NULLWIRE SECURITY

ANGEBOT FÜR MERIDIAN HEALTH SYSTEMS

Angebot für Penetrationstest des Portals

Eine umfassende Red-Team-Bewertung des Patientenportals, unterstützt durch ein Breach-Response-Abonnement – entwickelt für HIPAA-regulierte Infrastruktur.

2026

INHALT

AUF EINEN BLICK

ANGEBOT

PRO-2026-0771

ZUR FREIGABE

ERSTELLT FÜR

Meridian Health Systems — Renata Cole, Chief Information Security Officer

ERSTELLT VON
Nullwire Security, Seattle

AUSGESTELLT
22. Januar 2026

GÜLTIG BIS
6. März 2026

AUFTRAG
Sicherheitsbewert & Bereitschaftsvert

AUF EINEN BLICK

DAS PROJEKT IN FÜNF ZAHLEN

01
AUFTRAG
Sicherheitsbewertung & Bereitschaftsvertrag
Eine umfassende Red-Team-Bewertung des Patientenportals, unterstützt durch ein Breach-Response-Abonnement – entwickelt für HIPAA-regulierte Infrastruktur.

02
INVESTITION
$94,000
$94,000 zzgl. Umsatzsteuer (wa — professionelle Dienstleistungen befreit)

03
BEGINN
16. Februar 2026
Vorbehaltlich einer Annahme bis zum 6. März 2026

04
DAUER
12 Monate
Vom Projektstart bis zur finalen Übergabe

05
ERSTELLT FÜR
Meridian Health Systems
Renata Cole, Leiter Informationssicherheit

01

DIE CHANCE

Das Patientenportal von Meridian Health Systems verwaltet mittlerweile Laborergebnisse, Abrechnungen und Nachrichten für 340.000 Patienten – und wurde noch nie einem externen Red-Team-Assessment unterzogen. Dies ist der Plan, es ordentlich zu testen und vorbereitet zu sein, falls etwas durchdringt.

ZUSAMMENFASSUNG

Das Patientenportal von Meridian Health Systems hat sich von einem einfachen Terminplaner zum primären Kanal für Laborergebnisse, Abrechnung und sichere Nachrichten im gesamten Krankenhausnetzwerk entwickelt. Es wird vierteljährlich intern auf bekannte Schwachstellen gescannt, stand jedoch noch nie einem externen Angreifer gegenüber, der kleine Schwachstellen so verkettet, wie es ein echter Angreifer tun würde – und ein durchschnittlicher Datenschutzvorfall im Gesundheitswesen wird immer noch erst nach über 200 Tagen entdeckt.

Nullwire Security schlägt ein achtwöchiges Engagement vor, das einen umfassenden Penetrationstest – extern, intern und Social Engineering – mit einem laufenden Breach-Response-Abonnement kombiniert, sodass Meridian vor einem Vorfall getestet und während eines Vorfalls reaktionsbereit ist. Die folgenden Abschnitte erläutern den Ansatz, den Leistungsumfang, den Zeitplan und die Investition.

DIE HERAUSFORDERUNG

Interne Schwachstellenscans erkennen bekannte CVEs, übersehen jedoch verkettete Exploits, falsch konfigurierte Drittanbieter-Integrationen und die menschlichen Schwachstellen, auf die eine Phishing-Kampagne abzielen würde. Die Labor-Ergebnis-API und die Anbindung des Abrechnungsdienstleisters von Meridian wurden noch nie unabhängig geprüft.

Operativ wurden Erkennung und Reaktion noch nie anhand eines realen Szenarios geprobt. Käme es tatsächlich zu einem Sicherheitsvorfall, wäre der vorliegende Incident-Response-Plan ungetestet, und dem Team ist nicht bekannt, wie lange die Eindämmung tatsächlich dauern würde.

UNSER ANSATZ

Wir führen das Engagement so durch, wie es ein echter Angreifer tun würde: externe Aufklärung und Exploitation, laterale Bewegung von einem simulierten kompromittierten Endpunkt aus sowie eine Social-Engineering-Kampagne gegen den Helpdesk, ergänzt durch eine gezielte Prüfung der beiden Drittanbieter-Integrationen, über die Patientendaten laufen.

