INTRA

INTER

CYBERSÉCURITÉ POUR LES SYSTÈMES INDUSTRIELS : FOCUS SUR LA NORME IEC 62443

OBJECTIFS

1. Comprendre la structure des normes IEC62443
2. Dialoguer avec le vocabulaire adapté
3. Appréhender les exigences des principaux standards
4. Définir le plan d'actions de cybersécurité adapté à l'entreprise incluant la mise en conformité aux standards adaptés
5. Identifier les risques liés aux installations industrielles.

MOYENS PÉDAGOGIQUES

Projection du cours, support de cours papier et clés USB
Chaque point de la formation sera illustré par des exemples concrets afin que les participants puisse s'approprier le sujet.

MÉTHODES UTILISÉES

La progression pédagogique du participant est évaluée tout au long de la formation au moyen de QCM.

PUBLIC

> RSSI, responsable de projet sécurité industrielle, architecte sécurité industrielle, ingénieur cybersécurité, DSI, gestionnaire des risques

PRIX HT
À partir de 1 300 €

DATES
du 10 au 12 mars 2026
du 9 au 11 juin 2026

DURÉE
3 jours (21 heures)

LIEU
LCIE

INTERVENANT
Expert en cybersécurité industrielle

PRÉ-REQUIS
Connaissance du fonctionnement managérial et organisationnel d'une structure
Connaissance de base en sécurité de l'information et des systèmes industriels.
Compréhension des principaux termes utilisés en cybersécurité

PARCOURS DE FORMATION

> Module 0 «Principes de Cybersécurité»
- Définitions & Vocabulaire
- Types d'attaques cybernétiques (MITM, usurpation, DDOS, ingénierie sociale, ver, ransomware, etc.)
- Mécanismes de sécurité clés

> Module 1 «Introduction à la Norme IEC 62443»
- Énoncé et défis de la cybersécurité dans le monde OT
- Périmètre de la cybersécurité dans l'entreprise / les projets
- Architecture de la norme IEC 62443
- Concepts communs et vue d'ensemble des différentes sous-parties

> Module 2 «Introduction au Monde de l'Automatisation»
- Description des couches IACS (ISA95)
- PLC, RTUS, SCADA, IHM, Passerelle
- Protocoles utilisés dans le monde de l'industrialisation

> Module 3 «Organisation de la Cybersécurité»
- Menaces et risques dans la sécurité organisationnelle
- Exigences pour un système de gestion de la sécurité IACS

> Module 4 «Cycle de Vie & Évaluation des Risques»
- Cycle de vie des produits et IACS
- Concepts de zones et de conduits
- Évaluations des risques / Partitionnement d'architecture

> Module 5 «Focus sur IEC 62443 – 3-3 & 4-2»
- Description des exigences de sécurité (SR) et des exigences de composants (CR)
- Exigences spécifiques pour les appareils dédiés

> Module 6 «Mécanismes de Sécurité Clés»

> Module 7 «Focus sur IEC 62443 – 2-4»

> Module 8 «Focus sur IEC 62443 – 4-1»

> Module 9 «Vue d'Ensemble de la Certification selon le Schéma IECEE»

> Module 10 «VLAN»

> Module 11 «Gestion des Correctifs»

> Module 12 «Journaux et Événements»
- Meilleures pratiques et règles
- Protocole SYSLOG

> Module 13 «Pratiques de Codage PLC»
- Meilleures pratiques de développement
- Lien avec les attaques et les exigences 4-2/3-3

> Exercices
- Attaque Stuxnet
- Cyberattaque du réseau électrique ukrainien