

Detecting anomalies in huge Flow datasets

FLOWCUTTER

Mgr. Matej Pavelka PhD.

FLOWCUTTER








flow telemetry?

Photo from Matrix the movie

FLOWCUTTER

5 ways a tool can suck

-  **Schizophrenia**
-  **Cold coffee**
-  **Size matters**
-  **I have no mouth and I must scream**
-  **Inevitable degradation**



schizophrenia

In NOC

Photo from Matrix the movie

FLOWCUTTER



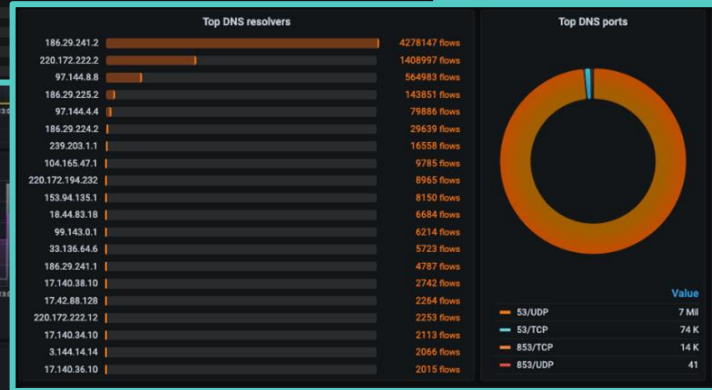
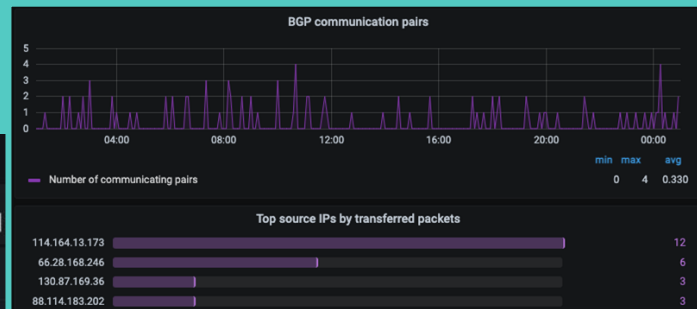
cold coffee

no way

Photo from twitter.com/billydracula/

FLOWCUTTER

Grafana examples





20y, 100y ago

libs used to be like that



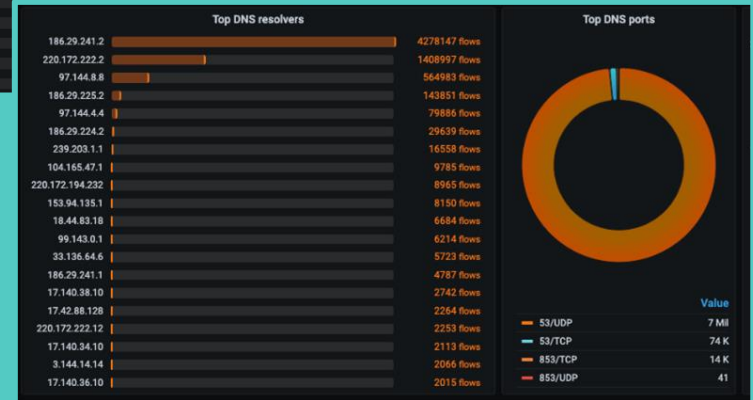
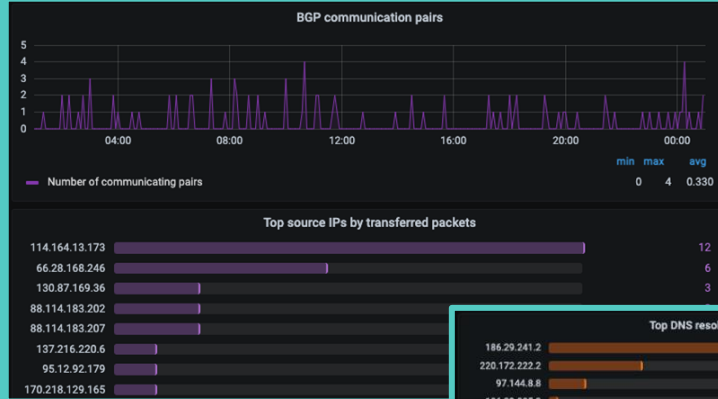
1M+fps

