LUTTE ANTI-FRAUDE EN ASSURANCE GRÂCE À L'IA

Intelligence Artificielle

Bulletin de participation sur www.caritat.fr

PPC 84

Durée de la formation ?

2 jours – soit 14 heures.

À qui s'adresse cette formation ?

Cette formation est destinée aux professionnels impliqués dans des dispositifs de lutte contre la fraude, notamment dans les secteurs de l'assurance, des finances ou tout autre domaine exposé à des risques frauduleux. Elle convient aux gestionnaires, analystes de données, responsables de la conformité et toute personne souhaitant maîtriser les outils et stratégies anti-fraude.

Pour obtenir quoi ?

Maîtrisez les méthodes les plus avancées de détection et de prévention des fraudes en assurance.

Quels objectifs pédagogiques ?

Comprendre et concevoir des processus anti-fraude efficaces, adaptés à divers types de fraudes (opportunistes, planifiées, internes ou externes).

Apprendre à exploiter les données internes et externes pour enrichir les analyses et fiabiliser les systèmes de détection.

Découvrir et appliquer des techniques avancées comme l'OCR, le NLP et l'analyse de réseaux relationnels pour détecter des comportements frauduleux.

Mettre en œuvre des outils d'automatisation pour optimiser la détection et la réponse aux fraudes.

Créer des tableaux de bord interactifs et des outils de visualisation pour suivre les indicateurs clés de performance et identifier les communautés frauduleuses.

Renforcer les compétences opérationnelles dans l'utilisation de méthodes supervisées et non supervisées pour détecter des anomalies et classifier les fraudes.

Quelles méthodes mobilisées ?

Études de cas pratiques : utilisation de techniques comme l'OCR, le NLP et des algorithmes avancés (clustering, classification, analyse de graphes).

Exemples concrets issus du terrain, illustrant les processus anti-fraude et les solutions mises en place.

Mises en application pratiques : travaux sur données tabulaires, textuelles et visuelles.

Construction collaborative de tableaux de bord et exploration des outils de surveillance en temps réel.

Quels sont les prérequis ?

Aucun prérequis technique spécifique n'est nécessaire. Cependant, une bonne compréhension des enjeux numériques et une appétence pour l'analyse de données seront un atout pour profiter pleinement de la formation.

Quelles modalités d'évaluation ?

Une évaluation des acquis des objectifs sera réalisée durant la formation.

Chaque participant se munira d'un ordinateur portable pour les travaux pratiques.

La formation en pratique...

Quand et où ?

2 et 3 septembre 2026
9 h 00 - 12 h 30 et 14 h 00 - 17 h 30
Caritat, Paris 8e

Combien ça coûte ?

2 300 € HT + TVA 20%, soit 2 760 € TTC.
Les frais de participation couvrent les deux journées de formation, la documentation complète, les déjeuners et les pauses café.

Qu'allez-vous apprendre ?

Partie 1 : Stratégies et automatisation anti-fraude

1.1 Conception des processus anti-fraude
- **Cadre légal des fraudes en assurance** : Réglementations et obligations.
- **Typologies des fraudes** : Opportunistes, planifiées, internes, externes.
- **Types d'anomalies et risques associés** : Analyse des comportements et signaux d'alerte.
- **Processus anti-fraude** : Méthodes pour détecter, prévenir et réduire les fraudes.

1.2 Détection de fraude documentaire
- **Types de documents concernés** : Déclarations, justificatifs, contrats, factures.
- **Techniques pour identifier les documents frauduleux** : Analyse de métadonnées, incohérences, signatures électroniques.
- **Utilisation de l'OCR et du NLP** : Extraction et vérification des informations textuelles.
- **Cas pratiques** : OCR et LLM

1.3 Automatisation des processus anti-fraude
- Actions prescriptives : recommandations et décisions automatiques.
- Utilisation de workflows pour rationaliser la détection et la réponse.

1.4 Évaluation et amélioration continue
- Suivi des performances des systèmes de détection.
- Ajustements des méthodes en fonction des retours et évolutions.

Partie 2 : Sources de données et enrichissements

2.1 Données internes
- Identification des problèmes de qualité et de cohérence.
- Solutions pour fiabiliser les données internes.

2.2 Dark data
- Défis liés à l'intégration des données inutilisées ou non structurées
- **Transformation des données** : Méthodes pour rendre exploitables ces données, notamment en utilisant des outils d'extraction et de traitement.

2.3 Données externes
- Utilisation de données publiques ou tierces pour enrichir les bases.
- Problématiques de jointures et de mise en cohérence des sources multiples.

2.4 Construction et transformation des indicateurs
- Création d'indicateurs pertinents pour la détection de fraudes.
- Préparation des données tabulaires, textuelles, et visuelles (images).

Partie 3 : Méthodes de détection de fraudes

3.1 Règles déterministes et détection d'anomalies
- Mise en place de seuils critiques et alertes.
- Analyse des comportements anormaux dans les données.

3.2 Méthodes non supervisées
- Clustering et détection d'anomalies sans étiquettes.
- Segmentation des données pour identifier des comportements suspects.

3.3 Classification des fraudes
- Utilisation des algorithmes supervisés : Arbre de décision, Régression logistique, SVM (Support Vector Machine), Autres techniques avancées.

3.4 Détection des fraudes dans les réseaux
- Analyse des réseaux relationnels : connexions entre parties prenantes.
- Détection de communautés frauduleuses grâce au clustering.
- Métriques des graphes : degré, connectivité, homophilie.

Partie 4 : Visualisation et suivi des résultats

4.1 Tableaux de bord pour le suivi des indicateurs clés
- Création de tableaux interactifs permettant de surveiller les performances des systèmes de détection.
- Suivi des indicateurs clés tels que les anomalies détectées, les taux de fraude confirmée, et les pertes évitées.

4.2 Outils de surveillance en temps réel
- Déploiement de systèmes d'alertes automatisés pour signaler des comportements suspects.
- Intégration d'outils analytiques pour un suivi constant et réactif.

4.3 Visualisation des réseaux et des communautés
- Représentation graphique des relations et clusters frauduleux pour une meilleure compréhension des réseaux suspects.
- Identification visuelle des communautés et connexions atypiques.

01 44 51 04 00
info@caritat.fr

Qui anime cette formation ?

Kezhan SHI,
Il est diplômé de l'École Centrale Paris et titulaire d'un master en actuariat de l'Université Paris Dauphine. Il a travaillé chez Axa Global Direct et Allianz, avant de rejoindre Diot Siaci en 2022, au titre de Directeur adjoint Data Lab.

Qu'en disent les stagiaires ?

Cette formation est une nouveauté du catalogue Caritat.