compliance audit reveals gaps in the tracking of privileged account activities. How can the team address this issue?

A. Automate report generation for privileged accounts
B. Use summary indexes to delete old data
C. Focus only on low-priority account activity
D. Exclude privileged accounts from reporting

Answer: A

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

Question: 55

A security team needs a dashboard to monitor incident resolution times across multiple regions.

Which feature should they prioritize?

A. Real-time filtering by region
B. Including all raw data logs for transparency
C. Using static panels for historical trends
D. Disabling drill-down for simplicity

Answer: A

Explanation:

A real-time incident dashboard helps SOC teams track resolution times by region, severity, and response efficiency.

Q 1. Real-time Filtering by Region (A)

Allows dynamic updates on incident trends across different locations.

Helps SOC teams identify regional attack patterns.

Example:

A dashboard with dropdown filters to switch between:

North America → Incident MTTR (Mean Time to Respond): 2 hours.

Europe → Incident MTTR: 5 hours.

X Incorrect Answers:

B . Including all raw data logs for transparency → Dashboards should show summarized insights, not raw logs.

C . Using static panels for historical trends → Static panels don't allow real-time updates.

D . Disabling drill-down for simplicity → Drill-down allows deeper investigation into regional trends.

Additional Resources:

Splunk Dashboard Design Best Practices

Question: 56

What is an essential step in building effective dashboards for program analytics?

A. Using predefined templates without modification
B. Applying accelerated data models for better performance
C. Avoiding the use of filters and tokens
D. Limiting the number of visualizations

Answer: B

Explanation:

Building Effective Dashboards for Program Analytics

Well-designed dashboards help SOC teams visualize security trends, performance metrics, and compliance adherence efficiently.

Q 1. Applying Accelerated Data Models for Better Performance (B)

Speeds up dashboard loading times by using pre-aggregated datasets.

Improves SIEM performance when analyzing large volumes of security logs.

Example:

Instead of running a full search, an accelerated data model pre-indexes event counts by severity level.

X Incorrect Answers:

A . Using predefined templates without modification → Dashboards should be customized for security needs.

C . Avoiding the use of filters and tokens → Filters improve usability by allowing analysts to refine searches.

D . Limiting the number of visualizations → Dashboards should balance performance and visibility rather than limit insights.

Additional Resources:

Splunk Accelerated Data Models

Building Fast and Efficient Dashboards

Question: 57

What methods can improve Splunk's indexing performance? (Choose two)

A. Enable indexer clustering.
B. Use universal forwarders for data ingestion.
C. Create multiple search heads.
D. Optimize event breaking rules.

Answer: A, D

Explanation:

Improving Splunk's indexing performance is crucial for handling large volumes of data efficiently while maintaining fast search speeds and optimized storage utilization.

Methods to Improve Indexing Performance:

Enable Indexer Clustering (A)

Distributes indexing load across multiple indexers.

Ensures high availability and fault tolerance by replicating indexed data.

Optimize Event Breaking Rules (D)

Defines clear event boundaries to reduce processing overhead.

Uses correct LINE_BREAKER and TRUNCATE settings to improve parsing speed.

Incorrect Answers:

X B. Use universal forwarders for data ingestion – Universal Forwarders reduce load on indexers but do not directly improve indexing performance.

X C. Create multiple search heads – Search heads optimize searches, not indexing performance. Reference:

Splunk Indexer Clustering Guide

Question: 58

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

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:

X A. Index-time field extraction – Happens during indexing and cannot be changed later.

X B. Event parsing – Splunk parses events before indexing, not at search time.

X D. Data modeling – Data models enhance searches but do not perform field extraction.

Reference:

Search-Time vs. Index-Time Extraction

Using rex and spath for Field Extraction

Question: 59

What is the primary purpose of developing security metrics in a Splunk environment?

A. To enhance data retention policies
B. To measure and evaluate the effectiveness of security programs
C. To identify low-priority alerts for suppression
D. To automate case management workflows

Answer: B

Explanation:

Security metrics help organizations assess their security posture and make data-driven decisions.

