Formation SCADA, la sécurité des systèmes industriels

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Les systèmes de contrôle industriel ICS, appelés SCADA, contrôlent les infrastructures critiques de la société (réseaux électriques, traitement de l'eau, industrie chimique...). A l'issue de ce cours, vous disposerez des éléments techniques pour appréhender les systèmes SCADA, les menaces et leurs vulnérabilités.

Référence	DAY
Durée	2 jours (14h)
Tarif	1 990 €HT
Repas	repas inclus

Objectifs

| 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

Public

| RSSI
| DSI
| architectes
| chefs de projets
| administrateurs système et réseau

Prérequis

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

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 1er au 2 juillet 2025
du 14 au 15 octobre 2025
du 16 au 17 décembre 2025

PARIS

du 24 au 25 juin 2025
du 7 au 8 octobre 2025
du 9 au 10 décembre 2025

VOIR TOUTES LES DATES

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'information 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 du 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 la définition des exigences de sécurité.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.