

• • • • •

NULLWIRE SECURITY — PORTAFOLIO  
DE ESTUDIO

# Trabajo seleccionado y capacidades

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.

► 01 ■

## SOBRE EL ESTUDIO

Un encargo de ocho semanas que combina una prueba de penetración de alcance completo con un servicio de retención permanente de respuesta ante brechas, para que Meridian Health Systems esté evaluado antes de un incidente y preparado para responder durante uno.

## CÓMO TRABAJAMOS

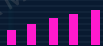
El portal de pacientes de Meridian Health Systems ha pasado de ser un programador de citas a convertirse en el canal principal para resultados de laboratorio, facturación y mensajería segura en toda su red hospitalaria. Se ha escaneado internamente en busca de vulnerabilidades conocidas cada trimestre, 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

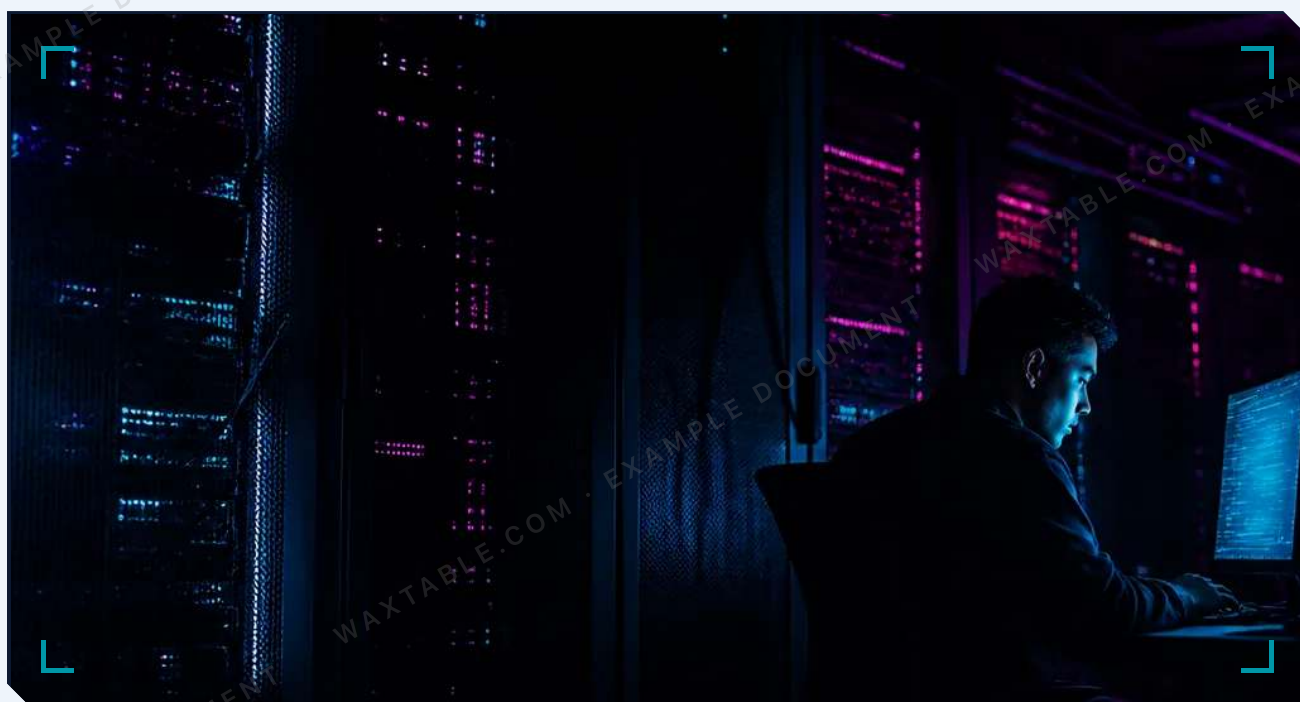


03

8  
semanas

DEL ALCANCE AL  
INFORME FINAL





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



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.

# QUÉ INCLUYE UN PROYECTO TÍPICO

| REF.   | ÍTEM                                    | ESPECIFICACIÓN                                                                                | ESFUERZO | TIEMPO | PRECIO UNITARIO |
|--------|-----------------------------------------|-----------------------------------------------------------------------------------------------|----------|--------|-----------------|
| SPC-01 | Alcance y reconocimiento                | Reglas de compromiso, enumeración de activos y mapeo de la superficie de ataque               | 2        | 2 sem. | \$9,500 / wk    |
| SPC-02 | Prueba de penetración externa           | Evaluación del portal de pacientes y la API expuestos a internet                              | 2        | 2 sem. | \$14,000 / wk   |
| SPC-03 | Pruebas internas y de ingeniería social | Escenario simulado de endpoint comprometido y ejercicio de phishing                           | 1        | 1 sem. | \$16,000 / wk   |
| SPC-04 | Revisión de integraciones de terceros   | Evaluación de seguridad de la API de resultados de laboratorio y del proveedor de facturación | 1        | 1 sem. | \$12,000 / wk   |
| SPC-05 | Informes y apoyo a la remediación       | Informe de hallazgos, mapeo HIPAA y guía de remediación                                       | 1        | 1 sem. | \$10,000 / wk   |

Las especificaciones quedan fijadas en el momento de la aceptación; cualquier cambio se gestiona mediante el procedimiento de control de cambios establecido en este documento.

[01]



## PRUEBAS DE NIVEL ADVERSARIO

Pruebas externas, internas y de ingeniería social ejecutadas de la forma en que un atacante real las encadenaría.

[02]



## INFORMES MAPEADOS A HIPAA

Cada hallazgo mapeado a la salvaguarda correspondiente de la Regla de Seguridad de HIPAA, listo para auditoría e informes a la junta.

[03]



## RESPUESTA PERMANENTE

Un manual de respuesta a brechas ensayado y una retención de guardia permanente, para que el próximo incidente esté ensayado, no improvisado.

### 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.

## ■ OPCIONES

# QUÉ MODALIDAD TE CONVIENE

|                    | 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.



■ TRABAJA CON NOSOTROS

# [ INICIAR UN PROYECTO ]

Cada proyecto comienza con una conversación sobre lo que realmente quiere cambiar. Nullwire Security responde en un día hábil.

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](mailto:contact@nullwiresecurity.com).



Nullwire Security

[contact@nullwiresecurity.com](mailto:contact@nullwiresecurity.com) · +1 206 555 0189 · [nullwiresecurity.com](http://nullwiresecurity.com) · Seattle, WA 98109