Analýza kořenových příčin

a benefit mnoha zdrojů dat

FLOWCUTTER

Mgr. Matej Pavelka PhD.

Čím začít?

- Čas techniků je drahý
- Troubleshooting je na problémy,

kt je levnější řešit hned a nečekat na důsledky

Use cases

- #1 Outgoing DDoS
- #2 Hacked camera damaged /22 prefix
- #3 Hotline on steroid
- #4 Syslog
- Co si odnést

#1 case

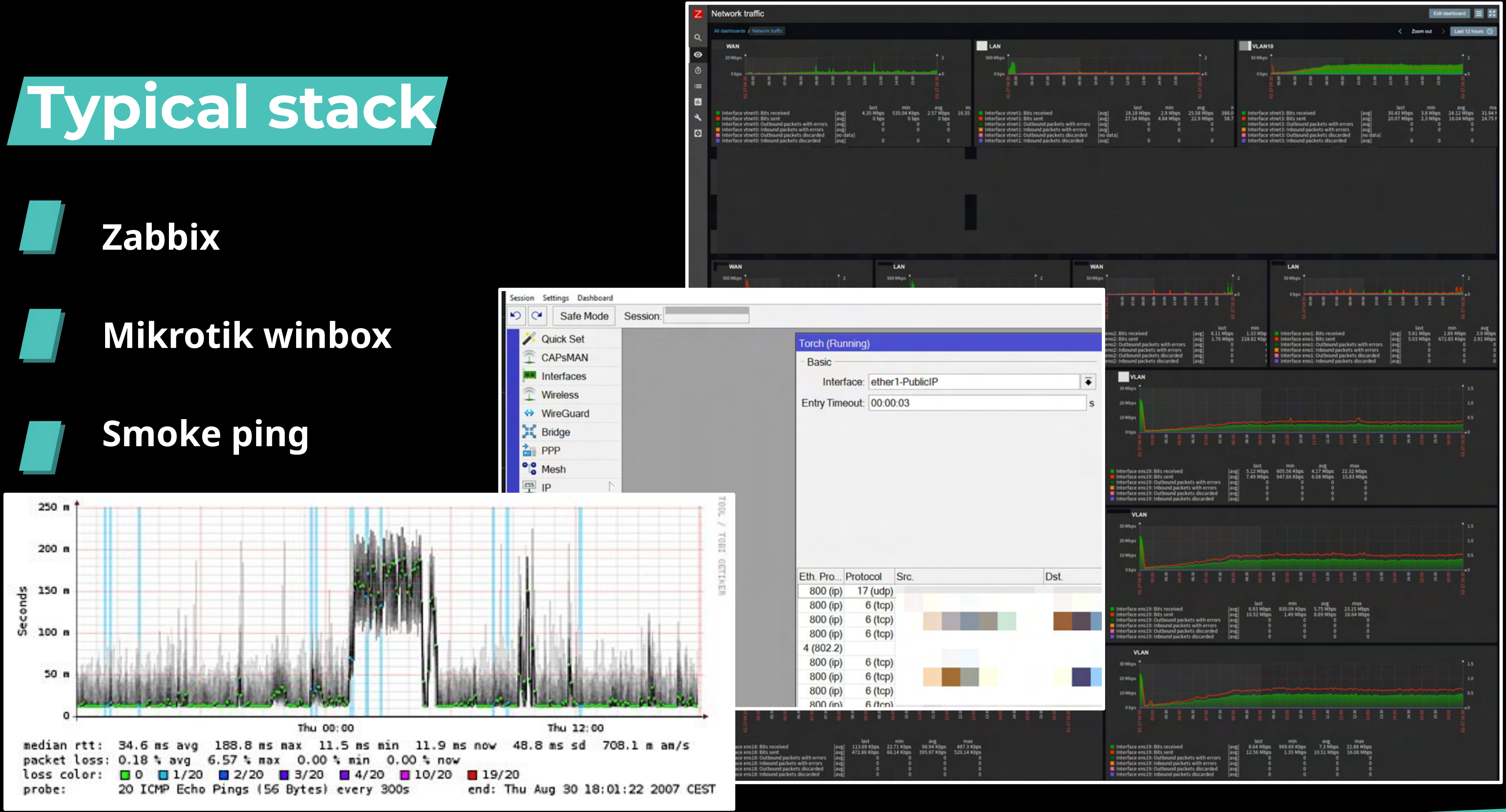
Latency issue at Enterprise customer

Anomaly

- Latency and connection issues in MS Teams
- For ~10 minutes
- Every ~1.5h

Typical stack

- Zabbix
- Mikrotik winbox
- Smoke ping



Torch (Running)