Flow records per second

Photo from www.timessquarenyc.org

FLOWCUTTER

Grafana examples





size

this time it matters



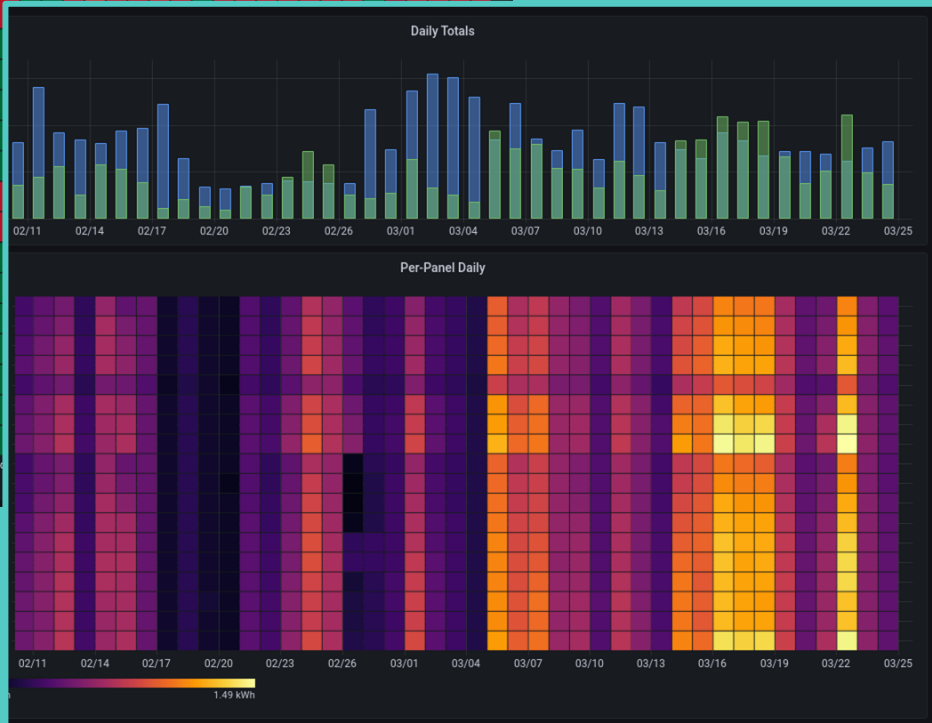
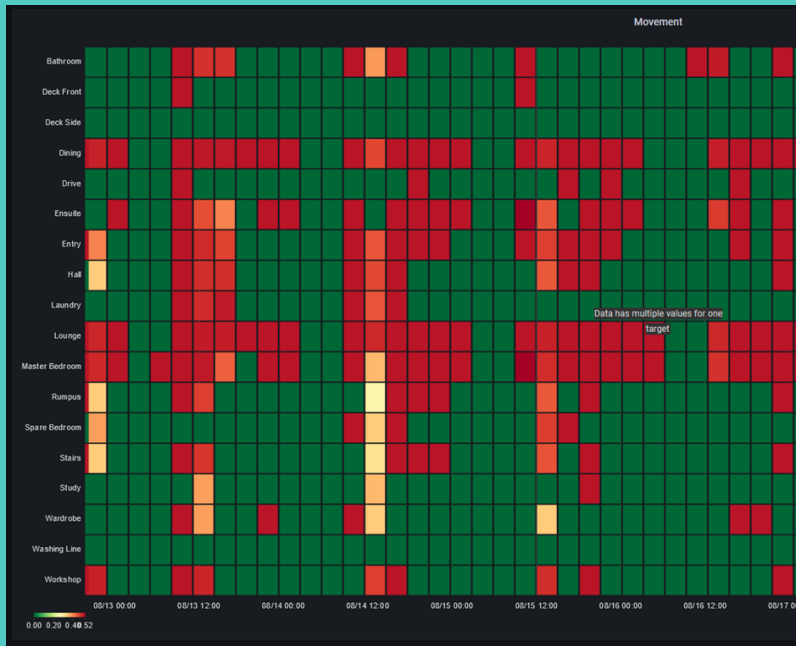
I have no mouth
and I must
scream

