Gouvernance

SCADA - Introduction à la sécurité des systèmes industriels

1 jour (7h00) | ★★★★½ 4,6/5 | SEMI-SCA | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 21/06/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

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

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains 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

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

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 émargée par demi-journée par les stagiaires et le formateur.

Programme

Les composants et les architectures des systèmes SCADA

- Les différents composants des systèmes industriels (systèmes de contrôle, bus, boucle de régulation...)
- Les composants hardwares et softwares des systèmes SCADA
- Les RTU (Unités Terminales Distantes)
- Les PLC (Contrôleurs Logiques Programmables)
- Les différents flux de communication entre tous les composants
- Les protocoles de communication temps réel

Introduction aux systèmes de supervision et de contrôle industriel

- Les attentes des nouveaux systèmes industriels
- La convergence de l'OT et de l'IT
- L'architecture des environnements de supervision et des outils de contrôle
- Les protocoles et flux entre les automates et les systèmes de supervision modernes

Les enjeux de la sécurité des systèmes SCADA

- Quelques chiffres
- Panorama de la cybersécurité
- Les spécificités de la cybersécurité industrielle
- Les profils des attaquants et leurs objectifs
- Les grandes familles d'attaque (spoofing, sniffing, forging...)
- Les référentiels sur la sécurité des systèmes d'information industriels
- Les normes de la sécurité industrielle (IEC 62443, ISO 27019, IEC 61508 et 61511, NIST 800-82)
- Qu'est-ce que l'ANSSI et quel est son rôle ?
- Les secteurs d'activités cibles, typologies et populations cibles
- Le "Threat modeling" en fonction des générations et équipements des systèmes SCADA

La sécurité des systèmes SCADA

- L'exposition publique des ICS : exemple avec Shodan, Censys, Zoomeye...
- L'exposition des ICS dans les réseaux privés

- Les méthodes de classification
- Les menaces et les vulnérabilités
- Les attaques APT (menaces persistantes avancées)
- Les attaques réelles sur les systèmes SCADA et retours d'expérience
  - Stuxnet, Duqu, Flame et Gauss
  - BlackEnergy
  - APT33
- Construction de l'arbre d'attaque de Stuxnet
- Les techniques d'authentification et les méthodes de chiffrement :
  - Leurs apports
  - Leurs mises 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

Exemples de travaux pratiques (à titre indicatif)

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

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d'accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.