SECURITY ARCHITECT · SECURE BY DESIGN TRAINING

Your teams find problems well. *I teach them to design the answer.*

I'm Fabien Soulis. In fifteen years inside large enterprises I learned that the hardest shift in security isn't technical, it's moving from executing tasks to structuring a posture. In four hands-on weeks I install that thinking in your consultants and engineers, and they finish on a real engagement with me alongside them. Here is what they walk away able to do, and why it earns its budget.

Fabien Soulis · 15 years in enterprise security **Taught** · Secure by Design at Paris 1 Panthéon-Sorbonne
Remote · delivered in French, English or Spanish

IN ONE PARAGRAPH

A four-week program that turns your engineers into the security checkpoint every project consults.

Not a certification, a posture. Hands-on, built on real cases from inside enterprises I have lived through, and it ends on your own live engagement, with me reviewing the work line by line.

- Your people learn to run a risk analysis and write it down, project after project.
- They get project teams to involve them before decisions, not after the breach.
- They produce deliverables that hold up in front of a CISO, a steering committee or an auditor.
- The capability stays inside your company, in your own people.

01 WHY NOW

The pressure is already on your teams

When a client or a new regulation asks for Security by Design, someone on your team has to know where to start. Increasingly, that is not optional. A documented risk-analysis and protection-by-design practice is written into the standards your clients and auditors hold you to.

WHAT THEY ALL ASK

Auditors, clients and regulators arrive at the same place: show me how you analyze and manage your risks.

FRAMEWORK	WHAT IT ASKS OF YOU
ISO 27001	A formal information-security risk analysis, embedded in your management system.
ISO 27005	The detailed method for running that risk analysis, applied consistently.

FRAMEWORK	WHAT IT ASKS OF YOU
GDPR	Data protection by design, and a data-protection impact assessment (DPIA) for risky processing.
PCI DSS	Targeted risk analyses for how you protect cardholder data.
CRA · Cyber Resilience Act	The same risk discipline from anyone shipping a product with digital elements into Europe.

That answer only exists if someone on your team can run the analysis and write it down, project after project. That is exactly what I train.

02 THE PROGRAM

Four weeks, real projects

Nothing here is theory I haven't lived, inside large organizations and as a consultant. Each phase builds on the last, and each one produces something real.

PHASE	WHAT YOUR PEOPLE LEARN	WHAT THEY CAN DO AFTER
Week 1 Think like an attacker, defend like a strategist	The CIA triad and impact types; how attackers move on Windows, Linux, Active Directory and cloud (Azure, GCP, M365); and the preventive, detective and corrective countermeasures for each.	See the full spectrum of what can go wrong, and rate each risk by probability and impact.
Weeks 2–3 Become the security checkpoint	How to get informed early, evaluate proposed solutions, propose measures that get accepted, and secure formal risk acceptance, learned by dissecting real disasters.	Get project teams to consult them before decisions, not after the breach.
Week 4 Risk-analyze an AI helpdesk agent	Threat actors, attack scenarios and the full control taxonomy for the AI agent every company is racing to deploy. I review the work line by line.	Produce a complete AI-agent risk register an executive committee will sign.
Shadowing Real work, real conditions	They bring a live task from their own work, and we run it together, with me alongside them, not ahead of them.	Turn the framework into instinct, on work that actually matters to you.

03 THE DELIVERABLES

What your people take back to work

They don't leave with a certificate. They leave with artifacts and a method they reuse on every future project.

1. **A repeatable risk-analysis methodology**
   One method that transfers to any IT or cloud project your teams touch.
2. **Board-ready deliverables**
   Risk analyses and Secure-by-Design reviews that hold up in front of a CISO, a steering committee or an auditor.
3. **Security involved early**
   People who pull project teams in before problems, cutting the cost of late fixes and shadow IT.

04 WHAT YOU GET

Why it's worth the budget

This is loss-avoidance and enablement, not overhead. Four ways it pays you back.

01 **Pass audits and client due-diligence**
Your people answer the "show me your risk process" question with real deliverables, and stop losing ground in security questionnaires and RFPs.

02 **Regulatory readiness in-house**
Meet ISO, GDPR, PCI DSS and CRA expectations with your own people, instead of buying a consultant for each new project.

03 **Fewer expensive surprises**
Teams that involve security early avoid the shadow IT and late redesigns that quietly cost the most.

04 **Capability that stays**
The skill, and the person who holds it, stays inside your company.

HOW IT WORKS

Small group, low disruption, alongside their real work.

- **Who.** One to three of your consultants or engineers, ideally with a current project to bring.
- **How long.** Four structured weeks plus a shadowing phase on a real engagement.
- **Time.** About half a day per week, running alongside their work, not instead of it.
- **Format.** Remote by default, optional in-person, in French, English or Spanish.

Beyond the four weeks, I also help teams run the process week after week with Risk Expert, the software I built, and review live deliverables when it gets real.

MY PROMISE, AND THE FIRST STEP

Start with a free audit of your context

This program doesn't promise miracles. It gives your people a structured path and someone to work through it with them. If they put the work in, the change is visible within three months. Before anything else, a no-commitment call, and I'll tell you plainly if I can help or not.

01 **A call**
You tell me how security decisions really get made, and what your clients and auditors are asking for.

02 **A written action plan**
How a Secure by Design process fits your context, and in what order to build it.

03 **No commitment**
Free, and yours to keep. Book it at https://www.securityarchitect.xyz/