



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

24 - 28 May 2027

أهستردام - فندق حي النعمال زوداس



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

المرجع: 1265_7649 التاريخ: 24 - 28 May 2027 الموقع: أمستردام - فندق حي النعمال زوداس الرسوم: SAR 23500

العقود التقني: مهارس - 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 النهج سيئة التدريب تفرق قائمة التنبيهات بالإنذارات الكاذبة وينحرف أدائها بصوت وقد تتعرض هي نفسها للهجوم. تأخذ هذه الدورة من كور كونسبت المهامسين عبر بناء قدرات الكشف والاستجابة بالذكاء الاصطناعي وتقييمها وحوكمتها في مختبرات تطبيقية، مستندة إلى CK&ATT MITRE وATLAS MITRE 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 CK&ATT 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 المسؤولين عن الفرز والتحقيق ممن يستخدمون أدوات مدعومة بالذكاء الاصطناعي
- مهندسو الكشف الذين يبنون قواعد الربط ومحتوي التحليلات ويضبطونها
- مهندسو البيانات الأمنية المسؤولين عن مسارات السجلات وهياكلها ومنصات SIEM
- مهندسو الأتمتة الأمنية المسؤولين عن أدلة SOAR وعمليات التكامل
- صانعو 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 وUEBA ومساعدات الذكاء الاصطناعي التوليدي
- تقييم الوضع الراهن لأتمتة المركز بنموذج CMM-SOC
- مسارات البيانات الأمنية وتوحيد السجلات بإطار OCSF
- خط الأساس لتغطية الكشف مقابل CK&ATT MITRE
- لوحة معلومات ومقاييس إرهاب التنبيهات وعبء المحللين

اليوم الثاني: نهاذج الكشف وأطر أمن الذكاء الاصطناعي

- التصنيف بالتعلم الموجه، لكشف التصيد والبرمجيات الخبيثة
- كشف السلوك غير المعتاد بالتعلم غير الموجه: DBSCAN و Means-k و Forest Isolation
- خطوط الأساس السلوكية في UEBA وتقدير مخاطر الكيانات
- ضوابط RMF AI NIST 1.0 و IEC/ISO 42001:2023 لتطبيقات الذكاء الاصطناعي الأمنية
- الهجمات على نهاذج الكشف: E2025 100-2 AI NIST و ATLAS MITRE

اليوم الثالث: بناء قدرات الكشف بالذكاء الاصطناعي ودرجتها

- هندسة الخصائص من سجلات المصادقة وتحقق الشبكة بلغة Python
- تقييم نهاذج بهياييس الدقة والاستدعاء ومحنيات ROC
- دمج درجات نهاذج في قواعد الربط في SIEM
- أتمتة أدلة SOAR للإثراء والاحتواء
- صياغة النواير لمساعدات الذكاء الاصطناعي التوليدي لتلخيص التنبيهات وبناء استعلامات الصيد

اليوم الرابع: الضبط والثقة ومخاطر الذكاء الاصطناعي

- خفض الإنذارات الكاذبة ومراقبة انحراف المفاهيم
- ضوابط حقن النواير وتسرب البيانات من قائمة OWASP Top 10 لتطبيقات نهاذج اللغوية الكبيرة 2025
- بوابات الموافقة البشرية على الاستجابة المؤتمتة
- تفسير نهاذج بأسلوب SHAP لتعزيز ثقة المحللين
- كشف الهجمات المدعومة بالذكاء الاصطناعي: التصيد بالترتيب 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 لهياييس نهاذج والدفاع عن الحزمة

المهارات المكتسبة

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

لهذا تحضر هذه الدورة

- تعود إلى عملك بحزمة حالات استخدام الكشف بالذكاء الاصطناعي لمركزك، وقد راجع الزملاء مقاييس نهائجها
- تميز بين ادعاءات الموردين عن الكشف بالذكاء الاصطناعي والتحسين القابل للقياس في الدقة وزمن الاستجابة
- تقلص أعمال الفرز المتكررة بالذممة 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 تغذي نهائجها بالبيانات الصحيحة وتقاس بأمانة وتبقى تحت السيطرة البشرية. تنتقل هذه الدورة من مواضيع الذكاء الاصطناعي في المركز، مروراً بنهائج الكشف وأطر أمن الذكاء الاصطناعي، وصولاً إلى هندسة الخصائص والتقييم والدمج مع SIEM وSOAR والانحراف والتفسير والمجهات على الذكاء الاصطناعي ذاته. ويطبق اليوم النخير ذلك في مختبرات الكشف ويحولهم إلى حزمة حالات استخدام يعود بها المشاركون إلى فريقهم، جاهزة للمراجعة الهندسية والنشر المرحلي.