Training Course on Network Segmentation and Micro-segmentation Forensics

Professional Development Training Course Outline

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

Course Introduction

In today’s dynamic cybersecurity environment, threats are not only more sophisticated but also harder to detect. Organizations increasingly rely on network segmentation and micro-segmentation to reduce attack surfaces and enforce zero trust architecture principles. Training Course Outline on Network Segmentation and Micro-segmentation Forensics is designed to empower professionals with the skills and knowledge to investigate, analyze, and respond to breaches within segmented network infrastructures using modern forensic techniques.

As cyber threats continue to bypass traditional perimeter defenses, mastering forensic analysis in micro-segmented environments becomes essential. This course bridges the gap between cybersecurity architecture and digital forensics, providing a robust understanding of network behavior, traffic flow analysis, and incident response strategies within complex, distributed systems. With a hands-on, case-driven approach, learners will gain proficiency in network traffic reconstruction, policy violation tracing, and compromise containment, aligned with industry best practices and compliance standards.

Programme Curriculum

Training Course Outline on Network Segmentation and Micro-segmentation Forensics

Introduction

In today’s dynamic cybersecurity environment, threats are not only more sophisticated but also harder to detect. Organizations increasingly rely on network segmentation and micro-segmentation to reduce attack surfaces and enforce zero trust architecture principles. Training Course Outline on Network Segmentation and Micro-segmentation Forensics is designed to empower professionals with the skills and knowledge to investigate, analyze, and respond to breaches within segmented network infrastructures using modern forensic techniques.

As cyber threats continue to bypass traditional perimeter defenses, mastering forensic analysis in micro-segmented environments becomes essential. This course bridges the gap between cybersecurity architecture and digital forensics, providing a robust understanding of network behavior, traffic flow analysis, and incident response strategies within complex, distributed systems. With a hands-on, case-driven approach, learners will gain proficiency in network traffic reconstruction, policy violation tracing, and compromise containment, aligned with industry best practices and compliance standards.

Course Objectives

1. Understand core concepts of network segmentation and micro-segmentation in cybersecurity.
2. Conduct forensic investigations within zero trust segmented networks.
3. Identify, analyze, and correlate security breaches across isolated zones.
4. Apply forensic tools to monitor and investigate east-west traffic.
5. Trace policy violations and unauthorized access in segmented environments.
6. Conduct packet-level inspection for breach reconstruction.
7. Develop incident reports from micro-segmentation investigations.
8. Detect lateral movement and apply containment strategies.
9. Understand segmentation-based risk management and compliance.
10. Use AI and machine learning for traffic analysis and anomaly detection.
11. Explore software-defined networking (SDN) and its impact on forensic workflows.
12. Simulate cyberattacks to evaluate segmentation defense effectiveness.
13. Perform root cause analysis and implement adaptive security policies.

Target Audiences

1. Cybersecurity Analysts
2. Network Security Engineers
3. Digital Forensic Investigators
4. SOC Team Members
5. IT Security Managers
6. Cloud Infrastructure Professionals
7. Penetration Testers
8. Compliance and Risk Officers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Network Segmentation Forensics

- Definition and benefits of segmentation
- Micro-segmentation vs. traditional segmentation
- Role in incident containment
- Integration with zero trust architecture
- Key protocols and access control enforcement
- **Case Study**: Containing a ransomware attack through segmentation

Module 2: Zero Trust Architecture & Forensics

- Understanding zero trust principles
- Forensic implications of zero trust
- Real-time traffic inspection
- Identity and access auditing
- Endpoint detection integration

- **Case Study**: Tracing insider threats in zero trust environments

Module 3: Micro-segmentation Policies and Compliance

- Writing segmentation policies
- Compliance mapping (HIPAA, PCI-DSS)
- Role of policy violations in breaches
- Regulatory requirements in forensic analysis
- Automated auditing tools
- **Case Study**: Forensic audit of non-compliant VLAN breach

