NULLWIRE SECURITY

PROPOSTA PARA MERIDIAN HEALTH SYSTEMS

Proposta de Teste de Invasão de Portal

Uma avaliação red-team de escopo completo do portal do paciente, apoiada por um contrato de resposta a violações — desenvolvida para infraestrutura regulada pela HIPAA.

2026

SUMÁRIO

RESUMO GERAL

PROPOSTA

PRO-2026-0771

PARA APROVAÇÃO

PREPARADO PARA

Meridian Health Systems — Renata Cole, Diretora de Segurança da Informação

PREPARADO POR
Nullwire Security, Seattle

EMITIDO
22 de janeiro de 2026

VÁLIDO ATÉ
6 de março de 2026

CONTRATAÇÃO
Avaliação de Segurança e Contrato de Retenção

RESUMO GERAL

O PROJETO EM CINCO NÚMEROS

01
CONTRATAÇÃO
Avaliação de Segurança e Contrato de Retenção
Uma avaliação red-team de escopo completo do portal do paciente, apoiada por um contrato de resposta a violações — desenvolvida para infraestrutura regulada pela HIPAA.

02
INVESTIMENTO
$94,000
$94,000, mais imposto sobre vendas (wa — serviços profissionais isentos)

03
INÍCIO
16 de fevereiro de 2026
Sujeito a aceitação até 6 de março de 2026

04
DURAÇÃO
12 meses
Do início à entrega final

05
PREPARADO PARA
Meridian Health Systems
Renata Cole, Diretor de segurança da informação

01

A OPORTUNIDADE

O portal do paciente da Meridian Health Systems agora reúne resultados de exames, faturamento e mensagens de 340.000 pacientes — e nunca passou por uma avaliação externa de red team. Este é o plano para testá-lo de forma adequada e estar preparado caso algo passe despercebido.

RESUMO EXECUTIVO

O portal do paciente da Meridian Health Systems evoluiu de um agendador de consultas para o principal canal de resultados de exames, faturamento e mensagens seguras em toda a sua rede hospitalar. Ele é escaneado internamente em busca de vulnerabilidades conhecidas a cada trimestre, mas nunca enfrentou um adversário externo que encadeia pequenas fraquezas da forma como um atacante real faria — e o tempo médio para detectar uma violação de dados na área da saúde ainda ultrapassa 200 dias.

A Nullwire Security propõe um projeto de oito semanas que combina um teste de invasão de escopo completo — externo, interno e de engenharia social — com um contrato permanente de resposta a violações, para que a Meridian seja testada antes de um incidente e esteja pronta para responder durante um.

As seções a seguir apresentam a abordagem, o escopo, o cronograma e o investimento.

O DESAFIO

As varreduras internas de vulnerabilidade detectam CVEs conhecidas, mas não identificam explorações encadeadas, integrações de terceiros mal configuradas nem os pontos fracos humanos que uma campanha de phishing exploraria. A API de resultados de exames da Meridian e a conexão com o fornecedor de faturamento nunca foram avaliadas de forma independente.

Operacionalmente, a detecção e a resposta nunca foram ensaiadas em um cenário real. Se ocorresse uma violação, o plano de resposta a incidentes registrado nunca foi testado, e a equipe não sabe, na prática, quanto tempo levaria a contenção.

NOSSA ABORDAGEM

Conduzimos o projeto como um adversário real faria: reconhecimento e exploração externos, movimentação lateral a partir de um endpoint comprometido simulado, e uma campanha de engenharia social contra a central de atendimento, somados a uma revisão dedicada das duas integrações de terceiros que carregam dados de pacientes.

Os achados são mapeados diretamente à HIPAA Security Rule e devolvidos com um reteste de correção, de modo que nada seja marcado como resolvido até que a correção seja verificada. O contrato de resposta a violações mantém então essa mesma equipe de plantão, para que o próximo incidente seja ensaiado, não improvisado.

01
140+
TESTES DE PENETRAÇÃO CONCLUÍDOS

02
<4 h
TEMPO MEDIANO DE ATIVAÇÃO DE RESPOSTA A VIOLAÇÕES

03
8 sem.
DO ESCOPO AO RELATÓRIO FINAL

SITUAÇÃO

REGISTROS, COBERTURAS E GARANTIAS

CREDENCIAL	ÓRGÃO EMISSOR	REFERÊNCIA	ESCOPO	STATUS
Entidade registrada	Registro de empresas, Estados Unidos	Nullwire Security LLC	Nome fantasia e identidade jurídica	Ativo
Registro fiscal	Autoridade fiscal, Estados Unidos	EIN 91-4820376	Todos os trabalhos faturados	Ativo
Seguro de responsabilidade civil profissional	Seguradora comercial	Disponível mediante solicitação	Avaliação de Segurança e Contrato de Retenção	Renovado anualmente
Seguro de responsabilidade civil geral	Seguradora comercial	Disponível mediante solicitação	Trabalhos no local e nas instalações do cliente	Renovado anualmente
Filiação a entidade de classe	Associação setorial, Estados Unidos	Disponível mediante solicitação	Código de conduta e canal de reclamações	Em situação regular

Certificados e apólices são fornecidos mediante solicitação e reemitidos para Meridian Health Systems mediante solicitação a qualquer momento durante o contrato.

