AI Cybersecurity 2026

AI Cybersecurity

Introduction:

This course bridges the world of Artificial Intelligence and Cybersecurity to prepare participants for the rapidly evolving landscape of digital threats. Through a blend of theoretical knowledge and hands-on practice, students will master how AI transforms threat detection, response, and system defense, while acquiring proficiency in leading tools such as TensorFlow, PyTorch, ChatGPT, Wireshark, and Splunk.

Designed for aspiring security professionals, data scientists, and curious learners alike, this course equips participants to design and implement cutting-edge security solutions powered by AI.

You must know!

Hours:
40 academic hours

Our lecturers:
INT College instructors are industry-leading cybersecurity and AI professionals with hands-on experience in academia, enterprise, and defense environments. The teaching staff brings practical insights and current practices from the field.

Eligibility for INT College's Certificate:
An INT College certificate will be awarded to students who complete all exercises, participate in at least 85% of sessions, and fulfill the course project requirements.

Target Audience:

- Cybersecurity beginners and IT professionals interested in AI-driven defense systems.
- Students and career changers aiming to enter the cyber-tech field.
- Developers seeking to apply machine learning to security problems.
- Security analysts looking to automate tasks and threat analysis using AI tools.

Prerequisites:

- Basic understanding of computers and networking.
- No programming background required – Python basics will be taught.
- Motivation to learn AI and cybersecurity in depth.
- Access to a computer with stable internet.

Course Objectives:

By the end of this course, students will be able to:

- Understand how AI and machine learning impact modern cybersecurity.
- Build and deploy AI models using PyTorch and TensorFlow for security applications.
- Automate security analysis and detection tasks using ChatGPT and Python.
- Analyze traffic and threats using tools like Wireshark and Splunk.
- Design an AI-driven phishing detection system.
- Simulate social engineering using AI voice cloning techniques.
- Apply the NIST AI Risk Management Framework to cybersecurity use cases.
- Detect anomalies and mitigate attacks through hands-on lab environments.

Course Topics:

1. **Introduction to AI and Cybersecurity**
    - Overview of cyber threats in the AI era
    - The role of AI in cyber defense
    - Real-world case studies
2. **Fundamentals of Cybersecurity**
    - Threat types, vulnerabilities, and risk
    - Firewalls, malware analysis, and encryption
    - Risk management basics
3. **Python for Security & AI Applications**
    - Python programming foundations
    - Scripting for automation and analysis
    - Using Python with cyber tools

4. **Machine Learning for Cyber Defense**
    - Intro to machine learning concepts
    - Supervised vs. unsupervised models
    - Building models for threat detection
5. **Tools of the Trade: Security and AI Stack**
    - Wireshark for packet analysis
    - Splunk for SIEM and log analysis
    - VirtualBox environments
    - TensorFlow, PyTorch, and ChatGPT
6. **ChatGPT for Cybersecurity**
    - Automating tasks with LLMs
    - Writing detection scripts
    - Prompt engineering for threat hunting
7. **Deep Learning with PyTorch for Cyber Tasks**
    - Training AI models
    - Evaluating models for intrusion detection
    - Neural networks in security
8. **AI-Based Project: Phishing Detection System**
    - Designing and training a model
    - Real-time detection and alerts
    - Accuracy and ethical considerations
9. **Voice Cloning & Social Engineering Simulation**
    - Tools for audio manipulation
    - Understanding risks of synthetic media
    - Awareness training design
10. **NIST AI Risk Management Framework**
    - Introduction and purpose
    - Applying the framework to AI security models
    - Compliance and risk mitigation

11. Capstone Project & Final Evaluation

- Project presentation: AI-powered cybersecurity solution
- Peer and instructor feedback
- Certification eligibility check

The college reserves the right to make changes to the curriculum, course duration, teaching staff, and other related aspects at its sole discretion. Any information provided in the college's informational materials shall not be considered binding or constitute any form of commitment by the college.

תל אביב

המרץ 2