

POSSIBLE EN INTRA

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

Les systèmes industriels sont de plus en plus exposés aux cyberattaques. Cette formation aide automaticiens et informaticiens à identifier les vulnérabilités, acquérir un langage commun et renforcer la sécurité des installations critiques.

**2 415 € HT****3 JOURS** (21 H.)**NOUS CONSULTER  
POUR LES DATES DE SESSION**

### 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

### LES + DE LA FORMATION

Approche collaborative entre automaticiens et informaticiens. Alternance théorie/TP et études de cas. Mise en pratique des normes, bonnes pratiques et recommandations ANSSI pour anticiper, détecter et contrer efficacement les cyberattaques industrielles.



#### 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



#### 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

## 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

### 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

#### ÉQUIPE PÉDAGOGIQUE

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

#### MOYENS ET MÉTHODES PÉDAGOGIQUES

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.

**97,2%**  
de clients  
satisfaits\*

\* enquête réalisée auprès  
de nos clients en  
septembre 2025

## 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

Évaluation des acquis des apprenants par auto-examen. 94.3% des apprenants ont acquis la compétence principale visée. (sur 177 apprenants évalués sur cette thématique depuis 2020)

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

4.3 par les participants. (sur 199 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](mailto:formation@insavalor.fr)

Préinscription sur [formation.insavalor.fr](http://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 29/09/2025