> **A Nullwire encontrou uma exploração encadeada que nossa equipe interna havia deixado passar por dois anos, e nos conteve em uma hora quando testamos o contrato de verdade.**
>
> OWEN MARSH

02

ESCOPO DO TRABALHO

Um contrato de oito semanas que combina um teste de invasão de escopo completo com um contrato de retenção permanente para resposta a violações, para que a Meridian Health Systems seja testada antes de um incidente e esteja pronta para responder durante um.

01
TESTE DE INVASÃO EXTERNO

Ativos voltados para a internet, o portal do paciente e suas APIs públicas, testados até a exploração.

02
MOVIMENTO INTERNO E LATERAL

Um cenário simulado de endpoint comprometido, testando até onde um invasor poderia se mover uma vez dentro da rede.

03
ENGENHARIA SOCIAL

Uma simulação de phishing e uma campanha de pretexting de help desk contra a equipe.

04
REVISÃO DE INTEGRAÇÕES DE TERCEIROS

Avaliação de segurança das conexões de API com fornecedores de resultados laboratoriais e faturamento.

05
CONTRATO DE RESPOSTA A VIOLAÇÕES

Resposta a incidentes sob demanda e um runbook de RI ensaiado e pronto para execução.

06
RELATÓRIO DE CONFORMIDADE

Achados mapeados diretamente para a HIPAA Security Rule, para auditoria e relatórios à diretoria.

ENTREGAS

[01] TESTES

RELATÓRIO DE TESTE DE INVASÃO DE ESCOPO COMPLETO

Descobertas externas, internas e de movimento lateral, com detalhes de prova de conceito e classificações de gravidade.

[02] TESTES

AVALIAÇÃO DE ENGENHARIA SOCIAL

Resultados de phishing e pretexting de help desk, com recomendações de conscientização voltadas à equipe.

[03] RESPOSTA

MANUAL DE RESPOSTA A VIOLAÇÕES

Um plano ensaiado de resposta a incidentes com funções definidas, caminhos de escalonamento e a linha de plantão da Nullwire.

[04] CONFORMIDADE

RELATÓRIO DE DESCOBERTAS MAPEADO À HIPAA

Cada descoberta mapeada à respectiva salvaguarda da HIPAA Security Rule, pronta para auditoria.

[05] HABILITAÇÃO

RETESTE DE REMEDIAÇÃO E APROVAÇÃO FINAL

Um reteste de acompanhamento que verifica o encerramento de cada descoberta, com aprovação por escrito.

FORA DO ESCOPO

- Teste de invasão física de instalações além dos dois data centers nomeados
- Auditoria de código-fonte de aplicações de fornecedores terceiros
- Monitoramento contínuo de SOC 24/7 além da janela de plantão do contrato de retenção
- Assessoria jurídica regulatória e de notificação de violação de dados



[01] ▸ SEMANAS 1–2 · DEFINIÇÃO DE ESCOPO E RECONHECIMENTO

Regras de engajamento, inventário de ativos e mapeamento da superfície de ataque.

[02] ▸ SEMANAS 3–5 · TESTES ATIVOS

Testes externos, internos e de engenharia social conforme o escopo acordado.

[03] ▸ SEMANA 6 · ACHADOS E MAPEAMENTO HIPAA

Achados consolidados e mapeados às salvaguardas relevantes da HIPAA Security Rule.

[04] ▸ SEMANA 7 · SUPORTE À CORREÇÃO

Suporte orientado à correção para a equipe de engenharia antes do reteste.

03

INVESTIMENTO E CONDIÇÕES

Contas de teste e uma carta de regras de engajamento assinada são fornecidas antes do início dos testes; um responsável tem autoridade para autorizar mudanças de escopo em cada etapa; e os testes ficam limitados ao portal do paciente e suas duas integrações nomeadas com terceiros. Alterações a esses pontos afetam o cronograma e o custo, o que acordaríamos por escrito antes de prosseguir. O valor é válido para contratações iniciadas até 6 de março de 2026.

