¿Por qué Cyber Crucible opera a nivel de kernel?

Respuesta breve: El kernel es la capa más profunda y privilegiada del sistema operativo. Operar allí permite a Cyber Crucible ver y controlar toda la actividad del sistema, identificar la intención de un proceso malicioso y detenerlo en milisegundos, además de hacer que la herramienta sea mucho más difícil de manipular o deshabilitar para un atacante.

Qué proporciona el acceso a nivel de kernel

- **Visibilidad completa** del comportamiento de la memoria, el comportamiento de los procesos y el acceso a archivos, incluida la actividad que nunca toca el disco.
- **La capacidad de actuar**, no solo de observar: los permisos pueden revocarse y los procesos pueden suspenderse en el momento en que se detecta la intención maliciosa.
- **Resiliencia**, porque los atacantes inevitablemente intentarán deshabilitar la propia herramienta de seguridad.

Sobre las críticas al desarrollo a nivel de kernel

Algunos actores establecidos y analistas desaconsejan el desarrollo a nivel de kernel. La ingeniería de kernel es genuinamente difícil y costosa, precisamente por eso gran parte del mercado la evitó, y por eso los endpoints quedaron dependientes de la telemetría en el espacio de usuario, que los ataques a nivel raíz pueden neutralizar.

La calidad y la resistencia a la manipulación de Cyber Crucible están validadas a través del Windows Hardware Compatibility Program (WHCP) de Microsoft.

Revision #1
Created 2026-07-24 01:49:11 UTC by Dennis Underwood
Updated 2026-07-24 01:49:11 UTC by Dennis Underwood