

How much data is produced by Cyber Crucible?

The data collected by the Cyber Crucible agent goes through multiple layers of filtering, in order to cut out noise from having too much raw telemetry. The raw data produced by the kernel sensors is trimmed down [**Filter #1**] to reduce both endpoint memory usage, and network bandwidth per-agent. Following that, the REST API will associate raw process/endpoint telemetry it receives to automated responses, such that the analyst can choose to view only relevant data [**Filter #2**].

Blank diagram-20240523-165941.png

As seen in the figure above, an average customer's workstation endpoints may produce multiple gigabytes of raw sensor data over a 24hr span, whereas only a few megabytes of which will be relevant to a SOC alert if an attack is attempted.

Revision #4

Created 2026-05-18 20:28:15 UTC by Dennis Underwood

Updated 2026-07-20 19:21:47 UTC by Dennis Underwood