Training Course on Cloud-Based Malware Analysis Environments

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$2,200 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As cyberattacks continue to evolve in sophistication, leveraging cloud-based environments for malware analysis has become a crucial skill for cybersecurity professionals, threat hunters, and digital forensics experts. Training Course on Cloud-Based Malware Analysis Environments equips learners with the knowledge to deploy, manage, and utilize scalable cloud-based sandboxing systems, behavioral malware analysis tools, and automation frameworks. It integrates real-world case studies, advanced malware detection techniques, and hybrid analysis methodologies aligned with global threat intelligence platforms.

The course focuses on building resilient and elastic environments for static and dynamic malware analysis, cloud automation, and cross-platform threat detection. Designed with trending cybersecurity standards, it addresses real-time incident response, AI-powered malware classification, and DevSecOps integration. Whether you are working in blue team operations, SOC, or malware reverse engineering, this course provides a future-ready skillset aligned with modern threat landscapes.

Programme Curriculum

Training Course on Cloud-Based Malware Analysis Environments

Introduction

As cyberattacks continue to evolve in sophistication, leveraging cloud-based environments for malware analysis has become a crucial skill for cybersecurity professionals, threat hunters, and digital forensics experts. Training Course on Cloud-Based Malware Analysis Environments equips learners with the knowledge to deploy, manage, and utilize scalable cloud-based sandboxing systems, behavioral malware analysis tools, and automation frameworks. It integrates real-world case studies, advanced malware detection techniques, and hybrid analysis methodologies aligned with global threat intelligence platforms.

The course focuses on building resilient and elastic environments for static and dynamic malware analysis, cloud automation, and cross-platform threat detection. Designed with trending cybersecurity standards, it addresses real-time incident response, AI-powered malware classification, and DevSecOps integration. Whether you are working in blue team operations, SOC, or malware reverse engineering, this course provides a future-ready skillset aligned with modern threat landscapes.

Objectives

1. Understand fundamentals of cloud-based malware analysis environments
2. Set up automated sandboxing solutions using cloud technologies
3. Analyze malware through dynamic and static analysis in cloud VMs
4. Integrate threat intelligence feeds into cloud-based analysis pipelines
5. Deploy malware detonation environments on AWS, Azure, and GCP
6. Use AI/ML for malware behavior classification
7. Implement real-time detection and alerting systems
8. Learn memory forensics and process injection analysis in cloud setups
9. Apply containerized analysis environments using Docker and Kubernetes
10. Detect zero-day malware using behavioral signatures
11. Leverage cloud automation for scalable incident response
12. Integrate SIEM and SOAR tools with malware analysis workflows
13. Perform secure data logging and evidence preservation

Target Audiences

1. Cybersecurity Analysts
2. Malware Reverse Engineers
3. Incident Responders
4. SOC Analysts
5. Penetration Testers
6. Cloud Security Engineers
7. Threat Intelligence Professionals
8. IT Risk Managers

Course Duration: 10 days

Course Modules

Module 1: Introduction to Malware Analysis in the Cloud

- Cloud computing and malware detection
- Benefits of remote malware analysis
- Threat landscape overview
- Common malware variants
- Essential analysis tools
- **Case Study**: Analyzing a phishing trojan via Google Cloud

Module 2: Static Malware Analysis Basics

- Binary unpacking
- File signature detection
- Hashing algorithms
- Code analysis tools
- PE structure overview
- **Case Study**: Investigating a ransomware sample statically

Module 3: Dynamic Malware Analysis in the Cloud

- Behavioral sandboxing
- Process monitoring
- File system activity logs
- API call tracing
- Anti-evasion detection
- **Case Study**: Remote detonation of a keylogger in AWS sandbox

Module 4: Memory Forensics and Malware Artifacts

- Volatility framework setup
- Memory image acquisition
- Detecting injected code
- Analyzing suspicious DLLs
- Memory dump automation
- **Case Study**: Memory analysis of a credential-stealing trojan

Module 5: Cloud Sandboxing Solutions

- Cuckoo sandbox in the cloud
- Integration with cloud storage
- Detonation environment setup
- Automated logging
- Web-based report generation
- **Case Study**: Multi-sandbox comparative malware evaluation

Module 6: Using Threat Intelligence with Malware Analysis

- Integrating MISP
- Correlating malware indicators
- IOC extraction techniques
- Feed integration via APIs
- Intelligence-driven detection
- **Case Study**: Threat intelligence-based campaign attribution

Module 7: Containerized Malware Labs

- Docker-based malware isolation
- Kubernetes pod security
- Immutable infrastructure benefits
- Orchestration best practices
- CI/CD pipeline integration
- **Case Study**: Malware detonation using Docker Compose

Module 8: Cloud Automation for Analysis Workflows

- Scripting in Python for automation
- Lambda functions for task scheduling
- Automated snapshot and rollback
- Workflow triggers and alerting
- Security policy enforcement
- **Case Study**: Serverless malware report generation pipeline

Module 9: Network Behavior Analysis

- PCAP capture in cloud labs

- DNS tunneling and callbacks
- Identifying C2 communication
- Anomaly detection
- Flow-based traffic analysis
- **Case Study**: Botnet detection in a hybrid cloud lab

Module 10: Reverse Engineering Malware

- Assembly basics and tools
- Using Ghidra and IDA in VMs
- Code obfuscation techniques
- String decryption
- Packer detection and bypass
- **Case Study**: Reverse engineering a remote access trojan

Module 11: Detection of Advanced Persistent Threats (APTs)

- Understanding APT tactics
- Malware staging and persistence
- Long dwell-time indicators
- Registry and service manipulation
- Lateral movement detection
- **Case Study**: Tracking APT malware in a hybrid environment

Module 12: Integration with SIEM/SOAR

- Data normalization
- Alert enrichment
- Workflow automation
- Cross-tool communication
- Custom rule creation
- **Case Study**: End-to-end workflow of malware alert to SOAR playbook

Module 13: Reporting and Visualization

- Report automation tools
- JSON and HTML formatting
- Graph-based malware relation mapping
- IOC report generation
- Integration with dashboard tools
- **Case Study**: Visualizing malware campaign using Kibana

Module 14: Zero-Day Malware Detection Techniques

- Behavioral modeling
- Emulation-based analysis
- ML-based anomaly detection
- Exploit detection frameworks
- Code similarity analysis
- **Case Study**: Detecting polymorphic malware using behavior signatures

Module 15: Legal, Ethical, and Compliance Aspects

- Data privacy in cloud analysis
- Regulatory concerns (GDPR, HIPAA)
- Chain of custody practices

- Secure evidence storage
- Legal implications of malware handling
- **Case Study**: Legal analysis of cross-border malware investigation

Training Methodology

- Instructor-led virtual labs with step-by-step guidance
- Hands-on assignments using AWS, Azure, and GCP environments
- Interactive case study deconstruction
- Downloadable reference materials and scripts
- Real-time collaboration and peer review sessions
- Post-course assessment and certification

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254724527104*

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
10 Aug 2026	21 Aug 2026	Online	$2,200
17 Aug 2026	28 Aug 2026	Online	$2,200
24 Aug 2026	04 Sep 2026	Online	$2,200

Start Date	End Date	Location	Price
31 Aug 2026	11 Sep 2026	Online	$2,200
07 Sep 2026	18 Sep 2026	Online	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200
28 Sep 2026	09 Oct 2026	Online	$2,200

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

Register Online Now

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