Primary Purpose of Security Metrics in Splunk:

Measure Security Effectiveness (B)

Tracks incident response times, threat detection rates, and alert accuracy.

Helps SOC teams and leadership evaluate security program performance.

Improve Threat Detection & Incident Response

Identifies gaps in detection logic and false positives.

Helps fine-tune correlation searches and notable events.

Incorrect Answers:

X A. To enhance data retention policies – Retention policies focus on data storage, not security performance.

X C. To identify low-priority alerts for suppression – While metrics help with prioritization, their primary goal is evaluating security effectiveness.

X D. To automate case management workflows – Security metrics inform automation but are not meant for workflow execution.

Reference:

Splunk Security Metrics Best Practices

How to Measure SOC Performance with Splunk

Question: 60

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

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)

Q Removes unnecessary or redundant correlation searches that may slow down performance.

Q Prevents false positives caused by outdated detection logic.

Q 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)

Q Regular updates ensure that new MITRE ATT&CK techniques and threat indicators are included.

Q 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?

X B. Scaling the Splunk deployment effectively – Lifecycle management improves detection accuracy, not infrastructure scalability.

X 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: 61

Which actions enhance the accuracy of Splunk dashboards? (Choose two)

A. Using accelerated data models
B. Avoiding token-based filters
C. Performing regular data validation
D. Disabling drill-down features

Answer: A, C

Explanation:

How to Improve Dashboard Accuracy in Splunk?

1. Using Accelerated Data Models (Answer A)

Q Increases search speed and ensures dashboards load faster.

Q Provides pre-processed structured data for real-time analysis.

Q Example: A SOC dashboard tracking failed logins uses an accelerated authentication data model for faster rendering.

2. Performing Regular Data Validation (Answer C)

Q Ensures that the indexed data is accurate and complete.

Q Prevents misleading dashboards caused by incomplete logs or incorrect field extractions.

Q Example: If a firewall log source stops sending data, regular validation detects missing logs before analysts rely on incorrect dashboards.

Why Not the Other Options?

X B. Avoiding token-based filters – Tokens improve dashboard flexibility; avoiding them reduces usability.

X D. Disabling drill-down features – Drill-downs enhance insights by allowing analysts to investigate details easily.

Reference & Learning Resources

Splunk Dashboard Performance Optimization:
https://docs.splunk.com/Documentation/Splunk/latest/Viz/Dashboards
Using Data Models for Fast and Accurate Dashboards: https://splunkbase.splunk.com
Regular Data Validation for SOC Dashboards: https://www.splunk.com/en_us/blog/security

Question: 62

What is the purpose of using data models in building dashboards?

A. To store raw data for compliance purposes
B. To provide a consistent structure for dashboard queries
C. To compress indexed data
D. To reduce storage usage on Splunk instances

Answer: B

Explanation:

Why Use Data Models in Dashboards?

Splunk Data Models allow dashboards to retrieve structured, normalized data quickly, improving search performance and accuracy.

How Data Models Help in Dashboards? (Answer B)

Q Standardized Field Naming – Ensures that queries always use consistent field names (e.g., src_ip instead of source_ip).

Q Faster Searches – Data models allow dashboards to run structured searches instead of raw log queries.

Q Example: A SOC dashboard for user activity monitoring uses a CIM-compliant Authentication Data Model, ensuring that queries work across different log sources.

Why Not the Other Options?

X A. To store raw data for compliance purposes – Raw data is stored in indexes, not data models.

X C. To compress indexed data – Data models structure data but do not perform compression.

X D. To reduce storage usage on Splunk instances – Data models help with search performance, not storage

reduction.

