Advanced Splunk Search Language for Security Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Advanced Splunk Search Language for Security Training Course is meticulously designed to transform security professionals into Advanced Splunk Power Users and Threat Hunters, leveraging the full potential of the Search Processing Language (SPL). In the modern Cybersecurity landscape, data volume is exploding, making it critical to move beyond basic searches to implement sophisticated Analytics-Driven Security models. This program focuses on mastering advanced SPL techniques including Correlation Searches, Data Modeling, and Machine Learning Toolkit (MLTK) integration to proactively identify complex threats like Advanced Persistent Threats (APTs), Insider Threats, and Zero-Day Vulnerabilities. Participants will gain hands-on experience in building and optimizing robust security content, ensuring rapid Incident Response and fortifying the organization's Security Posture against evolving global cyber risks.

The curriculum emphasizes practical application in a Security Operations Center (SOC) context, focusing on turning raw machine data into actionable Security Intelligence. By mastering efficient search optimization, Regular Expressions (Regex) for granular data extraction, and powerful commands like transaction, streamstats, and eval, learners will significantly enhance their ability to perform deep Forensic Analysis and deploy Risk-Based Alerting (RBA). The goal is to develop highly-skilled individuals capable of creating custom security use cases, dramatically reducing Mean Time to Detect (MTTD), and contributing to the maturity of an organization's overall Enterprise Security framework, making them indispensable assets in the fight against sophisticated cyber adversaries.

Programme Curriculum

Advanced Splunk Search Language for Security Training Course

Introduction

Advanced Splunk Search Language for Security Training Course is meticulously designed to transform security professionals into Advanced Splunk Power Users and Threat Hunters, leveraging the full potential of the Search Processing Language (SPL). In the modern Cybersecurity landscape, data volume is exploding, making it critical to move beyond basic searches to implement sophisticated Analytics-Driven Security models. This program focuses on mastering advanced SPL techniques including Correlation Searches, Data Modeling, and Machine Learning Toolkit (MLTK) integration to proactively identify complex threats like Advanced Persistent Threats (APTs), Insider Threats, and Zero-Day Vulnerabilities. Participants will gain hands-on experience in building and optimizing robust security content, ensuring rapid Incident Response and fortifying the organization's Security Posture against evolving global cyber risks.

The curriculum emphasizes practical application in a Security Operations Center (SOC) context, focusing on turning raw machine data into actionable Security Intelligence. By mastering efficient search optimization, Regular Expressions (Regex) for granular data extraction, and powerful commands like transaction, streamstats, and eval, learners will significantly enhance their ability to perform deep Forensic Analysis and deploy Risk-Based Alerting (RBA). The goal is to develop highly-skilled individuals capable of creating custom security use cases, dramatically reducing Mean Time to Detect (MTTD), and contributing to the maturity of an organization's overall Enterprise Security framework, making them indispensable assets in the fight against sophisticated cyber adversaries.

Course Duration

10 days

Course Objectives

1. Master Advanced SPL Syntax for optimal search performance and efficiency.
2. Design and implement complex Event Correlation logic for multi-stage attacks.
3. Develop custom Data Models to normalize and accelerate security data analysis.
4. Utilize Machine Learning to detect Anomalies and unknown threats.
5. Implement Risk-Based Alerting strategies to prioritize security incidents.
6. Perform deep-dive Digital Forensics and Incident Response (DFIR) using SPL.
7. Apply Threat Intelligence feeds within Splunk for proactive threat matching.
8. Optimize searches using Regex and knowledge objects like lookups and macros.
9. Configure and manage Splunk Enterprise Security (ES) correlation searches.
10. Create high-fidelity Security Dashboards and Visualizations for executive reporting.
11. Troubleshoot and tune slow searches for Performance Optimization.
12. Establish effective monitoring for Insider Threat Detection and privileged account abuse.
13. Integrate Splunk with SOAR platforms for automated response actions.

Target Audience

1. Security Operations Center Analysts
2. Threat Hunters and Security Researchers
3. Cybersecurity Engineers and Architects
4. Splunk Administrators focusing on Security
5. Incident Responders and Digital Forensics Specialists
6. Security Consultants and Auditors
7. IT Professionals transitioning to Security Information and Event Management
8. Anyone responsible for creating, optimizing, or maintaining Splunk Security Content

Course Modules

1. SPL Fundamentals for Security Optimization

- Search Pipeline review and command distribution.
- Optimizing searches for massive security datasets.
- Using Regex and rex command for advanced field extraction.
- Leveraging Knowledge Objects for normalization.
- Case Study: Optimizing a brute-force detection search query that was taking over 5 minutes to run across a 90-day data set, reducing execution time by 85%.

2. Advanced Correlation and Time-Series Analysis

- Mastering the transaction command for session-based event grouping.
- Using streamstats and eventstats for real-time aggregation and baselining.
- Advanced use of the timechart command and statistical functions.
- Correlating events across multiple data sources.
- Case Study: Correlating successful login events with preceding failed attempts from different systems to detect Account Takeover using a complex transaction search.

3. Data Modeling and Pivot for Security Analysts

- Understanding and creating security-focused Data Models.
- Accelerating Data Models for faster report and dashboard generation.
- Utilizing the Pivot interface for ad-hoc security reporting.
- Normalizing disparate security logs with the Common Information Model
- Case Study: Modeling firewall, endpoint, and web proxy logs into the CIM to create a unified dashboard for tracking lateral movement attempts.

