Training Course on Dynamic Malware Analysis and Sandboxing

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 cybersecurity landscape, sophisticated malware threats such as fileless attacks, polymorphic malware, and zero-day exploits continue to evolve. Training Course on Dynamic Malware Analysis and Sandboxing equips cybersecurity professionals with the advanced skills necessary to detect, analyze, and neutralize these threats in real-time environments. Through hands-on labs and sandbox-based investigations, participants will gain a deep understanding of malware behavior, threat emulation, reverse engineering, and behavioral analysis.

With the rise of Advanced Persistent Threats (APTs) and evasive malware, this course provides essential training for threat hunters, SOC analysts, and malware analysts. Leveraging modern sandboxing tools and dynamic analysis platforms, learners will explore the internals of malware in isolated environments, safely mimicking attack scenarios for comprehensive behavioral insight.

Programme Curriculum

Training Course on Dynamic Malware Analysis and Sandboxing

Introduction

In today’s cybersecurity landscape, sophisticated malware threats such as fileless attacks, polymorphic malware, and zero-day exploits continue to evolve. Training Course on Dynamic Malware Analysis and Sandboxing equips cybersecurity professionals with the advanced skills necessary to detect, analyze, and neutralize these threats in real-time environments. Through hands-on labs and sandbox-based investigations, participants will gain a deep understanding of malware behavior, threat emulation, reverse engineering, and behavioral analysis.

With the rise of Advanced Persistent Threats (APTs) and evasive malware, this course provides essential training for threat hunters, SOC analysts, and malware analysts. Leveraging modern sandboxing tools and dynamic analysis platforms, learners will explore the internals of malware in isolated environments, safely mimicking attack scenarios for comprehensive behavioral insight.

Course Objectives

1. Understand the fundamentals of dynamic malware analysis
2. Use sandboxing technology to detect evasive threats
3. Analyze polymorphic and metamorphic malware behavior
4. Detect fileless malware and memory-resident attacks
5. Deploy virtualized environments for threat containment
6. Perform API call and registry activity tracing
7. Monitor network communication of malware samples
8. Integrate dynamic analysis with incident response workflows
9. Identify evasion techniques used by modern malware
10. Correlate behavioral indicators with malware classification
11. Apply threat intelligence enrichment to analysis findings
12. Use tools like Cuckoo Sandbox and Any.Run effectively
13. Conduct end-to-end dynamic analysis lab simulations

Target Audiences

1. Malware Analysts
2. Cybersecurity Researchers
3. Threat Intelligence Teams
4. SOC Analysts
5. Incident Response Teams
6. Digital Forensics Experts
7. Penetration Testers
8. Network Security Engineers

Course Duration: 5 days

Course Modules

Module 1: Introduction to Dynamic Malware Analysis

- Basics of static vs dynamic analysis
- The malware lifecycle
- Virtualization for safe analysis
- Behavioral analysis foundations
- Introduction to sandbox environments
- **Case Study**: Analyzing a basic keylogger in a virtual sandbox

Module 2: Sandboxing Technology Deep Dive

- Architecture of sandboxing platforms
- Cloud vs on-premise sandboxes
- Evading sandbox detection
- Automated vs manual sandbox analysis
- Integrating sandboxing into SOC operations
- **Case Study**: Investigating ransomware using Cuckoo Sandbox

Module 3: Malware Behavioral Analysis

- Monitoring system calls and processes
- Registry and file system changes
- Memory forensics in dynamic analysis
- Using ProcMon and Wireshark

- Behavior-based detection indicators (IOCs)
- **Case Study**: Behavioral analysis of a trojan downloader

Module 4: Network and API Monitoring

- API hooking and DLL injection
- Interpreting API call chains
- Command & Control (C2) communication patterns
- Detecting data exfiltration
- Analyzing encrypted traffic behavior
- **Case Study**: Uncovering a backdoor through API activity

Module 5: Evasive Malware and Anti-Analysis Techniques

- Sandbox-aware malware behavior
- Anti-VM and anti-debugging tactics
- Code obfuscation and packers
- Tactics for bypassing behavior detection
- Strategies to counter evasive samples
- **Case Study**: Malware sample evading automated sandbox

Module 6: Integration with Threat Intelligence

- Enriching sandbox results with TI feeds
- Mapping IOCs to MITRE ATT&CK
- Pivoting across malware families
- Leveraging YARA rules for classification
- Automating threat reporting
- **Case Study**: Enriching sandbox output with MISP

Module 7: Tools and Platforms for Dynamic Analysis

- Overview of dynamic analysis tools
- Cuckoo, Any.Run, Joe Sandbox, Hybrid Analysis
- Setting up and configuring tools
- Tool comparison and limitations
- Open-source vs commercial solutions
- **Case Study**: Building a custom sandbox workflow

Module 8: End-to-End Malware Analysis Simulation

- Preparing a safe lab environment
- Analyzing an advanced persistent threat
- Documenting findings and indicators
- Mitigation strategies based on results
- Reporting and communicating with stakeholders
- **Case Study**: Full dynamic analysis of APT malware

Training Methodology

- Instructor-led sessions with real-world malware samples
- Hands-on virtual lab simulations
- Group-based malware analysis challenges
- Guided reverse engineering exercises
- Use of open-source and commercial sandbox tools
- Post-lab debriefing and threat modeling

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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