JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية للقادة

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية للقادة

مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية دورة تدريبية مدتها أسبوع للقادة غير التقنيين ومالكي المخاطر ومديري العمليات، يخرج منها المشاركون بموجز مجلس الإدارة للمرونة السيبرانية في عصر الذكاء الاصطناعي.
فالمهاجمون يوظفون تعلم الآلة لتوسيع التصيد الاحتيالي واستنساخ الأصوات والاستطلاع، بينما يعتمده المدافعون في الرصد، فصار على القادة الحكم على الجانبين معا. تقدم جوبيتر برايم للتدريب هذه الدورة في مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية.

لماذا تهم مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية الآن

تشكل ثلاث قوى هذا المجال اليوم: نماذج توليدية جعلت مكالمات التزييف العميق والرسائل المصممة لكل ضحية رخيصة الكلفة، ومجالس إدارة تنتظر بقاء الخدمات الحيوية ضمن حدود الاضطراب المحتمل، وموردون يدمجون تعلم الآلة في منتجات لا تستطيع المؤسسة فحصها. القائد الذي يحسن التعامل مع ذلك يحمي الخدمات الصحيحة أولا، أما من يغفل عنه فيكتشف حدود تحمله أثناء الانقطاع. وتستند الدورة إلى إطار NIST Cybersecurity Framework 2.0 المعروف اختصارا NIST CSF 2.0، وهو إطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتقنية، بما فيه وظيفة الحوكمة Govern.

المستفيدون من مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية

- مالكو خدمات الأعمال المسؤولون عن استمرار العمليات الموجهة للعملاء أثناء الاضطراب
- مالكو المخاطر الذين يقيمون التعرض السيبراني ويعتمدون خيارات المعالجة في نطاقهم
- مديرو العمليات الذين ينفذون مهام الاستعادة والحلول البديلة والإجراءات اليدوية الاحتياطية
- رعاة مبادرات الأتمتة وتعلم الآلة الذين يقبلون المخاطر المتبقية لها
- أعضاء اللجان الذين يدققون تقارير المرونة ويناقشون طلبات الاستثمار

تستفيد المجموعة القيادية أكثر حين ترسل قادة الخدمات والمخاطر والعمليات معا، فيعودون برؤية موحدة لحدود التحمل.

قدرات مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية

يحول المشاركون التهديدات المدفوعة بتعلم الآلة إلى خيارات على مستوى الخدمة.

- تقييم كيف يمكن للتزييف العميق والتصيد المؤتمت والتلاعب بالنماذج أن يصل إلى الخدمات الحيوية — مالكو المخاطر عند تحديد الأولويات
- موازنة فوائد تعلم الآلة وحدوده في أدوات الرصد والاستجابة — لجان الاستثمار
- تحديد حدود تحمل الأثر للخدمات الحيوية — اعتماد الإدارة التنفيذية لأولويات الاستعادة
- تصميم سيناريوهات اضطراب حادة ومعقولة لاختبار المرونة — مديرو العمليات ومالكو الخدمات
- اختبار الاعتماد على الأطراف الثالثة والموردين بحثا عن تعرض خوارزمي خفي — مسؤولو المشتريات والموردين
- إيصال وضع المرونة واحتياجات المعالجة بلغة واضحة — مجلس الإدارة ولجنة التدقيق

مصطلحات مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية الأساسية

- المرونة التشغيلية — قدرة المؤسسة على منع الاضطراب والتكيف معه والاستجابة له والتعافي منه.
- حد تحمل الأثر — أقصى مستوى من الاضطراب في خدمة حيوية تقبله المؤسسة، ويعبر عنه غالبا بمدة زمنية.
- الخدمة الحيوية — خدمة يسبب تعطلها ضررا لا يحتمل للعملاء أو للمؤسسة أو للسوق الأوسع.
- التزييف العميق — صوت أو صورة أو فيديو اصطناعي ينتجه تعلم الآلة لانتحال شخصية حقيقية.
- تعلم الآلة العدائي — أساليب تتلاعب بمدخلات النموذج أو بيانات تدريبه ليعطي نظام الذكاء الاصطناعي نتائج خاطئة.
- السيناريو الحاد المعقول — اضطراب صعب لكنه واقعي يستخدم لاختبار بقاء الخدمات ضمن حدود التحمل.

مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية يوما بيوم

اليوم 1: مشهد التهديدات في عصر الذكاء الاصطناعي

- أنماط هجمات الذكاء الاصطناعي التوليدي — قياس تعرض التنفيذيين والموظفين
- حالات احتيال التزييف العميق بالصوت والفيديو — تحصين خطوات اعتماد المدفوعات
- الاستطلاع والتصيد المؤتمت على نطاق واسع — ترتيب أولويات الإنفاق على التوعية
- أساسيات تسميم النماذج وحقن الأوامر — مساءلة ادعاءات الموردين حول الذكاء الاصطناعي
- مقارنة حوادث القطاع البنكي والرعاية الصحية — دروس من إخفاقات خدمية حديثة

اليوم 2: الذكاء الاصطناعي في صف المدافعين

- الرصد بتعلم الآلة في عمليات الأمن — وضع توقعات واقعية
- أتمتة فرز التنبيهات — الموازنة بين السرعة والإنذارات الكاذبة
- وظيفة الحوكمة في NIST CSF 2.0 — إسناد مساءلة القيادة عن المخاطر السيبرانية
- سجل استخدامات الذكاء الاصطناعي — كشف النماذج الخفية في وحدات الأعمال
- خريطة اعتماد الموردين على الخوارزميات — كشف مخاطر التركز والارتهان للمورد

اليوم 3: الخدمات الحيوية وحدود تحمل الأثر

- معايير تحديد الخدمات — اختيار العمليات التي تهم فعلا
- رسم الخدمة من طرف إلى طرف — تتبع الأفراد والأنظمة والموردين
- وضع حدود تحمل الأثر — تحويل الضرر إلى أقصى مدد انقطاع
- الحلول البديلة والإجراءات اليدوية للاستعادة — تمويل خيارات استمرارية متناسبة
- مسارات التصعيد عند تجاوز الحدود — تحديد من يتصرف ومتى

اليوم 4: اختبار المرونة تحت الضغط

- تصميم السيناريو الحاد المعقول — توسيع الافتراضات دون مبالغة خيالية
- تمرين محاكاة مكتبي بمحفز تزييف عميق — التدرب على قرارات التنفيذيين
- سيناريوهات برمجيات الفدية وسلامة البيانات — مقارنة خيارات الاسترجاع
- سجل نتائج التمارين — ترتيب الثغرات لتمويل المعالجة
- بروتوكول اتصالات الأزمات — إبلاغ العملاء والموظفين والشركاء

اليوم 5: التطبيق العملي لموجز مجلس الإدارة للمرونة السيبرانية

- ملخص التعرض للتهديدات — تطبيق أنماط هجمات اليوم 1 على خدمات المؤسسة
- مراجعة بيانات حدود التحمل — تطبيق خرائط الخدمات على طلبات الاعتماد
- سرد نتائج التمارين — تطبيق نتائج الاختبار على طلبات المعالجة
- لوحة مؤشرات المرونة — اختيار مؤشرات يتابعها مجلس الإدارة
- موجز مجلس الإدارة للمرونة السيبرانية — استكمال التهديدات وحدود التحمل وخطة المعالجة

تطبيق مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية بعد الدورة

- قيادة تمرين محاكاة مدته ساعة حول طلب دفع بتزييف عميق، مع تسجيل الثغرات في خطوات الاعتماد.
- رسم خدمة حيوية واحدة من طرف إلى طرف واقتراح حد تحمل الأثر لها.

أسئلة حول مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية

ما مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية، ولماذا تهم الآن؟

هي الحكم على كيفية تغيير تعلم الآلة للتهديدات السيبرانية مع إبقاء الخدمات الحيوية ضمن حدود الاضطراب المحتمل. وتهم الآن لأن الأدوات التوليدية الرخيصة تتيح للمهاجمين انتحال شخصيات التنفيذيين وتوسيع الاحتيال أسرع مما تتكيف معه الضوابط التقليدية.

من أكثر المستفيدين من تدريب مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية؟

يستفيد أكثر مالكو الخدمات ومالكو المخاطر ومديرو العمليات. فهم من يتخذ القرارات بشأن حدود التحمل وتمويل الاستعادة والاعتماد على الموردين.

كيف تختلف مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية عن دورة تقنية في الاستجابة للحوادث؟

تعمل على مستوى الخدمات وحدود التحمل وقرارات مجلس الإدارة لا على أدوات التحليل الجنائي أو تحليل السجلات. فالدورة التقنية تدرب المحللين على احتواء الاختراق، أما هذا المجال فيعد القادة لتقرير ما يجب أن يستمر في العمل.

ماذا تعود به من تدريب مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية؟

تعود بموجز مجلس الإدارة للمرونة السيبرانية. يلخص التهديدات المدفوعة بتعلم الآلة على خدماتك وحدود التحمل المقترحة ونتائج التمارين والمعالجة التي تحتاج إلى اعتمادها.

مخاطر الذكاء الاصطناعي السيبرانية والمرونة التشغيلية: الطريق إلى الأمام

يوجه موجز مجلس الإدارة للمرونة السيبرانية في عصر الذكاء الاصطناعي أول قرار حول الخدمات الحيوية التي تحصل على استثمار الاستعادة. ويستخدمه مالكو الخدمات ومالكو المخاطر واللجنة التنفيذية لاعتماد حدود التحمل ومتابعة المعالجة. وبعد أول دورة تمارين يستحق ملخص التعرض للتهديدات المراجعة، لأن استخدام المهاجمين للأدوات التوليدية يتغير بسرعة وتتبدل معه افتراضات مخاطر الانتحال.