Sécurité des systèmes de contrôle industriels - ICS/SCADA

VOTRE FORMATION

DURÉE : 5 JOURS

35 heures

PROCHAINE SESSION :

20, 21, 22, 27 et 28 juillet 2020

LIEU : En distanciel

PRIX : 1 495 €

net de taxes

LE PUBLIC

Responsables/Expert sécurité

Chefs de projets industriels

LES OBJECTIFS

Connaître le métier et les problématiques

Contrôler la surface d'attaque d'un système ICS/SCADA

Connaître et comprendre les normes propres au monde industriel

Sécuriser vos systèmes ICS/SCADA

Développer une politique de cyber-sécurité

PRÉ-REQUIS

Pour suivre cette formation il convient d'avoir une bonne connaissance générale en informatique et en sécurité des systèmes d'information.

Connaissances de base sur les systèmes industriels et les systèmes de contrôle ICS/SCADA

MODALITES

Formation 100 % à distance

De 4 à 16 participants

9h –17h30

Financement éligible au FNE Formation pour tout salarié d'entreprise en activité partielle

Matériel requis : cartes et composants électroniques. A défaut, prévoir un coût supplémentaire pour des logiiciels de simulation en ligne.

VOTRE CONTACT :

Andrea FALLOURD
Conseillère en formation
06 74 51 44 97
afallourd@itescia.fr

ITESCIA - Campus de Pontoise
8 rue Pierre de Coubertin
95300 PONTOISE

www.itescia.fr

VOTRE PROGRAMME

Les systèmes de contrôle industriel ICS communément appelés SCADA, contrôlent les infrastructures industrielles. La plupart des infrastructures critiques sont contrôlés par des systèmes ICS/SCADA : des réseaux électriques au traitement de l'eau, de l'industrie pharmaceutique, automobile et chimique aux transports Cette formation répond à la nécessité pour les ingénieurs et les opérateurs de systèmes de contrôle de mieux comprendre le rôle important qu'ils jouent dans la cybersécurité. Cela commence par s'assurer qu'un système de contrôle est conçu avec une cybersécurité intégrée, et que la cybersécurité a le même niveau de sensibilité que la fiabilité du système tout au long du cycle de vie du système.

Introduction à la cybersécurité des systèmes ICS/SCADA

- Surface d'attaque ICS
- Sources de menace et raisons de l'attaque
- Surface d'attaque et entrées
- Attaque Niveau 0 et 1
- Plateforme De contrôle des choses
- Exercice: Trouver des mots de passe dans les décharges EEPROM
- Purdue Niveau 0 et 1 Technologies & Communications
- Familles du protocole Fieldbus

ICS/SCADA & Système d'information

- Ethernet et TCP/IP
- Ethernet & TCP/IP Concepts
- Protocoles ICS sur TCP/IP
- Wireshark et ICS
- Attaques contre les réseaux: Enumérant Modbus TCP
- Surface d'attaque ICS
- Attaques contre les IHM et les interfaces Users
- Attaques contre les serveurs de contrôle
- Attaques contre les communications réseau
- Attaques sur les appareils distants

Sécurisation des systèmes ICS/SCADA

- Windows & Linux dans ICS
- Mises à jour et patching
- Processus et services Durcissement de la configuration
- Défense de point de terminaison
- Automatisation et audit
- Gestion des journaux, Bases de données et historiques

Sécurité organisationnelle du réseau industriel

- Architecture SCADA
- Détermination des zones et conduites
- Sécurisation d'architecture
- Détermination des niveaux de classification ANSSI

Exercices Pratiques

- Programmation d'un PLC, IHM
- L'architecture d'un SDC sécurisé
- Trouver des mots de passe dans les périphériques embarqués
- Explorer les protocoles de Fieldbus
- Forensic d'une attaque
- Contournant Auth avec SQL Injection
- Fuzzing de mot de passe
- Baselining avec PowerShell
- Configuration des pare-feu basés sur l'hôte
- Journaux d'événements Windows
- Trouver l'accès à distance