التدريبية: تطوير أنظمة الكشف عن الاحتيال المدعومة بالذكاء الاصطناعي الدورة

يونيو ٢٠٢٦ ٠٥ - ٠١

لشبونة

(للشخص الواحد) € ٤٤٠٠

Ref: #AI6175_243694

مقدمة الدورة التدريبية / لمحة عامة:

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

في تطبيق الذكاء الاصطناعي للكشف عن الاحتيال، مما ستقدم الدورة دراسات حالة واقعية لشركات رائدة نجحت لاتخاذ

يعزز فهم المشاركين للجوانب العملية والتطبيقية.

لـ: الفئات المستهدفة / هذه الدورة التدريبية مناسبة

- 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:

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

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

منهجية الدورة التدريبية:

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

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الاحتيال. الوحدة الأولى: أساسيات الذكاء الاصطناعي والكشف عن

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

الاحتيال.، الوحدة الثانية: نماذج التعلم الآلي للكشف عن

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

السلوكية.، الوحدة الثالثة: اكتشاف الشذوذ والتحليلات

- مفاهيم اكتشاف الشذوذ (Anomaly Detection).
- One-Class SVM)، خوارزميات الكشف عن الشذوذ (Isolation Forest،
- 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.

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

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

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

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

الأسئلة المتكررة:

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

لا توجد شروط مسبقة.

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

المدة إلى ٢٥٢٠- بمعدل يومي يتراوح بين ٤ إلى ٥ ساعات، تشمل فترات تمتد هذه الدورة التدريبية على مدار خمسة أيام،

ساعة تدريبية، راحة وأنشطة تفاعلية، ليصل إجمالي

سؤال للتأمل:

للمؤسسات ضمان أن الكشف عن الاحتيال، وكيفية قدرة المحتالين على في ظل التطور السريع لتقنيات الذكاء الاصطناعي في

على مواكبة هذه التهديدات المتغيرة أنظمتها المدعومة بالذكاء الاصطناعي تظل فعالة تكييف أساليبهم، كيف يمكن

باستمرار؟ وقادرة

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

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