Die Ergebnisse werden direkt der HIPAA Security Rule zugeordnet und mit einem Nachtest zur Behebung zurückgegeben, sodass nichts als abgeschlossen markiert wird, bevor die Behebung verifiziert ist. Das Breach-Response-Abonnement hält anschließend dasselbe Team einsatzbereit, sodass der nächste Vorfall geprobt statt improvisiert abläuft.

01
140+
DURCHGEFÜHRTE PENETRATIONSTESTS

02
<4 Std.
MITTLERE AKTIVIERUNGSZEIT BEI SICHERHEITSVORFÄLLEN

03
8 Wochen
VON DER SCOPE-FESTLEGUNG BIS ZUM ABSCHLUSSBERICHT

STATUS

REGISTRIERUNGEN, VERSICHERUNGSSCHUTZ UND NACHWEISE

NACHWEIS	AUSSTELLENDE STELLE	REFERENZ	UMFANG	STATUS
Eingetragene Gesellschaft	Handelsregister, Vereinigte Staaten	Nullwire Security LLC	Handelsname und Rechtsform	Aktiv
Steuerliche Registrierung	Finanzbehörde, Vereinigte Staaten	EIN 91-4820376	Alle in Rechnung gestellten Leistungen	Aktiv
Berufshaftpflichtversicherung	Gewerblicher Versicherer	Auf Anfrage erhältlich	Sicherheitsbewertung & Bereitschaftsvertrag	Wird jährlich erneuert
Betriebshaftpflichtversicherung	Gewerblicher Versicherer	Auf Anfrage erhältlich	Arbeiten vor Ort und in den Räumlichkeiten des Kunden	Wird jährlich erneuert

Mitgliedschaft in einem Branchenverband	Branchenverband, Vereinigte Staaten	Auf Anfrage erhältlich	Verhaltenskodex und Beschwerdeverfahren	In gutem Rechtsstand

Zertifikate und Versicherungsnachweise werden auf Anfrage zur Verfügung gestellt und werden Meridian Health Systems auf Anfrage jederzeit während des Auftrags erneut ausgestellt.

> **Nullwire hat eine verkettete Schwachstelle gefunden, die unser internes Team zwei Jahre lang übersehen hatte, und uns beim realen Test des Retainers innerhalb einer Stunde unter Kontrolle gebracht.**
>
> OWEN MARSH

02

LEISTUNGSUMFANG

Ein achtwöchiger Auftrag, der einen umfassenden Penetrationstest mit einem ständigen Bereitschaftsvertrag für die Reaktion auf Sicherheitsvorfälle verbindet, sodass Meridian Health Systems vor einem Vorfall getestet und während eines Vorfalls reaktionsbereit ist.

01
EXTERNER PENETRATIONSTEST

Internetzugängliche Systeme, das Patientenportal und dessen öffentliche APIs, bis zur Ausnutzung getestet.

02
INTERNE & LATERALE BEWEGUNG

Ein simuliertes Szenario eines kompromittierten Endgeräts, das testet, wie weit sich ein Angreifer nach dem Eindringen bewegen könnte.

03
SOCIAL ENGINEERING

Eine Phishing-Simulation und eine Pretexting-Kampagne gegen den Helpdesk bei Mitarbeitenden.

04
PRÜFUNG DER DRITTANBIETER-INTEGRATIONEN

Sicherheitsbewertung der API-Verbindungen zu Laborergebnis- und Abrechnungsdienstleistern.

05
RETAINER FÜR DIE REAKTION AUF SICHERHEITSVORFÄLLE

Rufbereite Vorfallreaktion und ein geprobtes, einsatzbereites Runbook für Sicherheitsvorfälle.

06
COMPLIANCE-BERICHTERSTATTUNG

Ergebnisse direkt der HIPAA Security Rule zugeordnet für Audits und Berichte an den Vorstand.

LEISTUNGEN

[01] TESTING

BERICHT ZUM UMFASSENDEN PENETRATIONSTEST

Externe, interne und laterale Bewegungsbefunde mit Proof-of-Concept-Details und Schweregradeinstufungen.

[02] TESTING

SOCIAL-ENGINEERING-BEWERTUNG

Ergebnisse zu Phishing und Helpdesk-Pretexting mit Sensibilisierungsempfehlungen für Mitarbeiter.

