CPFI
Cabinet Professionnel de Formation Industrielle



Détection d'Intrusion et SOC pour Systèmes Électriques Industriels : SEMSIEM OT

Lien : https://cpfi-formation.com/formation/detection-dintrusion-et-soc-pour-systemes-electriques-industriels-semsiem-ot

DURÉE
10 jours (70h)

RÉFÉRENCE
II41

CATÉGORIE
Cybersécurité OT & Sécurité Réseau Industrielle

CPFI Formation

OBJECTIFS DE LA FORMATION

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

- Comprendre les spécificités de la cybersécurité des systèmes électriques industriels et des environnements OT.
- Concevoir une architecture SOC adaptée aux infrastructures critiques du secteur de l'énergie.
- Déployer une plateforme SIEM pour centraliser, corréler et analyser les événements de sécurité.
- Mettre en œuvre des solutions de détection d'intrusion adaptées aux réseaux industriels et aux protocoles OT.
- Identifier rapidement les cyberattaques visant les systèmes SCADA, IED, RTU, DCS et automates industriels.
- Exploiter les référentiels MITRE ATT&CK ICS et les flux de Threat Intelligence pour améliorer les capacités de détection.
- Mettre en œuvre une stratégie efficace de réponse aux incidents de cybersécurité en environnement OT.
- Sécuriser les architectures réseau grâce à la segmentation, aux pare-feu industriels et aux principes Zero Trust.
- Automatiser les processus de supervision et de réponse grâce aux solutions SOAR.
- Réaliser des audits de cybersécurité et garantir la conformité aux normes IEC 62443, IEC 62351, NIST et NERC CIP.
- Utiliser l'intelligence artificielle et les technologies d'analyse comportementale pour améliorer la détection des menaces.
- Développer une expertise permettant de concevoir, exploiter et optimiser un SOC OT assurant la protection continue des infrastructures électriques critiques.
- Renforcer la résilience cyber des réseaux électriques industriels face aux menaces actuelles et émergentes.
- Intégrer les meilleures pratiques internationales pour la gouvernance, la surveillance et la sécurisation des systèmes industriels de production, de transport et de distribution d'énergie.

CPFI Formation

POUR QUI ?

- Ingénieurs en cybersécurité industrielle
- Ingénieurs réseaux et télécommunications
- Ingénieurs SCADA et contrôle-commande
- Ingénieurs systèmes électriques
- Analystes SOC et SOC OT
- Responsables cybersécurité (CISO)
- Responsables OT et ICS
- Responsables exploitation des réseaux électriques
- Administrateurs systèmes et réseaux industriels
- Auditeurs cybersécurité et gestion des risques
- Consultants en cybersécurité des infrastructures critiques
- Personnel des producteurs d'électricité, gestionnaires de réseaux de transport (TSO), gestionnaires de réseaux de distribution (DSO), industries de procédés, sociétés EPC, intégrateurs de systèmes, opérateurs d'infrastructures critiques, bureaux d'études et organismes de régulation
- Toute personne impliquée dans la conception, l'exploitation, la supervision, la maintenance ou la sécurisation des systèmes électriques industriels souhaitant développer une expertise avancée en détection d'intrusion, SOC OT, SIEM, réponse aux incidents et cybersécurité des infrastructures critiques.

CPFI Formation

CPFI
Cabinet Professionnel de Formation Industrielle



Programme détaillé

1 / INTRODUCTION À LA CYBERSÉCURITÉ DES SYSTÈMES ÉLECTRIQUES INDUSTRIELS

- Architecture des environnements IT, OT et ICS
- Spécificités des systèmes SCADA, DCS, EMS et postes numériques
- Panorama des cybermenaces visant les infrastructures critiques

2 / ARCHITECTURE D'UN SOC OT

- Organisation et missions d'un Security Operations Center OT
- Gouvernance, rôles et responsabilités
- Architecture centralisée, distribuée et hybride

3 / SIEM ET COLLECTE DES JOURNAUX INDUSTRIELS

- Principes de fonctionnement des plateformes SIEM
- Collecte des logs des automates, IED, RTU, pare-feu et SCADA
- Normalisation, corrélation et enrichissement des événements

4 / DÉTECTION D'INTRUSION DANS LES RÉSEAUX OT

- IDS, IPS et sondes passives industrielles
- Détection comportementale et basée sur les signatures
- Surveillance des protocoles IEC 61850, Modbus, DNP3, OPC UA et IEC 60870-5-104

CPFI Formation

5 / SURVEILLANCE DES RÉSEAUX ÉLECTRIQUES INDUSTRIELS

- Cartographie des actifs OT
- Analyse du trafic réseau industriel
- Détection des anomalies et comportements anormaux

6 / THREAT INTELLIGENCE ET MITRE ATT&CK ICS

- Veille sur les menaces ciblant les infrastructures énergétiques
- Utilisation de MITRE ATT&CK ICS
- Corrélation entre renseignements de menace et événements SIEM

7 / RÉPONSE AUX INCIDENTS CYBER OT

- Détection, qualification et priorisation des incidents
- Procédures de confinement, d'éradication et de reprise
- Coordination avec les équipes exploitation et maintenance

8 / PROTECTION DES SYSTÈMES SCADA ET SOUS-STATIONS

- Sécurisation des postes électriques numériques
- Protection des IED, RTU, API et passerelles industrielles
- Gestion des accès et authentification renforcée

9 / SEGMENTATION ET ARCHITECTURES SÉCURISÉES

- Zones et conduits selon IEC 62443
- Pare-feu industriels, DMZ et Zero Trust
- Microsegmentation des réseaux OT

10 / SUPERVISION AVANCÉE ET AUTOMATISATION

- SOAR (Security Orchestration, Automation and Response)
- Tableaux de bord SOC OT

CPFI Formation

- Automatisation des alertes et des réponses

11 / AUDIT, CONFORMITÉ ET GESTION DES RISQUES

- Analyse de risques cyber des infrastructures électriques
- Audits techniques et organisationnels
- Conformité IEC 62443, IEC 62351, NERC CIP et ISO 27001

12 / EXERCICES DE CYBERDÉFENSE ET SIMULATION

- Exercices Red Team / Blue Team
- Simulation d'attaques sur réseau électrique industriel
- Retour d'expérience et amélioration continue

13 / DIGITALISATION ET IA POUR LE SOC OT

- Intelligence artificielle appliquée à la détection d'anomalies
- Machine Learning pour la cybersurveillance
- Jumeaux numériques et cybersécurité prédictive

14 / ATELIER PRATIQUE : CONCEPTION D'UN SOC OT POUR UNE INFRASTRUCTURE ÉLECTRIQUE

- Déploiement d'une architecture SIEM intégrée à un réseau SCADA
- Configuration des règles de détection et des tableaux de bord
- Élaboration d'une stratégie complète intégrant détection d'intrusion, surveillance continue, réponse aux incidents, conformité réglementaire et résilience cyber des infrastructures électriques

CPFI Formation

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

30 Nov. au 11 Déc. 2026	Présentiel - Casablanca
01 au 12 Fév. 2027	Présentiel - Casablanca
29 Mars au 09 Avr. 2027	Présentiel - Casablanca
24 Mai au 04 Juin 2027	Présentiel - Casablanca
19 au 30 Juil. 2027	Présentiel - Casablanca

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

Réservation & Renseignements

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

CPFI Formation — Tous droits réservés