AI and Machine Learning for Cyber Defense (Blue Team) Training Course

Professional Development Training Course Outline

Category	Defense and Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

As cyber threats evolve at an unprecedented pace, Blue Team cybersecurity professionals face increasingly sophisticated attacks that demand advanced detection, response, and mitigation strategies. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as transformative technologies that enable predictive threat modeling, anomaly detection, and real-time automated defense mechanisms. AI and Machine Learning for Cyber Defense (Blue Team) Training Course equips participants with practical skills to leverage AI/ML tools for proactive cyber defense, integrating advanced analytics, behavioral threat analysis, and continuous monitoring to secure networks, endpoints, and cloud environments.

Participants will explore both the theoretical foundations and hands-on applications of AI and ML in defensive cybersecurity operations. Key focus areas include threat intelligence integration, automated incident response, anomaly detection, intrusion prevention, and AI-driven forensics. Through case studies, simulations, and practical exercises, learners gain the ability to implement machine learning pipelines, evaluate algorithm performance, and operationalize AI-driven defense strategies. By the end of the course, participants will enhance their capacity to anticipate threats, mitigate risks, and strengthen organizational cyber resilience.

Programme Curriculum

AI and Machine Learning for Cyber Defense (Blue Team) Training Course

Introduction

As cyber threats evolve at an unprecedented pace, Blue Team cybersecurity professionals face increasingly sophisticated attacks that demand advanced detection, response, and mitigation strategies. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as transformative technologies that enable predictive threat modeling, anomaly detection, and real-time automated defense mechanisms. AI and Machine

Learning for Cyber Defense (Blue Team) Training Course equips participants with practical skills to leverage AI/ML tools for proactive cyber defense, integrating advanced analytics, behavioral threat analysis, and continuous monitoring to secure networks, endpoints, and cloud environments.

Participants will explore both the theoretical foundations and hands-on applications of AI and ML in defensive cybersecurity operations. Key focus areas include threat intelligence integration, automated incident response, anomaly detection, intrusion prevention, and AI-driven forensics. Through case studies, simulations, and practical exercises, learners gain the ability to implement machine learning pipelines, evaluate algorithm performance, and operationalize AI-driven defense strategies. By the end of the course, participants will enhance their capacity to anticipate threats, mitigate risks, and strengthen organizational cyber resilience.

Course Objectives

1. Understand the fundamentals of AI and Machine Learning in cybersecurity defense.
2. Explore supervised, unsupervised, and reinforcement learning applications for threat detection.
3. Apply anomaly detection techniques to identify malicious activity.
4. Implement predictive modeling for intrusion detection and prevention.
5. Integrate threat intelligence with AI/ML-driven defense mechanisms.
6. Design and deploy automated incident response workflows.
7. Evaluate and optimize machine learning algorithms for cybersecurity tasks.
8. Analyze network traffic and endpoint data using AI/ML tools.
9. Implement AI-driven log analysis and threat correlation techniques.
10. Develop capabilities for AI-based malware detection and behavioral analysis.
11. Strengthen organizational defenses using predictive analytics.
12. Understand ethical, legal, and privacy considerations in AI-driven cybersecurity.
13. Build operational frameworks for deploying AI/ML at scale in cyber defense environments.

Organizational Benefits

- Enhanced threat detection and incident response speed
- Improved accuracy of anomaly detection and predictive analytics
- Increased efficiency in security operations through automation
- Reduced false positives in intrusion detection systems
- Strengthened endpoint, network, and cloud security posture
- Proactive identification of emerging cyber threats
- Enhanced integration of AI/ML tools with existing security infrastructure
- Data-driven decision-making for cybersecurity strategies
- Increased organizational resilience against advanced persistent threats
- Compliance with cybersecurity regulations and best practices

Target Audiences

- Security analysts and incident response teams
- SOC (Security Operations Center) personnel
- Cybersecurity managers and network defenders
- Threat intelligence analysts
- Security engineers and architects
- AI/ML specialists in cybersecurity
- IT risk and compliance officers
- Penetration testers and ethical hackers focused on defensive operations

Course Duration: 10 days

Course Modules

Module 1: Introduction to AI and ML in Cyber Defense

- Overview of AI and ML concepts in cybersecurity
- Role of Blue Team operations in modern cyber defense
- Benefits and limitations of AI/ML in threat detection
- Machine learning lifecycle and workflow for security applications
- Key tools and platforms for AI-driven defense
- Case Study: AI integration in a Security Operations Center

Module 2: Supervised Learning for Threat Detection

- Fundamentals of supervised learning algorithms
- Data labeling and feature engineering for security datasets
- Classification techniques for malware and intrusion detection
- Model evaluation metrics and performance assessment
- Challenges of supervised learning in cybersecurity
- Case Study: Using supervised learning to detect phishing attacks

