AI+ Security Level 1™

Duration: 40 hours

Course Overview

Our comprehensive course, AI+ Security level 1 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

- Basic Python Programming: Familiarity with loops, functions, and variables.
- Basic Cybersecurity Knowledge: Understanding of CIA triad and common threats (e.g., malware, phishing).
- Basic Machine Learning Concepts: Awareness of fundamental machine learning concepts, not mandatory.
- Basic Networking: Understanding of IP addressing and TCP/IP protocols.
- Linux/Command Line Skills: Ability to navigate and use the CLI effectively.

Course Agenda

Module 1: Introduction to Cybersecurity

- Definition and Scope of Cybersecurity
- Key Cybersecurity Concepts
- CIA Triad (Confidentiality, Integrity, Availability)
- Cybersecurity Frameworks and Standards (NIST, ISO/IEC27001)
- Cyber Security Laws and Regulations (e.g., GDPR, HIPAA)
- Importance of Cybersecurity in Modern Enterprises
- Careers in Cyber Security

Module 2: Operating System Fundamentals

- Core OS Functions (Memory Management, Process Management)
- User Accounts and Privileges
- Access Control Mechanisms (ACLs, DAC, MAC)
- OS Security Features and Configurations
- Hardening OS Security (Patching, Disabling Unnecessary Services)
- Virtualization and Containerization Security Considerations
- Secure Boot and Secure Remote Access
- OS Vulnerabilities and Mitigations

Module 3: Networking Fundamentals

- Network Topologies and Protocols (TCP/IP, OSI Model)
- Network Devices and Their Roles (Routers, Switches, Firewalls)
- Network Security Devices (Firewalls, IDS/IPS)
- Network Segmentation and Zoning
- Wireless Network Security (WPA2, Open WEP vulnerabilities)
- VPN Technologies and Use Cases
- Network Address Translation (NAT)
- Basic Network Troubleshooting

Module 4: Threats, Vulnerabilities and Exploits

- Types of Threat Actors (Script Kiddies, Hacktivists, Nation-States)
- Threat Hunting Methodologies using AI
- AI Tools for Threat Hunting (SIEM, IDS/IPS)
- Open-Source Intelligence (OSINT) Techniques
- Introduction to Vulnerabilities
- Software Development Life Cycle (SDLC) and Security Integration with AI
- Zero-Day Attacks and Patch Management Strategies
- Vulnerability Scanning Tools and Techniques using AI
- Exploiting Vulnerabilities (Hands-on Labs)

Module 5: Understanding of AI and ML

- An Introduction to AI
- Types and Applications of AI
- Identifying and Mitigating Risks in Real-Life
- Building a Resilient and Adaptive Security Infrastructure with AI
- Enhancing Digital Defenses using CSAI
- Application of Machine Learning in Cybersecurity
- Safeguarding Sensitive Data and Systems Against Diverse Cyber Threats
- Threat Intelligence and Threat Hunting Concepts

Module 6: Python Programming Fundamentals

- Introduction to Python Programming
- Understanding of Python Libraries
- Python Programming Language for Cybersecurity Applications
- AI Scripting for Automation in Cybersecurity Tasks
- Data Analysis and Manipulation Using Python
- Developing Security Tools with Python

Module 7: Applications of AI in Cybersecurity

- Understanding the Application of Machine Learning in Cybersecurity
- Anomaly Detection to Behavior Analysis
- Dynamic and Proactive Defense using Machine Learning

- Utilizing Machine Learning for Email Threat Detection
- Enhancing Phishing Detection with AI
- Autonomous Identification and Thwarting of Email Threats
- Employing Advanced Algorithms and AI in Malware Threat Detection
- Identifying, Analyzing, and Mitigating Malicious Software
- Enhancing User Authentication with AI Techniques
- Penetration Testing with AI

Module 8: Incident Response and Disaster Recovery

- Incident Response Process (Identification, Containment, Eradication, Recovery)
- Incident Response Lifecycle
- Preparing an Incident Response Plan
- Detecting and Analyzing Incidents
- Containment, Eradication, and Recovery
- Post-Incident Activities
- Digital Forensics and Evidence Collection
- Disaster Recovery Planning (Backups, Business Continuity)
- Penetration Testing and Vulnerability Assessments
- Legal and Regulatory Considerations of Security Incidents

Module 9: Open Source Security Tools

- Introduction to Open-Source Security Tools
- Popular Open Source Security Tools
- Benefits and Challenges of Using Open-Source Tools
- Implementing Open Source Solutions in Organizations
- Community Support and Resources
- Network Security Scanning and Vulnerability Detection
- Security Information and Event Management (SIEM) Tools (Open-Source options)
- Open-Source Packet Filtering Firewalls
- Password Hashing and Cracking Tools (Ethical Use)
- Open-Source Forensics Tools

Module 10: Securing the Future

- Emerging Cyber Threats and Trends
- Artificial Intelligence and Machine Learning in Cybersecurity
- Blockchain for Security
- Internet of Things (IoT) Security
- Cloud Security
- Quantum Computing and its Impact on Security
- Cybersecurity in Critical Infrastructure
- Cryptography and Secure Hashing
- Cyber Security Awareness and Training for Users
- Continuous Security Monitoring and Improvement

Module 10: Capstone Project

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