

SCADA, la sécurité des systèmes industriels



PL-76 2 Jours (14 Heures)

Description

Ce cours vise à vous fournir les compétences techniques nécessaires pour comprendre les systèmes de contrôle industriel SCADA qui sont responsables de la gestion des infrastructures critiques de la société telles que les réseaux électriques, les usines de traitement de l'eau et les installations industrielles chimiques. À la fin du cours, vous serez capable d'identifier les menaces et les vulnérabilités de ces systèmes SCADA.

À qui s'adresse cette formation ?

Pour qui

RSSI, DSI, architectes, chefs de projets, administrateurs système et réseau.

Prérequis

- Connaissances de base en architectures Ethernet, TCP/IP et des processus industriels.

Les objectifs de la formation

- Appréhender les composants d'un système de supervision et de contrôle industriel (SCADA).
- Analyser les risques d'une architecture SCADA.
- Appréhender les menaces et les vulnérabilités.
- Identifier les mesures de protection.

Programme de la formation

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

- Panorama de la cybersécurité industrielle.
- Les référentiels sur la sécurité des systèmes d'informations industriels.
- L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).
- Historique des systèmes SCADA, définition et terminologie (SCADA, systèmes de contrôle, boucle de régulation).
- Secteurs d'activité cibles, typologie, population cible dans l'industrie française.
- Les types d'architectures de système SCADA.
- Les principes fonctionnels et domaines d'application de la supervision et de contrôle industriel.
- Les automates programmables industriels (PLC), les terminaux distants (RTU).

Composants et architectures réseaux des systèmes SCADA

- Les composants hardware : architecture et fonctionnalités.
- Les composants software : architectures et fonctionnalités.
- Automates, vannes, capteurs chimiques ou thermiques, système de commande et contrôle, IHM (Interface Homme Machine).
- Les flux de communication dans les systèmes SCADA.
- Les architectures réseaux par besoin fonctionnel.
- Les protocoles de communication temps réel, PLC.
- Les langages de programmation d'automatismes industriels.
- La conception d'un système de contrôle en réponse à un cahier des charges.

Introduction à la sécurité des systèmes SCADA

- La problématique de sécurité dans les systèmes SCADA.
- La cybersécurité des systèmes industriels, les méthodes de classification.
- Les menaces et vulnérabilités, les intrusions connues, les attaques APT (menaces persistantes avancées).
- Les scénarios d'attaques réelles sur les systèmes SCADA : STUXNET, FLAME.
- L'analyse des attaques : construction de l'arbre d'attaque de STUXNET.
- Authentification/chiffrement.

Analyse de risque et exigences de sécurité des systèmes SCADA

- La méthodologie d'analyse de risques.
- L'analyse de risques d'une architecture SCADA.
- L'identification et définition des exigences de sécurité.