Cybersécurité

Cybersécurité des systèmes industriels
Mise en œuvre

Référence FORMCYBINDUS

3 jours
(21 h)

Présentiel

70% cours
30% travaux pratiques

Spécialiste

Conception
Mise en œuvre
Exploitation
Maintenance

Prix, dates, lieux et inscriptions
Scannez ou cliquez sur le QR code

Objectif
• Assurer la protection des installations industrielles communiquantes.

Compétences visées
• Identifier les besoins de sécurité dans les architectures industrielles.
• Mettre en œuvre des solutions de protection.

Personnes concernées
• Professionnels de la sécurité des systèmes d'informations (RSSI, DSI, auditeur, etc.).
• Professionnels des systèmes de contrôle-commande industriels (maintenance, production, intégrateur, automaticien).

Prérequis
Connaître les réseaux et bus de communication et plus particulièrement le réseau Ethernet.

SecNumedu
Formation continue
ANSSI

Cette formation entre dans le cadre de la transformation digitale de votre activité.
Voir page A9

Vidéo

FORMCYBINDUS : Formation Cybersécurité des systèmes industriels - Mise en œuvre

Formation basée sur le référentiel ANSSI "Guide pour une formation sur la cybersécurité des systèmes industriels".

Contenu de la formation

Cybersécurité

Rappels et introduction sur les systèmes industriels :
• définitions, les différents types de systèmes industriels,
• composition d'un système industriel,
• langages de programmation en automatisme,
• protocoles et bus de terrain industriels,
• architectures réseaux classiques des systèmes industriels.

Rappels et introduction sur la cybersécurité :
• définitions de la cybersécurité,
• enjeux de la cybersécurité,
• catégories d'attaques et modes opératoires,
• grands principes de déploiement d'un projet cybersécurité,
• introduction aux bonnes pratiques.

Cybersécurité industrielle :
• sûreté de fonctionnement et cybersécurité,
• exemples d'incidents sur les systèmes industriels,
• vulnérabilités et vecteurs d'attaques classiques,
• panorama des normes et standards,
• en France, la Loi de Programmation Militaire,
• recommandations de l'ANSSI : aspects organisationnels et techniques, méthode de classification, détails des principales mesures.

Exercices pratiques :
• mise en œuvre communication VPN (profil automaticien),
• prise en main programmation API (profil informaticien),
• inventaire et cartographie des équipements,
• classification et analyse de risque,
• identification des vulnérabilités,
• mise en œuvre firewall applicatif.

Matériel d'application
• Architecture réseau composée de :
- automates,
- switchs, routeurs, firewall,
- PC, etc.

Validation de la formation
• Questionnaire sur les connaissances théoriques.
• Mise en situation selon cahiers des charges.

Documents fournis
• Supports de cours accessibles sur votre espace client (campus-digital.schneider-electric.fr).

Nota : Le niveau "spécialiste" de cette formation est à considérer en tant que domaine d'approfondissement destiné à un public d'automaticiens, il ne participe nullement à la formation de spécialiste de la cybersécurité.