

# Cybersécurité des systèmes industriels (SCADA)

4 jours (28 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

**3 140 € HT** par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

## Objectifs

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

- Décrire le métier et les problématiques
- Dialoguer avec les automaticiens
- Identifier et expliquer les normes et standards propres au monde industriel
- Auditer un système SCADA
- Développer une politique de cybersécurité
- Proposer des mesures de consolidation et de sécurisation en milieu industriel.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

Responsables de la Sécurité des Systèmes d'Information (RSSI), Directeurs des Systèmes d'Information (DSI), auditeurs, responsables de sécurité, automaticiens, architectes et administrateurs réseaux et systèmes ICS / SCADA (Industrial Control Systems / Supervisory Control And Data Acquisition).

### Prérequis

Avoir de bonnes connaissances générales en informatique et en sécurité des systèmes d'information.

# Programme

## 1 Pendant votre formation

### Cybersécurité des systèmes industriels (SCADA)

Jour 1 – Matin

#### Tour d'horizon des systèmes industriels

- Les enjeux d'un système d'information
- Les spécificités et contraintes opérationnelles
- L'architecture des systèmes SCADA (IT / OT)
- Les familles et générations d'ICS
- Les types d'équipements et exemples d'architectures, l'IloT et l'XloT
- Les architectures par secteur d'activité
- Les attentes des nouveaux systèmes industriels
- Les principaux protocoles industriels

#### Exemples de travaux pratiques (à titre indicatif)

- *Modéliser l'environnement industriel d'un stagiaire ou proposé par le formateur*
- *Définir les enjeux de sécurité de cette architecture*

Jour 1 – Après-midi

#### Enjeux de la sécurité d'une infrastructure industrielle

- La convergence de l'OT et de l'IT : défis et opportunités
- Les principes de la cybersécurité
  - Confidentialité
  - Intégrité
  - Disponibilité
- Panorama des cybermenaces actuelles sur l'OT
- Les spécificités de la cybersécurité industrielle
- Les profils des attaquants et leurs objectifs
- Les grandes familles d'attaques :
  - Spoofing
  - Sniffing
  - Malware ICS...
- La prise de conscience de l'importance de la sécurité des SI industriels au sein de l'Etat et des entreprises
- Les référentiels sur la sécurité des systèmes d'information industriels
- Les normes de cybersécurité en milieu industriel
- Qu'est-ce que l'ANSSI et quel est son rôle ?

- Les OIV (Opérateur d'Importance Vitale) et les OSE (Opérateur de Services Essentiels)

Jour 2 – Matin

## Normes et standards

- Le panorama des normes et guides de la cybersécurité industrielle
- Les normes de sécurité des SI de gestion ISO 270xx
- Les normes ISO / IEC 27001 et 27019
- La norme de sécurité du NIST 800-82 Rev 3
  - Etendre la sécurité de l'ICS à l'OT global
- La convergence vers la norme de sécurité IEC 62443
  - Cadre global
  - IEC 62443-2-1(ed.2024)
  - IEC 62443-2-4 (ed.2023)
  - Evaluation des risques avec 62443-3-2
  - Les niveaux de sécurité avec 62443-3-3
  - La SDLC sécurisée avec 62443-4-1
- Les normes de la sécurité industrielle IEC 61508 et 61511
- Les réglementations spécifiques à l'industrie
  - NERC CIP pour l'énergie
  - Les standards pour l'eau et le traitement des eaux usées
- Les guides de l'ANSSI
  - Maîtriser la SSI pour les systèmes industriels
  - Méthode de classification et mesures principales
  - Cas pratique
  - Mesures détaillées

## Exemples de travaux pratiques (à titre indicatif)

- Mettre en oeuvre des méthodes de classification sur le système décrit dans le module précédent
- Proposer des mesures de sécurisation
- Décrire et organiser quelques points de passage d'une certification de cybersécurité évoquée dans ce chapitre

Jour 2 – Après-midi

## Panorama des menaces

- Les attaques réelles sur les systèmes SCADA et retours d'expérience :
  - Les célèbres Stuxnet, Duqu, Flame et Gauss
  - L'attaque Triton
  - Le malware Industroyer (CrashOverride)
  - Le malware Havex

- Les célèbres BlackEnergy, Dragonfly et Energetic Bear
- Pipedream / Incontroller (2022)
- COSMICENERGY (2023)
- Groupes APT récents : Sandworm, Volt Typhoon, CHERNOVITE, ransomware OT, APT34...

