

AI Security: Intrusion Detection & Malware Analysis

Learn to apply machine learning, deep learning, NLP and reinforcement learning to detect intrusions, analyse malware and defend AI security models.

5 Days

DURATION

15

MODULES

56

TOPICS

COURSE OVERVIEW

This course covers the role of artificial intelligence in cybersecurity, starting with Python tools and libraries for security projects. It then works through machine learning and deep learning methods for malware classification and anomaly detection, followed by natural language processing and reinforcement learning applications in security. Further modules address network intrusion detection, malware analysis, threat intelligence, adversarial attacks and defenses, SOC automation, identity and access management, and real-time model deployment. The course closes with ethical and privacy considerations and emerging trends in AI for cybersecurity.

WHO THIS COURSE IS FOR

Security Analysts

SOC Analysts

Malware Analysts

Threat Intelligence Analysts

Network Security Engineers

AI Security Engineers

PREREQUISITES

To get the most out of this course, participants should have:

- Basic Programming Skills: Familiarity with Python syntax and data structures.
- Introduction to Cybersecurity: Basic knowledge of network security concepts, including malware, intrusion detection, and encryption.
- Mathematics for AI: Understanding of basic linear algebra, probability, and statistics.

LEARNING OBJECTIVES

By the end of this course, participants will be able to:

- Understand the role of AI in identifying and mitigating security threats
- Develop and deploy AI-driven threat detection systems using Python
- Utilize machine learning and deep learning techniques for real-time intrusion detection
- Implement natural language processing and reinforcement learning in security applications
- Analyze and defend against adversarial attacks on AI security models

15 Modules, 56 Topics

01

Introduction to AI in Security

TOPICS

- Overview of Artificial Intelligence in Cybersecurity
- Key Challenges in Cybersecurity
- AI Solutions for Security Threats

02

Basics of Python for Security Applications

TOPICS

- Setting Up the Python Environment for Security Projects

ESSENTIAL PYTHON LIBRARIES FOR AI AND SECURITY

- **Libraries:** NumPy, Pandas, Matplotlib, Scikit-Learn, Keras, PyTorch, Scapy, Requests
- Data Handling and Preprocessing for Security Datasets

03

Machine Learning for Threat Detection

SUPERVISED LEARNING FOR MALWARE CLASSIFICATION

- Building and Training Classification Models
- Evaluating Model Performance

UNSUPERVISED LEARNING FOR ANOMALY DETECTION

- Clustering Techniques (K-Means, DBSCAN)
- Dimensionality Reduction for Network Traffic Analysis
- Semi-Supervised Learning and Its Applications in Security

04

Deep Learning Techniques for Security

TOPICS

- Introduction to Neural Networks for Security
- Convolutional Neural Networks for Intrusion Detection
- Recurrent Neural Networks for Log Analysis and Threat Detection
- Autoencoders for Anomaly Detection

05

Natural Language Processing (NLP) in Security

TOPICS

- Text Classification for Phishing Email Detection
- Named Entity Recognition (NER) for Threat Intelligence
- Sentiment Analysis on Security News
- Text Summarization for Threat Reports

06

Reinforcement Learning for Security Automation

TOPICS

- Basics of Reinforcement Learning (RL)
- RL for Intrusion Prevention Systems
- Adversarial Attacks and Defense Strategies with RL

07

AI for Network Security and Intrusion Detection

TOPICS

- Intrusion Detection Systems (IDS) with Machine Learning
- Deep Packet Inspection with Deep Learning
- Network Traffic Analysis and Anomaly Detection
- **Case Study:** Building an AI-Driven Intrusion Detection System

08

AI-Powered Malware Analysis and Detection

TOPICS

Static Analysis with Machine Learning · Dynamic Analysis Using Deep Learning · Behavioral Analysis of Malware · **Case Study:** Implementing a Malware Classifier

09

AI for Threat Intelligence

TOPICS

- Data Sources for Threat Intelligence
- Knowledge Graphs for Threat Intelligence
- Automated Threat Hunting with AI
- **Case Study:** Creating a Threat Intelligence Pipeline

10

Adversarial AI and Defense Mechanisms

TOPICS

- Understanding Adversarial Attacks on AI Models
- Defending Against Adversarial Attacks
- Securing AI Models in Production
- **Case Study:** Implementing Adversarial Defenses

11

AI for Security Operations Center (SOC) Automation

TOPICS

- Incident Detection and Response Automation
- Log Analysis and Event Correlation with AI
- AI-Powered Incident Prioritization and Analysis
- **Case Study:** Automating SOC Workflows with AI

12

AI-Driven Identity and Access Management (IAM)

TOPICS

- Machine Learning for Identity Verification
- Behavioral Biometrics and Anomaly Detection
- Facial Recognition and Authentication
- **Case Study:** Building an AI-Enhanced IAM System

13

Implementing AI Models in Real-Time Security Applications

TOPICS

- Model Deployment in Security Environments
- Using Docker and Kubernetes for Model Deployment
- Monitoring and Maintenance of Deployed Models

14

Ethical and Privacy Considerations in AI Security

TOPICS

Ethical AI in Security Contexts · Privacy Concerns and Compliance with GDPR · Addressing Bias in AI Security Models · Secure and Transparent Model Deployment

15

Future of AI in Cybersecurity

TOPICS

- Emerging Trends in AI for Security
- Challenges and Limitations of AI in Cybersecurity
- Potential Advancements and the Road Ahead

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