Training Course on Automating Malware Analysis Workflows

Professional Development Training Course Outline

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

Course Introduction

The rapid escalation in sophisticated cyber threats has amplified the need for advanced and scalable malware analysis strategies. Automating malware analysis workflows is now essential to reduce time-to-detection, increase efficiency, and streamline threat intelligence operations. Training Course on Automating Malware Analysis Workflows is tailored for cybersecurity professionals, malware analysts, and SOC engineers seeking to revolutionize their incident response, reverse engineering, and malware triage processes through automation, scripting, and cloud-based integrations. By integrating tools like YARA, Cuckoo Sandbox, Cortex, and MITRE ATT&CK, this training emphasizes hands-on learning and real-world automation pipelines.

As organizations combat ransomware, APTs, and polymorphic malware, manual methods are no longer scalable. This course offers a practical guide to automating repetitive malware analysis tasks using Python scripting, containerized environments, and workflow orchestration. Learners will build end-to-end pipelines that ingest, analyze, and report malicious activity with speed and precision. Each module includes interactive labs and case studies based on real-world malware samples, providing participants with a competitive advantage in cyber defense operations.

Programme Curriculum

Training Course on Automating Malware Analysis Workflows

Introduction

The rapid escalation in sophisticated cyber threats has amplified the need for advanced and scalable malware analysis strategies. Automating malware analysis workflows is now essential to reduce time-to-detection, increase efficiency, and streamline threat intelligence operations. Training Course on Automating Malware Analysis Workflows is tailored for cybersecurity professionals, malware analysts, and SOC engineers seeking to revolutionize their incident response, reverse engineering, and malware triage processes through automation, scripting, and cloud-based integrations. By integrating tools like YARA, Cuckoo Sandbox, Cortex, and MITRE ATT&CK, this training emphasizes hands-on learning and real-

world automation pipelines.

As organizations combat ransomware, APTs, and polymorphic malware, manual methods are no longer scalable. This course offers a practical guide to automating repetitive malware analysis tasks using Python scripting, containerized environments, and workflow orchestration. Learners will build end-to-end pipelines that ingest, analyze, and report malicious activity with speed and precision. Each module includes interactive labs and case studies based on real-world malware samples, providing participants with a competitive advantage in cyber defense operations.

Course Objectives

1. Understand the fundamentals of malware types and behavioral analysis.
2. Explore key automation tools for scalable malware triage.
3. Configure and deploy Cuckoo Sandbox for automated dynamic analysis.
4. Automate static analysis using YARA rules and PE analysis frameworks.
5. Develop Python scripts for malware classification and labeling.
6. Integrate automated workflows with threat intelligence feeds.
7. Build automation pipelines using SOAR platforms and Cortex analyzers.
8. Utilize MITRE ATT&CK mapping for tactic and technique correlation.
9. Implement automated report generation with STIX/TAXII standards.
10. Automate the collection of IOCs and artifacts from sandbox environments.
11. Apply containerization (Docker) for reproducible malware analysis labs.
12. Leverage cloud services (e.g., AWS Lambda, VirusTotal API) for scalable automation.
13. Evaluate automation strategies through red-teaming and blue-teaming use cases.

Target Audience

1. Malware Analysts
2. SOC Engineers
3. Cybersecurity Researchers
4. Threat Intelligence Analysts
5. Incident Responders
6. Penetration Testers
7. Digital Forensics Professionals
8. IT Security Administrators

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware Automation

- Overview of malware analysis lifecycle
- Limitations of manual analysis
- Benefits of automation in threat environments
- Key tools and technologies
- Automation use cases
- **Case Study:** Automating ransomware family detection

Module 2: Static Analysis Automation

- PE file structure overview
- YARA rules and their automation
- Feature extraction using tools like PEStudio
- Batch scanning with automated scripts
- Signature-based detection pipelines

