Wie trifft Cyber Crucible eine Entscheidung in unter 200 Millisekunden?

Kurze Antwort: Es durchläuft eine dreistufige Schleife – Detect, Decide, Respond –, die vollständig auf dem Endpunkt auf Kernel-Ebene ausgeführt wird, unter Verwendung einer patentierten Edge-Computing-Analyse-Engine. Da nichts zu einem Cloud-Dienst und zurück übertragen werden muss und kein Mensch involviert ist, wird der gesamte Zyklus in unter 200 Millisekunden abgeschlossen.

Die Schleife

1. **Detect** – neuartige Sensoren auf Kernel-Ebene identifizieren bösartige Verhaltensmuster im Arbeitsspeicher, in der Prozessaktivität und beim Dateizugriff.
2. **Decide** – das KI-gestützte Verhaltensmodell bewertet sofort die Absicht des Datenzugriffs des Programms.
3. **Respond** – ist die Absicht bösartig, wird das Programm abgefangen und angehalten.

Warum lokale Verarbeitung unverzichtbar ist

Das Senden von Telemetriedaten an einen Cloud-Server, das Warten auf die Analyse und der Empfang einer Antwort kostet Millisekunden, die der Angreifer nur allzu gerne nutzen wird. Zur Einordnung der Größenordnung: Diese Entscheidung erfolgt schneller, als ein Nervenimpuls vom Auge zum Gehirn gelangt. Jede Architektur mit einem Netzwerk-Roundtrip im kritischen Pfad hat dieses Rennen bereits verloren.

Rohe Telemetriedaten werden im Nachhinein weiterhin zu Servern kopiert, um Beweise zu sichern und Daten anzureichern – doch die Schutzentscheidung wartet niemals darauf.

Revision #1
Created 2026-07-24 04:34:46 UTC by Dennis Underwood
Updated 2026-07-24 04:34:46 UTC by Dennis Underwood