[03] REAKTION

RUNBOOK FÜR DIE REAKTION AUF SICHERHEITSVORFÄLLE

Ein erprobter Notfallreaktionsplan mit festgelegten Rollen, Eskalationswegen und der Nullwire-Bereitschaftsleitung.

[04] COMPLIANCE

HIPAA-ZUGEORDNETER BEFUNDBERICHT

Jeder Befund ist der jeweiligen HIPAA Security Rule-Schutzmaßnahme zugeordnet und auditbereit.

[05] BEREITSTELLUNG

NACHTEST ZUR BEHEBUNG & ABNAHME

Ein Nachtest, der die Behebung jedes Befunds bestätigt, mit schriftlicher Abnahme.

NICHT IM LEISTUNGSUMFANG ENTHALTEN

- Physische Penetrationstests von Einrichtungen über die beiden genannten Rechenzentren hinaus
- Quellcode-Audit von Anwendungen externer Anbieter
- Fortlaufende 24/7-SOC-Überwachung über das Bereitschaftsfenster des Vertrags hinaus
- Behördliche Meldungen und Rechtsberatung zur Verletzungsmeldung



[01] ▸ WOCHEN 1–2 · SCOPING & AUFKLÄRUNG

Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche.

[02] ▸ WOCHEN 3–5 · AKTIVE TESTS

Externe, interne und Social-Engineering-Tests gemäß vereinbartem Umfang.

[03] ▸ WOCHE 6 · ERGEBNISSE & HIPAA-MAPPING

Konsolidierung der Ergebnisse und Zuordnung zu den relevanten Schutzmaßnahmen der HIPAA Security Rule.

[04] ▸ WOCHE 7 · UNTERSTÜTZUNG BEI DER BEHEBUNG

Begleitete Unterstützung des Engineering-Teams bei der Behebung vor dem Nachtest.

03

INVESTITION & KONDITIONEN

Testkonten und ein unterschriebenes Rules-of-Engagement-Schreiben werden vor Testbeginn bereitgestellt; ein Stakeholder ist bei jeder Phase befugt, Änderungen am Umfang zu genehmigen; und die Tests sind auf das Patientenportal und dessen zwei benannte Drittanbieter-Integrationen begrenzt. Änderungen daran verschieben Zeitplan und Kosten, was wir vor Fortsetzung schriftlich vereinbaren würden. Das Honorar gilt für Aufträge, die bis spätestens 6. März 2026 beginnen.

ARBEITSBEREICH	WOCHEN	SATZ	BETRAG
Scoping & Aufklärung Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche	2	$9,500 / wk	$19,000
Externer Penetrationstest Bewertung des internetzugänglichen Patientenportals und der API	2	$14,000 / wk	$28,000
Interne & Social-Engineering-Tests Simuliertes Szenario mit kompromittiertem Endpunkt und Phishing-Übung	1	$16,000 / wk	$16,000
Prüfung der Drittanbieter-Integrationen Sicherheitsbewertung der API von Labor-Ergebnis- und Abrechnungsdienstleistern	1	$12,000 / wk	$12,000
Berichterstattung & Unterstützung bei der Behebung Ergebnisbericht, HIPAA-Mapping und Anleitung zur Behebung	1	$10,000 / wk	$10,000
Retest & Einrichtung Retainer Erneute Prüfung der Fehlerbehebung und Übergabe des Breach-Response-Runbooks	1	$9,000 / wk	$9,000
Gesamtsumme des Auftrags			**$94,000**

AUFTRAGSGEBÜHR	$94,000
UMSATZSTEUER WA (PROFESSIONELLE DIENSTLEISTUNGEN STEUERBEFREIT)	$0
GESAMT	$94,000

FÄLLIGER GESAMTBETRAG **$94,000**

Alle Beträge in USD. Abrechnung in drei Meilensteinen: 40% bei Unterzeichnung, 30% bei Baubeginn, 30% bei Lieferung. Das Honorar gilt für Aufträge, die bis spätestens 6. März 2026 beginnen.

01 BEWERTUNG

$94,000

- Vollständiges achtwöchiges Engagement
- Externe, interne und Social-Engineering-Tests
- HIPAA-zugeordneter Befundbericht
- Zwei Wochen Unterstützung bei der Behebung

02 BEWERTUNG + RETAINER

$6,500/mo

- Alles aus Assessment
- Rund um die Uhr erreichbare Hotline für Sicherheitsvorfälle
- Monatlicher erneuter Schwachstellenscan
- Priority-SLA für die Reaktion auf Sicherheitsvorfälle [<4 Std.]

