

دورة الدفاع السيبراني للمستشفيات للقيادات التنفيذية: الكشف والأجهزة الطبية والتعافي بالذكاء الاصطناعي

2027 – 21 يناير

مسقط





دورة الدفاع السيبراني للمستشفيات للقيادات التنفيذية: الكشف والأجهزة الطبية والتعافي بالذكاء الاصطناعي

المرجع: 694_34088 التاريخ: 17 - 21 يناير 2027 المكان: مسقط الرسوم: GBP 4300

ملخص البرنامج

الدفاع السيبراني للمستشفيات محور دورة تدريبية تمتد أسبوع لقيادات المستشفيات ومسؤولي أمن المعلومات ومديري الصحة الرقمية، ويخرج منها كل مشارك بخطة مرونة سيبرانية لمستشفى واحد. تعتمد الخدمات السريرية اليوم على أجهزة متصلة وسجلات مشتركة وموردين، ويستخدم المهاجمون الأتمتة للوصول إليها. وينتقل البرنامج من المخاطر إلى الكشف والأجهزة الطبية والتعافي والرقابة على أدوات الأمن بالذكاء الاصطناعي، بحالات من المستشفيات والمختبرات وشركات التأمين. تقدم مارس للتدريب المملكة المتحدة هذا البرنامج في الدفاع السيبراني للمستشفيات لمجموعات من منظمات مختلفة.

المبررات المؤسسية

حين يعطل برنامج فدية أو عطل في جهاز جناح كامل، يقاس الضرر أولاً بتأخر الرعاية ثم بالمال. والقائد الذي يربط الأنظمة السريرية بحسب الضرر المحتمل، ويعرف حدود الكشف بالذكاء الاصطناعي، ويتدرب على التعافي، يقرر أسرع ويشرح قراراته لمجلس الإدارة وللمرضى بالأدلة.

- استمرارية الخدمة السريرية: تتحسن حين تتفق الجهات مسبقاً على الأنظمة الحرجة وإجراءات التوقف وترتيب التعافي.
- انكشاف بيانات المرضى: ينخفض حين تراجع ضوابط الوصول والسجلات والموردين في ضوء مسارات البيانات الفعلية.
- زمن الكشف والاستجابة: يقصر حين تختبر التنبيهات ومسارات التصعيد وصلاحيات القرار في تمارين عملية.

المبادئ والأساس المعرفي

- إطار الأمن السيبراني NIST Cybersecurity Framework: يوفر بنية التحديد والحماية والكشف والاستجابة والتعافي التي تنتظم بها الجلسات من 1 إلى 4.
- ممارسات الأمن السيبراني للقطاع الصحي HHS 405d: تقدم تهديدات وممارسات خاصة بالصحة تشكل سجل المخاطر الذي يبنى في الجلسة 1.
- قاعدة الأمن HIPAA Security Rule: تحدد ضمانات حماية المعلومات الصحية المحمية التي تربط بالضوابط في الجلسة 2.



المشاركون المستهدفون

- القيادات التنفيذية في المستشفيات التي تقبل مخاطر الأمن السيبراني نيابة عن الخدمات السريرية.
- مسؤولو أمن المعلومات الذين يشرحون أدوات الكشف والحوادث لزملاء غير تقنيين.
- مديرو الصحة الرقمية وتقنية المعلومات الذين يشترون الأنظمة السريرية ويربطونها ويدعمونها.
- قادة الهندسة السريرية والأجهزة الطبية الحيوية المسؤولون عن الأجهزة الطبية المتصلة.
- مديرو المخاطر والشؤون القانونية واستمرارية الأعمال الذين يعدون الاستجابة للحوادث الكبرى.

يأتي المشاركون عادة من مجموعات المستشفيات وشركات التأمين الصحي والمختبرات التشخيصية وجهات الصحة العامة.

مخرجات التعلم

1. سيكون المشاركون قادرين على ترتيب الأنظمة السريرية والبيانات بحسب الضرر الذي يسببه فقدانها.
2. سيكون المشاركون قادرين على تشخيص مواطن الضعف في ترتيبات الوصول والموردين والأجهزة باستخدام سجل المخاطر.
3. سيكون المشاركون قادرين على تقييم أدوات الكشف بالذكاء الاصطناعي في ضوء الإنذارات الكاذبة والنقاط العمياء واحتياجات البيانات.
4. سيكون المشاركون قادرين على بناء تسلسل للاستجابة لبرامج الفدية والتعافي منها للخدمات السريرية.
5. سيكون المشاركون قادرين على تبرير الضوابط والرقابة على أدوات الأمن بالذكاء الاصطناعي أمام مجلس الإدارة.

هيكل البرنامج

اليوم 1: مخاطر الدفاع السيبراني للمستشفيات والأولويات السريرية

ما الأنظمة والبيانات الأهم لرعاية المرضى، وما الذي يهددها؟

- خريطة اعتماد الخدمات السريرية
- جرد مسارات بيانات المرضى
- فهرس سيناريوهات التهديد
- مواعمة وظائف إطار NIST Cybersecurity Framework
- سجل المخاطر القائم على الضرر

اليوم 2: الوصول والموردون وضمانات البيانات

من يستطيع الوصول إلى سجلات المرضى وأنظمتهم، وكيف يثبت ذلك؟



- مراجعة صلاحيات الوصول المرتفعة
- استبيان مخاطر اتصال الموردين
- مصفوفة ربط الضمانات بالضوابط
- معيار السجلات ومسار التدقيق
- تقييم التعرض للتصيد

اليوم 3: الكشف بالذكاء الاصطناعي والأجهزة الطبية المتصلة

ماذا يستطيع الكشف بالذكاء الاصطناعي أن يرى، وكيف تحمى الأجهزة التي يتعذر تحديثها؟

- حالات استخدام كشف الشذوذ
- اختبار الإنذارات الكاذبة والنقاط العمياء
- جرد الأجهزة الطبية وخطة العزل الشبكي
- إحاطة عن استخدام المهاجمين للذكاء الاصطناعي
- بطاقة تقييم لاختيار أداة الكشف

اليوم 4: مرونة مواجهة برامج الفدية والتعافي

كيف تستمر الخدمات وتعود بالترتيب الصحيح بعد الهجوم؟

- بطاقات إجراءات التوقف
- خطة اختبار النسخ الاحتياطي والاستعادة
- تسلسل أولويات التعافي
- سجل قرارات الحادث
- بيان التواصل مع المرضى والجمهور

اليوم 5: خطة المرونة السيبرانية لمستشفى واحد

هل تشكل السجلات السابقة خطة واحدة يستطيع القادة تشغيلها؟

- تطبيق سجل المخاطر القائم على الضرر من الجلسة 1
- اختبار بطاقة تقييم اختيار أداة الكشف من الجلسة 3
- التدريب على تسلسل أولويات التعافي من الجلسة 4
- وضع قواعد الرقابة على أدوات الأمن بالذكاء الاصطناعي
- إنجاز خطة المرونة السيبرانية للمستشفى



المنهجية

يقوم البرنامج على تمارين منظمة تعتمد على حالة مشتركة لمجموعة مستشفيات تعرضت لبرنامج فدية عبر وصلة مورد. يعمل المشاركون على سجلات مخاطر وعينات تنبيهات وجدول تعاف جاهزة، ثم يكيفون كل مخرج مع مؤسستهم ويقارنون خياراتهم بزملاء من قطاعات أخرى.

- نشاط مقترح: ترتيب عشرة أنظمة سريرية بحسب الضرر والاتفاق على ترتيب التعافي.
- نشاط مقترح: فحص مجموعة تنبيهات صادرة عن الذكاء الاصطناعي وتحديد ما يستدعي التصعيد.
- نشاط مقترح: إحاطة مجلس إدارة في لعب أدوار عن حادث وقع ليلاً.

المخرج الختامي

يعد كل مشارك خطة مرونة سيبرانية لمستشفى واحد. وتضم الخطة سجل مخاطر قائماً على الضرر، وقائمة ضوابط الوصول والموردين، وقرار اختيار أداة الكشف، وتسلسل التعافي، وتقويم رقابة على أدوات الأمن بالذكاء الاصطناعي. وتستخدم الخطة في العمل لإحاطة مجلس الإدارة ووضع شروط الموردين وإعداد تمرين على الحوادث.

الأسئلة الشائعة

هل يناسب تدريب الدفاع السيبراني للمستشفيات القيادات التنفيذية التي ليست لها خلفية تقنية؟

نعم، فالدفاع السيبراني للمستشفيات يدرس عبر حالات ونماذج جاهزة، ويفترض خبرة في إدارة المستشفيات أو العمليات السريرية أو المخاطر أو تقنية المعلومات دون مهارات برمجة أو هندسة أمنية.

على أي أطر يقوم تدريب الدفاع السيبراني للمستشفيات؟

يقوم تدريب الدفاع السيبراني للمستشفيات على NIST Cybersecurity Framework وممارسات HHS 405d للأمن السيبراني في القطاع الصحي وضمانات HIPAA Security Rule لحماية المعلومات الصحية.

كيف تستخدم الخطة الناتجة عن تدريب الدفاع السيبراني للمستشفيات في العمل؟

تستخدم خطة المرونة لإحاطة مجلس الإدارة، ووضع شروط للموردين، واختيار أدوات الكشف، وإجراء تمرين تعاف مع الفرق السريرية والتقنية.



بماذا يختلف الدفاع السيبراني للمستشفيات عن تدريب التوعية العامة بالأمن السيبراني؟

يعالج الدفاع السيبراني للمستشفيات استمرارية الخدمة السريرية والأجهزة الطبية المتصلة وبيانات المرضى والرقابة على أدوات الأمن بالذكاء الاصطناعي، بينما يركز تدريب التوعية العامة على سلوك الموظفين مثل اكتشاف رسائل التصيد.