CPFI
Cabinet Professionnel de Formation Industrielle

SCADA : sécurité des systèmes industriels

Lien : https://cpfi-formation.com/formation/scada-securite-des-systemes-industriels

DURÉE
4 jours (28h)

RÉFÉRENCE
PRS55

CATÉGORIE
Risques et Securité

CPFI Formation

OBJECTIFS DE LA FORMATION

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

- Comprendre le métier et les problématiques
- Communiquer avec les automaticiens
- Identifier et maitriser les normes et standards propres au monde industriel
- Auditer un système SCADA
- Développer une politique de cybersécurité

POUR QUI ?

- Auditeurs
- Responsables de sécurité
- Automaticiens
- Architectes et administrateurs réseaux et systèmes ICS
- SCADA (Industrial Control Systems / Supervisory Control And Data Acquisition)

CPFI Formation

CPFI
Cabinet Professionnel de Formation Industrielle

Programme détaillé

1 / Enjeux concernant les Systèmes Industriels

- Enjeux d'un système d'information
- Spécificités et contraintes opérationnelles
- Architecture des systèmes SCADA
- Familles et Générations d'ICS
- Types d'équipement et Exemples d'architectures
- Architectures par secteurs d'activité
- Attentes des nouveaux systèmes industriels
- Principaux protocoles industriels

2 / Enjeux de la Sécurité d'une Infrastructure industrielle

- Convergence de l'OT et de l'IT
- Panorama de la cybersécurité
- Spécificités de la Cybersécurité Industrielle
- Profils des attaquants et leurs objectifs
- Grandes familles d'attaques :
- Spoofing
- Sniffing
- Forging...
- Prise de conscience de l'importance de la sécurité des SI industriels au sein de l'Etat et des entreprises : les différents aspects
- Les référentiels sur la sécurité des sytèmes d'information industriels

CPFI Formation

- Normes de la sécurité industrielle :
- IEC 62443
- ISO 27019
- IEC 61508 et 61511
- NIST 800-82
- Le "Threat Modeling" en fonction des générations et des équipements des systèmes SCADA
- Qu'est-ce que l'ANSSI et quel est son rôle ?

3 / Normes

- Panorama des normes et guides de la sécurité industrielle
- Normes de sécurité des SI de gestion ISO 270xx
- Normes de la sécurité industrielle IEC 61508 et 61511
- Norme de sécurité du NIST 800-82
- La convergence vers la norme de sécurité IEC 62443
- Les guides de l'ANSSI
- Maîtriser la SSI pour les systèmes industriels
- Méthode de classification et mesures principales
- Cas pratique
- Mesures détaillées

4 / Détermination des niveaux de classification par l'ANSSI

- Analyse basée sur le guide ANSSI relatif aux réseaux industriels

5 / Risques et menaces

- Attaques réelles sur les systèmes SCADA et retours d'expérience :
- Stuxnet, Duqu, Flame et Gauss
- Triton
- BlackEnergy, Dragonfly et Energetic Bear
- Night Dragon

CPF Formation

- APT33
- Les autres attaques sur des ICS
- Les facteurs de risque
- Les grands risques et familles de vulnérabilités
- Les menaces APT (Advanced Persistent Threat)
- Les postures de sécurité modernes des systèmes ICS

6 / Vulnérabilités intrinsèques des ICS

- Les vulnérabilités :
- Réseau
- Systèmes
- Applicatives
- Analyse avancée de la sécurité des PLC

7 / Travaux pratiques

- TP offensif
- Découvrir les machines exploitant Modbus sur un réseau
- Mettre sur écoute le protocole Modbus
- Détourner le trafic Modbus
- Falsifier une trame sur le protocole Modbus
- Réaliser un "fuzzing" sur les protocoles d'ICS / SCADA
- Découvrir les attaques sur S7comm
- Découvrir les protocoles BACnet et EtherNet/IP
- Découvrir les surfaces d'attaque sur les PLC
- Maîtriser l'analyse de firmware sur les PLC
- Mettre en place une attaque par rebond via un PLC
- Réaliser un brute-force sur un PLC ou une supervision

8 / Evaluer la sécurité de ses installations

CPF Formation

- Réunir les éléments-clefs d'un diagnostic préalable
- Tests à prévoir pour des installations locales et/ou distribuées
- Outillage nécessaire pour l'audit
- Failles les plus couramment rencontrées
- Les plans d'actions types à appliquer et les outils requis

9 / Travaux Pratiques

- TP offensif
- Mettre en place un "Threat Modeling" pour attaquer les architectures réseaux ICS / SCADA
- Introduire Metasploit pour le test d'intrusion des systèmes ICS / SCADA
- Maîtriser l'exploitation de vulnérabilités dans les environnements ICS / SCADA
- Découvrir le pivoting dans les environnements ICS / SCADA
- TP défensif
- Analyse de trames / Forensic
- Réalisation de règles sur un IDS dédiées aux ICS
- Configuration d'un honeypot
- Conception d'une architecture sécurisée

10 / Accès distants

- Liaisons RTC
- Points d'accès VPN
- Boîtiers de télétransmission sans-fil et 4G
- Sécurité des liaisons sans-fil (Wi-Fi, liaisons radio)
- Problèmes spécifiques aux automates et IHM exposés sur Internet

11 / Postures défensives de protection des ICS

- Définir une politique de sécurité
- Mener une évaluation des risques
- Objets principaux de la sécurisation technique

CPFI Formation

- Authentification
- Chiffrement
- Le durcissement
- La traçabilité
- Les équipements dédiés
- Le patch management
- La sécurisation fonctionnelle et l'utilisation des garde-fous
- Comment réagir à un incident de sécurité
- Les facteurs-clés de succès et bonnes pratiques
- L'intégration avec la sûreté industrielle
- Sécurité organisationnelle des réseaux industriels

12 / CAS PRATIQUES ADAPTES A VOTRE ACTIVITE

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

20 au 23 Oct. 2026	Distanciel

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

Document généré le 23/09/2026 — Réf : PRS55
CPFI Formation — Tous droits réservés

CPFI Formation