Cours de synthèse de 1 jour(s)
Réf : EGN

Participants

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

Pré-requis

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

Prix 2019 : 980€ HT

Dates des sessions

AIX
21 juin 2019, 27 sep. 2019
20 déc. 2019

BORDEAUX
21 juin 2019, 27 sep. 2019
20 déc. 2019

LILLE
21 juin 2019, 27 sep. 2019
20 déc. 2019

LYON
22 mar. 2019, 21 juin 2019
27 sep. 2019, 20 déc. 2019

NANTES
27 mar. 2019, 21 juin 2019
27 sep. 2019, 20 déc. 2019

PARIS
29 mar. 2019, 24 juin 2019
30 sep. 2019, 20 déc. 2019

RENNES
21 juin 2019, 27 sep. 2019
20 déc. 2019

SOPHIA-ANTIPOLIS
21 juin 2019, 27 sep. 2019
20 déc. 2019

STRASBOURG
21 juin 2019, 27 sep. 2019
20 déc. 2019

TOULOUSE
21 juin 2019, 27 sep. 2019
20 déc. 2019

Modalités d'évaluation

L'objectif de cette formation étant essentiellement de fournir une synthèse des méthodes et technologies existantes, il n'est pas nécessaire d'avoir recours à une évaluation des acquis.

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

Sécurité des systèmes industriels

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 PEDAGOGIQUES

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

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.
- 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.

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.

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.

• A 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.