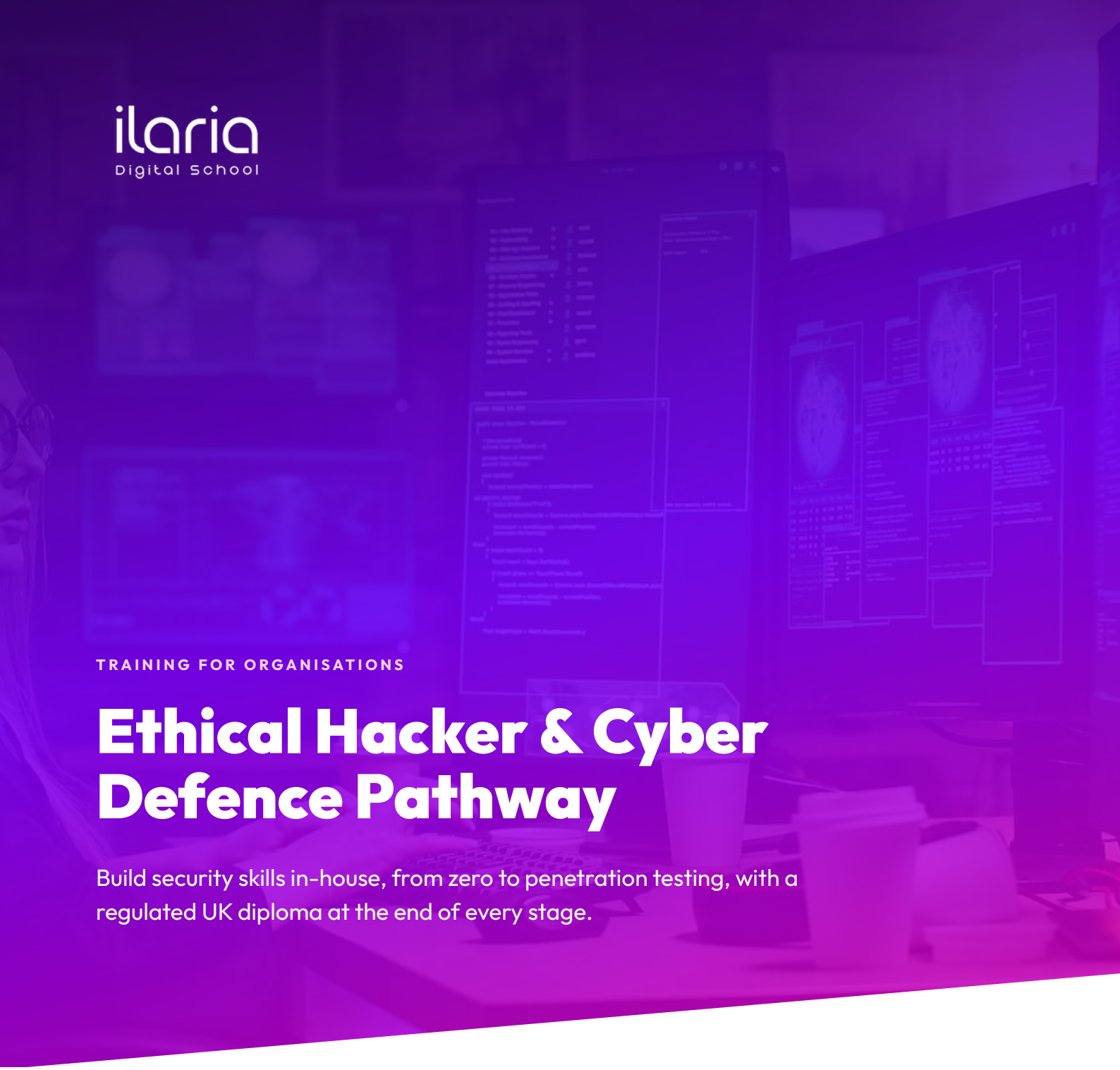
ilaria
Digital School



TRAINING FOR ORGANISATIONS

Ethical Hacker & Cyber Defence Pathway

Build security skills in-house, from zero to penetration testing, with a regulated UK diploma at the end of every stage.

1 or 2 stages
about 12 months each, one diploma per stage

Levels 4 and 5
OTHM diplomas regulated by Ofqual

from €1,250
by country, per stage

OTHM Level 4 Diploma in Cyber Security (610/5103/2) and OTHM Level 5 Extended Diploma in Cyber Security (610/5102/0), awarded by OTHM Qualifications, a UK awarding organisation regulated by Ofqual

01

WHAT'S AT STAKE

Why train your staff

Every week, another organisation learns the hard way that security is not optional. Training an employee who already knows your systems and your business is a direct way to build that capability in-house.

The pathway starts from zero and teaches by doing: systems and network foundations in Stage 1, then security testing, ethical hacking, digital forensics and malware analysis in Stage 2, always in safe, isolated virtual labs.

Starting level

Aged 18 or over, a relevant Level 3 qualification or 21+ with relevant work experience, English at B2 level. No programming or security experience required. Direct entry at Stage 2 with a relevant Level 4 diploma in cyber security or computing.

