+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 29/11/2023

S'inscrire

Formation ICS / SCADA Sécurité des Systèmes de Contrôle Industriels

5 jours (35 heures)

PRÉSENTATION

Les systèmes de contrôle industriel ICS communément appelés SCADA, contrôlent les infrastructures industrielles. La plupart des infrastructures critiques sont contrôlées par des systèmes ICS/SCADA : des réseaux électriques au traitement de l'eau, de l'industrie pharmaceutique, automobile et chimique aux transports. Cette formation répond à la nécessité pour les ingénieurs et les opérateurs de systèmes de contrôle de mieux comprendre le rôle important qu'ils jouent dans la cybersécurité. Cela commence par s'assurer qu'un système de contrôle est conçu avec une cybersécurité intégrée, et que la cybersécurité a le même niveau de sensibilité que la fiabilité du système tout au long du cycle de vie du système.

OBJECTIFS

- Connaître le métier et les problématiques
- Contrôler la surface d’attaque d’un système ICS/SCADA
- Connaître et comprendre les normes propres au monde industriel
- Sécuriser vos systèmes ICS/SCADA
- Développer une politique de cybersécurité

PUBLIC VISÉ

- Responsables/Expert sécurité
- Chefs de projets industriels

Pré-requis

- Bonne connaissance générale en informatique et en sécurité des systèmes d'information.
- Connaissances de base sur les systèmes industriels et les systèmes de contrôle ICS/SCADA

PROGRAMME DE NOTRE FORMATION reconversion cybersécurité : DEVSECOPS

Introduction à la cybersécurité des systèmes ICS/SCADA

- Surface d'attaque ICS
- Sources de menace et raisons de l'attaque
- Surface d'attaque et entrées
- Attaque Niveau 0 et 1
- Plateforme De contrôle des choses
- Exercice: Trouver des mots de passe dans les décharges EEPROM
- Purdue Niveau 0 et 1 Technologies & Communications
- Familles du protocole Fieldbus

ICS/SCADA & Système d’information

- Ethernet et TCP/IP
- Ethernet & TCP/IP Concepts
- Protocoles ICS sur TCP/IP
- Wireshark et ICS
- Attaques contre les réseaux: Enumérant Modbus TCP
- Surface d'attaque ICS
- Attaques contre les IHM et les interfaces Users
- Attaques contre les serveurs de contrôle
- Attaques contre les communications réseau
- Attaques sur les appareils distants

Sécurisation des systèmes ICS/SCADA

- Windows & Linux dans ICS
- Mises à jour et patching
- Processus et services Durcissement de la configuration
- Défense de point de terminaison
- Automatisation et audit
- Gestion des journaux, Bases de données et historiques

Sécurité organisationnelle du réseau industriel

- Architecture SCADA
- Détermination des zones et conduites
- Sécurisation d'architecture
- Détermination des niveaux de classification ANSSI

Exercices Pratiques

- Programmation d'un PLC, IHM
- L'architecture d'un SDC sécurisé
- Trouver des mots de passe dans les périphériques embarqués
- Explorer les protocoles de Fieldbus
- Forensic d'une attaque
- Contournant Auth avec SQL Injection
- Fuzzing de mot de passe
- Baselining avec PowerShell
- Configuration des pare-feu basés sur l'hôte
- Journaux d'événements Windows
- Trouver l'accès à distance

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.