# Tests d’Intrusion et Cybersécurité des Infrastructures Industrielles

*Lien : https://innov-systems.com/formation/tests-dintrusion-et-cybersecurite-des-infrastructures-industrielles*

| DURÉE | RÉFÉRENCE | CATÉGORIE |
| --- | --- | --- |
| **5 jours (35h)** | **SEC301** | **Cybersécurité technique** |

## OBJECTIFS DE LA FORMATION

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

- Identifier les spécificités techniques et organisationnelles des environnements industriels (ICS/OT)
- Maîtriser les outils et méthodologies adaptés aux tests d’intrusion sur systèmes industriels
- Réaliser des audits techniques sur des automates et réseaux industriels en toute sécurité
- Comprendre les vulnérabilités typiques et les moyens de sécurisation des SI industriels
- Mettre en œuvre un test d’intrusion complet sur un environnement industriel simulé

## POUR QUI ?

- Ingénieurs et responsables en cybersécurité de systèmes industriels
- Responsables techniques d’infrastructures critiques (énergie, eau, transport, production)
- Techniciens en charge de la maintenance ou de l’intégration de réseaux OT
- Chefs de projet ou responsables sécurité souhaitant comprendre les menaces et mesures défensives dans un contexte industriel

## Programme détaillé

### 1 / COMPRÉHENSION DES SYSTÈMES INDUSTRIELS

- Panorama des architectures ICS/OT : SCADA, DCS, PLC, HMI, RTU
- Différences entre IT et OT : contraintes, objectifs et enjeux
- Modèles de référence : Purdue, ISA95, zones et conduits
- Acteurs et écosystème industriel

### 2 / BASES DE LA CYBERSÉCURITÉ INDUSTRIELLE

- Typologie des menaces et attaques récentes sur ICS
- Composantes d'un système industriel typique
- Introduction à la défense en profondeur dans les environnements OT

### 3 / ATELIER PRATIQUE – CARTOGRAPHIE D'UN ENVIRONNEMENT INDUSTRIEL

- Identification des flux réseau
- Repérage des équipements critiques
- Élaboration d'un schéma d'architecture simplifié

### 4 / APPROCHE MÉTHODOLOGIQUE DES TESTS D'INTRUSION OT

- Étapes clés : reconnaissance, analyse, exploitation, post-exploitation
- Cadres méthodologiques : PTES, NIST SP800-115, IEC 62443
- Gestion des risques et périmètre des tests

### 5 / OUTILS SPÉCIFIQUES AUX ENVIRONNEMENTS INDUSTRIELS

- Présentation de Nmap, Wireshark, Metasploit, Crackmapexec
- Outils OT : modscan, plcscan, snap7, mbtget
- Bonnes pratiques d'utilisation pour éviter les interruptions de service

## 6 / ATELIER PRATIQUE – SCANS ET ANALYSES DE RÉSEAU OT

- Identification d’automates et équipements réseau
- Interprétation de trames industrielles avec Wireshark
- Reconnaissance passive sur un réseau simulé

## 7 / ENVIRONNEMENTS WINDOWS ET ACTIVE DIRECTORY DANS L’INDUSTRIE

- Rôles et dépendances IT/OT
- Failles classiques : authentification, partages, secrets
- Techniques de mouvement latéral entre zones IT et OT

## 8 / VULNÉRABILITÉS ET MAUVAIS USAGES COURANTS

- Segmentation réseau défaillante
- Protocoles non sécurisés (Modbus, S7, OPC-UA)
- Cas concrets de compromission d’automates et HMI

## 9 / ATELIER PRATIQUE – ATTAQUES CONTRÔLÉES SUR RÉSEAU HYBRIDE IT/OT

- Exploitation de failles de configuration
- Escalade de privilèges et rebonds vers le réseau industriel

## 10 / COMPRÉHENSION DES PRINCIPAUX PROTOCOLES INDUSTRIELS

- Présentation détaillée : Modbus/TCP, S7, DNP3, OPC-UA
- Vulnérabilités intrinsèques et contre-mesures
- Bonnes pratiques de surveillance réseau

## 11 / TESTS D’INTRUSION SUR AUTOMATES ET SCADA

- Surface d’attaque des automates : services web, FTP, HTTP
- Techniques d’exploitation spécifiques aux API Schneider et Siemens

- Interactions avec SCADA et supervision

## 12 / ATELIER PRATIQUE – TESTS D’INTRUSION SUR AUTOMATES SIMULÉS

- Utilisation de mbtget et snap7 pour communiquer avec des automates
- Observation de comportements anormaux et détection des intrusions
- Analyse de logs et recommandations correctives

## 13 / BONNES PRATIQUES ET CADRES DE RÉFÉRENCE

- Normes et référentiels : IEC 62443, NIST CSF, ISO 27019
- Cloisonnement, supervision, patch management et sensibilisation
- Focus sur les solutions de détection et diodes réseau

## 14 / ÉTUDE DE CAS COLLABORATIVE

- Analyse d’un environnement industriel fictif
- Identification des vulnérabilités critiques
- Élaboration d’un plan de remédiation et présentation synthétique

## 15 / EXERCICE DE SYNTHÈSE – CAPTURE THE FLAG INDUSTRIEL

- Compromission d’un poste bureautique
- Accès et pivot vers le réseau OT
- Interaction avec un automate et simulation d’impact physique contrôlé
- Débriefing collectif sur les enseignements et contre-mesures

## Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

## Prochaines dates programmées

| | |
|---|---|
| 29 Juin au 03 Juil. 2026 | Présentiel - Casablanca |
| 24 au 28 Août 2026 | Distanciel |
| 19 au 23 Oct. 2026 | Distanciel |

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

## Réservation & Renseignements

**Téléphone :** +212 522 247 210
**Email :** contact@innov-systems.com
**Web :** https//www.innov-systems.com