



PROGRAMME

Formation Cybersécurité et
Intelligence Artificielle

TECHNOLOGIES NUMÉRIQUES

SOFT SKILLS

MARQUE EMPLOYEUR

HANDICAP

PARCOURS CERTIFIANTS

PRÉVENTION

CENTRE

DE FORMATION PROFESSIONNELLE

depuis 2007

Qualiopi
processus certifié

Certification qualité délivrée au titre
de la catégorie «Actions de formation»

PARMI NOS THÉMATIQUES

Devictio
formations®

Informatique & Management

- Informatique / Bureautique
- PAO - 3D - Vidéo
- Web / E-Marketing
- Management / Communication
- Juridique / Comptabilité
- Commercial / Efficacité professionnelle
- Handicap
- QVCT / RPS
- Marque employeur
- Parcours certifiants

MAGNIS
FORMATION
by Devictio

Sécurité & Prévention

- AIPR
- SST (Sauveteur Secouriste du Travail) / MAC SST
- Habilitations électriques
- CACES
- Manipulation d'extincteurs
- Hygiène alimentaire
- Travail en hauteur
- CSE SSCT
- Geste & posture TMS
- Sécurité Incendie

PiXio
by Devictio

E-Learning & Développement personnel

- Langues étrangères
- Développement commercial DISC & WPMOT
- Développement personnel
- E-learning
- Marketing Entreprise
- Parcours en digital

DES FORMATIONS

QUALIFIANTES ET CERTIFIANTES



“ Tous nos formateurs sont des consultants et des professionnels **experts** dans leur domaine d'intervention [...] ”

VOUS ÊTES

Une entreprise et vous souhaitez développer les compétences de vos salariés ? Renforcer votre marque employeur ? Renforcer la prévention et la sécurité dans vos locaux ?

Un particulier (salarié ou demandeur d'emploi) et vous souhaitez acquérir ou renforcer vos compétences sur les outils informatiques, en soft skills ou en développement personnel ? Obtenir une certification professionnelle ?

NOS SOLUTIONS

Formation en groupe ou sur-mesure, en centre ou sur site. Présentiel, distanciel, e-learning, apprentissage mixte (blended learning). Nos stages comprennent des mises en situation et de nombreux travaux pratiques. Nos certifications professionnelles vous permettront de mettre en avant votre expertise.

NOS FORMATEURS

Nos formateurs sont à la fois professionnels et intervenants, ils vous font bénéficier de leur expérience professionnelle cumulée à leur compétence pédagogique. Quel que soit votre niveau, ils sauront vous écouter et vous accompagner pour vous aider à acquérir toutes les compétences nécessaires.

FAITES NOUS PART DE VOTRE PROJET

04 72 64 25 19

formation@devictio.fr

Formation Cybersécurité et Intelligence Artificielle



Référence : CECYB202

Nombre de stagiaires max : 5

Modalités d'inscription :

Les inscriptions sont possibles :

- **Jusqu'à 48 heures avant le début de la formation**, sous réserve des places disponibles, pour les financements en **autofinancement** ou **via le plan de développement des compétences de l'entreprise**.
- **Au plus tard 11 jours ouvrés avant le début de la session** pour toute inscription financée par le **Compte Personnel de Formation (CPF)**, conformément à la réglementation en vigueur.
- **Environ 4 semaines avant le début de la formation** pour les demandes de financement auprès d'un **OPCO** ou de **France Travail**, afin de permettre l'instruction du dossier.

Accessibilité aux personnes en situation de handicap :

Devictio s'engage à favoriser l'accès à ses formations aux personnes en situation de handicap. Pour étudier les possibilités d'adaptation de la formation à vos besoins, nous vous invitons à contacter notre référent handicap :

- 04 72 64 25 19
- formation@devictio.fr

Public visé :

- Responsables informatiques.
- Responsables SSI (RSSI).
- DSI.
- Chefs de projet informatique.
- Responsables métiers.
- Référents cybersécurité.
- Consultants.
- Administrateurs systèmes et réseaux.
- Dirigeants souhaitant intégrer l'Intelligence Artificielle de manière sécurisée.
- Toute personne souhaitant comprendre les enjeux de l'IA appliquée à la cybersécurité.

Objectifs :

- Comprendre le fonctionnement des principales intelligences artificielles génératives.
- Identifier les nouveaux risques cyber liés à l'utilisation de l'IA.
- Découvrir comment l'IA peut renforcer la cybersécurité.
- Adopter les bonnes pratiques d'utilisation des IA génératives en entreprise.
- Mettre en œuvre une politique d'utilisation responsable de l'IA.
- Connaître les obligations réglementaires relatives aux données utilisées par les IA.
- Être capable d'intégrer l'IA dans une stratégie globale de cybersécurité.

Compétences visées :

- Identifier les risques liés à l'utilisation des IA génératives.
- Sécuriser les usages professionnels de ChatGPT, Claude, Copilot, Gemini et autres assistants IA.
- Reconnaître les principales attaques exploitant l'Intelligence Artificielle.
- Utiliser l'IA pour renforcer la détection des menaces.
- Mettre en place des bonnes pratiques de gouvernance de l'IA.
- Sensibiliser les collaborateurs aux nouveaux risques numériques.
- Contribuer à une politique de cybersécurité intégrant les usages de l'IA.

