AI+ Security Level 3™

The AI+ Security Level 3 course provides a comprehensive exploration of the intersection between AI and cybersecurity, focusing on advanced topics critical to modern security engineering. It covers foundational concepts in AI and machine learning for security, delving into areas like threat detection, response mechanisms, and the use of deep learning for security applications. The course addresses the challenges of adversarial AI, network and endpoint security, and secure AI system engineering, along with emerging topics such as AI for cloud, container security, and blockchain integration. Key subjects also include AI in identity and access management (IAM), IoT security, and physical security systems, culminating in a hands-on capstone project that tasks learners with designing and engineering AI-driven security solutions.

Course Duration:

5 Days

Prerequisites:

- Completion of AI+ Security Level 1 and 2
- Intermediate / Advanced Python Programming: Proficiency or expert in Python, including deep learning frameworks (TensorFlow, PyTorch).
- Intermediate Machine Learning Knowledge: Proficiency in understanding of deep learning, adversarial AI, and model training.
- Advanced Cybersecurity Knowledge: Proficiency in threat detection, incident response, and network/endpoint security.
- AI in Security Engineering: Knowledge of AI's role in identity and access management (IAM), IoT security, and physical security.
- Cloud and Container Expertise: Understanding of cloud security, containerization, and blockchain technologies.
- Linux/CLI Mastery: Advanced command-line skills and experience with security tools in Linux environments.

Course Objectives:

- Gain advanced expertise in applying AI and ML to enhance cybersecurity measures.
- Become proficient in leveraging AI-driven techniques for threat detection, response, and prevention.
- Build skills to secure networks, endpoints, and cloud environments using advanced AI applications.
- Learn to address adversarial AI challenges and design robust defenses against emerging threats.
- Develop expertise in implementing secure AI systems for identity management, IoT security, and blockchain-based solutions.
- Complete a capstone project to gain practical experience in designing AI-powered security solutions.
- Prepare for advanced roles in AI-driven cybersecurity engineering and system architecture.

Outlines:

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

- 1.1 Core AI and ML Concepts for Security
- 1.2 AI Use Cases in Cybersecurity
- 1.3 Engineering AI Pipelines for Security
- 1.4 Challenges in Applying AI to Security

Module 2: Machine Learning for Threat Detection and Response

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

Module 3: Deep Learning for Security Applications

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

Module 4: Adversarial AI in Security

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

Module 5: AI in Network Security

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

Module 6: AI in Endpoint Security

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

Module 7: Secure AI System Engineering

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

Module 8: AI for Cloud and Container Security

- 8.1 AI for Securing Cloud Environments
- 8.2 AI-Driven Container Security
- 8.3 AI for Securing Serverless Architectures
- 8.4 AI and DevSecOps

Module 9: AI and Blockchain for Security

- 9.1 Fundamentals of Blockchain and AI Integration
- 9.2 AI for Fraud Detection in Blockchain
- 9.3 Smart Contracts and AI Security
- 9.4 AI-Enhanced Consensus Algorithms

Module 10: AI in Identity and Access Management (IAM)

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

Module 11: AI for Physical and IoT Security

- 11.1 AI for Securing Smart Cities
- 11.2 AI for Industrial IoT Security
- 11.3 AI for Autonomous Vehicle Security
- 11.4 AI for Securing Smart Homes and Consumer IoT

Module 12: Capstone Project - Engineering AI Security Systems

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

Who should attend

- Cybersecurity Professionals: Individuals looking to enhance their skills in compliance and security management.
- Risk Management Specialists: Those interested in improving risk assessment and mitigation strategies using AI.
- Compliance Officers: Professionals responsible for ensuring adherence to regulatory standards who want to leverage AI for compliance processes.
- IT Security Analysts: Analysts seeking to integrate AI technologies into their security practices and frameworks.
- Ethical Hackers and Penetration Testers: Individuals wanting to explore AI techniques for identifying vulnerabilities, defending against adversarial attacks, and stress-testing systems.
- Tech-Savvy Leaders: IT managers or security architects aiming to future-proof their organizations with AI-enhanced compliance, governance, and security practices.
- Aspiring AI Security Experts: Learners with foundational knowledge in AI and cybersecurity eager to master AI-powered solutions for emerging threats and advanced security challenges.