Fiche Technique:formation cybersécurité des systèmes industriels détection et prévention des intrusions

Objectifs de la formation

> Parcours orienté résultats, aligné IEC 62443 et ISO 27001, avec ateliers et labs OT applicables en production.

- Cartographier les actifs OT/IIoT et leurs dépendances critiques.
- Concevoir une segmentation réseau adaptée aux contraintes de production.
- Déployer des capacités de détection d’intrusions OT (passives et actives).
- Établir des playbooks de réponse à incident pour les sites industriels.
- Aligner les pratiques avec IEC 62443 et ISO 27001.
- Mesurer l’efficacité des contrôles via KPIs et tableaux de bord (MTTD, MTTR, couverture d’actifs).

Population cible

Pour celles et ceux qui concilient sécurité, disponibilité et conformité sur des sites industriels.

- Responsables de production, RSSI, DSI, ingénieurs d’automatisation, exploitants.
- Environnements multisites; secteurs régulés et non régulés (énergie, eau, manufacturing, etc.).
- Prérequis: bases réseaux industriels, architectures SCADA/PLC, fondamentaux sécurité IT (supports d’amorçage fournis).
- Profils techniques et métiers: structurer des contrôles et traduire les exigences en impacts opérationnels.
- Organisations dispersées: langage commun IT/OT et alignement avec intégrateurs et sous-traitants.

Durée de la formation

Formats adaptés avec évaluation continue et cas fil rouge.

Format	Durée typique	Modalités	Évaluation
Intensif	3 jours (21 h)	Présentiel sur site, labs OT	Quiz, étude de cas, atelier incident
Modulaire	5 × 4 h	Distanciel live + TP	Contrôle continu, mini-projet
Blended	2 jours + e-learning	Hybride (présentiel/distanciel)	Certification interne, feedback 360°

> Diagnostic initial pour choisir le format le plus pertinent et maximiser l’impact.

Programme de la formation

Cursus progressif mêlant théorie, retours d’expérience et ateliers sur environnements OT représentatifs.

Module 1 — Panorama des menaces OT et défense

- Typologie d’incidents, erreurs de configuration, principes Zero Trust en OT.
- Cas d’attaques réels et passage IT → OT; défense en profondeur.

Module 2 — Architecture, segmentation et durcissement

- Zones/conduits, DMZ, microsegmentation, whitelisting.
- Durcissement PLC/HMI/SCADA, accès, MFA, correctifs, journaux.

Module 3 — Visibilité réseau et détection d’intrusions

- Cartographie passive, analyse Modbus/DNP3/S7/OPC UA.
- Signatures vs comportemental, corrélation SOC.

Module 4 — Réponse à incident et continuité

- Confinement, isolement, restauration sécurisée, communication de crise.
- Playbooks OT, simulations table-top, preuves et traçabilité.

Module 5 — Conformité, audit et amélioration continue

- IEC 62443/ISO 27001, évaluation de maturité, plan d’action priorisé.
- KPIs OT (MTTD/MTTR), gouvernance IT/OT.

Module 6 — Intégration SOC et télémétrie OT

- Acheminement des journaux OT, connecteurs ICS, orchestration d’alertes.
- Contextualisation des use cases et corrélations spécifiques OT.

Module 7 — Accès distants, fournisseurs et bastions

- Portails/bastions, MFA, enrôlement hétérogène, traçabilité des sessions.
- Exigences contractuelles et cadres de contrôle des tiers.

Module 8 — Tests de résilience et exercices de crise

- Planification d’exercices sans perturber la production, tests de segmentation.
- Scénarios sectoriels, matrices d’activation, critères de sortie.