

Cybersécurité des systèmes de contrôle industriel (SCADAICS) des infrastructures critiques : eau, énergie et transport

Lien : https://afrique-formation.com/formation/cybersecurite-des-systemes-de-controle-industriel-scadaics-des-infrastructures-critiques-eau-energie-et-transport

DURÉE
5 jours (35h)

RÉFÉRENCE
GRC120

CATÉGORIE
Cybersécurité et Risques Numériques

Afrique Formation

OBJECTIFS DE LA FORMATION

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

- Comprendre l'architecture et le fonctionnement des systèmes SCADA/ICS.
- Identifier les principales cybermenaces pesant sur les infrastructures critiques.
- Maîtriser les normes internationales de cybersécurité industrielle.
- Concevoir une architecture sécurisée pour les réseaux OT.
- Sécuriser les automates, serveurs et équipements industriels.
- Déployer des mécanismes de détection et de réponse aux incidents.
- Réaliser des audits et des évaluations de vulnérabilité des systèmes industriels.
- Renforcer la résilience et la continuité des infrastructures critiques.
- Intégrer les nouvelles technologies dans une stratégie de cybersécurité industrielle.
- Développer une approche globale de protection des systèmes de contrôle industriel.

POUR QUI ?

- Ingénieurs en automatisme et contrôle industriel
- Responsables cybersécurité (RSSI/CISO)
- Ingénieurs réseaux industriels et OT
- Administrateurs SCADA, DCS et ICS
- Responsables des infrastructures critiques
- Responsables maintenance et exploitation industrielle
- Ingénieurs en énergie, eau, transport et télécommunications
- Responsables de la continuité d'activité et de la gestion des risques
- Intégrateurs de systèmes industriels et bureaux d'études
- Cadres des autorités de régulation et organismes publics
- Toute personne impliquée dans la sécurisation, l'exploitation ou la gouvernance des systèmes industriels et des infrastructures critiques.

Afrique Formation

AFRIQUE FORMATION
La Référence en Afrique pour la Formation



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ DES SYSTÈMES SCADA/ICS

- Architecture des systèmes de contrôle industriel (SCADA, ICS, DCS et PLC)
- Différences entre les environnements IT (Information Technology) et OT (Operational Technology)
- Enjeux de cybersécurité des infrastructures critiques : eau, énergie et transport

2 / MENACES, VULNÉRABILITÉS ET PAYSAGE DES CYBERATTAQUES

- Typologie des cybermenaces visant les systèmes industriels
- Analyse des vulnérabilités des réseaux et équipements industriels
- Études de cas d'incidents majeurs et retours d'expérience

3 / CADRE RÉGLEMENTAIRE, NORMES ET BONNES PRATIQUES

- Normes IEC 62443, ISO/IEC 27001, NIST Cybersecurity Framework
- Directives relatives à la protection des infrastructures critiques
- Gouvernance de la cybersécurité industrielle et gestion de la conformité

4 / ARCHITECTURE SÉCURISÉE DES RÉSEAUX INDUSTRIELS

- Segmentation des réseaux IT/OT et zones de sécurité
- Pare-feu industriels, DMZ et contrôle des accès
- Sécurisation des communications et des protocoles industriels

Afrique Formation

5 / PROTECTION DES ÉQUIPEMENTS ET DES SYSTÈMES DE CONTRÔLE

- Sécurisation des automates programmables (PLC), RTU, IED et HMI
- Gestion des correctifs, durcissement (Hardening) et contrôle des configurations
- Protection des serveurs SCADA et des postes d'exploitation

6 / DÉTECTION, SURVEILLANCE ET RÉPONSE AUX INCIDENTS

- Mise en place de systèmes de supervision et de détection (IDS/IPS)
- Surveillance des réseaux OT et collecte des journaux
- Gestion des incidents et coordination avec les équipes SOC et CERT

7 / GESTION DES RISQUES ET CONTINUITÉ D'ACTIVITÉ

- Analyse des risques cyber appliquée aux environnements industriels
- Élaboration de plans de continuité et de reprise d'activité
- Gestion des scénarios de crise et résilience opérationnelle

8 / AUDIT, TESTS DE SÉCURITÉ ET ÉVALUATION DES VULNÉRABILITÉS

- Méthodologie d'audit des systèmes SCADA/ICS
- Évaluation des vulnérabilités et tests de sécurité adaptés aux environnements OT
- Élaboration de plans de remédiation et de renforcement

9 / NOUVELLES TECHNOLOGIES ET CYBERSÉCURITÉ INDUSTRIELLE

- IoT industriel (IIoT), Edge Computing et Cloud industriel
- Intelligence artificielle appliquée à la détection des cybermenaces
- Jumeaux numériques (Digital Twin) et cybersécurité des infrastructures intelligentes

10 / CAS PRATIQUES ET ÉLABORATION D'UNE STRATÉGIE DE CYBERSÉCURITÉ OT

- Analyse d'une architecture SCADA/ICS d'une infrastructure critique
- Élaboration d'un plan de sécurisation conforme aux standards internationaux

Afrique Formation

- Simulation de gestion d'un incident cyber affectant une infrastructure critique

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 04 Déc. 2026	Présentiel - Casablanca
04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 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@afrique-formation.com
Web : https//www.afrique-formation.com

Afrique Formation

Afrique Formation — Tous droits réservés