KOENIG
step forward

KOENIG SOLUTIONS · COURSE OUTLINE

Engineering AI for Cybersecurity (Advanced)

Learn to engineer AI and machine learning solutions for threat detection, network security, endpoint protection and identity management.

40 Hours	9	37
DURATION	MODULES	TOPICS

COURSE OVERVIEW

This comprehensive course equips learners with the principles and practical skills needed to integrate AI and Machine Learning into modern cybersecurity systems. Starting with foundational concepts and progressing through advanced applications like threat detection, adversarial defense, and endpoint protection, participants will explore techniques using supervised, unsupervised, and deep learning models. With a focus on engineering secure AI pipelines, network and identity management solutions, and responsible system design, the program culminates in a capstone project that simulates real-world deployment and evaluation of AI-powered security systems.

WHO THIS COURSE IS FOR

- **Security Engineers**
- **AI Engineers**
- **Machine Learning Engineers**
- **Network Security Analysts**
- **Identity and Access Managers**
- **Threat Detection Analysts**

PREREQUISITES

- Basic understanding of programming (preferably in Python)
- Familiarity with cybersecurity fundamentals and common threat types
- Introductory knowledge of artificial intelligence or machine learning concepts
- Comfort with using data analysis tools or frameworks (e.g., Pandas, Scikit-learn)
- Experience with network security or endpoint protection is helpful but not mandatory

LEARNING OBJECTIVES

What You Will Learn

- Explain core AI and machine learning concepts for security engineering
- Apply supervised and unsupervised learning to threat detection
- Implement deep learning models such as CNNs, RNNs and autoencoders
- Assess adversarial AI attacks and defense mechanisms
- Design secure network architectures using AI-powered detection
- Develop AI models for endpoint malware and threat hunting
- Evaluate explainability and performance of secure AI systems
- Apply AI techniques to identity and access management

COURSE SYLLABUS

9 Modules, 37 Topics

01

Foundations of AI and Machine Learning for Security Engineering

TOPICS

Core AI and ML Concepts for Security · Machine Learning Workflow · AI Use Cases in Cybersecurity · Engineering AI Pipelines for Security · Challenges in Applying AI to Security

02

Machine Learning for Threat Detection and Response

TOPICS

- Engineering Feature Extraction for Cybersecurity Datasets
- Supervised Learning for Threat Classification
- Unsupervised Learning for Anomaly Detection
- Engineering Real-Time Threat Detection Systems

03

Deep Learning for Security Applications

TOPICS

- Convolutional Neural Networks (CNNs) for Threat Detection
- Recurrent Neural Networks (RNNs) and LSTMs for Security
- Autoencoders for Anomaly Detection
- Adversarial Deep Learning in Security

04

Adversarial AI in Security

TOPICS

- Introduction to Adversarial AI Attacks
- Defense Mechanisms Against Adversarial Attacks
- Adversarial Testing and Red Teaming for AI Systems
- Engineering Robust AI Systems Against Adversarial AI

05

AI in Network Security

TOPICS

- AI-Powered Intrusion Detection Systems
- AI for Distributed Denial of Service (DDoS) Detection
- AI-Based Network Anomaly Detection
- Engineering Secure Network Architectures with AI

06

AI in Endpoint Security

TOPICS

- AI for Malware Detection and Classification
- AI for Endpoint Detection and Response (EDR)
- AI-Driven Threat Hunting
- Implementing Lightweight AI Models for Resource-Constrained Devices

07

Secure AI System Engineering

TOPICS

- Designing Secure AI Architectures
- Cryptography in AI for Security
- Ensuring Model Explainability and Transparency in Security
- Performance Optimization of AI Security Systems

08

AI in Identity and Access Management (IAM)

TOPICS

AI for User Behavior Analytics in IAM · AI for Multi-Factor Authentication (MFA) · AI for Zero-Trust Architecture · AI for Role-Based Access Control (RBAC)

09

Capstone Project - Engineering AI Security Systems

TOPICS

Defining the Capstone Project Problem · Engineering the AI Solution · Deploying and Monitoring the AI System · Final Capstone Presentation and Evaluation

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