

Was bedeutet es, dass Cyber Crucible unabhängig von Windows-Bibliotheken ist?

Kurze Antwort: Cyber Crucible ist nicht auf die Windows-Systembibliotheken angewiesen, die es schützt. Es wurde bewusst von diesen entkoppelt, sodass Cyber Crucible auch dann weiterläuft, weiter durchsetzt und weiter meldet, wenn Angreifer diese Bibliotheken kompromittieren, zum Absturz bringen oder kapern.

Warum dies entwickelt wurde

In der zweiten Hälfte des Jahres 2025 verlagerten sich Angreifer darauf, zentrale Windows-Bibliotheken im Arbeitsspeicher zu infizieren. Da nahezu jeder Sicherheitsanbieter auf dieselben Bibliotheken angewiesen ist, um zu funktionieren, machte dieser eine Schritt einen Großteil des Marktes blind.

Cyber Crucible investierte rund neun Monate in die Entwicklung neuartiger Sensoren und weitere fünf Monate technische Arbeit, um Abhängigkeiten von Windows-Bibliotheken vollständig zu beseitigen – einschließlich der Eliminierung volatiler MiniFilter-Abhängigkeiten.

Wie sieht das architektonisch aus

Die Architektur betreibt sieben vollständig unabhängige Subsysteme innerhalb des Kernels, einschließlich eigener isolierter Verschlüsselung, Netzwerkkommunikation, Metadatenanalyse und Ereignisverfolgung. Eine weitere Phase dieser Arbeit ersetzt die standardmäßige Windows-Netzwerkbibliothek (`ws32_2.dll`) durch einen eigens entwickelten Netzwerk-Stack auf Kernel-Ebene.

In der Praxis bewährt

Bei zwei Kunden versuchten Angreifer, die von der ausschließlich im Kernel arbeitenden Entscheidungs-Engine blockiert wurden, anschließend zu verhindern, dass der Kunde benachrichtigt wird, indem sie die Netzwerkschicht des Betriebssystems angriffen. Da die Netzwerkkommunikation von Cyber Crucible unabhängig vom Betriebssystem ist, blieb der Schutz bestehen, und die Informationen erreichten den Kunden dennoch.

Revision #1

Created 2026-07-24 04:35:29 UTC by Dennis Underwood

Updated 2026-07-24 04:35:29 UTC by Dennis Underwood