¿Qué significa que Cyber Crucible sea independiente de las bibliotecas de Windows?

Respuesta breve: Cyber Crucible no depende de las bibliotecas del sistema Windows que está protegiendo. Fue desacoplado deliberadamente de ellas, de modo que cuando los atacantes comprometen, bloquean o secuestran esas bibliotecas, Cyber Crucible sigue funcionando, sigue aplicando controles y sigue informando.

Por qué se construyó así

En la segunda mitad de 2025, los atacantes cambiaron su enfoque hacia la infección de bibliotecas centrales de Windows en memoria. Dado que casi todos los proveedores de seguridad dependen de esas mismas bibliotecas para funcionar, ese único movimiento dejó ciega a una gran parte del mercado.

Cyber Crucible dedicó aproximadamente nueve meses a inventar sensores novedosos y un esfuerzo adicional de ingeniería de cinco meses para eliminar por completo las dependencias de las bibliotecas de Windows, incluida la eliminación de las dependencias volátiles de MiniFilter.

Cómo se ve esto a nivel arquitectónico

La arquitectura ejecuta siete subsistemas totalmente independientes dentro del kernel, incluidos su propio cifrado aislado, redes, análisis de metadatos y seguimiento de eventos. Una fase adicional de este trabajo reemplaza la biblioteca estándar de redes de Windows (`ws32_2.dll`) por una pila de red personalizada a nivel de kernel.

Comprobado en el campo

Con dos clientes, los atacantes bloqueados por el motor de decisión exclusivo del kernel intentaron luego impedir que se notificara al cliente atacando la capa de red del sistema operativo. Dado que las comunicaciones de red de Cyber Crucible son independientes del sistema operativo, la protección se mantuvo y la inteligencia igualmente llegó al cliente.

Revision #1
Created 2026-07-24 01:49:20 UTC by Dennis Underwood

Updated 2026-07-24 01:49:20 UTC by Dennis Underwood