Cybersécurité des Systèmes d'Informations Industriels

Cybersécurité, Systèmes & Réseaux informatiques

11/04/2025

RÉSUMÉ

Avec l'évolution rapide des technologies et la croissance des cyberattaques, la maîtrise de la cybersécurité des systèmes d'information industriels est devenue cruciale. Cette formation combine théorie et pratique, permettant aux participants de manipuler directement les matériels de contrôle-commande pour une compréhension approfondie des enjeux de sécurité.

Public Cible :

- Automaticiens industriels
- Services de maintenance industrielle
- Bureaux d'étude en conception industrielle

CENTRES DE FORMATION

Saint-Nazaire, Laval, La Roche-sur-Yon, Le Mans, Angers, Nantes

DURÉE DE LA FORMATION

3 jours / 21 heures

ACCUEIL PSH

Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.

PUBLIC ET PRÉREQUIS

Connaissances de base des systèmes d'information et des réseaux industriels. (Un quiz permettra de valider ces prérequis).

LES OBJECTIFS

A l'issue de la formation, les stagiaires seront capables de :

- Comprendre les enjeux et les risques de la cybersécurité industrielle
- Identifier les menaces spécifiques aux systèmes d'information industriels
- Manipuler, configurer et sécuriser le matériel de contrôle-commande
- Intégrer la cybersécurité dès la phase de conception des systèmes

OUTILS PÉDAGOGIQUES

Formation en présentiel avec alternance d'apports théoriques et de mises en situation pratiques pour ancrer les apprentissages et/ou en distanciel pour certains modules.

Salles de Formation équipées pour utilisation de supports pédagogiques classiques et numériques. Plateaux techniques adaptés et aménagés d'équipements spécifiques.

Les + Esiac

• 60 ans d'existence
• Une communauté de 3 100 alternautes
• 24 000 stagiaires formés par an
• 3 500 entreprises qui nous font confiance

• Un accompagnement personnalisé et un contact dédié
• L'expertise professionnelle de tous nos formateurs
• La diversité des diplômes sous accréditation par des partenaires de renom
• Une pédagogie active
• Des infrastructures technologiques et un environnement stimulant

MODALITÉ D'ÉVALUATION

Modalités d'évaluation des formations qualifiantes : Les connaissances et/ou capacités professionnelles de l'apprenant sont évaluées en cours et/ou en fin de formation par différents moyens : mises en situation, études de cas, QCM, ..

MODALITÉS D'ACCÈS

Délais d’accès de 6 mois maximum après confirmation via le bulletin d’inscription, sous réserve d’un nombre suffisant d’inscrits et dans la limite des places disponibles et sous réserve d'étude du dossier d'admissibilité

CONTENU DE LA FORMATION

Introduction à la cybersécurité industrielle (2h)

- Enjeux et contexte actuel
- Différences entre cybersécurité IT et OT

Menaces et vulnérabilités des systèmes industriels (3h)

- Typologie des attaques
- Études de cas d'incidents récents

Manipulation et configuration du matériel de contrôle-commande (8h)

- Présentation détaillée du matériel et des systèmes
- Atelier pratique : mise en place et configuration d'un système de contrôle-commande
- Identification des points de vulnérabilité
- Atelier pratique : simulation d'attaques et mise en place de contre-mesures

Principes de protection des systèmes industriels (5h)

- Architecture de sécurité
- Méthodes d'authentification et contrôle d'accès
- Sécurisation des communications
- Atelier pratique : mise en œuvre des principes de protection sur le matériel

Intégration de la cybersécurité dans la conception (3h)

- Bonnes pratiques de conception sécurisée
- Normes et réglementations en vigueur
- Atelier pratique : conception d'un système sécurisé

VALIDATION ET CERTIFICATION

Attestation de fin de formation

DATE DE MISE À JOUR

10/10/2023

VERSION DOCUMENTAIRE

V1