Wie reduziert Cyber Crucible das Dritt- und Anbieterrisiko für regulierte Kunden?

Kurze Antwort: Indem das Risiko beseitigt und nicht nur verwaltet wird. Die drei Tatsachen, die die schwierigsten Fragen zum Anbieterrisiko beantworten, sind: Cyber Crucible erfasst keine Kundeninhalte, Zugangsdaten oder Schlüssel; der Schutz läuft lokal und übersteht jeden Backend-Ausfall; und die KI existiert ausschließlich in der Entwicklung, niemals auf Ihrem Endpunkt. Zusammen verkleinern diese Faktoren die Angriffsfläche, die eine Due-Diligence-Prüfung untersuchen soll.

Die drei strukturellen Risikominderer

- **Keine Inhalte.** Es werden niemals Kundendateien, Zugangsdaten oder Schlüssel erfasst. Diese eine Tatsache beantwortet die Fragenkomplexe zu PCI, vertraulichen Daten und „was passiert, wenn Sie kompromittiert werden“ — die Daten sind schlicht nicht vorhanden, um verloren zu gehen.
- **Backend-unabhängiger Schutz.** Detect–Decide–Respond läuft lokal, mit einem effektiven Recovery-Time-Objective von null auf dem Endpunkt. Ein vollständiger Backend-Ausfall mindert den Schutz nicht.
- **Deterministische KI.** KI wird ausschließlich in der Entwicklung eingesetzt; zur Laufzeit laufen deterministische Heuristiken. Kein Live-Modell, kein Drift, testbare Ergebnisse.

Unabhängige Bestätigung

Wo unabhängige Testate Gewicht haben, verweist Cyber Crucible auf das, was real ist: die Microsoft-WHCP-Treibersignierung sowie — für das verwaltete Backend — die Testate Dritter der Infrastrukturanbieter, auf die es sich stützt. Ohne eigenes SOC 2 tragen diese die Last ehrlich, statt überbewertet zu werden.

Revision #1
Created 2026-07-24 04:52:38 UTC by Dennis Underwood
Updated 2026-07-24 04:52:38 UTC by Dennis Underwood