+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 15/01/2026

S'inscrire

Formation Introduction à la Cybersécurité Industrielle

1 jour (7 heures)

Présentation

La convergence IT/OT et l'entrée en vigueur du Cyber Resilience Act (CRA) imposent une nouvelle rigueur dans la conception des systèmes industriels. La sécurité n'est plus une option : elle devient une condition d'accès au marché européen (Marquage CE).

Notre formation "Introduction à la Cybersécurité Industrielle" synthétise en une journée les concepts clés de la norme de référence IEC 62443 et les nouvelles obligations réglementaires du CRA. Vous apprendrez à identifier les différences fondamentales entre sécurité IT et OT, à structurer une architecture sécurisée (Zones et Conduits) et à comprendre ce qu'implique le "Security by Design" pour vos produits ou vos installations.

À l'issue de la formation, vous disposerez d'une vision claire des actions à mener pour initier votre démarche de conformité et dialoguer efficacement avec les experts techniques et légaux.

Comme toutes nos formations, celle-ci s'appuie sur les dernières publications de l'ISA/IEC et privilégie une approche concrète basée sur des retours d'expérience industriels.

Objectifs

- Comprendre les enjeux spécifiques de la cybersécurité industrielle (Sûreté vs Confidentialité).
- Maîtriser le vocabulaire et les concepts de l'IEC 62443 (Zones, Conduits, SL).
- Décrypter les exigences du Cyber Resilience Act (CRA) pour les fabricants.
- Savoir définir une stratégie de "Security by Design".
- Identifier les vulnérabilités via les SBOM (Software Bill of Materials).

Public visé

- Chefs de projets industriels & Product Owners

- Architectes systèmes et solutions IoT
- Responsables qualité / conformité
- Décideurs techniques IT/OT

Pré-requis

- Culture générale informatique et industrielle.
- Aucune connaissance préalable de la norme IEC 62443 n'est requise.

Pré-requis matériels

- Un ordinateur portable standard suffit pour visualiser les documents et participer aux ateliers d'architecture.

Formation Cybersécurité Industrielle & CRA (Essentials)

[Matin]

Fondamentaux OT et Architecture IEC 62443

- Le contexte : Convergence IT/OT et panorama des menaces (Ransomware, Sabotage)
- La triade AIC (Availability, Integrity, Confidentiality) dans l'industrie
- Introduction à la norme IEC 62443 : philosophie et structure
- Segmentation réseau : Concepts de Zones et Conduits
- Comprendre les Niveaux de Sécurité (Security Levels - SL)
- Le modèle de "Défense en Profondeur" appliqué à l'usine
- Atelier pratique : Cartographie d'un système industriel et définition des Zones/Conduits (Sur papier/tableau blanc).

[Après-midi]

Conformité CRA et Cycle de vie Sécurisé

- Comprendre le Cyber Resilience Act (CRA) : périmètre et obligations
- Le lien entre CRA et IEC 62443-4-1 (Secure Product Development Lifecycle)
- Exigences essentielles : Security by Design et "Secure by Default"
- Gestion des vulnérabilités et SBOM (Software Bill of Materials)
- Maintenance et gestion des incidents (Notification sous 24h)
- Feuille de route : par où commencer la mise en conformité ?
- Atelier pratique : Audit flash (Gap Analysis) d'un produit fictif face aux exigences du CRA.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.