

# 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



site all filter +

Panel Title

Search:

sport	dport	proto	stime	etime
546.00	547.00	UDP	2021-06-02 11:24:43.982000	2021-06-02 11:54:40.440000
546.00	547.00	UDP	2021-06-02 10:54:32.508000	2021-06-02 11:24:13.178000
546.00	547.00	UDP	2021-06-02 10:24:24.670000	2021-06-02 10:54:24.572000
546.00	547.00	UDP	2021-06-02 09:53:38.573000	2021-06-02 10:23:25.106000
546.00	547.00	UDP	2021-06-02 09:23:31.083000	2021-06-02 09:52:57.031000

Panel Title

Panel Title

	Value
213.195.223.16/UDP	2 Mil
81.30.226.13/UDP	2 Mil
213.195.223.14/UDP	2 Mil
81.30.226.12/UDP	1 Mil
81.30.226.14/UDP	1 Mil
217.66.163.24/UDP	1 Mil
157.240.30.21/UDP	1 Mil
157.240.30.63/UDP	1 Mil
213.195.224.131/UDP	969 K
81.30.241.154/UDP	881 K
213.195.224.212/UDP	797 K
213.195.223.59/UDP	739 K
94.230.149.146/UDP	732 K
213.195.194.185/UDP	720 K
35.214.151.58/UDP	644 K
213.195.223.10/UDP	620 K
213.195.222.222/UDP	588 K
217.66.163.108/UDP	577 K
213.195.223.30/UDP	556 K
213.195.205.168/UDP	541 K

# cold coffee

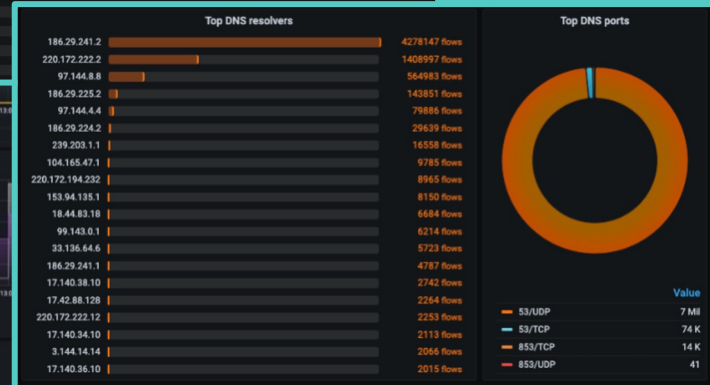
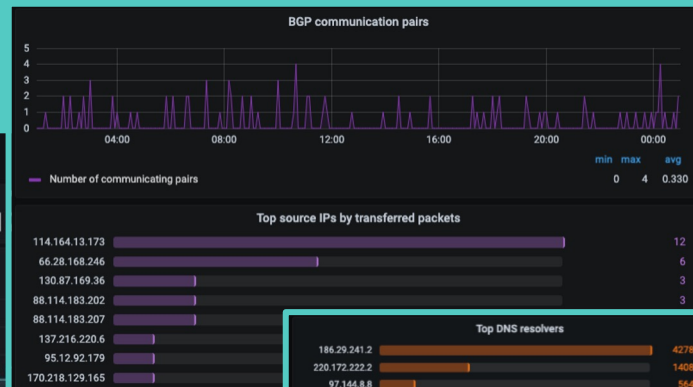
no way

Photo from [twitter.com/billydracula/](https://twitter.com/billydracula/)