Reference & Learning Resources

Splunk Data Models for Dashboard Optimization:
https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutdatamodels
Building Efficient Dashboards Using Data Models: https://splunkbase.splunk.com
Using CIM-Compliant Data Models for Security Analytics: https://www.splunk.com/en_us/blog/tips- and-tricks

Question: 63

What methods can improve dashboard usability for security program analytics? (Choose three)

A. Using drill-down options for detailed views
B. Standardizing color coding for alerts
C. Limiting the number of panels on the dashboard
D. Adding context-sensitive filters
E. Avoiding performance optimization

Answer: A, B, D

Explanation:

Methods to Improve Dashboard Usability in Security Analytics
A well-designed Splunk security dashboard helps SOC teams quickly identify, analyze, and respond to security threats.
Q 1. Using Drill-Down Options for Detailed Views (A)
Allows analysts to click on high-level metrics and drill down into event details.
Helps teams pivot from summary statistics to specific security logs.
Example:
Clicking on a failed login trend chart reveals specific failed login attempts per user.
Q 2. Standardizing Color Coding for Alerts (B)
Consistent color usage enhances readability and priority identification.
Example:
Red → Critical incidents
Yellow → Medium-risk alerts
Green → Resolved issues
Q 3. Adding Context-Sensitive Filters (D)
Filters allow users to focus on specific security events without running new searches.
Example:
A dropdown filter for "Event Severity" lets analysts view only high-risk events.
X Incorrect Answers:
C . Limiting the number of panels on the dashboard → Dashboards should be optimized, not restricted.
E . Avoiding performance optimization → Performance tuning is essential for responsive dashboards. Additional Resources:
Splunk Dashboard Design Best Practices
Optimizing Security Dashboards in Splunk

Question: 64

What are essential practices for generating audit-ready reports in Splunk? (Choose three)

A. Including evidence of compliance with regulations
B. Excluding all technical metrics
C. Ensuring reports are time-stamped
D. Automating report scheduling
E. Using predefined report templates exclusively

Answer: A, C, D

Explanation:

Audit-ready reports help demonstrate compliance with security policies and regulations (e.g., PCI DSS, HIPAA, ISO 27001, NIST).

Q 1. Including Evidence of Compliance with Regulations (A)

Reports must show security controls, access logs, and incident response actions.

Example:

A PCI DSS compliance report tracks privileged user access logs and unauthorized access attempts.

Q 2. Ensuring Reports Are Time-Stamped (C)

Provides chronological accuracy for security incidents and log reviews.

Example:

Incident response logs should include detection, containment, and remediation timestamps.

Q 3. Automating Report Scheduling (D)

Enables automatic generation and distribution of reports to stakeholders.

Example:

A weekly audit report on security logs is auto-emailed to compliance officers.

X Incorrect Answers:

B . Excluding all technical metrics → Security reports must include event logs, IP details, and correlation results.

E . Using predefined report templates exclusively → Reports should be customized for compliance needs.

Additional Resources:

Splunk Compliance Reporting Guide

Automating Security Reports in Splunk

Question: 65

A security engineer is tasked with improving threat intelligence sharing within the company. What is the most effective first step?

A. Implement a real-time threat feed integration.
B. Restrict access to external threat intelligence sources.
C. Share raw threat data with all employees.
D. Use threat intelligence only for executive reporting.

Answer: A

Explanation:

Improving Threat Intelligence Sharing in an Organization

Threat intelligence enhances cybersecurity by providing real-time insights into emerging threats.

Q 1. Implement a Real-Time Threat Feed Integration (A)

Enables real-time ingestion of threat indicators (IOCs, IPs, hashes, domains).

Helps automate threat detection and blocking.

Example:

Integrating STIX/TAXII, Splunk Threat Intelligence Framework, or a SOAR platform for live threat updates.

X Incorrect Answers:

B . Restrict access to external threat intelligence sources → Sharing intelligence enhances security, not restricting it.

C . Share raw threat data with all employees → Raw intelligence needs analysis and context before distribution.

D . Use threat intelligence only for executive reporting → SOC analysts, incident responders, and IT teams need actionable intelligence.

Additional Resources:

Splunk Threat Intelligence Framework

How to Integrate STIX/TAXII in Splunk

Question: 66

During a high-priority incident, a user queries an index but sees incomplete results.

What is the most likely issue?

