



La cybersécurité industrielle de l'organisationnel à l'opérationnel

Sécuriser les systèmes industriels face aux cybermenaces de demain

DURÉE

2 jours (14 heures)

EFFECTIF

Jusqu'à 12 personnes

TARIF ADHÉRENT

1 320 € HT

TARIF NON ADHÉRENT

1 590 € HT

OBJECTIFS DE LA FORMATION

- Appréhender le vocabulaire de la cybersécurité industrielle et les normes associées
- Identifier les menaces auxquelles les systèmes d'information industriels sont exposés
- Connaître les architectures et les moyens de protection
- Construire une analyse globale en se basant sur des exemples concrets
- Apporter des bonnes pratiques dans le quotidien des industriels
- Fournir quelques recommandations contractuelles pour garantir le système d'information au long terme

PUBLIC VISÉ & PRÉREQUIS

PUBLIC VISÉ

Ingénieurs, Techniciens expérimentés de bureaux d'études, Responsables, Professionnels impliqués dans la gestion des systèmes d'information industriels

PRÉREQUIS

Dimensionnée pour un public disposant d'un niveau minimum de type Bac+2

PROGRAMME DE LA FORMATION

JOUR 1	Cybersécurité des systèmes industriels : bases et menaces
9h - 12h30	Module 1 : Les bases de la cybersécurité industrielle - Fondements de la cybersécurité industrielle, initiation aux architectures - Histoire & vocabulaire - Les normes et l'organisation française et européenne - Les architectures (IT vs OT) et la data
12h30 - 13h30	Déjeuner
13h30 - 14h30	Module 2 : Atelier Décrypter les menaces d'un SI industriel
14h30 - 17h	Module 3 : Menaces ciblant les systèmes d'informations industriels Veille et outillage nécessaire
JOUR 2	Gouvernance et impacts de la cybersécurité industrielle
9h - 12h30	Module 4 : L'organisation de la cybersécurité - Définir les différentes missions et responsabilités - Le rôle des métiers - Les critères DICT - Gestion des accès
12h30 - 13h30	Déjeuner

13h30 - 14h30	Module 5 : Atelier • Identifier les impacts d'une attaque
14h30 - 17h	Module 6 : Impacts et recommandations • Les coûts de la cybersécurité • Exemples d'attaques • Investissement vs perte • Savoir intégrer contractuellement les exigences cybersécurité

MOYENS PÉDAGOGIQUES & MODALITÉS D'ÉVALUATION

MOYENS PÉDAGOGIQUES

- Exposés illustrés et séance de questions/réponses directement durant la formation
- Support de cours
- Déjeuner(s) – rencontre pris en commun avec l'intervenant
- Séance de questions/réponses directement durant la formation

MODALITÉS D'ÉVALUATION

- Questionnaire préalable à la formation
- Questionnaire d'évaluation et de satisfaction

FORMATEURS & CONTACTS

INTERVENANTS : KAIZEN SOLUTIONS

Experts en systèmes d'information industriels et cybersécurité

CONTACT FORMATIONS

Frédéric CABAS - Responsable Formations
frederic.cabas@polesmartpower.fr
06 12 25 21 26