SEC11 - NIS2 pour l'embarqué

Objectifs

- Comprendre le périmètre, les rôles et les obligations de NIS2 pour les entités essentielles et importantes.
- Transposer les mesures de gestion des risques de l'article 21 dans un contexte embarqué/OT.
- Appliquer les délais de notification d'incident (24h/72h/1 mois) avec des modèles prêts à l'emploi.
- Construire une feuille de route de conformité à 30/60/90 jours et une liste de preuves à réunir.

Environnement du cours

- Cours théorique
  - Support PDF (en anglais), imprimé en présentiel ; à distance via Teams.
  - Assistance du formateur tout au long de la formation.
- Chaque session débute par un point avec les stagiaires.

Audience visée

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

Plan du cours

Introduction et périmètre

- NIS2 en un coup d'œil
- Secteurs concernés et règle du « plafond de taille »
- Entités essentielles et entités importantes (EEs et IEs)
- Rôles, autorités, sanctions

Gouvernance et responsabilités

- Responsabilité de la direction
- Politique de sécurité et propriété du risque
- Rôles/RACI et coordination avec les équipes produit et OT

Mesures de gestion des risques

- Continuité d'activité et traitement des incidents
- Gestion des identités et des accès, journalisation
- Gestion des vulnérabilités et développement sécurisé
- Spécificités OT et embarqué (segmentation, interaction avec la sûreté)

Mise en correspondance avec les flux d'ingénierie

- Des exigences à la livraison (Dev → Test → Release → Update)
- Mises à jour sécurisées et durées de support (firmware/RTOS/chaînes d'outils)
- Réception, tri et correction des vulnérabilités, communication aux utilisateurs
- La preuve dès la conception : ce qu'il faut capturer pendant les builds

Notification des incidents

- Déclencheurs et seuils (incidents significatifs)
- Délais : rapports à 24h / 72h / 1 mois
- Procédure interne, contacts, escalade

Chaîne d'approvisionnement et composants tiers

- Vigilance vis-à-vis des fournisseurs et attentes contractuelles
- Mises à jour, programmes de divulgation et engagements de support
- Preuves fournies par les fournisseurs (SBOM/VEX, posture de sécurité)

Preuves et indicateurs

- Registres : risques, incidents, actifs, fournisseurs, formations
- KPIs et tableaux de bord pour la direction
- Préparation aux audits et aux inspections

Feuille de route

- Gains rapides
- Contrôles et contrats prioritaires
- Exercices, indicateurs, audit interne

Synthèse et questions

- Points clés à retenir
- Prochaines étapes et approfondissements optionnels (OT, IoT, alignement CRA)