# Customized Cybersecurity with AI integration

## Course Objectives
## Duration: 40 hrs

This course provides a practical introduction to Artificial Intelligence and its applications in enterprise cybersecurity. Participants will learn the fundamentals of AI, Machine Learning, Deep Learning, and Generative AI, and understand how these technologies enhance modern security operations. Through hands-on labs and real-world cybersecurity scenarios, learners will build AI models, explore intelligent security automation, and develop AI-powered solutions using Azure AI and modern AI technologies.

## Target Audience

- Cybersecurity Professionals
- SOC Analysts
- Security Engineers
- Network & Infrastructure Engineers
- Security Administrators
- IT Professionals interested in AI-driven cybersecurity

## Prerequisites:

Basics of cybersecurity

## Course Modules

### Module 1: Introduction to Artificial Intelligence

Gain a foundational understanding of Artificial Intelligence and its role in solving real-world business and cybersecurity challenges. Explore the evolution of AI, its different categories, and how it relates to Machine Learning, Deep Learning, and Data Science.

- Introduction to Artificial Intelligence
- Types of AI

- AI vs Machine Learning vs Deep Learning vs Data Science
- Enterprise AI Applications
- AI Project Lifecycle Overview

## Module 2: Fundamentals of Data Science for AI

Learn the fundamentals of Data Science and understand how data serves as the foundation for building intelligent AI solutions. Explore different types of data, data preparation concepts, and how datasets are used in Machine Learning.

- Introduction to Data Science
- Data Science Ecosystem
- Types of Data
- Data Collection & Preparation
- Features and Labels
- AI Datasets

## Module 3: Machine Learning Fundamentals

Understand the core concepts of Machine Learning and how intelligent systems learn from data. Explore different learning approaches and common enterprise cybersecurity applications of Machine Learning.

- Introduction to Machine Learning
- Types of Machine Learning
- Classification vs Regression
- Model Training Concepts
- Machine Learning Use Cases in Cybersecurity

## Module 4: Python Essentials

Build the programming foundation required for developing AI and Machine Learning solutions. Learn the essential Python concepts, data structures, and libraries commonly used for AI development.

- Python Fundamentals

- Control Flow
- Functions
- Data Structures
- File Handling
- NumPy & Pandas

## Module 5: Model Development lifecycle

Understand the complete lifecycle of developing an AI solution, from defining the problem to deploying and maintaining machine learning models. Learn the standard workflow followed in enterprise AI projects.

- AI Project Workflow
- Problem Definition
- Data Understanding
- Model Development
- Model Validation & Testing
- Model Deployment
- Model Monitoring

## Module 6: Machine Learning Algorithms for Cybersecurity

Explore the most widely used Machine Learning algorithms for cybersecurity and understand when to apply each technique for different threat detection and security analytics scenarios.

- Supervised Learning Algorithms
- Unsupervised Learning Algorithms
- Algorithm Selection
- Enterprise Cybersecurity Use Cases

## Module 7: Feature Engineering & Model Evaluation

Learn how to prepare meaningful features from cybersecurity data and evaluate machine learning models using industry-standard performance metrics. Understand

how feature engineering and model evaluation contribute to building accurate and reliable AI solutions.

- Feature Engineering for Cybersecurity Data
- Feature Selection and Importance
- Model Training and Prediction
- Model Evaluation Metrics (Accuracy, Precision, Recall & F1-Score)
- Improving Model Performance

## Module 8: Introduction to Deep Learning

Understand the fundamentals of Deep Learning and how neural networks enable AI systems to solve complex cybersecurity problems beyond the capabilities of traditional Machine Learning. Explore the key concepts, architectures, and enterprise use cases of Deep Learning in modern security solutions.

- Introduction to Deep Learning
- Artificial Neural Networks (ANN)
- Deep Learning vs Machine Learning
- Deep Learning Applications in Cybersecurity

## Module 9: Deep Learning Architectures

Explore the most widely used deep learning architectures and understand how each model is applied to different cybersecurity challenges such as malware detection, user behavior analysis, and network traffic monitoring.