Basic

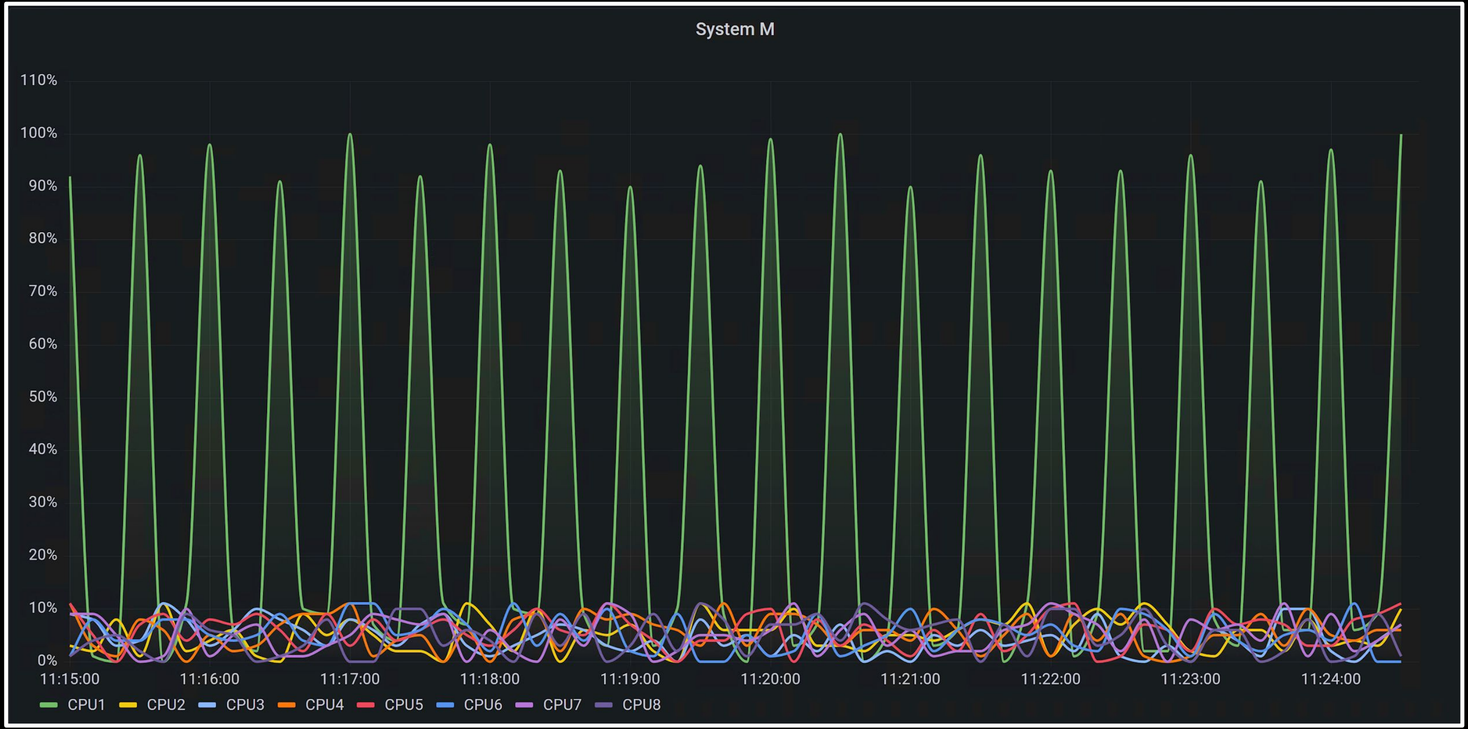
Interface: ether1-PublicIP

Entry Timeout: 00:00:03 s

Eth. Pro...	Protocol	Src.	Dst.
800 (ip)	17 (udp)		
800 (ip)	6 (tcp)		
800 (ip)	6 (tcp)		
800 (ip)	6 (tcp)		
4 (802.2)			
800 (ip)	6 (tcp)		
800 (ip)	6 (tcp)		
800 (ip)	6 (tcp)		
800 (ip)	6 (tcp)		

