# AI and Security for Cisco

1. Copyright Elephant Scale May 4, 2025

### Course Description

* Course goals
  + This course helps Cisco fulfill its strategy of enabling its clients to deliver secure AI systems
  + This is evidenced by Cisco’s acquisition of [Robust Intelligence](https://blogs.cisco.com/security/evaluating-security-risk-in-deepseek-and-other-frontier-reasoning-models), a leading security firm.
* The “Cybersecurity for AI Professionals” workshop aims to equip AI professionals with a comprehensive understanding of cybersecurity threats specific to AI systems.
* Participants will learn best practices for securing AI models, data, and pipelines, integrating these skills into the AI development lifecycle.
* By providing hands-on experience with real-world vulnerabilities and mitigation techniques, the program prepares professionals to implement robust cybersecurity frameworks, incident response protocols, and defence strategies against adversarial attacks.
* Additionally, the workshop emphasizes the importance of ethical and compliance considerations, ensuring participants are well-prepared to address privacy, transparency, and regulatory standards within AI cybersecurity.

### Learning Outcomes

* Upon completing this course, participants will:
* Understand and identify cybersecurity vulnerabilities in AI systems.
* Implement data protection and secure pipeline practices for AI development.
* Integrate cybersecurity frameworks and incident response protocols into AI workflows.
* Analyze and defend against adversarial attacks on AI systems.
* Address ethical considerations and compliance standards for cybersecurity in AI.

## Audience

* AI engineers and developers
* Data scientists working with AI models
* Cybersecurity professionals specializing in AI systems
* IT managers overseeing AI infrastructure
* AI ethics and compliance officers

## Skill Level

* Intermediate to advanced.

## Duration

* Two days

## Prerequisites

* General familiarity with machine learning and AI
* Exposure to coding in any language
* Familiarity with Python helpful

## Format

* Lectures and hands on labs. (50% - 50%)

## Lab environment

* Zero Install: There is no need to install software on students’ machines!
* A lab environment in the cloud will be provided for students.

### Students will need the following

* A reasonably modern laptop with unrestricted connection to the Internet. Laptops with overly restrictive VPNs or firewalls may not work properly.
  + A checklist to verify connectivity will be provided
* Chrome browser

## Course outline

### Introduction to AI Security

* Overview of Cybersecurity for AI Systems
  + The Intersection of AI and Cybersecurity, Unique AI Vulnerabilities
  + Importance of cybersecurity for AI.
  + Vulnerabilities in AI (data poisoning, model evasion, adversarial attacks).
* Protecting AI Models and Algorithms
  + Securing AI Models during Development and Deployment
  + Safeguarding AI algorithms and parameters.
  + Strategies for model integrity and tamper-proofing.
  + Labs: Identifying Vulnerabilities in AI Systems
    - Simulate and assess common vulnerabilities in AI models and data pipelines.

### Securing AI Data and Pipelines

* Data Security in AI Systems
* Securing Training Data, Data Privacy
  + Techniques for data encryption, masking, and anonymization.
  + Controlling access to sensitive training data.
* Pipeline Security in AI Systems
  + Securing each stage from data ingestion to deployment.
  + Implementing encryption and access controls for data at each pipeline stage.
  + Monitoring and vulnerability assessment in pipelines.
* Adversarial Attacks on AI Systems
  + Overview of adversarial attacks on models.
  + Case studies of adversarial examples affecting AI outputs.
  + Labs: Defending Against Adversarial Attacks
    - Detect and counteract adversarial examples in a hands-on lab setting.
* Cybersecurity Frameworks for AI Development
  + Embedding security from development to deployment.
  + Using secure development tools and environments.
  + Security testing methods (e.g., static analysis, dynamic testing, adversarial testing).
* AI System Monitoring and Incident Management
  + Continuous security monitoring for AI components.
  + Alert and logging systems for anomaly detection.
  + Incident response protocols and recovery mechanisms.
  + Labs: Securing AI Model Deployment
    - Implement deployment best practices with a focus on security controls and telemetry logging.

### Ethical Considerations in AI Security

* Ethics, Privacy, and Compliance
  + Addressing ethical concerns in cybersecurity for AI.
  + Ensuring data privacy, model transparency, and regulatory compliance.
  + Managing bias and fairness in AI security protocols.