03 KONTINUIERLICHE VERTEIDIGUNG

$13,000/mo

- Alles aus Retainer
- Vierteljährliche Red-Team-Übungen
- Kontinuierliche Überwachung der externen Angriffsfläche
- Eingebettete Zeit für Sicherheitsentwicklung

OPTIONEN

WELCHES FORMAT PASST ZU IHNEN

	BEWERTUNG	BEWERTUNG + RETAINER	KONTINUIERLICHE VERTEIDIGUNG
Preis	$94,000	$6,500/mo	$13,000/mo
Kernumfang	Vollständiges achtwöchiges Engagement	Alles aus Assessment	Alles aus Retainer
Was enthalten ist	Externe, interne und Social-Engineering-Tests	Rund um die Uhr erreichbare Hotline für Sicherheitsvorfälle	Vierteljährliche Red-Team-Übungen
Lieferung	HIPAA-zugeordneter Befundbericht	Monatlicher erneuter Schwachstellenscan	Kontinuierliche Überwachung der externen Angriffsfläche
Nachbetreuung	Zwei Wochen Unterstützung bei der Behebung	Priority-SLA für die Reaktion auf Sicherheitsvorfälle (<4 Std.)	Eingebettete Zeit für Sicherheitsentwicklung

Die Preise verstehen sich in USD zzgl. der Umsatzsteuer (wa — freiberufliche Dienstleistungen befreit). Optionen können kombiniert oder gestaffelt werden; die Empfehlung für Meridian Health Systems ist im Preisabschnitt hervorgehoben.

ZAHLUNGSPLAN

FÄLLIGKEIT DER EINZELNEN RATEN

NR.	MEILENSTEIN	AUSLÖSER	ANTEIL	BETRAG
01	Wochen 1–2 · Scoping & Aufklärung	16. Februar 2026	40%	$37,600
02	Wochen 3–5 · Aktive Tests	Bei Lieferbeginn	30%	$28,200

03	Woche 6 · Ergebnisse & HIPAA-Mapping	Bei Abnahme des Meilensteins	30%	$28,200
Gesamt (netto)			**100%**	**$94,000**

Die Raten werden entsprechend den oben genannten Meilensteinen in Rechnung gestellt und sind innerhalb von 30 Tagen nach Rechnungsdatum fällig. Alle Beträge verstehen sich in USD zzgl. Umsatzsteuer (wa — professionelle Dienstleistungen befreit).

ANNAHMEN, AUF DENEN DIESE KALKULATION BERUHT

Testkonten und ein unterschriebenes Schreiben zu den Regeln des Engagements werden vor Testbeginn bereitgestellt; ein Stakeholder ist befugt, Änderungen am Umfang bei jeder Phase zu genehmigen; und die Tests beschränken sich auf das Patientenportal und seine beiden benannten Drittanbieter-Integrationen. Änderungen daran wirken sich auf Zeitplan und Kosten aus, worüber wir vor der Umsetzung schriftlich Einvernehmen herstellen würden. Das Honorar gilt für Engagements, die bis zum 6. März 2026 beginnen.

Die Gegenzeichnung unten bedeutet die Annahme von Umfang, Zeitplan und Investition dieses Angebots und autorisiert den Arbeitsbeginn.

FÜR MERIDIAN HEALTH SYSTEMS

RENATA COLE

CHIEF INFORMATION SECURITY OFFICER

Datum

FÜR NULLWIRE SECURITY

NULLWIRE SECURITY

BEVOLLMÄCHTIGTER UNTERZEICHNER

Datum

NÄCHSTE SCHRITTE

BEREIT, WENN SIE ES SIND

Mit der Annahme dieses Angebots beginnt die Arbeit am 16. Februar 2026. Das Honorar gilt für Aufträge, die bis zum 6. März 2026 bestätigt werden.

Genehmigen Sie diesen Vorschlag, und wir reservieren einen Scoping-Start für die Woche vom 16. Februar. Antworten Sie auf dieses Dokument oder schreiben Sie eine E-Mail an contact@nullwiresecurity.com.

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