

¿Qué validación de seguridad independiente tiene Cyber Crucible?

Respuesta breve: Los controladores del kernel de Windows de Cyber Crucible se someten a pruebas objetivas y se firman criptográficamente bajo el Windows Hardware Compatibility Program (WHCP) de Microsoft. Se trata de una certificación externa e independiente de la calidad y la resistencia a la manipulación del componente más privilegiado del producto: el código en el que la corrección es más crítica.

Por qué el WHCP es relevante

La mayor parte del mercado de endpoints evitó el desarrollo a nivel de kernel porque es genuinamente difícil y costoso. Cyber Crucible opera deliberadamente en el kernel y somete sus controladores al programa de Microsoft para que una parte externa —no solo Cyber Crucible— valide que el código más sensible es correcto y resistente a la manipulación.

- La validación está **acotada específicamente al controlador**, y no se presenta como una certificación del producto en su conjunto.
- Se trata de una prueba objetiva y repetible, en lugar de una auditoría administrativa subjetiva.

Cómo encaja en el panorama general

Para un revisor acostumbrado a buscar un informe SOC 2, el WHCP es un dato concreto e independiente que un SOC 2 no proporciona: la validación directa del componente del kernel. Complementa —en lugar de reemplazar— la evidencia de controles incluida en el paquete para proveedores preparado por Cyber Crucible.

Revision #1

Created 2026-07-24 02:02:09 UTC by Dennis Underwood

Updated 2026-07-24 02:02:09 UTC by Dennis Underwood