

Gouvernance et Juridique

SCADA - Introduction à la sécurité des systèmes industriels

1 jour (7h00) | ★★★★★ 4,6/5 | SEMI-SCA | Évaluation qualitative de fin de stage |
Formation délivrée en présentiel ou distanciel ⁽¹⁾

Formations Informatique › Cybersécurité › Gouvernance et Juridique



À l'issue de ce stage vous serez capable de :

- Connaître le métier et les problématiques
- Dialoguer avec les automaticiens
- Connaître et comprendre les normes et standards de sécurité propres au monde industriel
- Auditer un système SCADA
- Développer une politique de cybersécurité.

Niveau requis

Avoir de bonnes connaissances générales en informatique.

Public concerné

Auditeurs, responsables de sécurité, DSI, managers, automaticiens, consultants, architectes réseaux et systèmes ICS/SCADA, administrateurs réseaux et systèmes ICS/SCADA ou toute autre personne en contact avec ces systèmes.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence élargée par demi-journée par les stagiaires et le formateur.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Programme

Introduction aux systèmes de supervision et de contrôle industriel (SCADA)

- Panorama de la cybersécurité industrielle
- Simulation d'attaques physiques
- Les menaces susceptibles d'affecter les systèmes industriels et les infrastructures informatiques de l'industrie
- Les référentiels sur la sécurité des systèmes d'information industriels
- Qu'est-ce que l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ? Quel est son rôle ?
- Secteurs d'activités cibles, typologie et population cible
- Les types d'architectures des systèmes SCADA
- "Threat modeling"

Composants et architectures réseaux des systèmes SCADA

- Les composants hardware et software : architectures et fonctionnalités des systèmes ICS/SCADA
- Les automates programmables industriels (PLC) et les terminaux distants (RTU)
- Les différents flux de communication dans les systèmes SCADA
- Les protocoles de communication temps réel
- PLC (Contrôleurs Logiques Programmables)

La sécurité des systèmes SCADA

- La problématique de sécurité dans les systèmes SCADA
- Introduction à Shodan et mise en situation par rapport à l'exposition des ICS
- Les méthodes de classification
- Les menaces et vulnérabilités, les intrusions connues, les attaques APT (menaces persistantes avancées) et les retours sur expérience
- Les cyberattaques ciblées sur les systèmes et infrastructures informatiques industriels
- Simulation d'un test d'intrusion sur les infrastructures ICS/SCADA
- Les scénarios d'attaques réelles sur les systèmes SCADA
 - Stuxnet
 - Flame
- L'analyse des attaques
 - Construction de l'arbre d'attaque de Stuxnet
- Simulation d'une cyberattaque sur les systèmes informatiques ICS/SCADA
- Les techniques d'authentification et les méthodes de chiffrement
 - Leurs apports
 - Leur mise en place
- Protéger l'ensemble de la chaîne industrielle et les postes opérationnels
- Bien sécuriser les accès et les postes à distance
- Garantir la disponibilité du réseau

Travaux pratiques

- Analyse du risque
- Sécurisation d'architectures ICS/SCADA

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques

- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)