02

THE SKILLS

What your staff will be able to do

01 Understand systems from the ground up, from logic gates to operating systems.

02 Work with networks: design, addressing and reconnaissance with Nmap.

03 Script and analyse algorithms in Python.

04 Test web and mobile applications and run a complete penetration test.

05 Analyse a disk image forensically and dissect malware in a sandbox.

06 Apply AI to security problems.

07 Document findings in professional reports, with CVSS scoring and the legal and ethical framework.

What your organisation gets back

Every unit, roughly every six weeks, ends with real work delivered, including:

- three professional security test reports, on web and mobile targets
- a full penetration test with a professional CVSS report
- a forensic investigation of a disk image, chain of custody included
- a malware analysis, from detection to reverse engineering

03

THE CONTENT

Programme

Details on ilaria-academy.com/en/course/ethical-hacker-cyber-defence-pathway

STAGE 1 · CYBER SECURITY FOUNDATIONS, OTHM LEVEL 4 DIPLOMA (120 UK CREDITS)

01 Mathematics for Computer Science
Logic, number theory for cryptography, linear algebra.

02 Computer Networks
OSI and TCP/IP, addressing, reconnaissance with Nmap.

03 Principles of Computer Systems
Architecture, logic circuits, ARM assembly.

04 Operating Systems
Linux administration, C, a Linux kernel module.

05 Algorithms and Data Structures
Python, complexity, optimisation and tests.

06 Information Technology Security
Zero Trust, access control, hardening, cryptography.

STAGE 2 · ETHICAL HACKING & SECURITY OPERATIONS, OTHM LEVEL 5 EXTENDED DIPLOMA (240 UK CREDITS IN TOTAL)

07 Databases
Relational design, SQL, a complete store database.

08 Artificial Intelligence
Machine learning, neural networks, AI in attack and defence.

09 Security Testing
Web and mobile testing with Burp Suite and OWASP ZAP.

10 Ethical Hacking
Reconnaissance, exploitation, CVSS reporting, a full penetration test.

11 Digital Forensics
Chain of custody, disk image analysis, incident response.

12 Malware Analysis
Static and dynamic analysis, reverse engineering with IDA or Ghidra.

04

HOW IT RUNS

How it works

Every company project is built with you. Format, rhythm and schedule are not imposed: we can handle them all, and we adapt them to your organisation.

What we adapt to your organisation

The format

At your premises, remotely or a mix of both: we choose together, according to your staff and your sites.

The rhythm

Full days, half days, short sessions or a longer programme: the schedule follows your staff's workload, not the other way round.

The group

One employee joining an open session, or a group dedicated to your organisation.

The content

Examples, exercises and a running project built on your tools, your data and your challenges.

The steps of a project

1

Scoping

We define the objectives, format, rhythm and schedule with you.

2

Positioning

Each participant takes a positioning interview and test, so the pathway matches their level.

3

Training

Short inputs, hands-on practice and a running project based on your organisation's case.

4

Follow-up

Progress reviews throughout the course, shared with the sponsor.

5

Qualification

Every unit assessed on the work delivered, then the OTHM qualification is awarded.

What HR keeps track of

- Progress reviews throughout the course
- Quote, training agreement, attendance and completion certificates
- Each participant's OTHM results, e-certificate and transcript

Assessment: no exams. Each unit is assessed through professional-scenario assignments (security reports, annotated code, lab evidence, a penetration test report), marked by the tutor, quality assured internally, then externally verified. One resubmission per assignment as of right.

Our open intakes

Our open intakes run 100% online on Microsoft Teams, live in English: half-day classes Monday to Thursday mornings, Fridays dedicated to coaching and labs.

A stage takes about 12 months over three terms. Every session is recorded, and each participant has individual coaching every week.

05

THE OFFER

Formats and fees

Open enrolment

Your staff join an open intake, stage by stage.

By country

see the grid below

In-company

An intake dedicated to your organisation.

On request

depending on group and format

Tailored

A pathway adapted to your security challenges

On request

depending on the programme

Fees by country

Our fees are adjusted to each country, so that the same programme, the same live classes and the same weekly coaching stay within reach wherever you live.

	Zone A Western Europe, North America, the Gulf, Australia, Japan	**Zone B** South Africa, Algeria, Brazil, China, Türkiye, the Balkans	**Zone C** West and East Africa, Morocco, Tunisia, South Asia
Stage 1	**€1,800**	**€1,350**	**€1,250**
Stage 2	**€1,800**	**€1,350**	**€1,250**
Level 5 Extended Diploma complete	**€3,600**	**€2,700**	**€2,500**

All-inclusive: tuition, live classes, weekly coaching, assessments, awarding body registration and e-certificate. No hidden fees. Pay in full, or in several instalments over your course. Payment in your own currency is possible. Prices in euros, taxes included where applicable.

Next intakes · open sessions

Three intakes a year (January, May, September), next date on request.

Apply at any time and join the next intake: free English placement test, admission interview, then a positioning test that confirms the entry stage (1 or 2).

Payment

As of 31 October 2026

Payment plans	Pay in full or in several instalments over the course, in your own currency if needed.

Our admissions team goes through fees and payment plans with you, with no obligation.

06

BEFORE YOU START

Questions to ask yourself

Which security needs do you want to cover in-house: operations, testing, investigation?

Which employee has the curiosity, rigour and persistence for this field?

Should they start at Stage 1, or do they already hold a Level 4 diploma?

How much time a week can they give to the course, over one or two years?

Who will mentor them on security matters inside your organisation?

Next steps

01

A 30-minute call

The target role, the employee's profile, the right rhythm.

02

Placement test, interview and quote

English check and admission interview for each participant.

03

Intake

Start at the next intake: January, May or September.

ilaria
Digital School

ETHICAL HACKER & CYBER DEFENCE PATHWAY

Let's talk about your project

formations@ilaria-academy.com