

Sécurité des systèmes industriels

Cours Synthèse de 1 jour

Réf : EGN - Prix 2022 : 890€ HT

Le prix pour les dates de sessions 2023 pourra être révisé

Les systèmes d'informatique industrielle SCADA contrôlent les infrastructures critiques comme les réseaux électriques, le traitement de l'eau... Ce stage vous apprendra les bases techniques des systèmes SCADA, les menaces et les vulnérabilités possibles ainsi que les actions à entreprendre pour améliorer la sécurité.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

- Appréhender les composants d'un système SCADA
- Analyser les risques d'une architecture SCADA
- Comprendre les menaces et les vulnérabilités de ces systèmes
- Identifier les mesures de protection

LE PROGRAMME

dernière mise à jour : 10/2018

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

- Panorama de la cybersécurité industrielle. Pourquoi un pirate informatique cible de plus en plus les systèmes SCADA ?
- Les menaces susceptibles d'affecter les systèmes industriels et les infrastructures informatiques de l'industrie.
- Quels sont les référentiels sur la sécurité des systèmes d'information industriels ?
- Qu'est-ce que l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) ? Quel est son rôle ?
- Secteurs d'activité cible, typologie, population cible dans l'industrie française.
- Les types d'architectures de système SCADA.

2) Composants et architectures réseaux des systèmes SCADA

- Les composants hardware et software : quelles sont les architectures et les fonctionnalités dans un système SCADA ?
- Que sont les automates programmables industriels (PLC) ? Les terminaux distants (RTU).
- Quels sont les différents flux de communication dans les systèmes SCADA ? Sont-ils sécurisés par défaut ?
- Les protocoles de communication temps réel, PLC (contrôleurs logiques programmables).

3) Introduction à la sécurité des systèmes SCADA

- La problématique de sécurité dans les systèmes SCADA. Les méthodes de classification.
- Les menaces et vulnérabilités, les intrusions connues, les attaques APT (menaces persistantes avancées).
- Les cyberattaques ciblées sur les systèmes et infrastructures informatiques industriels.
- Les scénarios d'attaques réelles sur les systèmes SCADA : STUXNET, FLAME.
- L'analyse des attaques : construction de l'arbre d'attaque de STUXNET.
- Les techniques d'authentification et les méthodes de chiffrement. Leurs apports, leur mise en place.

PARTICIPANTS

Toutes les personnes souhaitant apprendre les fondamentaux de la sécurité des SI.

PRÉREQUIS

Avoir suivi la formation "La sécurité dans le cyberspace".

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques... Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

- Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
- Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Protéger l'ensemble de la chaîne industrielle et les postes opérationnels.
- Bien sécuriser les accès et les postes à distance et garantir la disponibilité du réseau.

LES DATES

AIX-EN-PROVENCE

2023 : 31 mars, 23 juin, 29 sept.,
08 déc.

LYON

2023 : 09 févr., 12 mai, 04 août,
03 nov.

NANTES

2023 : 14 avr., 30 juin, 06 oct., 15
déc.

PARIS LA DÉFENSE

2022 : 02 déc.

TOULOUSE

2023 : 05 mai, 28 juil., 29 sept.,
08 déc.

2023 : 24 févr., 07 avr., 28 juil., 01
sept., 27 oct., 01 déc.

CLASSE A DISTANCE

2022 : 02 déc.

2023 : 24 févr., 07 avr., 28 juil., 01
sept., 27 oct., 01 déc.