¿Qué datos recopila Cyber Crucible — y qué datos nunca recopila?

Respuesta breve: Cyber Crucible opera bajo una directiva de Cero Recopilación de Contenido (Zero-Content Harvesting). Procesa telemetría operativa del sistema — rutas de ejecución de procesos, cadenas de procesos padre-hijo, indicadores de ejecución de hardware y estados de integridad de memoria — analizada localmente en el endpoint. No recopila, transmite, almacena ni procesa claves de cifrado, credenciales, tokens de sesión ni sus archivos.

Categorías estrictamente excluidas

El software de Cyber Crucible no recopila, transmite, almacena ni procesa:

- **Variables criptográficas** — claves privadas, claves de descifrado y claves de cifrado de aplicaciones.
- **Credenciales de usuario** — contraseñas de usuario, secretos de Active Directory y claves privadas de API.
- **Identificadores de sesión** — tokens OAuth, tokens de acceso, tokens de actualización y cookies de sesión.
- **Datos de contenido del cliente** — archivos propietarios, documentos, contenidos de bases de datos, cuerpos de correos electrónicos y comunicaciones de usuarios.

Por qué la protección completa no requiere recopilar contenido

La capacidad completa del software de prevención de amenazas se logra sin recopilar ni exfiltrar contenido privado del cliente. El motor de comportamiento evalúa *lo que un programa está haciendo* — a qué procesos está accediendo, habiendo hecho qué anteriormente — y nada de eso requiere abrir el archivo o leer el secreto.

Este es el mismo principio detrás de la protección de identidad: el acceso se rastrea y analiza sin que se acceda a la credencial en sí.

Dónde ocurre el análisis

Las rutas de ejecución de procesos, el linaje de procesos, los indicadores de ejecución de hardware y los estados de integridad de memoria se analizan **localmente en el endpoint**. Cuando la gestión asistida por la nube o centralizada está habilitada, la telemetría administrativa saliente se limita estrictamente a los indicadores operativos necesarios para el monitoreo de la salud del sistema y la generación de informes de seguridad.

Revision #1
Created 2026-07-24 01:54:45 UTC by Dennis Underwood
Updated 2026-07-24 01:54:45 UTC by Dennis Underwood