¿Qué es Rogue Process Prevention (RPP)?

Respuesta breve: Rogue Process Prevention es el enfoque patentado de Cyber Crucible que consiste en interceder contra un proceso malicioso en lugar de limitarse a observarlo. Ya sea que se trate de un ransomware que comienza a cifrar datos o de un infostealer que busca obtener un token de sesión, el proceso se detiene antes de que los datos salgan del dispositivo.

Observar frente a intervenir

La mayor parte del mercado de endpoints está diseñada para observar. RPP está diseñado para intervenir. La distinción es la diferencia entre una cámara de seguridad que graba un robo para su revisión posterior y un guardia que detiene al ladrón antes de que llegue a la bóveda.

Contra qué protege

RPP aborda las tres amenazas principales de manera conjunta, ya que los ataques modernos suelen tener múltiples vectores:

- **Robo de identidad** — acceso a claves, tokens y contraseñas, a menudo sin ninguna interacción por parte del empleado.
- **Robo de información** — exfiltración masiva de datos a velocidad de máquina.
- **Ransomware** — análisis de comportamiento junto con tecnología de engaño para hackers que impide el cifrado incluso de un solo archivo.

Una defensa centrada exclusivamente en el ransomware pasaría por alto las dos primeras etapas, que es donde suele comenzar el daño real.

Revision #1
Created 2026-07-24 01:48:51 UTC by Dennis Underwood
Updated 2026-07-24 01:48:51 UTC by Dennis Underwood