### Analyse de risque et modélisation

- Les facteurs de risque
- Menaces liées à l'IIOT et aux environnements hybrides
- Tactiques modernes : living-off-the-land, abus de protocoles légitimes
- Les menaces et les vulnérabilités spécifiques aux systèmes SCADA
- Les menaces APT (Advanced Persistent Threat)
- Les postures de sécurité modernes des systèmes ICS
- Les attaques sur la chaîne d'approvisionnement
- Le calcul d'un risque
- Les CVE (Common Vulnerabilities and Exposures)
- Le scoring CVSS (Common Vulnerability Scoring System)
- Les CWE (Common Weakness Enumeration)
- Les méthodes d'analyse des risques spécifiques à SCADA
- Le "Threat Modeling" en fonction des générations et des équipements des systèmes SCADA
- La modélisation avec ATT&CK
- Les plans de réponse aux incidents et de récupération après sinistre

#### Exemples de travaux pratiques (à titre indicatif)

- Modéliser le risque de l'architecture décrite dans le premier module
- Estimer le risque pour quelques composants

Jour 3 – Matin

### Vulnérabilités intrinsèques et fréquentes des ICS

- Les principales vulnérabilités
  - Réseaux (absence de segmentation, protocoles non chiffrés...)
  - Systèmes (OS obsolètes, droits excessifs...)
  - Applicatives (HMI non durcis, erreurs de configuration...)
- Le traitement de l'authentification, du contrôle d'accès et la gestion des identités
- La sécurisation des interfaces homme-machine (HMI) et des serveurs de données
- Fuzzing et tests de robustesse
- L'analyse avancée de la sécurité des PLC

#### Exemples de travaux pratiques (à titre indicatif)

- 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 surfaces d'attaques sur les PLC*
- *Mettre en place une attaque par rebond via un PLC*
- *Réaliser un brute-force sur un PLC ou une supervision*

Jour 3 – Après-midi

### Evaluer la sécurité de ses installations

- Réunir les éléments-clés d'un diagnostic préalable
- Tests à prévoir pour des installations locales et/ou distribuées
- Outillage nécessaire pour l'audit (scanners OT, sniffers, superviseurs)
- Les méthodes d'analyse de risque et d'audit OT
- Les plans d'actions types à appliquer et les outils requis
- Détermination des niveaux de classification par l'ANSSI
- Le processus d'audit et de conformité pour les systèmes SCADA / IEC 62443 / NIS2

*Exemples de travaux pratiques (à titre indicatif)*

- *Capturer et analyser des trames Modbus*
- *Analyser la sécurité d'un PLC avec un scanneur de vulnérabilité*
- *Evaluer le risque d'un processus industriel décrit par un stagiaire ou le formateur*

### Accès distants

- L'exposition publique des ICS (Shodan, Censys, Zoomeye...)
- L'exposition des ICS dans les réseaux privés
- Les liaisons RTC
- Les points d'accès VPN
- Les boîtiers de télétransmission sans-fil et 4G / 5G
- La sécurité des liaisons sans-fil (Wi-Fi, liaisons radio)
- Le chiffrement des liaisons

Jour 4 – Matin

### Postures défensives de protection des ICS

- Définir une politique de sécurité
- Principes de Zero Trust appliqués à l'OT
- Les objets principaux de la sécurisation technique
  - L'authentification / contrôle d'accès
  - Le chiffrement
  - Le durcissement
  - La traçabilité

- Les équipements dédiés
- Le patch management
- Firewalls industriels, DMZ, diode unidirectionnelle
- La sécurisation fonctionnelle et l'utilisation des garde-fous
- Les techniques de monitoring en temps réel et outils analytiques
- La détection d'anomalies et réponse aux alarmes
- Rôle des honeypots, sandboxing, supervision OT

Jour 4 – Après-midi

### Postures défensives de protection des ICS – Suite

- L'utilisation de SIEM (Security Information and Event Management) dans un contexte SCADA
- Gestion des SBOM (Software Bill of Materials)
- Comment réagir à un incident de sécurité
- Les facteurs clés de succès et bonnes pratiques
- L'intégration avec la sûreté industrielle
- La sécurité organisationnelle des réseaux industriels

*Exemples de travaux pratiques (à titre indicatif)*

- Installation d'un IDS et création de règles dédiées aux ICS
- Configuration d'un Honeypot
- Conception théorique d'une architecture sécurisée sur la base d'un schéma infrastructurel standard

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

### Accessibilité aux personnes en situation de handicap

## Détails de la session

Du 27 avril 2027 au 30 avril 2027 (4 jours / 28 heures)

Lyon

Du 27 avril 2027 au 30 avril 2027 **Lyon**

- 27 avril 2027 ..... 9h00 - 15h30
- 28 avril 2027 ..... 9h00 - 15h30
- 29 avril 2027 ..... 9h00 - 15h30
- 30 avril 2027 ..... 9h00 - 15h30