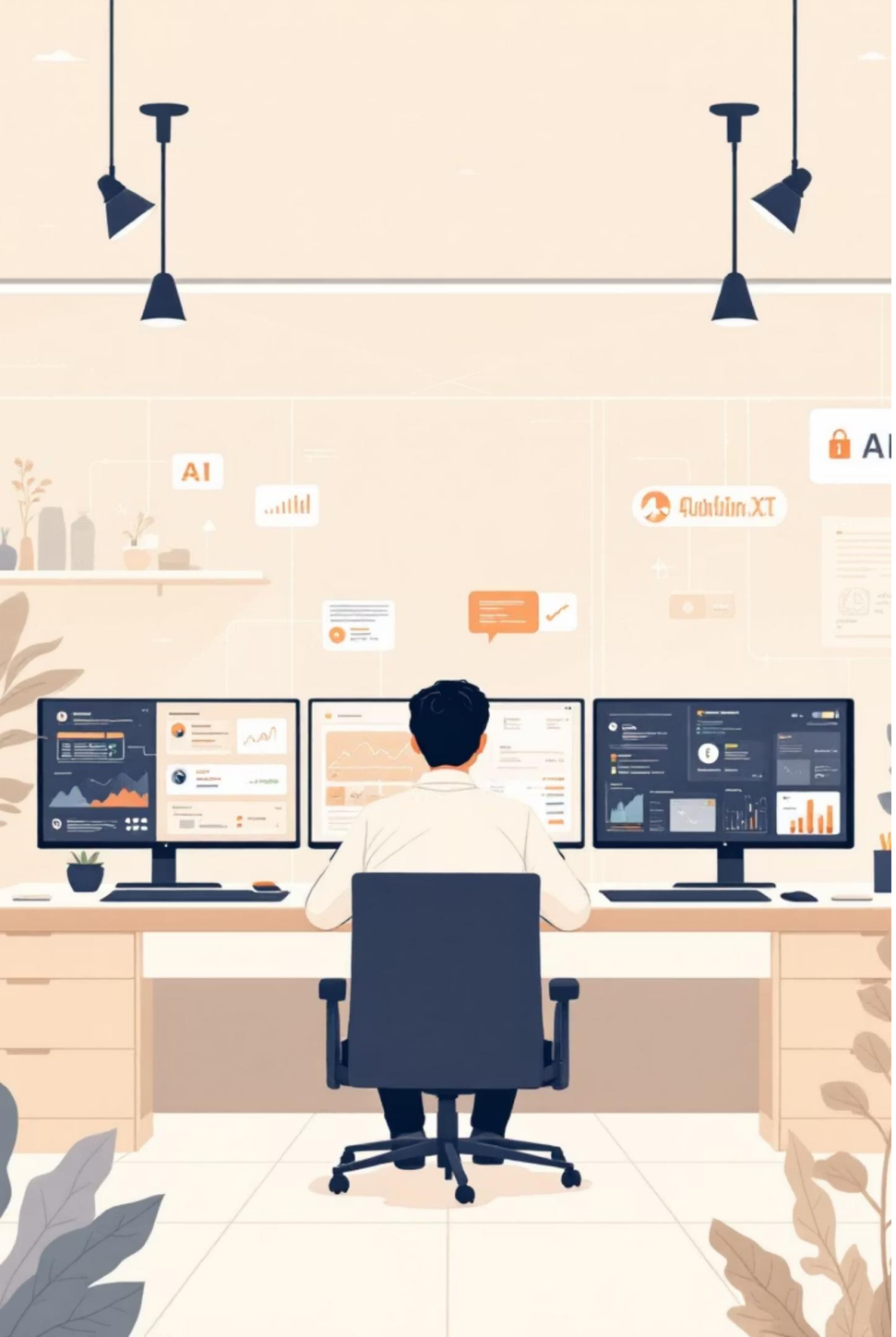

AI in Cyber Security: Course Outline

Course Duration: 2 Days (12 hours total, 6 hours per day)

Course Overview

This intensive two-day course explores the application of Artificial Intelligence (AI) in cybersecurity, covering foundational concepts, practical applications, and emerging trends. Participants will learn how AI enhances threat detection, response, and prevention, with hands-on examples and case studies.

