

Por que a Cyber Crucible opera no nível do kernel?

Resposta curta: O kernel é a camada mais profunda e privilegiada do sistema operacional. Operar nesse nível permite que a Cyber Crucible veja e controle toda a atividade do sistema, identifique a intenção de um processo malicioso e o interrompa em milissegundos — além de tornar a ferramenta muito mais difícil de ser adulterada ou desativada por um invasor.

O que o acesso ao kernel proporciona

- **Visibilidade completa** sobre o comportamento da memória, o comportamento dos processos e o acesso a arquivos, incluindo atividades que nunca chegam a tocar o disco.
- **A capacidade de agir**, não apenas observar — permissões podem ser revogadas e processos suspensos no momento em que a intenção maliciosa é detectada.
- **Resiliência**, pois os invasores inevitavelmente tentarão desativar a própria ferramenta de segurança.

Sobre as críticas ao desenvolvimento em nível de kernel

Alguns players estabelecidos e analistas desencorajam o desenvolvimento em nível de kernel. A engenharia de kernel é genuinamente difícil e cara, o que explica exatamente por que grande parte do mercado a evitou — e por que os endpoints ficaram dependentes de telemetria em espaço de usuário, que ataques em nível de root conseguem neutralizar.

A qualidade e a resistência à adulteração da Cyber Crucible são validadas pelo Windows Hardware Compatibility Program (WHCP) da Microsoft.

Revision #1

Created 2026-07-24 05:47:30 UTC by Dennis Underwood

Updated 2026-07-24 05:47:30 UTC by Dennis Underwood