MSI09

P&P
Training & Consulting

Sensibilisation à la cybersécurité

FRANCE - INTERNATIONAL
1 JOUR - 7 HEURES
PRESENTIEL ET DISTANCIEL
INTER - INTRA

+33 6 28 84 89 32
contact@p2tc.fr
www.p2tc.fr

Sommaire

Les points clés

Sensibilisation à la cybersécurité

La formation sur les bonnes pratiques d'utilisation des ressources du système d'information est conçue pour sensibiliser les professionnels aux risques liés à l'utilisation des outils numériques, que ce soit sur site, en mobilité ou en télétravail.

Grâce à de nombreux exemples concrets, cette formation met en lumière les bonnes pratiques essentielles pour limiter les risques d'erreur ou de malveillance. Vous apprendrez à adopter des comportements sécurisés pour protéger les données et les systèmes, tout en tenant compte des spécificités de votre environnement de travail, qu'il soit sédentaire ou à distance.

En suivant cette formation, vous serez mieux préparé à faire face aux menaces potentielles et à garantir une utilisation responsable et sécurisée des ressources informatiques de votre organisation.

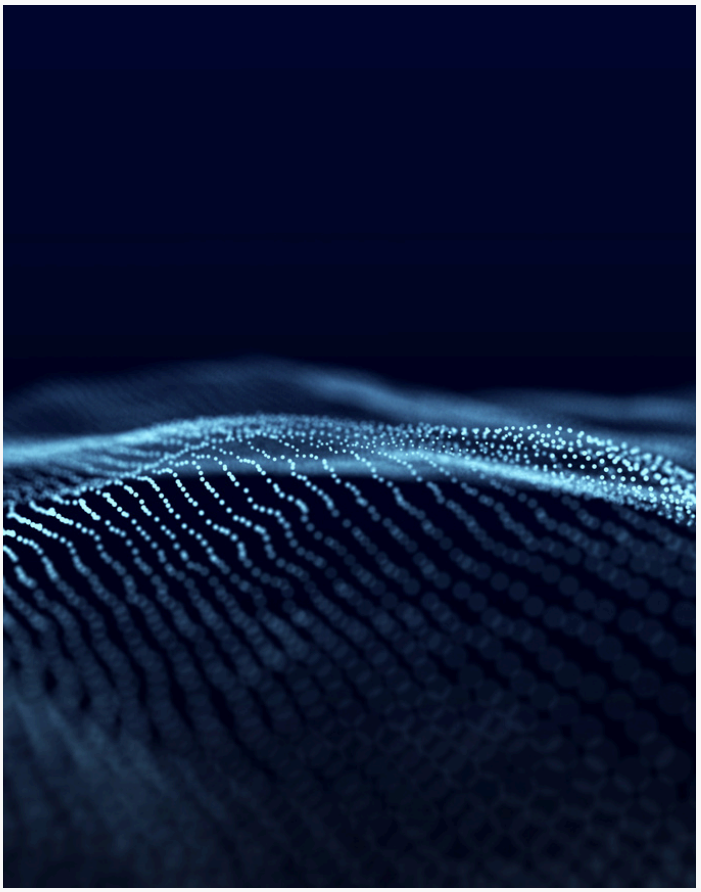
LES OBJECTIFS

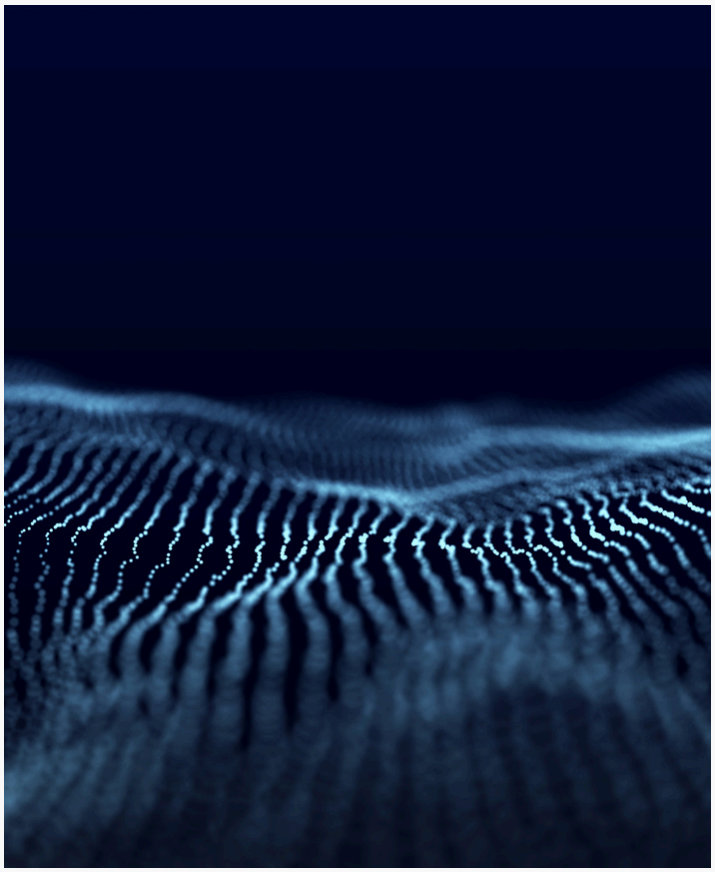
À la fin de cette formation, les participants seront capables de :

Identifier et évaluer les menaces numériques.

