CCI TUNISO FRANÇAISE

# FORMATION :
# « Cybersécurité des technologies opérationnelles des systèmes industriels »

## ➢ Planning :

2 jours de formation, 11 & 12 novembre 2024 de 8h30 à 15h30.

## ➢ Lieu :

La formation se tiendra dans les locaux de la CCITF : Rue Lac Van, Berges du lac 1

## ➢ Frais :

1 200 DT HT /personne pour 2 jours de formation incluant déjeuners et pauses-café

## ➢ Population cible :

- DSI, Responsable informatique, Personnel informatique
- RSSI, Responsable de la sécurité des systèmes industriels
- Ingénieurs et techniciens en informatique industrielle, automatisation et en contrôle
- Responsable des systèmes OT
- Auditeurs et consultants en cybersécurité IT
- Chef de projet cybersécurité
- Risk manager
- Responsable Qualité
- Toutes personnes en charge de la conception, du développement, de l'intégration, de l'exploitation ou de la maintenance des systèmes industriels
- Différents responsables qui souhaitent élargir leurs compétences dans le domaine de la cybersécurité des systèmes industriels, de l'IoT et de l'IIoT.

| Jour | Contenus / Concepts clés à aborder | Méthodes, moyens pédagogiques et équipements | Durée (Heures) | |
|---|---|---|---|---|
| | | | Théorique | Pratique |
| **J1** | **Principaux types d'environnements ICS/OT et systèmes de contrôle industriels** (qui couvrent pratiquement toutes les activités et tous les secteurs)<br>– L'IT vs l'OT et la convergence entre IT et OT : Les Mythes et réalités<br>– Principaux types d'environnements ICS/OT (centrales électriques, usines de fabrication, datacenters, etc.)<br>– Exemples de systèmes exposés à des cyberrisques : Hvac, systèmes de sécurité électronique et physique, datacenters, détection et extinction incendie, scada, chaine industrielle, robots industriels, chaine d'approvisionnement, etc.<br>– Types de systèmes de contrôle et protocoles industriels<br>– Introduction à la cybersécurité OT<br>– Architecture de référence Perdue pour les entreprises<br>– Cycle de vie de la cybersécurité et défis OT/IACS<br>– Vue d'ensemble de l'IEC/ISA 62443<br>– Terminologies et concepts clés<br>– Les risques liés à la chaine d'approvisionnement et aux tiers.<br>– Exemples d'attaques marquantes et quelques statistiques | Vidéo projecteur<br>Présentation<br>Discussion ouverte pour clarifier les concepts clés<br>Réponses aux questions et aux préoccupations des participants | **06** | |
| **J2** | **Mise en œuvre de la cybersécurité OT**<br>– Architecture de réseau sécurisée pour les environnements ICS/OT<br>– Gestion des correctifs dans les IACS<br>– Implémentation de l'IEC 62443<br>– Approche de la sécurité by design : intégration de la sécurité dans les projets<br>**Aspects essentiels de la cybersécurité industrielle**<br>– Système de gestion de la cybersécurité (CSMS)<br>– Evaluation de la maturité en matière de cybersécurité OT<br>– Gouvernance en matière de cybersécurité OT<br>– Technologies de sécurité OT émergentes<br>– Recommandations pour faire face aux différents types d'attaques : une approche proactive<br>**Evaluation** | Vidéo projecteur<br>Présentation<br>Discussion ouverte pour clarifier les concepts clés<br>Réponses aux questions et aux préoccupations des participants | **06** | |
| **Total** | | | **12** | |