CYBERSECURITE

Les règles de base en matière de cybersécurité

Objectif : Maitriser les bonnes pratiques pour diminuer le risque d'attaque cybersécurité

Public concerné : Artisans, ETI, PME et majors du secteur.

Prérequis : Savoir lire, écrire et parler le français, notions en informatique.

Durée : 1 jour en continu (7 heures).

Pédagogie : La progression pédagogique s'appuie sur des exposés théoriques, l'expérience des participants, et des exercices d'application
Échanges d'expériences entre stagiaires.

Cette formation est réalisée par des formateurs ingénieurs en cybersécurité

Évaluation des acquis : QCM d'évaluation

Outils pédagogiques : Salle de cours équipée d'un vidéoprojecteur, écran.

Accessibilité : En cas de restriction médicale ou autres restrictions, un plan de compensation individuel pourra être mis en œuvre en amont de l'inscription, sur demande et sur validation de la faisabilité technique.

Dotation du stagiaire : Documents, vêtements et EPI nécessaires **voir la liste détaillée page 3**.

Document de fin de formation : Attestation de formation.

Lieu : CACHAN (94), Dardilly (69). Pour tout autre lieu sur demande et sous condition.

Ce contenu ci-après peut être personnalisé à vos besoins dans le cadre d'une session intra entreprise

ASSOCIATION POUR LA FORMATION PROFESSIONNELLE CONTINUE DANS L'EQUIPEMENT ELECTRIQUE
Siège social : 30, av. du Président Wilson - 94234 CACHAN Cedex - Tél. : 01 49 08 03 03
Association loi de 1901 - Siret : 784 244 253 00067 - Code NAF 8559A - N° TVA Intracom. FR 02 784 244 253
Déclaration d'activité enregistrée sous le n° 11940646394 auprès du Préfet de Région d'Île-de-France

CONTENU DU STAGE

1 – Historique et définitions (1h)

- Qu'est-ce que la cybersécurité
- Identifier les enjeux de la cybersécurité

2 – Les différents types d'attaque (1h)

- Distinguer les risques auxquels peuvent être confrontés votre société

3 – Analyse et gestion des risques cyber (1h)

- Panorama des méthodologies d'analyse et de gestion des risques cyber
- Les référentiels associés : ISO 27005 et EBIOS Risk Manager
- Les grandes étapes d'une démarche d'analyse de risques

4 – La prévention des risques (1h30)

- Se protéger des menaces
- Eviter les risques et limiter les conséquences d'une cyberattaque
- Les différents moyens de protection
- Être prudent avec le nomadisme

5 – Gouvernance et SMSI (1h)

- Les principes de gouvernance de la sécurité de l'information
- Le Système de Management de la Sécurité de l'Information (SMSI)
- Les référentiels ISO 27001 et ISO 27002

6 – Procédure en cas d'attaque (1h30)

- Définir un plan d'action efficace en cas de cyberattaque.

DOCUMENTS À FOURNIR POUR L'INSCRIPTION

- Bulletin d'inscription.

DOCUMENTS QUE DOIT POSSÉDER LE STAGIAIRE POUR SUIVRE CETTE INFORMATION

- Néant

VÊTEMENTS ET EPI QUE DOIT POSSÉDER LE STAGIAIRE POUR SUIVRE CETTE INFORMATION

- Néant

ASSOCIATION POUR LA FORMATION PROFESSIONNELLE CONTINUE DANS L'EQUIPEMENT ELECTRIQUE
Siège social : 30, av. du Président Wilson - 94234 CACHAN Cedex - Tél. : 01 49 08 03 03
Association loi de 1901 - Siret : 784 244 253 00067 - Code NAF 8559A - N° TVA Intracom. FR 02 784 244 253
Déclaration d'activité enregistrée sous le n° 11940646394 auprès du Préfet de Région d'Île-de-France