MASTERCLASS · FIVE DAYS

AI + Cyber Security

The masterclass nobody else in Wales is teaching.

www.reskillwales.co.uk

01 · WHY THIS COURSE

The masterclass nobody else in Wales is teaching

Tackle AI phishing, deepfakes and AI-powered malware — and build the governance frameworks that organisations desperately need.

AI-ERA THREATS
Attacks written, voiced and filmed by machines.

PRACTICAL DEFENCE
Automation and detection you can deploy at work.

GOVERNANCE THAT LANDS
Policy, regulation and accountability, made usable.

02 · HOW THE WEEK WORKS

Five days. Five outcomes. One transformed career.

5
DAYS OF TRAINING

5
CORE OUTCOMES

1
TRANSFORMED CAREER

MORNINGS

Taught sessions

Expert-led teaching on the threat, the tooling and the frameworks — grounded in real UK and Welsh incidents.

AFTERNOONS

Hands-on labs

You build something real every day: detection pipelines, phishing analysis, policies and a full threat assessment.

03 · COURSE AT A GLANCE

Five days, mapped end to end

01

The AI Threat Landscape

How AI is reshaping the attack surface, from script kiddies to nation states.

LAB
Analyse real AI-powered attacks

02

AI Phishing & Deepfakes

The attacks that fool humans and machines alike — detect and defend.

LAB
Spot AI phishing in a live inbox

03

AI Defence & Automation

Fight fire with fire: AI-driven detection, response and hunting.

LAB
Build a detection pipeline

04

AI Governance & Risk

Frameworks, regulation and controls for safe AI adoption.

