

Por que a Cyber Crucible responde suspendendo um processo em vez de desligar o sistema?

Resposta breve: Suspende apenas o processo malicioso — por vezes chamado de Congelamento Seletivo — neutraliza o ataque enquanto tudo o resto continua a funcionar. Não há bloqueio total do sistema, nem reinicialização, nem interrupção do trabalho legítimo.

O problema com respostas do tipo bloqueio total

Quando muitas ferramentas de deteção identificam uma anomalia, as opções de contenção são drásticas: isolar a máquina ou colocá-la offline. Num hospital, numa fábrica ou numa operação de negociação financeira, essa resposta pode ser quase tão prejudicial quanto o próprio ataque.

O que a suspensão seletiva alcança

O ataque é suspenso na memória. As transações legítimas nunca param. Na implementação de serviços financeiros em que quase 10.000 processos maliciosos foram interceptados, as transações SQL legítimas continuaram sem interrupção durante todo o processo — as operações nunca foram interrompidas.

É isso que torna a prevenção compatível com a continuidade dos negócios, em vez de uma escolha de compromisso em relação a ela.

Revision #1

Created 2026-07-24 05:47:56 UTC by Dennis Underwood

Updated 2026-07-24 05:47:56 UTC by Dennis Underwood