

SECURITY, ARCHITECTURE AND AI

# Ongoing advisory

Someone with twenty years in security and development to ask before deciding.

Some months they consult me a lot and others hardly at all, and over time it evens out. Since I follow each company month after month, when a question comes in I already know the system and why each thing was decided.

---

**Fixed price**

no hours counted

**WhatsApp**

straight to me

**Same day**

answers, on working days

**Monthly**

no lock-in

## WHY IT EXISTS

# The costliest decisions get made with nobody to check them with

A development team decides things every week that are expensive to undo later. Which library to bring in, how to build an API's authorisation, whether an AI agent may touch production, what to do with the last pentest report.

There is rarely a security person sitting next to them. So the decision is made with whatever is at hand, and the problem shows up months later, when fixing it is already expensive.

Hiring someone senior full time for this does not pay off for many teams. One-off consulting does not either, because every time the system has to be explained from scratch.

That is why I work with each company for months. When a question comes in, I already know the system.

## What it includes

- 01 The sessions the work calls for, with me and with whoever the company chooses, from the CTO to whoever owns each topic. We agree the rhythm at the start and adjust it as we go.
- 02 Direct WhatsApp with me for whatever comes up between sessions.
- 03 Answers the same working day.

# What a month of work looks like

---

01

## Nobody watching the clock

The price is fixed and hours are not counted. Some months we will work a lot together and others it will hardly be needed. Over time it evens out, and neither of us has to log hours.

---

02

## Sessions at an agreed pace

At the start we agree how often we meet, based on the team and what it has open, and we change it whenever needed. I sit down with whoever the company chooses and we go over what is open: a design, a code review, a finding, an AI tool. The idea is to leave each session knowing what will be done.

---

03

## Between sessions, on WhatsApp

What comes up day to day cannot wait for the next session. The team messages me directly and I answer the same working day.

---

04

## Over time, like someone on the inside

This works better the longer it lasts. Every month I know a bit more about the system and the people, and I remember why each thing was decided. After a while they consult me like someone from the house, and that is when I add the most.

## WHAT WE COVER

# Security, AI and architecture, on the real system

These are the topics that come up most. If the case is about something else, we look at it on the first call.

### Code and API security

Authorisation, secrets management, dependencies, reviewing a design before it is built or a finding before deciding what to fix first.

### AI and agent security

What an agent may touch, how to protect an MCP server, what risks come with putting a model into a flow with customer data.

### Productivity with AI

Claude Code, Copilot and the like: how to use them in the team so they really help, without opening new holes.

### Architecture and technical decisions

Choosing between two paths, reviewing a design before the company commits to it, or thinking through how something will grow.

### Security architecture

How authentication, permissions, network and sensitive data fit together when the whole system is looked at at once.

### Offensive and defensive security

Reading a pentest report, separating what is serious from what can wait and knowing what to look at next.

### Python and performance

Slow Python code, concurrency, async, and where to start measuring.

## WHO IT IS FOR

# For technical teams that decide on their own

### A good fit if

- Companies with a development team and nobody dedicated to security.
- Teams bringing AI or agents into the product or into their daily work.
- Companies that want to check the big decisions before making them.
- Companies that prefer a long relationship to one-off consulting.

### What it does not include

- On-call or 24/7 availability
- Incident response
- Writing the team's code
- Full training: workshops are separate

## WHO I AM

# Security and development, from both sides



I'm Daniel Alfocea, and I've spent twenty years in development and security. At Banco Santander I was Principal Engineer in the AI department while the area was being set up. At BBVA I was Cybersecurity Tech Lead. At 42Crunch, in the UK, I was responsible for one of its API security products.

I've presented research at RSA Conference and OWASP AppSec EU, and I'm a regular speaker at RootedCON. I founded Navaja Negra and the OWASP Madrid chapter. I'm the author of security tools such as GoLismero, Plecost and Dockerscan, and with Alfonso Muñoz I wrote *Secure MCP: A practical guide for developers, software architects and tech leads*.

## What people usually ask

---

### How much does it cost?

From €990 a month plus VAT, at a fixed price. The exact figure depends on the team and what it has on its plate, and I give it on the first call.

---

### How many hours does it include?

It does not go by hours. Some months there is more work and others less, and over time it evens out. How often we meet is agreed at the start and adjusted whenever needed.

---

### What if it does not work for us?

It can be dropped any month, simple as that. I see it as a long-term thing, and those who stay do so because it works for them.

---

### Who from the team do you talk to?

Whoever the company chooses. It can be the tech lead, the CTO or whoever has each topic on their plate.

---

### What if we have an incident?

Incident response and on-call are not included. If it happens, they message me and we see separately whether I can help.

---

### Do you write code?

No. I help decide and I review what the team does, but the code is theirs to write.

---

### What if we want to train the team?

One-day workshops and six-week programmes are separate. They are at [danielalfocea.com/en/formacion](https://danielalfocea.com/en/formacion).

## HOW WE START

# Three steps, and the first one is free

1

### A 15-minute call

We talk about what is on the table and at the end I say whether I can help. If I do not see it clearly, I say that too.

Free

2

### A diagnostic session

I review the system and what is open, and at the end I say where I would start.

€290 + VAT, credited against the first month if we continue

3

### The advisory, month to month

Sessions at the pace we agree and direct WhatsApp with me.

Price

# From €990

a month, plus VAT, at a fixed price and with no lock-in.

**Book the 15 minutes**

EMAIL

[me@danielalfocea.com](mailto:me@danielalfocea.com)

ONLINE

[danielalfocea.com/en/servicios](https://danielalfocea.com/en/servicios)