CONCEPT

كشف التهديدات السيبرانية بالذكاء الاصطناعي: تعلم الآلة وتحليلات سلوك المستخدمين UEBA وأتمتة SOAR

20 – 24 سبتمبر 2027

برشلونة - فندق أربع نجوم في حي إيكسامبلا

كشف التهديدات السيبرانية بالذكاء الاصطناعي: تعلم الآلة وتحليلات سلوك المستخدمين UEBA وأتمتة SOAR

المرجع: 7647_1265 **التاريخ:** 20 – 24 سبتمبر 2027 **المكان:** برشلونة - فندق أربع نجوم في حي إيكسامبلا **الرسوم:** SAR 23500

العمق التقني: ممارس · **أسلوب التطبيق:** مختبر تطبيقي

مقدمة

تواجه فرق العمليات الأمنية بيانات رصد تفوق قدرة المحللين على قراءتها، في حين يستخدم المهاجمون بيانات دخول مسروقة وأدوات مشروعة لا تكشفها القواعد التقليدية. ويعد تعلم الآلة وتحليلات السلوك ومساعدات الذكاء الاصطناعي التوليدي بتخفيف العبء، لكن النماذج سيئة التدريب تغرق قائمة التنبيهات بالإنذارات الكاذبة وينحرف أداؤها بصمت وقد تتعرض هي نفسها للهجوم. تأخذ هذه الدورة من كور كونسبت الممارسين عبر بناء قدرات الكشف والاستجابة بالذكاء الاصطناعي وتقييمها وحوكمتها في مختبرات تطبيقية، مستندة إلى MITRE ATT&CK وMITRE ATLAS وإرشادات NIST. ويخرج المشاركون بحزمة حالات استخدام الكشف بالذكاء الاصطناعي لمراكزهم.

أهداف الدورة

- تقييم مواضع القيمة المضافة للذكاء الاصطناعي في مركز العمليات الأمنية بقياس تغطية ATT&CK ومصادر البيانات وعبء المحللين
- اختيار أساليب التعلم الموجه وغير الموجه وتحليلات السلوك المناسبة لكل حالة استخدام
- هندسة الخصائص من السجلات الأمنية وتدريب نماذج الكشف وتقييمها وضبط عتباتها على بيانات فعلية
- دمج مخرجات النماذج في قواعد الربط في SIEM وأدلة SOAR مع موافقة بشرية على الإجراءات عالية الأثر
- رصد انحراف النماذج والتلاعب العدائي بها ومخاطر الذكاء الاصطناعي التوليدي، وتطبيق الضوابط الواردة في إرشادات NIST وOWASP
- إعداد حزمة حالات استخدام الكشف بالذكاء الاصطناعي بصيغة جاهزة لمراجعة فريق هندسة المركز

الفئة المستهدفة

- محللو مراكز العمليات الأمنية المسؤولون عن الفرز والتحقيق ممن يستخدمون أدوات مدعومة بالذكاء الاصطناعي
- مهندسو الكشف الذين يبنون قواعد الربط ومحتوى التحليلات ويضبطونها
- مهندسو البيانات الأمنية المسؤولون عن مسارات السجلات وهياكلها ومنصات SIEM
- مهندسو الأتمتة الأمنية المسؤولون عن أدلة SOAR وعمليات التكامل
- صائدو التهديدات الذين يطبقون تحليلات السلوك غير المعتاد لاكتشاف النشاط الخفي

محاور الدورة

اليوم الأول: الذكاء الاصطناعي في العمليات الأمنية والوضع الراهن

- حالات استخدام الذكاء الاصطناعي في المركز: تعلم الآلة UEBAg ومساعدات الذكاء الاصطناعي التوليدي
- تقييم الوضع الراهن لأتمتة المركز بنموذج SOC-CMM
- مسارات البيانات الأمنية وتوحيد السجلات بإطار OCSF
- خط الأساس لتغطية الكشف مقابل MITRE ATT&CK
- لوحة معلومات مقاييس إرهاق التنبيهات وعبء المحللين

