Wie schützt Cyber Crucible Finanzdienstleistungsunternehmen?

Kurze Antwort: Es stoppt Infostealer und den Diebstahl von Sitzungs-Tokens auf Kernel-Ebene, bevor die Exfiltration beginnt, und analysiert alles lokal, sodass Schlüssel und Tokens niemals in eine Cloud eines Drittanbieters hochgeladen werden müssen.

Die Bedrohung, mit der Finanzunternehmen tatsächlich konfrontiert sind

Hyperautomatisierte „Smash-and-Grab“-Angriffe zielen auf Sitzungs-Tokens und API-Schlüssel ab. Sie bewegen sich innerhalb von Sekunden von der Infiltration bis zur Selbstlöschung — schneller, als eine Cloud-Warnung das Gebäude verlassen kann. Ein gestohlenes Sitzungs-Token umgeht oft Passwörter und MFA vollständig und verschafft einem Angreifer jederzeit einen scheinbar legitimen Weg zurück in das System.

Der dokumentierte Fall

Ein großes Finanzdienstleistungsunternehmen betrieb drei branchenführende EDR-Lösungen und einen ausgelagerten Top-50-MSSP. Cyber Crucible wurde eingesetzt, um den blinden Fleck zu finden. Innerhalb von 60 Tagen hatte es autonom fast 10.000 bösartige Prozesse abgefangen — 98 % davon auf der hochprivilegierten Microsoft-SQL-Server-Farm des Unternehmens — ohne jegliche Warnung durch die bestehenden Altsysteme.

Die Ursache ließ sich auf eine wahrscheinlich kompromittierte Anmeldeinformation für die Fernüberwachung zurückführen. Monate später berichtete die Branche über eine weltweite Ransomware-Welle, die SQL-Server durch Backdoors weltweit kompromittierte. Der Finanzsektor erlitt schwerwiegende Sicherheitsverletzungen. Dieser Kunde wurde nie zum Opfer.

Revision #1
Created 2026-07-24 04:38:56 UTC by Dennis Underwood
Updated 2026-07-24 04:38:56 UTC by Dennis Underwood