Mastering Log Analysis for Threat Detection Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In the modern cybersecurity landscape, the sheer volume of data makes effective threat detection a significant challenge. Mastering Log Analysis for Threat Detection Training Course moves beyond basic log monitoring to instill advanced analytical skills using real-world scenarios and popular tools. You'll master the art of transforming raw system and security logs including SIEM data, cloud logs, and endpoint telemetry into actionable cyber threat intelligence. By focusing on correlation, anomaly detection, and threat hunting methodologies, this training is essential for security professionals aiming to reduce their organization's Mean Time to Detect and effectively combat sophisticated Advanced Persistent Threats and insider threats.

This program is designed as a hands-on, practical deep dive into the defensive security domain. We equip participants with the skills to confidently perform forensic analysis, interpret complex log patterns indicative of attacks using frameworks like MITRE ATT&CK, and build robust detection engineering rules. The curriculum emphasizes the critical link between comprehensive log management and rapid incident response, ensuring graduates are prepared to immediately apply their expertise to safeguard critical assets in any environment, from on-premises infrastructure to large-scale multi-cloud deployments.

Programme Curriculum

Mastering Log Analysis for Threat Detection Training Course

Introduction

In the modern cybersecurity landscape, the sheer volume of data makes effective threat detection a significant challenge. Mastering Log Analysis for Threat Detection Training Course moves beyond basic log monitoring to instill advanced analytical skills using real-world scenarios and popular tools. You'll master the art of transforming raw system and security logs including SIEM data, cloud logs, and endpoint telemetry into actionable cyber threat intelligence. By focusing on correlation, anomaly detection, and threat hunting

methodologies, this training is essential for security professionals aiming to reduce their organization's Mean Time to Detect and effectively combat sophisticated Advanced Persistent Threats and insider threats.

This program is designed as a hands-on, practical deep dive into the defensive security domain. We equip participants with the skills to confidently perform forensic analysis, interpret complex log patterns indicative of attacks using frameworks like MITRE ATT&CK, and build robust detection engineering rules. The curriculum emphasizes the critical link between comprehensive log management and rapid incident response, ensuring graduates are prepared to immediately apply their expertise to safeguard critical assets in any environment, from on-premises infrastructure to large-scale multi-cloud deployments.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Implement a foundational Security Information and Event Management (SIEM) strategy for centralized log ingestion and parsing.
2. Apply Kusto Query Language (KQL) and similar advanced search syntaxes for deep-dive log analysis across diverse data sources.
3. Identify patterns of common cyberattacks, including brute-force, SQL injection, and web application attacks, within network and server logs.
4. Utilize behavioral analysis techniques to detect zero-day exploits and subtle anomalies that bypass signature-based defenses.
5. Map discovered malicious activity directly to the MITRE ATT&CK Framework for standardized reporting and defense improvement.
6. Perform effective cloud log analysis across major platforms to detect cloud-native threats.
7. Differentiate between normal and malicious activity in Windows Event Logs and Linux Syslogs for host-level threat hunting.
8. Develop, test, and tune high-fidelity detection engineering rules to minimize false positives and maximize true positive alerts.
9. Conduct forensic investigation and timeline creation using correlated log data following a security incident.
10. Integrate threat intelligence feeds with SIEM alerts to enrich log data and prioritize critical risks.
11. Master network flow data analysis to monitor lateral movement and data exfiltration attempts.
12. Establish best practices for log retention, compliance, and secure log archiving.
13. Automate basic incident response actions based on high-severity log-based alerts using SOAR concepts.

Target Audience

1. SOC Analysts
2. Cyber Threat Hunters.
3. Incident Responders.
4. Security Engineers.
5. Forensic Analysts.
6. IT Security Managers.
7. Cloud Security Architects.
8. Vulnerability Management.

Course Modules

Module 1: Foundations of Secure Log Management and SIEM

- Log Sources and Taxonomy
- Centralized Log Ingestion and Normalization for Unified Analysis.
- SIEM Architecture Deep Dive.
- Compliance Requirements.
- Case Study: Failure to Normalize Logs and the Resulting Delayed Detection in a Major Ransomware Attack.

Module 2: Advanced Log Querying and Search Techniques

- Mastering Query Languages
- Efficiently dealing with High-Volume Logs and low-value events.
- Utilizing basic functions to identify high-count or abnormal log activity.
- Log Correlation Strategies.
- Case Study: Correlating Firewall and Proxy Logs to Track a C2 Channel Using Advanced Search Commands.

Module 3: Host-Based Threat Detection

- Deep Dive into Windows Event IDs
- Linux Log Analysis.
- Endpoint Detection and Response Logs and Sysmon Data Analysis.
- Detecting Lateral Movement and Privilege Escalation through Host Logs.
- Case Study: Using Sysmon Logs to Reconstruct the Execution Chain of a "Living off the Land" Binary.

Module 4: Network and Perimeter Log Analysis

- Firewall and Network Device Logs.
- Proxy and DNS Logs.
- NetFlow/IPFIX Analysis.
- Intrusion Detection/Prevention System Alert Triage and Log Validation.
- Case Study: Analyzing DNS Logs to Uncover a Phishing Campaign and the Target IP Addresses.

Module 5: Web Application and Authentication Log Analysis

- Web Server Logs
- Identity and Access Management Logs.
- Failed Authentication Analysis.
- Monitoring Multi-Factor Authentication bypass attempts in access logs.
- Case Study: Identifying an Exploited Vulnerability via Web Server Logs and its Corresponding Post-Exploitation Activity.

Module 6: Cloud Log Analysis and Threat Hunting

- Cloud Logging Services.
- Detection of Cloud-Native Threats.
- Serverless and Container Log Monitoring for anomalies.
- Detecting Misconfigurations and Unauthorized Data Access in Cloud Storage Logs.

- Case Study: Tracking the compromise of an AWS Access Key and the Subsequent Creation of a Rogue EC2 Instance.

Module 7: Threat Hunting with the MITRE ATT&CK Framework

- Mapping Log Sources to MITRE ATT&CK Techniques for Coverage Assessment.
- Developing Hypotheses for Targeted Threat Hunting based on Log Data.
- Searching for subtle indicators of compromise that SIEM rules miss.
- Tuning and Improving Existing Detection Rules based on threat hunting findings.
- Case Study: A Threat Hunter's Journey to Uncover a Hidden Persistence Mechanism using Log Aggregation.

Module 8: Incident Response, Forensics, and Automation

- Log Analysis for Incident Scoping and Containment Decisions.
- Creating a Cohesive Digital Forensic Timeline from various log sources.
- Introduction to Security Orchestration, Automation, and Response integration with log data.
- Reporting and Communication.
- Case Study: Post-Mortem Analysis of a Data Breach using a Correlated Log Timeline to determine exfiltrated data.

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	11 Sep 2026	Online	$1,100
14 Sep 2026	18 Sep 2026	Online	$1,100
21 Sep 2026	25 Sep 2026	Online	$1,100
28 Sep 2026	02 Oct 2026	Online	$1,100
05 Oct 2026	09 Oct 2026	Online	$1,100
12 Oct 2026	16 Oct 2026	Online	$1,100
19 Oct 2026	23 Oct 2026	Online	$1,100
26 Oct 2026	30 Oct 2026	Online	$1,100

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

Register Online Now

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