



CYBERSÉCURITÉ DES SYSTÈMES D'INFORMATION INDUSTRIELS

Apprenez les fondamentaux de sécurisation des systèmes d'information industriels

Code : CYBERINDUS

NOUVEAUTÉ

Ce cours sur les fondamentaux à la cybersécurité des systèmes d'information industriels offre aux participants une immersion concrète dans les enjeux de sécurité des environnements SCADA et OT.

À travers une approche mêlant théorie et pratique, il permet de comprendre le fonctionnement des protocoles industriels comme Modbus TCP, d'identifier les vulnérabilités propres à ces systèmes et d'analyser différentes attaques. Les travaux pratiques basés sur l'analyse de traces réseau réelles fournissent aux apprenants les compétences techniques pour détecter des anomalies, interpréter des comportements malveillants et proposer des mesures d'atténuation adaptées.

Ce module constitue ainsi une base solide pour aborder les défis croissants de cybersécurité dans les infrastructures critiques et les environnements industriels connectés.

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : En amont de la formation, une évaluation des compétences de l'apprenant est effectuée. Puis, les objectifs sont évalués tout au long de la formation sous forme de questions réponses et d'études de cas, ainsi que par la grille d'évaluation des compétences complétée en fin de module par le formateur.

JOUR 1

Les installations industrielles

- Définition, et concepts usuels
- Des installations sous contraintes
- Les installations industrielles et les réglementations
- Homologation des systèmes industriels

Enjeux des systèmes d'information industriels

- Définition
- Fonctionnement
- Les protocoles dans un SI industriel
- Architecture et composants dans un SI industriel
- Spécificité et vulnérabilités
- Les protocoles de communication
- Les langages de programmation

CONTRÔLE DES CONNAISSANCES

JOUR 2

Problématiques liés à la cybersécurité des systèmes d'information industriels

- Mythes et réalités sur la sécurité des SI industriels
- Exemples d'attaques
- Cybersécurité et sûreté de fonctionnement

Sécurité des systèmes d'information industriels

- Un niveau de sécurité proportionné aux enjeux
- Gestion des risques et critères DICT
- Mesures de sécurité organisationnelles

- Mesures de sécurité techniques
- Normes et standards
- Les classes de cybersécurité selon l'ANSSI
- Les solutions du marché en cybersécurité des SI Industriel

CONTRÔLE DES CONNAISSANCES

JOUR 3

Operational Technology et Industrie 4.0

- Itinéraire de la cybersécurité des systèmes d'information industriels (maturité)
- L'industrie 4.0
- De nouvelles problématiques avec l'IA
- À l'heure de l'efficacité énergétique

ÉTUDES DE CAS PRATIQUES

PROCHAINES DATES



16 FEV - 20 MAI - 26 AOÛT - 23 NOV



OBJECTIFS

- Comprendre l'architecture et les composants clés d'un système industriel
- Analyser les protocoles industriels et distinguer les communications normales des comportements suspects
- Utiliser des outils d'analyse réseau pour détecter et diagnostiquer des cyberattaques sur les SI industriels
- Identifier les risques, proposer des mesures de sécurité adaptées et comprendre les principes du zoning selon la norme IEC 62443
- Développer une posture d'analyse critique face aux incidents cyber, en intégrant les enjeux de continuité opérationnelle et de cybersécurité



INFORMATIONS GÉNÉRALES

Code : CYBERINDUS**Durée :** 3 jours**Prix :** 2 390 € HT**Horaires :** 9h30 - 17h30**Lieu :** Levallois (92) - ou en distanciel**Les + :** petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

PUBLIC VISÉ

- RSSI
- Ingénieurs / Techniciens
- Administrateurs systèmes et réseaux
- Analyste SOC
- Analyste en conformité



PRÉ-REQUIS

- Connaissance de base en informatique et cybersécurité
- Rigueur d'analyse et approche méthodique
- Aucune expérience préalable en automatisme n'est exigée



RESSOURCES

- Support de cours
- Contrôle des connaissances acquises
- Exercices pratiques
- 1 PC par personne