



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

6 – 10 ديسمبر 2026

الدمام - فندق خمس نجوم في المنطقة الشرقية



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

المرجع: 16550_1265 التاريخ: 6 - 10 ديسمبر 2026 المكان: الدمام - فندق خمس نجوم في المنطقة الشرقية الرسوم: SAR 19500

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 OWASP و NIST
- 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

مهاور الءورة

اليوم الأول: الءكاء الاصطناعي في العمليات الأمنية والوضع الراهن

- حالات استخدام الءكاء الاصطناعي في المركز: تعلم الآلة وUEBA ومساعدات الءكاء الاصطناعي التوليءي
- تقييم الوضع الراهن لأتمتة المركز بنموء SOC-CMM
- مسارات البيانات الأمنية وتوءيد السجلات بإطار OCSF
- خط الأساس لتغطية الكشف مقابل MITRE ATT&CK
- لوحة معلومات مقاييس إرهاب التنبيهات وعبء المحليين

اليوم الثاني: نماءج الكشف وأطر أمن الءكاء الاصطناعي

- التصنيف بالتعلم الموجه لكشف التصيء والبرمجيات الخبيثة
- كشف السلوك غير المعتاد بالتعلم غير الموجه: DBSCANg k-Meansg Isolation Forest
- خطوط الأساس السلوكية في UEBA وتقييم مخاطر الكيانات
- ضوابط NIST AI RMF 1.0 وISO/IEC 42001:2023 لتطبيقات الءكاء الاصطناعي الأمنية
- الهجمات على نماءج الكشف: MITRE ATLAS وNIST AI 100-2 E2025

اليوم الثالث: بناء قدرات الكشف بالءكاء الاصطناعي وءمجها

- هندسة الخصائص من سجلات المصادقة وتءفقات الشبكة بلغة Python
- تقييم النماءج بمقاييس الءقة والاستءعاء ومنءنيات ROC
- ءمء ءرءات النماءج في قواعد الربط في SIEM
- أتمتة أدلة SOAR للإثراء والاحتواء
- صياغة الأوامر لمساعدات الءكاء الاصطناعي التوليءي لتلخيص التنبيهات وبناء استءعلامات الصيء

اليوم الرابع: الضبط والثقة ومخاطر الءكاء الاصطناعي

- خفض الإنءارات الكاذبة ومراقبة انحراف المفاهيم
- ضوابط حقن الأوامر وتسرب البيانات من قائمة OWASP Top 10 لتطبيقات النماءج اللغوية الكبيرة 2025
- بوابات الموافقة البشرية على الاستجابة المؤتمتة
- تفسير النماءج بأسلوب SHAP لتعزيز ثقة المحليين
- كشف الهجمات المءعومة بالءكاء الاصطناعي: التصيء 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 والتحسين 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 مواضيع الذكاء الاصطناعي في المركز، مروراً بنماذج الكشف وأطر أمن الذكاء الاصطناعي، وصولاً إلى هندسة الخصائص والتقييم والدمج مع SIEM وSOAR والانحراف والتفسير والهجمات على الذكاء الاصطناعي ذاته. ويطبق اليوم الأخير ذلك في مختبرات الكشف ويحوّله إلى حزمة حالات استخدام يعود بها المشارك إلى فريقه، جاهزة للمراجعة الهندسية والنشر النهائي.