CPFI
Cabinet Professionnel de Formation Industrielle



Sécurisation des communications industrielles : HART-IP, Modbus, DNP3

Lien : https://cpfi-formation.com/formation/securisation-des-communications-industrielles-hart-ip-modbus-dnp3

DURÉE
5 jours (35h)

RÉFÉRENCE
II57

CATÉGORIE
Cybersécurité OT & Sécurité Réseau Industrielle

CPFI Formation

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre l'architecture et les principes de fonctionnement des communications industrielles HART-IP, Modbus et DNP3.
- Identifier les différences entre les environnements IT et OT et leurs contraintes spécifiques en matière de cybersécurité.
- Identifier les principales vulnérabilités associées aux protocoles industriels.
- Comprendre les risques liés à l'absence ou aux limitations des mécanismes natifs d'authentification et de chiffrement.
- Analyser les flux de communication entre équipements de terrain, automates, RTU, SCADA et systèmes de supervision.
- Concevoir une architecture réseau OT reposant sur la segmentation et le principe de défense en profondeur.
- Mettre en œuvre des mécanismes de contrôle d'accès adaptés aux équipements industriels.
- Comprendre les principes de surveillance et de détection des anomalies dans les communications OT.
- Identifier les solutions IDS/IPS, SIEM et outils de monitoring adaptés aux environnements industriels.
- Développer des procédures de réponse aux incidents compatibles avec les exigences de disponibilité des systèmes OT.
- Renforcer la résilience des infrastructures industrielles par la sauvegarde, la restauration et la continuité d'activité.
- Développer une stratégie globale de sécurisation des communications industrielles permettant de réduire l'exposition aux cybermenaces tout en préservant la disponibilité et la sûreté des procédés.

CPFI Formation

POUR QUI ?

- Ingénieurs automatisme et contrôle-commande
- Ingénieurs réseaux industriels
- Ingénieurs instrumentation
- Ingénieurs électricité et systèmes industriels
- Ingénieurs cybersécurité OT
- Administrateurs réseaux industriels
- Architectes réseaux IT/OT
- Automaticiens et techniciens instrumentation
- Responsables SCADA et systèmes de contrôle
- Responsables cybersécurité industrielle
- Responsables systèmes d'information industriels
- Responsables maintenance et exploitation
- SOC Analysts spécialisés OT
- Ingénieurs téléconduite et systèmes électriques
- Intégrateurs de systèmes industriels
- Consultants en cybersécurité et infrastructures critiques
- Bureaux d'études et sociétés d'ingénierie
- Entreprises industrielles des secteurs de l'énergie, pétrole et gaz, eau, transport, chimie, mines, manufacturing et infrastructures critiques
- Toute personne impliquée dans la conception, l'exploitation, la maintenance, l'administration ou la sécurisation des réseaux et systèmes de communication industriels.

CPF Formation

CPFI
Cabinet Professionnel de Formation Industrielle



Programme détaillé

1 / ARCHITECTURE DES RÉSEAUX INDUSTRIELS OT

- Différences entre réseaux IT et OT
- Architecture terrain, contrôle, supervision et systèmes industriels
- Flux de communication entre capteurs, automates, SCADA et systèmes de supervision

2 / PROTOCOLE HART-IP : ARCHITECTURE ET SÉCURITÉ

- Principes de fonctionnement de HART-IP
- Communication entre instruments, passerelles et systèmes de contrôle
- Identification des risques et mesures de sécurisation

3 / MODBUS : FONCTIONNEMENT ET VULNÉRABILITÉS

- Modbus RTU, ASCII et TCP
- Architecture maître/esclave et échanges de données
- Limites de sécurité et risques liés à l'absence de mécanismes natifs d'authentification

4 / DNP3 ET SYSTÈMES DE TÉLÉCONDUITE

- Architecture et fonctionnement de DNP3
- Applications dans les réseaux électriques et infrastructures critiques
- Principes de sécurisation et authentification des communications

CPFI Formation

5 / ANALYSE DES VULNÉRABILITÉS DES PROTOCOLES INDUSTRIELS

- Menaces affectant les communications OT
- Usurpation, modification et rejeu des messages
- Déni de service et compromission des équipements

6 / SEGMENTATION ET ARCHITECTURE RÉSEAU SÉCURISÉE

- Segmentation des zones et conduits
- VLAN, pare-feu industriels et DMZ
- Séparation des réseaux IT, OT et systèmes critiques

7 / AUTHENTIFICATION, CONTRÔLE D'ACCÈS ET CHIFFREMENT

- Gestion des comptes et des privilèges
- Contrôle des accès aux équipements industriels
- Utilisation des mécanismes de sécurité disponibles et des tunnels sécurisés lorsque nécessaire

8 / SURVEILLANCE ET DÉTECTION DES ANOMALIES

- Analyse des flux réseau industriels
- Détection des comportements anormaux
- IDS/IPS, SIEM et supervision de sécurité OT

9 / GESTION DES INCIDENTS ET RÉSILIENCE OT

- Détection et qualification des incidents
- Procédures de réponse adaptées aux environnements industriels
- Sauvegarde, restauration et continuité des systèmes critiques

10 / ATELIER PRATIQUE : ARCHITECTURE OT SÉCURISÉE

- Analyse d'une architecture intégrant HART-IP, Modbus et DNP3
- Identification des vulnérabilités et définition des mesures de protection

CPTI Formation

- Élaboration d'une stratégie intégrant segmentation, contrôle d'accès, surveillance, détection des anomalies, réponse aux incidents et défense en profondeur

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Mises en Situation pour faciliter l'assimilation
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

07 au 11 Déc. 2026	Présentiel - Casablanca
18 au 22 Jan. 2027	Présentiel - Casablanca
15 au 19 Mars 2027	Présentiel - Casablanca
10 au 14 Mai 2027	Présentiel - Casablanca
05 au 09 Juil. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

CPFI Formation

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@cpfi-formation.com
Web : https//www.cpfi-formation.com

CPFI Formation — Tous droits réservés