¿Cuál es la diferencia entre la telemetría del sistema y los datos del cliente?

Respuesta breve: La telemetría del sistema describe cómo se comporta el software: qué proceso inició a cuál, cómo se ve la memoria, si los patrones de ejecución son anómalos. Los datos del cliente son el contenido que su empresa crea y conserva: archivos, correos electrónicos, registros de bases de datos, credenciales. Cyber Crucible analiza lo primero y nunca recopila lo segundo.

Una manera útil de entenderlo

La telemetría son metadatos sobre el *comportamiento de la máquina*. El contenido es la *información misma*.

Saber que el `proceso A` generó el `proceso B`, el cual luego intentó leer un almacén de credenciales del navegador mostrando indicios de modificación en memoria, es suficiente para identificar un ataque. No es necesario leer lo que contenía ese almacén de credenciales, y Cyber Crucible no lo hace.

Qué significa esto en la práctica

- El análisis de comportamiento se realiza sobre el acceso a la identidad **sin procesar la información de identidad en sí**.
- La telemetría que sale del endpoint en implementaciones asistidas por la nube se limita a indicadores operativos para el monitoreo de estado y los informes de seguridad.
- Los metadatos técnicos y de comportamiento se tratan como datos personales únicamente cuando pueden identificar directa o indirectamente a una persona, y en esos casos los identificadores se seudonimizan o enmascaran.

Control del cliente

Las fuentes de telemetría son configurables. Las organizaciones pueden ajustar qué fuentes se recopilan, de modo que no se adquiera información innecesaria. Los campos que no son esenciales para la detección de amenazas se excluyen o descartan.

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