Day 1: Foundations and Applications of AI in Cybersecurity

Duration: 6 hours (including breaks)

01

Session 1: Introduction to AI and Cybersecurity (1.5 hours)

Objectives: Understand the basics of AI and its relevance to cybersecurity.

Topics:

- Overview of AI: Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP).
- Cybersecurity challenges: Malware, phishing, insider threats, and advanced persistent threats (APTs).
- Role of AI in addressing cybersecurity
- challenges.

Activities:

- Interactive discussion: Real-world cyber threats and AI's potential.
- Case study: AI-driven threat detection in a corporate network.

02

Session 2: AI Techniques for Threat Detection (2 hours)

Objectives: Explore AI algorithms and their applications in detecting cyber threats.

Topics:

- Supervised vs. unsupervised learning for anomaly detection.
- Use of neural networks in identifying malware and phishing attacks.
- Behavioral analysis using AI for insider threat detection.

Activities:

- Hands-on demo: Using a pre-trained ML model to detect malicious network traffic (e.g., using Python and scikit-learn).
- Group exercise: Analyze a dataset for anomalies.

03

Session 3: AI in Threat Intelligence and Response (2.5 hours)

Objectives: Learn how AI enhances threat intelligence and incident response.

Topics:

- AI for real-time threat intelligence: Data aggregation and correlation.
- Automated incident response using AI-driven Security Orchestration, Automation, and Response (SOAR).
- Case studies: AI in combating ransomware and DDoS attacks.

Activities:

- Simulation: Respond to a simulated cyberattack using an AI-based tool.
- Discussion: Ethical considerations in AI-driven cybersecurity.

Day 2: Advanced Applications and Future Trends

Duration: 6 hours (including breaks)

Session 4: AI in Vulnerability Management and Prevention (2 hours)

Objectives: Understand how AI strengthens proactive cybersecurity measures.

Topics:

- AI for vulnerability assessment and patch management.
- Predictive analytics for anticipating cyber threats.
- AI in securing cloud and IoT environme

Activities:

- Hands-on exercise: Using AI tools to identify vulnerabilities in a sample system.
- Case study: AI in securing IoT devices.

Session 5: Adversarial AI and Countermeasures (2 hours)

Objectives: Explore the risks of adversarial AI and strategies to mitigate them.

Topics:

- Adversarial attacks on AI models (e.g., data poisoning, model evasion).
- Defending AI systems: Robustness and explainability.
- Emerging threats: AI-generated deepfakes and social engineering.

Activities:

- Group discussion: Mitigating adversarial AI risks in cybersecurity.
- Demo: Simulating an adversarial attack on a ML model.

Session 6: Future Trends and Wrap-Up (2 hours)

Objectives: Discuss the future of AI in cybersecurity and consolidate learning.

Topics:

- Emerging trends: Quantum computing, federated learning, and zero-trust architectures.
- Ethical and regulatory considerations in AI-driven cybersecurity.
- Building an AI ready workforce

Activities:

- Group project: Design an AI-based cybersecurity solution for a hypothetical organization.
- Q&A and course feedback.

Learning Outcomes

By the end of the course, participants will:

- Understand the role of AI in addressing modern cybersecurity challenges.
- Gain hands-on experience with AI tools for threat detection and response.
- Recognize the risks of adversarial AI and strategies to mitigate them.
- Be prepared to integrate AI into cybersecurity practices and stay updated on
- emerging trends.

Target Audience

- Cybersecurity professionals
- IT managers and analysts
- Data scientists interested in cybersecurity
- Anyone seeking to understand AI's role in securing digital systems

Prerequisites

- Basic understanding of cybersecurity concepts
- Familiarity with programming (Python preferred) is helpful but not
- mandatory

Delivery Method

- Instructor-led sessions
- Hands-on demos and group activities
- Case studies and real-world examples