طلب تغيير

طلب تغيير

تقييم أمني واتفاقية استبقاء خدمة

من

NULLWIRE SECURITY

Yale Ave N, Seattle, WA 98109, 500
United States

إلى

MERIDIAN HEALTH SYSTEMS

Forbes Blvd, Columbus, OH 43219, 4400
United States

يعدّل طلب التغيير هذا نطاق العمل المُشار إليه أدناه. ولا يسري مفعوله إلا بعد توقيع الطرفين عليه.

طلب تغيير رقم	تاريخ السريان	يعدّل	تاريخ الإصدار
CR-2026-0225	16 فبراير 2026	SOW-2026-0771	22 يناير 2026

Nullwire Security LLC

سرّي — أُعدّ من أجل Meridian Health Systems. لا يجوز تداوله خارج نطاق الأطراف المذكورة.

01

ملخص التغيير

طلبت Meridian توسيع نطاق التقييم ليشمل نسخة بوابة المرضى الخاصة بمركز Fairview Medical Center المستحوذ عليه حديثًا، مع إضافة أسبوع من الاختبار الخارجي وجولة ثانية من مطابقة معيار HIPAA، ليصبح الإجمالي المعدَّل 111,500 دولار.

المبررات

تطورت بوابة مرضى Meridian Health Systems من مجرد نظام لجدولة المواعيد إلى القناة الرئيسية لنتائج المختبر والفوترة والمراسلة الآمنة عبر شبكة مستشفياتها. جرى فحصها داخليًا بحثًا عن الثغرات المعروفة كل ربع سنة، لكنها لم تواجه قط خصمًا خارجيًا يربط بين الثغرات الصغيرة كما يفعل مهاجم حقيقي — ولا يزال متوسط اكتشاف اختراقات القطاع الصحي يستغرق أكثر من 200 يوم.

تقترح Nullwire Security تكليفًا مدته ثمانية أسابيع يجمع بين اختبار اختراق شامل — خارجي وداخلي وهندسة اجتماعية — واتفاقية استجابة دائمة للاختراقات، بحيث تُختبر Meridian قبل وقوع أي حادثة وتكون جاهزة للاستجابة أثناءها. توضح الأقسام التالية النهج المتبع، والنطاق، والجدول الزمني، والاستثمار المطلوب.

التحدي

تكتشف الفحوصات الداخلية للثغرات نقاط الضعف المعروفة [CVEs]، لكنها تفوّت سلاسل الاستغلال المركّبة، والتكاملات الخارجية سيئة الإعداد، ونقاط الضعف البشرية التي قد تستهدفها حملة تصيّد احتيالي. لم يخضع واجهة برمجة تطبيقات نتائج المختبر لدى Meridian ولا اتصال مزود الفوترة لتقييم مستقل من قبل.

من الناحية التشغيلية، لم يُختبَر الكشف والاستجابة قط في سيناريو حي. وإذا وقع اختراق فعلي، فإن خطة الاستجابة للحوادث المسجَّلة لم تُختبر، ولا يعرف الفريق فعليًا المدة التي ستستغرقها عملية الاحتواء.

نهجنا

ننفذ التكليف كما يفعل خصم حقيقي: استطلاع واستغلال خارجي، وحركة جانبية من نقطة نهاية مخترقة محاكاة، وحملة هندسة اجتماعية تستهدف مكتب الدعم الفني، مع مراجعة مخصصة للتكاملين الخارجيين اللذين يحملان بيانات المرضى.

تُربط النتائج مباشرة بقاعدة أمن HIPAA وتُسلَّم مع إعادة اختبار للتصحيح، بحيث لا يُعتبر أي بند مغلقًا إلا بعد التحقق من إصلاحه. تُبقي اتفاقية الاستجابة للاختراقات بعد ذلك الفريق نفسه جاهزًا عند الطلب، بحيث يكون التعامل مع الحادثة القادمة متدربًا عليه، لا ارتجاليًا.