NULLWIRE SECURITY

PROPOSITION POUR MERIDIAN HEALTH SYSTEMS

Proposition — Test d'intrusion du portail

Une évaluation en équipe rouge à périmètre complet du portail patient, adossée à un contrat de réponse aux violations — conçue pour une infrastructure soumise à la réglementation HIPAA.

2026

SOMMAIRE

01 En bref 2
02 La mission en chiffres 3
03 L'opportunité 5
04 Résumé exécutif 5
05 L'expérience actuelle 5
06 Défi et approche 6
07 Preuves à l'appui 7
08 Statut et couvertures 7
09 Ils en parlent 8
10 Périmètre de la mission 9
11 Ce qui est inclus 9
12 Livrables 9
13 Réalisations sélectionnées 10
14 Calendrier 11
15 Investissement et conditions 12
16 Détail des honoraires 12
17 Récapitulatif des coûts 13
18 Options de mission 13
19 Comparatif des options 13
20 Échéancier de paiement 14
21 Hypothèses sur lesquelles repose cette estimation 15
22 Acceptation 15

EN BREF

PROPOSITION

PRO-2026-0771

POUR APPROBATION

PRÉPARÉ POUR

EXAMPLE DOCUMENT · WAXTABLE.COM

Meridian Health Systems — Renata Cole, Directrice de la sécurité des systèmes d'information

PRÉPARÉ PAR
Nullwire Security, Seattle

ÉMIS LE
22 janvier 2026

VALABLE JUSQU'AU
6 mars 2026

MISSION
Évaluation de sécurité et abonnement de veille

EN BREF

LA MISSION EN CINQ CHIFFRES

01
MISSION
Évaluation de sécurité et abonnement de veille
Une évaluation en équipe rouge à périmètre complet du portail patient, adossée à un contrat de réponse aux violations — conçue pour une infrastructure soumise à la réglementation HIPAA.

02
INVESTISSEMENT
$94,000
$94,000, plus taxe de vente (wa — services professionnels exonérés)

03
DÉBUT
16 février 2026
Sous réserve d'acceptation avant le 6 mars 2026

04
DURÉE
12 mois
Du lancement à la livraison finale

05
PRÉPARÉ POUR
Meridian Health Systems

WAXTABLE.COM · EXAMPLE DOCUMENT

Renata Cole, Directeur de la sécurité des systèmes d'information

WAXTABLE.COM · EXAMPLE DOCUMENT

01

L'OPPORTUNITÉ

Le portail patient de Meridian Health Systems héberge désormais les résultats de laboratoire, la facturation et la messagerie de 340 000 patients — et n'a jamais fait l'objet d'une évaluation externe par une équipe de red team. Voici le plan pour le tester rigoureusement, et pour être prêt si une faille venait à être exploitée.

RÉSUMÉ EXÉCUTIF

Le portail patient de Meridian Health Systems, initialement un simple planificateur de rendez-vous, est devenu le canal principal pour les résultats de laboratoire, la facturation et la messagerie sécurisée dans l'ensemble de son réseau hospitalier. Il fait l'objet d'analyses internes trimestrielles des vulnérabilités connues, mais il n'a jamais fait face à un adversaire externe capable d'enchaîner de petites faiblesses comme le ferait un véritable attaquant — et le délai moyen de détection d'une violation de données dans le secteur de la santé dépasse toujours 200 jours.

Nullwire Security propose une mission de huit semaines combinant un test d'intrusion à périmètre complet — externe, interne et d'ingénierie sociale — avec un contrat de réponse aux violations permanent, afin que Meridian soit testé avant un incident et prêt à réagir pendant celui-ci. Les sections suivantes présentent la démarche, le périmètre, le calendrier et l'investissement.

LE DÉFI

Les analyses internes de vulnérabilités détectent les CVE connues, mais elles ne repèrent pas les exploits enchaînés, les intégrations tierces mal configurées ni les points faibles humains qu'une campagne de phishing viserait. L'API des résultats de laboratoire de Meridian et sa connexion au prestataire de facturation n'ont jamais été évaluées de façon indépendante.