Photo from Matrix the movie

FLOWCUTTER


vendor lock

time is the key



Heatmaps

Peering matrix

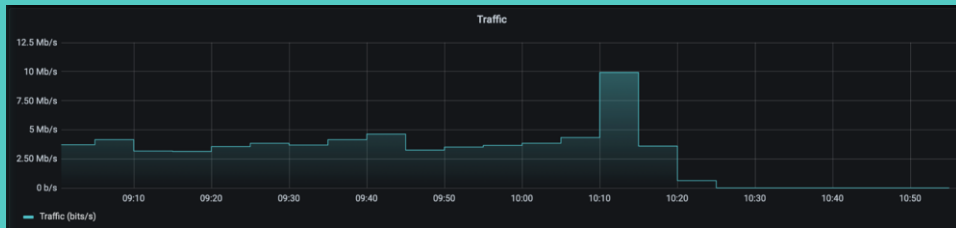


DAY 28

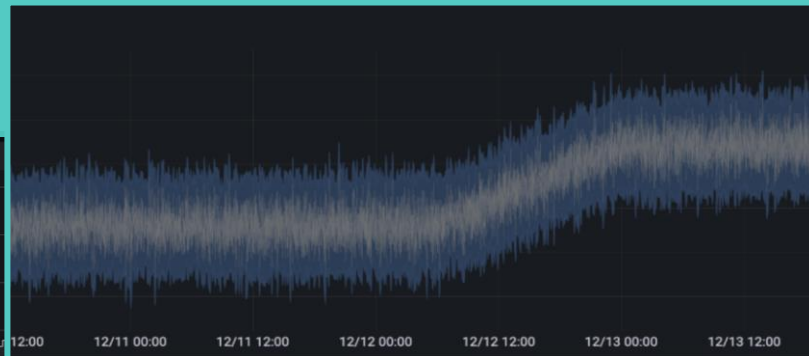
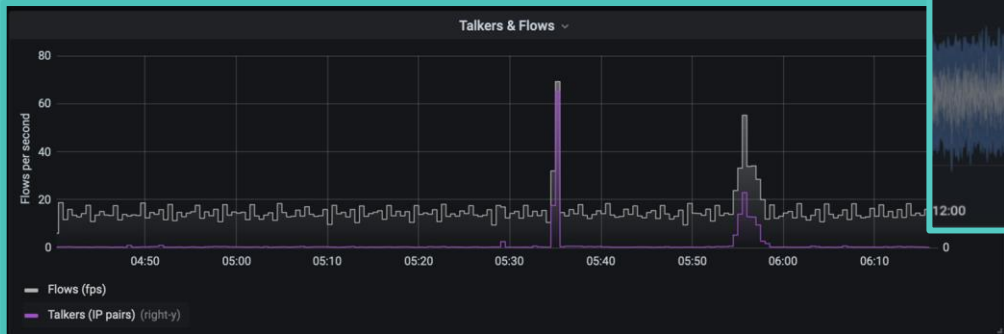
degradation

Is it inevitable?

