Number: SPLK-5002
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: SPLK-5002

Exam Name: Splunk Certified Cybersecurity Defense Engineer

Exam A

QUESTION 1
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

Correct Answer: B, D
Section:
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?
A. Indexing data with detailed metadata -- Adding too much metadata increases indexing overhead and slows down performance. 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 2
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

Correct Answer: B
Section:
Explanation:
Why Use Real-Time Notable Event Dashboards for Phishing Detection?
Phishing campaigns require real-time monitoring to detect threats as they emerge and respond quickly.
Why 'Real-Time Notable Event Dashboards' is the Best Choice? (Answer B) Shows live security alerts for phishing detections. Enables SOC analysts to take immediate action (e.g., blocking malicious domains, disabling compromised accounts). Uses correlation searches in Splunk Enterprise Security (ES) to detect phishing indicators.
Example in Splunk: Scenario: A company runs a phishing awareness campaign. Real-time dashboards track:
How many employees clicked on phishing links.
How many users reported phishing emails.

Any suspicious activity (e.g., account takeovers).
Why Not the Other Options?
A. Weekly incident trend reports -- Helpful for analysis but not fast enough for phishing detection. C. Risk score-based summary reports -- Risk scores are useful but not designed for real-time phishing detection. D. SLA compliance reports -- SLA reports measure performance but don't help actively detect phishing attacks.
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 3
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

Correct Answer: D
Section:
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) Prevents event misalignment -- Ensures logs appear in the correct order. Enables accurate correlation searches -- Helps SOC analysts trace attack timelines. 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. Without correct timestamps, login failures might appear out of order, making analysis difficult. With proper event timestamping, logs line up correctly, allowing SOC analysts to detect the exact attack timeline.
Why Not the Other Options?
A. Assigning data to a specific sourcetype -- Sourcetypes classify logs but don't affect timestamps. B. Tagging events for correlation searches -- Correlation uses timestamps but timestamping itself isn't about tagging. 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 4
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

Correct Answer: A
Section:
Explanation:
Why Configure Asset & Identity Information for Privileged Accounts First?
Risk-based detection focuses on identifying and prioritizing threats based on the severity of their impact. For privileged accounts (admins, domain controllers, finance users), understanding who they are, what they access, and how they behave is critical.
Key Steps for Risk-Based Detection in Splunk ES: 1 Define Privileged Accounts & Groups -- Identify high-risk users (Admin, HR, Finance, CISO). 2 Assign Risk Scores -- Apply higher scores to actions involving privileged users. 3 Enable Identity & Asset Correlation -- Link users to assets for better detection. 4 Monitor for Anomalies -- Detect abnormal login patterns, excessive file access, or unusual privilege escalation.

Example in Splunk ES:
A domain admin logs in from an unusual location Trigger high-risk alert
A finance director downloads sensitive payroll data at midnight Escalate for investigation
Why Not the Other Options?
B. Correlation searches with low thresholds -- May generate excessive false positives, overwhelming the SOC. C. Event sampling for raw data -- Doesn't provide context for risk-based detection. D. Automated dashboards for all accounts -- Useful for visibility, but not the first step for risk-based security.
Reference & Learning Resources
Splunk ES Risk-Based Alerting (RBA): https://www.splunk.com/en_us/blog/security/risk-based-alerting.html Privileged Account Monitoring in Splunk: https://docs.splunk.com/Documentation/ES/latest/User/RiskBasedAlerting Implementing Privileged Access Security (PAM) with Splunk: https://splunkbase.splunk.com

QUESTION 5
What is the primary purpose of data indexing in Splunk?

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

Correct Answer: B
Section:
Explanation:
Understanding Data Indexing in Splunk
In Splunk Enterprise Security (ES) and Splunk SOAR, data indexing is a fundamental process that enables efficient storage, retrieval, and searching of data.
Why is Data Indexing Important?
Stores raw machine data (logs, events, metrics) in a structured manner.
Enables fast searching through optimized data storage techniques.
Uses an indexer to process, compress, and store data efficiently.
Why the Correct Answer is B?
Splunk indexes data to store it efficiently while ensuring fast retrieval for searches, correlation searches, and analytics.
It assigns metadata to indexed events, allowing SOC analysts to quickly filter and search logs.
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 6
Which features are crucial for validating integrations in Splunk SOAR? (Choose three)

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

Correct Answer: A, C, D

Section:
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 Testing API Connectivity (A)
Ensures Splunk SOAR can communicate with external security tools (firewalls, EDR, SIEM, etc.).
Uses API testing tools like Postman or Splunk SOAR's built-in Test Connectivity feature.
2 Verifying Authentication Methods (C)
Confirms that integrations use the correct authentication type (OAuth, API Key, Username/Password, etc.).
Prevents failed automations due to expired or incorrect credentials.
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 7
How can you incorporate additional context into notable events generated by correlation searches?