4. Proactive Threat Hunting with Advanced SPL

- Developing Hypothesis-Driven Threat Hunting searches.
- Techniques for finding low-and-slow threats
- Using Set Theory Commands for baseline comparison.
- Identifying rare and suspicious events using rare and anomalousvalue.
- Case Study: Hunting for new persistence mechanisms by comparing current registry data against a six-month golden image baseline using set diff.

5. Machine Learning Toolkit (MLTK) for Security

- Introduction to Unsupervised Machine Learning in Splunk.
- Using the cluster command to group similar security events.
- Implementing Anomaly Detection using density and time-series algorithms.
- Creating custom algorithms and models for security use cases.
- Case Study: Deploying an MLTK model to detect anomalous user network traffic volumes indicative of potential Data Exfiltration.

6. Advanced Splunk Enterprise Security (ES) Content

- Creating and tuning custom Correlation Searches in Splunk ES.
- Understanding and configuring Risk-Based Alerting.
- Integrating Threat Intelligence data for enrichment and alerting.
- Customizing the Incident Review dashboard and notable events.

- Case Study: Implementing an RBA framework for privileged access abuse by assigning risk scores to specific failed activities on critical servers.

7. Insider Threat and Compliance Monitoring

- Building searches for monitoring user behavioral patterns
- Detecting privileged account abuse and unauthorized access.
- Creating Compliance Reports using SPL.
- Monitoring file integrity and critical system configuration changes.
- Case Study: Developing a multi-step search chain to flag a sequence of unauthorized attempts to access and modify sensitive HR files by an internal user.

8. Incident Response and Digital Forensics

- Utilizing Splunk for rapid Host and Network Forensics.
- Tracking Lateral Movement using network and authentication logs.
- Leveraging the iplocation and geostats commands for geographic analysis.
- Building response workflows to enrich and escalate notable events.
- Case Study: Reconstructing an entire attack timeline, from initial phishing email to C2 communication, using transaction and network flow data.

9. Dashboard and Visualization Best Practices

- Creating executive-level security dashboards using XML/Dashboard Studio.
- Implementing advanced drill-downs and form inputs for interactivity.
- Using various visualization types effectively.
- Optimizing dashboard performance and data refresh rates.
- Case Study: Redesigning the SOC's primary dashboard to focus on MTTD and MTTR metrics, leading to a 20% improvement in incident triage speed.

10. Advanced Log Analysis for Cloud and Endpoint

- Analyzing Cloud Infrastructure logs
- Deep-dive SPL for Endpoint Detection and Response data.
- Monitoring for suspicious process execution and command line activity.
- Handling multi-line and JSON/XML formatted logs using spath.
- Case Study: Developing searches to detect unauthorized creation of cloud resources or changes to security group policies in an AWS environment.

11. Custom Commands and External Data

- Using Lookups for data enrichment.
- Creating and managing Search Macros for reusable code blocks.
- Introduction to custom search commands
- Integrating external data sources into Splunk.
- Case Study: Implementing a custom lookup to dynamically blacklist newly discovered malicious IP addresses in real-time, significantly improving alert fidelity.

12. Splunk Performance Tuning and Troubleshooting

- Using the Job Inspector to analyze and debug slow searches.
- Best practices for index selection and time range definition.

- Understanding the role of Bloom Filters and segmenters in search speed.
- Advanced use of the metadata and tstats commands for high-performance reporting.
- Case Study: Troubleshooting a slow dashboard query by analyzing the Job Inspector and converting the core search to use tstats over a Data Model, reducing load time from 45s to 3s.

13. Threat Modeling and Use Case Development

- Mapping security logs to MITRE ATT&CK framework.
- A structured approach to Security Use Case development.
- Translating threat models into effective SPL correlation searches.
- Measuring the effectiveness and coverage of new security content.
- Case Study: Developing a new correlation search to detect the initial phase of the SolarWinds attack kill chain using DNS and HTTP traffic logs.

14. SOAR Integration and Automated Response

- Introduction to Security Orchestration, Automation, and Response
- Using Splunk alerts to trigger SOAR playbooks.
- Enriching alerts with external data before automation.
- Automating containment actions using SPL and API calls.
- Case Study: Automating the isolation of a host and creation of a Jira ticket when a high-risk notable event is triggered in Splunk ES.

15. Real-World Attack Scenario Simulation

- Full end-to-end simulation of a multi-stage Ransomware Attack.
- Applying all learned SPL and security concepts to investigate the breach.
- Creating a final Forensic Report and incident summary using Splunk dashboards.
- Peer review and debriefing of the investigation process.
- Case Study: A comprehensive capstone lab where learners detect, investigate, and contain a simulated attack, applying Data Loss Prevention and lateral movement detection techniques.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com **or call** +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200
28 Sep 2026	09 Oct 2026	Online	$2,200
05 Oct 2026	16 Oct 2026	Online	$2,200
12 Oct 2026	23 Oct 2026	Online	$2,200
19 Oct 2026	30 Oct 2026	Online	$2,200
26 Oct 2026	06 Nov 2026	Online	$2,200

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com