Cybersécurité des Systèmes Industriels - OT

Face au développement des systèmes industriels connectés et des systèmes permettant l'accès à distance à des fonctions opérationnelles de sécurité, la cybersécurité devient un nouvel enjeu à maîtriser dans le domaine du contrôle-commande et par les professionnels du terrain où elle était jusqu'alors peu présente.

Objectifs :

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

Prérequis :

- Connaissances de base en informatique et réseau, ou avoir suivi un de ces stage en réseau industriel : ARC p. 97, TCP-IP p. 89, ou RTI p. 33.
- Connaissances de base en systèmes de Contrôle-Commande ou avoir suivi un de ces stages en automatisme : ICS p. 91.

Méthode Pédagogique :

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

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.).
- Personnes souhaitant renforcer la cybersécurité des systèmes industriels (suivi, accompagnement, intégration, analyse, audit).

Programme :

INTRODUCTION - LA CYBERSÉCURITÉ ET LES SYSTÈMES INDUSTRIELS

- 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.
- Différence de contexte et d'approche relative 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.

PRINCIPES GÉNÉRAUX - CADRE RÉGLEMENTAIRE ET NORMATIF

- Loi de programmation Militaire (LPM), ANSSI, etc.
- 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 et 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 les 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 protection.
- 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.).

DÉMONSTRATIONS PRATIQUES 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.

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

Horaires
mardi 9 h - jeudi 12 h

Niveau d'acquis
Fondamentaux ★★☆

Nature des connaissances
Action d'acquisition des connaissances

Modalités d'évaluation
QCM, QUIZ

Participants
Mini : 2 - Maxi : 8

Responsable
Fabien CIUTAT

Formateur Principal
Fabien CIUTAT

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

Formation disponible en INTRA à la demande.

Infos complémentaires

Formateur expert en cybersécurité et Contrôle-Commande industriel.

À l'issue de la formation : Remise d'une attestation de formation avec évaluation des acquis.

Évaluation de la formation par les stagiaires.

Les repas sur Arles vous sont offerts.

Présentations & Démonstrations