CODE
5510

GÉNIE INDUSTRIEL / AUTOMATISME - ARCHITECTURE DE COMMANDES

POSSIBLE EN INTRA

CYBERSÉCURITÉ INDUSTRIELLE AVANCÉE - SÉCURISER UN SYSTÈME INDUSTRIEL SELON NIS2

Face à l'entrée en vigueur de NIS2 et à la multiplication des cyberattaques visant les systèmes industriels, les organisations doivent renforcer la sécurité de leurs environnements OT et démontrer une gestion efficace des risques

0 € HT | **3 JOURS** (21 H.) | **NOUS CONSULTER** POUR LES DATES DE SESSION

COMPÉTENCE PRINCIPALE VISÉE

Mettre en œuvre une démarche de sécurisation d'un système industriel conforme aux exigences de NIS2

LES + DE LA FORMATION

75 % de la formation sont consacrés à la mise en pratique sur une plateforme industrielle réelle complète (automates, réseau et SCADA) afin d'appliquer immédiatement les mesures de cybersécurité OT conformes à NIS2

PUBLIC

- Techniciens et ingénieurs chargés de concevoir les architectures réseaux, d'assurer la sécurité des systèmes d'information et l'exploitation des équipements en réseau
- Informaticiens

PRÉREQUIS

- Connaissances techniques dans le domaine du contrôle-commande industriel

OBJECTIFS PÉDAGOGIQUES

- Comprendre le fonctionnement du système industriel et identifier les vulnérabilités principales
- Réduire la surface d'attaque et limiter la propagation
- Surveiller le système, détecter une anomalie et organiser la réponse à un incident

CONTENU

PARTIE 1 - OT (AUTOMATISME), CARTOGRAPHIE ET ANALYSE DES RISQUES

Objectif : Comprendre le fonctionnement du système industriel et identifier les vulnérabilités principales

Contenu :

- Rappel NIS2 appliqué à l'OT :
  - risques,
  - continuité,
  - détection,
  - incident,
  - preuves
- Fonctionnement d'une architecture OT :
  - capteurs,
  - actionneurs,
  - automates,
  - IHM,
  - supervision,
  - postes d'ingénierie,
  - chaîne de commande,
  - protocoles industriels
- Vulnérabilités classiques
  - Réseau plat,
  - mots de passe faibles,
  - accès maintenance mal contrôlé,
  - services inutiles,
  - protocoles peu sécurisés,
  - propagation de l'attaques dans la couche de pilotage,
  - basculement ou mode dégradé mal maîtrisé,
- Cartographie active et passive
- Vulnerability management

TRAVAUX PRATIQUES :

- Observation du fonctionnement normal
- Identification des équipements
- Capture simple des flux
- Identification des actifs, versions, ports et services
- Première liste de vulnérabilités ou faiblesses de configuration
- Construction d'une matrice actifs/flux/vulnérabilités
- Identification des principaux scénarios d'attaque

PARTIE 2 - SEGMENTER ET DURCIR L'ARCHITECTURE

Objectif : Réduire la surface d'attaque et limiter la propagation

Contenu :

- Principes de segmentation OT
- Séparation des zones
  - supervision,
  - métiers,
  - maintenance, etc.)
- VLAN, pare-feu industriel, diode, etc.
- Matrice des flux autorisés/interdits
- Durcissement

- automates,
- supervision,
- équipements réseau,
- postes d'ingénierie,
- sauvegarde/restauration,
- accès maintenance,

TRAVAUX PRATIQUES :

- Création d'une architecture segmentée
- Définition des règles de filtrage
- Test des flux autorisés et bloqués
- Durcissement de quelques équipements
- Comparaison avant/après

PARTIE 3 - DETECTER ET REAGIR

Objectif : Surveiller le système, détecter une anomalie et organiser la réponse à un incident

Contenu :

- Rôle d'une sonde OT passive
- Placement de la sonde
  - flux supervision,
  - flux métier, etc.
- Détection
  - nouvel équipement,
  - scan réseau,
  - flux interdit,
  - écriture anormale vers automate,
  - comportement anormal d'un sous-système
- Réponse à incident
  - qualification,
  - isolement,
  - maintien du service,
  - fonctionnement en mode dégradé,
  - restauration

TRAVAUX PRATIQUES :

- Détecter l'anomalie
- Identifier l'équipement ou le flux concerné
- Isoler la zone compromise
- Vérifier le maintien du service
- Compléter une fiche incident
- Proposer des mesures correctives
- Mettre à jour la cartographie et les règles

ÉQUIPE PÉDAGOGIQUE

Enseignants/chercheurs INSA Lyon spécialistes du milieu industriel et experts en cybersécurité IT et OT

MOYENS ET MÉTHODES PÉDAGOGIQUES

Cours - Travaux Pratiques - Exercices - Etude de cas et Echanges avec des experts du domaine Un support de cours sera remis à chacun des participants.

PROCHAINE SESSION

L'ouverture de la session est conditionnée par un nombre minimum de participants. Nous consulter pour d'autres dates.

ÉVALUATION ET RÉSULTATS

Évaluation des acquis de la formation

Evaluation des acquis des apprenants par auto-examen. 95.4% des apprenants ont acquis la compétence principale visée. (sur 215 apprenants évalués sur cette thématique depuis 2020)

Évaluation de la satisfaction des participants en fin de formation (Niveau 1 KIRKPATRICK)

4.4 par les participants. (sur 244 participants ayant suivi une formation dans la thématique depuis 2020)

RENSEIGNEMENTS ET INSCRIPTION
Tel : +33 (0)4 72 43 83 93
Fax : +33 (0)4 72 44 34 24
mail : formation@insavalor.fr
Préinscription sur formation.insavalor.fr

Accueil des personnes en situation de handicap nécessitant un besoin spécifique d'accompagnement : nous contacter à l'inscription. Nos locaux sont accessibles aux personnes à mobilité réduite.

Actualisée le 08/07/2026