A. Buckets in the warm state are inaccessible.
B. Data normalization was not applied.
C. Indexers have reached their queue capacity.
D. The search head configuration is outdated.

Answer: C

Explanation:

If a user queries an index during a high-priority incident but sees incomplete results, it is likely that the indexers are overloaded, causing queue bottlenecks.

Why Indexer Queue Capacity Issues Cause Incomplete Results:

When indexing queues fill up, incoming data cannot be processed efficiently.

Search results may be incomplete or delayed if events are still in the indexing queue and not fully written to disk.

Heavy search loads during incidents can also increase pressure on indexers.

How to Fix It:

Monitor indexing queues via the Monitoring Console (indexing>indexing performance).

Check metrics.log on indexers for max_queue_size_exceeded warnings.

Increase indexer capacity or optimize search scheduling to reduce load.

Incorrect Answers:

X A. Buckets in the warm state are inaccessible – Warm buckets are still searchable unless there is a storage failure.

X B. Data normalization was not applied – Normalization affects data consistency but does not cause incomplete results.

X D. The search head configuration is outdated – This does not affect indexing, only the execution of searches.

Question: 67

What is the main benefit of automating case management workflows in Splunk?

A. Eliminating the need for manual alerts

B. Enabling dynamic storage allocation
C. Reducing response times and improving analyst productivity
D. Minimizing the use of correlation searches

Answer: C

Explanation:

Automating case management workflows in Splunk streamlines incident response and reduces manual overhead, allowing analysts to focus on higher-value tasks.
Main Benefits of Automating Case Management:
Reduces Response Times (C)
Automatically assigns cases to analysts based on predefined rules.
Triggers playbooks and workflows in Splunk SOAR to handle common incidents.
Improves Analyst Productivity (C)
Reduces time spent on manual case creation and updates.
Provides integrated case tracking across Splunk and ITSM tools (e.g., ServiceNow, Jira). Incorrect Answers:
X A. Eliminating the need for manual alerts – Alerts still require analyst verification and triage.
X B. Enabling dynamic storage allocation – Case management does not impact Splunk storage.
X D. Minimizing the use of correlation searches – Correlation searches remain essential for detection, even with automation.
Reference:
Splunk Case Management Best Practices
Automating Incident Response with Splunk SOAR

Question: 68

An engineer observes a delay in data being indexed from a remote location. The universal forwarder is configured correctly.
What should they check next?

A. Review forwarder logs for queue blockages.
B. Increase the indexer memory allocation.
C. Optimize search head clustering.
D. Reconfigure the props.conf file.

Answer: A

Explanation:

If there is a delay in data being indexed from a remote location, even though the Universal Forwarder (UF) is correctly configured, the issue is likely a queue blockage or network latency.
Steps to Diagnose and Fix Forwarder Delays:
Check Forwarder Logs (splunkd.log) for Queue Issues (A)
Look for messages like TcpOutAutoLoadBalanced or Queue is full.
If queues are full, events are stuck at the forwarder and not reaching the indexer.
Monitor Forwarder Health Using metrics.log
Use index=_internal source=*metrics.log* group=queue to check queue performance.
Incorrect Answers:
X B. Increase the indexer memory allocation – Memory allocation does not resolve forwarder delays.

X C. Optimize search head clustering – Search heads manage search performance, not forwarder ingestion.

X D. Reconfigure the props.conf file – props.conf affects event processing, not ingestion speed. Reference: Splunk Forwarder Troubleshooting Guide

Monitoring Forwarder Queue Performance

Question: 69

Which Splunk feature helps in tracking and documenting threat trends over time?

A. Event sampling
B. Risk-based dashboards
C. Summary indexing
D. Data model acceleration

Answer: B

Explanation:

Why Use Risk-Based Dashboards for Tracking Threat Trends?

Risk-based dashboards in Splunk Enterprise Security (ES) provide a structured way to track threats over time.

How Risk-Based Dashboards Help:

Q Aggregate security events into risk scores → Helps prioritize high-risk activities.

Q Show historical trends of threat activity.

