How does Cyber Crucible protect financial services firms?

Short answer: It stops infostealers and session-token theft at the kernel level, before exfiltration begins, and it analyzes everything locally so keys and tokens never have to be uploaded to a third-party cloud.

The threat financial firms actually face

Hyper-automated "smash and grab" attacks target session tokens and API keys. These move from infiltration to self-deletion in seconds — faster than a cloud alert can leave the building. A stolen session token often bypasses passwords and MFA entirely, giving an attacker a legitimate-looking way back in at any time.

The documented case

A major financial services firm ran three industry-leading EDRs and an outsourced Top-50 MSSP. Cyber Crucible was deployed to find the blind spot. Within 60 days it had autonomously intercepted nearly 10,000 malicious processes — 98% of them on the firm's highly privileged Microsoft SQL server farm — with no alerts from the legacy stack.

The root cause traced to a likely compromised remote monitoring credential. Months later, the industry reported a global wave of ransomware backdooring SQL servers worldwide. The financial sector suffered severe breaches. This client was never a victim.

Revision #3
Created 2026-07-20 19:24:11 UTC by Dennis Underwood
Updated 2026-07-21 19:32:26 UTC by Dennis Underwood