



CYBER-RÉSILIENCE EN MILIEU INDUSTRIEL

FFCNCERCERXIO15

PRIX : 1930 €

DURÉE : 2 JOURS

Pauses et déjeuners offerts

PRÉSENTATION

La cyber-résilience est devenue un enjeu stratégique pour garantir la continuité, la robustesse et la souveraineté des systèmes numériques face aux cyberattaques, aux évolutions réglementaires et aux risques géopolitiques. Cette formation apporte les méthodes et les référentiels essentiels (Cyber Resilience Act, NIS2, Cloud Sovereignty Framework) pour intégrer durablement la cyber-résilience dans les produits et les infrastructures industrielles.

OBJECTIFS

- Expliquer les fondamentaux de la cyber-résilience industrielle
- Évaluer les risques et les dépendances des systèmes numériques
- Définir une stratégie de résilience conforme aux bonnes pratiques
- Appliquer une méthodologie opérationnelle sur un cas concret

PROGRAMME

Introduction

Cyberespace industriel autonome et résilient

Retours d'expérience

- 2010 – Stuxnet : sabotage des installations nucléaires iraniennes
- 2024 – CrowdStrike : une mise à jour provoque le blocage de 8,5 millions de postes Windows
- 2025 – BrickStorm & Grimbolt : découverte de portes dérobées sur Dell RecoveryPoint pour environnements VMware
- 2025 – Sanctions américaines : suspension de services numériques pour des responsables européens et de la Cour pénale internationale

Résilience, autonomie et souveraineté

- Impact d'une attaque physique sur les infrastructures critiques de l'Internet français
- Enjeux des réglementations Cyber Resilience Act, NIS2 et European Digital Networks Act

Composantes d'un cyberespace industriel

Équipements concernés par la résilience

- Bâtiments, énergie, infrastructures réseau et accès Internet
- PLC, robots et automates industriels
- Routeurs, serveurs locaux et cloud
- Systèmes de contrôle d'accès et de sécurité physique

Éléments du cycle de vie

- Achat et qualification des équipements
- Cyber Resilience Act
- NIST 800-193 – Platform Firmware Resiliency Guidelines

Mise en œuvre

- Déploiement sécurisé
- Inventaire matériel et logiciel

- Gestion des droits d'administration et des sous-traitants
- Détection continue des anomalies (IETF Manufacturer Usage Description)
- Résilience des environnements d'exploitation (OAM)
- Fin de vie, recyclage et cession

Communication et services numériques

- Résilience des protocoles et architectures industrielles
- ROS2
- OPC-UA, DDS
- Ethernet et Time Sensitive Networking
- Services Cloud

Approche méthodologique

Définitions et périmètre

- Réglementations (NIS2, etc.) et standards (ISO/IEC 62443, etc.)

Modélisation

- Méthodologie d'architecture, de déploiement et d'exploitation

Analyse de risques orientée résilience

- Identifier les dépendances critiques et leurs impacts
- Élaboration de fiches d'analyse adaptées aux référentiels en vigueur

Plans d'urgence

- Construction de modèles de plans de continuité et de réaction

Atelier de mise en œuvre

- Réalisation d'une mission de conseil en cyber-résilience pour une entreprise industrielle
- Élaboration collective d'un diagnostic, d'un plan d'action et d'un plan d'urgence
- Cas pratique : robots industriels, PLC, ROS2, Movelt2, OPC-UA, DDS et réseaux Ethernet temps réel

Synthèse et conclusion



PANORAMA



RÉALISABLE
EN ANGLAIS

Du 14/05/2027 au 15/05/2027 à Paris
Du 06/12/2027 au 07/12/2027 à Paris

PUBLIC/PRÉREQUIS

Cette formation s'adresse aussi bien à des cadres techniques qu'à des architectes, des experts en sécurité, des chefs de projet cybersécurité, des acheteurs de produits digitaux (serveurs & portables, PLC, commutateurs, système de gestion d'accès, de vidéo-surveillance, etc.). Pour le public non ou peu technique, l'apport majeur est l'identification de domaines et méthodes à considérer pour que les opérationnels prennent en compte la résilience de façon complète et détaillée.

Des connaissances de base en cybersécurité permettront de transformer les éléments très techniques de cette formation en un référentiel interne pour la cyber-résilience.

RESPONSABLE(S)

François-Frédéric OZOG

Consultant auprès de la Commission européenne pour les plateformes digitales et précédemment directeur du groupe Edge/Fog Computing chez Linaro. Fondateur de sociétés en France et aux États-Unis. Entrepreneur depuis plus de 40 ans dans des rôles techniques, commerciaux et marketing, il allie compétences techniques et business pour former des stratégies pertinentes. Il est l'inventeur de 7 brevets.

MODALITÉS PÉDAGOGIQUES

Alternance d'ateliers interactifs pour accompagner la compréhension et sessions magistrales pour formaliser et acquérir les connaissances.