Q Correlate multiple risk factors across different security events.

Example in Splunk ES:

Scenario: A SOC team tracks insider threat activity over 6 months.

Q The Risk-Based Dashboard shows:

Users with rising risk scores over time.

Patterns of malicious behavior (e.g., repeated failed logins + data exfiltration).

Correlation between different security alerts (e.g., phishing clicks → malware execution).

Why Not the Other Options?

X A. Event sampling – Helps with performance optimization, not threat trend tracking.

X C. Summary indexing – Stores precomputed data but is not designed for tracking risk trends.

X D. Data model acceleration – Improves search speed, but doesn't track security trends.

Reference & Learning Resources

Splunk ES Risk-Based Alerting Guide: https://docs.splunk.com/Documentation/ES

Tracking Security Trends Using Risk-Based Dashboards: https://splunkbase.splunk.com

How to Build Risk-Based Analytics in Splunk: https://www.splunk.com/en_us/blog/security

Question: 70

An engineer observes a high volume of false positives generated by a correlation search.
What steps should they take to reduce noise without missing critical detections?

A. Increase the frequency of the correlation search.
B. Add suppression rules and refine thresholds.
C. Disable the correlation search temporarily.
D. Limit the search to a single index.

Answer: B

Explanation:

How to Reduce False Positives in Correlation Searches?

High false positives can overwhelm SOC teams, causing alert fatigue and missed real threats. The best solution is to fine-tune suppression rules and refine thresholds.

How Suppression Rules & Threshold Tuning Help:

Q Suppression Rules: Prevent repeated false positives from low-risk recurring events (e.g., normal system scans).

Q Threshold Refinement: Adjust sensitivity to focus on true threats (e.g., changing a login failure alert from 3 to 10 failed attempts).

Example in Splunk ES:

Scenario: A correlation search generates too many alerts for failed logins.

Q Fix: SOC analysts refine detection thresholds:

Suppress alerts if failed logins occur within a short timeframe but are followed by a successful login.

Only trigger an alert if failed logins exceed 10 attempts within 5 minutes.

Why Not the Other Options?

X A. Increase the frequency of the correlation search – Increases search load without reducing false positives.

X C. Disable the correlation search temporarily – Leads to blind spots in detection.

X D. Limit the search to a single index – May exclude critical security logs from detection.

Reference & Learning Resources

Splunk ES Correlation Search Optimization Guide: https://docs.splunk.com/Documentation/ES

Reducing False Positives in SOC Workflows: https://splunkbase.splunk.com

Fine-Tuning Security Alerts in Splunk: https://www.splunk.com/en_us/blog/security

Question: 71

What are key elements of a well-constructed notable event? (Choose three)

A. Meaningful descriptions
B. Minimal use of contextual data
C. Proper categorization
D. Relevant field extractions

Answer: ACD

Explanation:

A notable event in Splunk Enterprise Security (ES) represents a significant security detection that requires investigation.

Key Elements of a Good Notable Event:

Q Meaningful Descriptions (Answer A)

Helps analysts understand the event at a glance.

Example: Instead of "Possible attack detected," use "Multiple failed admin logins from foreign IP address".

Q Proper Categorization (Answer C)

Ensures events are classified correctly (e.g., Brute Force, Insider Threat, Malware Activity).

Example: A malicious file download alert should be categorized as "Malware Infection", not just "General Alert".

Q Relevant Field Extractions (Answer D)
Ensures that critical details (IP, user, timestamp) are present for SOC analysis.
Example: If an alert reports failed logins, extracted fields should include username, source IP, and login method.

Why Not the Other Options?
X B. Minimal use of contextual data – More context helps SOC analysts investigate faster.

Reference & Learning Resources
Building Effective Notable Events in Splunk ES: https://docs.splunk.com/Documentation/ES
SOC Best Practices for Security Alerts: https://splunkbase.splunk.com
How to Categorize Security Alerts Properly: https://www.splunk.com/en_us/blog/security

Question: 72

During an incident, a correlation search generates several notable events related to failed logins. The engineer notices the events are from test accounts.
What should be done to address this?