Sur le plan opérationnel, la détection et la réponse n'ont jamais été répétées face à un scénario réel. En cas de violation, le plan de réponse aux incidents en vigueur n'a jamais été testé, et l'équipe ignore le temps réel que prendrait le confinement.

NOTRE DÉMARCHE

Nous menons la mission comme le ferait un véritable adversaire : reconnaissance et exploitation externes, mouvement latéral à partir d'un poste compromis simulé, et campagne d'ingénierie sociale contre le service d'assistance, complétées par un examen dédié des deux intégrations tierces qui traitent des données patient.

Les constats sont directement rattachés à la HIPAA Security Rule et renvoyés avec un nouveau test de correction, de sorte que rien n'est marqué comme résolu tant que la correction n'est pas vérifiée. Le contrat de réponse aux violations maintient ensuite la même équipe disponible, afin que le prochain incident soit répété, et non improvisé.

01
140+
TESTS D'INTRUSION RÉALISÉS

02
< 4 h
DÉLAI MÉDIAN D'ACTIVATION DE LA RÉPONSE À INCIDENT

03
8 sem.
DU CADRAGE AU RAPPORT FINAL

STATUT

IMMATRICULATIONS, COUVERTURES ET GARANTIES

HABILITATION	ORGANISME ÉMETTEUR	RÉFÉRENCE	PÉRIMÈTRE	STATUT
Entité enregistrée	Registre des sociétés, États-Unis	Nullwire Security LLC	Nom commercial et identité juridique	Actif
Immatriculation fiscale	Administration fiscale, États-Unis	EIN 91-4820376	Toutes les prestations facturées	Actif
Assurance responsabilité civile professionnelle	Assureur commercial	Disponible sur demande	Évaluation de sécurité et abonnement de veille	Renouvelé chaque anné
Assurance responsabilité civile générale	Assureur commercial	Disponible sur demande	Travaux sur site et dans les locaux du client	Renouvelé chaque anné
Adhésion à un organisme professionnel	Association professionnelle, États-Unis	Disponible sur demande	Code de déontologie et procédure de réclamation	En règle

Les certificats et les tableaux de garanties sont fournis sur demande et sont réémis à Meridian Health Systems sur demande à tout moment pendant la mission.

> **Nullwire a découvert une faille en chaîne que notre équipe interne avait manquée pendant deux ans, et nous a permis d'être maîtrisés en une heure lorsque nous avons testé le forfait en conditions réelles.**
>
> OWEN MARSH

WAXTABLE.COM · EXAMPLE DOCUMENT

02

PÉRIMÈTRE DE LA MISSION

Une mission de huit semaines associant un test d'intrusion complet à un abonnement permanent de réponse aux incidents, afin que Meridian Health Systems soit testé avant un incident et prêt à réagir pendant celui-ci.

01 TEST D'INTRUSION EXTERNE

Actifs exposés sur Internet, le portail patient et ses API publiques, testés jusqu'à l'exploitation.

02 MOUVEMENT LATÉRAL ET INTERNE

Un scénario simulé de terminal compromis, testant jusqu'où un attaquant pourrait se déplacer une fois à l'intérieur.

03 INGÉNIERIE SOCIALE

Une simulation d'hameçonnage et une campagne de prétexte auprès du service d'assistance visant le personnel.

04 EXAMEN DES INTÉGRATIONS TIERCES

Évaluation de sécurité des connexions API avec les prestataires de résultats de laboratoire et de facturation.

05 FORFAIT DE RÉPONSE AUX INCIDENTS

Réponse aux incidents sur appel et un plan d'intervention répété et prêt à exécuter.

06 RAPPORTS DE CONFORMITÉ

Constats directement rattachés à la règle de sécurité HIPAA pour l'audit et le reporting au conseil d'administration.

LIVRABLES

[01] TESTS

RAPPORT DE TEST D'INTRUSION COMPLET

Constats externes, internes et de mouvement latéral, avec détail des preuves de concept et notation de gravité.

