



ACTION DE FORMATION INTER-ENTREPRISE CYBERSECURITE INDUSTRIELLE (POUR PROFIL AUTOMATICIEN / OT) : VULNERABILITES ET RENFORCEMENT DES SYSTEMES EXISTANTS

RÉF. CYBR-02

DURÉE : 3,00 jours - 21,00 h.

PUBLIC VISÉ (FONCTIONS & SERVICES)

Automaticiens, techniciens et ingénieurs chargés d'installer, programmer, régler ou dépanner des équipements automatisés, machines-outils et robots industriels issus des services : Automatisme, Electricité, Instrumentation (AEI), Maintenance industrielle, Informatique industrielle, Systèmes

PRÉREQUIS

- Connaissances techniques dans le domaine contrôle-commande industriel

OBJECTIFS DE L'ACTION DE FORMATION

- Comprendre 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.

À l'issue de la formation, les stagiaires seront capables d'appréhender les vulnérabilités de systèmes existants et de mettre en œuvre une méthodologie de renforcement du niveau de cybersécurité d'un système de contrôle-commande industriel.

MÉTHODE PÉDAGOGIQUE

Pédagogie active basée sur des échanges avec des experts publics et privés du domaine, la session alternera :

- Exposés généraux théoriques,
- Exercices pratiques et travaux pratiques sur plateforme (d'une durée d'environ 1 jour).

INTERVENANT

Experts du domaine, spécialistes du milieu industriel et experts publics et privés en cybersécurité OT et IT

COMMENTAIRES COMPLEMENTAIRES EVENTUELS

Nous vous invitons à prendre contact en cas de participation de personnes en situation de handicap.

DOCUMENTATION STAGIAIRE

Une documentation sera remise à chaque participant.

SPC Formation

204 route de Vourles - Parc Inopolis - 69230 Saint-Genis-Laval - France

Tél : +33 4 72 67 12 34 - E-mail : formation@groupe-spc.com

Web : www.groupe-spc.com/fr/formation

RCS Lyon B 391 572 567 - NAF 8559A - Id. TVA FR 86 391 572 567

SARL au capital de 10.000 euros

Organisme de formation enregistré sous le n° 82 69 04028 69 auprès du préfet de la Région Auvergne-Rhône-Alpes.

Membre les acteurs de la compétence (Fédération de la Formation Professionnelle)



les acteurs de
la compétence

v.12 - 2025



CONTENU DE LA FORMATION

I - la sécurité des systèmes des systèmes d'information (SSI)

- 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

TRAVAUX PRATIQUES SUR PLATEFORME

II - Cybersécurité des systèmes d'information industriels

- 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

ÉVALUATION

-Une évaluation globale destinée à mesurer l'atteinte des objectifs pédagogiques sera réalisée en fin de stage, au moyen de fiches appropriées fournies par SPC, ou à défaut par le service formation du Client.

-Une évaluation des acquis est réalisée tout au long de la formation à partir d'une pédagogie active et participative, à l'aide de QCM, d'exercices pratiques ou de mises en situation.