Wie unterscheidet sich Cyber Crucible von EDR, XDR und MDR?

Kurze Antwort: EDR, XDR und MDR sind Erkennungs- und Reaktionswerkzeuge: Sie beobachten einen Angriff, erzeugen eine Warnung und verlassen sich auf einen Menschen oder einen Cloud-Dienst, um zu entscheiden, was zu tun ist. Cyber Crucible ist ein Präventionswerkzeug: Es entscheidet autonom auf dem Endpunkt und stoppt den bösartigen Prozess in unter 200 Millisekunden, bevor Schaden entsteht.

Die praktischen Unterschiede

	EDR / XDR / MDR	Cyber Crucible
Reaktionszeit	Minuten bis Stunden	Unter 200 Millisekunden
Erkennungsmethode	Signaturen und historische Daten	Verhaltensbasierte Absicht, keine Signaturen
Zero-Day-Abdeckung	Teilweise	Für unbekannte Bedrohungen konzipiert
Abhängigkeit von Menschen	Hoch — Analysten und SOCs	Keine — vollständig autonom
Wo Entscheidungen getroffen werden	Cloud-Analysen	Lokal, im Kernel

Warum diese Lücke wichtig ist

Erkennungstools wurden für eine Zeit entwickelt, in der sich Angriffe über Stunden oder Tage erstreckten. Automatisierte Angriffe laufen heute in Sekunden ab. Ein Tool, das eine präzise Warnung erzeugt, nachdem die Daten bereits exfiltriert wurden, hat den Verlust dokumentiert, nicht verhindert.

Das bedeutet nicht, dass Erkennung keinen Wert hat — Forensik und Untersuchungen sind wichtig. Es bedeutet vielmehr, dass Erkennung allein einen Angriff in Maschinengeschwindigkeit nicht stoppen kann.

Revision #1
Created 2026-07-24 04:31:53 UTC by Dennis Underwood
Updated 2026-07-24 04:31:54 UTC by Dennis Underwood