CONCEPT

مكافحة الاحتيال بالتزييف العميق وكشف الوسائط المصطنعة وانتحال الهوية بالذكاء الاصطناعي

15 – 19 مارس 2027

أمستردام - فندق حي الأعمال زوداس

مكافحة الاحتيال بالتزييف العميق وكشف الوسائط المصطنعة وانتحال الهوية بالذكاء الاصطناعي

المرجع: 5985_1146 **التاريخ:** 15 – 19 مارس 2027 **المكان:** أمستردام - فندق حي الأعمال زوداس **الرسوم:** SAR 23500

العمق التقني: ممارس · **أسلوب التطبيق:** محاكاة

مقدمة

أصبحت أدوات الذكاء الاصطناعي التوليدي تتيح للمحتالين استنساخ صوت شخص من تسجيل قصير، وحقن وجه مصطنع في عملية التحقق من الهوية عن بعد، وتزوير مستندات تجتاز الفحص البصري. ولم تعد ضوابط مكافحة الاحتيال وفتح الحسابات والمدفوعات القائمة على تمييز صوت أو وجه مألوف كافية، وكثير من المؤسسات لا تكتشف الثغرة إلا بعد تنفيذ التحويل. تزود هذه الدورة من كور كونسبت الفرق التشغيلية بمنهجيات كشف هجمات الوسائط المصطنعة والتحقق منها والاستجابة لها وفق المعايير المعتمدة للقياسات الحيوية وإدارة الحوادث. ويتدرب المشاركون على سيناريوهات هجوم محددة بزمن، ويخرجون بدليل التصدي للاحتيال بالتزييف العميق لمؤسساتهم.

أهداف الدورة

- تصنيف الوسائط المصطنعة وأنماط الاحتيال بالتزييف العميق، وتحديد مواضع دخولها إلى قنوات فتح الحسابات والمدفوعات والتواصل
- تطبيق معايير كشف هجمات العرض والحقن، ومنها ISO/IEC 30107-3 وCEN/TS 18099، عند تحديد متطلبات ضوابط التحقق من الهوية أو اختبارها
- التحقق من المقاطع الصوتية والمرئية والصور المشتبه بها باستخدام قوائم الفحص الجنائي وبيانات مصدر المحتوى وبروتوكولات التأكيد عبر قناة مستقلة
- تصميم ضوابط للمدفوعات والوصول تظل فعالة حين لا يعود صوت المتصل أو وجهه دليلا موثوقا
- الاستجابة لهجوم تزييف عميق مشتبه به، مع حفظ الأدلة وتنسيق معالجة الحادث وفق ISO/IEC 27035-1
- إعداد دليل التصدي للاحتيال بالتزييف العميق بصيغة جاهزة لاعتماده لدى فرق مكافحة الاحتيال والأمن والمالية

الفئة المستهدفة

- موظفو مكافحة الاحتيال والتحقيق فيه المسؤولون عن قضايا انتحال الشخصية والاحتيال على الهوية
- فرق التحقق من الهوية وتسجيل العملاء التي تشغل التحقق عن بعد وفحوص الحيوية
- موظفو مراكز العمليات الأمنية والاستجابة للحوادث الذين يفرزون هجمات الهندسة الاجتماعية
- موظفو المالية والخزينة وعمليات الدفع المسؤولون عن اعتماد التحويلات وتغيير بيانات حسابات الموردين
- موظفو مراكز الاتصال والتحقق من هوية العملاء المعرضون لانتحال الصوت
- موظفو الاتصال المؤسسي وحماية العلامة الذين يتعاملون مع الوسائط المصطنعة التي تستهدف المؤسسة

محاور الدورة

اليوم الأول: الوسائط المصطنعة وبيئة تهديدات الاحتيال

- تصنيف الوسائط المصطنعة: تبديل الوجه ومزامنة الشفاه واستنساخ الصوت والوسائط المولدة بالكامل
- نظرة عامة على تقنيات التوليد: الشبكات التوليدية التنافسية GANs ونماذج الانتشار وتوليف الصوت العصبي
- أنماط الاحتيال بالتزييف العميق: انتحال شخصية المسؤولين التنفيذيين والهوية المصطنعة والاستيلاء على الحسابات
- أدوات المهاجمين: تطبيقات تبديل الوجه وبرمجيات الكاميرا الافتراضية والاحتيال ككخدمة
- تقييم التعرض الحالي باستخدام خريطة نقاط التماس المعرضة للاحتيال