FRENTE DE TRABALHO	SEMANAS	TAXA	VALOR
Definição de escopo e reconhecimento Regras de engajamento, inventário de ativos e mapeamento da superfície de ataque	2	$9,500 / wk	$19,000
Teste de invasão externo Avaliação do portal do paciente e da API expostos à internet	2	$14,000 / wk	$28,000
Testes internos e de engenharia social Cenário simulado de endpoint comprometido e exercício de phishing	1	$16,000 / wk	$16,000
Revisão de integrações de terceiros Avaliação de segurança das APIs de resultados de exames e do fornecedor de faturamento	1	$12,000 / wk	$12,000
Relatório e suporte à correção Relatório de achados, mapeamento HIPAA e orientação de correção	1	$10,000 / wk	$10,000
Reteste e configuração de retenção Reteste de verificação de correções e entrega do manual de resposta a violações	1	$9,000 / wk	$9,000
Total da contratação			**$94,000**

TAXA DO PROJETO	$94,000
IMPOSTO SOBRE VENDAS (WA — SERVIÇOS PROFISSIONAIS ISENTOS)	$0
TOTAL	$94,000

TOTAL DEVIDO **$94,000**

Todos os valores estão em USD. Faturamento em três marcos: 40% na assinatura, 30% no início da construção, 30% na entrega. O valor é válido para contratações iniciadas até 6 de março de 2026.

01
AVALIAÇÃO
$94,000

- Engajamento completo de oito semanas
- Testes externos, internos e de engenharia social
- Relatório de descobertas mapeado à HIPAA
- Duas semanas de suporte à remediação

02
AVALIAÇÃO + CONTRATO CONTÍNUO
$6,500/mo

- Tudo do plano Avaliação
- Linha direta de resposta a violações 24/7
- Nova varredura mensal de vulnerabilidades
- SLA de resposta a incidentes prioritária (<4 h)

03
DEFESA CONTÍNUA
$13,000/mo

- Tudo do plano Contrato Contínuo
- Exercícios trimestrais de red team
- Monitoramento contínuo da superfície de ataque externa
- Tempo dedicado de engenharia de segurança

OPÇÕES

QUAL MODELO COMBINA COM VOCÊ

	AVALIAÇÃO	AVALIAÇÃO + CONTRATO CONTÍNUO	DEFESA CONTÍNUA

Preço	$94,000	$6,500/mo	$13,000/mo
Escopo principal	Engajamento completo de oito semanas	Tudo do plano Avaliação	Tudo do plano Contrato Contínuo
O que está incluído	Testes externos, internos e de engenharia social	Linha direta de resposta a violações 24/7	Exercícios trimestrais de red team
Entrega	Relatório de descobertas mapeado à HIPAA	Nova varredura mensal de vulnerabilidades	Monitoramento contínuo da superfície de ataque externa
Suporte pós-entrega	Duas semanas de suporte à remediação	SLA de resposta a incidentes prioritária (<4 h)	Tempo dedicado de engenharia de segurança

Os preços estão em USD e não incluem o imposto sobre vendas (wa — serviços profissionais isentos). As opções podem ser combinadas ou escalonadas; a recomendação para Meridian Health Systems está destacada na seção de preços.

CRONOGRAMA DE PAGAMENTO

QUANDO CADA PARCELA VENCE

N.º	MARCO	GATILHO	PARCELA	VALOR
01	Semanas 1–2 · Definição de escopo e reconhecimento	16 de fevereiro de 2026	40%	$37,600
02	Semanas 3–5 · Testes ativos	No início da entrega	30%	$28,200
03	Semana 6 · Achados e mapeamento HIPAA	Na aceitação do marco	30%	$28,200
Total (sem impostos)			**100%**	**$94,000**

As parcelas são faturadas conforme os marcos acima e são pagáveis em até 30 dias após cada fatura. Todos os valores estão em USD e não incluem imposto sobre vendas (wa — serviços profissionais isentos).

PREMISSAS DAS QUAIS ESTA ESTIMATIVA DEPENDE

Contas de teste e uma carta assinada com as regras de engajamento são fornecidas antes do início dos testes; um representante é autorizado a aprovar alterações de escopo em cada etapa; e os testes ficam limitados ao portal do paciente e às suas duas integrações de terceiros nomeadas. Alterações a esses itens afetam o cronograma e o custo, o que acordaríamos por escrito antes de prosseguir. O valor é válido para projetos iniciados até 6 de março de 2026.

A contra-assinatura abaixo aceita o escopo, o cronograma e o investimento definidos nesta proposta e autoriza o início do trabalho.

PELA MERIDIAN HEALTH SYSTEMS

RENATA COLE

DIRETORA DE SEGURANÇA DA INFORMAÇÃO

Data

PELA NULLWIRE SECURITY

NULLWIRE SECURITY

SIGNATÁRIO AUTORIZADO

Data

PRÓXIMOS PASSOS

PRONTOS QUANDO VOCÊ ESTIVER

A aceitação desta proposta dá início ao trabalho em 16 de fevereiro de 2026. O valor permanece válido para contratações confirmadas até 6 de março de 2026.

Aprove esta proposta e poderemos reservar o início do escopo para a semana de 16 de fevereiro. Responda a este documento ou envie um e-mail para contact@nullwiresecurity.com.

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