EduGroupe
Accompagner pour réussir

Cybersécurité des systèmes industriels

Référence : **SECINDUS** Durée : **5 jours (35 heures)** Certification : **Aucune**

Connaissances préalables

- 1-Bonne connaissance générale en informatique et en sécurité des systèmes d'information
- 2-Pour les profils automaticiens, la connaissance des fondamentaux de la cybersécurité est essntielle
- 3-Aucune connaissance des systèmes industriels n'est nécessaire

Profil des stagiaires

- 1-Responsables sécurité, sureté, cybersécurité, sécurité industrielle
- 2-RSSI
- 3-Automaticiens
- 4-Consultants en sécurité
- 5-Auditeurs en sécurité

Objectifs

- Aborder la cybersécurité des systèmes industriels par une approche pragmatique et pratique
- Développer un plan de sécurisation des systèmes informatiques industriels
- Pouvoir auditer les SI industriels
- Initier la préparation de plans de réponse à incident sur les systèmes industriels

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-Formateur expert Management de la sécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Introduction à la cybersécurité des systèmes industriels

- Vocabulaire
- Familles de SI industriels
- Bestiaire des équipements
- Particularismes de gestion des SI industriels

2. Architectures des SI industriels

- Architecture ISA95
- Approches de l'ISA/IEC 62443
- Spécificité des systèmes de sureté
- Accès partenaires
- Réalité du terrain

3. Protocoles, applications sécurisations possibles

- Grandes familles de protocole industriels
- Exemple de ModBus
- Exemple d'OPC
- Possibilité de détection et filtrage sur les flux industriels

4. Incidents représentatifs et évolutions

- Principaux incidents SSI ICS publics
- Cadre des SIV LPM
- Industrial IOTs et le cloud industriel

5. Référentiels sur la sécurité des systèmes d'information industriels

- Guides ANSSI
- Normes IEC 62443 (ISA 99) : IEC 62443-2-1, IEC 62443-3-3
- NIST SP800-82, NERC CIP, ISO 27019, etc

6. Sécurisation des SI industriels

- Organisation
- Appréciation des risques
- Cartographie et inventaire
- Intégration et recette de sécurité
- Maintien en condition de sécurité
- Surveillance

7. Réponse à incident sur un système industriel

- Premières réactions
- Détection et marqueur de compromission
- Analyse forensique d'artefacts industriel
- Préparer sa réponse à incident

8. Exercices

- Audit technique : Analyse de traces réseaux, Exploitation de vulnérabilités du protocole Modbus/TCP
- Sécurité organisationnelle et architecturale du réseau industriel : Architecture sécurisée, Détermination des zones et conduites, Points sensibles, Sécurisation d'architecture, Détermination des niveaux de classification ANSSI, Analyse basée sur le guide ANSSI relatif aux réseaux industriels
- Réponse à incident : Recherche de compromission du système sur capture réseau, Analyse des projets de processus industriel

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.