FLOWCUTTER



# Grafana examples





# 20y, 100y ago

**libs used to be like that**





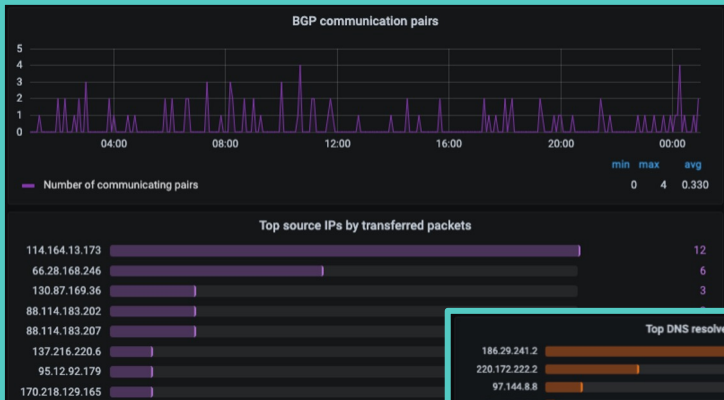
1M+fps

Flow records per second

Photo from [www.timessquarenyc.org](http://www.timessquarenyc.org)

**FLOWCUTTER**

# Grafana examples





A large, blue, saucer-shaped alien spaceship with glowing green lights and a laser beam is shown in space. The laser beam is hitting a group of smaller, white, T-shaped ships. The background is a dark space with stars and a planet's horizon.

size

this time it matters

A close-up photograph of Keanu Reeves from the movie 'The Matrix'. He is wearing a white dress shirt and has a very intense, almost pained or shocked expression on his face. His eyes are wide open, and his mouth is slightly open and distorted. The background is a solid teal color. Overlaid on the left side of the image is the text 'I have no mouth and I must scream' in a large, bold, sans-serif font. The first line 'I have no mouth' is in black, and the second and third lines 'and I must' and 'scream' are in white.