اليوم الثاني: معايير الكشف وأطر إثبات مصدر المحتوى

- اختبار كشف هجمات العرض وفق ISO/IEC 30107-3 ومقياسا APCER وBPCER
- كشف هجمات حقن البيانات الحيوية وفق CEN/TS 18099
- مستويات ضمان الهوية وضوابط التحقق عن بعد في NIST SP 800-63-4
- بيانات اعتماد المحتوى C2PA Content Credentials وبيانات إثبات المصدر
- تقنيات الاستخدام العدائي للذكاء الاصطناعي في قاعدة MITRE ATLAS

اليوم الثالث: التحقق والكشف في العمليات اليومية

- قائمة الفحص الجنائي للوسائط: الآثار المرئية والصوتية وآثار البيانات الوصفية
- ضبط فحص الحيوية: أساليب التحدي النشطة والسلبية
- بروتوكولات التحقق بمعاودة الاتصال عبر قناة مستقلة وكلمات الرمز المتفق عليها
- ضوابط اعتماد المدفوعات: الاعتماد المزدوج وفحص طلبات تغيير البيانات المصرفية
- بطاقة تقييم أدوات الكشف: الدقة ومعدل الرفض الخاطئ وقابلية التفسير

اليوم الرابع: نمذجة التهديدات ومعالجة الحوادث والصمود

- نمذجة التهديدات بمنهجية STRIDE لقنوات تسجيل العملاء ومراكز الاتصال
- سجل مخاطر الاحتيال بالتزييف العميق المتوافق مع ISO 31000
- معالجة حوادث الوسائط المصطنعة وفق ISO/IEC 27035-1
- إجراء حفظ الأدلة وسلسلة الحيازة للوسائط المشتبه بها
- التحايل على أدوات الكشف وانحراف النماذج وخطط اختبار الفريق الأحمر

اليوم الخامس: محاكاة الهجمات ودليل التصدي

- محاكاة احتيال الدفع بالصوت المستنسخ: مسؤول تنفيذي مزيف يطلب تحويلا عاجلا
- محاكاة التسجيل عن بعد: حقن فيديو مصطنع بالتزييف العميق في عملية فتح حساب
- مراجعة ما بعد الحادث باستخدام التسلسل الزمني وتحليل إخفاق الضوابط
- إعداد مسودة دليل التصدي للاحتيال بالتزييف العميق
- استعراض الدليل ومراجعته النقدية مع الزملاء

المهارات المكتسبة

- الفحص الجنائي للوسائط المصطنعة
- كشف هجمات القياسات الحيوية
- ضمان إجراءات التحقق من الهوية
- مقاومة الهندسة الاجتماعية
- ضبط احتيال المدفوعات
- معالجة حوادث التزييف العميق
- تقييم أدوات الكشف
- التعامل مع الأدلة الرقمية

لماذا تحضر هذه الدورة

- تخرج بدليل التصدي للاحتيال بالتزييف العميق يشمل خريطة التعرض في القنوات وبروتوكولات التحقق ودليل الاستجابة
- تتدرب تحت ضغط الوقت على القرارات التي توقف احتيال الصوت المستنسخ أو الفيديو المزيف في أثناء وقوعه
- تطرح على موردي أنظمة التحقق من الهوية وأدوات الكشف أسئلة دقيقة عما تغطيه اختباراتهم وما لا تغطيه
- تتبادل أنماط الهجمات ودروس الضوابط مع مختصين في الاحتيال والأمن من قطاعات المصارف والحكومة والاتصالات والتجزئة

الخاتمة

ينجح الاحتيال بالتزييف العميق حيث لا تزال الضوابط تفترض أن رؤية الشخص أو سماع صوته دليل على هويته. تنتقل هذه الدورة من التقنيات وأنماط الاحتيال التي تقف وراء الوسائط المصطنعة، مرورا بالمعايير التي تحكم كشف هجمات العرض والحقن، وصولا إلى ضوابط التحقق والمدفوعات ومعالجة الحوادث التي تصمد تحت الضغط. ويختبر اليوم الأخير هذه الضوابط في محاكاة محددة بزمن ويجمعها في دليل التصدي للاحتيال بالتزييف العميق، فيعود المشاركون باستجابة موثقة ومجربة يشاركونها مع زملائهم في فرق الاحتيال والأمن والمالية.