AI and Machine Learning for Cybercrime Detection Training Course

Professional Development Training Course Outline

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

Course Introduction

As cybercrime rapidly evolves, traditional detection techniques struggle to keep up with sophisticated and adaptive threats. The integration of Artificial Intelligence (AI) and Machine Learning (ML) offers a transformative edge in cybercrime detection, enabling real-time threat intelligence, predictive analytics, anomaly detection, and automated incident response. Training Course on AI & Machine Learning for Cybercrime Detection is designed to empower cybersecurity professionals, law enforcement personnel, and IT specialists with cutting-edge knowledge and practical skills in applying AI and ML to detect and counter cyber threats.

With the rise of deepfake technology, AI-powered phishing, and ransomware-as-a-service (RaaS), this training equips learners with the tools to recognize and mitigate these modern threats effectively. Emphasis is placed on hands-on application using real-world datasets, supervised and unsupervised learning models, natural language processing (NLP), and neural network-based threat detection. Learners will explore the ethical implications, data privacy concerns, and operational frameworks necessary for deploying AI responsibly in cybersecurity environments.

Programme Curriculum

AI and Machine Learning for Cybercrime Detection Training Course

Introduction

As cybercrime rapidly evolves, traditional detection techniques struggle to keep up with sophisticated and adaptive threats. The integration of Artificial Intelligence (AI) and Machine Learning (ML) offers a transformative edge in cybercrime detection, enabling real-time threat intelligence, predictive analytics, anomaly detection, and automated incident response. AI and Machine Learning for Cybercrime Detection Training Course is designed to empower cybersecurity professionals, law enforcement personnel, and IT specialists with cutting-edge knowledge and practical skills in applying AI and ML to detect and counter cyber threats.

With the rise of deepfake technology, AI-powered phishing, and ransomware-as-a-service (RaaS), this training equips learners with the tools to recognize and mitigate these modern threats effectively. Emphasis is placed on hands-on application using real-world datasets, supervised and unsupervised learning models, natural language processing (NLP), and neural network-based threat detection. Learners will explore the ethical implications, data privacy concerns, and operational frameworks necessary for deploying AI responsibly in cybersecurity environments.

Course Objectives

1. Understand the fundamentals of AI and Machine Learning in cybersecurity.
2. Analyze cybercrime patterns using AI-driven data analytics.
3. Implement anomaly detection systems using supervised learning.
4. Apply unsupervised machine learning models to identify hidden cyber threats.
5. Use natural language processing (NLP) to detect social engineering attacks.
6. Explore the role of neural networks and deep learning in threat detection.
7. Detect and analyze malware and ransomware using AI algorithms.
8. Design and deploy predictive analytics tools for cybercrime prevention.
9. Address ethical challenges and AI bias in cybercrime detection.
10. Evaluate real-time threat intelligence systems powered by AI.
11. Build AI-enabled incident response frameworks.
12. Integrate AI with cybersecurity tools like SIEM and SOAR.
13. Interpret legal and regulatory standards for AI in digital forensics.

Target Audiences

1. Cybersecurity Analysts
2. Law Enforcement Agencies
3. Data Scientists
4. IT Security Managers
5. Digital Forensics Experts
6. Ethical Hackers
7. Compliance Officers
8. AI & Machine Learning Engineers

Course Duration: 10 days

Course Modules

Module 1: Introduction to AI & ML in Cybersecurity

- Basics of AI and ML
- Supervised vs. unsupervised learning
- Key algorithms in cybersecurity
- Overview of cyber threats
- Cybersecurity landscape
- **Case Study: AI vs. Traditional Detection in Phishing Campaigns**

Module 2: Data Collection & Preprocessing for Cybercrime Detection

- Gathering relevant data sources
- Cleaning and normalizing datasets
- Feature selection and extraction
- Data labeling for supervised learning
- Time-series data in threat detection
- **Case Study: Dataset Preparation for Financial Fraud Detection**

Module 3: Supervised Learning Techniques in Cybercrime Analysis

- Classification models (SVM, Decision Trees)
- Training vs. testing datasets
- Model evaluation metrics
- Binary vs. multiclass classification
- Cyber threat classification
- **Case Study: Email Spam Detection using Naive Bayes**

