Engineering AI for CyberSecurity

Duration: 40 hours

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.

Pre-requisites

- 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

Course Agenda

Module 1: Foundations of AI and Machine Learning for Security Engineering

- 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

Module 2: Machine Learning for Threat Detection and Response

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

Module 3: Deep Learning for Security Applications

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

Module 4: Adversarial AI in Security

- 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

Module 5: AI in Network Security

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

Module 6: AI in Endpoint Security

- 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

Module 7: Secure AI System Engineering

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

Module 8: AI in Identity and Access Management (IAM)

- 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)

Module 9: Capstone Project - Engineering AI Security Systems

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