الدورة التدريبية: تطوير أنظمة الكشف عن الاحتيال المدعومة بالذكاء الاصطناعي

#AI6175

الدورة التدريبية: تطوير أنظمة الكشف عن الاحتيال المدعومة بالذكاء الاصطناعي

مقدمة الدورة التدريبية / لمحة عامة:

يقدم BIG BEN Training Center هذه الدورة التدريبية المتخصصة حول تطوير أنظمة الكشف عن الاحتيال المدعومة بالذكاء الاصطناعي، وهي مصممة للمحللين الماليين، ومدققي الاحتيال، ومتخصصي الأمن السيبراني، ومطوري أنظمة البيانات، وقادة المخاطر والامتثال، الذين يسعون إلى الاستفادة من قوة الذكاء الاصطناعي (AI) والتعلم الآلي (ML) لـتعزيز قدرات الكشف عن الاحتيال، وتقليل الخسائر المالية، وحماية المؤسسات من التهديدات المتزايدة. في عالم تتزايد فيه تعقيدات الاحتيال المالي والإلكتروني، أصبحت الأنظمة الذكية ضرورة لـتحديد الأنماط المشبوهة والتنبؤ بالاحتيال المحتمل بفعالية. ستغطي الدورة مفاهيم مثل تحليل البيانات للكشف عن الاحتيال، نماذج التعلم الآلي للكشف عن المعاملات الاحتيالية، التعلم العميق في اكتشاف الشذوذ (Anomaly Detection)، التحليلات السلوكية للمستخدمين، وبناء أنظمة إنذار مبكر. سيتعلم المشاركون كيفية تطبيق خوارزميات الذكاء الاصطناعي لـتحليل كميات هائلة من البيانات، واكتشاف الاحتيال في الوقت الحقيقي تقريباً، وتحسين دقة التنبؤات. تهدف الدورة إلى تمكين المختصين من فهم إمكانات الذكاء الاصطناعي في مجالهم، وتطوير استراتيجيات متقدمة لمكافحة الاحتيال، وقيادة الابتكار في أقسامهم. نستلهم في هذه الدورة من أعمال البروفيسور توم دافنبورت (Tom Davenport)، Tom Davenport، وهو خبير رائد في التحليلات والبيانات الضخمة، والذي يؤكد على أهمية الاستفادة من البيانات لاتخاذ قرارات أفضل، بما في ذلك مكافحة الاحتيال. ستقدم الدورة دراسات حالة واقعية لشركات رائدة نجحت في تطبيق الذكاء الاصطناعي للكشف عن الاحتيال، مما يعزز فهم المشاركين للجوانب العملية والتطبيقية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- محللي الاحتيال المالي.
- متخصصي الأمن السيبراني.
- مدققي الحسابات الداخلية والخارجية.
- مديري المخاطر والامتثال.
- خبراء مكافحة غسل الأموال (AML).
- محللي البيانات وعلماء البيانات.
- مديري المنتجات المالية.
- المستشارين في مجال الأمن المالي.
- المحققين في جرائم الاحتيال.
- قادة التحول الرقمي في المؤسسات المالية.

القطاعات والصناعات المستهدفة:

- البنوك والمؤسسات المالية.
- التأمين.
- التجارة الإلكترونية والمدفوعات الرقمية.
- الاتصالات.
- الرعاية الصحية.
- الحكومة (مكافحة الاحتيال الضريبي والمالي).
- شركات التكنولوجيا المالية (FinTech).
- الخدمات الاستشارية.
- التجزئة.
- شركات الأمن السيبراني.

الأقسام المؤسسية المستهدفة:

- قسم إدارة المخاطر.
- قسم الامتثال.
- قسم الأمن السيبراني.
- قسم التدقيق الداخلي.
- قسم مكافحة الاحتيال وغسل الأموال (AML/Fraud).
- قسم تحليل البيانات.
- قسم تكنولوجيا المعلومات.
- قسم العمليات المصرفية.
- قسم إدارة الائتمان.
- قسم تطوير المنتجات.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم دور الذكاء الاصطناعي في الكشف عن الاحتيال.
- تطبيق خوارزميات التعلم الآلي لتحديد المعاملات المشبوهة.
- بناء نماذج لاكتشاف الشذوذ (Anomaly Detection).
- تحليل سلوك المستخدمين للكشف عن الأنشطة الاحتيالية.
- التمييز بين أنواع الاحتيال المختلفة (ائتمان، تأمين، سيبراني).
- استخدام البيانات الضخمة في أنظمة الكشف عن الاحتيال.
- تطوير أنظمة إنذار مبكر للتهديدات الاحتيالية.
- تقييم أداء نماذج الكشف عن الاحتيال.
- فهم التحديات الأخلاقية والقانونية في تطبيق الذكاء الاصطناعي.
- تصميم استراتيجيات متكاملة لمكافحة الاحتيال المدعومة بالذكاء الاصطناعي.