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

Correct Answer: A
Section:
Explanation:
In Splunk Enterprise Security (ES), notable events are generated by correlation searches, which are predefined searches designed to detect security incidents by analyzing logs and alerts from multiple data sources. Adding additional context to these notable events enhances their value for analysts and improves the efficiency of incident response.
To incorporate additional context, you can:
Use lookup tables to enrich data with information such as asset details, threat intelligence, and user identity.
Leverage KV Store or external enrichment sources like CMDB (Configuration Management Database) and identity management solutions.
Apply Splunk macros or eval commands to transform and enhance event data dynamically.
Use Adaptive Response Actions in Splunk ES to pull additional information into a notable event.
The correct answer is A. By adding enriched fields during search execution, because enrichment occurs dynamically during search execution, ensuring that additional fields (such as geolocation, asset owner, and risk score) are included in the notable event.
Splunk ES Documentation on Notable Event Enrichment
Correlation Search Best Practices
Using Lookups for Data Enrichment

QUESTION 8
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

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

QUESTION 9
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.

Correct Answer: C
Section:
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. Without CIM: Each log source uses a different field name for failed logins, requiring multiple search queries. 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?
A. Create field extraction rules at search time -- Helps with parsing data but doesn't standardize field names across sources. B. Use data model acceleration for real-time searches -- Accelerates searches but doesn't fix inconsistent field naming. 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 10
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

Correct Answer: C
Section:
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:
Parsed, transformed, and stored efficiently before indexing. Normalized before indexing, so the SOC team doesn't need to clean up fields later. 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. 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 11
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

Correct Answer: B, C
Section:
Explanation:
Effective documentation ensures that security teams can standardize response procedures, reduce incident response time, and improve compliance.
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.
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).
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 12
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

Correct Answer: A
Section:
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.
Managing Notable Events in Splunk ES
Best Practices for Tuning Correlation Searches
Using Suppression in Splunk ES

QUESTION 13
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

Correct Answer: A, C
Section:
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: B. Increasing the indexing frequency -- This improves data availability but does not directly optimize case management. D. Reducing the number of search heads -- This might degrade search performance rather than optimize case handling.
Splunk ES Case Management
Integrating Splunk with ServiceNow
Automating Ticket Creation in Splunk

QUESTION 14
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

Correct Answer: A, C
Section:
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: B. DELETE for archiving historical data -- DELETE is rarely used in Splunk as it does not archive data; instead, retention policies handle old data. D. PUT for updating index configurations -- While PUT can modify configurations, it is not a core automation function in SOC workflows.
Splunk REST API Documentation
Using Splunk API for Automation
Best Practices for Automating Security Workflows

QUESTION 15
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

Correct Answer: B
Section:
Explanation:
Splunk SOAR (Security Orchestration, Automation, and Response) playbooks help SOC teams automate, orchestrate, and respond to threats faster.
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.
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 16
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

Correct Answer: A, B, E
Section:
Explanation:
Key Elements of Meaningful Security Metrics
Security metrics should align with business goals, be validated regularly, and have standardized definitions to ensure reliability.
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.
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.
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).
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 17
Which REST API method is used to retrieve data from a Splunk index?

A. POST
B. GET
C. PUT
D. DELETE

Correct Answer: B
Section:
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: A. POST -- Used for submitting new search jobs or sending data to Splunk. C. PUT -- Used for modifying existing Splunk configurations, not retrieving data. D. DELETE -- Used to remove Splunk objects like reports or alerts, not for retrieval.
Splunk REST API - GET Method
How to Use Splunk API for Search Queries

QUESTION 18
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

Correct Answer: B
Section:
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: A. Automating detection workflows -- Lean Six Sigma focuses on process improvement, not automation. C. Monitoring the performance of detection searches -- While Lean Six Sigma enhances efficiency, it does not specifically monitor search performance. D. Enhancing user activity logs -- This is related to logging and auditing, not Lean Six Sigma.
Lean Six Sigma in Cybersecurity
Using Six Sigma to Improve SOC Processes

QUESTION 19
What Splunk process ensures that duplicate data is not indexed?

