الكشف عن الاحتيال في المصارف بواسطة تقنية الذكاء الاصطناعي

Duration: 5 Days

Language: ar

Course Code: PI2 - 123

Objective

بحلول نهاية هذه الدورة، سيكون المشاركون قادرين على:

- فهم مشهد الاحتيال في أنظمة البنوك الرقمية.
- استكشاف كيفية استخدام الذكاء الاصطناعي وتعلم الآلة لاكتشاف الاحتيال المالي.
- تحليل بيانات المعاملات والسلوك لتحديد الإشارات الحمراء والإشارات الخطرة.
- بناء وتقييم نماذج تعلم الآلة لاكتشاف الاحتيال.
- تطبيق كشف الشذوذ وتحليلات الرسوم البيانية لمراقبة الاحتيال في الوقت الحقيقي.
- معالجة تغير النموذج، الإيجابيات الزائفة، وتحديات الامتثال التنظيمي.
- دمج نماذج الذكاء الاصطناعي في خطوط أنابيب اكتشاف الاحتيال وأنظمة البنوك.

Audience

هذا الدورة مثالية لـ:

- محللي الاحتيال ومحترفي مخاطر البنوك.
- علماء البيانات ومهندسي الذكاء الاصطناعي في المؤسسات المالية.
- ضباط أمن المعلومات والامتثال.
- فرق عمليات البنوك ومراقبة المعاملات.

- مديري تقنية المعلومات الذين يطورون بنية مكافحة الاحتيال.
- محترفي التكنولوجيا المالية الذين يبنون أدوات مكافحة الاحتيال القائمة على الذكاء الاصطناعي.

Training Methodology

يجمع هذا الدورة بين التعليم الفني والمختبرات العملية وتحليل دراسات الحالة وتمارين المحاكاة. سيستخدم المشاركون لغة بايثون ومجموعات بيانات حقيقية من القطاع المصرفي لبناء نماذج لاكتشاف الاحتيال، واختبار خوارزميات متنوعة، وتطبيق مقاييس التقييم. تركز المناقشات التفاعلية على التحديات الأخلاقية والتشغيلية.

Summary

مع تزايد تعقيد المعاملات المصرفية الرقمية والتحول إلى الطرق الإلكترونية، تتطور أيضًا طرق استخدامها من قِبل المحتالين. لم تعد أنظمة الكشف التقليدية عن الاحتيال القائمة على القواعد كافية لمواجهة التهديدات المتطورة والمعقدة. تقدم الذكاء الاصطناعي (AI) نهجًا أكثر ذكاءً وسرعة وقابلية للتوسيع ـ باستخدام تحليل البيانات في الوقت الحقيقي والاعتراف بالأنماط والكشف عن الشذوذ لتحديد الأنشطة المشبوهة قبل أن تتسبب في الضرر.

يقدم هذا الدورة التدريبية للمشاركين تقنيات حديثة لاكتشاف الاحتيال بدعم من الذكاء الاصطناعي، بما في ذلك التعلم الرقابي وغير الرقابي، والتعلم العميق، والنهج المعتمد على الرسوم البيانية. من خلال تمارين عملية ودراسات حالات من الحياة الواقعية، ومناقشات أخلاقية، سيتعلم المشاركون كيفية بناء ونشر نماذج لاكتشاف الاحتيال مصممة خصيصًا لبيئات البنوك.

Course Content & Outline

القسم 1: الاحتيال في عصر البنوك الرقمية

- أنواع الاحتيال المالي: سرقة الهوية، احتيال المعاملات، التصيد الاحتيالي، الحسابات الاصطناعية
- الطبيعة المتطورة للاحتيال في البنوك الإلكترونية والجوالة
- قيود أنظمة اكتشاف الاحتيال التقليدية
- كيف يعزز الذكاء الاصطناعي اكتشاف الاحتيال: السرعة، التكيف، والأتمتة
- دراسات حالة صناعية: كيف يكتشف الذكاء الاصطناعي الاحتيال قبل انتشاره

