Fomos vítimas de uma violação recentemente. O Cyber Crucible pode ser implementado num ambiente que já possa estar comprometido?

Resposta rápida: Sim. O Cyber Crucible avalia o que os programas estão a fazer neste momento, em vez de procurar ficheiros conhecidos como maliciosos, pelo que começa a impedir comportamentos maliciosos assim que é implementado — incluindo os de um atacante que já tenha conseguido entrar no ambiente.

Porque é que um comprometimento prévio não o "cega"

Como a prevenção se baseia na intenção comportamental ao nível do kernel, um atacante que já esteja presente ainda tem de *agir* — aceder a dados de identidade, injetar-se em processos, iniciar a encriptação ou movimentar dados. São precisamente essas ações que desencadeiam a interceção.

Foi assim que a implementação no setor de serviços financeiros revelou uma intrusão ativa e em curso que a stack de segurança existente nunca tinha sinalizado. O Cyber Crucible não foi implementado para investigar uma violação já conhecida; foi implementado para procurar um ponto cego, e encontrou quase 10.000 processos maliciosos já em curso.

O que esperar

A implementação num ambiente comprometido produz frequentemente uma atividade de interceção imediata e de elevado volume. É a ferramenta a funcionar como previsto, e é muitas vezes a primeira prova concreta que uma organização tem de que algo já estava a acontecer.

Revision #1
Created 2026-07-24 05:51:20 UTC by Dennis Underwood
Updated 2026-07-24 05:51:20 UTC by Dennis Underwood