Detecting anomalies in huge Flow datasets



Mgr. Matej Pavelka PhD.



telemetry?

Phto from Matrix the movie



5 ways a tool can suck

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



schizophrenia

34.5 kpps 41.2 kpps 114 K

Photo from Matrix the movie

FLOWCUTTER



site all - filter +

0 \$

cold coffee

no way

Photo from twitter.com/billydracula/



Grafana examples



BGP communication pairs

FLOWCUTTER

Value

7 Mil

Top DNS ports

- 53/UDP

- 53/TCP

- 853/TCP

- 853/UDP

libs used to be like that

EC.

Photo from www.timessquarenyc.org



Flow records per second

V-HOS

Photo from www.timessquarenyc.org



Grafana examples



	Top source IPs by transferred packets	
73		
46 (
36		
02		

114.164.13.173 66.28.168.246 130.87.169.36 88.114.183.202 88.114.183.207 137.216.220.6 95.12.92.179 170.218.129.165

	Top DNS resolvers		Top DNS ports
186.29.241.2		4278147 flows	
220.172.222.2		1408997 flows	
97.144.8.8		564983 flows	
186.29.225.2		143851 flows	
97.144.4.4		79886 flows	
186.29.224.2		29639 flows	
239.203.1.1		16558 flows	
104.165.47.1		9785 flows	
220.172.194.232		8965 flows	
153.94.135.1			
18.44.83.18		6684 flows	
99.143.0.1			
33.136.64.6			
186.29.241.1		4787 flows	
17.140.38.10			
17.42.88.128		2264 flows	Value
220.172.222.12			- 53/UDP 7 Mil
17.140.34.10		2113 flows	- 53/TCP 74 K
3.144.14.14		2066 flows	- 853/TCP 14 K
17.140.36.10			- 853/UDP 41



this time it matters

1.

Photo from thewertzone.blogspot.com

SIZE



I have no mouth and i must

scream

Photo from Matrix the m



vendor

time is the key

Photo from www.geocaching.com





1.49 kWh

Heatmaps Peering matrix

FLOWCUTTER

CEGITAO Is it inevitable?

DAY 28



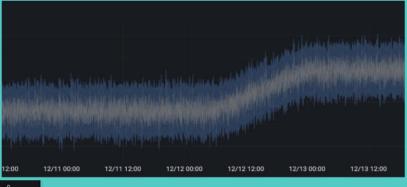
Photo from www.vice.com/

Link down



Spikes and shifts

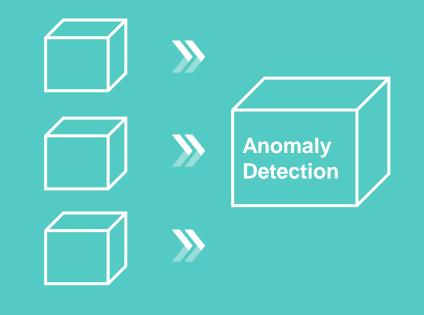




FLOWCUTTER

Anomalies not for humanz





FLOWCUTTER

Anomaly detection

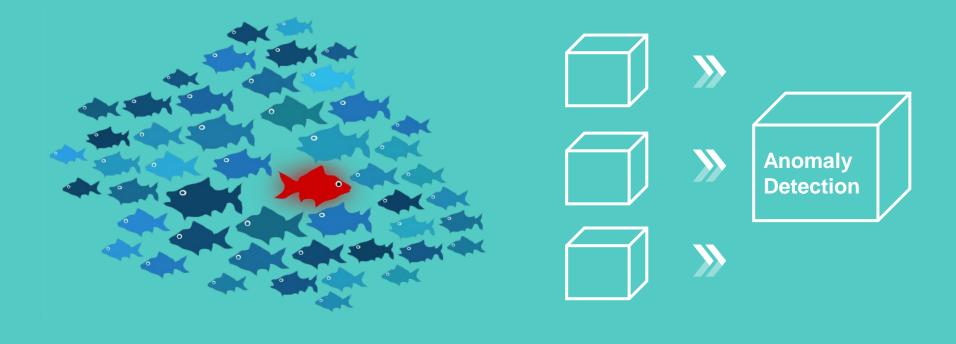
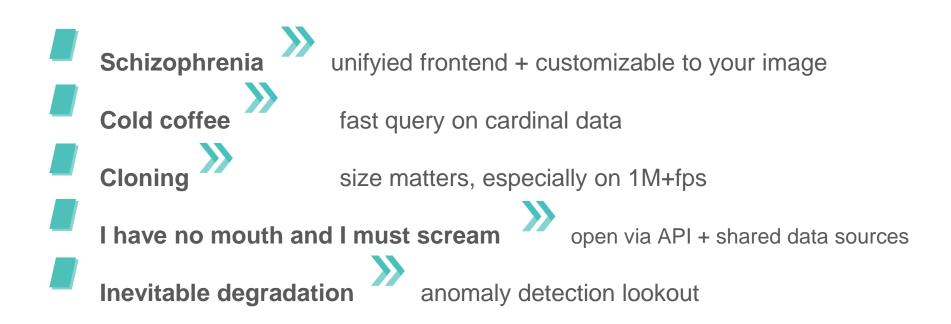


Photo from thedatascientist.com/



5 ways of solution



60 mph do you know?

ANGT ACY

DIAN

0

Photo from /www.carismo.cz



TOP



thank you

www.flowcutter.com

Photo from www.sciencefocus.com/planet-eart

