JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة تدريبية في الذكاء الاصطناعي في الأمن السيبراني الصحي

1 – 5 أغسطس 2027

القاهرة

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة تدريبية في الذكاء الاصطناعي في الأمن السيبراني الصحي

المرجع: 2306_92 **التاريخ:** 1 – 5 أغسطس 2027 **المكان:** القاهرة **الرسوم:** GBP 4000

الذكاء الاصطناعي في الأمن السيبراني الصحي دورة تدريبية مدتها أسبوع لمديري أمن تقنية المعلومات في المستشفيات وقادة الأنظمة السريرية ومسؤولي المعلومات الصحية ومديري المخاطر، يخرج منها المشاركون بخطة الاستجابة الأمنية للذكاء الاصطناعي في الرعاية الصحية. فعصابات برامج الفدية تستهدف المستشفيات لأن توقف الأنظمة يهدد المرضى، بينما توسع مضخات التسريب المتصلة وأجهزة التصوير والخوارزميات التشخيصية سطح الهجوم باستمرار. تقدم جوبيتر برايم للتدريب دورة الذكاء الاصطناعي في الأمن السيبراني الصحي.

لماذا يهم الذكاء الاصطناعي في الأمن السيبراني الصحي الآن

يستخدم المهاجمون الأتمتة للعثور على الأنظمة السريرية غير المحدثة وصياغة رسائل تصيد موجهة لكوادر الأجنحة. وتربط المستشفيات مزيدا من الأجهزة السريرية ومحللات المختبر وخدمات السجل الصحي الإلكتروني السحابية، وكثير منها يصعب تحديثه. ويتوقع الأطباء والمرضى أن يبقى تحويل سيارات الإسعاف وإلغاء العمليات وتسرب السجلات أمرا نادرا. المستشفى الذي يحسن ذلك يكتشف الاختراق مبكرا ويحافظ على استمرار الرعاية، أما الذي يسيء فيعود إلى الورق ويؤخر العلاج ويفقد ثقة المرضى. تستند الدورة إلى معيار ISO/IEC 42001 لأنظمة إدارة الذكاء الاصطناعي، وإلى إطار Framework NIST AI Risk Management لإدارة مخاطر الذكاء الاصطناعي NIST AI RMF في تأمين النماذج السريرية.

المستفيدون من الذكاء الاصطناعي في الأمن السيبراني الصحي

- قادة الأمن الذين يديرون مراقبة المستشفى ومعالجة الحوادث واستخبارات التهديدات
- مالكو الأنظمة السريرية الذين يحافظون على توافر السجلات الإلكترونية وأنظمة التصوير والمختبر
- قادة الهندسة الطبية الحيوية الذين يحصرون الأجهزة الطبية المتصلة ويحدثونها
- مسؤولو المعلومات الذين يقررون من يصل إلى سجلات المرضى ولماذا
- قادة المخاطر الذين يقدرون التعرض السيبراني لمجلس الإدارة وشركات التأمين

تستفيد مجموعة المستشفيات أو الهيئة الصحية أكثر عندما يحضر قادة الأمن والأنظمة السريرية والهندسة الطبية الحيوية معا ويتدربون على سيناريو واحد لبرامج الفدية من بدايته إلى نهايته.

قدرات الذكاء الاصطناعي في الأمن السيبراني الصحي

يقرأ المشاركون طوابير التنبيهات وسجلات حصر الأجهزة وسجلات الوصول إلى الملفات من بيئات سريرية، ويقررون أين يطلق تعلم الآلة الإنذار وأين يؤكده المحلل.

- تقييم كشف الشذوذ على الشبكات السريرية مقابل حدود الإنذارات الكاذبة المقبولة — مركز العمليات الأمنية
- تصميم الدفاع ضد برامج الفدية وإجراءات التوقف التي تبقي الأجنحة عاملة — المديرون السريريون
- تحديد أولويات التجزئة والتحديث للأجهزة الطبية المتصلة — الهندسة الطبية الحيوية
- تطبيق مراقبة الوصول التي ترصد الاطلاع غير المعتاد على سجلات المرضى — مسؤولو المعلومات
- اختبار النماذج السريرية ضد التسميم والتهرب والمدخلات المتلاعب بها — مالكو النماذج
- إيصال التعرض السيبراني وجاهزية التعافي إلى مجالس الإدارة وشركات التأمين — لجان المخاطر

مصطلحات الذكاء الاصطناعي في الأمن السيبراني الصحي الأساسية

- كشف الشذوذ — نماذج تتعلم السلوك المعتاد للشبكة أو المستخدم وترصد الانحرافات التي قد تدل على اختراق.
- برامج الفدية — برمجيات خبيثة تشفر الأنظمة أو السجلات وتطلب مقابلا، وغالبا بعد سرقة نسخ منها.
- إنترنت الأشياء الطبية — أجهزة سريرية متصلة بالشبكة مثل مضخات التسريب والشاشات والماسحات تتبادل البيانات مع أنظمة المستشفى.
- تجزئة الشبكة — تقسيم شبكة المستشفى إلى مناطق كي لا ينتشر اختراق منطقة واحدة إلى الأنظمة السريرية.
- الهجوم العدائي — مدخلات مصممة عمدا تدفع النموذج إلى تصنيف خاطئ، مثل صور معدلة تخدع خوارزمية تشخيصية.
- تسميم بيانات التدريب — إفساد سجلات التدريب كي يتعلم النموذج أنماطا خاطئة يستغلها المهاجم لاحقا.

