

Qual é a quantidade de dados produzida pela Cyber Crucible?

Os dados coletados pelo agente da Cyber Crucible passam por múltiplas camadas de filtragem, a fim de eliminar o ruído decorrente do excesso de telemetria bruta. Os dados brutos produzidos pelos sensores do kernel são reduzidos [**Filtro nº 1**] para diminuir tanto o uso de memória do endpoint quanto a largura de banda de rede por agente. Em seguida, a API REST associará a telemetria bruta de processo/endpoint recebida a respostas automatizadas, de modo que o analista possa optar por visualizar apenas os dados relevantes [**Filtro nº 2**].

Blank diagram-20240523-165941.png

Como visto na figura acima, os endpoints de estações de trabalho de um cliente médio podem produzir vários gigabytes de dados brutos de sensores ao longo de um período de 24 horas, enquanto apenas alguns megabytes desses dados serão relevantes para um alerta do SOC caso um ataque seja tentado.

Revision #1

Created 2026-07-24 05:29:21 UTC by Dennis Underwood

Updated 2026-07-24 05:29:21 UTC by Dennis Underwood