Cybersécurité des Systèmes Industriels - OT

CYB

SecNumedu
Formation continue
ANSSI

Objectifs :

- Comprendre les enjeux liés à la cybersécurité des systèmes de Contrôle-Commande industriels, des technologies opérationnelles (OT) et les particularités de ce domaine.
- Avoir les éléments de base d'identification des points faibles de ces systèmes ainsi que des recommandations et une méthodologie de renforcement du niveau de cybersécurité de systèmes existants.
- Comprendre les points clés à examiner lors de la conception de systèmes industriels.

Prérequis :

Connaissances de base en informatique et réseau ou avoir suivi un stage en réseau industriel «ARC», «TCP-IP», «RTI» ou «AUT5». Connaissances de base en systèmes de Contrôle-Commande (Industrial Control System) ou avoir suivi un stage en automatisme (ICS, BE-ICC ou AUT4).

Méthode Pédagogique :

- Approche conforme au guide ANSSI pour une formation sur la cybersécurité des systèmes industriels.
- Formation basée sur du cours, démonstrations pratiques sur système industriel.
- Intervenants expérimentés en cybersécurité et Contrôle-Commande industriel.

Formation en partenariat avec Cap Gemini - SOGETI High Tech

Public :

- Personnes en charge de la conception, du développement, de l'intégration, de la maintenance ou de l'exploitation de systèmes industriels (maîtrise d'ouvrage, maîtrise d'oeuvre, exploitants, etc.).
- Toute personne souhaitant renforcer (suivi, accompagnement, intégration, analyse, audit, ...) la cybersécurité des systèmes industriels.

Durée
3jours / 18h (hors temps de certification)

Horaires
mardi 9h00 - jeudi 12h00

Niveau d'acquis
Fondamentaux

Nature des connaissances
Action d'acquisition des connaissances

Modalités d'évaluation
QCM, QUIZ

Certification *(p132)*
(Optionnelle) Évaluation réalisée de 13h à 15h le dernier jour de la formation : QCM de 2 heures

Participants
Mini : 2 - Maxi : 12

Responsable
Fabien CIUTAT
Ce stage est susceptible d'être animé par un autre formateur (cf p134)

Dates, Prix & Certification
Consulter notre site internet : www.ira.eu

Formation disponible en partie en INTRA à la demande.

Informations Complémentaires :

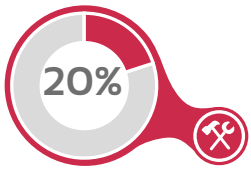
Formateur expert en Sécurité.

A l'issue de la formation : Remise d'une attestation de formation avec ou sans évaluation des acquis. Évaluation de la formation par les stagiaires.

Les repas sur Arles vous sont offerts.

Présentations &

Démonstrations



Programme :

INTRODUCTION - LA CYBERSÉCURITÉ ET SYSTÈMES INDUSTRIEL

- Définitions de la cybersécurité et principaux concepts.
- Définitions, les différents types, composants et caractéristiques de systèmes industriels - réseaux industriels (profibus, modbus, modbus TCP, ...).
- Différences entre sécurité (safety), sûreté (security), sûreté de fonctionnement et cybersécurité.
- Appréhender la différence de contexte et d'approche relatives aux menaces liées aux technologies de l'information (IT) des technologies opérationnelles (OT).
- Les systèmes de Contrôle-Commande industriels (SNCC, DCS, API, PLC, PAC, CN, systèmes embarqués, ...) - caractéristiques et spécificités.
- Retour d'expérience et exemples d'incidents.

PRINCIPES GÉNÉRAUX - CADRE RÉGLEMENTAIRE ET NORMATIF

- Loi de programmation Militaire (LPM), ANSSI, ...
- Grands principes pour déployer un projet cybersécurité (analyse de risque, DEP, PSSI, ...).
- Panorama des normes et standards (2700X, certification de produits, etc.) .
- Security level - CEI 62443.
- Safety Integrity Level - CEI 61508, CEI 61511, ...
- Exigences de cybersécurité pour les prestataires d'intégration et de maintenance de systèmes industriels.

ANALYSE DES RISQUES ET MENACES

- Approches d'analyses de risques adaptées à l'OT.
- Identification des enjeux, contexte et sources de menaces, utilisation du REX, état des lieux et surveillance, historique.
- Les vulnérabilités et vecteurs d'attaques classiques (Buffer overflow, MITM - man in the middle attack, spoofing, ingénierie sociale, détournement de sessions, DDOS - distributed denial of service attack, APT - Advanced Persistent Threat, Vers).
- Services présents dans les équipements industriels (API/PLC, SNCC/DCS, IHM, supervision/ SCADA, variateur, positionneur, instrumentation de terrain Smart, réseaux de terrain, liaison sans fil, etc.) : Web (HTTP/HTTPs), gestion d'équipements (SNMP, SYSLOG, etc.), émulation de terminal (Telnet), transfert de fichier (FTP).
- Les réseaux industriels (Profibus/Profinet, Ethernet/IP, Modbus RTU, Modbus/TCP, AS-I, WirelessHart, ...) et équipements (commutateur, routeur, pont, passerelle, ...).
- Les réseaux avec profil de sécurité (Profisafe, SafeEthernet, AS-i SAW, ...).

TECHNIQUES DE CYBERSÉCURITÉ

- Principe de cloisonnement des réseaux, moyens et équipements permettant de le réaliser (VLAN, VPN, diode, ...).
- Mise en œuvre de passerelles VPN (IPsec, SSL/TLS, MPLS, etc.).
- Analyses des différentes couches de protections.
- Sécurisation des équipements (durcissement des configurations, gestion des vulnérabilités, interfaces de connexion, équipements mobiles, sécurité des postes d'administration, développement sécurisé (principe du moindre privilège, éviter les dépassements de capacité, white listing applicatif).
- Surveillance d'un réseau (journaux d'évènements et alertes, système de détection d'intrusion (N-IDS).
- Principe de cryptographie (chiffrement symétrique/asymétrique, les fonctions de hachage, la signature, etc.).

DÉMONSTRATION PRATIQUE SUR SYSTÈMES INDUSTRIELS (20% DU TEMPS)

- À travers des architectures de Contrôle-Commande (Siemens, Schneider, Honeywell, Yokogawa, ABB, ...), SCADA et réseaux industriels, analyse des configurations, recherche des services et failles, identification et mise en œuvre de différentes couches et fonctions de cybersécurité.
- À travers des études de cas et des retours d'expérience.

* Certification IACS (Industrial Automation Control System)

Cette formation fait partie du cursus de formation associé à la certification «IACS - Cybersécurité industrielle - Cybersecurity OT».
Le cursus comprend les modules de formation suivant :
ARC + CYB
L'évaluation se déroule à l'issue du cursus lors du stage CYB (cybersécurité des systèmes industriels).