

PROGRAMME DE FORMATION EN PRÉSENTIEL ET DISTANCIEL

CYBERSÉCURITÉ - POUR LES PROS

OBJECTIFS PÉDAGOGIQUES

Apprendre à intégrer le concept de "security by design"
Aider les informaticiens en leur faisant adopter une approche préventive
Identifier les risques en prévenant et reconnaissant les types d'attaque
Déterminer le "stack technologique" du système d'information
Sécuriser les éléments du système d'information (accès, navigation, données, appareils),

Adopter des réflexes de vigilance
Contribuer activement à la résilience de l'entreprise face aux cybermenaces
Comprendre le darkweb
Comprendre les risques liés à l'IA

Nos équipes s'engagent à vous rappeler sous 24 à 72 heures

Public concerné

Les informaticiens

Pré-requis

Maîtriser l'architecture du système d'information de l'entreprise

Durée de la formation

En distanciel

4 heures

En présentiel

1/2 journée

La durée vous sera confirmée après étude de vos besoins.

Prix de la formation

En distanciel

Nous consulter

En présentiel intra

À partir de 1000€ ht la 1/2 journée

Lieu de la formation

Dans vos locaux ou à distance

Moyens et méthodes pédagogiques

Explications, démonstrations, exercices, vérification des acquis

Profil du(des) formateur(s)

Plusieurs années d'expérience dans l'enseignement et dans la production.

Modalités d'évaluation

Questionnaire d'évaluation en fin de session

Moyens techniques

Un ordinateur par personne. Vidéo projecteur. Connexion Internet

10/2025

► Analyse approfondie des différents types d'attaque

Le phishing: reconnaître un e-mail frauduleux, identifier les signaux d'alerte

Les mots de passe faibles: importance de mots de passe robustes et uniques
Détecter les faux ordres de virement et les arnaques par téléphone

Les logiciels malveillants (malwares, ransomwares) comment éviter les infections?

Les fuites de données: comment éviter de divulguer des informations sensibles?

► La navigation sécurisée sur Internet
Identifier les sites web sécurisés (HTTPS, certificats de sécurité)
Téléchargement de fichiers et installation de logiciels: les risques associés

Gérer ses informations personnelles sur les réseaux sociaux

► Sécuriser les accès et les données de l'entreprise

Les règles de base pour créer et gérer les mots de passe

L'importance de l'authentification à deux/multiples facteurs (2FA / MFA)

Autres concepts d'authentification (Comment protéger les informations des salariés)

► Sécurité des appareils et du télétravail

Pourquoi mettre à jour les logiciels et les architectures système de l'entreprise?

Risques liés aux connexions Wi-Fi publiques

Aider à la validation des outils de collaboration

Discussion et analyse des bonnes pratiques concernant les applications et logiciels installés sur les smartphones, tablettes et ordinateurs

► Sauvegarder des données
Protection contre les pertes accidentelles, ransomwares, et erreurs humaines

Les bonnes pratiques de la sauvegarde:

La règle du 3-2-1: 3 copies des données, 2 supports différents, 1 copie hors site

Fréquence des sauvegardes et automatisation

Reconnaître les tentatives de fraude et d'escroquerie

Escroqueries en ligne: Faux ordres de virement, arnaques par téléphone

Fuite de données: Comment éviter de divulguer des informations sensibles?

► Comprendre le Dark Web

Différences avec le Web visible et le Deep Web

À quoi sert-il? Usages légitimes et illégaux

Les dangers du Dark Web: vente de données volées, cybercriminalité

► Risques liés à l'IA

Attaques plus sophistiquées grâce à l'IA

Messages frauduleux (phishing et smishing)

Cyberattaques automatisées

Création de contenus falsifiés: deepfakes (voix, vidéos, images)

Risque sur les données personnelles
Ce que l'IA apprend sur nous via nos « prompts »

Manipulation des systèmes automatisés pour fausser les résultats (fraude, sabotage)

L'importance de l'éducation et de la vigilance face aux outils intelligents

► Réagir en cas d'incident

Les erreurs à éviter en cas de cyberattaque

Rédiger un reporting pour les décideurs de l'entreprise?

Analyser les erreurs en vue d'actions correctives?