¿Cómo protege y controla Cyber Crucible los endpoints?

Respuesta breve: De dos maneras. El producto en sí es una prevención autónoma de endpoints que opera en la capa del kernel, y Cyber Crucible controla sus propios endpoints corporativos y de ingeniería bajo un programa formal. Ambos se apoyan en el desarrollo interno del código con mayores privilegios.

Protección de endpoints del producto

El producto ofrece prevención autónoma contra ransomware, ataques en memoria (fileless) e inyección de procesos, aplicada en la capa del kernel. Está deliberadamente desacoplado de las bibliotecas del sistema operativo, de modo que cuando los atacantes comprometen o secuestran esas bibliotecas en memoria, el producto continúa ejecutándose, aplicando controles e informando. Debido a que la detección y respuesta se ejecutan localmente, la protección continúa durante una interrupción del backend de gestión o en una implementación deliberadamente aislada (air-gapped).

Integridad de la cadena de suministro y validación independiente

Los algoritmos de detección, las heurísticas del kernel, los sensores y los controladores se diseñan y mantienen internamente; no se integran en el software bibliotecas de terceros no verificadas ni ganchos de telemetría ocultos. Debido a que el componente con mayores privilegios es propietario, se elimina por completo una categoría de exposición de la cadena de suministro de terceros, en lugar de simplemente gestionarla. Todos los controladores de kernel de Windows se validan y firman bajo el Programa de Compatibilidad de Hardware de Windows (WHCP) de Microsoft.

Controles de endpoints corporativos

Los endpoints gestionados siguen líneas de base de configuración segura aprobadas, ejecutan protección y análisis de endpoints, y aplican los mismos controles a los medios extraíbles y portátiles que a los medios fijos, restringiendo el uso no autorizado de medios. La instalación de software se rige por políticas, los datos en reposo en los endpoints se cifran, y los endpoints se

mantienen actualizados conforme al programa de gestión de parches.

Alineación con marcos de referencia y el límite honesto

Los controles de endpoints se alinean con los Controles Críticos de Seguridad del CIS (v8) y el NIST SP 800-53 (SI-3, CM-2, MP-7). No se reclama ninguna certificación. Se proporcionan estándares de configuración detallados y evidencia a los revisores bajo un acuerdo de confidencialidad (NDA).

Revision #1
Created 2026-07-24 23:16:53 UTC by Dennis Underwood
Updated 2026-07-24 23:16:54 UTC by Dennis Underwood