

SIX-WEEK PROGRAMME FOR TECHNICAL TEAMS

OWASP in the team's code: a six-week programme

Six weeks that leave the repository changed and the improvement measured in numbers.

First I measure where the team stands. Then I run the secure development workshop, review real pull requests from the team in writing and measure again in week 6. The company ends up with the controls in its repository, the evidence for the auditor and a before and after built from the team's own numbers.

6

weeks, from the baseline to the final review

90 min

remote review in week 6

5

phases, each with a deliverable

4 to 6

indicators agreed with the team

WHERE TEAMS START

The team leaves the course fired up and three weeks later the code looks the same as ever

If training is a single day, what people learned has to compete with the sprint, the deadlines and the incidents. Broken access control, injection and secrets in git history stay where they are, however well the team understood them on a Tuesday. They go when someone looks for them in the code, fixes them and leaves a test so they don't come back.

And whoever asks for training often wants proof of it. If the company sells to banks, handles payments, holds ISO 27001 or goes through a SOC 2 audit, developer training has to be documented, with date, content and attendees. An attendance sheet sometimes falls short.

The programme covers both. I measure the starting point, move from the workshop into the company's repository by reviewing real changes, and finish by measuring again so whoever decides can see what moved and what didn't.

The five phases of the programme

01 Diagnosis and baseline

Week 0. A 10-minute survey of the team, a sample of the company's code and 4 to 6 agreed indicators.

02 In-person workshop (5 to 8 hours depending on the team)

Week 1. Labs adapted to the team's stack, and the last part of the day spent on the company's repository.

03 Evidence and leadership report

Weeks 1 and 2. An evidence pack for the auditor and a 3 to 5 page report with 5 prioritised actions.

04 Questions and pull request review

Weeks 1 to 5. A channel to ask me things, with a closing date, and a written review of 2 or 3 of the team's pull requests.

05 Review and second measurement

Week 6. Ninety minutes remotely and the comparison with the baseline.

Five phases, one deliverable each. At the end there is a comparison built from the team's numbers.

WHAT THE PROGRAMME DELIVERS

What the company has at the end of week 6

All of this can be shown to whoever has to approve it. None of it depends on me promising a percentage.

01

A measured starting point

Indicators we choose together, measured on the company's own code and pipeline before a single hour of training.

Evidence: a diagnosis sheet with the week 0 values.

02

Controls in the company's repository

In the last block of the workshop I leave the configurations and the pull request checklist on a branch of the repository, and the team reviews and merges them.

Evidence: a branch with the changes, in the company's repository and under its permissions.

03

Leadership gets decisions to make, with no slide deck in between

Three to five pages with what came out of the diagnosis, what we worked on and five prioritised actions, each with a proposed owner.

Evidence: a leadership report delivered in week 2. Careful, it is not an audit.

04

The workshop applied to real pull requests

Two or three of the team's changes reviewed in writing with the same guidelines as the workshop, so the team sees how they apply to its own code and not to a practice app.

Evidence: written comments on the team's own pull requests.

05

A before and after with the team's numbers

The same indicators from week 0, measured again in week 6, with what moved, what didn't and what I think happened.

Evidence: a comparison of week 0 against week 6.

Six weeks, five phases

Every phase has an owner (the team or me) and a deliverable. The programme includes the full secure development workshop, and its syllabus is on its own page.

Week 0

Diagnosis and baseline

The team answers a 10-minute survey about its stack, its practices and its doubts. I look at a sample of code and pipeline that the team lets me see, and we agree 4 to 6 indicators. With all of that I adapt the labs to the team's stack.

Deliverable: A diagnosis sheet with the baseline measurement.

Week 1

In-person workshop (5 to 8 hours depending on the team)

I run the full workshop at the company's premises. We do the last block on the company's repository, and there I leave the configurations and the pull request checklist on a branch. The team decides what to merge.

Deliverable: A branch with configurations and checklist; individual certificates.

Weeks 1 and 2

Evidence and leadership report

I prepare the evidence pack from the attendance signed on the day of the workshop. With what came out of the diagnosis and the block on the company's own code, I write the leadership report, present it and we go through it together.

Deliverable: Evidence pack and a 3 to 5 page report with 5 prioritised actions.

Weeks 1 to 5

Q&A channel and pull request review

We open a channel in the company's Slack or Teams. I reply within two working days and it closes at the end of week 5. The team sends me two or three pull requests it wants reviewed with the workshop's guidelines and I comment on them in writing.

Deliverable: Written comments on 2 or 3 pull requests.

