

دورة كشف الاحتيال بالذكاء الاصطناعي ومراقبة المعاملات الفورية

4 – 8 يوليو 2027

عن بعد





دورة كشف الاحتيال بالذكاء الاصطناعي ومراقبة المعاملات الفورية

المرجع: 18670_241 التاريخ: 4 - 8 يوليو 2027 المكان: عن بعد الرسوم: GBP 1700

ملخص البرنامج

كشف الاحتيال بالذكاء الاصطناعي ومراقبة المعاملات الفورية محور دورة تدريبية تمتد 5 أيام بمستوى متقدم لقيادات مكافحة الاحتيال والجرائم المالية والمخاطر، ويخرج منها كل مشارك بخارطة طريق لكشف الاحتيال بالذكاء الاصطناعي في منتج أو قناة دفع واحدة. فالاحتيال يتحرك اليوم بسرعة المدفوعات الفورية، والتنبيهات القائمة على القواعد إما أن تفوت الأساليب الجديدة أو تغرق المحليين بالإشارات الكاذبة. ويتدرج البرنامج من حوكمة مخاطر الاحتيال، مروراً بنماذج الكشف وتحليلات الشبكات، إلى التحقق وتصميم التشغيل. تقدم هذا البرنامج في كشف الاحتيال بالذكاء الاصطناعي مارس للتدريب المملكة المتحدة.

المبررات المؤسسية

كل مخطط احتيال لا يكتشف يتحول إلى خسارة مباشرة، وكل تنبيه غير ضروري يستهلك وقت المحليين ويزعج العملاء الحقيقيين. ويستطيع التعلم الآلي تقييم المعاملات فوراً وكشف الروابط الخفية بين الحسابات، شرط أن تكون مخرجاته قابلة للتفسير وخاضعة للتحقق. أما القيادات التي تحكم هذه النماذج ضمن برنامج إدارة مخاطر الاحتيال فتكشف احتيالا أكثر بتدخلات أقل.

- خسائر الاحتيال: تنخفض حين تكشف نماذج الشذوذ والنماذج الموجهة الأساليب الناشئة مبكراً.
- معدل الإنذارات الكاذبة: يتراجع حين تحل درجات المخاطر محل القواعد الجامدة وترتب قوائم التنبيهات.
- زمن دورة التحقيق: يقصر حين تكشف تحليلات الشبكات الحسابات المترابطة وشبكات الاحتيال.

المبادئ والأساس المعرفي

- دليل COSO/ACFE لإدارة مخاطر الاحتيال: تحدد مبادئه الخمسة موقع الكشف الذكي في برنامج مكافحة الاحتيال في الجلسة 1.
- التعلم الموجه وغير الموجه: تبني أساليب التصنيف وكشف الشذوذ مقارنة النماذج في الجلسة 2.
- تحليلات الرسوم البيانية: تقوم عليها العلاقات بين الحسابات والأجهزة والأطراف المقابلة لكشف شبكات الاحتيال في الجلسة 3.
- ISO/IEC 42001، معيار نظام إدارة الذكاء الاصطناعي: توجه متطلباته حوكمة النماذج وضوابط التحقق في الجلسة 4.



المشاركون المستهدفون

- القيادات المسؤولة عن خسائر الاحتيال وبرامج إدارة مخاطره.
- رؤساء الجرائم المالية المشرفون على مراقبة المعاملات وعمليات التنبيهات.
- كبار قيادات المخاطر والامتثال ومخاطر النماذج الذين يعتمدون نماذج الكشف.
- قيادات المراجعة الداخلية التي تؤكد فاعلية ضوابط مكافحة الاحتيال.
- قيادات المدفوعات والقنوات الرقمية التي توازن بين ضبط الاحتيال وتجربة العميل.

يخدم البرنامج إدارات مكافحة الاحتيال والجرائم المالية والمخاطر والتدقيق والمدفوعات في قطاعات المصارف والتأمين والاتصالات وجهات تحصيل الإيرادات الحكومية.

مخرجات التعلم

1. سيكون المشاركون قادرين على تشخيص فجوات الكشف الحالية مقارنة بمبادئ إدارة مخاطر الاحتيال.
2. سيكون المشاركون قادرين على تقييم النماذج الموجهة ونماذج كشف الشذوذ لنمط احتيال محدد.
3. سيكون المشاركون قادرين على تصميم تقييم فوري وترتيب للتنبيهات يخفف الإنذارات الكاذبة.
4. سيكون المشاركون قادرين على تطبيق تحليلات الشبكات لتحديد الحسابات المترابطة والمخططات المنظمة.
5. سيكون المشاركون قادرين على بناء متطلبات التحقق وقابلية التفسير لنماذج الاحتيال.
6. سيكون المشاركون قادرين على تبرير خارطة طريق كشف الاحتيال بالذكاء الاصطناعي أمام الإدارة العليا.

