Training Course on Enterprise Network Security Monitoring for DFIR

Professional Development Training Course Outline

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

Course Introduction

In today’s rapidly evolving cyber threat landscape, enterprise network security monitoring plays a critical role in effective Digital Forensics and Incident Response (DFIR). Training Course on Enterprise Network Security Monitoring for DFIR is designed to empower cybersecurity professionals, SOC analysts, and incident responders with hands-on, tactical skills to monitor, detect, and investigate network intrusions and anomalies within enterprise infrastructures. With rising threats such as APTs, zero-day exploits, and lateral movements, organizations must adopt proactive threat hunting, packet analysis, and real-time alerting mechanisms to secure critical assets. This training integrates threat intelligence with deep packet inspection, behavioral analytics, and endpoint telemetry to build robust incident response strategies.

By leveraging real-world scenarios and advanced security toolkits, this course bridges the gap between traditional monitoring and modern DFIR tactics. Learners will master tools such as Zeek, Suricata, Security Onion, ELK Stack, Wireshark, and PCAP analysis, enabling rapid detection of malicious activity across distributed environments. Through practical labs, live case studies, and MITRE ATT&CK mapping, participants will gain a comprehensive understanding of data correlation, log analysis, and incident triage processes. The curriculum is tailored for enterprise defenders who want to stay ahead of threat actors using evidence-based, threat-driven defense models.

Programme Curriculum

Training Course on Enterprise Network Security Monitoring for DFIR

Introduction

In today’s rapidly evolving cyber threat landscape, enterprise network security monitoring plays a critical role in effective Digital Forensics and Incident Response (DFIR). Training Course on Enterprise Network Security Monitoring for DFIR is designed to empower cybersecurity professionals, SOC analysts, and incident responders with hands-on, tactical skills to

monitor, detect, and investigate network intrusions and anomalies within enterprise infrastructures. With rising threats such as APTs, zero-day exploits, and lateral movements, organizations must adopt proactive threat hunting, packet analysis, and real-time alerting mechanisms to secure critical assets. This training integrates threat intelligence with deep packet inspection, behavioral analytics, and endpoint telemetry to build robust incident response strategies.

By leveraging real-world scenarios and advanced security toolkits, this course bridges the gap between traditional monitoring and modern DFIR tactics. Learners will master tools such as Zeek, Suricata, Security Onion, ELK Stack, Wireshark, and PCAP analysis, enabling rapid detection of malicious activity across distributed environments. Through practical labs, live case studies, and MITRE ATT&CK mapping, participants will gain a comprehensive understanding of data correlation, log analysis, and incident triage processes. The curriculum is tailored for enterprise defenders who want to stay ahead of threat actors using evidence-based, threat-driven defense models.

Course Objectives

1. Understand the fundamentals of enterprise network security monitoring in DFIR workflows
2. Implement threat detection techniques using Security Onion, Zeek, and Suricata
3. Analyze PCAPs and log files to identify Indicators of Compromise (IoCs)
4. Integrate MITRE ATT&CK framework for adversary behavior detection
5. Perform real-time network traffic monitoring and anomaly detection
6. Build centralized logging using the ELK Stack for forensic investigation
7. Conduct deep packet inspection for intrusion analysis and evidence extraction
8. Develop threat intelligence pipelines for contextual incident response
9. Correlate endpoint and network data for comprehensive threat visibility
10. Automate alert triage and playbook-based incident handling
11. Apply statistical and behavioral methods for proactive threat hunting
12. Document and report forensic findings using industry best practices
13. Enhance readiness for breach detection, containment, and recovery

Target Audiences

1. SOC Analysts
2. Network Security Engineers
3. Incident Responders
4. Cybersecurity Analysts
5. Digital Forensics Investigators
6. Threat Hunters
7. IT Security Managers
8. Government/Defense Cyber Units

Course Duration: 5 days

Course Modules

Module 1: Introduction to DFIR and Network Security Monitoring

- Overview of DFIR lifecycle
- Role of network monitoring in DFIR
- Key terminologies and concepts
- Common attack vectors and artifacts
- Importance of baselining network traffic
- **Case Study: Initial Compromise via Malicious Email Attachment**

Module 2: Network Traffic Capture and Analysis

- Introduction to packet capture tools (tcpdump, Wireshark)

- Understanding protocols and packet headers
- Filtering and dissecting PCAPs
- Identifying anomalies and suspicious sessions
- Hands-on: Capture analysis with Wireshark
- **Case Study: Detecting Beaconing Activity from a Compromised Host**

Module 3: Intrusion Detection Systems (IDS) in DFIR

- Zeek and Suricata architecture
- Signature-based vs behavior-based detection
- Writing and tuning IDS rules
- Integration with Security Onion
- Alert triage and metadata enrichment
- **Case Study: Uncovering Command and Control (C2) via Suricata**

Module 4: Centralized Logging with the ELK Stack

- Setting up Elasticsearch, Logstash, and Kibana
- Ingesting logs from various sources
- Building dashboards for SOC visibility
- Querying data using Kibana and Elasticsearch DSL
- Visualizing threats and patterns
- **Case Study: Ransomware Detection Using ELK Dashboard Correlation**

Module 5: Threat Intelligence and MITRE ATT&CK Integration

- Introduction to threat intelligence sources (STIX/TAXII)
- Mapping logs to MITRE ATT&CK tactics and techniques
- Enriching alerts with threat context
- YARA rules and threat feed integration
- Using OpenCTI and MISP
- **Case Study: Attribution of APT Group Using MITRE Technique Mapping**

Module 6: Endpoint and Network Correlation Techniques

- Combining endpoint telemetry and network logs
- Detecting lateral movement and privilege escalation
- Leveraging EDR platforms with SIEM
- Timeline reconstruction and session stitching
- Reducing false positives with layered visibility
- **Case Study: Investigating Credential Dumping in a Hybrid Cloud Network**

Module 7: Proactive Threat Hunting and Anomaly Detection

- Hypothesis-driven vs data-driven hunting
- Leveraging machine learning for pattern recognition
- Behavioral analytics and baseline deviations
- Custom detection scripts using Sigma/KQL
- Developing repeatable hunting procedures
- **Case Study: Discovery of Insider Threat Through Statistical Anomaly**

Module 8: Reporting, Documentation, and Legal Considerations

- Incident reporting standards (NIST, ISO)
- Chain of custody and evidence handling
- Creating actionable incident reports

- Communication with legal/compliance teams
- Lessons learned and post-mortem analysis
- **Case Study: Incident Disclosure and Compliance Reporting for GDPR Breach**

Training Methodology

- **Hands-on Labs:** Real-world scenarios using open-source tools and sandbox environments
- **Live Demonstrations:** Tool walkthroughs and DFIR workflows with instructor guidance
- **Interactive Case Studies:** Learners analyze, respond, and report on attack simulations
- **Group Discussions:** Collaborative analysis and peer reviews
- **Assessments and Quizzes:** Knowledge checks to reinforce learning outcomes
- **Downloadable Resources:** Cheat sheets, detection rules, and configuration templates

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	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500

Start Date	End Date	Location	Price
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500
26 Oct 2026	30 Oct 2026	Physical	$1,500

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

Register Online Now

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