NULLWIRE SECURITY

ERSTELLT FÜR MERIDIAN HEALTH SYSTEMS

Leistungsbeschreibur

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

2026

INHALT

01 Auf einen Blick 2
02 Umfang, Zeitplan & Honorar 3
03 Überblick & Ziele 5
04 Hintergrund & Ziele 5
05 Leistungen 5
06 Arbeitsstränge 6
07 Workstream-Spezifikation 7
08 Zeitplan 7
09 Abnahmekriterien 8
10 Kostenaufstellung 8
11 Kostenübersicht 9
12 Zahlungsplan 9
13 Annahme 10

AUF EINEN BLICK

SOW

SOW-2026-0771

ENTWURF

ERSTELLT FÜR
Meridian Health Systems — Renata Cole, Chief Information Security Officer

ERSTELLT VON
Nullwire Security, Seattle

SOW-NUMMER
SOW-2026-0771

STARTDATUM
16. Februar 2026

DAUER
Sicherheitsbewert & Bereitschaftsvert

STATUS
Entwurf — zur Prüfung

AUF EINEN BLICK

UMFANG, ZEITPLAN UND HONORAR

01
ARBEITSBEREICH

Sicherheitsbewertung & Bereitschaftsvertrag

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

02
BEGINN

16. Februar 2026

Bei Gegenzeichnung

03
DAUER

12 Monate

Gestaffelt gemäß nachstehendem Zeitplan

04
HONORAR

$94,000

$94,000 zzgl. Umsatzsteuer (wa – professionelle Dienstleistungen befreit)

05
ANGENOMMEN VON

Renata Cole

Chief Information Security Officer

01

ÜBERBLICK & ZIELE

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.

HINTERGRUND & ZIELE

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.

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]

TESTS AUF ANGREIFERNIVEAU

Externe, interne und Social-Engineering-Tests, verkettet, wie es ein echter Angreifer tun würde.

[02]

HIPAA-ZUGEORDNETES REPORTING

Jeder Befund der relevanten Sicherheitsmaßnahme der HIPAA Security Rule zugeordnet, bereit für Audit und Berichterstattung an den Vorstand.

[03]

STÄNDIGE EINSATZBEREITSCHAFT

Ein eingeübtes Runbook für die Reaktion auf Sicherheitsvorfälle und ein Bereitschaftsdienst, sodass der nächste Vorfall geübt statt improvisiert abläuft.

SPEZIFIKATION

WORKSTREAM-SPEZIFIKATION

REF.	POSITION	SPEZIFIKATION	AUFWAND	VORLAUFZEIT	EINZELPREIS
SPC-01	Scoping & Aufklärung	Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche	2	2 Wo.	$9,500 / wk
SPC-02	Externer Penetrationstest	Bewertung des internetzugänglichen Patientenportals und der API	2	2 Wo.	$14,000 / wk
SPC-03	Interne & Social-Engineering-Tests	Simuliertes Szenario mit kompromittiertem Endpunkt und Phishing-Übung	1	1 Wo.	$16,000 / wk
SPC-04	Prüfung der Drittanbieter-Integrationen	Sicherheitsbewertung der API von Labor-Ergebnis- und Abrechnungsdienstleistern	1	1 Wo.	$12,000 / wk
SPC-05	Berichterstattung & Unterstützung bei der Behebung	Ergebnisbericht, HIPAA-Mapping und Anleitung zur Behebung	1	1 Wo.	$10,000 / wk

Die Spezifikationen werden mit der Abnahme festgelegt; jede Änderung wird über das in diesem Dokument beschriebene Änderungsverfahren abgewickelt.

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

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

[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.

[05] ▸ WOCHE 8 · NACHTEST & AKTIVIERUNG DES RETAINERS

Erneute Fehlerbehebungsprüfung und Übergabe des Runbooks zur Vorfallsreaktion.

ABNAHMEKRITERIEN

REF.	ANFORDERUNG	PRIORITÄT
R-01	Externe und interne Tests müssen das Patientenportal und seine zwei benannten Drittanbieter-Integrationen umfassen	MUSS
R-02	Testkonten und ein unterschriebenes Rules-of-Engagement-Schreiben werden vor Testbeginn bereitgestellt	MUSS
R-03	Alle Feststellungen werden der jeweiligen HIPAA-Security-Rule-Schutzmaßnahme zugeordnet	MUSS
R-04	Kritische und hohe Feststellungen werden vor der endgültigen Abnahme erneut getestet und als geschlossen verifiziert	MUSS
R-05	Die Social-Engineering-Kampagne beschränkt sich auf den Helpdesk und benannte Abteilungen	MUSS

ARBEITSBEREICH	WOCHEN	SATZ	BETRAG
Scoping & Aufklärung Regeln des Engagements, Erfassung der Assets und Mapping der Angriffsfläche	2	$9,500 / wk	$19,000

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
Zwischensumme Honorare			**$94,000**

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

GESAMT **$94,000**

Alle Beträge verstehen sich in USD und exklusive geltender Steuern. Honorare werden in drei Meilensteinen abgerechnet: 40 % bei Unterzeichnung, 30 % bei Baubeginn, 30 % beim Go-Live.

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).

Mit der Gegenzeichnung unten werden Umfang, Zeitplan, Abnahmekriterien und Honorare dieser Leistungsbeschreibung akzeptiert und der Arbeitsbeginn zum angegebenen Startdatum autorisiert.

FÜR MERIDIAN HEALTH SYSTEMS

RENATA COLE

CHIEF INFORMATION SECURITY OFFICER

Datum

FÜR NULLWIRE SECURITY

NULLWIRE SECURITY

BEVOLLMÄCHTIGTER UNTERZEICHNER

Datum

NULLWIRE SECURITY

500 Yale Ave N, Seattle, WA 98109, United States

contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com

Nullwire Security LLC · EIN 91-4820376