

► VERTRAG

RAHMENVERTRAG ÜBER DIENSTLEISTUNGEN

Sicherheitsbewertung &
Bereitschaftsvertrag



► DER AUFTRAGNEHMER

NULLWIRE SECURITY

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

► DER KUNDE

**MERIDIAN HEALTH
SYSTEMS**

4400 Forbes Blvd, Columbus, OH 43219,
United States

Dieser Vertrag wird zwischen den nachstehend genannten Parteien geschlossen und tritt zum angegebenen Wirksamkeitsdatum in Kraft. Er ersetzt alle vorherigen Besprechungen zum selben Gegenstand.

VERTRAG NR.

CTR-2026-0771

DATUM DES
INKRAFTTRETENS

**16. Februar
2026**

LAUFZEIT

12 Monate

ANWENDBARES RECHT

**Bundesstaat
Washington,
USA**

AUFTRAG

**Sicherheitsbewertung
&
Bereitschaftsvertrag**

STATUS

**Zur
Unterzeichnung**

Nullwire Security LLC

Vertraulich – erstellt für Meridian Health Systems. Nicht zur Weitergabe über die genannten Parteien hinaus.

INHALT

► 01	Vertrag	1
► 02	Die Parteien	2
► 03	Kommerzielle Bedingungen	2
► 04	Auftragsübersicht	4
► 05	Hintergrund	4
► 06	Leistungsumfang & Liefergegenstände	4
► 07	Leistungsbeschreibung	5
► 08	Projektzeitplan	7
► 09	Honorarplan	7
► 10	Honorarübersicht	8
► 11	Zahlungsplan	8
► 12	Status & Versicherungsschutz	9
► 13	Allgemeine Geschäftsbedingungen	10
► 14	Unterzeichnung	11

► DER AUFTRAGNEHMER ■

NULLWIRE SECURITY

NULLWIRE SECURITY LLC · EIN
91-4820376

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

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

|||||

► DER KUNDE ■

**MERIDIAN HEALTH
SYSTEMS**

MERIDIAN HEALTH SYSTEMS (EIN
GEMEINNÜTZIGES
KRANKENHAUSNETZWERK)

4400 Forbes Blvd, Columbus, OH 43219,
United States

accountspayable@meridianhealthsystems.or
· +1 614 555 0143

|||||

► KOMMERZIELLE BEDINGUNGEN ■

DIE BEDINGUNGEN, DIE DIESEN VERTRAG REGELN

01

DATUM DES INKRAFTTRETENS

16. Februar 2026

Das Datum, an dem die Verpflichtungen beginnen

02

ANFÄNGLICHE LAUFZEIT

12 Monate

Verlängert sich nur durch schriftliche Vereinbarung

03

GESAMTHONORAR

\$94,000

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

04

ZAHLUNGSBEDINGUNGEN

Netto 30 Tage

Ab dem Datum jeder gültigen Rechnung

05

ANWENDBARES RECHT

Bundesstaat

Washington, USA

King County, Washington

► 01 ■

AUFTRAGSÜBERSICHT

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

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.

LEISTUNGSUMFANG & LIEFERGEGENSTÄNDE

[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

NACHTTEST 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

SPEZIFIKATION

LEISTUNGSBESCHREIBUNG

REF.	POSITION	SPEZIFIKATION	AUFWAND	VORLAUFZEIT	INZELPREIS
------	----------	---------------	---------	-------------	------------

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 Abrechnungsdienstleistungen	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.

[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.

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
Gesamthonorar			\$94,000

HONORARE FÜR
PROFESSIONELLE
DIENSTLEISTUNGEN \$94,000

UMSATZSTEUER WA
(PROFESSIONELLE
DIENSTLEISTUNGEN
STEUERBEFREIT) \$0

MAXIMALER VERTRAGSWERT \$94,000

MAXIMALER
VERTRAGSWERT \$94,000

Alle Beträge verstehen sich in USD zzgl.
anwendbarer Steuern zum jeweils geltenden Satz.
Honorare werden monatlich nachträglich nach
Projektfortschritt in Rechnung gestellt und sind
innerhalb von 30 Tagen ab Rechnungsdatum zahlbar.
Spesen werden nach vorheriger schriftlicher
Zustimmung zu Selbstkosten abgerechnet.

■ Z A H L U N G S P L A N

FÄLLIGKEIT DER
EINZELNEN RATEN

NR.	MEILENSTEIN	AUSLÖSER	ANTEIL	BETRAG
01	Wochen 1–2 · Scoping & Aufklärung	16. Februar 2026	30%	\$28,200
02	Wochen 3–5 · Aktive Tests	Bei Lieferbeginn	30%	\$28,200
03	Woche 6 · Ergebnisse & HIPAA-Mapping	Bei Abnahme des Meilensteins	20%	\$18,800
04	Woche 7 · Unterstützung bei der Behebung	Bei der endgültigen Übergabe	20%	\$18,800
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).

■ 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
Berufshaftpflichtvers icherung	Gewerblicher Versicherer	Auf Anfrage erhältlich	Sicherheitsbe wertung & Bereitschaftsv ertrag	Wird jährlich erneuert
Betriebshaftpflichtve rsicherung	Gewerblicher Versicherer	Auf Anfrage erhältlich	Arbeiten vor Ort und in den Räumlichkeite n des Kunden	Wird jährlich erneuert
Mitgliedschaft in einem Branchenverband	Branchenverband , Vereinigte Staaten	Auf Anfrage erhältlich	Verhaltenskod ex und Beschwerdeve rfahren	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.

