IA : Protection des données et cybersécurité usages responsables du numérique

Public concerné

- > Tout public
- > Principalement le public avec un niveau intermédiaire

Durée

2 journées soit 14h de formation.

Pré-requis

Diagnostic préalable nécessaire : fiche individuelle d'analyse des besoins à compléter en amont

OBJECTIFS PROFESSIONNELS

- > Comprendre l'empreinte numérique et les risques liés aux données personnelles en ligne.
- > Identifier les menaces de cybersécurité courantes et le rôle de l'intelligence artificielle dans celles-ci.
- > Maîtriser les bonnes pratiques de sécurité de l'information au quotidien (mots de passe, hameçonnage, etc.).
- > Appréhender comment l'IA est utilisée par les cybercriminels et les cyberdéfenseurs.
- > Développer une culture de cybersécurité

PROGRAMME

Jour 1 : L'empreinte numérique, les données et les menaces cyber

Matin : Vie numérique et données

- > L'empreinte numérique : Qu'est-ce que c'est et comment se constitue-t-elle (navigation web, réseaux sociaux, applications mobiles).
- > La valeur de vos données : Pourquoi vos données personnelles sont-elles si convoitées (ciblage publicitaire, vente de données, ingénierie sociale).
- > Protection des données personnelles : Principes de base du RGPD (Règlement Général sur la Protection des Données) et de la CNIL.
- > Atelier pratique : Découvrir son empreinte numérique et les informations accessibles en ligne.

IA : Protection des données et cybersécurité usages responsables du numérique

PROGRAMME

Après-midi : Panorama des menaces cyber courantes

- > *Phishing, OSINT, ingénierie sociale : Comment ça marche, les signaux d'alerte et comment s'en protéger.*
- > *Malwares et ransomwares : Qu'est-ce que c'est, comment ils se propagent et leurs conséquences.*
- > *Fraude en ligne et usurpation d'identité avec l'IA : Reconnaître les tentatives et les réflexes à adopter.*
- > *Les mots de passe et l'authentification forte : Création de mots de passe robustes, gestionnaires de mots de passe, double authentification.*

Jour 2 : L'IA dans la cybersécurité et la cybercriminalité

Matin : L'IA : alliée et ennemie dans la cybersécurité

- > *L'IA pour les cybercriminels :*
 - ✳ *Génération de faux contenus (deepfakes) pour l'ingénierie sociale et la désinformation.*
 - ✳ *Phishing amélioré et personnalisation des attaques (spear phishing).*
 - ✳ *Automatisation des attaques (recherche de vulnérabilités, attaques par force brute).*
- > *L'IA pour les cybersécurité :*
 - ✳ *Détection avancée des menaces (malwares, intrusions).*
 - ✳ *Analyse comportementale des utilisateurs et des réseaux.*
 - ✳ *Automatisation de la réponse aux incidents de sécurité.*
 - ✳ *Prédiction des vulnérabilités et gestion des risques.*

Après-midi : Bonnes pratiques de sécurité au quotidien et usage responsable du numérique

- > *Naviguer en sécurité : Reconnaître les sites sécurisés, les risques du Wi-Fi public, l'importance des mises à jour logicielles.*
- > *Utilisation sécurisée des réseaux sociaux et de la messagerie : Paramètres de confidentialité, informations à ne pas partager.*
- > *Réagir face à une cyberattaque : Les premiers réflexes, qui contacter en interne.*
- > *L'importance d'une culture d'entreprise de cybersécurité : Le rôle de chacun.*
- > *Echanges et débat sur l'avenir de la cybersécurité et de l'intelligence artificielle*