I have no mouth  
and I must  
scream

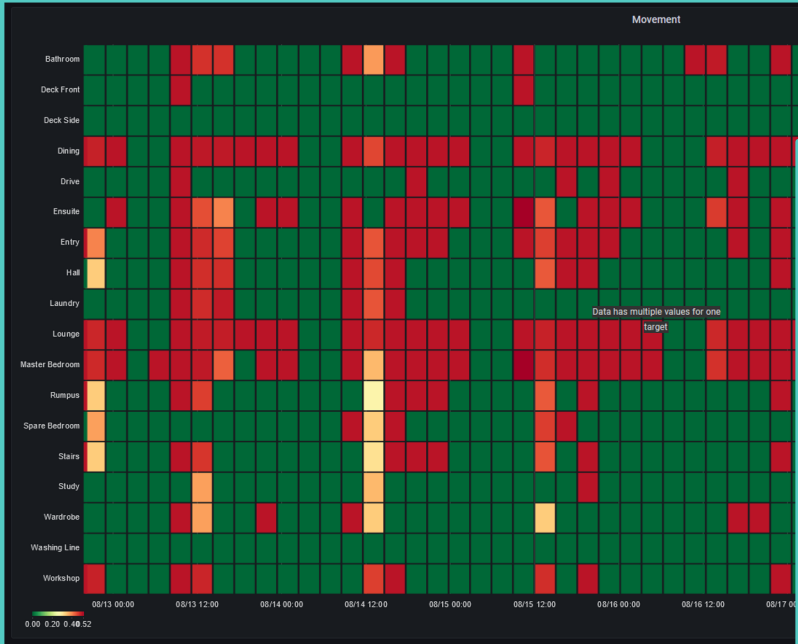
Photo from Matrix the movie

**FLOWCUTTER**



# vendor lock

time is the key



# Heatmaps

# Peering matrix

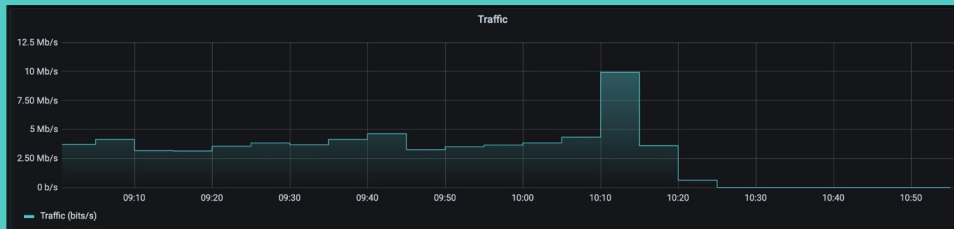


DAY 28

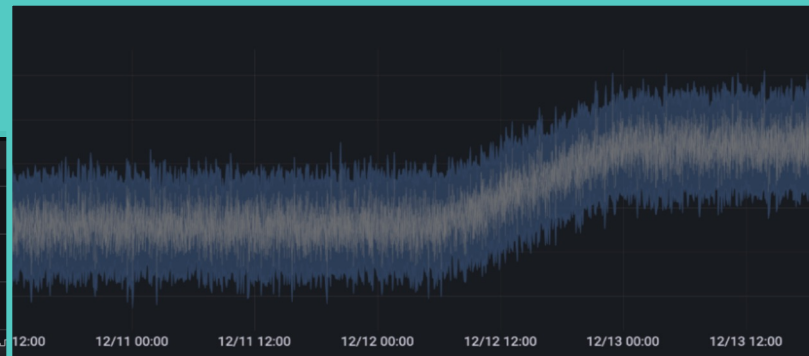
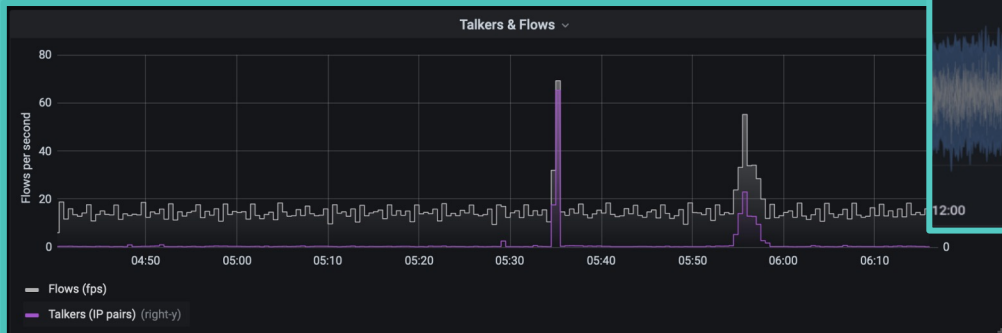
# degradation

Is it inevitable?

# Link down

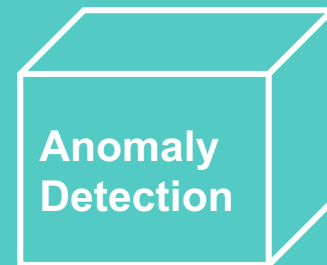
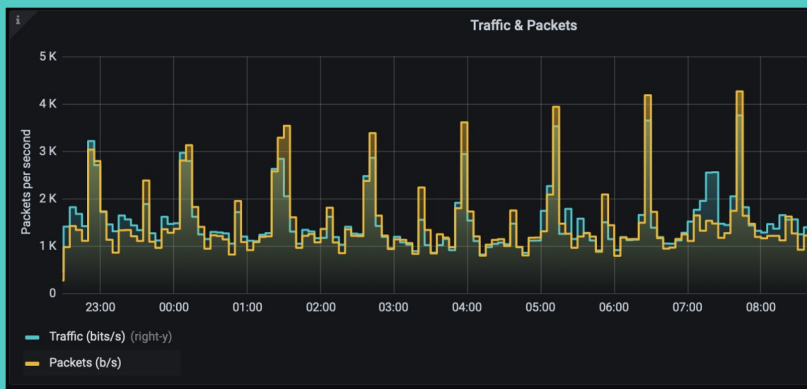


