Training Course on Network Signatures for Malware Detection

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 the digital era, network security is paramount, and malware continues to evolve with unprecedented sophistication. Training Course on Network Signatures for Malware Detection is designed to equip cybersecurity professionals with in-depth knowledge and actionable skills in identifying, analyzing, and defending against advanced persistent threats (APTs) using signature-based detection techniques. With a surge in encrypted malware and polymorphic threats, the role of accurate, automated, and behavioral signature detection has never been more critical.

This course blends theory with practical, hands-on labs and real-world case studies. Participants will learn how to detect malicious traffic using deep packet inspection (DPI), analyze payloads, reverse engineer malware behavior, and build effective defense mechanisms through custom signatures. Emphasis will be placed on modern tools like Suricata, Snort, Zeek (Bro), and YARA, and how to integrate them into a scalable malware detection framework.

Programme Curriculum

Training Course on Network Signatures for Malware Detection

Introduction

In the digital era, network security is paramount, and malware continues to evolve with unprecedented sophistication. Training Course on Network Signatures for Malware Detection is designed to equip cybersecurity professionals with in-depth knowledge and actionable skills in identifying, analyzing, and defending against advanced persistent threats (APTs) using signature-based detection techniques. With a surge in encrypted malware and polymorphic threats, the role of accurate, automated, and behavioral signature detection has never been more critical.

This course blends theory with practical, hands-on labs and real-world case studies. Participants will learn how to detect malicious traffic using deep packet inspection (DPI), analyze payloads, reverse engineer malware behavior, and build effective defense mechanisms through custom signatures. Emphasis will be placed on modern tools like Suricata, Snort,

Zeek (Bro), and YARA, and how to integrate them into a scalable malware detection framework.

Course Objectives

1. Understand the fundamentals of malware signature detection and intrusion detection systems (IDS).
2. Identify various types of network-based malware attacks and their behaviors.
3. Build custom Snort and Suricata rules for signature-based detection.
4. Analyze packet captures (PCAPs) to detect malware using tools like Wireshark.
5. Apply deep packet inspection (DPI) to dissect and analyze suspicious payloads.
6. Utilize YARA rules and pattern matching for malware classification.
7. Learn the process of reverse engineering malware signatures for defense strategies.
8. Integrate machine learning with signature-based detection for hybrid protection.
9. Detect encrypted malware traffic using heuristic and signature-based methods.
10. Leverage real-time threat intelligence to enhance signature libraries.
11. Design scalable network defense architectures using signature detection tools.
12. Automate signature updates using CI/CD pipelines for dynamic environments.
13. Conduct forensic investigations using network artifacts and malware indicators.

Target Audience

1. Cybersecurity Analysts
2. Incident Response Teams
3. SOC Engineers
4. Penetration Testers
5. Malware Analysts
6. Network Security Engineers
7. IT Forensic Experts
8. Security Researchers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware and Network Signatures

- Definition and evolution of malware
- Overview of signature-based detection
- Behavioral vs. static signatures
- Network-based vs. host-based signatures
- IDS and IPS technologies
- **Case Study:** WannaCry malware signature dissection

Module 2: Network Packet Analysis

- Introduction to network protocols
- Deep Packet Inspection (DPI)
- Analyzing headers and payloads
- Tools: Wireshark, tcpdump
- Extracting IOCs (Indicators of Compromise)
- **Case Study:** Malware communication in HTTP traffic

Module 3: Snort Signature Development

- Snort architecture overview
- Rule syntax and header fields

- Writing alert and drop rules
- Customizing rule options
- Tuning performance for production use
- **Case Study:** Snort detection of Zeus Trojan

Module 4: Suricata for Threat Detection

- Suricata vs. Snort comparison
- Rule writing best practices
- Performance profiling
- EVE JSON output and logging
- Suricata with Elasticsearch/Logstash
- **Case Study:** Detecting Emotet using Suricata

Module 5: YARA Rules and Pattern Matching

- Introduction to YARA
- Creating rules for file-based detection
- Combining YARA with network monitoring
- Regular expressions and byte patterns
- Best practices for avoiding false positives
- **Case Study:** YARA analysis of Cobalt Strike beacons

Module 6: Behavioral Signature Engineering

- Behavior-based vs. static analysis
- Malware sandboxing techniques
- Process injection and registry manipulation
- Memory scanning approaches
- Behavioral rule triggers in IDS
- **Case Study:** Detecting TrickBot with behavioral signatures

Module 7: Threat Intelligence Integration

- Types of threat intelligence feeds
- Automating signature enrichment
- STIX, TAXII protocols
- IOC correlation with signatures
- Using open-source feeds like MISP
- **Case Study:** Integrating abuse.ch feed for ransomware detection

Module 8: Reverse Engineering Malware for Signatures

- Introduction to static/dynamic reverse engineering
- Using Ghidra/IDA Pro for binary analysis
- Extracting string and opcode patterns
- Code obfuscation and evasion techniques
- Signature generation from binary analysis
- **Case Study:** Reverse engineering a cryptojacker

Module 9: Detecting Encrypted Malware Traffic

- Identifying anomalies in encrypted channels
- Certificate analysis and JA3 fingerprinting
- TLS fingerprinting tools
- SSH and DNS tunneling detection

- Pattern matching in encrypted payload metadata
- **Case Study:** Detecting HTTPS-based RAT using JA3

Module 10: PCAP Analysis and Malware Identification

- Capturing and filtering traffic
- Reconstructing sessions
- Identifying malicious payloads
- Payload extraction for sandboxing
- Using Zeek/Bro for flow analysis
- **Case Study:** Malware exfiltration via FTP in PCAP

Module 11: Machine Learning in Malware Signature Detection

- Basics of ML in security
- Supervised vs. unsupervised learning
- Feature extraction from network data
- Training models on labeled signatures
- Anomaly detection with ML models
- **Case Study:** ML-assisted malware signature classification

Module 12: Automating Signature Pipelines

- Automating with Python and Bash
- Using GitLab CI/CD for updates
- Scheduled rule deployment
- Signature validation frameworks
- Logging and auditing automation
- **Case Study:** CI/CD pipeline for daily Suricata rule updates

Module 13: Signature Evasion and Counter-Evasion

- Common evasion techniques
- Polymorphic and metamorphic malware
- Signature obfuscation
- Mitigation strategies
- Updating rules against evasion
- **Case Study:** Evasion tactics used in LokiBot

Module 14: Incident Response Using Signatures

- Steps of incident handling
- Signature use in detection and containment
- Retrospective analysis with signatures
- Forensic correlation with other logs
- Documentation and reporting
- **Case Study:** Real-life ransomware breach detection via IDS signatures

Module 15: Building Scalable Malware Detection Infrastructure

- Infrastructure planning for detection systems
- Cloud vs. on-premise deployment
- Load balancing and redundancy
- Log centralization and SIEM integration
- Maintenance and signature updates
- **Case Study:** Large-scale deployment in a government SOC

Training Methodology

- Instructor-led theoretical sessions
- Real-world case studies with hands-on labs
- Use of open-source and enterprise-grade tools
- Scenario-based learning using malware simulation
- Daily quizzes and post-module assessments
- Capstone project: Full malware detection lifecycle simulation

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
21 Sep 2026	02 Oct 2026	Physical	$0
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

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

Register Online Now

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