A. Data deduplication

B. Metadata tagging
C. Indexer clustering
D. Event parsing

Correct Answer: D
Section:
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: A. Data deduplication -- While deduplication removes duplicates in searches, it does not prevent duplicate indexing. B. Metadata tagging -- Tags help with categorization but do not control duplication. C. Indexer clustering -- Clustering improves redundancy and availability but does not prevent duplicates.
Splunk Data Parsing Process
Splunk Indexing and Data Handling

QUESTION 20
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.

Correct Answer: B
Section:
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. 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.
Optimized using tstats:
| tstats count where index=security sourcetype=auth_logs action=failed by user
Advantage: Faster results without scanning raw events.
Why Not the Other Options?
A. Increase search head memory allocation -- May help, but inefficient queries will still slow down searches. C. Configure a search head cluster -- A single search head isn't necessarily the problem; improving search performance is more effective. D. Implement accelerated data models -- Useful for prebuilt dashboards, but won't improve ad-hoc searches.

QUESTION 21
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.

Correct Answer: A
Section:
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
This forces all logs from /var/log/auth.log to be assigned sourcetype=auth_logs.
Why Not the Other Options?
B. Define the sourcetype in the search head -- Sourcetypes are assigned at ingestion time, not at search time. C. Configure the sourcetype in the deployment server -- The deployment server manages configurations, but props.conf is what actually assigns sourcetypes. 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 22
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

Correct Answer: B
Section:
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: Early Threat Detection -- Identifies known attack patterns (IP addresses, domains, hashes). Proactive Defense -- Blocks threats before they impact systems. Better Incident Response -- Speeds up triage and forensic analysis. 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). Splunk Enterprise Security (ES) correlates security events with known malicious IPs or domains. 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?
A. To automate response workflows -- While automation is beneficial, threat intelligence is primarily for proactive identification. C. To generate incident reports for stakeholders -- Reports are a byproduct, but not the main goal of threat intelligence. 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 23
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

Correct Answer: A, B
Section:
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.
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.
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.
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 24
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

Correct Answer: A, C, D
Section:
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: B. Using predefined alert templates -- Static templates don't dynamically prioritize risk. E. Enforcing strict search head resource limits -- This impacts system performance but does not directly improve detection prioritization.
Splunk Risk-Based Alerting (RBA) Documentation
Best Practices for Prioritizing Security Alerts
Using Machine Learning for Threat Detection

QUESTION 25
What are the main steps of the Splunk data pipeline? (Choose three)

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

Correct Answer: A, C, D
Section:
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: B. Visualization -- Happens later in dashboards, but not part of the data pipeline itself. E. Alerting -- Occurs after the data pipeline processes and analyzes events.
Splunk Data Processing Pipeline Overview
How Splunk Parses and Indexes Data

QUESTION 26
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

Correct Answer: A, D
Section:
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: B. Limiting the number of correlation searches -- Reducing correlation searches may lead to missed threats. C. Using summary indexing for raw events -- Summary indexing improves performance but does not enhance risk-based detection.
Splunk Risk-Based Alerting Guide
Threat Intelligence in Splunk ES

QUESTION 27
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

Correct Answer: B
Section:
Explanation:
Understanding Risk-Based Prioritization
Risk-based prioritization is a methodology that evaluates both the likelihood and impact of risks to determine which threats require immediate action.
Why Risk-Based Prioritization?
Focuses on high-impact and high-likelihood risks first.
Helps SOC teams manage alerts effectively and avoid alert fatigue.
Used in SIEM solutions (Splunk ES) and Risk-Based Alerting (RBA).
Example in Splunk Enterprise Security (ES):
A failed login attempt from an internal employee might be low risk (low impact, low likelihood).
Multiple failed logins from a foreign country with a known bad reputation could be high risk (high impact, high likelihood).
Incorrect Answers:
A . Threat modeling Identifies potential threats but doesn't prioritize risks dynamically.
C . Incident lifecycle management Focuses on handling security incidents, not risk evaluation.
D . Statistical anomaly detection Detects unusual activity but doesn't prioritize based on impact.
Additional Resources:
Splunk Risk-Based Alerting (RBA) Guide
NIST Risk Assessment Framework