# Spikes and shifts

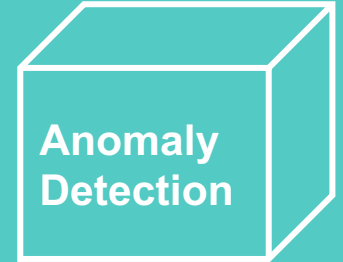
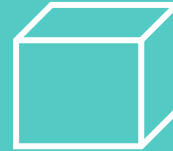
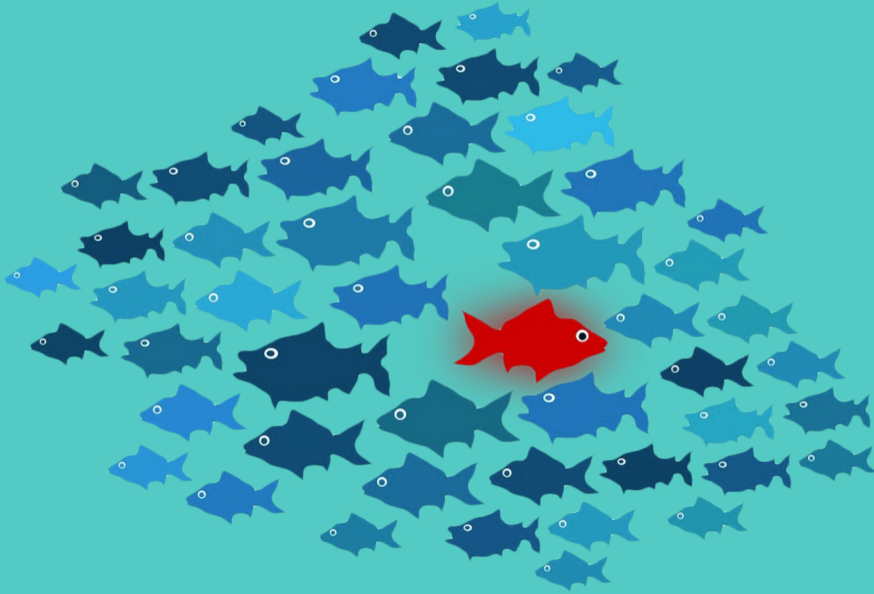




# Anomalies not for humanz



# Anomaly detection



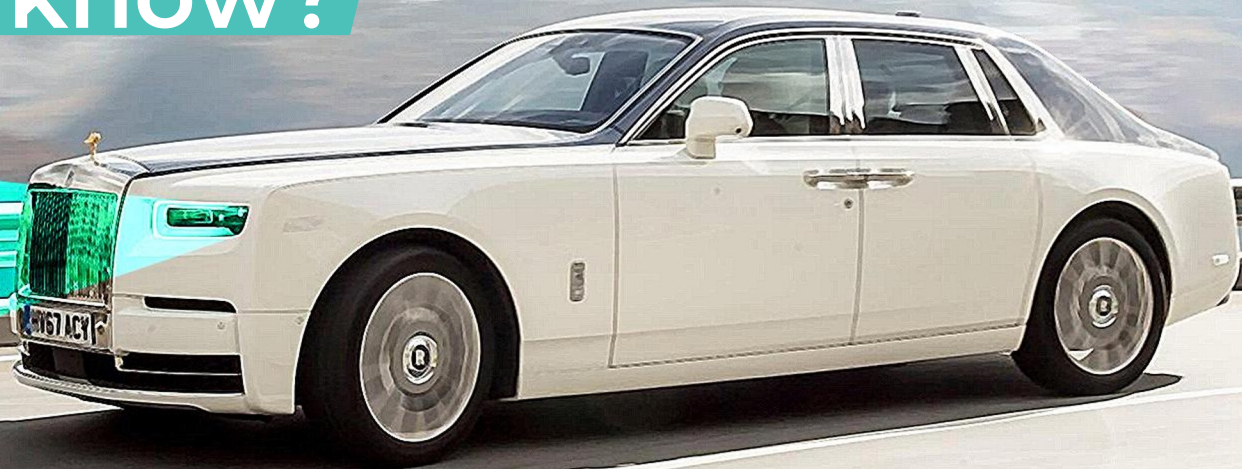


# 5 ways of solution

- **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

спасибо тебе, благодаря ти  
thank you

[www.flowcutter.com](http://www.flowcutter.com)