Training Course on AI/ML for Malware Detection and Classification

Professional Development Training Course Outline

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

Course Introduction

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing the cybersecurity landscape, offering cutting-edge solutions for malware detection and classification. With the explosive growth of sophisticated cyber threats, conventional antivirus techniques are no longer sufficient. Training Course on AI ML for Malware Detection and Classification is designed to equip cybersecurity professionals, data scientists, and IT leaders with the advanced skills necessary to implement AI/ML-based malware detection techniques. Through hands-on labs, real-world case studies, and theoretical foundations, participants will gain actionable insights into threat modeling, neural network development, and anomaly detection.

This program offers comprehensive coverage of deep learning algorithms, supervised and unsupervised learning methods, malware feature extraction, and real-time threat prediction. With a focus on modern attack vectors, polymorphic malware, and evasion techniques, this training provides essential knowledge and tools for defending enterprise networks. By the end of the course, attendees will be able to design and deploy intelligent threat detection systems capable of identifying and classifying known and unknown malware in real-time environments.

Programme Curriculum

Training Course on AI/ML for Malware Detection and Classification

Introduction

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing the cybersecurity landscape, offering cutting-edge solutions for malware detection and classification. With the explosive growth of sophisticated cyber threats, conventional antivirus techniques are no longer sufficient. Training Course on AI ML for Malware Detection and Classification is designed to equip cybersecurity professionals, data scientists, and IT leaders with the advanced skills necessary to implement AI/ML-based malware detection techniques. Through hands-on labs, real-world case studies, and theoretical foundations, participants will gain actionable insights into threat modeling, neural network development, and

anomaly detection.

This program offers comprehensive coverage of deep learning algorithms, supervised and unsupervised learning methods, malware feature extraction, and real-time threat prediction. With a focus on modern attack vectors, polymorphic malware, and evasion techniques, this training provides essential knowledge and tools for defending enterprise networks. By the end of the course, attendees will be able to design and deploy intelligent threat detection systems capable of identifying and classifying known and unknown malware in real-time environments.

Course Objectives

1. Understand the fundamentals of AI and machine learning in cybersecurity.
2. Learn the taxonomy and classification of malware types and behaviors.
3. Develop ML-based models for signatureless malware detection.
4. Apply supervised, unsupervised, and reinforcement learning to malware analysis.
5. Extract and engineer features from malware datasets.
6. Analyze datasets using tools like VirusShare, VirusTotal, and EMBER.
7. Use neural networks, SVM, and deep learning models for malware classification.
8. Detect zero-day threats using anomaly-based ML algorithms.
9. Evaluate model performance using precision, recall, and confusion matrix.
10. Understand evasion tactics and adversarial ML in malware detection.
11. Leverage AutoML tools for rapid model prototyping.
12. Implement scalable threat detection pipelines in cloud-based environments.
13. Conduct malware forensics using AI-assisted classification models.

Target Audiences

1. Cybersecurity Analysts
2. SOC Engineers
3. Malware Researchers
4. AI/ML Engineers
5. Threat Intelligence Specialists
6. IT Security Managers
7. Penetration Testers
8. Incident Response Teams

Course Duration: 10 days

Course Modules

Module 1: Introduction to AI and Machine Learning in Cybersecurity

- Overview of AI/ML fundamentals
- Cybersecurity landscape and malware evolution
- Importance of intelligent threat detection
- AI/ML roles in SOC environments
- Tools and platforms used
- **Case Study:** Evolution of malware detection from 2000s to present

Module 2: Malware Fundamentals and Classification

- Types of malware (worms, trojans, ransomware, etc.)
- Static vs dynamic analysis
- Malware behaviors and attack vectors
- Obfuscation and polymorphism
- Real-time detection challenges

- **Case Study:** WannaCry ransomware behavior analysis

Module 3: Feature Extraction from Malware

- Importance of feature engineering
- PE headers, opcodes, API calls
- Static feature extraction tools
- Dynamic analysis and sandboxing
- Labeling and preprocessing datasets
- **Case Study:** Feature selection for EMBER dataset

Module 4: Supervised Learning for Malware Detection

- Classification algorithms overview
- Decision trees, random forests, SVMs
- Labeling malware datasets
- Training and validation
- Overfitting and model tuning
- **Case Study:** SVM model for classifying ransomware

Module 5: Unsupervised Learning Techniques

- Clustering malware families
- Dimensionality reduction (PCA, t-SNE)
- Outlier detection
- Similarity detection
- Visualizing clustering results
- **Case Study:** Uncovering malware variants with K-means

Module 6: Deep Learning for Malware Analysis

- CNNs and RNNs for sequence data
- Handling binary files as images
- LSTM for time-series behavior
- Transfer learning for malware datasets
- Building deep nets with TensorFlow/PyTorch
- **Case Study:** Image-based CNN malware classifier

Module 7: Anomaly Detection and Zero-Day Threats

- Anomaly detection methods
- Gaussian models and One-Class SVM
- Autoencoders and reconstruction errors
- Behavioral anomaly modeling
- Identifying zero-day exploits
- **Case Study:** Detecting zero-day with unsupervised autoencoders

Module 8: Adversarial Machine Learning

- Adversarial example generation
- Evasion attacks on classifiers
- Robust model training
- Defense strategies against adversarial inputs
- Model interpretability techniques
- **Case Study:** Evasion of deep learning malware classifier

Module 9: Malware Datasets and Benchmarking

- Public malware datasets overview
- Dataset curation and challenges
- Balancing and cleaning data
- Benchmarking and metrics
- Dataset licensing and ethics
- **Case Study:** Comparative analysis using EMBER and Malimg

Module 10: Evaluating AI/ML Models

- Confusion matrix, F1-score, ROC
- Cross-validation and grid search
- Real-time performance monitoring
- Explainable AI techniques
- Debugging underperforming models
- **Case Study:** Performance evaluation of CNN vs Random Forest

Module 11: AutoML in Malware Detection

- What is AutoML and its benefits
- Tools: Google AutoML, H2O.ai, TPOT
- Configuring AutoML pipelines
- Feature selection automation
- Hyperparameter optimization
- **Case Study:** Rapid model development using H2O AutoML

Module 12: Malware Detection in Cloud Environments

- Cloud-native security challenges
- Using AI in AWS/Azure/GCP environments
- CI/CD for security ML models
- Streaming data ingestion for detection
- Cloud logging and analysis
- **Case Study:** Deploying AI-based detection in AWS Lambda

Module 13: Threat Intelligence and AI Integration

- Threat intelligence platforms (TIPs)
- Integrating ML with TI feeds
- IOC extraction and enrichment
- Real-time alerting with AI logic
- Threat hunting automation
- **Case Study:** Enhancing TI with ML-based enrichment

Module 14: Explainable and Ethical AI in Malware Analysis

- Need for explainable AI in cybersecurity
- Tools for model explainability (SHAP, LIME)
- Ethical concerns in malware data use
- AI bias in classification
- Regulatory and privacy considerations
- **Case Study:** Ethical implications of malware model deployment

Module 15: Capstone Project and Practical Lab

- Full project: Design malware detection pipeline
- Dataset selection and labeling

- Model training, tuning, and evaluation
- Deployment on a simulated environment
- Presentation and peer review
- **Case Study:** End-to-end pipeline using real malware samples

Training Methodology

- Interactive lectures with industry experts
- Hands-on labs and exercises with real datasets
- Group discussions and live Q&A sessions
- Access to cloud-based virtual labs
- Real-world case studies and capstone projects
- Course certification upon completion

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