

Como a Cyber Crucible protege empresas de serviços financeiros?

Resposta rápida: Ela interrompe infostealers e o roubo de tokens de sessão ao nível do kernel, antes que a exfiltração comece, e analisa tudo localmente, de modo que chaves e tokens nunca precisam ser enviados para uma nuvem de terceiros.

A ameaça que as empresas financeiras realmente enfrentam

Ataques hiperautomatizados do tipo "smash and grab" visam tokens de sessão e chaves de API. Eles avançam da infiltração à autoeliminação em segundos — mais rápido do que um alerta na nuvem consegue sair do prédio. Um token de sessão roubado frequentemente contorna senhas e MFA por completo, dando a um atacante uma forma aparentemente legítima de voltar a entrar a qualquer momento.

O caso documentado

Uma grande empresa de serviços financeiros operava três EDRs líderes do setor e um MSSP terceirizado entre os 50 principais. A Cyber Crucible foi implantada para encontrar o ponto cego. Em 60 dias, ela havia interceptado autonomamente quase 10.000 processos maliciosos — 98% deles no farm de servidores Microsoft SQL altamente privilegiados da empresa — sem nenhum alerta da pilha de segurança legada.

A causa raiz foi rastreada a uma credencial de monitoramento remoto provavelmente comprometida. Meses depois, o setor reportou uma onda global de ransomware instalando backdoors em servidores SQL em todo o mundo. O setor financeiro sofreu graves violações. Este cliente nunca foi uma vítima.

Revision #1

Created 2026-07-24 05:50:46 UTC by Dennis Underwood

Updated 2026-07-24 05:50:46 UTC by Dennis Underwood