Adopter les bonnes pratiques pour le travail en ligne.

Comprendre les obligations légales en cybersécurité.





Renforcer la sécurité des systèmes d'information.
Protéger les données sensibles selon les besoins métiers.

Limiter les risques juridiques et opérationnels. de l'IA par la Propriété intellectuelle.

LES PRÉREQUIS

Aucun prérequis n'est nécessaire pour cette formation, elle est accessible à toute personne souhaitant se former.

LES PARTICIPANTS

P2TC réuni dans cette formation différents acteurs :

Tous les salariés d'une entreprise

LES MATÉRIELS PÉDAGOGIQUES

01

Documents écrits détaillés
Des guides pratiques sur les risques des systèmes d'information, adaptés aux environnements sédentaires, nomades et télétravail.

02

Connaissance des participants
Un test d'évaluation initial pour identifier les niveaux de sensibilisation et un test final pour valider l'assimilation des bonnes pratiques en matière de sécurité informatique.

03

Exercices pratiques et études de cas
Des exercices interactifs et des scénarios réels pour identifier les menaces, évaluer les risques et mettre en place des comportements responsables face aux situations courantes.

04

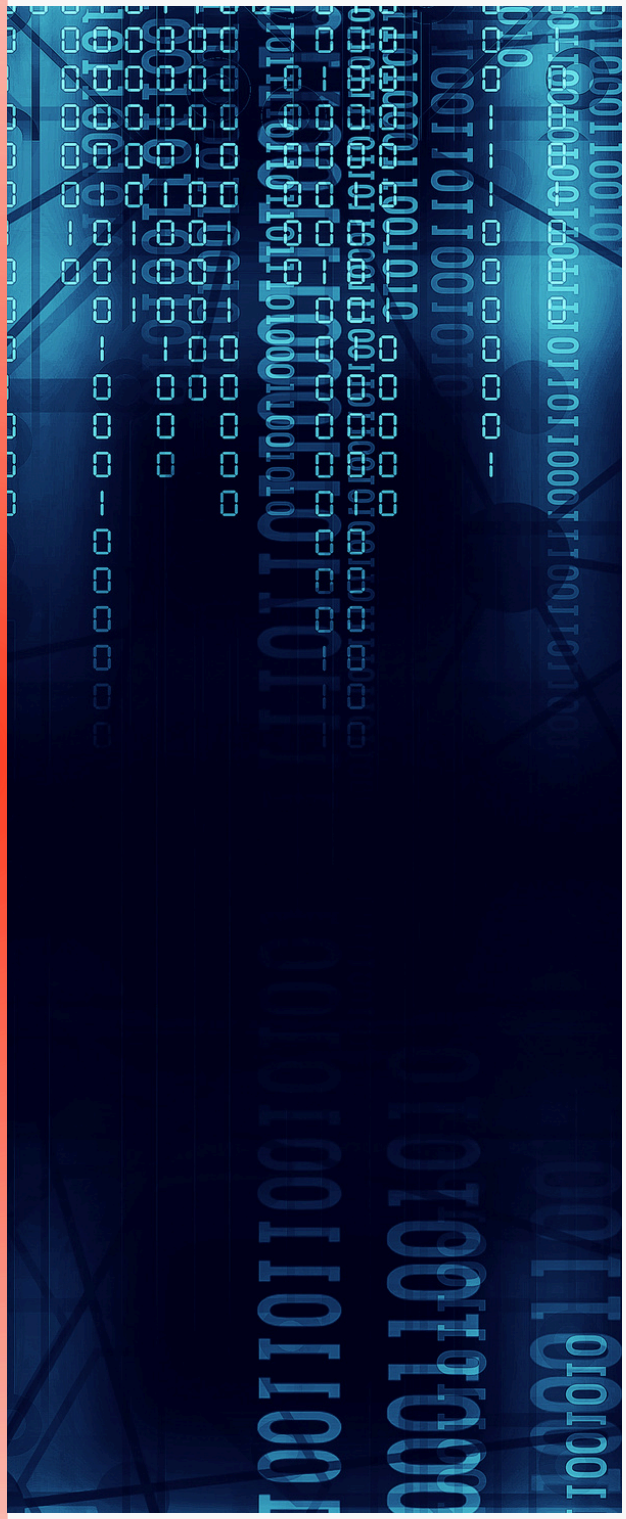
Études de cas et discussions de groupe
Des cas concrets sur les menaces comme le phishing, l'ingénierie sociale et les malwares, suivis de discussions pour partager des retours d'expérience et élaborer des solutions adaptées.

05

Evaluation et certification
Un questionnaire final et des mises en situation pour valider les acquis, avec la délivrance d'un certificat de sensibilisation à la sécurité des systèmes d'information.

LE PROGRAMME

EN 1 JOUR



Introduction

Préjugés, périmètres, valeurs à protéger, et menaces principales.

Responsabilités et organisation

Rôles clés : direction, DSI, RSSI, DPO, utilisateurs.

Risques et menaces

Vols, malwares, phishing, espionnage, réseaux sociaux.

Bonnes pratiques

Comportements adaptés sur site, à l'extérieur et pour les supports sensibles.

Utilisation des ressources SI

Installation, identification, sauvegarde, anonymisation, et VPN.

Conclusion

Synthèse des pratiques et engagements.

POUR ALLER PLUS LOIN :

MSI07 : Introduction à l'utilisation de ChatGPT
MSI08 : Maitriser les aspects juridiques et éthiques de l'intelligence artificielle