CYBERSÉCURITÉ DES SYSTÈMES DE CONTRÔLE INDUSTRIELS

FFCNCERCERXCS19 | PRIX : 2 550 € | DURÉE : 3 JOURS

Pauses et déjeuners offerts

AVANCÉ | ATELIER | FAISABLE À DISTANCE | RÉALISABLE EN ANGLAIS

PRÉSENTATION

Les systèmes industriels sont soumis à une concurrence mondiale accrue. Ils doivent se digitaliser en vue d'automatiser leurs processus et d'optimiser leur efficacité. Ceci apporte innovation et sophistication, mais étend la surface d'attaque et rallonge la liste des vulnérabilités et des menaces auxquelles ces systèmes industriels peuvent être exposés.

La formation permet d'analyser le paysage de la menace qui pèse sur les systèmes industriels et l'illustre avec des cas concrets. Elle passe en revue les standards de sécurité et les solutions de protection associées.

OBJECTIFS

- Sensibiliser les acteurs du monde industriel aux menaces qui pèsent sur les installations industrielles
- Illustrer les menaces avec des exercices de type « Ethical Hacking » sur des systèmes cyber-physiques
- Analyser la menace et définir la politique de sécurité
- Prendre en main des solutions de sécurité (Firewall, contrôle d'accès, détection d'intrusion, etc.)
- Mettre en œuvre une stratégie de maintien en condition de sécurité et maintien en condition opérationnelle (mise à jour, gestion des correctifs, CTI, OSINT, etc.)

PROGRAMME

Introduction

Système de contrôle industriel, Industrial Control System (ICS)
- Technologies (automates programmables industriels, etc.)
- Composants d'un système industriel (PLC, capteurs, actionneurs, etc.)
- Protocoles industriels (Modbus, DNP3, OPC UA, TSN, etc.)
- Architectures et applications associées (SCADA, EMS, Historian, CIM, etc.)

Travaux pratiques
- Déploiement d'une infrastructure industrielle (Swtich, automate programmable, interface homme machine (IHM) et application de supervision)

Panorama d'attaques visant les installations industrielles
- Illustrer avec des cas concrets et des démonstrations

Travaux pratiques
- Mise en pratique des techniques d'audit et de reconnaissance pour la découverte de vulnérabilités
- Lancement d'attaques de type « rejeu », « Man in the Middle », « DoD », « Scan », etc.

Mesures de protection visant à renforcer la sécurité des systèmes
- Déploiement et mise en œuvre de solutions de protection
- Normes et standards de sécurité
- Mise en œuvre d'une défense en profondeur
- Déploiement et configuration de Firewall industriels
- Installation de sondes de détection, etc.

Politique de maintien de sécurité
- Mise en œuvre d'une politique de maintien en condition de sécurité (MCS) et maintien en condition opérationnelle (MCO)
- Gestion des correctifs, CTI, OSINT
- Cyber Threat Intelligence et son application à la sécurité des systèmes industriels
- Intérêt du renseignement sur sources ouvertes (OSINT) pour le maintien en condition de sécurité

Travaux pratiques
- Déploiement et configuration de solutions de sécurité : firewall, control d'accès, IDS/IPS
- Mise en place d'infrastructure de la Cyber Threat Intelligence pour le maintien en condition de sécurité

Synthèse et conclusion

PUBLIC/PRÉREQUIS

Responsables de sécurité, automaticiens, architectes et administrateurs réseaux et systèmes ICS/SCADA, auditeurs.

Des connaissances générales en système de contrôle industriel sont souhaitables afin de tirer pleinement profit de cette formation.

RESPONSABLE(S)

Reda YAICH
Responsable de l'équipe Sécurité Numérique de l'IRT SystemX. Son expertise porte sur la cybersécurité, tels que l'autorisation, le contrôle d'accès et la détection d'intrusion. Il a piloté des projets nationaux (ANR, PIA) et européens (FP7, COST, H2020, etc.) et enseigne. Il est titulaire d'un doctorat de l'École des Mines de Saint-Etienne et d'un Master Recherche de l'Université Paris-Sud.

MODALITÉS PÉDAGOGIQUES

La formation repose sur l'utilisation de matériel de pointe tel que la CyberRange. Un environnement cyber-physique sera également utilisé pour se rapprocher au mieux des conditions réelles. Des cas d'usages réalistes, issus de projets collaboratifs, seront utilisés afin d'illustrer les exemples de la formation.

PARTENAIRE

SystemX INSTITUT DE RECHERCHE TECHNOLOGIQUE