JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة في مركز العمليات الأمنية

24 – 28 مايو 2027

ميلانو

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة في مركز العمليات الأمنية

المرجع: 1134_42697 **التاريخ:** 24 – 28 مايو 2027 **المكان:** ميلانو **الرسوم:** GBP 7200

كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة دورة تدريبية مدتها أسبوع لقادة العمليات الأمنية ومديري مخاطر تقنية المعلومات الذين يقررون كيف تدخل نماذج تعلم الآلة الكاشفة وأدلة الاستجابة المؤتمتة إلى مركز العمليات الأمنية SOC، وينتهي المشاركون بإعداد خطة بنية الدفاع بالذكاء الاصطناعي. ويكتب المهاجمون اليوم نصوص الاستطلاع والتصيد بسرعة الآلة، فتتجاوز طوابير التنبيهات طاقة المحللين. وتتناول جوبيتر برايم للتدريب كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة من واقع نوبات العمل في المركز.

لماذا يهم كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة الآن

تلتقي ثلاثة ضغوط داخل المركز. فأحجام التنبيهات القادمة من الأجهزة الطرفية والهويات والسحابة تفوق قدرة محللي المستوى الأول على الفرز، والمهاجمون يختبرون نماذج الكشف نفسها بالتهرب والتسميم، ومجالس الإدارة تسأل عن مقدار الاستجابة الذي يمكن تشغيله بأمان دون نقرة بشرية. والمركز الذي يضبط كواشفه ويؤتمت الاحتواء ضمن حدود واضحة يقلص مدة بقاء المهاجم. وتستند الدورة إلى إطار إدارة مخاطر الذكاء الاصطناعي NIST AI RMF Management Framework وإلى معيار نظام إدارة الذكاء الاصطناعي ISO/IEC 42001 في الإشراف على النماذج والمساءلة. NIST AI Risk

المستفيدون من كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة

- القادة المسؤولون عن قواعد الكشف وعتبات التنبيه وطوابير الفرز
- المديرون الذين يوافقون على خطوات الاحتواء التي تعمل دون توقيع المحلل
- مالكو المخاطر الذين يرفعون التعرض السيبراني المتبقي إلى الإدارة العليا
- المهندسون الذين يربطون مسارات السجلات بنظام إدارة المعلومات والأحداث الأمنية SIEM ومنصات التنسيق
- المختصون الذين يختبرون نماذج الكشف أمام التهرب وتسميم البيانات

وتستفيد مجموعة قيادة المركز أكثر حين يحضر قائد الكشف وقائد الاستجابة ومالك المخاطر معا ويتفقون على حد واحد للأتمتة.

قدرات كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة

يحكم المشاركون على الكواشف بدقتها على بيانات القياس الخاصة بهم، ويرسمون الحد الفاصل بين فعل الآلة وحكم المحلل.

- تقييم كشف الشذوذ والمصنفات الموجهة مقابل سجل الحوادث المصنف — قادة الكشف
- حساب الدقة والاستدعاء وتكلفة التنبيه لكل كاشف — مديرو المركز
- تصميم خطوط أساس سلوك المستخدمين والكيانات مع مراقبة الانجراف — مالكو الهويات
- تحديد خطوات الأدلة التي تعمل تلقائيا وتلك المعلقة على الموافقة — قادة الاستجابة
- اختبار النماذج أمام التهرب والتسميم والتلاعب بالأوامر — قادة الفريق الأحمر
- إبلاغ التعرض المتبقي وحدود الأتمتة — كبار مسؤولي أمن المعلومات

مصطلحات كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة الأساسية

- تحليلات سلوك المستخدمين والكيانات UEBA — نماذج تتعلم النشاط المعتاد للحسابات والأجهزة وتنبه إلى الانحرافات.
- التنسيق والأتمتة والاستجابة الأمنية SOAR — منصة تشغل أدلة الاستجابة عبر الأدوات الأمنية.
- إرهاق التنبيهات — تراجع انتباه المحللين بسبب كثرة التنبيهات منخفضة القيمة.
- هجوم التهرب — مدخل مصمم ليجعل نموذج الكشف يصنف نشاطا خبيثا على أنه سليم.
- تسميم البيانات — العبث ببيانات التدريب ليتعلم النموذج نقطة عمياء.
- متوسط زمن الاحتواء — متوسط المدة بين كشف الحادث وعزل مصدره.

كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة يوما بيوم

اليوم 1: صورة التهديد بسرعة الآلة

- استخدام المهاجمين للأتمتة والأدوات التوليدية — تغير أحجام التنبيهات
- تقييم نضج مركز العمليات الأمنية — الجاهزية للكشف القائم على النماذج
- جرد بيانات القياس عبر الأجهزة الطرفية والهويات والسحابة — فجوات التغطية
- تشخيص إرهاق التنبيهات — مواضع ضياع ساعات المحللين
- تأطير مخاطر النماذج وفق NIST AI RMF — خيارات كشف خاضعة للمساءلة

اليوم 2: نماذج الكشف وخطوط الأساس السلوكية

- كشف الشذوذ مقابل المصنفات الموجهة — الملاءمة لنوع التهديد
- خطوط أساس UEBA للحسابات والأجهزة — إشارات التهديد الداخلي والاستيلاء
- اختيار الخصائص من مصادر السجلات — جودة الإشارة قبل حجمها
- تقييم الدقة والاستدعاء وتكلفة التنبيه — عتبات قبول الكواشف
- مراقبة انجراف النماذج — محفزات إعادة التدريب بعد تغير البيئة

اليوم 3: أتمتة الفرز والاستجابة

- إثراء التنبيهات وتقدير خطورتها — ترتيب الطابور للمحللين
- تصميم أدلة SOAR — خطوات الاحتواء وبوابات الموافقة
- المساعدات التوليدية لملاحظات التحقيق — واجبات مراجعة المحلل
- مصفوفة حدود الأتمتة — فعل الآلة مقابل القرار البشري
- تصميم التراجع ومفتاح الإيقاف — الحد من ضرر الإجراءات الخاطئة

اليوم 4: حماية نماذج الكشف

- اختبار تهرب المصنفات — التحصين أمام المدخلات المصممة
- ضوابط تسميم البيانات — حماية مسارات التدريب والتصنيفات
- التلاعب بأوامر المساعدات الأمنية — الحواجز الوقائية والتسجيل
- جرد النماذج وفق ISO/IEC 42001 — الملكية وسجلات التغيير
- تمارين الفريق البنفسجي على الكواشف الذكية — مكاسب تغطية مقاسة

اليوم 5: تطبيق بنية الدفاع بالذكاء الاصطناعي

- تقييم الكواشف في حالة مركز عمليات لبنك تجزئة — الإبقاء أو السحب
- خطوط الأساس السلوكية في حالة مشغل مرافق — الإشارات ذات الأولوية
- حدود الأدلة لاحتواء برمجيات الفدية — اختبار نقاط الموافقة
- إحاطة الإدارة العليا بالتعرض — بيان المخاطر السيبرانية المتبقية
- تجميع خطة بنية الدفاع بالذكاء الاصطناعي — الكواشف والأدلة والضوابط والمسؤولون

تطبيق كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة بعد الدورة

- تقييم أكثر ثلاثة كواشف إزعاجا في نظام SIEM من حيث الدقة وتكلفة التنبيه وسحب أضعفها أو إعادة ضبطه.
- صياغة مصفوفة حدود الأتمتة لدليل احتواء واحد والاتفاق على بوابات الموافقة مع مالك المخاطر.

أسئلة حول كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة

ما كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة، ولماذا يهم الآن؟

هو استخدام تعلم الآلة لرصد الهجمات واستخدام الأدلة المؤتمتة لاحتوائها داخل مركز العمليات الأمنية. ويهم الآن لأن الهجمات المؤتمتة تولد تنبيهات تفوق قدرة المحللين على الفرز اليدوي.

من يستفيد أكثر من كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة؟

يستفيد أكثر مديرو المركز وقادة الكشف والاستجابة ومالكو مخاطر تقنية المعلومات. ويستفيد كذلك مهندسو الأمن الذين يشغلون منصات SIEM وSOAR، لأنهم يحولون خيارات الكواشف والأدلة إلى مسارات عاملة.

كيف يختلف كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة عن دورة في أمن وكلاء الذكاء الاصطناعي؟

يدافع عن المؤسسة بالذكاء الاصطناعي بدلا من تأمين الوكلاء الذكية ذاتها. فدورة أمن الوكلاء تحصن المساعدات المستقلة، أما هنا فيضبط المشاركون الكواشف ويؤتمتون الاحتواء ويحمون نماذج الكشف من التهرب.

ماذا تعود به من تدريب كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة؟

تعود بخطة بنية لمركزك أنت. وتضم الكواشف مع عتبات قبولها وخطوط الأساس السلوكية والأدلة مع بوابات الموافقة ودفاعات النماذج والمسؤولين بالاسم.

كشف التهديدات بالذكاء الاصطناعي وأتمتة الاستجابة: الطريق إلى الأمام

توجه خطة بنية الدفاع بالذكاء الاصطناعي أولا قرار الكواشف التي تبقى في التشغيل وخطوات الاحتواء التي يمكن أن تعمل دون مراقبة. ويستخدمها مديرو المركز لإحاطة الإدارة العليا. وبعد أول حادث كبير يعالج وفقها، تستحق حدود الأتمتة المراجعة، فقد يثبت أمان أتمتة إجراءات كانت معلقة على الموافقة، وقد تحتاج إجراءات أخرى إلى بوابة بشرية.