

¿Cómo toma Cyber Crucible una decisión en menos de 200 milisegundos?

Respuesta breve: Ejecuta un ciclo de tres pasos —Detect-Decide-Respond— completamente en el endpoint, a nivel de kernel, utilizando un motor patentado de análisis de edge computing. Como nada tiene que viajar hacia un servicio en la nube y regresar, y no hay ningún humano en el ciclo, todo el proceso se completa en menos de 200 milisegundos.

El ciclo

1. **Detect (Detectar)** — sensores novedosos a nivel de kernel identifican patrones de comportamiento malicioso en la memoria, la actividad de procesos y el acceso a archivos.
2. **Decide (Decidir)** — el modelo de comportamiento mejorado con IA evalúa instantáneamente la intención del acceso a datos del programa.
3. **Respond (Responder)** — si la intención es maliciosa, el programa es interceptado y suspendido.

Por qué el procesamiento local no es negociable

Enviar telemetría a un servidor en la nube, esperar el análisis y recibir una respuesta añade milisegundos que el atacante aprovechará con gusto. Para dimensionar la escala involucrada: esta decisión ocurre más rápido de lo que un impulso nervioso viaja desde el ojo hasta el cerebro. Cualquier arquitectura con un viaje de ida y vuelta por la red en la ruta crítica ya ha perdido esa carrera.

La telemetría bruta se sigue copiando posteriormente a los servidores para fines de evidencia y enriquecimiento, pero la decisión de protección nunca espera por ello.

Revision #1

Created 2026-07-24 01:48:44 UTC by Dennis Underwood

Updated 2026-07-24 01:48:44 UTC by Dennis Underwood