

# AI Security Architecture Training

**Architect, Secure, and Defend  
Modern AI-Enabled Environments**



## Course Highlights



16-Hour LIVE Instructor-led Training



Hands-on Labs Integrated Across Multiple Modules



Perform AI Threat Modeling and Attack-Path Analysis



Apply Practical Security Engineering, Architecture, and Defence



Assess OWASP LLM, Agentic AI, and ML Threats



Identify Memory, Context, and RAG Abuse Paths



Analyze Agent Internals and Security Vulnerabilities



Build Layered Controls for AI Systems



Test AI Security Controls and Assurance Mechanisms

## About Course

The AI Security Architecture Training is designed for security professionals seeking practical expertise in securing modern AI-enabled environments. The course examines how LLM platforms, agentic systems, RAG architectures, AI infrastructure, and external dependencies introduce new security considerations beyond traditional applications. Participants learn to analyze AI architectures, identify attack paths, assess AI-specific threats, apply security controls, and evaluate system resilience through integrated hands-on labs. The program also covers governance, risk management, compliance, agent vulnerabilities, AI-assisted attacks, testing, assurance, and secure design patterns, helping participants translate cybersecurity principles into practical architecture and engineering decisions for real-world AI systems.

## Course Objectives

Upon successful completion of the training, participants will be able to:

- ✓ Understand how LLMs, AI platforms, & MLOps environments differ from traditional applications
- ✓ Analyze the architecture & security boundaries of modern AI-enabled systems
- ✓ Apply governance, risk management, & compliance principles to AI environments
- ✓ Conduct threat modeling for AI, LLM, & multi-agent architectures
- ✓ Identify AI-specific attack surfaces & emerging adversarial techniques
- ✓ Assess risks associated with memory, context, RAG, MCP, & A2A architectures
- ✓ Apply defense-in-depth principles across AI systems & infrastructure
- ✓ Evaluate security controls through practical testing and assurance activities
- ✓ Identify vulnerabilities within agent architectures & workflows
- ✓ Apply secure design patterns to agentic AI systems
- ✓ Assess external dependencies, third-party components, & AI supply chain risks
- ✓ Translate AI security risks into practical architectural controls & defensive strategies

## Target Audience

This course is ideal for cybersecurity professionals who already understand foundational security concepts and want to develop deeper architectural and engineering expertise for AI-enabled environments.

- ✔ **Security Architects** responsible for designing secure enterprise architectures and integrating AI-related security requirements
- ✔ **Security Engineers** responsible for implementing, testing, and operating security controls and technologies
- ✔ **GRC Professionals** responsible for governance, risk, compliance, security frameworks, and emerging AI-related risks
- ✔ **Cloud Architects** responsible for designing and securing cloud environments supporting AI workloads and services

## Pre-requisites

Participants should have a basic understanding of cybersecurity and core security concepts. This is not an introductory cybersecurity or AI course.

Participants should be comfortable with:

- ✓ Security architecture and security controls
- ✓ Threats, vulnerabilities, and risk
- ✓ Authentication and authorization
- ✓ Network and application security
- ✓ Security monitoring and incident response

The course builds on these concepts to address advanced AI security architecture, attack surfaces, and defensive engineering.

# Course Content

## **Module 1**

### **AI Foundations for Architects**

**Objectives:** Understand enough of how LLMs and AI platforms work to reason about where they break.

- 1.1 Basics of LLMs
- 1.2 Why AI infrastructure is not a traditional application
- 1.3 Anatomy of an AI system
- 1.4 MLOps

## **Module 2**

### **Governance, Risk Management and Compliance (GRC)**

**Objectives:** Translate AI risk into governance structures, controls, and audit-ready evidence.

- 2.1 Governance structure
- 2.2 Frameworks and regulations
- 2.3 AI risk management
- 2.4 Compliance evidence

## Module 3

### AI Threats

**Objectives:** Systematically identify threats to AI systems, including multi-agent designs.

- 3.1 Threat modeling basics and flows
- 3.2 Threat modeling AI systems
- 3.3 Multi-Agent Systems (MAS)

## Module 4

### AI Attack Surface

**Objectives:** Know the concrete attack techniques and the architecture-level mitigations.

- 4.1 OWASP Top 10 for LLM Applications, OWASP Agentic AI threats and OWASP ML Top 10 for non-LLM models.
- 4.2 Memory and context abuse
- 4.3 RAG system attacks
- 4.4 MCP and A2A

## Module 5

### AI Defense and Security AI Agents

**Objectives:** Build layered defenses and understand where AI can strengthen security operations.

- 5.1 Defense-in-depth for AI systems
- 5.2 Testing and assurance
- 5.3 Security AI agents

## Module 6

### Agent Architecture and Vulnerabilities

**Objectives:** Analyze agent internals and design secure agentic systems.

- 6.1 Agent anatomy
- 6.2 Agent vulnerabilities
- 6.3 Secure agent design patterns

## Module 7

### External Dependencies

**Objectives:** Manage third-party and supply chain risk across the AI stack.

- 7.1 Dependency map
- 7.2 Risks
- 7.3 Controls

**Note:** Labs will be integrated with multiple sections to supplement Theory with practical.

## Lab Prerequisites and Requirements

### System Requirements

Participants are required to have access to a computer that meets the following minimum specifications:

| Component        | Requirement                                       |
|------------------|---------------------------------------------------|
| Operating System | macOS, Windows, or Linux                          |
| CPU              | 4 or more cores recommended                       |
| RAM              | 8 GB minimum; 16 GB recommended                   |
| Disk Space       | At least 10 GB of free disk space                 |
| Internet Access  | Required for initial software downloads and setup |

**Note:** Admin access to the machine may be needed to run some of the software so personal computers are preferred over corporate machine that may limit access.



**Contact us**

[www.infosectrain.com](http://www.infosectrain.com)  
[sales@infosectrain.com](mailto:sales@infosectrain.com)

**Follow us on**