A. Disable the correlation search for test accounts.
B. Apply filtering to exclude test accounts from the search results.
C. Lower the search threshold for failed logins.
D. Suppress all notable events temporarily.

Answer: B

Explanation:

When a correlation search in Splunk Enterprise Security (ES) generates excessive notable events due to test accounts, the best approach is to filter out test accounts while keeping legitimate detections active.
Q 1. Apply Filtering to Exclude Test Accounts (B)
Modifies the correlation search to exclude known test accounts.
Reduces false positives while keeping real threats visible.
Example:
Update the search to exclude test accounts:
index=auth_logs NOT user IN ("test_user1", "test_user2")
X Incorrect Answers:
A . Disable the correlation search for test accounts → This removes visibility into all failed logins, including those that may indicate real threats.
C . Lower the search threshold for failed logins → Would increase false positives, making it harder for SOC teams to focus on real attacks.
D . Suppress all notable events temporarily → Suppression hides all alerts, potentially missing real security incidents.
Additional Resources:
Splunk ES: Managing Correlation Searches
Reducing False Positives in SIEM

Question: 73

Which actions help to monitor and troubleshoot indexing issues? (Choose three)

A. Use btool to check configurations.
B. Monitor queues in the Monitoring Console.
C. Review internal logs such as splunkd.log.
D. Enable distributed search in Splunk Web.

Answer: A, B, C

Explanation:

Indexing issues can cause search performance problems, data loss, and delays in security event processing.

Q 1. Use btool to Check Configurations (A)

Helps validate Splunk configurations related to indexing.

Example:

Check indexes.conf settings:

splunk btool indexes list --debug

Q 2. Monitor Queues in the Monitoring Console (B)

Identifies indexing bottlenecks such as blocked queues, dropped events, or indexing lag.

Example:

Navigate to: Settings → Monitoring Console → Indexing Performance.

Q 3. Review Internal Logs Such as splunkd.log (C)

The splunkd.log file contains indexing errors, disk failures, and queue overflows.

Example:

Use Splunk to search internal logs:

X Incorrect Answer:

D . Enable distributed search in Splunk Web → Distributed search improves scalability, but does not troubleshoot indexing problems.

Additional Resources:

Splunk Indexing Performance Guide

Using btool for Debugging

Question: 74

An organization uses MITRE ATT&CK to enhance its threat detection capabilities. How should this methodology be incorporated?

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.

Q 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.

X 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: 75

What is the primary purpose of Splunk SOAR (Security Orchestration, Automation, and Response)?

A. To accelerate data ingestion
B. To automate and orchestrate security workflows
C. To improve indexing performance
D. To provide threat intelligence feeds

Answer: B

Explanation:

Splunk SOAR (Security Orchestration, Automation, and Response) helps SOC teams automate threat detection, investigation, and response by integrating security tools and orchestrating workflows. Primary Purpose of Splunk SOAR:

Automates Security Tasks (B)

Reduces manual efforts by using playbooks to handle routine incidents automatically.

Accelerates threat mitigation by automating response actions (e.g., blocking malicious IPs, isolating endpoints).

Orchestrates Security Workflows (B)

Connects SIEM, threat intelligence, firewalls, endpoint security, and ITSM tools into a unified security workflow.

Ensures faster and more effective threat response across multiple security tools.

Incorrect Answers:

X A. To accelerate data ingestion – Splunk SOAR focuses on incident response automation, not data ingestion.

X C. To improve indexing performance – Indexing is managed by Splunk Enterprise, not Splunk SOAR.

X D. To provide threat intelligence feeds – While SOAR can use threat intelligence, it does not provide them.

