



NOUVEAUTE

CYBERSÉCURITÉ INDUSTRIELLE POUR PUBLIC D'INFORMATIENS : IDENTIFICATION DES VULNÉRABILITÉS ET RENFORCEMENT DES SYSTÈMES EXISTANTS

COMPÉTENCE PRINCIPALE VISÉE

Appréhender les vulnérabilités des systèmes existants et mettre en œuvre une méthodologie de renforcement du niveau de cybersécurité d'un système de contrôle-commande industriel

OBJECTIFS PÉDAGOGIQUES

- Appréhender les enjeux de la cybersécurité dans la production industrielle (manufacturing, production et distribution d'énergie, traitement d'eau, etc.)
- Identifier les menaces sur les systèmes de contrôle-commande industriels
- Évaluer, vérifier et valider le niveau de sécurité
- Mettre en œuvre des solutions afin d'éviter les intrusions extérieures, déjouer les cyberattaques
- Fournir un socle de connaissances aux informaticiens afin de leur permettre de travailler en collaboration avec les automaticiens

PUBLIC

INFORMATIENS : techniciens et ingénieurs chargés de concevoir les architectures réseaux, d'assurer la sécurité des systèmes d'information et l'exploitation des équipements en réseau

PRÉREQUIS

- Connaissances techniques dans le domaine de l'informatique des systèmes d'information : SSI

CONTENU

Cette formation est à destination de 2 publics, le profil « automaticien » et le profil « informaticien »

La formation permet à un public d'automaticiens et d'informaticiens :

- d'appréhender les apports et enjeux de chaque métiers sur des projets relatifs à la cybersécurité d'installations industrielles.
- d'acquérir les bases de la cybersécurité des systèmes industriels,
- ainsi qu'un vocabulaire commun leur permettant de travailler ensemble

La première journée est spécifique à chaque profil.

Les stagiaires sont ensuite réunis en un seul groupe afin d'initier des échanges et des collaborations.

Module IT (1 Jour)

L'objectif essentiel de ce module est de donner les connaissances nécessaires pour appréhender la sécurité des systèmes de contrôle-commande industriels à un public d'informaticiens.

½ journée de cours théoriques - ½ journée de TP sur plateforme

- Définitions des différents types de systèmes de contrôle-commande industriels
- Principaux organes d'un système de contrôle-commande industriel : Automate Programmable Industriel (API/PLC), capteurs / actionneurs, SCADA, Historian, poste d'ingénierie, MES, RTU, IED, etc.
- Les langages de programmation d'un PLC
- Les protocoles et bus de terrain
- Les architectures réseaux classiques d'un système industriel :
- Introduction à la Sûreté De Fonctionnement (SDF)
- Panorama des normes et standards

SESSIONS

Villeurbanne : Du 14/03/23 à 09h00 au 16/03/23 à 17h00

L'ouverture de la session est conditionnée par un nombre minimum de participants.

DURÉE

3 jours (21 heures)

FRAIS INDIVIDUELS

Coût de la formation (repas inclus) : 2160 € H.T.

ÉQUIPE PÉDAGOGIQUE

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

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

Module principal (2 jours)

1 ½ journée cours théorique – ½ journée de TP

- Enjeux de la cybersécurité industrielle
- État des lieux et historique
- Dualité Sûreté De Fonctionnement (SDF) et cybersécurité industrielle
- Exemples d'incidents sur les systèmes industriels
- Les vulnérabilités et vecteurs d'attaques classiques
- Panorama des normes et standards
- En France, la Loi de Programmation Militaire (LPM)
- Le projet de cybersécurité du système industriel
- Les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI)
- Etat des lieux des équipements et produits de cybersécurité : apports et limites
- Exercices et travaux pratiques

MÉTHODE PÉDAGOGIQUE

Cours - Travaux Pratiques - Exercices - Etude de cas et Echanges avec des experts publics et privés du domaine

ÉVALUATION ET RÉSULTATS

Évaluation des acquis de la formation

Evaluation des acquis des apprenants réalisée en fin de formation

Évaluation de la formation

Evaluation du ressenti des participants en fin de formation (Niveau 1 KIRKPATRICK)

Résultats de l'évaluation

Le niveau d'appréciation globale de la thématique est évalué à 4.4/5 par les participants