Wie unterstützt Cyber Crucible HIPAA, und wird eine Business Associate Agreement unterzeichnet?

Kurze Antwort: Cyber Crucible unterstützt die HIPAA-Verpflichtungen einer Covered Entity in erster Linie dadurch, dass niemals geschützte Gesundheitsinformationen (PHI) erfasst werden. Die Analyse erfolgt lokal auf dem Endpunkt, sodass PHI für die Sicherheitsverarbeitung nicht in eine Drittanbieter-Cloud hochgeladen werden. Da Cyber Crucible keine PHI im Auftrag einer Covered Entity erstellt, empfängt, verwaltet oder überträgt, erfüllt es in der Regel nicht die Definition eines Business Associate — sofern jedoch der Risikoprozess eines Kunden dies erfordert, kann eine Business Associate Agreement abgeschlossen werden.

Warum die Architektur für das Gesundheitswesen geeignet ist

- **PHI verlässt für die Sicherheitsanalyse niemals das Gerät.** Viele anbietergehostete SOC/MDR-Lösungen laden Dateien, Schlüssel oder Telemetriedaten in eine Drittanbieter-Cloud hoch; Cyber Crucible analysiert auf dem Endpunkt, sodass diese Gefährdung vermieden wird.
- **Klinische Kontinuität.** Nur der bösartige Prozess wird angehalten — keine vollständige Systemisolierung oder erzwungener Neustart — sodass angeschlossene Geräte und klinische Systeme weiterlaufen, während ein Angriff neutralisiert wird.
- **Ransomware-Schutz ohne 24/7-SOC.** Die autonome Prävention stoppt Angriffe bereits vor der Ausführung, ohne dass Analysten erforderlich sind, die ein Krankenhaus möglicherweise nicht bereitstellen kann.

Die ehrliche Grenze

Cyber Crucible ist nicht „HIPAA-zertifiziert" — eine solche Zertifizierung gibt es nicht. Es unterstützt Ihr Compliance-Programm; Ihre Datenschutz- und Sicherheitsbeauftragten treffen die Entscheidung für Ihre Umgebung. Eine BAA ist auf Anfrage über **dpo@cybercrucible.com** erhältlich.

Revision #1
Created 2026-07-24 04:53:09 UTC by Dennis Underwood
Updated 2026-07-24 04:53:09 UTC by Dennis Underwood