هيكل البرنامج

اليوم 1: حوكمة مخاطر الاحتيال وفرص الذكاء الاصطناعي

أين يقصر كشف الاحتيال الحالي، وأين يمكن للذكاء الاصطناعي أن يساعد؟

- مبادئ دليل COSO/ACFE لإدارة مخاطر الاحتيال
- أنماط الاحتيال في المدفوعات والإقراض والمطالبات
- مراجعة أداء الكشف القائم على القواعد
- مصادر بيانات الاحتيال: المعاملات والأجهزة وسلوك العملاء
- خريطة حالات استخدام الكشف الذكي وتقييم النضج

اليوم 2: نماذج كشف الاحتيال بالذكاء الاصطناعي

أي أساليب النمذجة تكشف الاحتيال المعروف والناشئ بموثوقية أعلى؟



- التصنيف الموجه باستخدام حالات احتيال موسومة
- كشف الشذوذ غير الموجه للأساليب الجديدة
- التنميط السلوكي وتصميم المتغيرات
- اختلال توازن الفئات وجودة الوسوم وحلقات التغذية الراجعة
- الدقة والاستدعاء ومقارنة النماذج المرجحة بالتكلفة

اليوم 3: مراقبة المعاملات الفورية وتحليلات الشبكات

كيف توقف المعاملات الخطرة في الوقت المناسب وتكشف شبكات الاحتيال؟

- بنية التقييم الفوري للمعاملات
- حدود التنبيه القائمة على المخاطر وترتيب القوائم
- تحليلات الرسوم البيانية للحسابات المترابطة وشبكات الحسابات الوسيطة
- قرارات احتكاك العميل والتحقق الإضافي من الهوية
- التكامل مع إدارة الحالات وتغذية المحللين الراجعة

اليوم 4: التحقق من النماذج وقابلية التفسير والحوكمة

هل يمكن الوثوق بكل نموذج احتيال وتفسيره والدفاع عنه؟

- ضوابط ISO/IEC 42001 لنماذج كشف الاحتيال
- التحقق المستقل من النماذج والاختبار الرجعي
- تفسير التنبيهات للمحللين والعملاء
- مراقبة انحراف النماذج وتكيف المحللين
- خصوصية البيانات والعدالة في قرارات الاحتيال

اليوم 5: تطبيق كشف الاحتيال بالذكاء الاصطناعي

هل خارطة طريق كشف الاحتيال جاهزة لاعتماد الإدارة العليا؟

- سد فجوات الكشف من الجلسة 1 بالنماذج المختارة
- تحديد حدود التنبيه من الجلسة 3 للقناة المختارة
- إدراج التحقق من الجلسة 4 في دورة حياة النموذج
- نموذج التشغيل والمهارات وتصميم سير عمل المحللين
- إنجاز خارطة طريق كشف الاحتيال بالذكاء الاصطناعي



المنهجية

يجمع البرنامج بين ورش البيانات وتحليل الحالات، إذ يقارن المشاركون تنبيهات القواعد بتنبيهات النماذج على عينة من بيانات المعاملات، ويتتبعون شبكة احتيال عبر رسم بياني، ويصوغون متطلبات التحقق. وتستمد الحالات من مدفوعات البطاقات ومطالبات التأمين واحتيال اشتراكات الاتصالات.

- نشاط مقترح: مقارنة معدلات الإنذارات الكاذبة بين القواعد ونموذج تقييم على البيانات نفسها.
- نشاط مقترح: رسم شبكة حسابات وسيطة من روابط المعاملات.
- نشاط مقترح: صياغة تفسير للتنبيه يستطيع المحلل التصرف بناء عليه.

المخرج الختامي

يعد كل مشارك خارطة طريق لكشف الاحتيال بالذكاء الاصطناعي لمنتج أو قناة واحدة، تتضمن تقييما للفجوات، والنماذج المختارة، وتصميم الحدود والتنبيهات، ومتطلبات التحقق وقابلية التفسير، ونموذج التشغيل. وتعرض على الإدارة العليا أساسا لاستثمار الكشف التالي.

الأسئلة الشائعة

هل يناسب تدريب كشف الاحتيال بالذكاء الاصطناعي كبار قيادات مكافحة الاحتيال والمخاطر؟

نعم، فهو بمستوى متقدم للقيادات المسؤولة عن خسائر الاحتيال أو اعتماد النماذج، ولا يفترض خلفية برمجية.

ما الأطر التي يقوم عليها برنامج كشف الاحتيال بالذكاء الاصطناعي؟

يقوم على دليل COSO/ACFE لإدارة مخاطر الاحتيال والتعلم الموجه وغير الموجه وتحليلات الرسوم البيانية وISO/IEC 42001.

كيف تستخدم خارطة الطريق الناتجة عن تدريب كشف الاحتيال بالذكاء الاصطناعي في العمل؟

تستخدمها لترتيب أولويات الاستثمار في الكشف، وتحديد حدود التنبيه، والاتفاق على قواعد التحقق مع إدارتي مخاطر النماذج والتدقيق.

بم يختلف كشف الاحتيال بالذكاء الاصطناعي عن برامج التحقيق في الاحتيال؟

يركز على كشف الاحتيال بالنماذج والمراقبة الفورية، بينما تتناول برامج التحقيق جمع الأدلة وإجراء المقابلات بعد الاشتباه في الاحتيال.