

FLOWCUTTER

Analýza netflow **jinak**

Mgr. Matej Pavelka PhD.

FLOWCUTTER

FLOWCUTTER

Network Visibility Tool

Analýza netflow jinak

Mgr. Matej Pavelka PhD.

www.flowcutter.com



Foto z Pexels.com

FLOWCUTTER

What?



Foto z Pexels.com

FLOWCUTTER

FLOWCUTTER

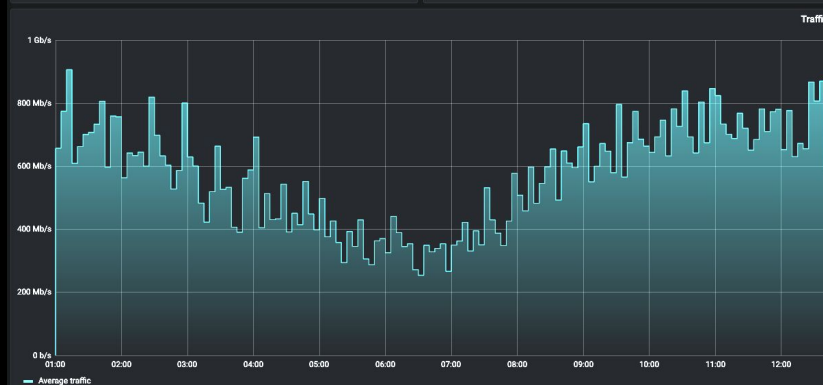
Nástroj na vizualizaci a analýzu syrových flow dat

- + Nejrychlejší**
- + K obrazu svému**
- + Otevřený**

FLOWCUTTER

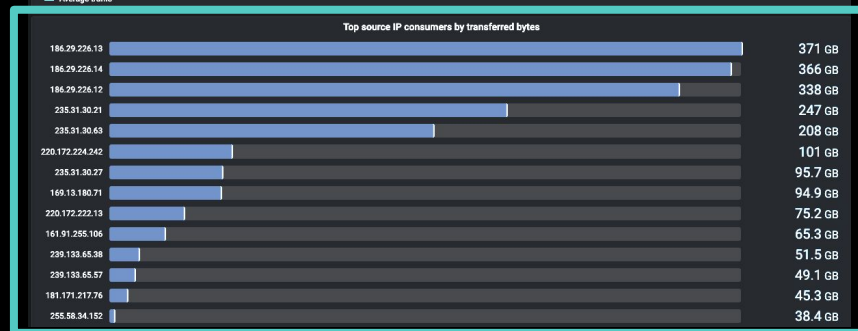
Total transferred bytes
7.06 TB

Average traffic
647 Mb/s



Využití šířky pásma

TOP konzumenti .



FLOWCUTTER

FLOWCUTTER

Filtering

Filtrování přes source IP

Site	Lhota - Perimet ▾	Source IP	1.2.3.4/23	Destination IP	
------	-------------------	-----------	------------	----------------	--

umožňuje filtrovat přes jakékoliv IPFIX pole,
(IP, port, protocol, vlan, asn, ...).

