Quels objectifs ?

Identifier les principales menaces et vulnérabilités en cybersécurité ;

Appliquer les bonnes pratiques de sécurité informatique ;

Réagir de manière appropriée en cas d'incident de cybersécurité ;

Comprendre les enjeux réglementaires et organisationnels liés à la cybersécurité.

Contenu de la formation :

Prévention des risques :
→ Identifier les principales menaces et comprendre l'importance de protéger les actifs de l'entreprise.

Les bonnes pratiques :
→ Mettre en place des politiques claires et appliquer les règles essentielles de sécurité.

Gestion des incidents :
→ Réagir efficacement à un incident, gérer la crise et organiser la reprise.

Conformité et réglementation :
→ Respecter les obligations légales et normatives en matière de cybersécurité..

Culture de la sécurité :
→ Sensibiliser les collaborateurs et encourager des comportements responsables.

Protection des données :
→ Sécuriser les informations sensibles et prévenir les accès non autorisés.

Évaluation des risques :
→ Analyser les menaces propres à l'entreprise et mettre en place des mesures adaptées.

Technologies de sécurité :
→ Connaître les outils disponibles et savoir les utiliser efficacement.

Communication/collaboration :
→ Favoriser le dialogue interne et la coopération entre services.

Veille technologique.

Protéger sa croissance, se protéger des menaces cyber

Durée : 1 jour

Heures : 7 heures

Dates : 25/06/2026
OU 16/11/2026
OU 15/12/2026

Pour qui ? Dirigeants - Tous collaborateurs d'entreprise TPE, PME et ETI.

Pré-requis : Aucun niveau de connaissance préalable n'est requis.

Profil du formateur : Manager Audit et IT.

Nombre de participants : Entre 6 et 15 personnes.

Format : Présentiel - INTER - INTRA.

Programme et inscription

€ Coût = 850 € HT