QUESTION 28
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

Correct Answer: B
Section:
Explanation:
Splunk's REST API allows external applications and security tools to automate workflows, integrate with Splunk, and retrieve/search data programmatically.
Why Use REST APIs in Splunk Automation?
Automates interactions between Splunk and other security tools.
Enables real-time data ingestion, enrichment, and response actions.
Used in Splunk SOAR playbooks for automated threat response.
Example:
A security event detected in Splunk ES triggers a Splunk SOAR playbook via REST API to:
Retrieve threat intelligence from VirusTotal.
Block the malicious IP in Palo Alto firewall.
Create an incident ticket in ServiceNow.
Incorrect Answers:
A . To configure storage retention policies Storage is managed via Splunk indexing, not REST APIs.
C . To compress data before indexing Splunk does not use REST APIs for data compression.
D . To generate predefined reports Reports are generated using Splunk's search and reporting functionality, not APIs.
Additional Resources:
Splunk REST API Documentation
Automating Workflows with Splunk API

QUESTION 29
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

Correct Answer: A, C, E
Section:
Explanation:
Splunk SOAR (Security Orchestration, Automation, and Response) playbooks automate security processes, reducing response times.
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.
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.
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
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 30
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

Correct Answer: B
Section:
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:
Create, update, and retire correlation searches and security content Manage use case coverage for different threat categories Tune detection rules to reduce false positives 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. 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?
A. Data model acceleration -- Improves search performance but does not manage detection lifecycles. C. Metrics indexing -- Used for time-series data (e.g., system performance monitoring), not for managing detections. 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 31
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

Correct Answer: B
Section:
Explanation:
Why Use 'Data Models' for Standardized Search Accuracy and Detection Logic?
Splunk Data Models provide a structured, normalized representation of raw logs, improving:
Search consistency across different log sources Detection logic by ensuring standardized field names 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. Without Data Models: Different logs use src_ip, source_ip, or ip_address, making searches complex.
With Data Models: All fields map to a standard format, enabling consistent detection logic.
Why Not the Other Options?
A. Field Extraction -- Extracts fields from raw events but does not standardize field names across sources. C. Event Correlation -- Detects relationships between logs but doesn't normalize data for search accuracy. 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 32
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

Correct Answer: A
Section:
Explanation:
Why Focus on High-Level Summaries & Actionable Insights?
Executive security reports should provide concise, strategic insights that help leadership teams make informed decisions.
Key Elements for an Executive-Level Report: Summarized Security Incidents -- Focus on major threats and trends. Actionable Recommendations -- Include mitigation steps for ongoing risks. Visual Dashboards -- Use charts and graphs for easy interpretation. Compliance & Risk Metrics -- Highlight compliance status (e.g., PCI-DSS, NIST).
Example in Splunk: Scenario: A CISO requests a weekly security report. Best Report Format:
Threat Summary: 'Detected 15 phishing attacks this week.'
Key Risks: 'Increase in brute-force login attempts.'
Recommended Actions: 'Enhance MFA enforcement & user awareness training.'
Why Not the Other Options?
B. Detailed logs of every notable event -- Too technical; executives need summaries, not raw logs. C. Excluding compliance metrics to simplify reports -- Compliance is critical for risk assessment. D. Avoiding visuals to focus on raw data -- Visuals improve clarity; raw data is too complex for executives.
Reference & Learning Resources
Splunk Security Reporting Best Practices: https://www.splunk.com/en_us/blog/security Creating Effective Executive Dashboards in Splunk: https://splunkbase.splunk.com Cybersecurity Metrics & Reporting for Leadership Teams: https://www.nist.gov/cyberframework

QUESTION 33
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

Correct Answer: C
Section:
Explanation:
Key Elements of Security Program Documentation
A security program's documentation ensures consistency, compliance, and efficiency in cybersecurity operations.
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.
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 34
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

Correct Answer: A, C, E
Section:
Explanation:
Critical Elements of an Effective Incident Report
An incident report documents security breaches, outlines response actions, and provides prevention strategies.
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.
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.
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.

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 35
What are the key components of Splunk's indexing process? (Choose three)

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

Correct Answer: A, C, E
Section:
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.
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.
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.
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.
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 36
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.

Correct Answer: A, B, D
Section:
Explanation:
Ensuring Efficient Detection Tuning in Splunk Enterprise Security
Detection tuning is essential to minimize false positives and improve security visibility.
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.
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.
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.
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