Cybersécurité IT/OT

Informatique - Numérique - Cybersécurité - IA

16/09/2026

Résumé

Cette formation « Cybersécurité IT/OT » s'adresse aux dirigeants, responsables informatiques ou industriels et membres de comités de direction. Elle permet de comprendre les enjeux de la cybersécurité OT et de maîtriser les principes essentiels pour protéger les systèmes industriels, réduire les risques et renforcer la résilience opérationnelle, de la gouvernance NIS2 à la gestion de crise.

CENTRES DE FORMATION
Colmar, Strasbourg, Mulhouse, Reichshoffen

DURÉE DE LA FORMATION
1 jour / 7 heures

ACCUEIL PSH
Formation ouverte aux personnes en situation de handicap. Solutions personnalisées à étudier avec le référent handicap du centre concerné

Public et prérequis

Public : Dirigeants, responsables informatiques / industriels, membres de comités de direction.

Prérequis : Aucun prérequis technique, mais une compréhension de l'environnement numérique de l'entreprise est recommandée.

Objectifs pédagogiques et professionnels

- Comprendre les enjeux stratégiques et les principes clés de la cybersécurité IT/OT.
- Analyser les conséquences d'une cyberattaque OT et définir les rôles et responsabilités des dirigeants.
- Construire une stratégie de cybersécurité IT/OT et développer une culture de vigilance.
- Savoir réagir à un incident et anticiper les nouveaux défis.

Contenu de la formation

Enjeux et fondamentaux de la cybersécurité industrielle

- La cybersécurité, un enjeu stratégique : protéger la continuité industrielle face aux attaques menaçant production, équipements et sécurité.
- Les principes clés : disponibilité, intégrité, traçabilité.
- La protection des automates, IHM, réseaux et capteurs contre les menaces ciblées.

Risques industriels et gouvernance

- Les conséquences d'une cyberattaque OT : arrêts de production, pertes économiques, impacts humains, contraintes réglementaires et perturbation de la supply chain.
- La gouvernance IT/OT : obligations NIS2, pilotage stratégique, arbitrages production/sécurité.
- La coordination entre IT, OT et maintenance.

Stratégie de cybersécurité IT/OT et culture cyber industrielle

- La conception d'une stratégie IT/OT : segmentation, durcissement, inventaire, supervision continue et bonnes pratiques IEC 62443.
- La gestion des accès et la maîtrise des périphériques.

Les + du Pôle formation

+ de 4000 personnes formées/an dont 1600 apprentis
+ de 1250 entreprises nous font confiance
+ de 10 partenariats avec des écoles

• Une pédagogie innovante et participative assurée par des formateurs experts
• Une approche agile pour se former aux métiers de demain

• Taux de réussite : www.formation-industries-alsace.fr/nos-taux-de-reussite

- Les comportements sûrs sur SCADA/IHM et la sensibilisation des équipes.

Gestion de crise, résilience et perspectives

- La réaction à un incident : isolement rapide, fonctionnement en mode dégradé, communication maîtrisée et capitalisation via les retours d'expérience.
- Les tendances et perspectives : IA, IIoT, convergence IT/OT, attaques supply chain et nécessité d'architectures industrielles résilientes.

Méthodes pédagogiques et d’encadrement

Exposés et cas pratiques favorisant l'apprentissgae collaboratif et le partage d'expériences.

Validation et certification

Les acquis sont évalués en continu par des mises en situation, cas pratiques ou quiz, afin de valider l'atteinte des compétences visées.

Délai d'accès à la formation

Sessions programmées tout au long de l'année, nous consulter.

Suite de parcours, passerelles et équivalences

Des modules complémentaires sont disponibles et peuvent être intégrés à votre projet. Pour toute demande spécifique, nous consulter.