AI+ Security Level 2™

Duration: 40 hours

Course Overview

Our comprehensive course, AI+ Security Level 2 offers professionals a thorough exploration of the integration of AI and Cybersecurity. Beginning with fundamental Python programming tailored for AI and Cybersecurity applications, participants delve into essential AI principles before applying machine learning techniques to detect and mitigate cyber threats, including email threats, malware, and network anomalies. Advanced topics such as user authentication using AI algorithms and the application of Generative Adversarial Networks (GANs) for Cybersecurity purposes are also covered, ensuring participants are equipped with cutting-edge knowledge. Practical application is emphasized throughout, culminating in a Capstone Project where attendees synthesize their skills to address real-world cybersecurity challenges, leaving them adept in leveraging AI to safeguard digital assets effectively.

Course Prerequisites

- Completion of AI+ Security Level 1, not mandatory
- **Basic Python Skills:** Familiarity with Python basics, including variables, loops, and functions
- **Basic Cybersecurity:** Basic understanding of cybersecurity principles, such as the CIA triad and common cyber threats
- **Basic Machine Learning Awareness:** General awareness about machine learning, no technical skills required
- **Basic Networking Knowledge:** Understanding of IP addresses and how the internet works.
- **Basic Command Line Skills:** Comfort using the command line like Linux or Windows terminal for basic tasks
- **Interest in AI for Security:** Willingness to explore how AI can be applied to detect and mitigate security threats.

Course Agenda

Module 1: Introduction to Artificial Intelligence (AI) and Cyber Security

- Understanding the Cyber Security Artificial Intelligence (CSAI)
- An Introduction to AI and its Applications in Cybersecurity
- Overview of Cybersecurity Fundamentals
- Identifying and Mitigating Risks in Real-Life
- Building a Resilient and Adaptive Security Infrastructure

- Enhancing Digital Defenses using CSAI

Module 2: Python Programming for AI and Cybersecurity Professionals

- Python Programming Language and its Relevance in Cybersecurity
- Python Programming Language and Cybersecurity Applications
- AI Scripting for Automation in Cybersecurity Tasks
- Data Analysis and Manipulation Using Python
- Developing Security Tools with Python

Module 3: Applications of Machine Learning in Cybersecurity

- Understanding the Application of Machine Learning in Cybersecurity
- Anomaly Detection to Behaviour Analysis
- Dynamic and Proactive Defense using Machine Learning
- Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats

Module 4: Detection of Email Threats with AI

- Utilizing Machine Learning for Email Threat Detection
- Analyzing Patterns and Flagging Malicious Content
- Enhancing Phishing Detection with AI
- Autonomous Identification and Thwarting of Email Threats
- Tools and Technology for Implementing AI in Email Security

Module 5: AI Algorithm for Malware Threat Detection

- Introduction to AI Algorithm for Malware Threat Detection
- Employing Advanced Algorithms and AI in Malware Threat Detection
- Identifying, Analyzing, and Mitigating Malicious Software
- Safeguarding Systems, Networks, and Data in Real-time
- Bolstering Cybersecurity Measures Against Malware Threats
- Tools and Technology: Python, Malware Analysis Tools

Module 6: Network Anomaly Detection using AI

- Utilizing Machine Learning to Identify Unusual Patterns in Network Traffic
- Enhancing Cybersecurity and Fortifying Network Defenses with AI Techniques
- Implementing Network Anomaly Detection Techniques

Module 7: User Authentication Security with AI

- Introduction
- Enhancing User Authentication with AI Techniques
- Introducing Biometric Recognition, Anomaly Detection, and Behavioural Analysis
- Providing a Robust Defence Against Unauthorized Access
- Ensuring a Seamless Yet Secure User Experience
- Tools and Technology: AI-based Authentication Platforms

Module 8: Generative Adversarial Network (GAN) for Cyber Security

- Introduction to Generative Adversarial Networks (GANs) in Cybersecurity
- Creating Realistic Mock Threats to Fortify Systems
- Detecting Vulnerabilities and Refining Security Measures Using GANs
- Tools and Technology: Python and GAN Frameworks

Module 9: Penetration Testing with Artificial Intelligence

- Enhancing Efficiency in Identifying Vulnerabilities Using AI
- Automating Threat Detection and Adapting to Evolving Attack Patterns
- Strengthening Organizations Against Cyber Threats Using AI-driven Penetration Testing
- Tools and Technology: Penetration Testing Tools, AI-based Vulnerability Scanners

Module 10: Capstone Project

- Introduction
- Use Cases: AI in Cybersecurity
- Outcome Presentation