الذكاء الاصطناعي في الأمن السيبراني الصحي يوما بيوم

اليوم 1: مشهد التهديدات السريرية

- رسم سطح الهجوم في المستشفى — السجلات والأجهزة والروابط السحابية
- دراسات حالة لبرامج الفدية في المستشفيات والمختبرات — الأثر على المرضى
- استخدام المهاجمين للأتمتة — التصيد واكتشاف الثغرات
- اعتماديات التوقف السريري — أي الخدمات تتعطل أولا
- فحص نضج العمليات الأمنية — المراقبة والكوادر وأدلة الاستجابة

اليوم 2: تعلم الآلة لكشف التهديدات

- كشف الشذوذ في الشبكة — خطوط الأساس لحركة البيانات السريرية
- تحليلات سلوك المستخدمين — وصول غير معتاد إلى السجلات من الكوادر
- أتمتة فرز التنبيهات — ترتيب الحوادث أمام المحللين
- إثراء استخبارات التهديدات — مطابقة المؤشرات مع أصول المستشفى
- ضبط الكشف — الإنذارات الكاذبة مقابل الاختراقات الفائتة

اليوم 3: الأجهزة الطبية وسجلات المرضى

- حصر الأجهزة الطبية وتقدير مخاطرها — أولويات التحديث
- تجزئة الشبكة للأجهزة السريرية — احتواء الحركة الجانبية
- ضوابط الوصول إلى السجل الصحي الإلكتروني — أقل صلاحية للأطباء
- تصميم النسخ الاحتياطي والتعافي — استعادة السجلات بعد التشفير
- بنود الأمن مع الموردين — مصنعو الأجهزة ومزودو الخدمات السحابية

اليوم 4: تأمين النماذج السريرية

- الهجمات العدائية على النماذج التشخيصية — صور وإشارات معدلة
- تسميم بيانات التدريب — فحص مصدر مجموعات البيانات السريرية
- سرقة النماذج واستنتاج مدخلاتها — حماية الأوزان وبيانات المرضى
- وظيفة الإدارة في NIST AI RMF — الاستجابة لحوادث أمن النماذج
- ضوابط ISO/IEC 42001 — الملكية والمراقبة واعتماد التغيير

اليوم 5: تطبيق خطة الاستجابة الأمنية للذكاء الاصطناعي في الرعاية الصحية

- خريطة سطح الهجوم والتوقف من اليوم 1 — التعرض الابتدائي
- قواعد الكشف والفرز من اليوم 2 — معالجة التنبيهات
- ضمانات الأجهزة والسجلات من اليوم 3 — خيارات الاحتواء
- حماية النماذج السريرية من اليوم 4 — خطوات الضمان
- خطة الاستجابة الأمنية للذكاء الاصطناعي في الرعاية الصحية — نسخة مختبرة بتمرين محاكاة للاعتماد

تطبيق الذكاء الاصطناعي في الأمن السيبراني الصحي بعد الدورة

- تنفيذ تمرين محاكاة لبرامج الفدية مع مديري الأجنحة ومالكي الأنظمة السريرية، وحصر الخدمات التي تفتقر إلى إجراء للتوقف.
- ترتيب الأجهزة الطبية المتصلة حسب التعرض، والاتفاق مع الهندسة الطبية الحيوية على تجزئة الوحدات العشر الأعلى خطرا.

أسئلة حول الذكاء الاصطناعي في الأمن السيبراني الصحي

ما الذكاء الاصطناعي في الأمن السيبراني الصحي ولماذا يهم الآن؟

الذكاء الاصطناعي في الأمن السيبراني الصحي هو استخدام تعلم الآلة لكشف الهجمات على أنظمة المستشفى، وحماية النماذج السريرية نفسها. ويهم الآن لأن برامج الفدية تعطل رعاية المرضى والأجهزة المتصلة توسع التعرض.

ما الأدوار الأكثر استفادة من تدريب الذكاء الاصطناعي في الأمن السيبراني الصحي؟

يستفيد أكثر مديرو أمن تقنية المعلومات في المستشفيات وقادة الأنظمة السريرية ومسؤولو المعلومات الصحية ومديرو المخاطر. ويستفيد كذلك قادة الهندسة الطبية الحيوية لأنهم يؤمنون الأجهزة الطبية المتصلة.

كيف تختلف دورة الذكاء الاصطناعي في الأمن السيبراني الصحي عن دورة عامة في إدارة الأمن السيبراني؟

تركز الدورة على البيئة السريرية: أجهزة المرضى وسجلاتهم وتوقف الرعاية والنماذج التشخيصية، لا شبكات المكاتب. فتخطط الدفاعات حول سلامة المرضى إلى جانب حماية البيانات.

ماذا تعود به من دورة الذكاء الاصطناعي في الأمن السيبراني الصحي؟

تعود بخطة الاستجابة الأمنية للذكاء الاصطناعي في الرعاية الصحية، تحدد قواعد الكشف وضمانات الأجهزة والسجلات وحماية النماذج السريرية وخطوات التوقف بعد اختبارها في تمرين محاكاة.

الذكاء الاصطناعي في الأمن السيبراني الصحي: الطريق إلى الأمام

تعين خطة الاستجابة الأمنية للذكاء الاصطناعي في الرعاية الصحية على القرار الأول: أي قواعد الكشف وأي مقاطع الأجهزة تدخل التشغيل قبل دورة التدقيق القادمة. ويستخدمها مركز العمليات الأمنية ومالكو الأنظمة السريرية ومهندسو الأجهزة الطبية أثناء الحوادث والتمارين. وبعد أول تمرين أو تنبيه حقيقي تستحق إجراءات التوقف وحماية النماذج مراجعة جديدة، لأن المهاجمين يتكيفون سريعا مع الدفاعات الجديدة.