

دورة التهديدات السيبرانية المدعومة بالذكاء الاصطناعي والمرونة التشغيلية واستجابة القيادات

3 – 7 يناير 2027

كوالالمبور





دورة التهديدات السيبرانية المدعومة بالذكاء الاصطناعي والمرونة التشغيلية واستجابة القيادات

المراجع: 19172_256 التاريخ: 3 - 7 يناير 2027 المكان: كوالالمبور الرسوم: GBP 4000

ملخص البرنامج

التهديدات السيبرانية المدعومة بالذكاء الاصطناعي والمرونة واستجابة القيادات محور دورة تدريبية تمتد 5 أيام بمستوى إداري إلى استراتيجي للقيادات العليا من غير المتخصصين في التقنية، ويخرج منها كل مشارك دليل تنفيذي للمرونة السيبرانية. فالمهاجمون يستخدمون الذكاء الاصطناعي لانتحال شخصيات الزملاء وتوسيع نطاق الاحتيال، بينما تبنى المؤسسات أنظمة ذكاء اصطناعي تضيف نقاط ضعف جديدة. ويتدرج البرنامج من التهديد والتعرض، مروراً بتصميم المرونة ومخاطر أنظمة الذكاء الاصطناعي، إلى قرارات الأزمة وتمارين الاستجابة. يقدم هذا البرنامج في التهديدات السيبرانية المدعومة بالذكاء الاصطناعي والمرونة مارس للتدريب المملكة المتحدة.

المبررات المؤسسية

تحسم الحوادث السيبرانية في ساعاتها الأولى، ومن يتخذ القرار فيها نادراً ما يكون تقنياً. والقيادات التي تدرك كيف يغير الذكاء الاصطناعي أساليب الهجوم، وأي الخدمات لا يجوز أن تتوقف، ومن يملك صلاحية إقرار خطوات التعافي، تتحرك أسرع وتتواصل بصوت واحد وتحمي الخدمات التي تعنى بها الجهات الرقابية والعملاء قبل غيرها.

- مدة تعطل الخدمة: تقصر حين تتفق القيادة على أولويات التعافي وصلاحيات القرار قبل وقوع الحادث.
- التعرض لاحتياال الانتحال: ينخفض حين تعالج قواعد التحقق وإجراءات التوعية الخداع المولد بالذكاء الاصطناعي.
- جودة رقابة مجلس الإدارة: تتحسن حين يطلب القادة أدلة على المرونة بدلا من تطمينات عامة.

المبادئ والأساس المعرفي

- ISO/IEC 27001، معيار إدارة أمن المعلومات: تؤطر متطلباته أسئلة المخاطر والضوابط التي تطرحها القيادات في الجلستين 1 و 2.
- ISO 22301، معيار إدارة استمرارية الأعمال: تشكل متطلباته تحليل الأثر وأولويات التعافي في الجلسة 3.
- NIST Cybersecurity Framework، إطار الأمن السيبراني: تنظم وظائفه الخمس عمل الأزمة والتعافي في الجلستين 4 و 5.
- ISO/IEC 42001، معيار نظام إدارة الذكاء الاصطناعي: توجه متطلباته الرقابة على أنظمة الذكاء الاصطناعي في الجلسة 2.



المشاركون المستهدفون

- المدبرون المسؤولون عن خدمات يجب أن تستمر أثناء الحادث السيبراني.
- التنفيذيون الذين يجلسون في لجان الأزمات والحوادث ويقرون قرارات التعافي.
- رؤساء الوظائف الذين يعتمدون على التقنية دون أن يديروها.
- مستشارو مجالس الإدارة الذين يراجعون الإدارة في مخاطر الأمن السيبراني والذكاء الاصطناعي.

يخدم البرنامج المصارف وقطاع الطاقة والرعاية الصحية والجهات الحكومية وشركات الاتصالات.

مخرجات التعلم

1. سيكون المشاركون قادرين على تقييم كيف يغير الذكاء الاصطناعي أساليب الهجمات السيبرانية وسرعتها ونطاقها على مؤسساتهم.
2. سيكون المشاركون قادرين على تشخيص التعرض الناشئ عن استخدام المؤسسة لأنظمة الذكاء الاصطناعي ومورديها.
3. سيكون المشاركون قادرين على بناء حدود تحمل الأثر وأولويات التعافي للخدمات الحرجة.
4. سيكون المشاركون قادرين على ترتيب أولويات إجراءات الحماية بحسب الأثر على الأعمال لا بحسب التفاصيل التقنية.
5. سيكون المشاركون قادرين على تبرير قرارات الأزمة، ومنها المفاضلة بين التواصل والتعافي، تحت ضغط الوقت.
6. سيكون المشاركون قادرين على تصميم دليل تنفيذي للمرونة السيبرانية يحدد أصحاب القرار بالاسم.

هيكل البرنامج

اليوم 1: التهديدات السيبرانية المدعومة بالذكاء الاصطناعي للقيادات غير التقنية

كيف يغير الذكاء الاصطناعي هوية المهاجم وأسلوبه وسرعته؟

- مراحل الهجوم بلغة مبسطة
- التصيد وانتحال الصوت والفيديو المولد بالذكاء الاصطناعي
- نماذج أعمال برامج الفدية والابتزاز
- صيغة الإحاطة بالتهديدات للتنفيذيين
- مراجعة حالتين لحوادث في قطاعين

اليوم 2: التعرض ومخاطر أنظمة الذكاء الاصطناعي

أين تتعرض المؤسسة للخطر، ومنه عبر استخدامها هي للذكاء الاصطناعي؟



- خريطة التعرض للأصول والخدمات الحرجة
- أسئلة المخاطر والضوابط وفق ISO/IEC 27001 للقيادات
- مراجعة الاعتماد على الموردين والخدمات السحابية
- إساءة استخدام أنظمة الذكاء الاصطناعي وتسرب البيانات والتلاعب بالنماذج
- قائمة فحص الرقابة على أدوات الذكاء الاصطناعي وفق ISO/IEC 42001

اليوم 3: تصميم المرونة التشغيلية

أي الخدمات لا يجوز أن تتوقف، وكم تحتمل من التعطل؟

- تحليل الأثر على الأعمال وفق ISO 22301
- بيانات حدود تحمل الأثر
- أولويات التعافي وتسلسل الاعتماديات
- خيارات النسخ الاحتياطي والاسترداد والحلول اليدوية البديلة
- جدول المفاضلة في استثمارات المرونة

اليوم 4: قيادة الأزمة وقرارات الاستجابة

من يقرر ماذا في الساعات الأولى من الأزمة السيبرانية؟

- وظيفتا الاستجابة والتعافي في إطار NIST للتنفيذيين
- أدوار فريق الأزمة وصلاحيات القرار
- إطار القرار في الفدية والإفصاح والإيقاف
- خطة التواصل مع أصحاب المصلحة والإعلام
- محاكاة زمنية لحادث

اليوم 5: تطبيق المرونة أمام التهديدات السيبرانية المدعومة بالذكاء الاصطناعي في دليل تنفيذي

هل الدليل جاهز للاعتماد والتمرين عليه؟

- تطبيق إحاطة التهديدات من الجلسة 1 على مؤسسة مختارة
- تطبيق نتائج التعرض من الجلسة 2 على الخدمات ذات الأولوية
- اختبار حدود التحمل من الجلسة 3 مقابل نتيجة المحاكاة
- تحديد أصحاب القرار ومحفزات التصعيد
- إنجاز الدليل التنفيذي للمرونة السيبرانية



المنهجية

يقوم البرنامج على محاكاة السيناريوهات وتحليل الحالات، إذ يتناول المشاركون حادثاً مرحلياً في فريق قيادي مختلط، فيتخذون قراراتهم بمعلومات ناقصة ثم يراجعون كلفة خياراتهم، ولا تستخدم أي أدوات برمجية أو تقنية.

- نشاط مقترح: تقدير طلب دفع مشتبه به بصوت منتحل ووضع قاعدة تحقق.
- نشاط مقترح: ترتيب الخدمات الحرجة والاتفاق على حدود التحمل في لجنة تمثيلية.
- نشاط مقترح: إحاطة مجلس إدارة محاكى عن حادث بعد ساعاته الاثنتي عشرة الأولى.

المخرج الختامي

يعد كل مشارك دليلاً تنفيذياً للمرونة السيبرانية لمؤسسة أو وحدة أعمال بعينها، يتضمن إحاطة بالتهديدات وخريطة للتعرض وحدودا لتحمل الأثر وأولويات للتعافي وصلاحيات للقرار وبيانات تواصل جاهزة ومحفزات للتصعيد. ويستخدم لإحاطة الفريق التنفيذي ولإجراء أول تمرين استجابة.

الأسئلة الشائعة

هل يناسب التدريب على التهديدات السيبرانية المدعومة بالذكاء الاصطناعي القيادات من غير ذوي الخلفية التقنية؟

نعم، فالتدريب على التهديدات السيبرانية المدعومة بالذكاء الاصطناعي مصمم للمديرين والتنفيذيين من غير المتخصصين، ويفترض مسؤولية عن خدمات أو قرارات لا خبرة في الأمن أو البرمجة.

ما المعايير التي تقوم عليها التهديدات السيبرانية المدعومة بالذكاء الاصطناعي والمرونة في هذا البرنامج؟

يقوم العمل على التهديدات السيبرانية المدعومة بالذكاء الاصطناعي والمرونة على ISO/IEC 27001 و ISO 22301 وإطار NIST Cybersecurity Framework و ISO/IEC 42001g لأنظمة الذكاء الاصطناعي.

كيف يستخدم الدليل الناتج عن التدريب على التهديدات السيبرانية المدعومة بالذكاء الاصطناعي والمرونة في العمل؟

تستخدم الدليل لإحاطة الفريق التنفيذي وتحديد أصحاب القرار وتمارين الاستجابة، كما يمنح مجالس الإدارة أساساً واضحاً لمساءلة الإدارة عن المرونة.