FLOWCUTTER

Ports and Protocols

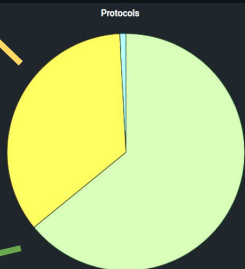
UDP

227 kpps

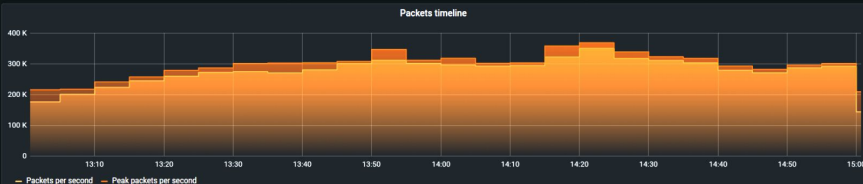
350 kpps

1.026 Mil

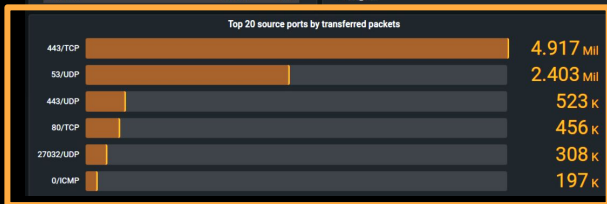
2552 fps



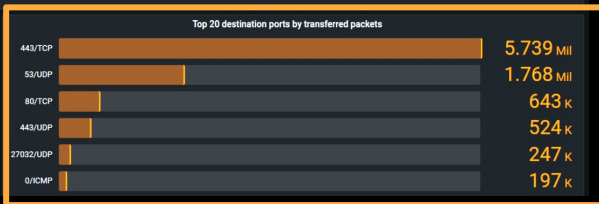
TCP



Top source ports



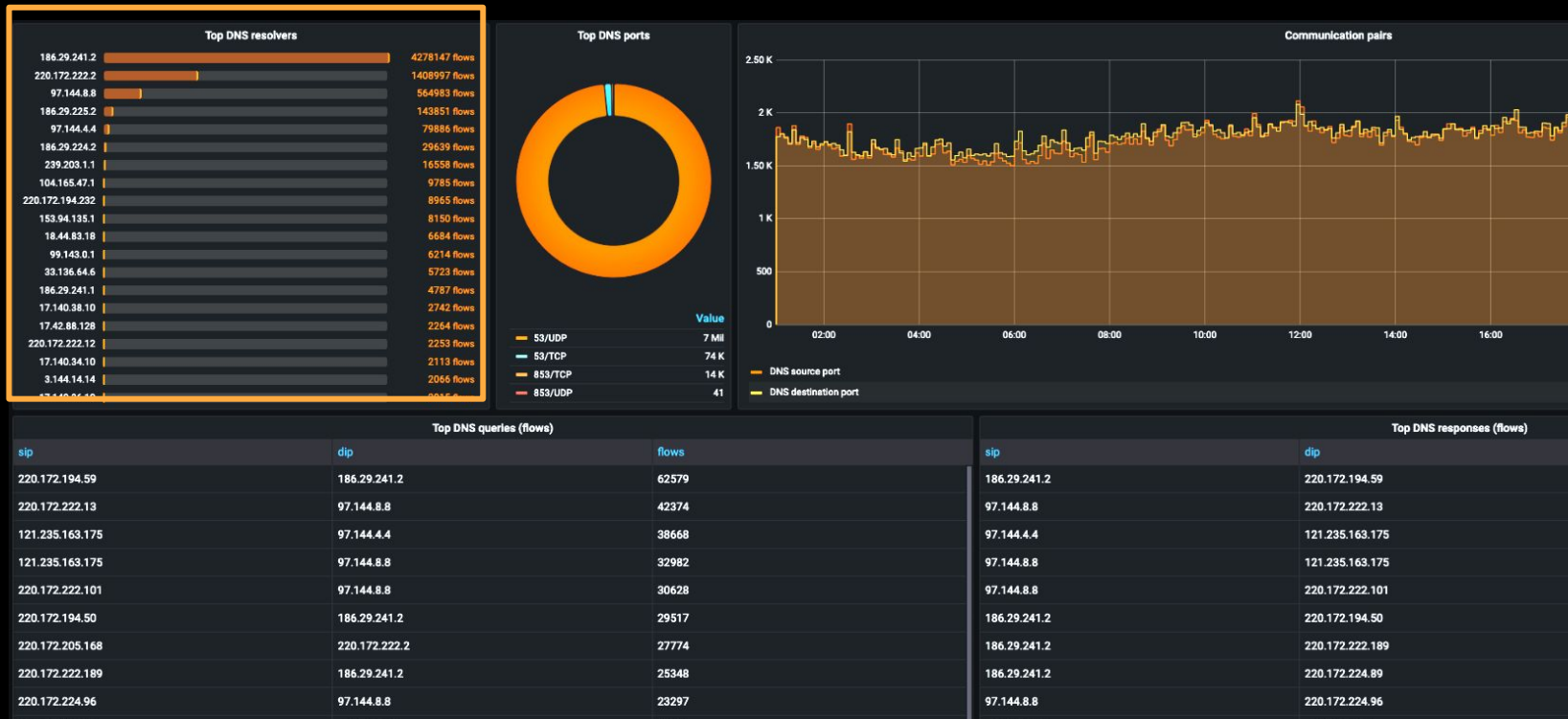
Top dest. ports



FLOWCUTTER

Visibility to DNS traffic

Top DNS Resolvers



What?



