Cybersécurité industrielle : de la prise de conscience à l'action

Informatique - Numérique

06/11/2026

Conditions d'inscription

Pour les salariés en formation continue :

- Validation du projet de formation par l'entreprise.

Date(s) de session

A déterminer en fonction du nombre de candidats
Formation en groupe de 8 participants maximum et 3 minimum.

Les objectifs

La transformation numérique des installations industrielles multiplie les échanges entre équipements, réseaux et systèmes d'information. Un accès mal maîtrisé ou une vulnérabilité non corrigée peut perturber un procédé et provoquer un arrêt de production.

Cette sensibilisation s'adresse aux décideurs et aux acteurs de l'industrie. Grâce à une véritable platine industrielle, les participants découvrent les mécanismes d'une cyberattaque et les questions essentielles à poser pour engager une démarche de sécurisation.

Public et prérequis

Dirigeants d'entreprise et d'usine, responsables de production, maintenance, exploitation, sécurité, informatique et OT, communication, et toute personne impliquée dans la gestion ou le fonctionnement d'installations industrielles.

Aucun prérequis.

Points forts

Une approche concrète et accessible sans prérequis technique : expérimentation sur une véritable platine industrielle connectée et de matériel informatique standard. Les participants observent différentes conséquences d'une attaque informatique et ses conséquences, jusqu'à la remise en service de la ligne de production. Étude de cas de cyberattaque réelle, échanges entre professionnels et outil d'aide à la décision pour prolonger la réflexion en entreprise.

Programme et contenu

PROGRAMME - Sensibilisation à la cybersécurité industrielle

Objectifs pédagogiques - À l'issue de la formation, le participant sera capable de :

- Identifier les principales vulnérabilités et les risques auxquels sont exposées les installations industrielles.

CENTRES DE FORMATION
Poitiers

DURÉE DE LA FORMATION
4 heures

TARIF
350 € HT

ACCUEIL PSH
Nos établissements sont engagés dans une démarche de progrès pour l'accessibilité des centres de formation, en collaboration avec le Centre Ressource Formation Handicap. Pour connaitre la faisabilité de votre projet de formation, contactez directement notre référent handicap au 05 49 37 44 56

Les + Pôle Formation UIMM Poitou Charentes

• 1200 Jeunes formés par an
• 600 contrats d'alternance à pourvoir
• 500 entreprises partenaires
• Accompagnement individualisé
• Diplômes reconnus par l'Etat

• Savoir-être, management, sécurité
• Pédagogie innovante (par projets, en îlots, projet Voltaire, Olympiades des métiers)
• Equipement en machines modernes qui préparent aux métiers de demain

- Analyser les mécanismes et les conséquences d'une cyberattaque industrielle, à partir d'expérimentations sur une maquette et d'une étude de cas réelle.
- Identifier les principaux points de vigilance en cybersécurité industrielle et questionner les pratiques de son organisation à partir de recommandations de l'ANSSI.

Contenu :

- Introduction aux risques cyber industriels : contexte, exemples et chiffres clés de la cybercriminalité en France.
- Étude d'un scénario d'intrusion : recherche d'informations, accès non autorisé à un réseau industriel et identification de vulnérabilités connues.
- Expérimentations encadrées sur la platine : prise de contrôle du procédé, lecture d'informations sensibles, altération et interruption du fonctionnement de l'automate.
- Observation de la remise en service : rechargement du projet automate et mesure du temps nécessaire . analyse collective des conséquences sur la continuité d'activité.
- Étude de cas et échanges sur les impacts des cyberattaques dans l'industrie.
- Principaux points de vigilance et recommandations de l'ANSSI . questionnement des pratiques de l'entreprise et présentation des suites possibles de formation.
- Démonstration d’une attaque générée par IA.

Méthodes pédagogiques et modalités d'évaluation

Formation exclusivement en présentiel, au Pôle Formation de Poitiers. Alternance d'apports illustrés, d'étude de cas, de manipulations encadrées sur platine industrielle et d'échanges collectifs.

Attestation de fin de formation remise aux participants. Un outil de questionnement et d'aide à la décision est prévu pour engager les échanges avec les équipes de production, de maintenance, d'informatique.

Contact

Site de Poitiers (86)
Michael BLAINEAU

- Tél : 06 28 62 49 20
- Mail : mblaineau@fi-pc.fr

Guillaume BOTHOREL

- Tél : 06 35 31 30 76
- Mail : gbothorel@fi-pc.fr

Site de Niort (79)
Xavier CHARBONNEAU

- Tél : 06 03 19 11 69
- Mail : xcharbonneau@fi-pc.fr

Dernière mise à jour

20/10/2026