NULLWIRE SECURITY

PREPARADO PARA A MERIDIAN HEALTH SYSTEMS

Escopo de Trabalho

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

SOW

SOW-2026-0771

RASCUNHO

STATUS

Rascunho — para revisão

RESUMO GERAL

ESCOPO, CRONOGRAMA E HONORÁRIOS

01
FRENTE DE TRABALHO

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
INÍCIO

16 de fevereiro de 2026

Mediante contra-assinatura

03
DURAÇÃO

12 meses

Faseado conforme cronograma abaixo

04
HONORÁRIOS

$94,000

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

05
ACEITO POR

Renata Cole

Diretora de Segurança da Informação

01

VISÃO GERAL E OBJETIVOS

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.

CONTEXTO E METAS

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.

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]

TESTES EM NÍVEL DE ADVERSÁRIO REAL

Testes externos, internos e de engenharia social executados da forma como um atacante real os encadearia.

[02]

RELATÓRIO MAPEADO À HIPAA

Cada achado mapeado à salvaguarda correspondente da HIPAA Security Rule, pronto para auditoria e relatórios ao conselho.

[03]

RESPOSTA SEMPRE ATIVA

Um manual de resposta a violações ensaiado e um contrato de plantão, para que o próximo incidente seja ensaiado, não improvisado.

ESPECIFICAÇÃO

ESPECIFICAÇÃO DA FRENTE DE TRABALHO

REF.	ITEM	ESPECIFICAÇÃO	ESFORÇO	PRAZO	PREÇO UNITÁRIO
SPC-01	Definição de escopo e reconhecimento	Regras de engajamento, inventário de ativos e mapeamento da superfície de ataque	2	2 sem.	$9,500 / wk
SPC-02	Teste de invasão externo	Avaliação do portal do paciente e da API expostos à internet	2	2 sem.	$14,000 / wk
SPC-03	Testes internos e de engenharia social	Cenário simulado de endpoint comprometido e exercício de phishing	1	1 sem.	$16,000 / wk
SPC-04	Revisão de integrações de terceiros	Avaliação de segurança das APIs de resultados de exames e do fornecedor de faturamento	1	1 sem.	$12,000 / wk
SPC-05	Relatório e suporte à correção	Relatório de achados, mapeamento HIPAA e orientação de correção	1	1 sem.	$10,000 / wk

As especificações são fixadas no momento da aceitação; qualquer alteração é tratada por meio do processo de controle de mudanças definido neste documento.

[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.

[05] ▸ SEMANA 8 · RETESTE E ATIVAÇÃO DO CONTRATO DE SUPORTE

Reteste de verificação da correção e transferência do runbook de resposta a violações.

CRITÉRIOS DE ACEITAÇÃO

REF.	REQUISITO	PRIORIDADE
R-01	Os testes externos e internos devem incluir o portal do paciente e suas duas integrações nomeadas de terceiros	OBRIGATÓRIO
R-02	Contas de teste e uma carta assinada de regras de engajamento fornecidas antes do início dos testes	OBRIGATÓRIO
R-03	Todas as descobertas mapeadas para a salvaguarda relevante da Regra de Segurança da HIPAA	OBRIGATÓRIO
R-04	Descobertas críticas e altas retestadas e verificadas como resolvidas antes da aprovação final	OBRIGATÓRIO
R-05	Campanha de engenharia social limitada à central de atendimento e aos departamentos nomeados	OBRIGATÓRIO

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
Subtotal de honorários			**$94,000**

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

TOTAL $94,000

Todos os valores estão em USD e não incluem impostos aplicáveis. Os honorários são cobrados em três marcos: 40% na assinatura, 30% no início da construção, 30% na entrada em operação.

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).

A contra-assinatura abaixo aceita o escopo, o cronograma, os critérios de aceitação e os honorários estabelecidos neste Escopo de Trabalho e autoriza o início dos trabalhos na data de início indicada.

PELA MERIDIAN HEALTH SYSTEMS

RENATA COLE
DIRETORA DE SEGURANÇA DA INFORMAÇÃO
Data

PELA NULLWIRE SECURITY

NULLWIRE SECURITY
SIGNATÁRIO AUTORIZADO
Data

NULLWIRE SECURITY

500 Yale Ave N, Seattle, WA 98109,
Estados Unidos
contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com
Nullwire Security LLC · EIN 91-4820376