

¿Cyber Crucible integra bibliotecas de terceros o código extranjero?

Respuesta breve: No. Los sensores de kernel, los controladores y los modelos de comportamiento de Genetic AI se diseñan internamente. No se integra en el software ningún SDK patrocinado por estados extranjeros, biblioteca de terceros no verificada ni mecanismo de telemetría oculto. Los controladores de kernel de Windows se presentan para su certificación en el marco del Windows Hardware Compatibility Program (WHCP) de Microsoft.

La ventaja de la ingeniería propia

Desarrollar sensores de kernel y modelos de comportamiento de manera interna es costoso y lento. La mayoría de los proveedores ensamblan componentes en su lugar. Ese ensamblaje es precisamente el punto por el que el riesgo de la cadena de suministro se introduce en un producto de seguridad: la herramienta con los privilegios de sistema más profundos es también aquella en la que una dependencia no verificada puede causar el mayor daño.

Los componentes de Cyber Crucible son propietarios y se mantienen de forma interna, lo que elimina esa categoría de exposición en lugar de simplemente gestionarla.

Validación externa

Todos los controladores de kernel de Windows se someten a pruebas internas de control de calidad y se presentan para su certificación en el marco del Windows Hardware Compatibility Program (WHCP) de Microsoft, una validación independiente de la calidad y la resistencia a manipulaciones del código que se ejecuta a nivel de kernel.

Sin telemetría oculta

No existen mecanismos de telemetría ocultos. Lo que el software recopila está documentado, y las categorías que nunca recopila se enumeran de forma explícita.