Cabinet Professionnel de Formation Industrielle



Cryptographie Avancée pour la Cybersécurité des Systèmes Industriels : Protégez vos MES, SCADA et IoT

Lien : https://cpfi-formation.com/formation/cryptographie-avancee-pour-la-cybersecurite-des-systemes-industriels-protegez-vos-mes-scada-et-iot

DURÉE
5 jours (35h)

RÉFÉRENCE
II28

CATÉGORIE
Cybersécurité OT & Sécurité Réseau Industrielle

CPFI Formation

OBJECTIFS DE LA FORMATION

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

- Maîtriser les concepts avancés de cryptographie appliqués aux systèmes industriels
- Savoir implémenter des mécanismes de protection des données dans MES, SCADA et IoT industriel
- Apprendre à gérer la sécurité des clés, certificats et communications chiffrées
- Comprendre et appliquer les standards internationaux (NIST, ISO/IEC 27001, IEC 62443)
- Être capable de détecter, répondre et prévenir les incidents liés à la cryptographie
- Renforcer la résilience et la continuité des opérations industrielles
- Développer une approche globale de cybersécurité intégrant IT et OT
- Optimiser la confidentialité, l’intégrité et la disponibilité des données industrielles

POUR QUI ?

- Ingénieurs et responsables cybersécurité IT/OT
- Responsables de la traçabilité et des systèmes industriels
- Architectes et urbanistes des systèmes d’information industriels
- Techniciens et développeurs impliqués dans la sécurité industrielle

CPFI Formation

CPFI
Cabinet Professionnel de Formation Industrielle



Programme détaillé

1 / Introduction à la cryptographie industrielle

- Comprendre les principes fondamentaux de la cryptographie et son rôle dans la cybersécurité industrielle
- Identifier les menaces spécifiques aux systèmes d'information industriels (MES, SCADA, IoT industriel)
- Présenter les normes et standards internationaux (NIST, ISO/IEC 27001, IEC 62443)

2 / Chiffrement symétrique

- Étudier les algorithmes AES, DES et ChaCha20 adaptés aux SI industriels
- Démontrer la mise en œuvre du chiffrement pour protéger les données en transit et au repos
- Expliquer la gestion sécurisée des clés symétriques dans un environnement industriel

3 / Chiffrement asymétrique

- Comprendre RSA, ECC et Diffie-Hellman pour l'échange sécurisé de clés
- Démontrer les applications pour l'authentification et la signature numérique dans les SI industriels
- Étudier les scénarios d'intégration avec les protocoles industriels (OPC UA, MQTT)

4 / Hashing et intégrité des données

- Présenter les fonctions de hachage (SHA-2, SHA-3) pour garantir l'intégrité des données
- Expliquer la détection des altérations dans les bases MES et systèmes SCADA
- Illustrer l'utilisation des HMAC pour les communications sécurisées

CPFI Formation

5 / Gestion des clés et PKI

- Implémenter une infrastructure à clés publiques (PKI) dans un contexte industriel
- Définir les politiques de cycle de vie des clés (génération, distribution, renouvellement, révocation)
- Étudier les bonnes pratiques pour sécuriser les certificats et autorités de certification internes

6 / Protocoles sécurisés pour l’IoT industriel

- Analyser TLS, DTLS et MQTT-S pour les échanges sécurisés entre capteurs et systèmes MES
- Détecter les vulnérabilités spécifiques à l'IoT industriel et proposer des mesures cryptographiques
- Mettre en place des canaux de communication chiffrés pour les automates et SCADA

7 / Authentification et contrôle d’accès

- Implémenter des mécanismes d’authentification forte (2FA, certificats, tokens)
- Étudier la gestion des droits d’accès aux données critiques MES et SCADA
- Introduire l’authentification basée sur PKI pour les systèmes industriels

8 / Sécurité des données au repos et en transit

- Chiffrer les bases de données MES et journaux SCADA sensibles
- Protéger les backups et transferts inter-sites via des canaux sécurisés
- Mettre en œuvre la séparation des environnements IT et OT avec sécurité cryptographique

9 / Détection et réponse aux incidents cryptographiques

- Identifier les attaques sur les algorithmes et clés cryptographiques
- Étudier les stratégies de réponse en cas de compromission de clés ou de certificats
- Développer des plans de continuité et récupération sécurisée des SI industriels

10 / Audit, conformité et amélioration continue

- Réaliser des audits cryptographiques internes sur les systèmes industriels

CPF Formation

- Assurer la conformité aux standards internationaux et réglementations locales
- Mettre en place un processus d’amélioration continue pour la cybersécurité industrielle

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
12 au 18 Jan. 2027	Présentiel - Casablanca
08 au 12 Mars 2027	Présentiel - Casablanca
03 au 07 Mai 2027	Présentiel - Casablanca
28 Juin au 02 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