SCADA INTRODUCTION À LA SÉCURITÉ DES SYSTÈMES INDUSTRIELS

Public	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.
Durée	1 journée - 7 heures
Pré-requis	Avoir de bonnes connaissances générales en informatique.
Objectifs	Reconnaître le métier et les problématiques Dialoguer avec les automaticiens Identifier et décrire les normes et standards de sécurité propres au monde industriel Développer une politique de cybersécurité.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (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. 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 Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1. LES COMPOSANTS ET LES ARCHITECTURES DES SYSTÈMES SCADA

- Les différents composants des systèmes industriels (systèmes de contrôle, bus, boucles 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

2. 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 quatre générations de SCADA

3. 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'attaques (spoofing, sniffing, forging...)
- Les référentiels sur la sécurité des systèmes d'information industriels
- Les normes de la sécurité industrielle (IEC 62443, ISO 270xx, 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

4. LA SÉCURITÉ DES SYSTÈMES SCADA

- L'exposition publique des ICS (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
- 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
- Outils et technologies de sécurité (Firewall, IPS, IDS, SIEM...)
- Sécuriser les accès et les postes à distance (Sans-fil, VPN, 4G...)
- Garantir la disponibilité du réseau
- Gestion de crise et plan de continuité d'activité

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation