

Proč Seznam zvažuje

FLOWCUTTER

?

Mgr. Matej Pavelka PhD.

FLOWCUTTER



Foto z newsweek.com



Foto z seznam.cz

1M

záznamů za sekundu

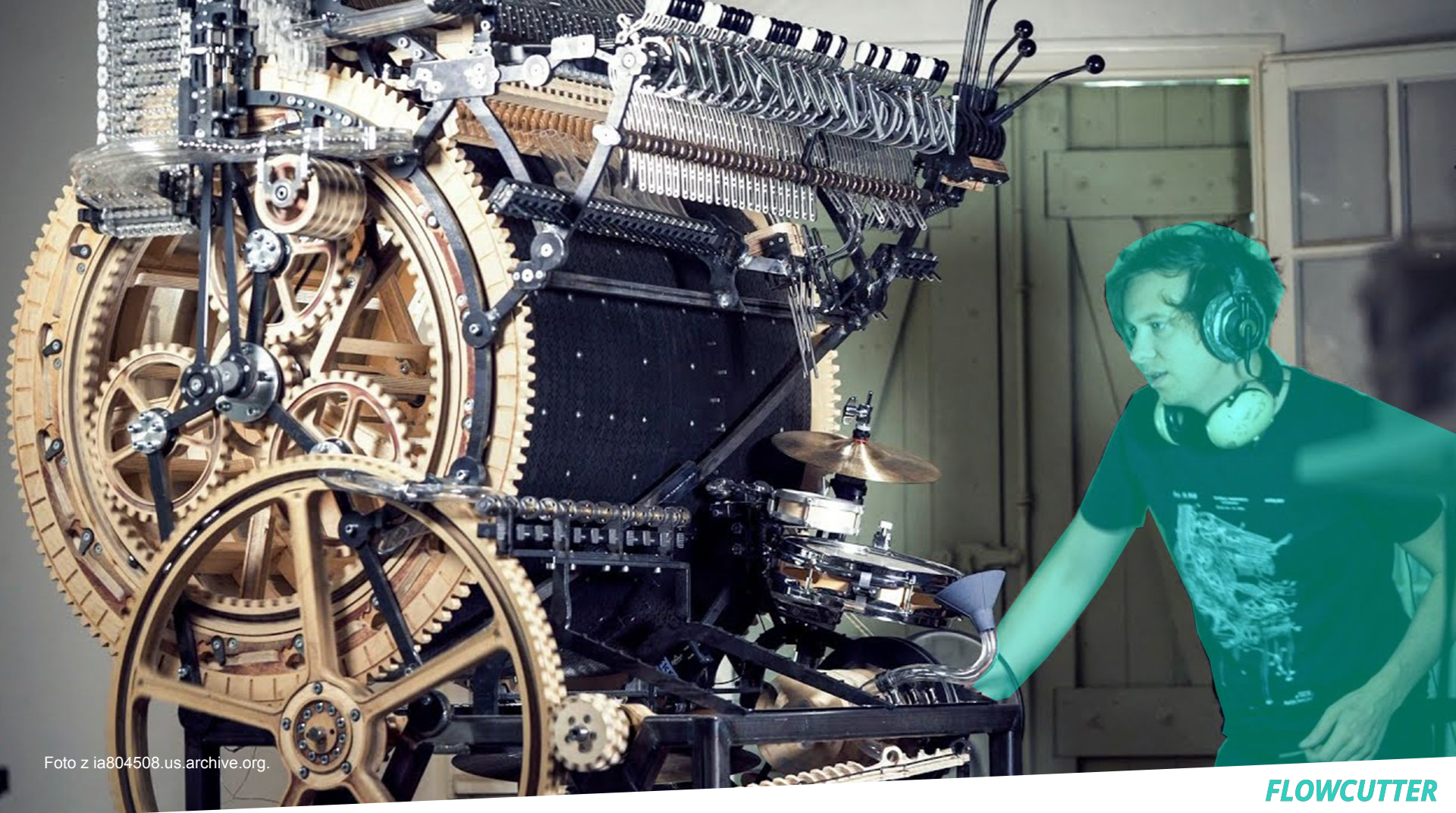
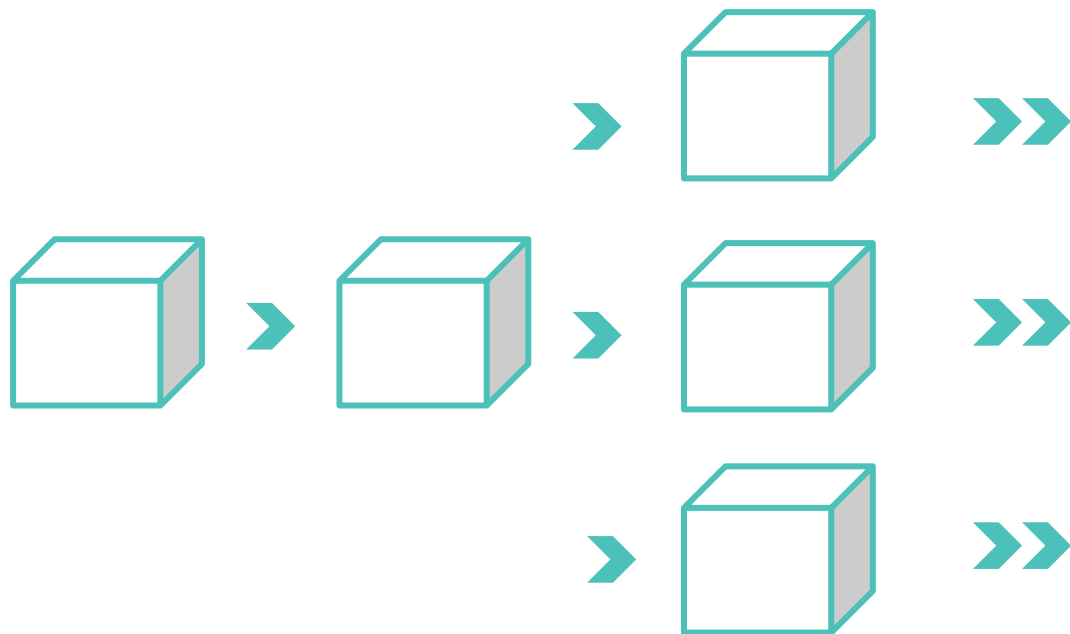


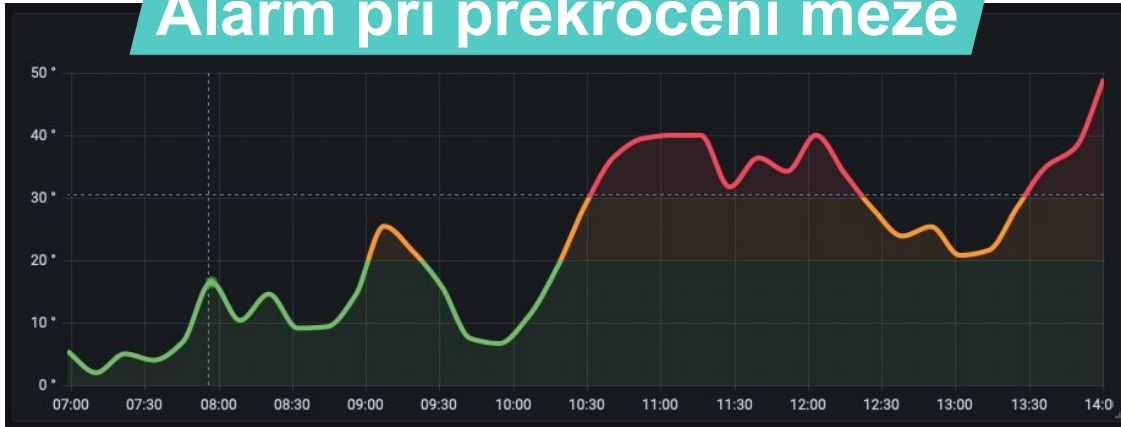
Foto z ia804508.us.archive.org.

FLOWCUTTER

Lateral movement



Alarm při překročení meze



Vytvořit vlastní profil >

> Export BGP Flowspec

PS

+ Add profile

Web in

Web out

Profile name*

Sip

Dip

Sport

Dport

Sensor

Save Profile

Forenzní analýza

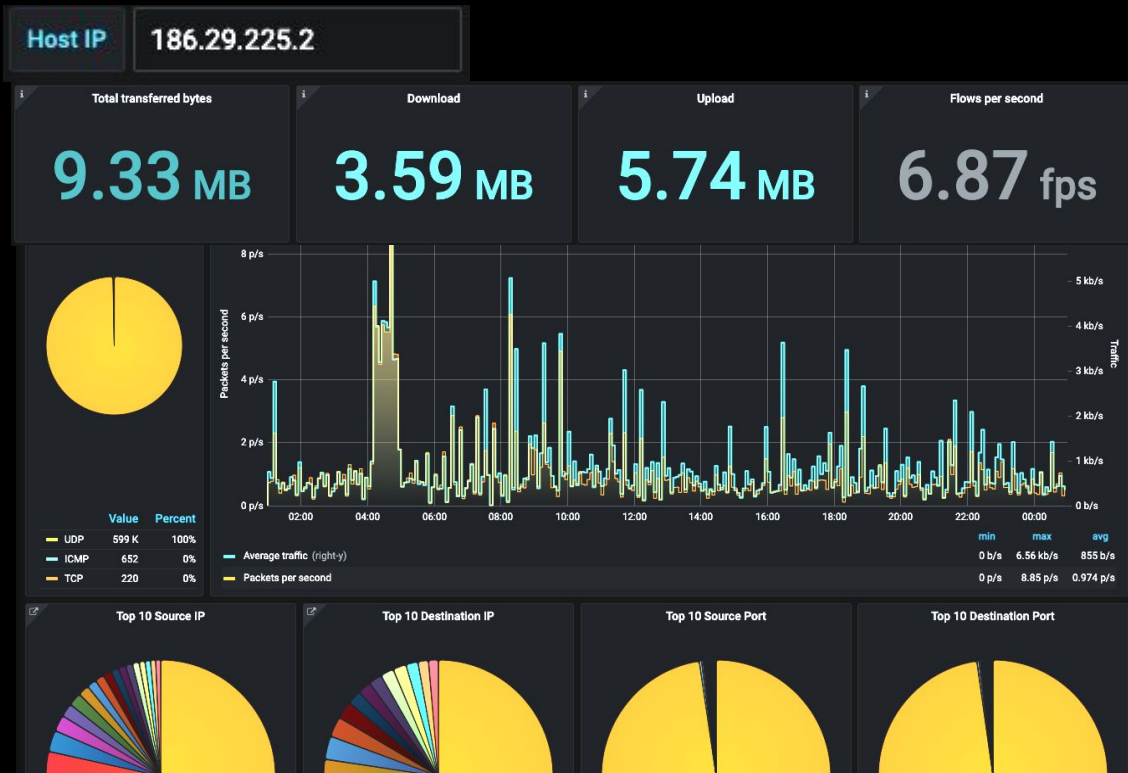


Foto z bluewire.com

FLOWCUTTER

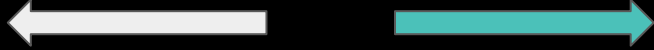
FLOWCUTTER

Filter, and quick check of device behavior



FLOWCUTTER

Scanners and bots examples



228.113.248.52 1

Port = 21 (telnet)

220.172.197.210	1
220.172.37.177	1
220.172.41.150	1
220.172.138.72	1
145.209.28.251	1
220.172.224.151	1
220.172.223.93	1
220.172.173.126	1
220.172.228.169	1
177.195.202.54	1
220.172.165.79	1
220.172.235.62	1
220.172.226.172	1

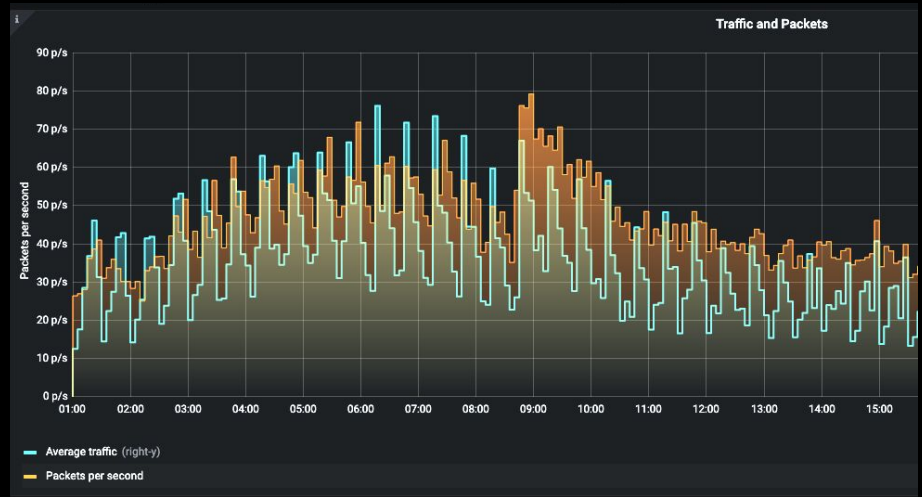


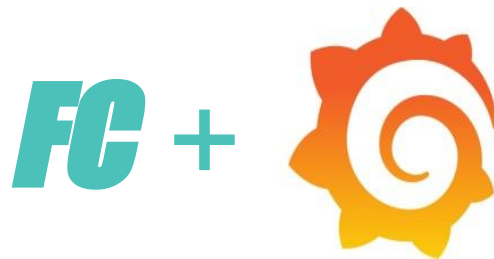


Foto z [writingsolife.com](https://www.writingsolife.com)

FLOWCUTTER

FLOWCUTTER + Grafana

- Ingest 1Mfps (2022)
- Nejrychlejší dotazy (2021)
- Grafana (2021)



“Roadmap”

- Open API
- Alerting a detekce



FLOWCUTTER

Děkuji

www.flowcutter.com

FLOWCUTTER