منهجية الدورة التدريبية:

يعتمد BIG BEN Training Center في هذه الدورة على منهجية تدريبية عملية ومتقدمة، تهدف إلى تمكين المشاركين من تطوير أنظمة كشف الاحتيال المدعومة بالذكاء الاصطناعي بفعالية. تشمل المنهجية محاضرات نظرية متعمقة حول مفاهيم الذكاء الاصطناعي والتعلم الآلي في سياق مكافحة الاحتيال، بالإضافة إلى ورش عمل تطبيقية مكثفة. سيقوم المشاركون بتحليل مجموعات بيانات احتيالية، وبناء نماذج تعلم آلي للكشف عن الاحتيال، وتطبيق تقنيات التعلم العميق لاكتشاف الشذوذ. سيتم التركيز على دراسات حالة واقعية لشركات رائدة في مجال مكافحة الاحتيال بالذكاء الاصطناعي، مما يعزز فهم المشاركين للجوانب العملية والتحديات المرتبطة بالتطبيق. سيتم تشجيع العمل الجماعي والمناقشات لتبادل الخبرات وتطوير حلول مبتكرة لمواجهة أساليب الاحتيال المتطورة. يتلقى المشاركون تغذية راجعة منتظمة من المدربين الخبراء لضمان تطوير مهاراتهم في حماية المؤسسات من الاحتيال من خلال تطبيقات الذكاء الاصطناعي.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: أساسيات الذكاء الاصطناعي والكشف عن الاحتيال.

- مقدمة إلى الاحتيال وأنواعه المختلفة.
- دور الذكاء الاصطناعي في مكافحة الاحتيال.
- البيانات الضخمة والتحليلات في الكشف عن الاحتيال.
- خوارزميات التعلم الآلي الأساسية (التصنيف، التجميع).
- الفرق بين أساليب الكشف التقليدية والذكاء الاصطناعي.
- الفرص والتحديات في بناء أنظمة ذكية لمكافحة الاحتيال.
- نظرة عامة على دورة حياة مشروع الكشف عن الاحتيال بالذكاء الاصطناعي.

الوحدة الثانية: نماذج التعلم الآلي للكشف عن الاحتيال.

- تجهيز البيانات وتنظيفها لتدريب النماذج.
- هندسة الميزات (Feature Engineering) لبيانات الاحتيال.
- بناء نماذج تصنيف للكشف عن المعاملات الاحتيالية.
- التعلم العميق (Deep Learning) في اكتشاف الأنماط المعقدة.
- استخدام الشبكات العصبية للكشف عن الاحتيال.
- تقييم أداء النماذج (الدقة، الاستدعاء، مقياس F1).
- معالجة مشكلة عدم توازن البيانات في الاحتيال.

الوحدة الثالثة: اكتشاف الشذوذ والتحليلات السلوكية.

- مفاهيم اكتشاف الشذوذ (Anomaly Detection).
- خوارزميات الكشف عن الشذوذ (Isolation Forest, One-Class SVM).
- تطبيق اكتشاف الشذوذ على المعاملات المالية.
- التحليل السلوكي للمستخدمين للكشف عن الاحتيال.
- بناء ملفات تعريف سلوكية طبيعية.
- تحديد السلوكيات المنحرفة والمشبوهة.
- دراسات حالة في اكتشاف الشذوذ السلوكي.

الوحدة الرابعة: بناء أنظمة الكشف عن الاحتيال في الوقت الحقيقي.

- معالجة البيانات المتدفقة للكشف عن الاحتيال الفوري.
- بناء خطوط أنابيب (Pipelines) للبيانات في الوقت الحقيقي.
- دمج أنظمة الذكاء الاصطناعي مع الأنظمة التشغيلية.
- تنبيهات الاحتيال وأنظمة الإنذار المبكر.
- تفاعل الإنسان في حلقة الكشف عن الاحتيال (Human-in-the-loop).
- التعلم المستمر وتحديث النماذج.
- تطبيقات الكشف عن الاحتيال في القطاعات المختلفة.

الوحدة الخامسة: التحديات، الأخلاقيات، ومستقبل مكافحة الاحتيال بالذكاء الاصطناعي.

- التحديات القانونية والتنظيمية (GDPR، AML).
- أخلاقيات الذكاء الاصطناعي: التحيز والعدالة.
- أمن البيانات والخصوصية في أنظمة مكافحة الاحتيال.
- الهجمات المضادة (Adversarial Attacks) على نماذج الذكاء الاصطناعي.
- التعلم المعزز (Reinforcement Learning) في مكافحة الاحتيال.
- الذكاء الاصطناعي التفسيري (Explainable AI) في الكشف عن الاحتيال.
- التوجهات المستقبلية في مكافحة الاحتيال الذكية.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20–25 ساعة تدريبية.

سؤال للتأمل:

في ظل التطور السريع لتقنيات الذكاء الاصطناعي في الكشف عن الاحتيال، وكيفية قدرة المحتالين على تكييف أساليبهم، كيف يمكن للمؤسسات ضمان أن أنظمتها المدعومة بالذكاء الاصطناعي تظل فعالة وقادرة على مواكبة هذه التهديدات المتغيرة باستمرار؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها العملي والشامل على تطوير أنظمة الكشف عن الاحتيال المدعومة بالذكاء الاصطناعي، مما يوفر للمشاركين فهماً عميقاً لكيفية حماية المؤسسات من المخاطر المالية. ما يميزنا هو دمج الأسس النظرية للذكاء الاصطناعي والتعلم الآلي مع التطبيقات العملية في مكافحة الاحتيال، مما يتيح للمشاركين بناء نماذج قوية قادرة على اكتشاف الأنماط المشبوهة. نغطي دورة حياة الكشف عن الاحتيال من الألف إلى الياء، من تحليل البيانات إلى بناء النماذج وتقييمها، مع التركيز على أفضل الممارسات والتحديات الأمنية والأخلاقية. الدورة تركز على تزويد المشاركين بالمهارات اللازمة لـتقليل الخسائر الناتجة عن الاحتيال، وتعزيز الأمن المالي، وقيادة مبادرات الابتكار في هذا المجال الحيوي.