The Resilience Cycle for NIS2 Readiness

CONTENTS

This masterclass provides a complete, end-to-end journey through the capabilities required to achieve operational NIS2 readiness. Participants learn how to identify weaknesses, engineer secure systems, manage suppliers, and produce audit-ready evidence — following a structured resilience cycle that connects technical execution with regulatory obligations.

LED BY TWO COMPLEMENTARY EXPERTS

The course is co-delivered by:

- A Cloud Security & DevSecOps specialist who guides participants through technical design, automation, and evidence generation.
- A Governance & Risk management expert who translates operations into frameworks, metrics, and audit-ready documentation.

Together they provide a 360-degree perspective—linking technology, regulation, and leadership decision-making.

TARGET AUDIENCE

- Cybersecurity engineers, SOC analysts, cloud architects, DevSecOps and IT professionals
- CISOs, risk and compliance managers, and internal auditors
- IT leaders and project owners contributing to NIS2 implementation

PREREQUISITES

No prior NIS2 experience required—concepts are introduced progressively and reinforced through guided labs.

KEY LEARNING OUTCOMES

By the end of this masterclass, participants will be able to:

- Understand how modern threats and NIS2 converge into a resilience mandate
- Prioritize vulnerabilities using risk and business impact
- Build secure-by-design technical environments aligned with NIS2.
- Translate technical controls into measurable indicators.
- Manage NIS2-compliant incident response, including third-party breaches

WHY CHOOSE THIS PROGRAM

- Designed around the latest EU NIS2 operational requirements.
- Co-taught by two senior instructors bridging technical engineering and regulatory governance.
- Hands-on and live simulations, not just lectures.
- Have tangible takeaways

COURSE STRUCTURE

Resilience Foundations

Theme: Clarifying threats, obligations, and organisational weaknesses.

- Overview of modern cyber threats and NIS2 accountability expectations
- How regulation aligns with resilience, not checklists
- Strategic vulnerability and exposure management
- Workshop: Prioritising real vulnerabilities using business context

Outcome: A clear resilience baseline connected to NIS2 expectations.

Building the Resilient Engine

Theme: Moving from reactive defence to proactive, engineered security.

- Security-by-design principles: identity, access, segmentation, data protection
- Establishing secure baselines and architectural discipline
- Detection engineering and behaviour-based investigation
- Hands-On Lab: Analysing a simulated incident and recommending improvements

Outcome: Practical resilience-building techniques applicable to modern environments.

Governance & NIS2 Assurance

Theme: Converting technical controls into provable, governed resilience.

- NIS2-compliant incident response (24h/72h requirements)
- Third-party and supply-chain risk integration
- Assurance, reporting, and board-level communication
- Simulation: Drafting a NIS2 early-warning notification from a vendor breach

Outcome: The ability to demonstrate readiness, manage supplier incidents, and produce audit-ready resilience evidence.