

Objectifs

- Identifier les principales menaces pesant sur les données, les comptes et l'identité numérique dans un environnement professionnel.
- Comprendre les enjeux de sécurité, de confidentialité et de souveraineté liés à l'utilisation des outils d'intelligence artificielle.
- Identifier les informations pouvant ou non être transmises à un outil d'IA et appliquer les principes essentiels du RGPD et des règles de confidentialité.
- Découvrir et expérimenter des solutions d'IA orientées vers la protection des données, notamment Eurix et Lumo.
- Comprendre les orientations de l'État concernant l'utilisation d'une IA utile, humaine et souveraine dans les services publics, notamment à travers le plan « Notre IA ».
- Adopter des pratiques responsables et éthiques lors de l'utilisation professionnelle de l'IA : confidentialité, vérification des résultats, protection des données et maintien d'une validation humaine.
- Identifier les principales menaces visant l'identité numérique : hameçonnage, usurpation d'identité, compromission de comptes, vol d'identifiants, ingénierie sociale et fuite de données.
- Analyser des situations réelles et récentes de compromission afin d'identifier les facteurs de risque et les mesures de prévention adaptées.
- Comprendre, à travers des démonstrations encadrées de Kali Linux, les grandes familles d'outils susceptibles d'être utilisées par des attaquants, sans mise en œuvre offensive.
- Mettre en œuvre les bonnes pratiques permettant de réduire les risques liés à l'identité numérique, aux données professionnelles et à l'utilisation des services d'IA.
- Comprendre les principaux enjeux du **Règlement européen sur l'intelligence artificielle (AI Act)** et ses implications pour les organisations et les utilisateurs.
- Identifier les grandes catégories de risques prévues par l'AI Act et comprendre les principales obligations associées.
- Comprendre l'importance de la **maîtrise de l'IA (AI literacy)** prévue par l'article 4 et son application aux collaborateurs utilisant des systèmes d'IA.
- Adopter des pratiques d'utilisation de l'IA compatibles avec les exigences de sécurité, de transparence, de protection des données et de supervision humaine.

Prérequis : Aucun prérequis technique particulier n'est nécessaire. Une utilisation courante d'un ordinateur et d'un navigateur Internet est recommandée. Un ordinateur portable ou un ordinateur individuel est obligatoire pour chaque participant afin de réaliser les exercices, ateliers et mises en pratique proposés pendant la formation.

Public concerné : Tous les salariés d'une entreprise, quel que soit leur niveau de compétence en informatique.

THEMES TRAITES

Sécurité des données et identité numérique

- Les enjeux de la sécurité numérique dans les usages professionnels.
- Les données personnelles, professionnelles et confidentielles : identification et niveaux de sensibilité.
- Les principales menaces : phishing, ingénierie sociale, usurpation d'identité, compromission de comptes, logiciels malveillants et fuites de données.
- Les bonnes pratiques pour sécuriser ses comptes et son identité numérique.
- Mots de passe, gestionnaires de mots de passe, authentification multifacteur et récupération de compte.
- Reconnaître une tentative de fraude ou d'hameçonnage.

Atelier : analyser des situations de fraude et identifier les signaux d'alerte.

Atelier : réagir face à une compromission potentielle d'un compte.

Actualités et cas réels de cybersécurité

- Analyse d'exemples récents d'attaques et de compromissions.
- Étude de cas : accès illégitimes au système d'information de la Direction générale des Finances publiques en 2026.
- Identification des facteurs humains et techniques pouvant favoriser une compromission.
- Atelier : que faire lorsqu'un identifiant professionnel ou personnel est compromis ?

IA & Cybersécurité : Utiliser l'IA sans mettre vos données en danger

« Blended »

Mise en situation : reconnaître, signaler et limiter les conséquences d'un incident.

