

O que significa o facto de a Cyber Crucible ser independente das bibliotecas do Windows?

Resposta breve: A Cyber Crucible não depende das bibliotecas do sistema Windows que está a proteger. Foi deliberadamente dissociada delas, de modo que, quando os atacantes comprometem, bloqueiam ou sequestram essas bibliotecas, a Cyber Crucible continua a funcionar, continua a aplicar as políticas e continua a reportar.

Porque é que isto foi construído

Na segunda metade de 2025, os atacantes passaram a infetar bibliotecas centrais do Windows em memória. Como praticamente todos os fornecedores de segurança dependem dessas mesmas bibliotecas para funcionar, esta única mudança tornou cega uma grande parte do mercado.

A Cyber Crucible passou aproximadamente nove meses a inventar novos sensores e mais cinco meses de esforço de engenharia para eliminar por completo as dependências das bibliotecas do Windows — incluindo a eliminação das dependências voláteis do MiniFilter.

Como isto se apresenta a nível arquitetónico

A arquitetura executa sete subsistemas totalmente independentes dentro do kernel, incluindo a sua própria encriptação isolada, rede, análise de metadados e monitorização de eventos. Uma fase adicional deste trabalho substituiu a biblioteca de rede padrão do Windows (`ws32_2.dll`) por uma pilha de rede personalizada ao nível do kernel.

Comprovado em ambiente real

Com dois clientes, os atacantes bloqueados pelo motor de decisão exclusivo do kernel tentaram então impedir que o cliente fosse notificado, atacando a camada de rede do sistema operativo. Como as comunicações de rede da Cyber Crucible são independentes do sistema operativo, a proteção manteve-se e a informação chegou, ainda assim, ao cliente.

Revision #1

Created 2026-07-24 05:47:40 UTC by Dennis Underwood

Updated 2026-07-24 05:47:40 UTC by Dennis Underwood