

Wie viel Daten werden von Cyber Crucible erzeugt?

Die vom Cyber Crucible Agent erfassten Daten durchlaufen mehrere Filterebenen, um Rauschen durch zu viel Roh telemetrie herauszufiltern. Die von den Kernel-Sensoren erzeugten Rohdaten werden reduziert [**Filter #1**], um sowohl den Speicherverbrauch am Endpunkt als auch die Netzwerkbandbreite pro Agent zu verringern. Anschließend ordnet die REST-API die empfangene Roh-Prozess-/Endpunkt telemetrie automatisierten Reaktionen zu, sodass der Analyst wählen kann, nur relevante Daten anzuzeigen [**Filter #2**].

Blank diagram-20240523-165941.png

Wie in der obigen Abbildung zu sehen ist, können die Workstation-Endpunkte eines durchschnittlichen Kunden über einen Zeitraum von 24 Stunden mehrere Gigabyte an Rohsensordaten erzeugen, während bei einem versuchten Angriff nur wenige Megabyte davon für einen SOC-Alarm relevant sind.

Revision #1

Created 2026-07-24 04:14:19 UTC by Dennis Underwood

Updated 2026-07-24 04:14:19 UTC by Dennis Underwood