SECURE SCADA

Administrez votre réseau industriel de manière cyber sécurisée

Objectif

Intégrer les bonnes pratiques de sécurité informatique dans l'administration d'un réseau industriel et savoir réaliser un audit et des tests de sécurité.

Destinataires

Administrateurs, automaticiens, responsables techniques, responsables supervision, intégrateurs.

Prérequis

Des connaissances générales en informatique et la connaissance des bases d'un langage de script (Python, Ruby, etc.) sont nécessaires.
La connaissance de notions en réseau et en programmation est un plus.

Méthode pédagogique

Une pédagogie immersive qui allie apports théoriques, retours d'expériences et cas pratiques pour un ancrage durable des compétences.
Les cas pratiques sont réalisés sur un système vulnérable fourni par SECURESPHERE.

Moyens techniques

Salle de formation équipée de postes de travail informatiques disposant de tous les logiciels nécessaires au déroulement de la formation.

Compétences acquises

- Détecter les vulnérabilités des équipements industriels en répertoriant les éléments constitutifs des réseaux industriels et les composants ainsi que les connexions entre ces éléments afin de localiser les fragilités
- Définir les grands principes de sécurité liés aux équipements industriels en analysant les règles de sécurité liées à TCP/IP dans le monde industriel ainsi que les architectures et technologies utilisées
- Contrôler l'application des recommandations et prescriptions nationales (Guides ANSSI et textes réglementaires) pour s'assurer d'une prise en compte des exigences liées à la sécurité des systèmes industriels, en vérifiant leur implémentation dans les procédures
- Sécuriser par des mesures techniques les réseaux et systèmes industriels afin de maintenir leur intégrité en déployant les correctifs adaptés aux vulnérabilités des installations
- Maintenir les systèmes industriels en fonctionnement et les protéger des intrusions en mettant en œuvre des procédures pour auditer régulièrement la fiabilité et la sécurité de ces systèmes
- Développer les outils adaptés pour contrôler régulièrement la sécurité (et la robustesse) des systèmes industriels et déployer les tests d'intrusion

Formateurs

Consultants-Formateurs spécialistes de la sécurité informatique.

DURÉE
4 jours - 28 heures

TARIF INTER
3 200 € HT
par stagiaire

TARIF INTRA
Nous contacter

LIEU
Campus Cyber
Tour Eria,
5 rue Bellini
92800 Puteaux

ou dans vos locaux

ACCESSIBILITÉ
Cette formation est accessible aux personnes en situation de handicap.

SECURESPHERE
est détenteur de la certification Qualiopi au titre de la catégorie d'actions de formation.

PROGRAMME

INTRODUCTION

- Préparation des machines et plateforme
- Vocabulaire et définitions
- Évolution depuis la logique câblée vers les réseaux industriels
- Problématiques liées aux différences de culture monde informatique / monde industriel
- Risques, notions de sureté et environnement de sécurité : le grand écart entre l'informatique et les réseaux industriels

CONVERGENCE DES NOTIONS ENTRE RÉSEAUX INDUSTRIELS ET RÉSEAUX INFORMATIQUES

Présentation des réseaux industriels

- Connexions des éléments : automates, supervision, protocoles
- Langages de programmation
- Fonctions logiques

La sécurité liée à TCP/IP dans le monde industriel

- Revue des protocoles (IP/ICMP/TCP/UDP, etc.)
- Attaques réseau
- Attaques couche Application
- Problématique du sans-fil en environnement industriel

Présentation des composants

- Partie industrielle (vannes, boutons, capteur, etc.)
- Automates
- Supervision/IHM
- Protocoles industriels (série, IP)

Architecture et technologies des réseaux industriels

- Architecture
- Technologies utilisées
- Isolation des réseaux industriels

OUTILLAGE POUR LES RÉSEAUX INDUSTRIELS

Le Python industriel

Fonctions de base en programmation permettant d'utiliser et lancer quelques commandes avec une bibliothèque python réalisée pour un protocole industriel.

PROBLÈMES DE SÉCURITÉ DES RÉSEAUX INDUSTRIELS

- Sécurité des protocoles industriels
- Faiblesses des automates (services ouverts, authentification, mots de passe en dur, etc.)
- Vulnérabilités des logiciels de supervision
- Faiblesses des couches réseau
- IHM et sécurité
- Sécurité des systèmes d'exploitation
- Sécurité des architectures

FOCUS SÉCURITÉ SCADA : BUZZ OU RÉALITÉ

- Exemples médiatiques
- Veille technologique dans le domaine industriel

RETOURS D'EXPÉRIENCES

Les audits et tests d'intrusion en milieu industriel

- Malware
- Intrusions externes, intrusions internes
- Audits

Un exemple concret : le cas Stuxnet

- Réalité des attaques
- Description de l'attaque

SOLUTIONS POUR SÉCURISER LES RÉSEAUX INDUSTRIELS

- Défense en profondeur
- Cloisonnement réseau
- Multi niveaux
- Politiques d'accès distants, de mots de passe, etc.
- Journalisation
- Sauvegarde
- Authentification effective
- Contrôles d'accès

ÉVALUATION
L'évaluation est réalisée tout au long de la formation, sous la forme d'exercices ou de mises en situation.

ATTESTATION
Certificat attestant le suivi et la validation des acquis de la formation labellisée SecNumedu-FC par l'ANSSI.

Référent handicap : marie.moin@epita.fr

Siège Social : 14-16 rue Voltaire 94270 le Kremlin Bicêtre - Campus EPITA
RCS Créteil 809 748 635 - Déclaration d'activité N° 11 94 08975 94