O que é a Rogue Process Prevention (RPP)?

Resposta breve: A Rogue Process Prevention é a abordagem patenteada da Cyber Crucible que consiste em intervir contra um processo malicioso, em vez de apenas observá-lo. Seja um ransomware a iniciar a encriptação, seja um infostealer a tentar obter um token de sessão, o processo é interrompido antes que os dados saiam do dispositivo.

Observar versus intervir

A maior parte do mercado de endpoint está construída para observar. A RPP está construída para intervir. A distinção é a diferença entre uma câmara de segurança que regista um assalto para análise posterior e um guarda que impede o ladrão de chegar ao cofre.

Contra o que protege

A RPP combate os três tipos de ameaças fundamentais em conjunto, porque os ataques modernos são normalmente multifacetados:

- **Roubo de identidade** — acesso a chaves, tokens e palavras-passe, muitas vezes sem qualquer interação por parte do funcionário.
- **Roubo de informação** — exfiltração massiva de dados à velocidade da máquina.
- **Ransomware** — análise comportamental aliada a tecnologia de engano de hackers que impede a encriptação de sequer um único ficheiro.

Uma defesa focada exclusivamente no ransomware deixaria escapar as duas primeiras fases, que são normalmente onde começa o verdadeiro dano.

Revision #1
Created 2026-07-24 05:47:10 UTC by Dennis Underwood
Updated 2026-07-24 05:47:10 UTC by Dennis Underwood