Warum reagiert Cyber Crucible mit dem Anhalten eines Prozesses anstatt das System herunterzufahren?

Kurze Antwort: Das Anhalten nur des bösartigen Prozesses — manchmal auch als Selective Freeze bezeichnet — neutralisiert den Angriff, während alles andere weiterläuft. Es gibt keine vollständige Systemsperre, keinen Neustart und keine Unterbrechung der legitimen Arbeit.

Das Problem mit Lockdown-artigen Reaktionen

Wenn viele Erkennungstools eine Anomalie identifizieren, sind die Eindämmungsoptionen grobschlächtig: die Maschine isolieren oder vom Netz nehmen. In einem Krankenhaus, einer Fabrik oder einem Handelsbetrieb kann diese Reaktion nahezu so schädlich sein wie der Angriff selbst.

Was selektives Anhalten erreicht

Der Angriff wird im Arbeitsspeicher angehalten. Legitime Transaktionen werden niemals gestoppt. In der Implementierung im Finanzdienstleistungsbereich, bei der fast 10.000 bösartige Prozesse abgefangen wurden, liefen die legitimen SQL-Transaktionen durchgehend ununterbrochen weiter — der Betrieb wurde nie eingestellt.

Genau das macht Prävention mit Geschäftskontinuität vereinbar, anstatt einen Kompromiss dazu darzustellen.

Revision #1
Created 2026-07-24 04:35:48 UTC by Dennis Underwood
Updated 2026-07-24 04:35:48 UTC by Dennis Underwood