Training Course on Malware Triage and Classification Automation

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 ever-evolving world of cybersecurity, rapidly identifying and classifying malicious software is no longer a luxury—it's a necessity. With the sheer volume and sophistication of modern malware, organizations face critical challenges in minimizing response times and automating threat analysis. Training Course on Malware Triage and Classification Automation empowers cybersecurity professionals with the skills and tools to automate and accelerate malware identification, classification, and response processes using cutting-edge technologies like machine learning, sandboxing, YARA rules, and behavioral analytics.

This course bridges the gap between manual malware analysis and fully automated, intelligence-driven triage systems. Participants will learn how to leverage advanced tools and frameworks to build scalable and responsive triage systems, streamline threat intelligence integration, and deploy real-time malware detection pipelines. Through hands-on labs, real-world case studies, and interactive modules, learners will develop the expertise to future-proof their organization’s malware response capabilities.

Programme Curriculum

Training Course on Malware Triage and Classification Automation

Introduction

In the ever-evolving world of cybersecurity, rapidly identifying and classifying malicious software is no longer a luxury—it's a necessity. With the sheer volume and sophistication of modern malware, organizations face critical challenges in minimizing response times and automating threat analysis. Training Course on Malware Triage and Classification Automation empowers cybersecurity professionals with the skills and tools to automate and accelerate malware identification, classification, and response processes using cutting-edge technologies like machine learning, sandboxing, YARA rules, and behavioral analytics.

This course bridges the gap between manual malware analysis and fully automated, intelligence-driven triage systems. Participants will learn how to leverage advanced tools and frameworks to build scalable and responsive triage systems, streamline threat intelligence integration, and deploy real-time malware detection pipelines. Through hands-on labs, real-world case studies, and interactive modules, learners will develop the expertise to future-proof their organization's malware response capabilities.

Course Objectives

1. Understand automated malware triage techniques and frameworks
2. Utilize AI-driven malware classification models effectively
3. Apply sandboxing and dynamic analysis for behavior-based detection
4. Implement YARA rules for efficient threat identification
5. Integrate machine learning in cybersecurity workflows
6. Identify APT threats through automated pattern recognition
7. Build and deploy malware detection pipelines using open-source tools
8. Leverage MITRE ATT&CK mapping for malware attribution
9. Analyze polymorphic and metamorphic malware variants
10. Automate malware forensics and reverse engineering tasks
11. Design an effective malware triage workflow for enterprise use
12. Integrate SIEM and threat intelligence platforms
13. Evaluate and optimize malware classification models using performance metrics

Target Audience

1. Cybersecurity Analysts
2. Malware Researchers
3. Threat Intelligence Specialists
4. Incident Response Teams
5. Network Security Engineers
6. Forensic Analysts
7. SOC Team Members
8. Penetration Testers and Ethical Hackers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware Triage Automation

- Importance of rapid malware analysis
- Overview of triage techniques
- Manual vs. automated triage
- Common malware behavior traits
- Tools landscape and evolution
- **Case Study: A ransomware outbreak mitigated using triage automation**

Module 2: Malware Classification Fundamentals

- Static vs. dynamic analysis
- Taxonomy of malware families
- Feature extraction techniques
- Labeling datasets for classifiers
- Signature vs. behavior-based approaches
- **Case Study: Detecting an unknown dropper using classification logic**

Module 3: Machine Learning for Malware Detection

- Supervised learning techniques
- Dataset preparation and validation
- Feature engineering for malware traits
- Model evaluation and tuning
- Addressing adversarial machine learning
- **Case Study: Using Random Forest to classify trojans in real-time**

Module 4: Sandboxing and Dynamic Analysis

- Architecture of sandbox environments
- Behavior capture and logging
- Detection evasion by malware
- Choosing sandboxing platforms
- Analyzing process, registry, and file changes
- **Case Study: Analysis of a stealthy keylogger in Cuckoo Sandbox**

Module 5: YARA Rules and Threat Detection

- Writing effective YARA rules
- Pattern-matching and strings
- Rule testing and tuning
- Integration with triage systems
- Community-driven rule repositories
- **Case Study: Preventing Emotet infections using advanced YARA detection**

Module 6: Automated Malware Triage Pipelines

- Building triage automation workflows
- Input/output channels (SIEM, EDR)
- Integrating sandbox, classifiers, and alerts
- Logging and auditing automation flows
- Failover and exception handling
- **Case Study: Streamlining alerts for zero-day threats using triage pipelines**

Module 7: Behavioral Analysis and Heuristics

- Anomaly detection in behavior traces
- Building heuristics models
- Comparison to known malware behavior
- Temporal and context correlation
- Reducing false positives
- **Case Study: Heuristic-based detection of PowerShell-based malware**

Module 8: Threat Intelligence Integration

- Connecting to threat feeds (MISP, STIX/TAXII)
- Consuming IOCs for malware detection
- Mapping threats with MITRE ATT&CK
- Enriching triage data with context
- Bidirectional intelligence sharing
- **Case Study: Responding to a global campaign with TI-enhanced triage**

Module 9: Polymorphic and Metamorphic Malware Handling

- Obfuscation and packing techniques

- Detection through entropy and signatures
- Unpacking and emulation tools
- Limitations of traditional AV
- Advanced classification strategies
- **Case Study: Deobfuscating a polymorphic worm with automation**

Module 10: Reverse Engineering in Automated Environments

- Basics of malware reverse engineering
- Static disassembly automation
- Extracting IOCs from binary
- Binary similarity comparison
- IDA, Ghidra, and other tools
- **Case Study: Automating malware unpacking in RE pipeline**

Module 11: SIEM and SOAR Integration

- Feeding triage output to SIEM
- Automating response with SOAR
- Alert prioritization via classification score
- Playbook development for malware
- Chaining alerts into incidents
- **Case Study: Enhancing SOC efficiency through triage-SOAR integration**

Module 12: Performance Evaluation and Metrics

- Defining success in malware automation
- Confusion matrix and ROC analysis
- Comparing model architectures
- Reduction of triage time metrics
- Cost-benefit analysis of automation
- **Case Study: Benchmarking manual vs. automated classification accuracy**

Module 13: Compliance, Ethics, and Legal Considerations

- Data privacy in malware analysis
- Compliance with cyber laws (GDPR, CCPA)
- Ethical analysis of malware samples
- Responsibility in automation
- Securing triage environments
- **Case Study: Legal challenge involving sandbox logs as evidence**

Module 14: Advanced Threat Hunting with Triage Data

- Proactive hunting with behavior patterns
- Querying triage results in threat hunts
- Correlation with historical data
- Combining manual and automated hunting
- Reporting and documentation
- **Case Study: Discovering a long-standing APT using triaged indicators**

Module 15: Capstone Project and Final Assessment

- Design your own triage workflow
- Build a lightweight classifier
- Integrate sandbox and intelligence feeds

- Present findings in a simulated SOC
- Peer review and feedback
- **Case Study: Final project review simulating real-world incident response**

Training Methodology

- **Instructor-led live sessions** with real-world examples
- **Hands-on labs** in sandboxed and virtualized environments
- **Case study-driven learning** to reinforce key concepts
- **Assessment quizzes** and capstone project for practical evaluation
- **Collaborative workshops** for interactive problem-solving
- **Tool walkthroughs and guided implementation** using open-source platforms

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	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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