Week 6

Remote review and second measurement

Ninety minutes with the team to see what has been applied, what has not and why, and to adjust the configurations if needed. Before the session we repeat the measurement with the same indicators as in week 0.

Deliverable: A comparison between week 0 and week 6.

Week 1 is the full workshop. Its syllabus, labs and agenda are at danielalfocea.com/en/formacion/workshop-desarrollo-seguro

We choose the indicators together and measure them twice

I don't promise that the code will have a given percentage fewer vulnerabilities. It depends on what the team applies, and any figure I gave would be made up. What I do is measure the same things before and after, with the team's data, and report what moved. These are the candidates, and we pick between four and six.

SAST findings per pull request

How many new findings come in with each change, measured over a window of pull requests before and another after.

Pull requests reviewed with the authorisation checklist

What share of the changes that touch endpoints goes through the programme's checklist.

Secrets found in the repository and its history

How many a secret scanner finds, and how many have been rotated and removed by week 6.

Dependencies with a known vulnerability and time to fix

How many the repository has and how long the team takes to update the critical ones.

Pipelines with a lockfile and actions pinned by SHA

What share of pipelines installs from the lockfile and references actions by full commit.

Team confidence, by survey

The same questions in week 0 and week 6 on whether people know how to review authorisation, inputs and dependencies. It is a perception and I report it as one.

Course or programme

NEED	WORKSHOP	PROGRAMME
The team learns to exploit and fix the most repeated flaws.	The course is fine. One day, six labs and the block on the company's own code.	Includes the whole course.
Knowing whether anything has changed weeks later.	It measures nothing. The team takes templates away and the measuring is left to the team.	Measured in week 0 and week 6, with the same indicators.
Leadership sees what to do and in what order.	No report. The findings stay with the team.	A 3 to 5 page report with five prioritised actions.
The team applies the workshop to its own code, with someone reviewing.	Everyone works on their own laptop during the last block.	A Q&A channel and written review of 2 or 3 of the team's pull requests.

WHAT STAYS WITH THE COMPANY

Programme deliverables

Everything belongs to the company from the week it is delivered. The lab material comes with an internal-use licence for 12 months.

Diagnosis sheet

What the team answers in the survey, what I see in the code sample and the baseline indicators.

Configurations and PR checklist on a branch of the repository

A per-endpoint authorisation checklist and CI gates adapted to the team's pipeline. It is a technical template and the team reviews it before merging.

Compliance evidence pack

Signed attendance, an individual certificate with date, hours and content, a syllabus mapped to the standards that apply to the company, and a one-page letter for the auditor.

Leadership report

Three to five pages with five prioritised actions and a proposed owner for each.

Written review of 2 or 3 pull requests

Comments on the team's real changes, on the company's platform or on fragments, whichever the team prefers.

Measurement comparison

Week 0 and week 6 with the same indicators, and what I would keep an eye on over the following months.

Lab repository with solutions

ByteBazaar, the lab briefs and the solutions. Internal-use licence for 12 months, to run them again with new joiners.

INCLUDED IN THE PROGRAMME

Four things the company keeps on top of the six weeks of work

They are the same ones that come with the course. In the programme they sit inside the phases instead of arriving separately.

+1

Compliance evidence pack

Signed attendance, an individual certificate with date, hours and content, a syllabus mapped to the standards that apply to the company, and a one-page letter for the auditor.

+2

Pre-workshop team survey

Ten minutes per person in week 0 to adapt the labs to the team's stack. If it doesn't arrive in time, I carry on with the standard syllabus.

+3

Configurations on a branch of the company's repository

CI gates and a pull request checklist, which I leave in the last block of the workshop. It is a technical template that the team reviews and merges.

+4

Lab repository with solutions

The day's practice exercises to repeat with new team members, with an internal-use licence for 12 months.

COMPLIANCE

What evidence the programme leaves and what it is for

The programme leaves the training documented. It does not certify compliance with any standard, the auditor assesses that, and this record is one of the pieces they can use.

STANDARD	WHAT IT ASKS FOR	WHAT I LEAVE AS EVIDENCE
PCI DSS 4.0 · 6.2.2	Training at least every 12 months for staff who develop bespoke software, covering secure design, secure coding and testing tools, documented.	A syllabus mapped to the requirement's points, signed attendance and an individual dated certificate.
ISO/IEC 27001:2022 · A.6.3	Information security awareness, education and training appropriate to each person's role.	A record per person and per role with content and date.
ISO/IEC 27001:2022 · A.8.25 and A.8.28	A secure development life cycle and secure coding, which includes training the people who write the code.	A mapped syllabus, plus the PR checklist and the CI gates left on the company's branch.
SOC 2 · CC1.4 and CC2.2	A documented training programme, with completion records per employee and depth that fits the role.	A list with name, date, content and role, plus the leadership report.
DORA · Article 13(6)	Digital operational resilience training programmes for the staff of financial entities, proportionate to their role.	Attendance record and syllabus, for those within DORA's scope.

