

AI Security Simplified™

THE FIRST 24 HOURS DECIDE THE NEXT 24 MONTHS.

Containment. Recovery. Reporting. Communication.

Then a room full of people who will never be surprised by a perfect voice again.



Consulting —
data minimization, provenance,
agent kill-switch, IR

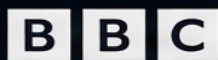


Training —
2-day flagship, bootcamp,
AIGP path



HSBC

Bank of America



AIB



Uber

amazon



aisecuritysimplified.ie



contact@aisecuritysimplified.ie

TWO ENGINES. ONE FIRM.

Consulting in the stack. Training in the room.

CONSULTING

- Data that must never become a prompt — minimization, redaction, index scope
- Agents that must be able to die — *kill switch, token revoke, egress cut*
- The first 24 hours — *detect, classify, assemble, preserve, contain*
- Provenance and detection as signals — *not as a verdict.*

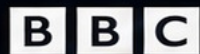
TRAINING

- Flagship: *AI Security — Simplified* • 2 days • 20-21 Oct 2026 • The Dylan, Dublin • €1,395
- Agenda punch: prompt injection, poisoning, agentic risk, deepfakes, *EU AI Act, AI IR, tabletop*
- Also: *4-day Bootcamp* • *AIGP* certification path
- *Private / on-site* for the team that cannot wait for a public date.



HSBC

BANK OF AMERICA



Uber

amazon



aisecuritysimplified.ie



contact@aisecuritysimplified.ie

THE MODEL IS NOT THE VAULT. THE PIPE IS.

Data did not need to be secret. It needed to be present, specific, and in the wrong room.

1.

MEMORIZED

What was on the open web, in a ticket, or in a few-shot example can come back as a completion.

2.

WRONG ROOM

A deal-team folder retrieved for a marketing prompt. Shared memory. Sloppy index. Cross-context leakage.

—.

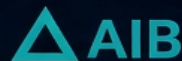
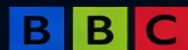
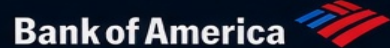
STILL ACTING

An agent that can mail, pay, or deploy after you noticed the incident is not contained. It is still at work.

4.

BELIEVED

A perfect voice or a live video is not authentication. High-stakes asks still need a second channel you already own.



AMERICAN EXPRESS



AI Security Simplified™

CONSULTING THAT CHANGES THE STACK

We do not sell a detector and leave. We shrink what the model can see, what it can do, and how long it can keep doing it.

1.

MINIMIZE THE PILE

Collect less. Index less. Keep logs shorter. Send the model a clause, not the contract.

2.

SCOPE THE INDEX

RAG and copilots see this team and this ticket. Not the whole drive. Wrong-room leakage starts with a search that can see both rooms.

3.

GIVE THE AGENT A DEATH

Kill switch: halt tool calls, revoke tokens, cut egress. If it can still pay or mail, you have not contained it.

4.

RUN THE FIRST 24 HOURS

Detect, classify, assemble, preserve, then contain. Snapshots before helpful deletes.

5.

TREAT DETECTION AS ONE SIGNAL

Provenance, source path, incentive, and a second channel you already own. A score is not a verdict.



Engagements start with a scoped discovery. They end with controls your team can operate.



HSBC

Bank of America



Uber



AI Security **Simplified**TM

TRAINING THAT CHANGES THE ROOM.

Not a compliance seminar. Live AI security,
taught by someone who **does the work**.

FLAGSHIP

AI Security – Simplified



2 days · 9:00-17:00 · 20-21 October 2026



The Dylan Hotel, Dublin · €1,395



Audience: technical, privacy, and AI governance teams



Day 1: fundamentals, adversarial ML, poisoning, prompt injection, model theft, supply chain, agentic AI



Day 2: deepfakes, AI social engineering, privacy disclosure. EU AI Act, vendor risk, AI incident response, capstone tabletop.

ALSO IN THE LINEUP

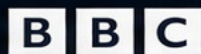
- 4-day AI Security Bootcamp – for people who must build it
- AIGP certification training – exam path plus EU AI Act as it hits your org
- Private / on-site – same material, your stack, your calendar.

**Oct 6-7 Dublin sold out.
Oct 20-21 is the next public seat.**



HSBC

BANK OF AMERICA



Uber



AI Security Simplified™

HOW AN ENGAGEMENT RUNS

Discover. Harden. Drill. Leave a program
your people can run on a Tuesday.

1 DISCOVER



Where data meets models,
indexes, agents, and tools.
What can be seen. What
can still act.

2 HARDEN



Minimize the pile. Scope
the index. Fit a kill switch.
Put a human gate on
irreversible actions.

3 DRILL



Tabletop the first 24 hours:
confirm, classify, assemble,
preserve, contain. Then
communicate.

4 LEAVE IT RUNNING



Playbooks, owners, and
a second channel for
high-stakes asks. We
leave. The controls stay.

Consulting can stand alone. Training can stand alone. The strongest work is both.



aisecuritysimplified.ie

contact@aisecuritysimplified.ie

AI Security Simplified™

PICK THE ROOM OR PICK THE STACK. OR PICK BOTH.



1 – BOOK THE FLAGSHIP

AI Security – Simplified
20-21 October 2026 • The Dylan Hotel, Dublin

aisecuritysimplified.ie/training

2 – START A SCOPING CALL

Consulting that changes what the model
can see and do.

contact@aisecuritysimplified.ie

3 – BRING IT ON-SITE

Private training on your stack,
your calendar.

The first 24 hours decide the next 24 months. Do not wait for the perfect voice.



aisecuritysimplified.ie

contact@aisecuritysimplified.ie