NUMERIQUE RESPONSABLE

CYBERSÉCURITÉ INDUSTRIELLE : IDENTIFICATION DES VULNÉRABILITÉS ET RENFORCEMENT DES SYSTÈMES EXISTANTS

1 / 2

opéré par INSA VALOR

Renforcer le niveau de cybersécurité d'un système de contrôle-commande industriel.

Villeurbanne
100 % présentiel

3 jours
21 heures

07 - 09 juillet 2026
INTRA possible

2 415 € H.T. / pers.
INTER entreprise

Cette formation est à destination de 2 publics :
- un profil « automaticien »
- un profil « informaticien ».

La première journée est spécifique à chaque profil.
Les deux journées suivantes sont communes et permettent d'initier des échanges et des collaborations.

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 CIBLE

La formation s'adresse à un public d'automaticiens et d'informaticiens qui souhaitent :
- appréhender les apports et enjeux de chaque métier sur des projets relatifs à la cybersécurité d'installations industrielles,
- acquérir un vocabulaire commun leur permettant de travailler ensemble

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

>> Informaticiens et 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

AUTOMATICIENS - Connaissances techniques dans le domaine du contrôle-commande industriel.

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

CONTENU

La première journée est spécifique à chaque profil.

1) Automaticiens

Acquérir les connaissances nécessaires pour appréhender la sécurité des systèmes d'information (SSI). 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

2) Informaticiens
[½ journée théorique + ½ journée de TP sur plateforme]

Acquérir les connaissances nécessaires pour appréhender la sécurité des systèmes de contrôle-commande industriels.
- 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

NUMERIQUE RESPONSABLE

CYBERSÉCURITÉ INDUSTRIELLE : IDENTIFICATION DES VULNÉRABILITÉS ET RENFORCEMENT DES SYSTÈMES EXISTANTS

2 / 2

opéré par INSA VALOR

Renforcer le niveau de cybersécurité d'un système de contrôle-commande industriel.

Villeurbanne
100 % présentiel

3 jours
21 heures

07 - 09 juillet 2026
INTRA possible

2 415 € H.T. / pers.
INTER entreprise

Cette formation est à destination de 2 publics :
- un profil « automaticien »
- un profil « informaticien ».

La première journée est spécifique à chaque profil.
Les deux journées suivantes sont communes et permettent d'initier des échanges et des collaborations.

CONTENU (suite)

Les deux journées suivantes réunissent les deux publics.

JOURS 2 & 3 – Commun
[1 ½ journée 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)
- État des lieux des équipements et produits de cybersécurité : apports et limites
- Exercices et travaux pratiques

FORMATEURS

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

MÉTHODES PÉDAGOGIQUES

- Apports théoriques
- Travaux Pratiques
- Exercices
- Étude de cas
- Échanges avec des experts publics et privés du domaine.
- Un support de cours sera remis à chacun des participants.

ÉVALUATION ET RÉSULTATS

- Évaluation des acquis des apprenants réalisée en lors de la formation par des exercices, des travaux pratiques et un questionnaire ouvert contextualisé.
- 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 du ressenti des participants en fin de formation (Niveau 1 KIRKPATRICK)
- Le niveau de satisfaction globale est évalué à 4.3/5 par les participants.
- Évaluations réalisées auprès des 192 participants ayant suivi une formation dans la thématique sur les 5 dernières années.

ACCESSIBILITÉ

Cette formation est handi-accessible.
Contactez-nous !