41 rue Garibaldi – 69006 LYON

Valérie Thoraval
04.72.32.50.60

contact@cpe-formation.fr
cpe-formation.fr

CYBERSÉCURITÉ

CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS – IEC 62 443. COMPRENDRE LA NORME AFIN DE SÉCURISER SON ARCHITECTURE

OBJECTIFS

Sensibiliser aux principaux risques afin de concevoir des produits et des systèmes industriels plus robustes. Cas d'attaques cyber en milieu industriel, les principes de sécurité en profondeur, la cryptologie, les normes 27002, de l'ISO 27005 et IEC62443. Être capable de concevoir des produits et des systèmes industriels renforcés.

CONTENU PÉDAGOGIQUE

JOUR 1

Introduction
• Présentation
Cybersécurité dans le monde industriel
• Comprendre la cybersécurité dans le contexte industriel
• Menaces et méthodologies d'attaques
• Divergence et convergence IT / OT
Norme ISA/IEC 62443
• Comprendre les concepts de la norme
• Processus d'évaluation des risques
• Évaluation initiale des risques détaillés
• Acceptation et comparaison des risques
Ateliers
• WS1 – Définir le système considéré
• WS2 – Effectuer l'évaluation initiale des risques
• WS3 – Partitionnement des Zones et conduits

JOUR 2

Norme ISA/IEC 62443
• Processus d'évaluation détaillée des risques Défense en profondeur
• Systèmes – Sécurité physique
• Systèmes – Sécurité périmétrique
• Systèmes – Sécurité interne des réseaux Démonstration
• Cas classique de Mifare
• Attaque par Brute force WPA2 et usurpation ARP
• Crypto : Mauvaise implémentation du chiffrement Cryptographie
• Symétrique et asymétrique • Certificat et PKI (Infrastructure à clés publiques)
• Fonction de hachage avec "sel" et "poivre"
Ateliers
• WS4 – Évaluation des risques détaillée (1/2) – Scénarios de menaces

JOUR 3

Norme ISA/IEC 62443
• Cycle de vie du développement d'un produit sécurisé
• Exigences fondamentales
Défense en profondeur
• Produit – Sécurité de l'hôte
• Produit – Sécurité des applications
• Produit – Sécurité des données
Démonstration
• Rubber Ducky – Attaque USB
• Radiofréquence – Attaque par rejeu
Ateliers
• WS5 – Évaluation des risques détaillée (2/2) – Estimation des risques
• WS6 – Définition des niveaux de sécurité
• WS7 – Spécification des exigences de cybersécurité Détails sur les vulnérabilités
• MCS, CVE & CVSS

Tour de table

DURÉE
3 jours
21 heures

SESSIONS
- 22 - 24 juin 2027 en présentiel à Lyon

FRAIS D'INSCRIPTION (DÉJEUNER INCLUS)
2 500 € HT

PRÉREQUIS & PUBLIC CONCERNÉ
Ingénieurs ou architectes informatiques, responsables en sécurité industrielle, consultants, auditeurs en sécurité industrielle.
Bonne connaissance générale de l'informatique, notions en architecture informatique.

FORMATION À DISTANCE POSSIBLE, NOUS CONSULTER

Coordonnées

CPE Lyon Formation Continue

41 rue Garibaldi – 69006 LYON

04.72.32.50.60