

AI-Powered Cybersecurity

Advanced Training for Modern Threats

5 Days

40 HOURS

5

MODULES

30

TOPICS

12

HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course covers the application of artificial intelligence, machine learning, and deep learning techniques to cybersecurity challenges. It begins with foundational concepts of AI-driven threat detection and network traffic analysis, then progresses to supervised and unsupervised machine learning models for intrusion and anomaly detection. The course continues with deep learning applications for malware classification, endpoint security, fraud detection, and phishing detection using natural language processing. It concludes with securing AI systems against adversarial attacks, using AI for penetration testing, and applying AI cybersecurity tools and frameworks in a capstone project.

WHO THIS COURSE IS FOR

Cybersecurity Analysts

Threat Detection Engineers

Security Researchers

Penetration Testers

Machine Learning Engineers

LEARNING OBJECTIVES

- Explain key AI, ML, and DL concepts used in cybersecurity
- Identify AI-driven techniques for threat detection and anomaly analysis
- Apply supervised learning models to detect malware and intrusions
- Implement clustering techniques for insider threat and zero-day detection
- Develop deep learning models for malware and phishing classification
- Analyse adversarial attacks and vulnerabilities in AI systems
- Apply techniques such as adversarial training to secure AI models
- Evaluate AI-powered tools and frameworks for cybersecurity solutions

5 Modules, 30 Topics

01

2 Hands-On Labs

Foundations of AI and Cybersecurity

INTRODUCTION TO AI IN CYBERSECURITY

- **Key concepts:** AI, ML, and DL in cybersecurity
- Types of AI systems (rule-based, supervised, unsupervised, and reinforcement learning)
- Differences between traditional cybersecurity and AI-driven approaches

ROLE OF AI IN CYBERSECURITY DOMAINS

- Threat detection and response
- Predictive analytics for attack prevention
- Behavioural analysis and anomaly detection

AI IN NETWORK TRAFFIC ANALYSIS

- Common attacks detectable via AI (DDoS, spoofing, port scans)
- Features extraction for network traffic using packet analysers (e.g., Wireshark)

02

2 Hands-On Labs

Machine Learning for Threat Detection

SUPERVISED LEARNING IN CYBERSECURITY

- Training classifiers to detect malware, phishing, and fraud
- Using decision trees, random forests, and support vector machines (SVM)

UNSUPERVISED LEARNING

- Clustering techniques for anomaly detection
- Applications in insider threat detection and zero-day attack identification

DATA PREPARATION FOR ML MODELS

- Handling imbalanced datasets (e.g., oversampling with SMOTE)
- Feature selection using mutual information or principal component analysis (PCA)

03**2 Hands-On Labs**

Advanced Deep Learning Applications in Cybersecurity

DEEP LEARNING FUNDAMENTALS FOR CYBERSECURITY

- **Architectures:** Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Transformers
- How deep learning enhances malware detection and email classification

AI FOR ENDPOINT SECURITY AND FRAUD DETECTION

- Endpoint vulnerability detection using DL models
- Fraud detection techniques with recurrent models

PHISHING EMAIL DETECTION WITH NATURAL LANGUAGE PROCESSING (NLP)

- Using pretrained NLP models (e.g., BERT, GPT) for phishing classification
- Tokenization and text vectorization for cybersecurity datasets

04**2 Hands-On Labs**

Securing AI Systems and Ethical Hacking with AI

AI VULNERABILITIES AND ADVERSARIAL ATTACKS

- Types of attacks on AI models (e.g., poisoning, evasion)
- Adversarial examples and how attackers exploit AI systems

TECHNIQUES TO SECURE AI MODELS

- Defensive distillation and adversarial training
- Role of explainable AI (XAI) in improving model robustness

USING AI FOR PENETRATION TESTING

- AI-driven tools for vulnerability scanning and exploitation (e.g., Metasploit with ML extensions)
- Predicting attack vectors using AI models

05**4 Capstone Projects**

Real-World AI Cybersecurity Solutions and Capstone Project

AI CYBERSECURITY TOOLS AND FRAMEWORKS

- Tools like IBM Watson for Cybersecurity, Darktrace, and Splunk with AI modules
- Frameworks for building AI models (TensorFlow, PyTorch, Scikit-learn)

EMERGING TRENDS IN AI CYBERSECURITY

- AI in quantum cryptography
- The rise of generative AI in crafting and detecting cyber threats

Practise What You Learn

#	MODULE	ACTIVITY
01	Foundations of AI and Cybersecurity	HANDS-ON LAB ■ Setting up a network traffic dataset ■ Preprocessing the data for training AI models using Python and pandas
02	Machine Learning for Threat Detection	HANDS-ON LAB ■ Build a supervised ML model for intrusion detection using a public dataset (e.g., KDDCup99 or UNSW-NB15) ■ Implement a clustering algorithm (e.g., K-means) for anomaly detection
03	Advanced Deep Learning Applications in Cybersecurity	HANDS-ON LAB ■ Train and fine-tune a neural network for phishing detection ■ Use a malware dataset to train a CNN for malware classification
04	Securing AI Systems and Ethical Hacking with AI	HANDS-ON LAB ■ Simulate adversarial attacks on a pre-trained AI model and implement mitigation strategies ■ Conduct AI-powered penetration testing on a virtual environment
05	Real-World AI Cybersecurity Solutions and Capstone Project	CAPSTONE PROJECT ■ Build an end-to-end AI-based cybersecurity solution: ■ Dataset collection and preprocessing ■ Model training for anomaly detection ■ Deploy a proof-of-concept (PoC) in a simulated environment

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com