NULLWIRE SECURITY

NULLWIRE SECURITY · ÉVALUATION DE SÉCURITÉ ET FORFAIT DE SUIVI

Portal Penetration Test

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.

WAXTABLE.COM · EXAMPLE DOCUMENT

2026

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.

POURQUOI MAINTENANT

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.

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

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 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.

> 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



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

WAXTABLE.COM · EXAMPLE DOCUMENT

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 année
Assurance responsabilité civile générale	Assureur commercial	Disponible sur demande	Travaux sur site et dans les locaux du client	Renouvelé chaque année
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.

[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.

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

MODÈLE ÉCONOMIQUE

COMMENT SE COMPARENT LES TROIS FORMULES

	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

WAXTABLE.COM · EXAMPLE DOCUMENT

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.

WAXTABLE.COM · EXAMPLE DOCUMENT

LA DEMANDE

REJOINDRE LE TOUR DE FINANCEMENT

Nous levons des fonds pour financer la feuille de route présentée à la page précédente. Nullwire Security accueillerait volontiers un échange de suivi ce trimestre.

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