G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Programme de formation

Cybersécurité des systèmes industriels

But de la formation

- 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

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.

Type de public

- Responsables sécurité, sûreté, cyber sécurité, sécurité industrielle,
- RSSI
- Automaticiens,
- Auditeurs en sécurité,
- Consultants en sécurité.

Moyens pédagogiques

- 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

Sanction de la formation

- 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 par HS2.
- Formation délivrée en partenariat avec HS2

G-echo
6 Avenue de la Gare - C24
31380 Garidech
+33.6.03.62.14.40
contact@g-echo.fr

Méthodes pédagogiques

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

Durée

28 heures (4 jours).

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