اليوم الثاني: نماذج الكشف وأطر أمن الذكاء الاصطناعي

- التصنيف بالتعلم الموجه لكشف التصيد والبرمجيات الخبيثة
- كشف السلوك غير المعتاد بالتعلم غير الموجه: Isolation Forest k-Meansg DBSCANg
- خطوط الأساس السلوكية في UEBA وتقدير مخاطر الكيانات
- ضوابط NIST AI RMF 1.0 وISO/IEC 42001:2023g لتطبيقات الذكاء الاصطناعي الأمنية
- الهجمات على نماذج الكشف: MITRE ATLAS وNIST AI 100-2 E2025g

اليوم الثالث: بناء قدرات الكشف بالذكاء الاصطناعي ودمجها

- هندسة الخصائص من سجلات المصادقة وتدفقات الشبكة بلغة Python
- تقييم النماذج بمقاييس الدقة والاستدعاء ومنحنيات ROC
- دمج درجات النماذج في قواعد الربط في SIEM
- أتمتة أدلة SOAR للإثراء والاحتواء
- صياغة الأوامر لمساعدات الذكاء الاصطناعي التوليدي لتلخيص التنبيهات وبناء استعلامات الصيد

اليوم الرابع: الضبط والثقة ومخاطر الذكاء الاصطناعي

- خفض الإنذارات الكاذبة ومراقبة انحراف المفاهيم
- ضوابط حقن الأوامر وتسرب البيانات من قائمة OWASP Top 10 لتطبيقات النماذج اللغوية الكبيرة 2025
- بوابات الموافقة البشرية على الاستجابة المؤتمتة
- تفسير النماذج بأسلوب SHAP لتعزيز ثقة المحللين
- كشف الهجمات المدعومة بالذكاء الاصطناعي: التصيد بالتزييف العميق والاستطلاع المؤتمت

اليوم الخامس: مختبرات الكشف وحزمة حالات الاستخدام

- مختبر كشف إساءة استخدام بيانات الدخول على مجموعة بيانات معدة
- مختبر كشف تسريب البيانات من الداخل بتقدير مخاطر UEBA
- بناء دليل SOAR وتجربته التشغيلية
- إعداد مسودة حزمة حالات استخدام الكشف بالذكاء الاصطناعي
- مراجعة الزملاء لمقاييس النماذج والدفاع عن الحزمة

المهارات المكتسبة

- هندسة البيانات الأمنية
- نمذجة كشف السلوك غير المعتاد
- تقييم نماذج الكشف
- تحليلات السلوك
- التنسيق والأتمتة الأمنية
- ضبط مخاطر نماذج الذكاء الاصطناعي
- تصميم حالات استخدام الكشف

لماذا تحضر هذه الدورة

- تعود إلى عملك بحزمة حالات استخدام الكشف بالذكاء الاصطناعي لمركزك، وقد راجع الزملاء مقاييس نماذجها
- تميز بين ادعاءات الموردين عن الكشف بالذكاء الاصطناعي والتحسن القابل للقياس في الدقة وزمن الاستجابة
- تقلص أعمال الفرز المتكررة بالأتمتة مع إبقاء المحللين أصحاب القرار في الإجراءات عالية الأثر
- تقارن تبني الذكاء الاصطناعي في العمليات الأمنية بممارسين من قطاعات ودول مختلفة

الخاتمة

لا يحسن الذكاء الاصطناعي العمليات الأمنية إلا حين تغذى نماذجه بالبيانات الصحيحة وتقاس بأمانة وتبقى تحت السيطرة البشرية. تنتقل هذه الدورة من مواضع الذكاء الاصطناعي في المركز، مرورا بنماذج الكشف وأطر أمن الذكاء الاصطناعي، وصولا إلى هندسة الخصائص والتقييم والدمج مع SIEM وSOAR والانحراف والتفسير والهجمات على الذكاء الاصطناعي ذاته. ويطبق اليوم الأخير ذلك في مختبرات الكشف ويحوله إلى حزمة حالات استخدام يعود بها المشارك إلى فريقه، جاهزة للمراجعة الهندسية والنشر المرحلي.