ALLGEMEINE GESCHÄFTSBEDINGUNGEN

[01] 1. LAUFZEIT & KÜNDIGUNG

Dieser Vertrag tritt am oben genannten Datum des Inkrafttretens in Kraft und läuft für die oben angegebene anfängliche Laufzeit weiter, sofern er nicht gemäß dieser Klausel vorzeitig gekündigt wird. Jede Partei kann den Auftrag oder ein Statement of Work mit einer Frist von 30 Tagen schriftlich kündigen. Jede Partei kann fristlos schriftlich kündigen, wenn die andere Partei eine wesentliche Vertragsverletzung begeht, die nicht innerhalb von 15 Werktagen nach entsprechender Mitteilung behoben wird, oder wenn sie zahlungsunfähig wird. Bei Kündigung hat der Kunde alle ordnungsgemäß erbrachten Leistungen und ordnungsgemäß entstandenen Auslagen bis zum Zeitpunkt der Kündigung zu bezahlen.

[02] 2. HONORARE & ZAHLUNG

Der Kunde zahlt die im Honorarplan festgelegten Gebühren, zuzüglich anfallender Steuern. Nullwire Security stellt monatlich nachträglich entsprechend dem Fortschritt Rechnung; jede Rechnung ist innerhalb von 30 Tagen ab Rechnungsdatum zahlbar. Vorab genehmigte Auslagen werden zum Selbstkostenpreis weiterberechnet und dürfen den vereinbarten Höchstbetrag ohne vorherige schriftliche Zustimmung des Kunden nicht überschreiten. Nullwire Security kann auf überfällige Beträge Zinsen zum gesetzlich zulässigen Höchstsatz berechnen, die täglich anfallen.

[03] 3. GEISTIGES EIGENTUM

Jede Partei behält das Eigentum an geistigem Eigentum, das sie vor Beginn des Auftrags besaß oder das sie unabhängig davon entwickelt. Nach vollständiger Zahlung der jeweiligen Gebühren überträgt Nullwire Security dem Kunden alle Rechte an geistigem Eigentum an den speziell für den Kunden im Rahmen dieser Vereinbarung erstellten individuellen Leistungen. Nullwire Security behält das Eigentum an seinen Methoden, Rahmenwerken, Werkzeugen und Know-how und gewährt dem Kunden eine unbefristete, nicht-exklusive Lizenz zu deren Nutzung, soweit sie in die Leistungen eingebettet sind, für seine internen Geschäftszwecke.

[04] 4. VERTRAULICHKEIT

Jede Partei hält alle nicht öffentlichen Informationen, die die andere Partei im Zusammenhang mit diesem Vertrag offenlegt, vertraulich, verwendet sie nur zur Erfüllung ihrer Pflichten und schützt sie mit mindestens der Sorgfalt, die sie auf ihre eigenen vertraulichen Informationen anwendet. Diese Pflichten gelten nicht für Informationen, die öffentlich sind oder ohne Verschulden der empfangenden Partei öffentlich werden, die vor der Offenlegung bereits rechtmäßig bekannt waren oder deren Offenlegung gesetzlich oder behördlich vorgeschrieben ist. Diese Klausel gilt nach Beendigung des Vertrags für einen Zeitraum von fünf Jahren fort.

[05] 5. HAFTUNG & FREISTELLUNG

Keine der Parteien schließt die Haftung für Tod oder Personenschäden aus, die durch ihre Fahrlässigkeit verursacht wurden, für Betrug oder für Haftung, die gesetzlich nicht ausgeschlossen werden kann. Vorbehaltlich dessen haftet keine der Parteien für indirekte oder Folgeschäden oder für entgangenen Gewinn, Umsatz oder erwartete Einsparungen. Die gesamte Haftung von Nullwire Security, die sich aus dieser Vereinbarung ergibt oder damit im Zusammenhang steht, ist auf die Gesamtgebühren beschränkt, die im Rahmen des betreffenden Leistungsscheins in den 12 Monaten vor dem Ereignis, das den Anspruch begründet, gezahlt wurden. Nullwire Security unterhält eine Berufshaftpflichtversicherung in wirtschaftlich angemessener Höhe.

[06] 6. ANWENDBARES RECHT & STREITIGKEITEN

Diese Vereinbarung und jede daraus oder in Verbindung damit entstehende Streitigkeit unterliegen den Gesetzen des Bundesstaates Washington, USA. Die Parteien werden zunächst versuchen, jede Streitigkeit in gutem Glauben durch Eskalation an ihre jeweiligen leitenden Ansprechpartner beizulegen. Wird die Streitigkeit nicht innerhalb von 30 Tagen beigelegt, haben die Gerichte von King County, Washington die ausschließliche Zuständigkeit, wobei jede Partei einstweiligen Rechtsschutz bei jedem zuständigen Gericht beantragen kann.

ANWENDBARES RECHT

Bundesstaat Washington, USA

GERICHTSSTAND

King County, Washington

Dieser Vertrag wird von den ordnungsgemäß bevollmächtigten Vertretern der Parteien unterzeichnet und tritt am oben genannten Datum des Inkrafttretens in Kraft.

FÜR UND IM NAMEN
 ▶ VON MERIDIAN
 HEALTH SYSTEMS

RENATA COLE
 CHIEF INFORMATION
 SECURITY OFFICER

Datum

FÜR UND IM NAMEN VON
 ▶ 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