NULLWIRE SECURITY

NULLWIRE SECURITY · EVALUACIÓN DE SEGURIDAD Y RETAINER

Prueba de Penetración del Portal

Una evaluación de equipo rojo de alcance completo del portal de pacientes, respaldada por un contrato de retención para respuesta a brechas — diseñada para infraestructura regulada por HIPAA.

2026

01

LA OPORTUNIDAD

El portal de pacientes de Meridian Health Systems gestiona hoy resultados de laboratorio, facturación y mensajería para 340 000 pacientes, y nunca ha sido sometido a una evaluación externa de red team. Este es el plan para ponerlo a prueba como corresponde y estar preparados si algo llega a filtrarse.

POR QUÉ AHORA

El portal de pacientes de Meridian Health Systems ha pasado de ser un programador de citas a convertirse en el canal principal para resultados de laboratorio, facturación y mensajería segura en toda su red hospitalaria. Se ha escaneado internamente en busca de vulnerabilidades conocidas cada trimestre, pero nunca ha enfrentado a un adversario externo que encadene pequeñas debilidades de la manera en que lo haría un atacante real, y la brecha de salud promedio todavía tarda más de 200 días en detectarse.

Nullwire Security propone un compromiso de ocho semanas que combina una prueba de penetración de alcance completo — externa, interna e ingeniería social — con un contrato de retención permanente para respuesta a brechas, de modo que Meridian sea evaluado antes de un incidente y esté listo para responder durante uno. Las siguientes secciones exponen el enfoque, el alcance, el cronograma y la inversión.

01

Más de 140

PRUEBAS DE PENETRACIÓN COMPLETADAS

02

<4 hrs

TIEMPO MEDIO DE ACTIVACIÓN DE RESPUESTA ANTE BRECHAS

03

8 semanas

DEL ALCANCE AL INFORME FINAL

EL DESAFÍO

Los escaneos internos de vulnerabilidades detectan CVEs conocidos, pero pasan por alto exploits encadenados, integraciones de terceros mal configuradas y los puntos débiles humanos que una campaña de phishing atacaría. La API de resultados de laboratorio de Meridian y la conexión con el proveedor de facturación nunca han sido evaluadas de forma independiente.

A nivel operativo, la detección y respuesta nunca se han ensayado frente a un escenario real. Si ocurriera una brecha, el plan de respuesta a incidentes registrado no ha sido probado, y el equipo no sabe cuánto tiempo tomaría realmente la contención.

NUESTRO ENFOQUE

Ejecutamos el compromiso como lo haría un adversario real: reconocimiento y explotación externos, movimiento lateral desde un endpoint comprometido simulado, y una campaña de ingeniería social contra la mesa de ayuda, junto con una revisión dedicada de las dos integraciones de terceros que manejan datos de pacientes.

Los hallazgos se mapean directamente a la Regla de Seguridad de HIPAA y se entregan con una reprueba de remediación, de modo que nada se marca como cerrado hasta que se verifica que fue corregido. El contrato de retención para respuesta a brechas mantiene luego al mismo equipo disponible, de modo que el próximo incidente sea ensayado, no improvisado.

01
PRUEBA DE PENETRACIÓN EXTERNA

Activos expuestos a internet, el portal de pacientes y sus API públicas, evaluados hasta la explotación.

02
MOVIMIENTO INTERNO Y LATERAL

Un escenario simulado de endpoint comprometido, evaluando hasta dónde podría desplazarse un atacante una vez dentro.

03
INGENIERÍA SOCIAL

Una simulación de phishing y una campaña de pretexting de mesa de ayuda dirigida al personal.

04
REVISIÓN DE INTEGRACIONES DE TERCEROS

Evaluación de seguridad de las conexiones API con los proveedores de resultados de laboratorio y facturación.

05
RETAINER DE RESPUESTA ANTE BRECHAS

Respuesta a incidentes disponible bajo demanda y un manual de respuesta ensayado y listo para ejecutarse.

06
INFORMES DE CUMPLIMIENTO

Hallazgos vinculados directamente con la Regla de Seguridad de HIPAA para auditoría e informes a la junta directiva.

Nullwire encontró un exploit encadenado que nuestro equipo interno había pasado por alto durante dos años, y nos tuvo contenidos en una hora cuando pusimos a prueba el retainer en un caso real.

