

Wie unterstützt Cyber Crucible die HIPAA-Konformität im Gesundheitswesen?

Kurze Antwort: Die gesamte Analyse erfolgt lokal auf Kernel-Ebene, sodass geschützte Gesundheitsdaten für die Sicherheitsverarbeitung niemals den Endpunkt verlassen. Damit wird das HIPAA-Risiko vermieden, das durch Sicherheitstools entsteht, die sensible Dateien oder Schlüssel in Drittanbieter-Clouds hochladen, und Angriffe werden gestoppt, ohne klinische Systeme offline zu nehmen.

Das Problem mit anbietergehosteter Sicherheit

Viele anbietergehostete SOC- und MDR-Vereinbarungen erfordern das Hochladen sensibler Schlüssel, Dateien oder Telemetriedaten in Cloud-Datenbanken von Drittanbietern. Für eine dem Gesetz unterliegende Einrichtung (Covered Entity) entsteht dadurch ein reales Compliance-Risiko, und die Anzahl der Parteien, die geschützte Daten verarbeiten, wird erweitert.

Lokale Analyse, lokale Daten

Cyber Crucible führt die Analyse am Endpunkt durch. Sensible Assets verlassen niemals die sichere Grenze des Geräts – dies unterstützt sowohl die Datensouveränität als auch die damit verbundene regulatorische Position.

Kontinuität ist klinisch entscheidend

Eine Eindämmung, die das Isolieren eines Geräts oder einen erzwungenen Neustart erfordert, ist inakzeptabel, wenn die Patientenversorgung davon abhängt. Die selektive Aussetzung ausschließlich des bösartigen Prozesses bedeutet, dass der Angriff in weniger als 200 Millisekunden neutralisiert wird, während medizinische Abläufe, vernetzte Geräte und klinische Systeme weiterlaufen.