القسم 2: البيانات لاكتشاف الاحتيال

- مصادر البيانات الرئيسية: المعاملات، سلوك تسجيل الدخول، الموقع الجغرافي، بيانات الجهاز
- هندسة الميزات للاكتشاف الاحتيالي: السرعة، التكرار، انحراف المبلغ
- تحليل البيانات الاستكشافي (EDA) لأنماط الاحتيال
- تصنيف البيانات، اختلال التوازن في الفئات، وتوليد البيانات الاصطناعية
- مختبر: إعداد واستكشاف بيانات الاحتيال باستخدام بايثون وباندا

القسم 3: نماذج التعلم الآلي لاكتشاف الاحتيال

- التعلم الموجه: الأشجار القرارية، الغابات العشوائية، تعزيز التدرج
- التعلم غير الموجه: التجميع والغابات العازلة للاحتيال غير المعروف
- التعلم العميق لاكتشاف أنماط الاحتيال المعقدة في التسلسلات
- مقاييس التقييم: الدقة، الاسترجاع، F1، تكلفة الإيجابيات الكاذبة
- ورشة عمل: تدريب وتقييم نموذج اكتشاف الاحتيال على بيانات المعاملات

القسم 4: الاكتشاف في الوقت الحقيقي، التنبيهات، ومراقبة الشذوذ

- معالجة التدفق للاكتشاف في الوقت الحقيقي: كافكا، سبارك، وواجهات برمجة التطبيقات
- بناء أنظمة تنبيه في الوقت الحقيقي باستخدام محفزات الذكاء الاصطناعي
- تحليل الرسوم البيانية للاحتيال القائم على الشبكات (مثل شبكات نقل الأموال)
- التصدي للهجمات العدائية وسلوك الاحتيال المتطور
- التكامل مع منصات البنوك وأنظمة الإجراءات الآلية

القسم 5: الحوكمة، الأخلاقيات، والتشغيل

- الاعتبارات التنظيمية (مثل PSD2، قوانين مكافحة غسل الأموال، الامتثال للائحة العامة لحماية البيانات)
- إدارة انحراف النموذج وضمان الشرح في السياقات الحساسة
- موازنة دقة الاكتشاف مع تجربة العميل
- التقارير الشفافة ومسارات التدقيق في الأنظمة المدفوعة بالذكاء الاصطناعي
- المشروع النهائي: تقديم استراتيجية اكتشاف الاحتيال وهيكلية النموذج

Certificate Description

عند إتمام هذه الدورة التدريبية بنجاح، سيحصل المشاركون على شهادة إتمام التدريب من Holistique Training. (e-Certificate) وبالنسبة للذين يحضرون ويكملون الدورة التدريبية عبر الإنترنت، سيتم تزويدهم بشهادة إلكترونية من Holistique Training.

شهادات Holistique Training معتمدة من المجلس البريطاني للتقييم (BAC) وخدمة اعتماد التطوير المهني المستمر (CPD)، كما أنها معتمدة وفق معايير ISO 9001 وISO 21001 وISO 29993.

لهذه الدورة من خلال شهاداتنا، وستظهر هذه النقاط على شهادة إتمام (CPD) يتم منح نقاط التطوير المهني المستمر واحدة عن كل ساعة CPD يتم منح نقطة، CPD ووفقًا لمعايير خدمة اعتماد Holistique Training. التدريب من لأي دورة واحدة نقدمها حاليًا CPD حضور في الدورة. ويمكن المطالبة بحد أقصى قدره 50 نقطة.

Categories

الذكاء الاصطناعي وإدارة البيانات, الخدمات المصرفية والمالية, التكنولوجيا

Related Articles

الذكاء الاصطناعي والمصرفية المفتوحة: الفوائد التحديات والمستقبل

تُعد المصرفية المفتوحة و الذكاء الاصطناعي من أبرز التطورات التقنية التي تشهدها الصناعة المصرفية في الوقت الراهن. حيث تمثل المصرفية المفتوحة تحولًا جذريًا في كيفية تعامل المؤسسات المالية مع البيانات، من خلال إتاحتها للجهات الثالثة عبر واجهات برمجة التطبيقات (APIs) لتطوير خدمات مالية مبتكرة ومتنوعة. وفي المقابل، يساهم الذكاء الاصطناعي