Moyens techniques et pédagogiques :

Mises en situation par le biais d'exercices.

Répétitions des manipulations pour mémoriser l'utilisation des outils présentés.

Un ordinateur par personne.

Support de cours remis sur clé USB ou en format papier à la fin de la formation.

Modalités d'évaluation :

Évaluation pédagogique (orale et/ou écrite) effectuée à la fin de la formation afin d'attester l'acquisition de compétences. Exercice de synthèse.

Validation de la formation :

Attestation de fin de formation envoyée par mail.

Pré-requis :

- Utiliser régulièrement un ordinateur et les principaux outils numériques.
- Connaître les bases du fonctionnement d'une entreprise et de son système d'information.
- Aucune compétence en programmation n'est nécessaire.

- Une première sensibilisation à la cybersécurité constitue un plus mais n'est pas obligatoire.

Durée : 2 jour(s) / 14 heures

Points abordés :

Jour 1 – Comprendre les enjeux de l'IA appliquée à la cybersécurité

- Panorama de l'Intelligence Artificielle.
- Comprendre le fonctionnement des modèles de langage (LLM).
- Les IA génératives : ChatGPT, Claude, Copilot, Gemini, Mistral...
- Comment fonctionnent les modèles d'IA ?
- Données d'entraînement et confidentialité.
- Les hallucinations de l'IA.
- Protection des données sensibles.
- Quels risques pour les entreprises ?
- Fuite de données confidentielles.
- Prompt Injection.
- Vol de propriété intellectuelle.
- Deepfakes.
- Usurpation d'identité.
- Ingénierie sociale assistée par IA.
- Phishing généré automatiquement.
- Les obligations réglementaires :
 - RGPD.
 - AI Act européen.
 - NIS2.
- Études de cas réels.
- Analyse d'incidents récents.

Jour 2 – Utiliser l'IA comme levier de cybersécurité

- L'IA au service des équipes cybersécurité.
- Détection automatique des comportements anormaux.
- Analyse intelligente des journaux (logs).
- Threat Intelligence.
- Réponse assistée aux incidents.
- Automatisation des tâches répétitives.
- IA et SOC (Security Operations Center).
- Utiliser ChatGPT en toute sécurité.
- Sécuriser Microsoft Copilot.
- Sécuriser Claude en entreprise.

- Les règles de gouvernance des IA génératives.
- Élaborer une charte d'utilisation de l'IA.
- Construire une politique interne.
- Atelier pratique :
 - Création de prompts sécurisés.
 - Détection des risques liés à une requête IA.
 - Audit d'usages IA dans une entreprise.
 - Construction d'un plan d'action.
- Synthèse des bonnes pratiques.

Méthodes pédagogiques

- Alternance permanente entre théorie et pratique.
- Démonstrations en direct sur plusieurs IA génératives.
- Études de cas d'entreprises.
- Travaux de groupe.
- Ateliers pratiques.
- Mises en situation.
- Quiz interactifs.
- Support de cours numérique remis à chaque participant.

Moyens pédagogiques

- Salle informatique équipée ou salle de formation.
- Connexion Internet haut débit.
- Ordinateur par participant.
- Accès aux principaux outils d'IA.
- Supports numériques.
- Vidéoprojecteur.

Modalités d'évaluation

- Questionnaire de positionnement avant l'entrée en formation.
- Évaluations formatives durant les ateliers.
- Quiz de validation des connaissances.
- Mises en situation professionnelles.
- Questionnaire de satisfaction.
- Attestation individuelle de fin de formation.

Modalités d'accès

- Formation disponible en inter-entreprises à Lyon.
- Formation intra-entreprise partout en France.
- Possibilité de réalisation à distance.

- Inscription possible jusqu'à 48 heures avant le démarrage (hors dispositifs spécifiques).

Accessibilité

- Cette formation est accessible aux personnes en situation de handicap. Devictio étudie avec chaque participant les adaptations pédagogiques et matérielles nécessaires afin de garantir un accès équitable à la formation.

Sanction de la formation

- Attestation individuelle de fin de formation.
- Remise du support pédagogique.
- Évaluation des acquis.

NOS TARIFS

INTER dans nos locaux	1890 €* (945 €* / jour)
INTRA dans toute la France	sur devis

* Nos formations ne sont pas soumises à la TVA



FINANCEMENT



COMMENT FINANCER **SA FORMATION** ?

IL EXISTE PLUSIEURS DISPOSITIFS DE FINANCEMENT

- Compte Personnel de Formation (CPF)
- AIF (Pôle Emploi)
- FNE-Formation
- Fonds d'assurances formations (FAF)
- Contrats cadres
- Opérateurs de compétences (OPCO)
- Plan de Développement des compétences



CONTACTEZ NOUS !

04 72 64 25 19



magnis-formation.fr



pixio-formation.fr



devictio.fr

CENTRE

DE FORMATION PROFESSIONNELLE

📍 12 place Bir Hakeim - 69003 Lyon (siège)

📍 57 rue d'Amsterdam - 75008 Paris

✉ formation@devictio.fr

f facebook.com/organisme.de.formation

in fr.linkedin.com/company/devicto

📷 instagram.com/devictioformations