TRAINING PROGRAMS · 2026–2027

AI SECURITY
SIMPLIFIED
EU AI SECURITY & COMPLIANCE

AI SECURITY SIMPLIFIED

Live training. Built by a practitioner.

30
years IT & security

10+
years AI security

7
countries trained

aisecuritysimplified.ie

+353 1 960 9264

FLAGSHIP COURSE

AI Security — Simplified

The 2-day course this entire program is built around.

DATES **October 20–21, 2026**	TIME **9:00 AM – 5:00 PM daily**
VENUE **The Dylan Hotel, Dublin**	INVESTMENT **€1,350**
FORMAT **2 days · in-person · capped at 18 seats**	AUDIENCE **Technical, privacy & AI governance teams**

What You'll Walk Away With

— Practical defenses against prompt injection, jailbreaking, data poisoning, model theft, and RAG / supply-chain attacks

— A working map of your AI risk to the OWASP LLM Top 10, MITRE ATLAS, and NIST AI RMF frameworks

— The ability to ask any AI vendor, or any engineering team, the questions that actually matter

---

30 years IT & security · 10+ years AI security · AIGP Consultant · Former FBI data security trainer

COURSE AGENDA

14 Modules Across Two Days

Every module pairs the attack with the defense — not just theory.

DAY 1 — 9AM–5PM

1. AI Fundamentals & Threat Landscape
2. Adversarial Machine Learning
3. Data & Model Poisoning
4. Prompt Injection (OWASP #1 LLM risk)
5. Model Extraction & Theft
6. Supply Chain Risk
7. Agentic AI & Excessive Agency

DAY 2 — 9AM–5PM

8. Deepfakes & Synthetic Media
9. AI-Powered Social Engineering
10. Privacy & Sensitive Info Disclosure
11. EU AI Act — What Security Teams Need to Know
12. Vendor & Third-Party AI Risk
13. Incident Response for AI Systems
14. Building an AI Security Program — capstone tabletop exercise

OWASP LLM Top 10 **MITRE ATLAS** **NIST AI RMF** **EU AI Act**

This is the most important class you can take this year, as a manager, IT Engineer, or C-Suite executive, to secure your company and boost your CV.

BEYOND THE FLAGSHIP

Upcoming Classes

The full 2026–2027 training lineup.

AIGP Certification Class

2 days · 9:00 AM–5:00 PM · In-person

Audience: C-suite, senior managers, IT & privacy staff

— Full IAPP AIGP body-of-knowledge coverage, taught by an AIGP-credentialed practitioner

— Real-time Q&A on EU AI Act obligations as they apply to your organization

— Certificate of completion and exam voucher included

AI Data Security for the C-Suite

1 day · Executive briefing · In-person or on-site

Audience: CEOs, boards, CISOs, department heads

— What "AI data security" means for your business, in plain, board-ready language

— The vendor questions almost no one is asking about how AI tools handle company data

— Leave with a one-page AI data risk framework for your next board meeting

AI Data Security Fundamentals

2 days · In-person

Audience: IT & security teams new to AI-specific data risk

— How data actually moves through an AI system — training, inference, memory, logs

— Spotting sensitive data exposure in prompts, outputs, and third-party AI tools

— Practical data classification and DLP approaches built for AI, not bolted on

AI DATA SECURITY TRACK

Upcoming Classes, Continued

Deeper technical and governance tracks for the AI data security niche.

Securing the AI Data Pipeline

2 days · Technical, hands-on

Audience: Engineers, architects, ML/AI teams

— Protecting ingestion, embeddings, and vector databases in RAG systems

— Fine-tuning data protection, provenance, and lineage tracking

— Encryption and access control at every stage of the pipeline

AI Data Governance & Regulatory Compliance

2 days · In-person

Audience: Privacy, legal, compliance & governance teams

— Where the EU AI Act and GDPR intersect on AI training and inference data

— Data minimization, retention, and cross-border transfer for AI systems

— Building the audit trail regulators actually expect to see

AI Vendor & Third-Party Data Risk

1 day · In-person or on-site

Audience: Procurement, security & vendor-risk teams

— The right questions to ask any AI vendor before you sign

— Finding “shadow AI” already running inside your organization

— A practical framework for ongoing third-party AI data risk review

Private / on-site delivery available worldwide — every course is built to travel.

TRAINING PROGRAMS · 2026–2027

AI SECURITY
SIMPLIFIED
EU AI SECURITY & COMPLIANCE

AI SECURITY SIMPLIFIED

Live training. Built by a practitioner.

+353 1 960 9264
Brian.Harper@aisecuritysimplified.ie
77 Camden Street Lower, Saint Kevin's, Dublin, D02 XE80, Ireland