Artificial Intelligence for Security Professionals

Duration: 05 days

Pre-requisites:

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.

Course Outcomes:

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

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

Table of Contents

Module 1: Introduction to AI in Security

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

Module 2: Basics of Python for Security Applications

- 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

Module 3: 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

Module 4: Deep Learning Techniques for Security

- 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

Module 5: Natural Language Processing (NLP) in Security

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

Module 6: Reinforcement Learning for Security Automation

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

Module 7: AI for Network Security and Intrusion Detection

- 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

Module 8: AI-Powered Malware Analysis and Detection

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

Module 9: AI for Threat Intelligence

- Data Sources for Threat Intelligence
- Knowledge Graphs for Threat Intelligence

- Automated Threat Hunting with AI
- Case Study: Creating a Threat Intelligence Pipeline

Module 10: Adversarial AI and Defense Mechanisms

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

Module 11: AI for Security Operations Center (SOC) Automation

- 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

Module 12: AI-Driven Identity and Access Management (IAM)

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

Module 13: Implementing AI Models in Real-Time Security Applications

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

Module 14: Ethical and Privacy Considerations in AI Security

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

Module 15: Future of AI in Cybersecurity

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