INSA VALOR

SÉCURITÉ NUMÉRIQUE

98,8% de clients satisfaits*

* enquête réalisée auprès de nos clients en septembre 2024

CODE : 7400

CYBERSÉCURITÉ INDUSTRIELLE POUR PUBLIC D'INFORMATICIENS : VULNÉRABILITÉS & SÉCURISATION DES SYSTÈMES

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

- Informaticiens
- 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 différentes 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.

SESSIONS

VILLEURBANNE : du 07/07/2026 au 09/07/2026
Frais pédagogiques individuels : 2 415 € 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 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

- 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

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

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

Taux de réussite

90.5% des apprenants ont acquis la compétence principale visée

Résultat obtenu pour 155 participants évalués ayant suivi une formation dans la thématique sur les 5 dernières années

Évaluation de la satisfaction

Evaluation 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.

Evaluations réalisées auprès des 192 participants ayant suivi une formation dans la thématique sur les 5 dernières années

Actualisée le 29/09/2025