Foto z Pexels.com

FLOWCUTTER

10+ nodes cluster

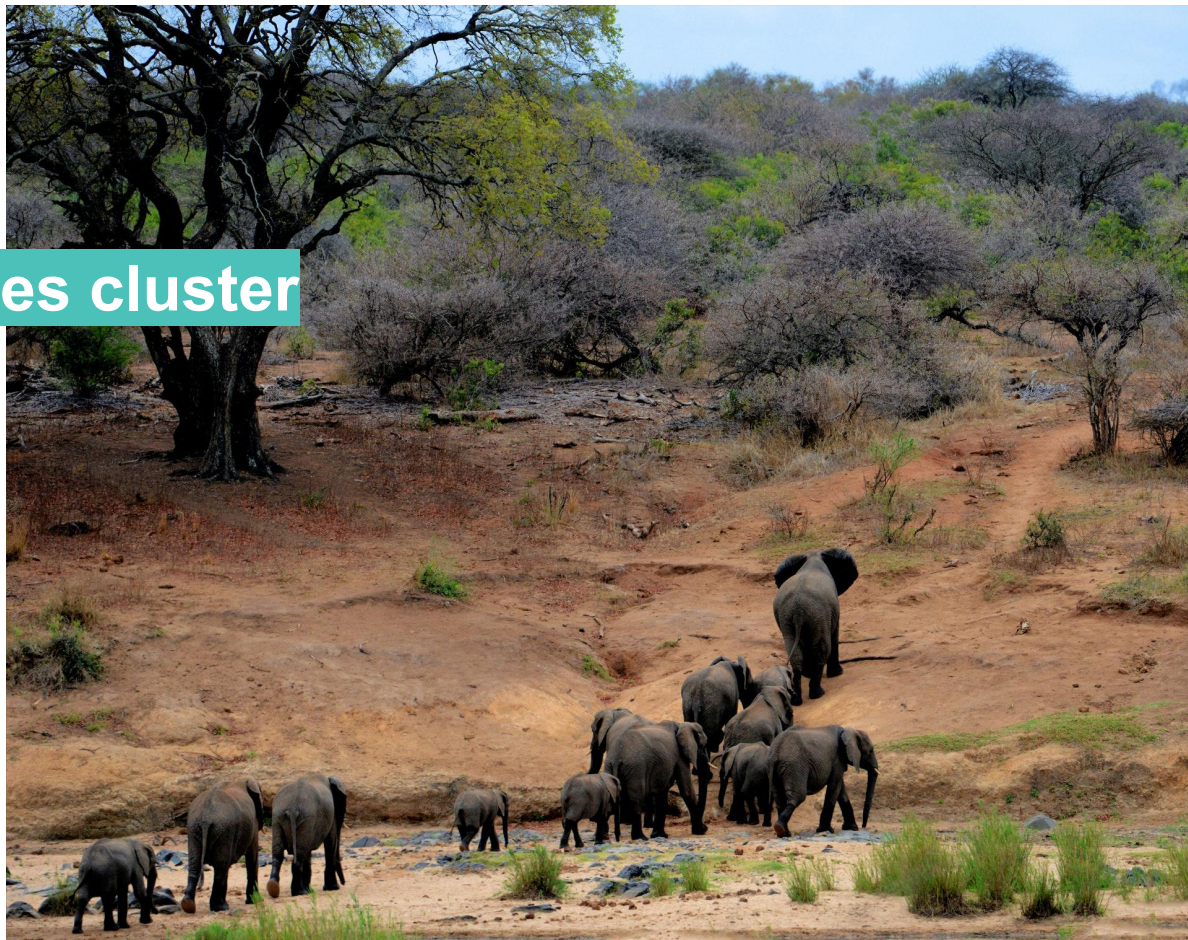


Foto z Pexels.com

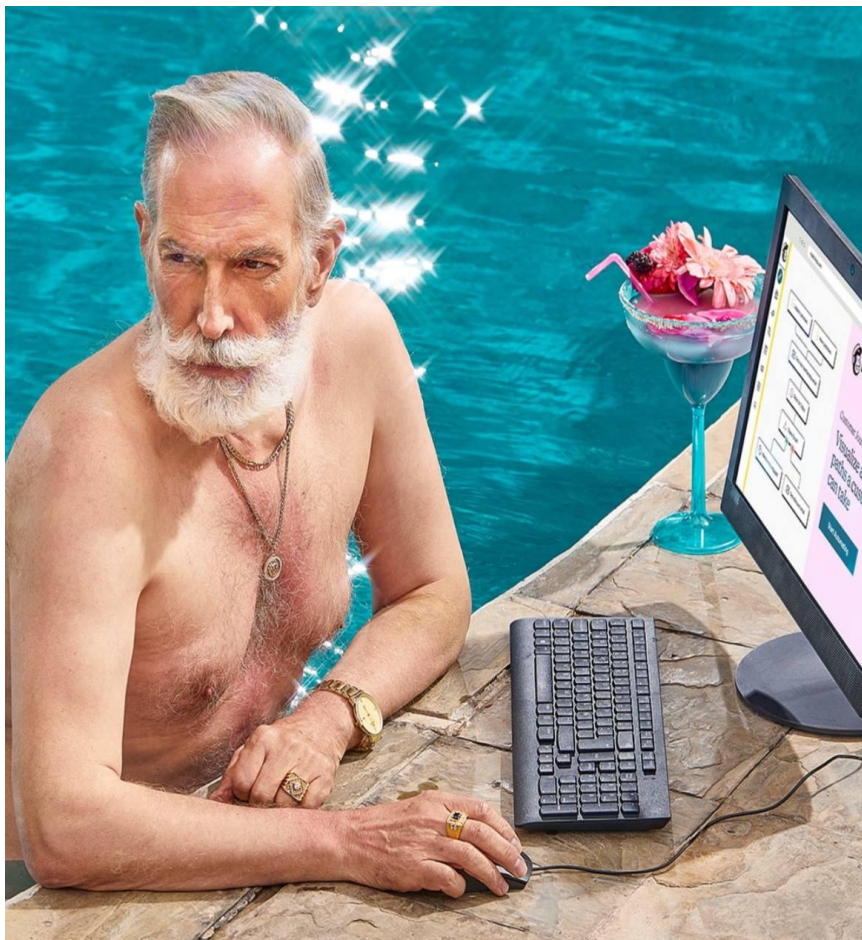
Netflow /
IPFIX



sFlow

Foto z Pexels.com

FLOWCUTTER



Data jsou Vaše

Nikam do cloudu

Možnost šifrovat



Foto z Pexels.com

FLOWCUTTER

Filter, and quick check download/upload





