CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS SCADA

Public	Auditeurs, responsables de sécurité, automaticiens, architectes et administrateurs réseaux et systèmes ICS / SCADA (Industrial Control Systems / Supervisory Control And Data Acquisition).
Durée	3 jours - 21 heures
Pré-requis	Avoir de bonnes connaissances générales en informatique et en sécurité des systèmes d'information.
Objectifs	Décrire le métier et les problématiques Dialoguer avec les automaticiens Identifier et expliquer les normes et standards propres au monde industriel Auditer un système SCADA 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.

TOUR D'HORIZON DES SYSTÈMES INDUSTRIELS

- Les enjeux d'un système d'information
- Spécificités et contraintes opérationnelles
- Architecture des systèmes SCADA
- Les familles et générations d'ICS
- Les types d'équipement et exemples d'architectures
- Les architectures par secteurs d'activité
- Les attentes des nouveaux systèmes industriels
- Les principaux protocoles industriels

ENJEUX DE LA SÉCURITÉ D'UNE INFRASTRUCTURE INDUSTRIELLE

- La convergence de l'OT et de l'IT
- 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
- Prise de conscience de l'importance de la sécurité des SI industriels au sein de l'Etat et des entreprises : les différents aspects
- Les référentiels sur la sécurité des sytèmes d'information industriels
- Les normes de la sécurité industrielle : IEC 62443, ISO 27019, IEC 61508 et 61511, NIST 800-82
- Le "Threat Modeling" en fonction des générations et des équipements des systèmes SCADA
- Qu'est-ce que l'ANSSI et quel est son rôle ?

NORMES

- Panorama des normes et guides de la sécurité industrielle
- Les normes de sécurité des SI de gestion ISO 270xx
- Les normes de la sécurité industrielle IEC 61508 et 61511
- La norme de sécurité du NIST 800-82
- La convergence vers la norme de sécurité IEC 62443
- Les guides de l'ANSSI
- Maîtriser la SSI pour les systèmes industriels
- Méthode de classification et mesures principales
- Cas pratique
- Mesures détaillées

DÉTERMINATION DES NIVEAUX DE CLASSIFICATION PAR L'ANSSI

- Analyse basée sur le guide ANSSI relatif aux réseaux industriels

RISQUES ET MENACES

- Les attaques réelles sur les systèmes SCADA et retours d'expérience :
- Stuxnet, Duqu, Flame et Gauss
- Triton
- BlackEnergy, Dragonfly et Energetic Bear
- Night Dragon
- APT33
- Les autres attaques sur des ICS
- Les facteurs de risque
- Les grands risques et familles de vulnérabilités
- Les menaces APT (Advanced Persistent Threat)
- Les postures de sécurité modernes des systèmes ICS

VULNÉRABILITÉS INTRINSÈQUES DES ICS

- Les vulnérabilités : Réseau, Systèmes, Applicatives
- Analyse avancée de la sécurité des PLC

EVALUER LA SÉCURITÉ DE SES INSTALLATIONS

- Réunir les éléments-clefs d'un diagnostic préalable
- Tests à prévoir pour des installations locales et/ou distribuées
- Outillage nécessaire pour l'audit
- Failles les plus couramment rencontrées
- Les plans d'actions types à appliquer et les outils requis

ACCÈS DISTANTS

- Les liaisons RTC
- Les points d'accès VPN
- Les boîtiers de télétransmission sans-fil et 4G
- La sécurité des liaisons sans-fil (Wi-Fi, liaisons radio)
- Les problèmes spécifiques aux automates et IHM exposés sur Internet

POSTURES DÉFENSIVES DE PROTECTION DES ICS

- Définir une politique de sécurité
- Mener une évaluation des risques
- Les objets principaux de la sécurisation technique : L'authentification, Le chiffrement, Le durcissement, La traçabilité, Les équipements dédiés, Le patch management
- La sécurisation fonctionnelle et l'utilisation des garde-fous
- Comment réagir à un incident de sécurité
- Les facteurs-clés de succès et bonnes pratiques
- L'intégration avec la sûreté industrielle
- La sécurité organisationnelle des réseaux industriels

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