- Artificial Neural Networks (ANN)
- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN & LSTM)
- Transformer Models
- Architecture Selection for Security Use Cases

## Module 10: Building Deep Learning Models

Learn how to build, train, evaluate, and use deep learning models for cybersecurity applications using TensorFlow and Keras. Gain hands-on experience in developing neural network models for different security scenarios.

- Building CNN Models for Security Classification
- Developing RNN/LSTM Models for Sequential Security Data
- Model Evaluation and Performance Optimization

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

Explore how Artificial Intelligence transforms modern Security Operations Centers (SOC) by enhancing threat detection, alert management, and incident response. Learn how AI helps SOC analysts improve operational efficiency, reduce manual effort, and accelerate security investigations.

- Security Operations Center (SOC) Overview
- AI in SOC Operations
- Alert Correlation & Prioritization
- Threat Hunting & Incident Investigation
- AI-Assisted Incident Response

## Module 12: AI for Threat Intelligence & Network Security

Learn how AI enhances enterprise security by analyzing threat intelligence, strengthening network monitoring, optimizing firewall policies, and supporting proactive risk management. Explore how organizations use AI to improve visibility and make faster security decisions.

- Threat Intelligence Analysis
- Network Traffic Analytics
- Firewall Policy Optimization
- Vulnerability Prioritization
- Compliance & Risk Monitoring

## Module 13: Generative AI for Cybersecurity

Discover how Generative AI assists cybersecurity professionals in automating documentation, analyzing security incidents, summarizing threat intelligence, and improving operational decision-making while following enterprise AI best practices.

- AI-Assisted Security Documentation
- Incident Report Generation
- Threat Intelligence Summarization
- Security Policy & Compliance Assistance
- Responsible AI Best Practices

## Module 14: Generative AI & Large Language Models (LLMs)

Understand the fundamentals of Generative AI and Large Language Models (LLMs), and explore how they are transforming enterprise cybersecurity. Learn the core concepts behind modern AI systems and their practical applications in security operations.

- Introduction to LLMs
- LLM Architecture Overview
- Prompt Engineering Fundamentals
- Context Management
- Enterprise AI Applications

## Module 15: Enterprise AI with Azure AI

Explore the Microsoft Azure AI ecosystem and understand how organizations build, deploy, and manage secure enterprise AI solutions using Azure AI services.

- Azure AI Services Overview
- Azure AI Foundry
- Azure OpenAI Service
- Model Catalog
- Enterprise AI Solution Development

## Module 16: Building AI Agents for Cybersecurity

Learn how AI Agents extend the capabilities of Large Language Models by combining reasoning, enterprise knowledge, and external tools. Explore how AI Agents automate cybersecurity workflows and assist security professionals in day-to-day operations.

- Introduction to AI Agents
- Agent Architecture
- Retrieval-Augmented Generation (RAG)
- Model Context Protocol (MCP)
- Tool Calling & Enterprise Knowledge Integration
- AI Agents for Security Operations

## Module 17: Responsible AI & Enterprise Best Practices

Understand the principles of responsible AI and the best practices for securely deploying AI solutions in enterprise environments. Learn how organizations address governance, security, privacy, and ethical considerations when adopting AI.

- Responsible AI Principles
- AI Governance
- Prompt Security
- Data Privacy & Compliance
- Enterprise AI Best Practices

## Module 18: Capstone Project – AI Security Consultant

Apply the concepts learned throughout the course by building an end-to-end AI-powered cybersecurity solution. Integrate AI, Machine Learning, Generative AI, and enterprise AI technologies to automate security tasks, analyze threats, and support security operations.

- Data Preparation & AI Model Development
- AI-Powered Threat Detection & Analysis
- Generative AI & AI Agent Integration
- Responsible AI & Enterprise Best Practices