

# Mise en oeuvre et audit des contrôles CIS

3 jours (21 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

**2 925 € 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 :

- Reconnaître les enjeux de cybersécurité dans les environnements industriels et les attentes exprimées par les grands cadres internationaux (IEC 62443, NIST, ISA/99)
- Cartographier un système ICS selon les principes de zones, conduits, actifs critiques et niveaux de sécurité (SL)
- Mettre en oeuvre les contrôles fondamentaux de sécurité OT (segmentation, durcissement, journalisation) adaptés à un environnement de production
- Réaliser un audit de conformité et de posture sécurité OT, basé sur IEC 62443-2-4 et enrichi par les techniques MITRE ATT&CK for ICS et les recommandations du NIST SP 800-82
- Proposer un plan d'action réalisable et priorisé, structuré selon la maturité de l'organisation et les référentiels reconnus.

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

## À qui s'adresse cette formation ?

Exploitants, intégrateurs et responsables ICS / SCADA, consultants en cybersécurité industrielle, architectes réseaux industriels, RSSI, DSI et responsables conformité OT / IT / OT.

### Prérequis

Avoir une connaissance des architectures industrielles (topologie, automates, protocoles Modbus, OPC UA...) ainsi que des bases en sécurité des réseaux (VLAN, firewall) et idéalement une expérience en exploitation, intégration ou sécurisation d'environnement OT.

# Programme

## 1 Pendant votre formation

### Mise en oeuvre et audit des contrôles CIS

Jour 1 – Matin

#### Cadres de référence et cartographie de l'environnement OT

- Présentation des menaces spécifiques aux environnements industriels (TRITON, Colonial Pipeline, Industroyer 2, Volt Typhoon)
- Tour d'horizon des cadres normatifs et guides internationaux :
  - IEC 62443 : structure et niveaux de sécurité (SL)
  - NIST SP 800-82 Rev.2 : sécurité des ICS selon les standards US
  - ISA/99, C2M2, ISO/IEC 27019 : vision complémentaire sur la maturité et la gestion du risque OT
- Positionnement comparé : ce que chaque cadre apporte et quand l'utiliser

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

- Cartographie d'un environnement ICS en zones et conduits avec SL cibles, points critiques et flux sensibles

Jour 1 – Après-midi

#### Cadres de référence et cartographie de l'environnement OT – Suite

- Inventaire des actifs : comment identifier les systèmes réellement présents, incluant les Shadow OT
- Techniques de scan (Zeek, Wireshark), confrontation avec la CMDB ou plans réseaux existants
- Identification des points de faiblesse récurrents selon les cadres IEC / NIST : actifs obsolètes, systèmes non durcis, segments mal isolés

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

- Analyse d'un réseau OT simulé : identification des actifs, anomalies dans l'architecture, mise en parallèle avec les recommandations du NIST SP 800-82 (zones, segmentation, accès)

Jour 2 – Matin

#### Mise en oeuvre des contrôles de sécurité OT

- Contrôles de segmentation réseau (IEC 62443-3-2 et NIST) : DMZ, filtrage, séparation logique / physique
- Contrôle d'accès (IEC 62443-3-3) : gestion des identités, accès console automate, sécurité des postes d'ingénierie
- Mise en perspective avec les modèles C2M2 : liens entre organisation de la sécurité et architecture réseau

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

- Diagnostic d'une segmentation insuffisante dans un réseau ICS simulé, proposition de mesures correctrices compatibles avec les contraintes de production

Jour 2 – Après-midi

## Mise en oeuvre des contrôles de sécurité OT – Suite

- Durcissement des équipements industriels (IEC 62443-4-2) : patching impossible, désactivation des services, protection physique
- Introduction à la surveillance réseau OT : journalisation locale, centralisation, détection minimale attendue selon le NIST
- Utilisation raisonnée de MITRE ATT&CK for ICS : comme catalogue de techniques exploitables et base d'illustration pour les écarts de sécurité

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

- *Détection de comportements suspects dans un flux OT, lecture croisée avec les techniques MITRE et les points de contrôle du NIST SP 800-82*

Jour 3 – Matin

## Audit structuré et plan d'action priorisé

- Méthodologie d'audit OT selon IEC 62443-2-4 : préparation, collecte des preuves, grille d'évaluation
- Notions de maturité et référentiels d'aide à la décision : ISO 27019, C2M2 (résilience OT)
- Evaluations SL atteintes : comment identifier objectivement un niveau SL1, SL2 ou SL3 dans un contexte industriel

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

- *Réaliser un mini-audit OT : grille de contrôle simplifiée, analyse des preuves, classification des écarts (niveau SL, criticité, exploitabilité)*

Jour 3 – Après-midi

## Audit structuré et plan d'action priorisé – Suite

- Elaboration d'un plan d'action priorisé :
  - Intégrer les contraintes OT (production, fournisseurs, obsolescence)
  - Distinguer les quick wins des actions structurelles
  - Recommander des mesures compatibles avec les recommandations NIST / IEC / C2M2
- Techniques de restitution : comment convaincre un comité de direction ou RSSI sans surcharger de technique

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

- *Restitution orale d'un audit ICS et présentation d'un plan de remédiation argumenté avec feuille de route et priorisation*

## 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 2 décembre 2026 au 4 décembre 2026 (3 jours / 21 heures)

**À distance**

Du 2 décembre 2026 au 4 décembre 2026

**À distance**

- 2 décembre 2026 ..... 9h00 - 16h00
- 3 décembre 2026 ..... 9h00 - 16h00
- 4 décembre 2026 ..... 9h00 - 16h00