Intelligence artificielle : sécurité et confidentialité

- Comprendre les risques spécifiques liés à l'utilisation des IA génératives.
- Quelles informations ne faut-il pas transmettre à une IA ?
- Données personnelles, données sensibles, informations confidentielles et documents professionnels.
- Risques liés aux prompts, fichiers transmis, historiques de conversations et comptes utilisateurs.
- Vérification des réponses générées par l'IA et maintien d'une validation humaine.
- Utilisation éthique et responsable de l'IA.
- Principes essentiels du RGPD appliqués aux usages de l'IA.
- Respect des politiques internes et des directives de l'État.

Mise en situation : identifier les risques dans plusieurs prompts professionnels.

Atelier : anonymiser et reformuler une demande avant de la transmettre à une IA.

IA souveraine et solutions orientées confidentialité

- Définition et enjeux de la souveraineté numérique.
- Différence entre souveraineté, localisation des données, confidentialité et sécurité.
- Présentation d'Euria et de ses caractéristiques en matière de souveraineté et de confidentialité.
- Présentation de Lumo et de ses mécanismes orientés vers la confidentialité.

Mise en pratique sur Euria.

Mise en pratique sur Lumo.

Comparaison des fonctionnalités et des mécanismes de confidentialité.

Identification des informations pouvant être transmises à ces outils.

Atelier : choisir l'outil adapté selon la nature et la sensibilité des données.

L'IA dans les services publics

- Présentation du plan gouvernemental « Notre IA » pour les services publics.
- Enjeux de sécurisation et de maîtrise des usages de l'IA dans les administrations.
- Principes d'utilisation responsable de l'IA dans un contexte professionnel et administratif.
- Articulation entre efficacité, protection des données, sécurité, souveraineté et contrôle humain.

Étude de situations : quelles données transmettre à une IA dans le cadre d'une mission professionnelle ou de service public ?

Cadre réglementaire : l'AI Act

- Présentation du Règlement européen sur l'intelligence artificielle (AI Act).
- Pourquoi l'AI Act concerne les entreprises, les administrations et les utilisateurs de systèmes d'IA.
- Comprendre l'approche par niveaux de risque : pratiques interdites, systèmes à haut risque et obligations de transparence.
- Article 4 : la maîtrise de l'intelligence artificielle (AI literacy).
- Responsabilités des organisations vis-à-vis de la sensibilisation et de la montée en compétence des collaborateurs utilisant l'IA.
- Identifier les bonnes pratiques permettant d'encadrer les usages de l'IA dans une organisation.
- Articulation entre AI Act, RGPD, confidentialité, cybersécurité et politiques internes.
- Cas pratiques : analyser différents usages de l'IA et identifier les principaux enjeux réglementaires, éthiques et de sécurité.

Atelier : construire une check-list de bonnes pratiques pour une utilisation responsable et sécurisée de l'IA.

Démonstration encadrée : comprendre les outils utilisés par les attaquants

- Présentation de l'environnement Kali Linux dans une perspective de sensibilisation à la cybersécurité.
- Découverte des grandes familles d'outils utilisées dans les différentes phases d'une attaque.
- Reconnaissance et collecte d'informations.
- Analyse des services et de l'exposition d'un système.
- Analyse réseau.
- Recherche de vulnérabilités.
- Tests de mots de passe et d'authentification.
- Analyse de trafic et de fichiers.
- Présentation conceptuelle des phases d'exploitation et de post-exploitation.

- Démonstrations contrôlées sur environnement de test.
- Identification des mesures permettant de se protéger contre les techniques observées.
- Aucun accès à des systèmes tiers et aucune exploitation réelle.

Atelier final – Maîtriser son exposition numérique

- Analyse de son environnement numérique professionnel.
- Identification des principales données à protéger.

- Identification des comptes et services présentant un niveau de risque particulier.

Élaboration d'une check-list personnelle de sécurité numérique et d'utilisation responsable de l'IA.

Mise en situation finale.

Évaluation des acquis.

