What evidence is there that Cyber Crucible actually stops attacks?

Short answer: Documented customer deployments, independent testing by a major accounting and advisory firm, and repeated instances of stopping zero-day attacks months before other vendors reported them.

Documented outcomes

- **Financial services:** nearly 10,000 malicious processes autonomously intercepted in 60 days, 98% on a highly privileged Microsoft SQL server farm — with no alerts from three deployed EDRs, an MDR, or an outsourced Top-50 SOC.
- **Independent testing:** one of North America's largest accounting and advisory firms put Cyber Crucible through its own evaluation against ransomware, data theft, and identity fraud scenarios.
- **Ahead of the industry:** Cyber Crucible has stopped multiple zero-day attacks on customer networks up to 90 days before any other vendor reported or responded to them.
- **Browser-based attacks:** from Q4 2023 onward, automated responses against Chrome, Edge, and Chromium activity rose from zero into the thousands, with related CVEs later published by Google and Microsoft.
- **Ransom payments:** roughly 90% of ransomware victims paid in 2023. Cyber Crucible customers paid $0.

Resilience under direct attack

In maritime deployment, adversaries escalated to hijacking Windows credentials and locking systems at the BIOS level when conventional attempts failed. With two other customers, attackers who couldn't defeat the kernel decision engine tried instead to block customer notification by attacking the OS networking stack — and failed, because Cyber Crucible's network communications are independent of the operating system.

Revision #3
Created 2026-07-20 19:24:16 UTC by Dennis Underwood
Updated 2026-07-21 19:32:30 UTC by Dennis Underwood