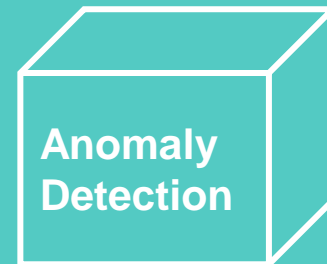
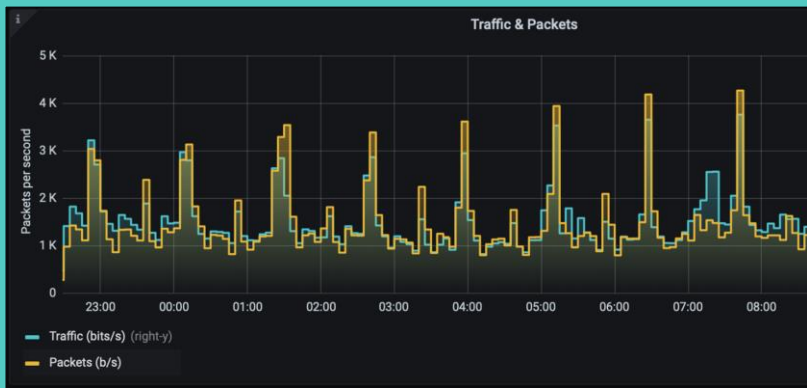
Link down



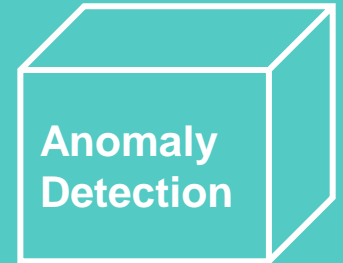
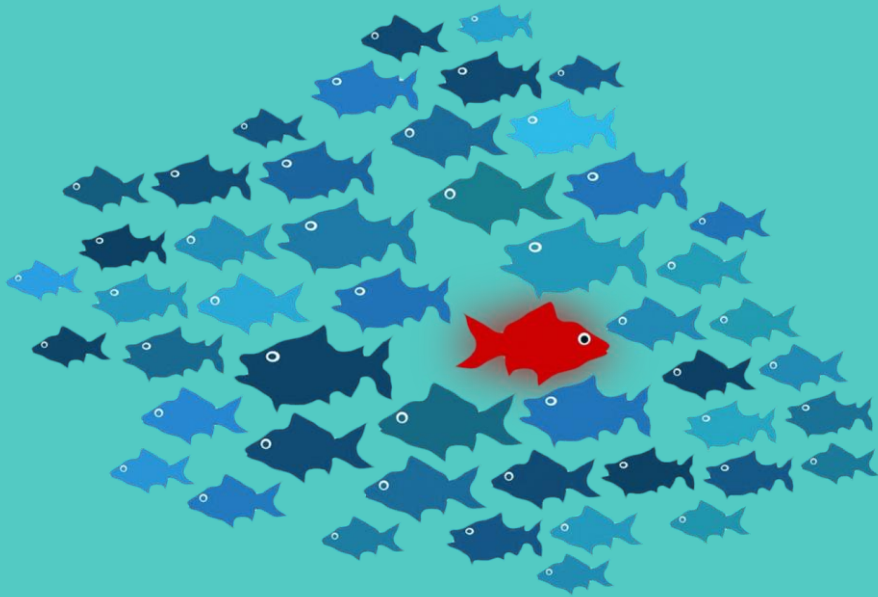
Spikes and shifts













Anomalies not for humans



Anomaly detection



5 ways of solution

-  **Schizophrenia**  unified frontend + customizable to your image
-  **Cold coffee**  fast query on cardinal data
-  **Cloning**  size matters, especially on 1M+fps
-  **I have no mouth and I must scream**  open via API + shared data sources
-  **Inevitable degradation**  anomaly detection lookout

60 mph

do you know?



TOP

exp

thank you

www.flowcutter.com

Photo from www.sciencefocus.com/planet-earth

FLOWCUTTER