Moyens et méthodes pédagogiques

En Présentiel :

Salle de formation, vidéo projection, un support de formation sera communiqué à l'ensemble des participants résumant les aspects théoriques, les astuces et les points clés.

Les techniques d'animation seront actives et se baseront sur des cas concrets apportés par le formateur et/ou les participants. Elles alterneront les apports de connaissances, des exemples réels (situations rencontrées par les participants ou le formateur). Les participants travailleront sur des études de cas pratiques et des mises en situation.

En Distanciel :

Les sessions en distanciel se déroulent sur le logiciel Teams. Les classes virtuelles sont supervisées par notre équipe digitale, pour accompagner les participants.

Via le potentiel des outils du logiciel, la pédagogie sera active et ludique. Les participants pourront travailler par groupe ou sous-groupe dans des salles séparées. Les documents peuvent être partagés et interactifs pour une animation vivante et stimulante.

En Live :

Formation se déroulant dans nos locaux en présentiel, sur un écran Multifonctions de communications (MFC). Cette modalité est proposée afin de garder les bénéfices de la formation présentielle, tout en ayant un formateur à distance. Cela offre la possibilité également d'intégrer des participants à distance dans une formation en présentiel. La borne interactive permet un affichage dynamique et une meilleure fluidité et cohérence dans les échanges. C'est un outil complet qui permet au formateur d'offrir une formation présentielle enrichie d'interactivités digitales.

Blended :

Le Blended propose un approfondissement des objectifs de stage, d'une durée variable de 3 à 5 heures, selon la formation choisie. Il est accessible durant 30 jours. Des vidéos de mise en situation, de mise en pratique assurent la pérennité de ces acquis dans votre quotidien professionnel.

La formation en ligne est dispensée à travers une plateforme e-Learning, un espace numérique de travail et de suivi. Une équipe digitale assure le suivi des participants tout au long de la formation.

Un espace d'échange via le forum permet aux participants de garder le lien avec leur groupe et leur formateur.

Evaluations

Un questionnaire de préformation est transmis aux participants avant le démarrage de la formation. Il permet au formateur d'évaluer les besoins des participants et peut ainsi calibrer au mieux son intervention.

Des évaluations formatives jalonnent le parcours afin de mettre en évidence les points forts des apprenants et leurs axes d'amélioration. Ces évaluations permettent aux formateurs d'identifier les problématiques et d'affiner leurs approches pédagogiques.

IA & Cybersécurité : Utiliser l'IA sans mettre vos données en danger

« Blended »

Une évaluation de satisfaction à « chaud » évalue les différents axes « qualité » de la formation, puis une à « froid » 2 mois après la fin du parcours pour prendre en considération le retour d'expérience, l'adaptation au poste de travail, l'évolution et les besoins des participants.

Toutes nos évaluations seront transmises à travers un lien ou un QR code qui redirigera vers la plateforme « Drag'n Survey ». Celle-ci centralise les retours et nous permet une analyse opérationnelle des résultats et de nos axes d'amélioration à mettre en place. La qualité et la pertinence de nos formations reste notre priorité.

Intervenant :

Chargé de projet digital. Formateur de modules digitaux à distance. Diplômé d'un bachelor « Chef de projet digital ».

Modalités et délai d'accès :

Pour toute inscription, contactez nos conseillers qui vous accompagneront (conseil@sesame-formation.re) /02.62.22.02.02

Aucun délai n'est requis.

Durée : 7h

Lieu et date(s) actualisé(s) : cf site web : www.sesame-formation.re

Coût HT : Nous consulter.

Accessibilité : Nos salles, ainsi que celles de nos partenaires sont accessibles aux personnes en situation de handicap. Nos logiciels distanciels offrent également des outils qui permettent de répondre à vos besoins.

Pour toute demande, nous vous invitons à contacter notre référent Handicap.

Programme mis à jour en septembre 2026.