



CYBERSÉCURITÉ INDUSTRIELLE POUR PUBLIC D'AUTOMATICIENS : 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 automaticiens afin de leur permettre de travailler en collaboration avec les informaticiens

PUBLIC

- Automaticiens
- Techniciens et ingénieurs chargés d'installer, programmer, régler ou dépanner des équipements automatisés, machines-outils et robots industriels

PRÉREQUIS

- Connaissances techniques dans le domaine du contrôle-commande industriel

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 OT (1 jour)

L'objectif essentiel de ce module est de donner les connaissances nécessaires pour appréhender la sécurité de la sécurité des systèmes d'information (SSI) à un public d'automaticiens.

Des TP sont réalisés tout au long de la journée

- Définitions de la cybersécurité/SSI et principaux concepts
- Enjeux de la cybersécurité/SSI
- Catégories d'attaques (DDOS, Advanced Persistent Threat (APT), Vers, MITM, spoofing, ingénierie sociale, détournement de sessions, etc.) et modes opératoires
- Exemples d'attaques
- Grands principes de déploiement d'un projet cybersécurité
- Connaître les bonnes pratiques
- Panorama des normes et standards
- Introduction à la Cryptographie

SESSIONS

VILLEURBANNE : du 08/07/2025 au 10/07/2025

Frais pédagogiques individuels : 2 380 € H.T.

* Repas inclus

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

DURÉE

3 jours (21 heures)

ÉQUIPE PÉDAGOGIQUE

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


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

MOYENS ET MÉTHODE PÉDAGOGIQUE

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

Un support de cours sera remis à chacun des participants.

ÉVALUATION ET RÉSULTATS

Évaluation des acquis de la formation

Évaluation des acquis des apprenants réalisée en fin de formation par un questionnaire ouvert contextualisé.

Taux de réussite

91.6% des apprenants ont acquis la compétence principale visée

Résultat obtenu pour 200 participants évalués ayant suivi une formation dans la thématique sur les 5 dernières années

Évaluation de la satisfaction

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

Résultats de l'évaluation

Le niveau de satisfaction globale est évalué à 4.3/5 par les participants.

Évaluations réalisées auprès des 276 participants ayant suivi une formation dans la thématique sur les 5 dernières années

