We are not using datasets yet in production, but one big issue is our datasets are constantly changing and managing static files and suricata reloads is pain. What about tying a dataset to a Redis keyspace? Much easier to dynamically swap out data there. (edited)

2 replies

Andreas Herz  1 day ago
Can you elaborate a bit more why it's a pain?
Not to say that using something like redis might be worth to look into, right now it's only used for logging output

Chris G  1 day ago
Missed this one. Mostly because we already want that data in place where other applications can easily access and not worry about keeping it in sync. Also if I understand it correctly, we basically want to use dynamic sets exclusively and have them persist across restarts/reloads.

Datasets are persistent (suricata restart will save/load). Data can be added and removed through the unix socket interface. What else is needed? I think using extra tooling the bridge with redis could be made.