Reference:

Splunk SOAR Overview

Automating Incident Response with Splunk SOAR

Question: 76

What key elements should an audit report include? (Choose two)

A. Analysis of past incidents
B. List of unprocessed log data
C. Compliance metrics
D. Asset inventory details

Answer: A, C

Explanation:

An audit report provides an overview of security operations, compliance adherence, and past incidents, helping organizations ensure regulatory compliance and improve security posture. Key Elements of an Audit Report:
Analysis of Past Incidents (A)
Includes details on security breaches, alerts, and investigations.
Helps identify recurring threats and security gaps.
Compliance Metrics (C)
Evaluates adherence to regulatory frameworks (e.g., NIST, ISO 27001, PCI-DSS, GDPR).
Measures risk scores, policy violations, and control effectiveness.
Incorrect Answers:
X B. List of unprocessed log data – Unprocessed logs do not contribute to security insights in an audit report.
X D. Asset inventory details – While asset tracking is important, audit reports focus on security and compliance data.
Reference:
Security Audit Reports Best Practices
Splunk Compliance and Audit Frameworks

Question: 77

What are key benefits of using summary indexing in Splunk? (Choose two)

A. Reduces storage space required for raw data
B. Improves search performance on aggregated data
C. Provides automatic field extraction during indexing
D. Increases data retention period

Answer: B D

Explanation:

Summary indexing in Splunk improves search efficiency by storing pre-aggregated data, reducing the need to process large datasets repeatedly.
Key Benefits of Summary Indexing:
Improves Search Performance on Aggregated Data (B)
Reduces query execution time by storing pre-calculated results.
Helps SOC teams analyze trends without running resource-intensive searches.
Increases Data Retention Period (D)
Raw logs may have short retention periods, but summary indexes can store key insights for longer.
Useful for historical trend analysis and compliance reporting.
Incorrect Answers:
X A. Reduces storage space required for raw data – Summary indexing creates additional storage, rather than

reducing raw data size.

X C. Provides automatic field extraction during indexing – Field extraction is not automatic in summary indexing; it depends on how data is processed.

Reference:

Splunk Summary Indexing Best Practices

Improving Search Performance with Summary Indexing

Question: 78

Which practices improve the effectiveness of security reporting? (Choose three)

A. Automating report generation
B. Customizing reports for different audiences
C. Including unrelated historical data for context
D. Providing actionable recommendations
E. Using dynamic filters for better analysis

Answer: A, B, D

Explanation:

Effective security reporting helps SOC teams, executives, and compliance officers make informed decisions.

Q 1. Automating Report Generation (A)

Saves time by scheduling reports for regular distribution.

Reduces manual effort and ensures timely insights.

Example:

A weekly phishing attack report sent to SOC analysts.

Q 2. Customizing Reports for Different Audiences (B)

Technical reports for SOC teams include detailed event logs.

Executive summaries provide risk assessments and trends.

Example:

SOC analysts see incident logs, while executives get a risk summary.

Q 3. Providing Actionable Recommendations (D)

Reports should not just show data but suggest actions.

Example:

If failed login attempts increase, recommend MFA enforcement.

X Incorrect Answers:

C . Including unrelated historical data for context → Reports should be concise and relevant.

E . Using dynamic filters for better analysis → Useful in dashboards, but not a primary factor in reporting effectiveness.

Additional Resources:

Splunk Security Reporting Guide

Best Practices for Security Metrics

Question: 79

A security analyst needs to update the SOP for handling phishing incidents. What should they prioritize?

A. Ensuring all reports are manually verified by analysts
B. Automating the isolation of suspected phishing emails
C. Documenting steps for user awareness training
D. Reporting incidents to the executive board immediately

Answer: C

Explanation:

Updating the SOP for Handling Phishing Incidents
A Standard Operating Procedure (SOP) should focus on prevention, detection, and response.
Q 1. Documenting Steps for User Awareness Training (C)
Training employees helps prevent phishing incidents.
Example:
Teach users to identify phishing emails and report them via a Splunk SOAR playbook.
X Incorrect Answers:
A . Ensuring all reports are manually verified by analysts → Automation (via SOAR) should be used for initial triage.
B . Automating the isolation of suspected phishing emails → Automation is useful, but user education prevents incidents.
D . Reporting incidents to the executive board immediately → Only major security breaches should be escalated to executives.
Additional Resources:
NIST Incident Response Guide
Splunk Phishing Detection Playbooks

