Formation « Cybersécurité des systèmes industriels »

Réf : SECUINDUS

Les systèmes industriels sont maintenant informatisés et connectés. Longtemps isolés, ils sont maintenant dans le cœur de cible des attaques informatiques. Généralement, trop peu d'automaticiens ont une expérience significative de l'état de l'art de la sécurité informatique, et trop peu d'experts en cybersécurité ont une bonne connaissance du monde de l'informatique industrielle. La présente formation s'efforce de proposer un état des enjeux, des méthodes et des moyens de sécurisation, et de la gestion d'incident.

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

Durée & horaires

- 4 jours soit 28 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Responsables sécurité, sureté, cybersécurité, sécurité industrielle
- RSSI
- Automaticiens
- Consultants en sécurité
- Auditeurs en sécurité

Pré-requis

- Bonne connaissance générale en informatique et en sécurité des systèmes d'information, par exemple une certification SECUCYBER d'HS2 ou CISSP d'(ISC)2.
- Pour les profils automaticiens, le suivi de la formation ESSCYBER d'HS2 est indispensable
- Aucune connaissance des systèmes industriels n'est nécessaire.

Méthode pédagogique

- Cours magistral
- Démonstrations
- Exercices de mise en œuvre
- Travaux pratiques

Supports

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais

- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUINDUS par HS2.**

Programme

Introduction à la cybersécurité des systèmes industriels
- Vocabulaire
- Familles de SI industriels
- Bestiaire des équipements
- Particularismes de gestion des SI industriels

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

Protocoles, applications sécurisations possibles
- Grandes familles de protocole industriels
- Exemple de ModBus
- Exemple d'OPC
- Possibilité de détection et filtrage sur les flux industriels

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

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

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

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

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