

IT MANAGEMENT AND CYBER SECURITY | IMCS-035

AI Security: Protecting Machine Learning Systems

Contact

+31 85 7444446
info@aractech.com
https://aractech.com

Address

Waarderweg 50, 2031PB Haarlem - Netherlands.

Course content

Why Attend

As organisations deploy AI and machine learning, attackers are targeting these systems through data poisoning, model theft, prompt injection and adversarial inputs. AI systems need specific security controls.

This Aractech course explains AI system architectures, AI-specific threats, securing training data and models, protecting large language model applications, AI supply chain risks, monitoring and incident response for AI, and governance frameworks. Participants threat-model an AI application.

Course Methodology

- Technical presentations
- Threat modelling workshop
- Demonstrations
- Case studies
- Governance discussions

Course Objectives

- Explain AI system components and attack surfaces
- Identify AI-specific threats
- Protect training data and models
- Secure large language model applications
- Manage AI supply chain risks
- Monitor and govern AI security

Target Audience

- Security engineers and architects
- AI and data science teams

Course content

- IT risk managers
- Application developers

Course outline

Detailed course outline

Day-by-day outline for AI Security: Protecting Machine Learning Systems.

Day 1 - AI Systems and Risks

- 09:00-09:39 | AI system architecture
- 09:39-10:18 | Attack surfaces
- 10:18-10:57 | AI threat landscape
- 10:57-11:00 | Frameworks
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Frameworks (continued)
- 12:05-12:43 | Regulation
- 12:43-14:00 | Exercise: AI inventory

Day 2 - Attacks on Machine Learning

- 09:00-09:39 | Data poisoning
- 09:39-10:18 | Evasion attacks
- 10:18-10:57 | Model theft
- 10:57-11:00 | Privacy attacks
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Privacy attacks (continued)
- 12:05-12:43 | Defences
- 12:43-14:00 | Demonstration: Adversarial example

Course outline

Detailed course outline

Day-by-day outline for AI Security: Protecting Machine Learning Systems.

Day 3 - Securing LLM Applications

- 09:00-09:39 | Prompt injection
- 09:39-10:18 | Data leakage
- 10:18-10:57 | Output handling
- 10:57-11:00 | Guardrails
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Guardrails (continued)
- 12:05-12:43 | Access control
- 12:43-14:00 | Workshop: LLM threat model

Day 4 - Supply Chain and Operations

- 09:00-09:39 | Model and data provenance
- 09:39-10:18 | Third-party models
- 10:18-10:57 | Monitoring
- 10:57-11:00 | Incident response
- 11:00-11:30 | Coffee break
- 11:30-12:05 | Incident response (continued)
- 12:05-12:43 | Testing
- 12:43-14:00 | Case study: AI security incident

Course outline

Detailed course outline

Day-by-day outline for AI Security: Protecting Machine Learning Systems.

Day 5 - Governance

- 09:00-09:45 | AI security policies
- 09:45-10:30 | Risk assessment
- 10:30-11:00 | Roles
- 11:00-11:30 | Coffee break
- 11:30-11:45 | Roles (continued)
- 11:45-12:30 | Metrics
- 12:30-13:15 | Roadmap
- 13:15-14:00 | Capstone: AI security plan

Seminar dates

Available seminar dates

Live dates and pricing for AI Security: Protecting Machine Learning Systems generated from the course details page.

Date	Location	Format	Fee
2 - 6 November 2026	Vienna	Classroom	€3,225
9 - 13 November 2026	Barcelona	Classroom	€2,815
14 - 18 December 2026	Paris	Classroom	€3,825
21 - 25 December 2026	Barcelona	Classroom	€2,815
18 - 22 January 2027	London	Classroom	€2,315
15 - 19 February 2027	Frankfurt	Classroom	€1,875
15 - 19 March 2027	Geneva	Classroom	€4,315
19 - 23 April 2027	Istanbul	Classroom	€1,978
17 - 21 May 2027	Vienna	Classroom	€3,225
21 - 25 June 2027	Barcelona	Classroom	€2,815

Seminar dates

Available seminar dates

Live dates and pricing for AI Security: Protecting Machine Learning Systems generated from the course details page.

Date	Location	Format	Fee
19 - 23 July 2027	Cape Town	Classroom	€1,625
16 - 20 August 2027	Geneva	Classroom	€4,315
20 - 24 September 2027	Rome	Classroom	€3,460
18 - 22 October 2027	Cape Town	Classroom	€1,625
15 - 19 November 2027	Dubai	Classroom	€1,845
20 - 24 December 2027	London	Classroom	€2,315
2 - 6 November 2026	Online / Live	Online / Live	€1,815
9 - 13 November 2026	Online / Live	Online / Live	€1,815
14 - 18 December 2026	Online / Live	Online / Live	€1,815
21 - 25 December 2026	Online / Live	Online / Live	€1,815

Seminar dates

Available seminar dates

Live dates and pricing for AI Security: Protecting Machine Learning Systems generated from the course details page.

Date	Location	Format	Fee
18 - 22 January 2027	Online / Live	Online / Live	€1,815
15 - 19 February 2027	Online / Live	Online / Live	€1,815
15 - 19 March 2027	Online / Live	Online / Live	€1,815
19 - 23 April 2027	Online / Live	Online / Live	€1,815
17 - 21 May 2027	Online / Live	Online / Live	€1,815
21 - 25 June 2027	Online / Live	Online / Live	€1,815
19 - 23 July 2027	Online / Live	Online / Live	€1,815
16 - 20 August 2027	Online / Live	Online / Live	€1,815
20 - 24 September 2027	Online / Live	Online / Live	€1,815
18 - 22 October 2027	Online / Live	Online / Live	€1,815

Seminar dates

Available seminar dates

Live dates and pricing for AI Security: Protecting Machine Learning Systems generated from the course details page.

Date	Location	Format	Fee
15 - 19 November 2027	Online / Live	Online / Live	€1,815
20 - 24 December 2027	Online / Live	Online / Live	€1,815