WHO IT IS FOR

For a team that wants to finish with a changed repository and numbers

A strong fit for

- Teams who run web applications or APIs in production.
- Tech leads and engineering managers who are asked to show that the team is trained in secure development.
- Companies with PCI DSS, ISO 27001, SOC 2 or DORA on the horizon, who need to document the training of the people who write code.
- Teams that would rather have a before and after comparison than a promise.

Not the right programme if

- The company is looking for an inspirational talk for a whole department.
- The goal is to train two hundred people. A training platform costs less for that.
- What is needed is an audit or a pen-test. Here the team searches its own code and there is no technical findings report.
- One day is enough. In that case, the one-day workshop is the better fit.

WHO DELIVERS IT

Security and development from someone who has worked on 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 when 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. Spain's National Cybersecurity Institute (INCIBE) has asked me to judge its competitions several times. I founded Navaja Negra and the OWASP Madrid chapter. I'm the author of widely used security tools such as GoLismero, Plecost and Dockerscan, and of LAPIS, research published on arXiv on how to describe an API to a model with fewer tokens. With Alfonso Muñoz I wrote *Secure MCP: A practical guide for developers, software architects and tech leads*.

The lab application is mine and it is public. I run the six weeks myself from start to finish, from the baseline to the final review.

What I fix without charging a cent

Configurations that do not work

If the configurations I leave in the company's repository do not work in the team's pipeline, I fix them in a free remote session and we repeat the week 6 review.

A team still stuck after 30 days

If 30 days after the final review the team has got stuck applying something from the programme, I spend an hour with the team remotely, free.

This is not an audit, and I don't promise fewer vulnerabilities or any percentage of improvement. What I leave is the before and after, measured with the team's numbers.

Questions worth settling now

Which part is in person?

The workshop, 5 to 8 hours depending on the team. The survey, the diagnosis, the channel, the pull request review and the final session are all remote.

Do you see or take our code?

I see a sample of code and pipeline on the company's platform, under its permissions, for the diagnosis and for reviewing the pull requests the team sends me. I don't keep copies. If the company would rather not give me access, I work on fragments it chooses.

What if the team does not answer the survey?

There is a fixed deadline. If it does not arrive in time, I continue with the standard syllabus and with the indicators that can be measured without the survey.

Who decides the indicators?

We agree them together in week 0, from the six candidates on this page or others that make sense in each case. I prefer a few that can really be measured.

Is the Q&A channel open-ended support?

No. It is a channel in the company's Slack or Teams. I reply within two working days and it closes at the end of week 5. After that comes the week 6 review.

Does the evidence pack certify that we comply with PCI, ISO or SOC 2?

No. It is the documentation of the training, which the auditor can use as evidence for a control. Whether the control counts as met is their call.

Can it be funded through FUNDAE?

When a date is requested, I send the information the training department or the advisers need.

How much does it cost?

It depends on the duration and the size of the team. After a first conversation I send a fixed proposal.

Can the workshop also be delivered remotely?

Yes, although in person works better for unblocking labs and for the block on the company's own code. The scope stays the same.

Does it guarantee we will have no security incidents?

No. What I guarantee are the phases and deliverables on this page and the two guarantees above. Whether the risk goes down depends on the team applying and maintaining the controls afterwards.

FORMAT

A fixed proposal, once we have talked

The price depends on the duration and the size of the team, and we fix it after a call because the amount of code to review and the number of indicators we agree also count. It includes the full workshop, the evidence pack, the leadership report, the Q&A channel, pull request review, the final review and the second measurement.

- Participants from the same team or from areas that work together.
- In-person workshop at the company and everything else remote. In English or Spanish.
- Room, screen, wifi and laptops provided by the company, with Docker installed and access to each participant's repository.
- Access to a sample of code and pipeline for the diagnosis, on the company's platform and under its permissions.
- Travel outside Madrid agreed before the date is confirmed.

Write to me at

me@danielalfocea.com

On the call we check whether the programme is a fit, which indicators and which dates. If the one-day course is enough, I say so.

Can be subsidised through FUNDAE (Spanish training credit).

EMAIL

me@danielalfocea.com

PROGRAMME ONLINE

danielalfocea.com/en/formacion/programa-desarrollo-seguro