



## SEC11 - NIS2 for Embedded

### Objectives

- Understand NIS2 scope, roles, and obligations for essential/important entities.
- Translate Article 21 risk-management measures into an embedded/OT context.
- Apply incident reporting timelines (24h/72h/1-month) with ready-to-use templates.
- Build a 30/60/90-day compliance roadmap and evidence checklist.

### Environnement du cours

- Cours théorique
  - Support de cours au format PDF (en anglais) et une version imprimée lors des sessions en présentiel
  - Cours dispensé via le système de visioconférence Teams (si à distance)
  - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique
- Au début de chaque demi-journée une période est réservée à une interaction avec les stagiaires pour s'assurer que le cours répond à leurs attentes et l'adapter si nécessaire

### Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

## Plan du cours

### Introduction & Scope

- NIS2 at a glance
- Sectors in scope & “size-cap” rule
- Essential vs Important Entities (EEs vs IEs)
- Roles, authorities, penalties

### Governance & Responsibilities

- Management accountability
- Security policy & risk ownership
- Roles/RACI and coordination with product/OT teams

### Risk Management Measures

- Business continuity & incident handling
- Identity & Access and logging
- Vulnerability management & secure development
- OT/embedded specifics (segmentation, safety interplay)

### Mapping to Engineering Workflows

- From requirements to release (Dev & Test & Release & Update)
- Secure updates & support periods (firmware/RTOS/toolchains)
- Vulnerability intake, triage, remediation, and user communication
- Evidence-by-design: what to capture during builds

## Incident Reporting

- Triggers & thresholds (significant incidents)
- Timelines: 24h / 72h / 1-month reports
- Internal playbook, contacts, escalation

## Supply Chain & Third-Party Components

- Supplier due diligence & contractual expectations
- Updates, disclosure programs, and support commitments
- Evidence from vendors (SBOM/VEX, security posture)

## Evidence & Metrics

- Registers: risks, incidents, assets, suppliers, training
- KPIs & dashboards for management
- Preparing for audits/inspections

## Roadmap

- Quick wins
- Priority controls & contracts
- Exercises, metrics, internal audit

## Wrap-Up & Q&A

- Key takeaways
- Next steps & optional deep-dives (OT, IoT, CRA alignment)