Module 4: Tools for Network Forensics

- Wireshark, Zeek, and Security Onion
- Flow data analysis (NetFlow, sFlow)
- EDR integration
- Using SIEM platforms for segmentation logs
- Packet capture strategies
- **Case Study**: Leveraging Zeek for east-west traffic anomalies

Module 5: East-West Traffic Analysis

- What is east-west traffic?
- Detection strategies for internal threats
- Traffic mapping and visualization
- Behavioral baselining techniques
- Identifying unauthorized lateral movement
- **Case Study**: Malicious pivoting within segmented networks

Module 6: Cloud-Based Network Segmentation

- Cloud-native segmentation (AWS, Azure)
- Hybrid environment investigations
- API and VPC logging
- Challenges in virtualized network forensics
- Data exfiltration detection in cloud
- **Case Study**: Tracking insider misuse in AWS micro-segmented VPC

Module 7: Intrusion Detection in Segmented Networks

- Integrating IDS with segmentation
- IDS rule tuning for zones
- Signature vs anomaly-based detection
- Detecting slow-moving threats
- Logging and alerting frameworks
- **Case Study**: IDS logs leading to discovery of rogue agent

Module 8: Advanced Packet Capture & Analysis

- Deep packet inspection in segmented zones
- Decrypting SSL/TLS traffic for forensics
- Payload reconstruction
- Time-series packet correlation
- Correlation with flow data
- **Case Study**: Reconstructing a data breach timeline using PCAP

Module 9: Threat Hunting in Micro-Segmented Networks

- Establishing hunting hypotheses
- Endpoint behavior correlation
- Threat intelligence feeds
- Threat emulation tools (CALDERA, Atomic Red Team)
- Pivot analysis within segmentation layers
- **Case Study**: Discovery of APT lateral movement using hypothesis testing

Module 10: Behavioral Analytics and AI for Forensics

- Introduction to UEBA
- AI-based anomaly detection
- Integrating ML with SIEM/SOAR
- Training models with segmented data
- Interpreting anomalies for evidence
- **Case Study**: ML-assisted detection of policy misuse

Module 11: Forensic Logging and Chain of Custody

- Log aggregation from segmented zones
- Timestamp synchronization and integrity
- Chain of custody best practices
- Secure storage of forensic artifacts
- Audit trail generation
- **Case Study**: Using logs for admissible court evidence

Module 12: Incident Response Integration

- Coordinating forensics with IR teams
- Playbooks for segmented networks
- Communication protocols during breaches
- Evidence triage and prioritization
- Integrating IR tools (XDR, SOAR)
- **Case Study**: Incident response playbook execution post-breach

Module 13: SDN and Micro-segmentation Challenges

- Understanding SDN controllers
- Dynamic policy updates and forensics
- Forensic blind spots in overlays
- Monitoring SDN events and logs
- Reducing SDN-based attack vectors
- **Case Study**: Compromised SDN controller in a micro-segmented network

Module 14: Red Team Simulation & Defense

- Red team methodologies
- Simulating internal segmentation breaches
- Blue team response and detection
- Red-blue collaboration for resilience
- Key metrics to evaluate segmentation strength
- **Case Study**: Red team success due to segmentation misconfigurations

Module 15: Final Capstone and Report Writing

- Synthesizing findings into a forensic report
- Legal aspects of forensic documentation

- Executive summaries for stakeholders
- Lessons learned and future policies
- Presenting evidence to non-technical audiences
- **Case Study**: Final project - breach scenario analysis and presentation

Training Methodology

- Hands-on labs and simulations
- Real-world case studies per module
- Live demonstrations of forensic tools
- Group analysis and roleplay exercises
- Capstone project presentation and peer review

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org 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
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$0

Start Date	End Date	Location	Price
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0
21 Sep 2026	02 Oct 2026	Physical	$0

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

Register Online Now

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