Module 3: Unsupervised Learning & Anomaly Detection

- Overview of unsupervised learning techniques
- Clustering and dimensionality reduction for anomaly identification
- Detecting abnormal network behavior and system logs
- Application in detecting insider threats
- Limitations and tuning of unsupervised models
- Case Study: Anomaly detection in enterprise network traffic

Module 4: Reinforcement Learning for Cyber Defense

- Fundamentals of reinforcement learning (RL) in cybersecurity
- RL applications for automated threat response
- Training AI agents in simulated environments
- Optimizing reward functions for defense strategies
- Challenges in implementing RL in production
- Case Study: RL-driven adaptive firewall management

Module 5: Network Traffic Analysis with AI/ML

- Feature extraction from network data
- AI-driven intrusion detection systems (IDS)
- Traffic pattern analysis using machine learning
- Real-time monitoring and alert generation
- Model evaluation and validation on network datasets
- Case Study: Network anomaly detection in financial services

Module 6: Endpoint Security & Malware Detection

- AI techniques for malware classification and detection

- Behavioral analysis of endpoint activity
- Signature-based vs ML-based detection approaches
- Automating endpoint response and remediation
- Integrating ML models with EDR solutions
- Case Study: Malware detection using ML classifiers

Module 7: Log Analysis and Threat Correlation

- Parsing and normalizing logs for ML analysis
- Correlating events across multiple sources
- AI-driven pattern recognition in security logs
- Reducing alert fatigue with automated prioritization
- Integration with SIEM platforms
- Case Study: Detecting multi-stage attacks using ML log correlation

Module 8: Predictive Analytics for Incident Response

- Building predictive models for attack likelihood
- Forecasting attack vectors using historical data
- Automation of response workflows based on predictions
- Integration with ticketing and SOC systems
- Performance monitoring and model retraining
- Case Study: Predictive incident response in a large enterprise

Module 9: Threat Intelligence Integration

- Collection and enrichment of threat intelligence data
- Using AI/ML to process and analyze threat feeds
- Correlation of external threat indicators with internal data
- Prioritizing threats using predictive scoring
- Visualization of AI-driven intelligence outputs
- Case Study: Leveraging AI to enhance threat intelligence sharing

Module 10: AI in Cloud Security

- AI/ML techniques for cloud threat detection
- Securing cloud workloads and containerized applications
- Identifying anomalous access patterns
- Automating cloud security policy enforcement
- Integrating cloud telemetry into ML models
- Case Study: Detecting unauthorized cloud access using AI

Module 11: Adversarial Machine Learning & Defense

- Understanding adversarial attacks on ML models
- Techniques to harden ML models against manipulation
- Detection and mitigation of model poisoning
- Evaluating model robustness in cybersecurity applications
- Designing resilient ML pipelines
- Case Study: Adversarial attack on a predictive IDS

Module 12: AI-Powered SIEM & SOAR Integration

- Overview of SIEM and SOAR platforms
- Leveraging AI for event correlation and automation
- Enhancing incident response with ML recommendations
- Designing alert prioritization frameworks
- Continuous improvement of AI models within SIEM
- Case Study: AI integration with a commercial SIEM platform

Module 13: Ethical and Legal Considerations

- Data privacy and regulatory compliance in AI applications
- Ethical implications of automated defense systems
- Mitigating bias and ensuring fairness in ML models
- Documentation and audit trails for AI decisions
- Governance frameworks for AI in cybersecurity
- Case Study: Compliance challenges in AI-driven cyber defense

Module 14: Evaluating and Optimizing AI/ML Models

- Performance metrics and model validation
- Feature selection and hyperparameter tuning
- Continuous monitoring of model drift
- Model retraining and lifecycle management
- Integration of feedback loops from SOC teams
- Case Study: Optimizing ML model accuracy in anomaly detection

Module 15: Operationalizing AI for Blue Team Defense

- Deploying ML models in production environments
- Automation of repetitive defense tasks
- Training teams to interpret AI outputs
- Incident response workflow integration
- Scaling AI solutions across enterprise systems
- Case Study: End-to-end AI-powered SOC deployment

Training Methodology

- Instructor-led lectures with practical demonstrations
- Hands-on labs and simulations for AI/ML applications
- Case study analysis from real-world cyber defense scenarios
- Group exercises and collaborative threat hunting tasks
- Tools, templates, and scripts for AI/ML pipeline implementation
- Action plans and project presentations for organizational adoption

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
02 Nov 2026	06 Nov 2026	Online	$1,000
02 Nov 2026	06 Nov 2026	Physical	$1,500
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$3,000
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$4,500
02 Nov 2026	06 Nov 2026	Physical	$6,000
02 Nov 2026	06 Nov 2026	Physical	$6,000

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

Register Online Now

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