Cybersécurité des installations Industrielles IEC 62443

Programme *(Mis à jour le 10/09/2025)*

JOUR 1

- Panorama cybersécurité
- Les enjeux et contraintes
- Les principes de sécurité
- Vocabulaire
- Architecture et composants
- Les protocoles usuels
- L'écosystème
- Les typologies de menaces
- Les attaques courantes
- IT vs OT
- Pourquoi mettre en place un programme de cybersécurité industrielle
- Exercices sur les attaques, quizz sur les notions théoriques essentielles et vocabulaire
- Les concepts
- Les 7 exigences fondamentales (62433-1-1)
- SL, SL-A, SL-C SL-T
- Niveaux de maturité
- Les certifications
- Rôles et responsabilités
- Les actifs
- Les risques
- Les phases du CSMS
- Les politiques et procédures
- Les zones de sécurité
- Les conduits
- Les niveaux de sécurité
- Les modèles
- Ensemble d'exigences pour aborder le CSMS
- Exercices à partir d'études de cas, réflexion et préparation du projet d'implémentation d'un CSMS

JOUR 2 Composition du CSMS

- Les éléments
- Gestion des risques
- Lien entre risques et CSMS
- Les catégories
- Les mesures
- Implémentation
- Surveillance et amélioration
- Réaliser une analyse de maturité des processus
- Réaliser une analyse du niveau de sécurité
- Travaux Dirigés / Exercices : analyse des écarts

JOUR 3 62443 et les fournisseurs de services IACS

- 62443 2-4 overview
- Propriétaire vs fournisseur : différentes façons d'utiliser la norme
- Intégration des services

Référence

THIS3630

Durée

5 jours / 35 heures

Prix HT / stagiaire

3950€

Objectifs pédagogiques

- Identifier les exigences et la structure des normes IEC62443
- Dialoguer avec le vocabulaire adapté
- Réaliser une évaluation de maturité des processus
- Réaliser une évaluation de niveau des mesures de sécurité
- Choisir les certifications adaptées à la stratégie de l'entreprise
- Identifier les risques liés aux installations industrielles

Niveau requis

- Connaissance du fonctionnement managérial et organisationnel d'une structure
- Connaissance de base en sécurité de l'information et des systèmes industriels

Public concerné

- Responsable de projet sécurité industrielle
- Architecte sécurité industrielle
- Concepteur produits pour industrie
- Ingénieur cyber sécurité
- Consultant sécurité
- DSI
- RSSI
- Risk Manager

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation de handicap peuvent avoir des besoins spécifiques pour suivre la formation. N'hésitez pas à nous contacter pour en discuter) équipée d'un ordinateur de dernière génération par stagiaire, réseau haut débit et vidéo-projection UHD
Documents supports de formation projetés
Apports théoriques, étude de cas concrets et exercices

- Maintenance
- Overview des exigences
- Gestion de la maturité
- Travaux Dirigés : Etude de cas

JOUR 4 Gestion des développements des produits sécurisés

- La défense en profondeur
- Management de la sécurité
- Exigences de sécurité : spécifications
- Secure by design
- Implémentation sécurisée
- Vérification et test de validation
- Gestion des écarts
- Mise à jour
- Pratiques de sécurité
- Niveaux de sécurité
- Évaluation du niveau de sécurité d’un produit
- Exercices : à partir d’une étude de cas, réalisation d’une évaluation du niveau de sécurité et proposition d’amélioration.

JOUR 5 Préparation certification

- Quizz global.
- Etude de cas
- Examen final : Qcm sur la cybersécurité industrielle, vocabulaire, 63443 ; Mise en situation sur analyse des écarts, développement, SL, étude de cas