OWEN MARSH



SITUACIÓN

REGISTROS, COBERTURAS Y GARANTÍAS

CREDENCIAL	ENTIDAD EMISORA	REFERENCIA	ALCANCE	ESTADO
Entidad registrada	Registro de sociedades, Estados Unidos	Nullwire Security LLC	Nombre comercial e identidad jurídica	Activo
Registro fiscal	Autoridad fiscal, Estados Unidos	EIN 91-4820376	Todos los trabajos facturados	Activo
Seguro de responsabilidad civil profesional	Aseguradora comercial	Disponible a solicitud	Evaluación de Seguridad y Servicio de Retención	Se renueva anualmente
Seguro de responsabilidad civil general	Aseguradora comercial	Disponible a solicitud	Trabajos en sitio y en las instalaciones del cliente	Se renueva anualmente
Afiliación a un organismo profesional	Asociación sectorial, Estados Unidos	Disponible a solicitud	Código de conducta y procedimiento de reclamaciones	Al corriente

Los certificados y anexos de pólizas se entregan a solicitud y se reemiten a Meridian Health Systems a solicitud en cualquier momento durante el encargo.

[01] ▸ SEMANAS 1–2 · ALCANCE Y RECONOCIMIENTO

Reglas de compromiso, enumeración de activos y mapeo de la superficie de ataque.

[02] ▸ SEMANAS 3–5 · PRUEBAS ACTIVAS

Pruebas externas, internas y de ingeniería social contra el alcance acordado.

[03] ▸ SEMANA 6 · HALLAZGOS Y MAPEO HIPAA

Consolidación de hallazgos y mapeo a las salvaguardas relevantes de la Regla de Seguridad de HIPAA.

[04] SEMANA 7 · APOYO A LA REMEDIACIÓN

Apoyo guiado en la remediación para el equipo de ingeniería antes de la reprueba.

01
EVALUACIÓN
$94,000

- Compromiso completo de ocho semanas
- Pruebas externas, internas y de ingeniería social
- Informe de hallazgos vinculado a HIPAA
- Dos semanas de soporte de remediación

02
EVALUACIÓN + RETAINER
$6,500/mo

- Todo lo incluido en Evaluación
- Línea directa de respuesta ante brechas 24/7
- Reescaneo mensual de vulnerabilidades
- SLA de respuesta prioritaria a incidentes (<4 hrs)

03
DEFENSA CONTINUA
$13,000/mo

- Todo lo incluido en Retainer
- Ejercicios trimestrales de equipo rojo
- Monitoreo continuo de la superficie de ataque externa
- Tiempo integrado de ingeniería de seguridad

MODELO DE NEGOCIO

CÓMO SE COMPARAN LOS TRES NIVELES

	EVALUACIÓN	EVALUACIÓN + RETAINER	DEFENSA CONTINUA
Precio	$94,000	$6,500/mo	$13,000/mo
Alcance principal	Compromiso completo de ocho semanas	Todo lo incluido en Evaluación	Todo lo incluido en Retainer
Qué incluye	Pruebas externas, internas y de ingeniería social	Línea directa de respuesta ante brechas 24/7	Ejercicios trimestrales de equipo rojo

Entrega	Informe de hallazgos vinculado a HIPAA	Reescaneo mensual de vulnerabilidades	Monitoreo continuo de la superficie de ataque externa
Servicio posterior	Dos semanas de soporte de remediación	SLA de respuesta prioritaria a incidentes (<4 hrs)	Tiempo integrado de ingeniería de seguridad

Los precios están en USD y no incluyen el impuesto sobre las ventas (wa — servicios profesionales exentos). Las opciones se pueden combinar o escalonar; la recomendación para Meridian Health Systems se destaca en la sección de precios.

LA SOLICITUD

ÚNETE A LA RONDA

Estamos levantando capital para financiar la hoja de ruta de la página anterior. Nullwire Security agradecería una conversación de seguimiento este trimestre.

Apruebe esta propuesta y podremos reservar el inicio del alcance para la semana del 16 de febrero. Responda a este documento o escriba a contact@nullwiresecurity.com.

Nullwire Security
contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com · Seattle, WA 98109