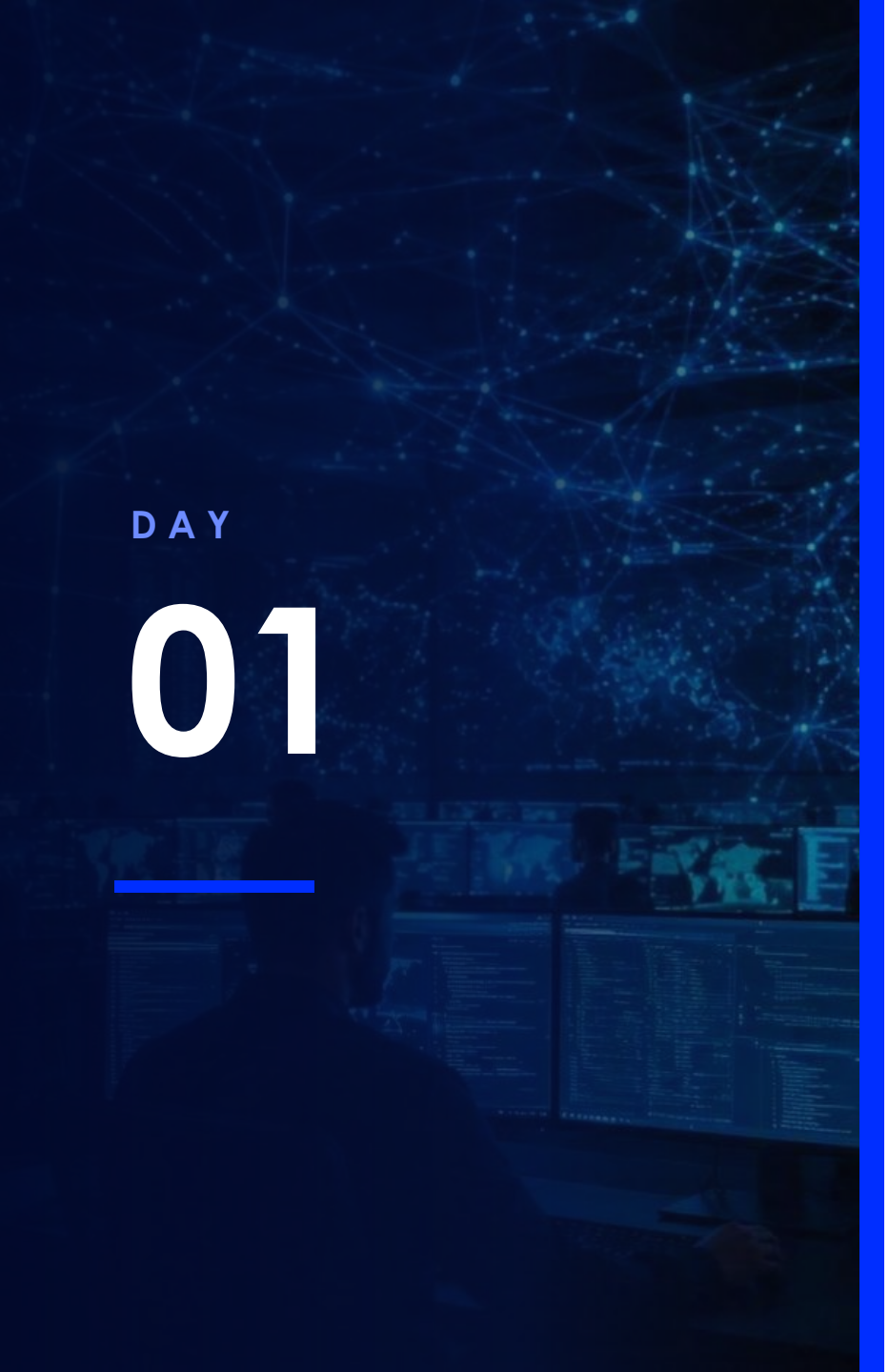
LAB
Draft an AI governance policy

05

AI-Aware Security Ops

Design a SOC that accounts for AI on both sides of the fight.