[02] TESTS

ÉVALUATION D'INGÉNIERIE SOCIALE

Résultats des tests de phishing et de manipulation du support technique, avec recommandations de sensibilisation destinées au personnel.

[03] RÉPONSE

PLAN D'INTERVENTION EN CAS DE VIOLATION

Un plan de réponse aux incidents répété, avec rôles définis, filières d'escalade et ligne d'astreinte Nullwire.

[04] CONFORMITÉ

RAPPORT DE CONSTATS CARTOGRAPHIÉ SUR LA NORME HIPAA

Chaque constat rattaché à la mesure de sécurité HIPAA correspondante, prêt pour un audit.

[05] LIVRAISON TECHNIQUE

NOUVEAU TEST DE REMÉDIATION ET VALIDATION

Un nouveau test vérifiant que chaque constat a été corrigé, avec validation écrite.

HORS PÉRIMÈTRE

- Tests d'intrusion physique des installations au-delà des deux centres de données nommés
- Audit du code source des applications de fournisseurs tiers
- Surveillance SOC continue 24 h/24 et 7 j/7 au-delà de la plage d'astreinte de l'abonnement
- Dépôts réglementaires et conseil juridique en notification de violation de données

WAXTABLE.COM · EXAMPLE DOCUMENT

[01] SEMAINES 1 À 2 · CADRAGE ET RECONNAISSANCE

Règles d'engagement, recensement des actifs et cartographie de la surface d'attaque.

[02] SEMAINES 3 À 5 · TESTS ACTIFS

Tests externes, internes et d'ingénierie sociale sur le périmètre convenu.

[03] SEMAINE 6 · CONSTATS ET CARTOGRAPHIE HIPAA

Consolidation des constats et mise en correspondance avec les mesures de sauvegarde pertinentes de la HIPAA Security Rule.

[04] SEMAINE 7 · ACCOMPAGNEMENT À LA CORRECTION

Accompagnement guidé de l'équipe d'ingénierie pour la correction avant nouveau test.

WAXTABLE.COM · EXAMPLE DOCUMENT

03

INVESTISSEMENT ET CONDITIONS

Des comptes de test et une lettre de règles d'engagement signée sont fournis avant le début des tests ; un interlocuteur est habilité à autoriser toute modification de périmètre à chaque étape ; et les tests se limitent au portail patient et à ses deux intégrations tierces désignées. Toute modification de ces conditions modifierait le calendrier et le coût, ce que nous conviendrions par écrit avant de poursuivre. Ce tarif est garanti pour tout engagement débutant au plus tard le 6 mars 2026.

FLUX DE TRAVAIL	SEMAINES	TAUX	MONTANT
Cadrage et reconnaissance Règles d'engagement, recensement des actifs et cartographie de la surface d'attaque	2	$9,500 / wk	$19,000
Test d'intrusion externe Évaluation du portail patient et de l'API exposés sur Internet	2	$14,000 / wk	$28,000
Tests internes et d'ingénierie sociale Scénario de poste compromis simulé et exercice de phishing	1	$16,000 / wk	$16,000
Examen des intégrations tierces Évaluation de la sécurité des API des résultats de laboratoire et du prestataire de facturation	1	$12,000 / wk	$12,000
Rapport et accompagnement à la correction Rapport de constats, cartographie HIPAA et recommandations de correction	1	$10,000 / wk	$10,000
Contre-test et mise en place de la maintenance Contre-test de vérification des correctifs et transmission du plan d'intervention en cas d'incident	1	$9,000 / wk	$9,000

Total de la mission	$94,000

HONORAIRES DE MISSION	$94,000
TAXE DE VENTE (WA – SERVICES PROFESSIONNELS EXONÉRÉS)	$0
TOTAL	$94,000

TOTAL DÛ **$94,000**

Tous les montants sont en USD. Facturation en trois étapes : 40 % à la signature, 30 % au début de la réalisation, 30 % à la livraison. Ce tarif est garanti pour tout engagement débutant au plus tard le 6 mars 2026.