Question: 80

What are key benefits of automating responses using SOAR? (Choose three)

A. Faster incident resolution
B. Reducing false positives
C. Scaling manual efforts
D. Consistent task execution
E. Eliminating all human intervention

Answer: A, C, D

Explanation:

Splunk SOAR (Security Orchestration, Automation, and Response) improves security operations by automating routine tasks.
Q 1. Faster Incident Resolution (A)
SOAR playbooks reduce response time from hours to minutes.
Example:
A malicious IP is automatically blocked in the firewall after detection.
Q 2. Scaling Manual Efforts (C)
Automation allows security teams to handle more incidents without increasing headcount.
Example:

Instead of manually reviewing phishing emails, SOAR triages them automatically.

Q 3. Consistent Task Execution (D)

Ensures standardized responses to security incidents.

Example:

Every malware alert follows the same containment process.

X Incorrect Answers:

B . Reducing false positives → SOAR automates response but does not inherently reduce false positives (SIEM tuning does).

E . Eliminating all human intervention → Human analysts are still needed for decision-making. Additional Resources:

Splunk SOAR Automation Guide

Best Practices for SOAR Implementation

Question: 81

What is the role of aggregation policies in correlation searches?

A. To group related notable events for analysis
B. To index events from multiple sources
C. To normalize event fields for dashboards
D. To automate responses to critical events

Answer: A

Explanation:

Aggregation policies in Splunk Enterprise Security (ES) are used to group related notable events, reducing alert fatigue and improving incident analysis.

Role of Aggregation Policies in Correlation Searches:

Group Related Notable Events (A)

Helps SOC analysts see a single consolidated event instead of multiple isolated alerts.

Uses common attributes like user, asset, or attack type to aggregate events.

Improves Incident Response Efficiency

Reduces the number of duplicate alerts, helping analysts focus on high-priority threats.

Incorrect Answers:

X B. To index events from multiple sources – Correlation searches analyze indexed data but do not control indexing.

X C. To normalize event fields for dashboards – Field normalization is handled by Splunk CIM (Common Information Model).

X D. To automate responses to critical events – While SOAR automates response actions, aggregation focuses on event grouping.

Reference:

Splunk ES Aggregation Policies Documentation

Best Practices for Correlation Searches

Question: 82

What are essential steps in developing threat intelligence for a security program? (Choose three)

A. Collecting data from trusted sources

B. Conducting regular penetration tests
C. Analyzing and correlating threat data
D. Creating dashboards for executives
E. Operationalizing intelligence through workflows

Answer: A, C, E

Explanation:

Threat intelligence in Splunk Enterprise Security (ES) enhances SOC capabilities by identifying known attack patterns, suspicious activity, and malicious indicators.

Essential Steps in Developing Threat Intelligence:

Collecting Data from Trusted Sources (A)

Gather data from threat intelligence feeds (e.g., STIX, TAXII, OpenCTI, VirusTotal, AbuseIPDB).

Include internal logs, honeypots, and third-party security vendors.

Analyzing and Correlating Threat Data (C)

Use correlation searches to match known threat indicators against live data.

Identify patterns in network traffic, logs, and endpoint activity.

Operationalizing Intelligence Through Workflows (E)

Automate responses using Splunk SOAR (Security Orchestration, Automation, and Response).

Enhance alert prioritization by integrating intelligence into risk-based alerting (RBA).

Incorrect Answers:

X B. Conducting regular penetration tests – Important for security, but not a core part of threat intelligence development.

X D. Creating dashboards for executives – Helps in reporting but does not develop threat intelligence.

Reference:

Splunk Threat Intelligence Framework

How to Use Threat Intelligence in Splunk

Question: 83

What does Splunk's term "bucket" refer to in data indexing?

A. A storage unit for archived data
B. A collection of events with a specific retention policy
C. A directory containing indexed data
D. A database table for search results

Answer: C

Explanation: