CONCEPT

الأمن السيبراني في القطاع الصحي: حماية أنظمة المستشفيات والأجهزة الطبية وبيانات المرضى

4 – 8 يناير 2027

دبي - فندق خمس نجوم في وسط الأعمال



الأمن السيبراني في القطاع الصحي: حماية أنظمة المستشفيات والأجهزة الطبية وبيانات المرضى

المرجع: 975_21967 **التاريخ:** 4 – 8 يناير 2027 **المكان:** دبي - فندق خمس نجوم في وسط الأعمال **الرسوم:** SAR 21450

مقدمة:

الأمن السيبراني في القطاع الصحي دورة مدتها أسبوع لفرق تقنية المعلومات وأمن المعلومات والهندسة الطبية الحيوية والمعلوماتية السريرية وحماية البيانات الصحية في المستشفيات، يخرج منها المشاركون بسجل مخاطر سيبرانية صحية ودليل للتوقف السريري. تعمل المستشفيات على السجل الصحي الإلكتروني وأرشيف الصور الطبية وأنظمة المختبر والأجهزة الطبية المتصلة، فيتحول أي انقطاع ببرمجيات الفدية أو تسرب للبيانات إلى مشكلة في سلامة المرضى وسرية معلوماتهم لا مجرد عطل تقني. والمشاركون ممن يدعمون الأنظمة السريرية في عملهم، ويطبقون كل أسلوب على دراسات حالة من مستشفيات متنوعة. وتقدم كور كونسبت هذه الدورة في الأمن السيبراني الصحي.

أهداف الدورة:

- رسم خريطة الأنظمة السريرية والأجهزة الطبية المتصلة وتدفقات بيانات المرضى في المستشفى وترتيب تعرضها السيبراني حسب الأثر السريري
- تطبيق إدارة المخاطر وفق IEC 80001-1 معيار إدارة مخاطر شبكات تقنية المعلومات التي تضم أجهزة طبية على الشبكات الحاملة للأجهزة الطبية وتحديد مناطق تجزئة الأنظمة السريرية
- إدارة أمن الأجهزة الطبية من الشراء حتى الإخراج من الخدمة بالتعاون مع المصنعين باستخدام بيانات SBOM قائمة مكونات البرمجيات ونماذج MDS2 نموذج إفصاح المصنع عن أمن الجهاز واتفاقيات التحديثات الأمنية
- ضبط الهوية والصلاحيات واتصالات الموردين في مسارات العمل السريرية دون تأخير رعاية المرضى
- تنسيق الاستجابة للحوادث السيبرانية وإجراءات التوقف السريري التي تبقي الأجنحة والأشعة والمختبر والصيدلية في الخدمة
- بناء سجل المخاطر السيبرانية الصحية ورفع تقارير المخاطر السيبرانية إلى قيادة المستشفى بلغة سلامة المرضى

الفئة المستهدفة:

- فرق البنية التحتية والتطبيقات في تقنية المعلومات بالمستشفيات المسؤولة عن السجل الصحي الإلكتروني وأرشيف الصور الطبية وأنظمة المختبر والصيدلية
- وحدات أمن المعلومات المسؤولة عن المراقبة ومعالجة الثغرات والاستجابة للحوادث في البيئات السريرية
- فرق الهندسة الطبية الحيوية والهندسة السريرية المسؤولة عن حصر الأجهزة الطبية المتصلة وصيانتها والتنسيق مع المصنعين
- فرق المعلوماتية السريرية المسؤولة عن إعداد الأنظمة وصلاحيات المستخدمين وتصميم مسارات العمل السريرية
- وحدات حماية البيانات الصحية والخصوصية المسؤولة عن سرية سجلات المرضى ومعالجة حوادث التسرب

محاور الدورة:

اليوم 1: لماذا يستهدف القطاع الصحي ومشهد تقنية المعلومات السريرية

- ملف التهديدات في القطاع الصحي ودوافع سرقة بيانات المرضى
- خريطة التطبيقات السريرية من السجل الصحي الإلكتروني إلى أنظمة الأشعة والمختبر والصيدلية
- بناء سجل أصول الأجهزة الطبية المتصلة وإنترنت الأشياء الطبية
- سلسلة أثر برمجيات الفدية من تشفير الخوادم إلى تحويل سيارات الإسعاف
- خط الأساس للتعرض السيبراني السريري بقائمة تحقق للوضع الحالي

اليوم 2: معايير أمن المعلومات الصحية وبنية الشبكة السريرية

- إدارة مخاطر شبكات تقنية المعلومات الطبية وفق IEC 80001-1
- متطلبات دورة حياة أمن البرمجيات الصحية وفق IEC 81001-5-1 معيار أمن البرمجيات الصحية
- ضوابط أمن المعلومات في المنشآت الصحية وفق ISO 27799 معيار أمن المعلومات في الصحة
- أمن واجهات تبادل البيانات السريرية عبر HL7 وDICOM معايير تبادل البيانات والصور الطبية
- مناطق تجزئة الشبكة السريرية للأجهزة والأشعة وشبكة الزوار

اليوم 3: الأجهزة الطبية والوصول السريري وحماية بيانات المرضى

- مراجعة نموذج MDS2 والبنود الأمنية في عقود شراء الأجهزة
- تحليل SBOM لتتبع ثغرات الأجهزة الطبية
- الضوابط التعويضية للأجهزة القديمة وتنسيق التحديثات الأمنية مع المصنع
- إدارة الهوية السريرية لمحطات العمل المشتركة وتسجيل الدخول السريع بالبطاقة
- ضوابط سرية سجلات المرضى والتشفير وسجلات تدقيق الوصول

اليوم 4: مخاطر الموردين والمراقبة بالذكاء الاصطناعي والاستجابة للحوادث والتوقف السريري

- قواعد الوصول عن بعد للمصنعين والموردين الخارجيين
- كشف الأنماط الشاذة في حركة الشبكة السريرية بمساعدة الذكاء الاصطناعي
- أدوار الاستجابة للحوادث الصحية بين فرق الأمن والفرق السريرية وفرق الاتصال
- إجراءات التوقف السريري بالنماذج الورقية والاطلاع على السجلات للقراءة فقط
- توعية الكوادر السريرية بالإبلاغ عن التصيد ومخاطر مشاركة بيانات الدخول

اليوم 5: دراسة حالة: سجل المخاطر السيبرانية الصحية ودليل التوقف

- إحاطة مستشفى الحالة بالأنظمة والأجهزة والموردين وتدفقات البيانات
- بناء سجل المخاطر السيبرانية الصحية بتقييم الأثر السريري
- تمرين طاولة للتوقف إثر انقطاع ببرمجيات الفدية في قسم الأشعة
- لوحة المخاطر السيبرانية وحزمة التقارير لقيادة المستشفى
- استكمال دليل التوقف السريري والاستجابة للحوادث ومراجعة الأقران

المهارات التي ستكتسبها:

- رسم خريطة الأصول السريرية
- تقييم مخاطر شبكات تقنية المعلومات الطبية
- إدارة أمن الأجهزة الطبية
- حوكمة الوصول السريري
- ضبط وصول الموردين
- حماية سرية بيانات المرضى
- تخطيط التوقف السريري
- الإبلاغ عن المخاطر السيبرانية الصحية

لماذا تحضر هذه الدورة:

- العودة بسجل مخاطر سيبرانية صحية ودليل للتوقف السريري تعتمدهما اللجنة التوجيهية للأمن والقيادة السريرية في المستشفى
- تحديد الأجهزة الطبية القديمة التي تعزل أو تحدث عبر المصنع أو تخرج من الخدمة مع توثيق سبب كل قرار
- تجنب انقطاع الخدمة المطول عند تعطل الأنظمة السريرية لأن الأجنحة والأقسام التشخيصية تعرف إجراءات التوقف مسبقا
-

نقل ممارسات الدخول الآمن والإبلاغ عن التصيد والتعامل مع بيانات المرضى إلى الأطباء والممرضين وفرق القسم في عملهم اليومي

الخاتمة:

بعد عودة المشاركين يستطيع مسؤول الأمن في المستشفى ورئيس الهندسة السريرية ووحدة حماية البيانات استخدام سجل المخاطر السيبرانية الصحية لتحديد أولويات الاستثمار في تجزئة الشبكة واستبدال الأجهزة وضوابط الوصول، بينما يمنح دليل التوقف السريري مديري الأجنحة والأقسام إجراء مجربا لاستمرار الرعاية أثناء الانقطاع. وبذلك يصبح الأمن السيبراني في القطاع الصحي بندا ثابتا على جدول أعمال القيادة بدل أن يكون رد فعل على الحوادث. وبعد أول توقف فعلي أو تمرين ينبغي مراجعة درجات السجل وخطوات الدليل في ضوء ما حدث فعلا.