- **Case Study:** Using YARA rules to classify Emotet variants

Module 3: Dynamic Analysis with Cuckoo Sandbox

- Deploying Cuckoo in virtual environments
- Automation via task scheduling and submission APIs
- Collecting runtime artifacts
- Automating behavioral logs parsing
- Integrating Cuckoo results with dashboards
- **Case Study:** Automating Cuckoo for trojan behavior profiling

Module 4: Python for Malware Analysis

- Scripting malware feature extraction
- Automating hash comparison
- Writing batch file renaming/cleanup tools
- Automating IOC extraction
- Using Python libraries (pefile, yara-python)
- **Case Study:** Python script for multi-family sample classification

Module 5: IOC Collection and Enrichment

- Automated extraction of IPs/domains/URLs
- Integrating with VirusTotal API
- Enriching data with WHOIS/DNS info
- IOC correlation and deduplication
- Visualization of IOC networks
- **Case Study:** IOC automation pipeline for phishing malware

Module 6: Threat Intelligence Integration

- Threat feeds and formats (STIX, TAXII)
- Enriching malware context with MISP
- Automating IOC ingestion into SIEM/SOAR
- Linking malware to campaigns
- Custom threat intel dashboards
- **Case Study:** MITRE ATT&CK mapping via automated feed enrichment

Module 7: Cloud Automation for Malware Analysis

- Using AWS Lambda and GCP Functions
- Storage and task automation via S3, Cloud Functions
- API-based sandbox submissions
- Autoscaling malware processing
- Cost-efficient analysis at scale
- **Case Study:** AWS-based automated malware scanning system

Module 8: Workflow Orchestration with SOAR

- SOAR introduction (Cortex XSOAR, TheHive)
- Automating response to malicious attachments
- Integration with analysis tools
- Designing playbooks
- Alert enrichment workflows
- **Case Study:** Automated phishing response playbook

Module 9: Building Analysis Pipelines

- Architecting modular analysis flows
- File ingestion pipelines
- Automated task chaining
- Logging and error handling
- Notification and alerting setup
- **Case Study:** End-to-end pipeline for malicious PDF detection

Module 10: Sandboxing at Scale

- Sandbox deployment automation
- Using open-source and commercial sandboxes
- Load balancing and queueing
- Analyzing evasive malware
- API-based orchestration
- **Case Study:** High-volume sandbox cluster for worm detection

Module 11: Visualization and Reporting Automation

- Auto-generating threat reports
- Dashboards using Kibana/Grafana
- Automated PDF/HTML report builders
- Integrating charts and graphs
- Stakeholder-friendly output formats
- **Case Study:** Report generation for executive SOC briefings

Module 12: MITRE ATT&CK Integration

- Mapping tactics, techniques, procedures
- Automating coverage analysis
- ATT&CK Navigator integration
- Gap identification in detection
- Reporting automation based on ATT&CK
- **Case Study:** Mapping malware family to ATT&CK matrix

Module 13: Containerizing Malware Labs

- Docker basics for malware analysis
- Container security for safe sample handling
- Automating lab setup with Docker Compose
- Version control with containers
- Cloud-based lab deployments
- **Case Study:** Dockerized Cuckoo environment for team training

Module 14: Real-Time Alerting and Notifications

- Triggering alerts via Slack/Email/Webhooks
- Monitoring analysis queue and results
- Escalation workflows
- Prioritization rules
- Reducing alert fatigue with filters
- **Case Study:** Slack bot for real-time malware alerts

Module 15: Advanced Use Cases and Red Teaming

- Using automation in red team operations
- Creating evasive malware with automation

- Simulating attacks for blue team validation
- Automation as a detection evasion strategy
- Testing SOC workflows under stress
- **Case Study:** Red team automation simulating APT techniques

Training Methodology

- Hands-on Labs: Real-world malware samples, sandbox execution, and automation scripting.
- Interactive Demos: Guided simulations of end-to-end workflow automation.
- Case Studies: Detailed analysis of real incidents to contextualize automation benefits.
- Assessments: Quizzes and challenges to reinforce key concepts.
- Capstone Project: Participants build and present a fully automated malware analysis workflow.

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