Foto z Pexels.com

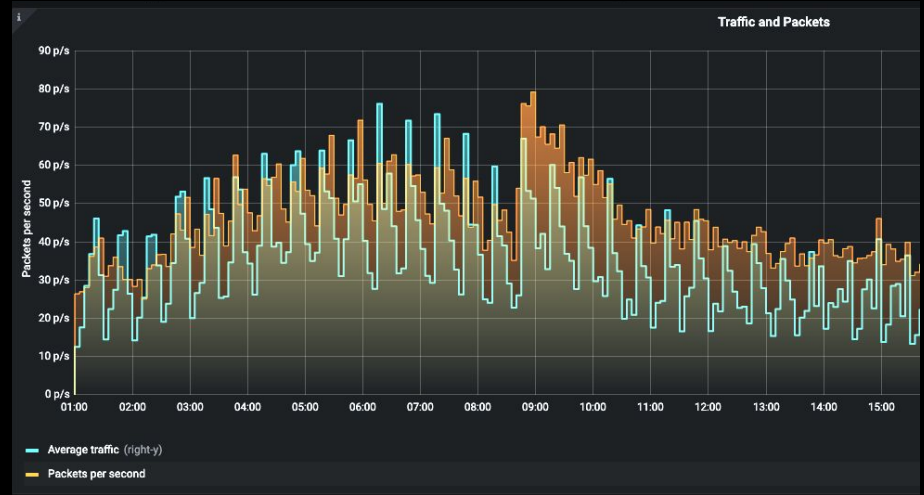
FLOWCUTTER

Scanners and bots examples



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



Cyber
džungle,

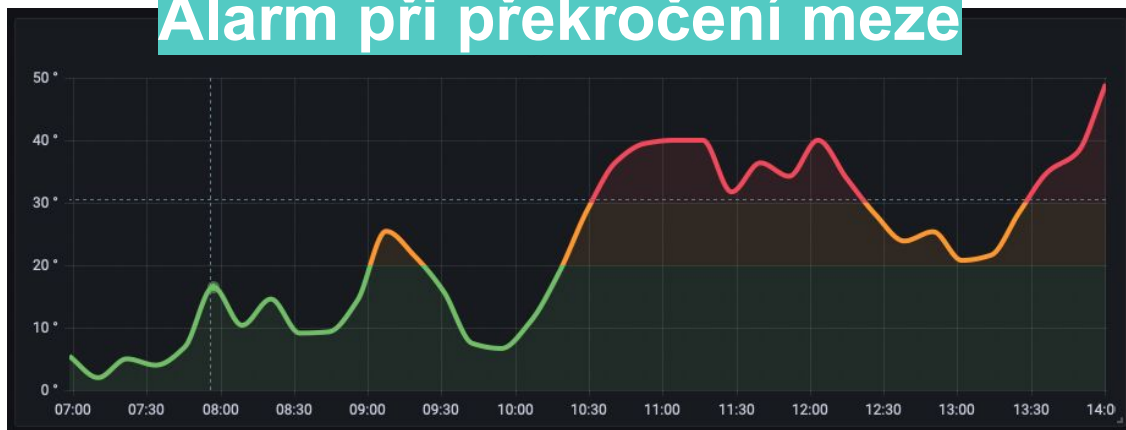
Žádný
Mauglí

Skeny, hesla

Malware, Blisty

NUKIB

Alarm při překročení meze



Vytvořit vlastní profil >

PS

+ Add profile

Web in

Web out

Profile name*

Profile name

Sip

IP / subnet

Dip

IP / subnet

Sport

Source port/s

Dport

Destination port/s

Sensor

SID

Save Profile



Foto z Pexels.com

FLOWCUTTER

FLOWCUTTER

Nástroj na vizualizaci a analýzu syrových flow dat

- + Nejrychlejší**
- + K obrazu svému**
- + Otevřený**

FLOWCUTTER

13

matej.pavelka@flowcutter.com

FLOWCUTTER