Module 4: Unsupervised Learning & Clustering for Anomaly Detection

- Clustering techniques (K-means, DBSCAN)
- Dimensionality reduction (PCA, t-SNE)
- Detecting outliers
- Behavioral anomaly detection
- Network flow analysis
- **Case Study: Detecting Insider Threats via Clustering**

Module 5: Deep Learning for Advanced Cybercrime Detection

- Introduction to neural networks
- CNNs and RNNs in cybersecurity
- Deep learning architectures
- Overfitting and regularization
- GPU acceleration
- **Case Study: Deep Learning for Malware Classification**

Module 6: Natural Language Processing (NLP) in Cybercrime Investigation

- Text classification and sentiment analysis
- Detecting phishing through NLP
- Named entity recognition (NER)
- Chatbot and dark web analysis
- Language model tuning
- **Case Study: Phishing Email Analysis with NLP**

Module 7: AI-Driven Threat Intelligence Systems

- Threat hunting with AI
- Correlating indicators of compromise (IOCs)
- Integrating threat feeds
- Automation in threat intelligence
- Use of MITRE ATT&CK with AI
- **Case Study: Threat Intelligence Platform Using ML**

Module 8: AI for Ransomware Detection and Response

- Ransomware behavior profiling
- ML-based file encryption detection
- Monitoring unusual access patterns
- Proactive vs. reactive strategies
- Isolation and response automation
- **Case Study: Stopping Ryuk Ransomware with AI**

Module 9: Predictive Analytics for Cybercrime Prevention

- Time-series forecasting

- Regression models
- Trend analysis
- Risk scoring using ML
- Predicting zero-day exploits
- **Case Study: Predictive Risk Scoring in Healthcare Cybersecurity**

Module 10: Ethics, Bias & Accountability in AI

- AI fairness in security
- Discrimination in ML models
- Transparency and explainability (XAI)
- Auditing ML systems
- AI misuse in surveillance
- **Case Study: Biased AI in Social Media Threat Detection**

Module 11: Legal & Regulatory Aspects of AI in Cybercrime

- GDPR, CCPA, and AI implications
- AI in legal evidence gathering
- Cross-border data governance
- Digital rights and AI
- AI in law enforcement policy
- **Case Study: Legal Challenges of AI Surveillance Tools**

Module 12: Cyber Forensics with AI

- AI in digital evidence analysis
- Log and metadata analysis
- AI tools for forensic timelines
- File integrity verification
- Chain of custody with AI
- **Case Study: AI-Assisted Forensic Analysis in Financial Crimes**

Module 13: Integration of AI in Cybersecurity Tools (SIEM/SOAR)

- Overview of SIEM and SOAR
- Machine learning plugins
- Custom rule creation with AI
- Workflow automation
- Alert triage using ML
- **Case Study: AI-SIEM Integration in a Corporate Breach**

Module 14: Building AI-Powered Incident Response Systems

- Incident lifecycle automation
- AI in detection and response
- Orchestration and playbooks
- Real-time decision-making
- Recovery and mitigation
- **Case Study: AI Response to DDoS Attack**

Module 15: Future of AI in Cybercrime Detection

- AI trends in cybersecurity
- Quantum computing threats
- AI vs. AI in cyber warfare

- Cybersecurity in IoT and 5G
- Emerging ML models
- **Case Study: Predicting Cyber Threats in Smart Cities**

Training Methodology

- Interactive lectures with practical AI demonstrations
- Hands-on labs using real datasets and open-source tools
- Case study analysis for applied learning
- Group projects on AI deployment in cybersecurity scenarios
- Assessment quizzes and practical exams after each module
- Guided mentorship and career-oriented feedback sessions

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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
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

Start Date	End Date	Location	Price
28 Sep 2026	09 Oct 2026	Online	$2,200
05 Oct 2026	16 Oct 2026	Online	$2,200
12 Oct 2026	23 Oct 2026	Online	$2,200
19 Oct 2026	30 Oct 2026	Online	$2,200
26 Oct 2026	06 Nov 2026	Online	$2,200

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

Register Online Now

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