CAPSTONE
Capstone presentation



DAY

01

DAY 01 · MODULE

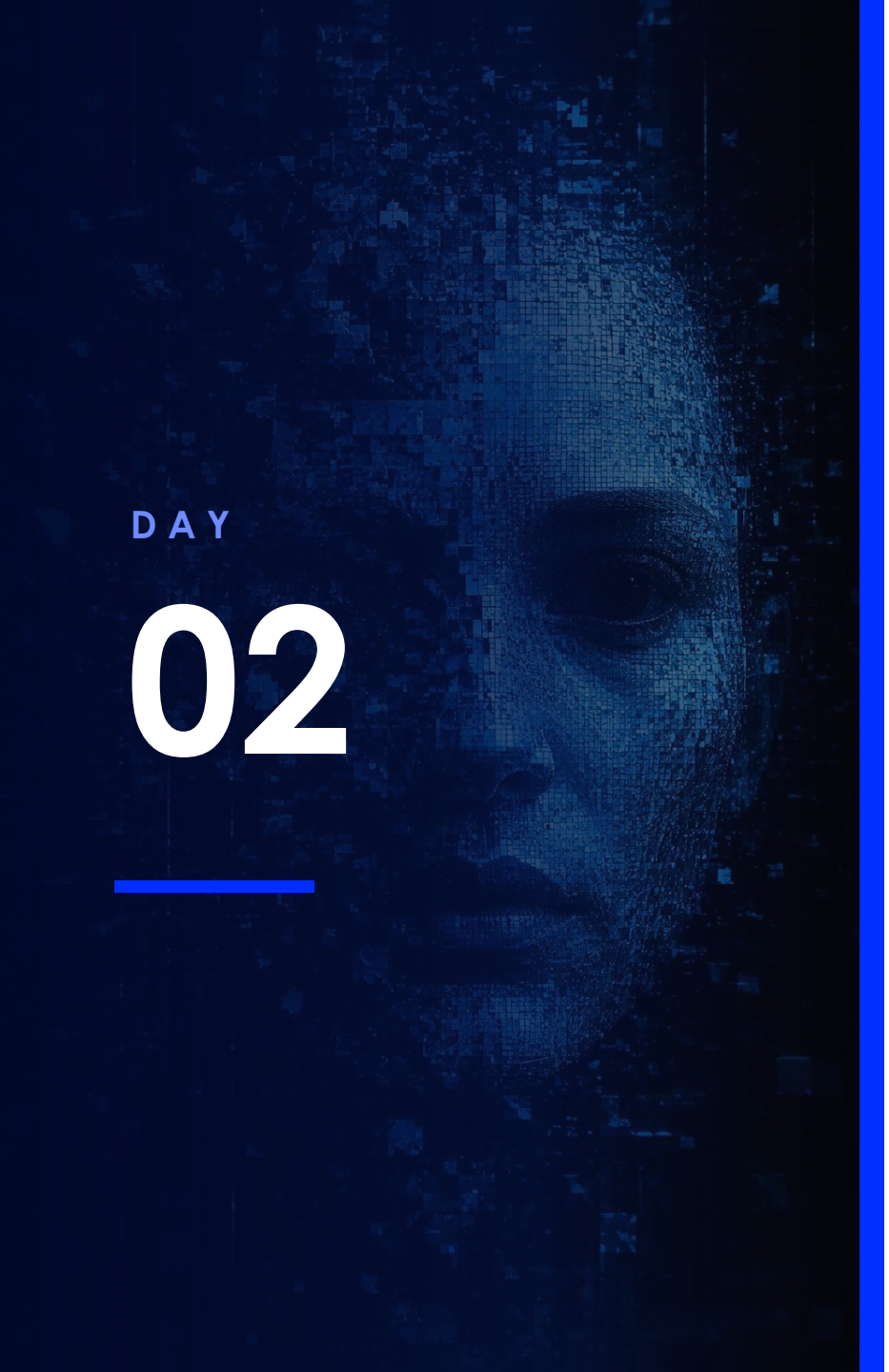
The AI Threat Landscape

How AI is changing the attack surface — from script kiddies to nation-state actors using generative AI at scale.

- AI in the hands of attackers
- Generative AI attack techniques
- AI-enhanced reconnaissance
- The economics of AI-powered crime
- Welsh & UK threat intelligence
- AI vs traditional attack comparison

LAB

Analyse real-world AI-powered attack case studies



DAY

02

DAY 02 · MODULE

AI-Powered Phishing & Deepfakes

The attacks that fool humans and machines alike. Detect, defend and respond to AI-generated social engineering.

- AI-generated phishing at scale
- Voice cloning & vishing
- Deepfake video detection
- Business email compromise with AI
- Defence strategies & tools
- Building awareness programmes

LAB

Detect AI-generated phishing in a simulated inbox exercise

DAY

03

DAY 03 · MODULE

AI Defence & Security Automation

Fight fire with fire. Use AI to automate detection, response and hunting — the tools SOCs are adopting now.

- AI-powered SIEM & threat detection
- Automated incident response
- AI-assisted threat hunting
- Behavioural analytics
- ML for anomaly detection
- Security orchestration (SOAR)

LAB

Build an automated detection pipeline for AI-powered attacks

DAY 04 · MODULE

AI Governance & Risk Management

The frameworks, policies and controls organisations need to adopt AI safely. Regulation, compliance, accountability.

- AI governance frameworks
- EU AI Act & UK regulation
- AI risk assessment methods
- Responsible AI principles
- Bias & fairness in AI security
- Building an AI governance board

LAB **Draft an AI governance policy for a Welsh organisation**

DAY

05

DAY 05 · MODULE

Building AI-Aware Security Operations

Bring it all together: design a security operations capability that accounts for AI on both sides of the fight.

- AI-aware SOC design
- Threat modelling with AI
- Red team vs blue team with AI
- AI security roadmap planning
- Measuring AI security maturity
- Career paths in AI security

CAPSTONE

Present your AI threat assessment and governance policy

04 · HANDS-ON LABS

Every afternoon, you build something real

01 Analyse real-world AI-powered attack case studies

02 Detect AI-generated phishing in a simulated inbox exercise

03 Build an automated detection pipeline for AI-powered attacks

04 Draft an AI governance policy for a Welsh organisation

CAPSTONE

Day 05

Present your AI threat assessment and governance policy to the room — the piece of work you take back to your organisation.

05 · WHAT YOU WALK AWAY WITH

Five outcomes that change your role

THREAT FLUENCY
Explain how attackers use generative AI — and what changes about your risk.

DETECTION SKILLS
Identify AI phishing, cloned voices and deepfake media with confidence.

AUTOMATION
Stand up AI-assisted detection, hunting and response workflows.

GOVERNANCE
Apply the EU AI Act, UK regulation and responsible AI principles.

RISK LEADERSHIP
Run AI risk assessments and chair an AI governance board.

CAREER MOMENTUM
Leave with a portfolio piece and a clear AI security roadmap.

READY WHEN YOU ARE

Lead on AI security

AI + Cyber Security · Five days at Reskill Wales, Llynfi Enterprise Centre.

01656 737349 · hello@reskillwales.co.uk

www.reskillwales.co.uk