01
ÉVALUATION
$94,000

- Engagement complet de huit semaines
- Tests externes, internes et d'ingénierie sociale
- Rapport de constats cartographié sur la norme HIPAA
- Deux semaines d'assistance à la remédiation

02
ÉVALUATION + FORFAIT
$6,500/mo

- Tout ce qui est inclus dans Évaluation
- Ligne directe de réponse aux incidents 24 h/24, 7 j/7
- Nouvelle analyse mensuelle des vulnérabilités
- SLA de réponse aux incidents prioritaire (< 4 h)

03
DÉFENSE CONTINUE
$13,000/mo

- Tout ce qui est inclus dans Forfait
- Exercices trimestriels d'équipe rouge
- Surveillance continue de la surface d'attaque externe
- Temps dédié en ingénierie de sécurité

OPTIONS

QUELLE FORMULE VOUS CONVIENT

	ÉVALUATION	ÉVALUATION + FORFAIT	DÉFENSE CONTINUE
Prix	$94,000	$6,500/mo	$13,000/mo
Périmètre principal	Engagement complet de huit semaines	Tout ce qui est inclus dans Évaluation	Tout ce qui est inclus dans Forfait
Ce qui est inclus	Tests externes, internes et d'ingénierie sociale	Ligne directe de réponse aux incidents 24 h/24, 7 j/7	Exercices trimestriels d'équipe rouge
Livraison	Rapport de constats cartographié sur la norme HIPAA	Nouvelle analyse mensuelle des vulnérabilités	Surveillance continue de la surface d'attaque externe
Suivi après livraison	Deux semaines d'assistance à la remédiation	SLA de réponse aux incidents prioritaire (< 4 h)	Temps dédié en ingénierie de sécurité

Les prix sont en USD et excluent la taxe sur les ventes (wa — services professionnels exonérés). Les options peuvent être combinées ou échelonnées ; la recommandation pour Meridian Health Systems est mise en avant dans la section tarifaire.

ÉCHÉANCIER DE PAIEMENT

ÉCHÉANCE DE CHAQUE VERSEMENT

N°	JALON	DÉCLENCHEUR	PART	MONTANT
01	Semaines 1 à 2 · Cadrage et reconnaissance	16 février 2026	40%	$37,600
02	Semaines 3 à 5 · Tests actifs	Au démarrage de la livraison	30%	$28,200
03	Semaine 6 · Constats et cartographie HIPAA	À l'acceptation du jalon	30%	$28,200
Total (HT)			**100%**	**$94,000**

Les échéances sont facturées au fur et à mesure des jalons ci-dessus et sont payables dans les 30 jours suivant chaque facture. Tous les montants sont exprimés en USD et s'entendent hors taxe de vente (wa — services professionnels exonérés).

HYPOTHÈSES SUR LESQUELLES REPOSE CETTE ESTIMATION

Des comptes de test et une lettre de règles d'engagement signée sont fournis avant le début des tests ; un interlocuteur est habilité à autoriser les changements de périmètre à chaque étape ; et les tests sont limités au portail patient et à ses deux intégrations tierces nommées. Toute modification de ces éléments affecte le calendrier et le coût, ce dont nous conviendrions par écrit avant de procéder. Ce tarif est valable pour les missions débutant au plus tard le 6 mars 2026.

La contresignature ci-dessous vaut acceptation du périmètre, du calendrier et de l'investissement définis dans cette proposition et autorise le démarrage des travaux.

POUR MERIDIAN HEALTH SYSTEMS

RENATA COLE

DIRECTRICE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Date

POUR NULLWIRE SECURITY

NULLWIRE SECURITY

SIGNATAIRE AUTORISÉ

Date

WAXTABLE.COM · EXAMPLE DOCUMENT

PROCHAINES ÉTAPES

PRÊTS QUAND VOUS LE SEREZ

L'acceptation de cette proposition déclenche le début des travaux le 16 février 2026. Le tarif reste valable pour les missions confirmées avant le 6 mars 2026.

Approuvez cette proposition et nous pourrons réserver un démarrage du cadrage pour la semaine du 16 février. Répondez à ce document ou écrivez à contact@nullwiresecurity.com.

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

WAXTABLE.COM · EXAMPLE DOCUMENT