

¿Cuánta información produce Cyber Crucible?

Los datos recopilados por el agente de Cyber Crucible pasan por múltiples capas de filtrado, con el fin de eliminar el ruido derivado de contar con demasiada telemetría en bruto. Los datos sin procesar producidos por los sensores del kernel se reducen [**Filtro n.º 1**] para disminuir tanto el uso de memoria del endpoint como el ancho de banda de red por agente. A continuación, la API REST asociará la telemetría en bruto de procesos/endpoints que reciba con respuestas automatizadas, de modo que el analista pueda optar por ver únicamente los datos relevantes [**Filtro n.º 2**].

Blank diagram-20240523-165941.png

Como se observa en la figura anterior, los endpoints de estaciones de trabajo de un cliente promedio pueden producir varios gigabytes de datos de sensores sin procesar durante un período de 24 horas, mientras que solo unos pocos megabytes de esos datos serán relevantes para una alerta del SOC si se intenta un ataque.

Revision #1

Created 2026-07-24 01:31:11 UTC by Dennis Underwood

Updated 2026-07-24 01:31:11 UTC by Dennis Underwood