

Public et prérequis

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

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

Les objectifs

Assurer la protection des installations industrielles communicantes
Identifier les besoins de sécurité dans les architectures industrielles
Mettre en oeuvre des solutions de protection

Les méthodes pédagogiques et d'encadrement

La formation est animée par des formateurs experts, validés par nos équipes pédagogiques et disposant de 5 à 10 années d'expérience dans leur domaine de compétences.

Validation et certification

Attestation de formation

Outils pédagogiques

Architecture réseau composée de :
automates
switchs, routeurs, firewall
PC ...

Contenu de la formation

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

Définition 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

RÉFÉRENCE

INFO0003

CENTRES DE FORMATION

Beauvais

DURÉE DE LA FORMATION

3 jours / 21 heures

ACCUEIL PSH

Formation ouverte aux personnes en situation de handicap. Moyens de compensation à étudier avec le référent handicap du centre concerné.

PARTENAIRE

SCHNEIDER-ELECTRIC



Les + Promeo

- 60 ans d'existence
- Une communauté de 3 100 alternantes
- 24 000 stagiaires formés par an
- 3 500 entreprises qui nous font confiance
- Un accompagnement personnalisé et un contact dédié
- L'expertise professionnelle de tous nos formateurs
- La diversité des diplômes sous accréditation par des partenaires de renom
- Une pédagogie active
- Des infrastructures technologiques et un environnement stimulant

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 oeuvre 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 oeuvre firewall applicatif

Modalité d'évaluation

Questionnaire sur les connaissances théoriques.

Mise en situation selon le cahier des charges.