Verlangsamt Cyber Crucible meine Systeme?

Kurze Antwort: Nein. Die typische CPU-Auslastung liegt bei rund 1 % oder darunter, und die Architektur vermeidet bewusst die Technik, die bei den meisten Endpoint-Agenten für Verlangsamungen sorgt – das Einfügen von Hooks in Windows-Systembibliotheken.

Warum andere Agenten zu Verzögerungen führen

Herkömmliche Sicherheitstools fügen „Hooks“ in hochgradig optimierte Systembibliotheken ein, um schädliches Verhalten zu überwachen. Diese Bibliotheken wurden nie dafür entwickelt, zur Laufzeit verändert zu werden. Wenn ein Sicherheitstool und ein Angreifer gleichzeitig daran manipulieren, führt dies zu einer erheblichen Beeinträchtigung der Systemleistung.

Das darauffolgende Muster ist vorhersehbar: Der Anwender macht das Sicherheitstool für die Verlangsamung verantwortlich und entfernt es. Der Hersteller kann das Problem im Labor nicht reproduzieren, ohne zu wissen, dass ein Angreifer mit Root-Rechten das System manipuliert. Angreifer haben gelernt, dies gezielt auszunutzen – indem sie die Leistung so lange beeinträchtigen, bis Opfer ihre eigenen Schutzmaßnahmen deaktivieren.

Ein anderer Ansatz

Cyber Crucible arbeitet über unabhängige Subsysteme innerhalb des Kernels, anstatt anfällige Windows-Komponenten zu hooken. Dadurch konkurriert es weder mit dem Betriebssystem noch mit einem Angreifer um dieselben störanfälligen Codepfade.

Revision #1
Created 2026-07-24 04:32:51 UTC by Dennis Underwood
Updated 2026-07-24 04:32:51 UTC by Dennis Underwood