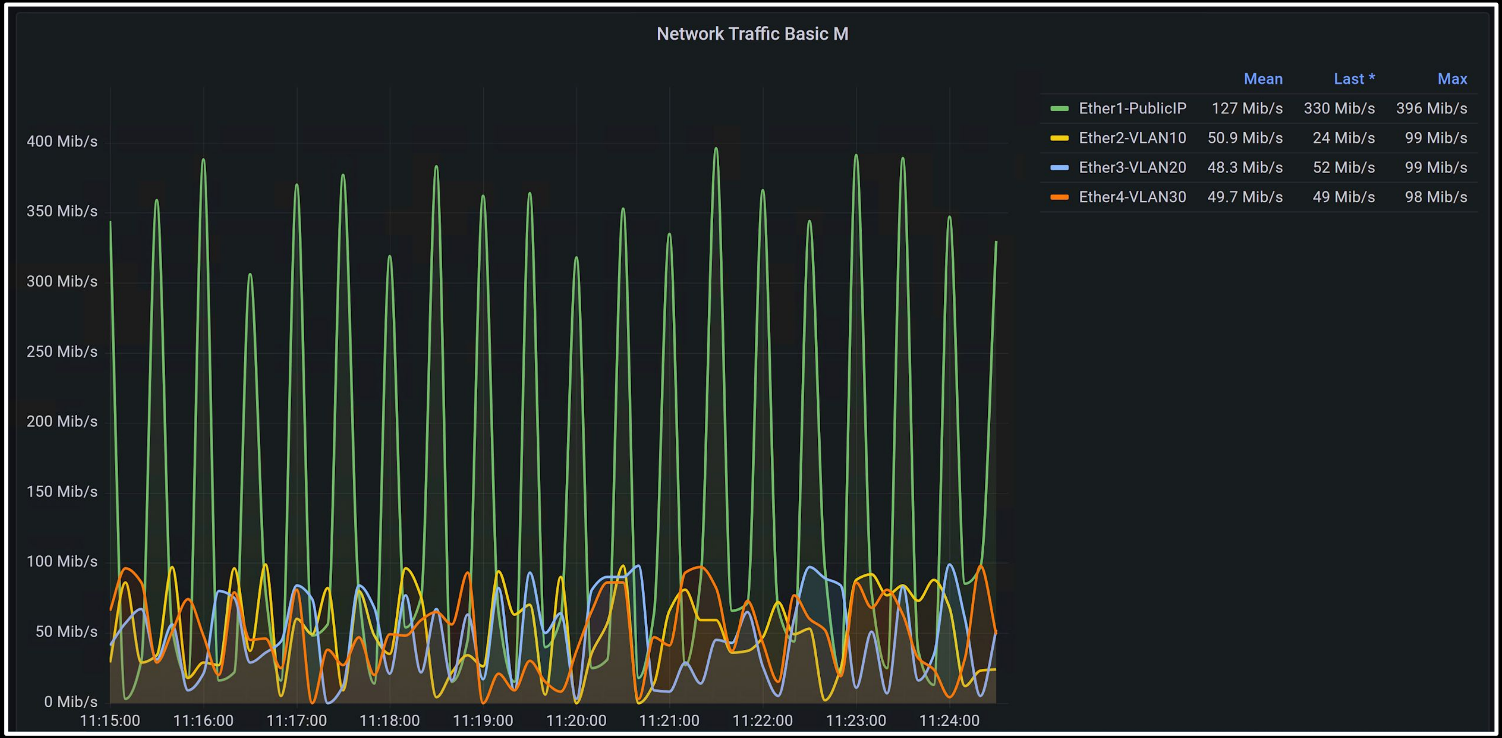
```
median rtt:   34.6 ms avg   188.8 ms max   11.5 ms min   11.9 ms now   48.8 ms sd   708.1 m am/s
packet loss:  0.18 % avg   6.57 % max   0.00 % min   0.00 % now
loss color:   🟩 0  □ 1/20  ■ 2/20  ■ 3/20  ■ 4/20  ■ 10/20  🟥 19/20
probe:        20 ICMP Echo Pings (56 Bytes) every 300s          end: Thu Aug 30 18:01:22 2007 CEST
```

CPU on router



Traffic on port

One eth port w/ peaks in bps



Network Traffic Basic M

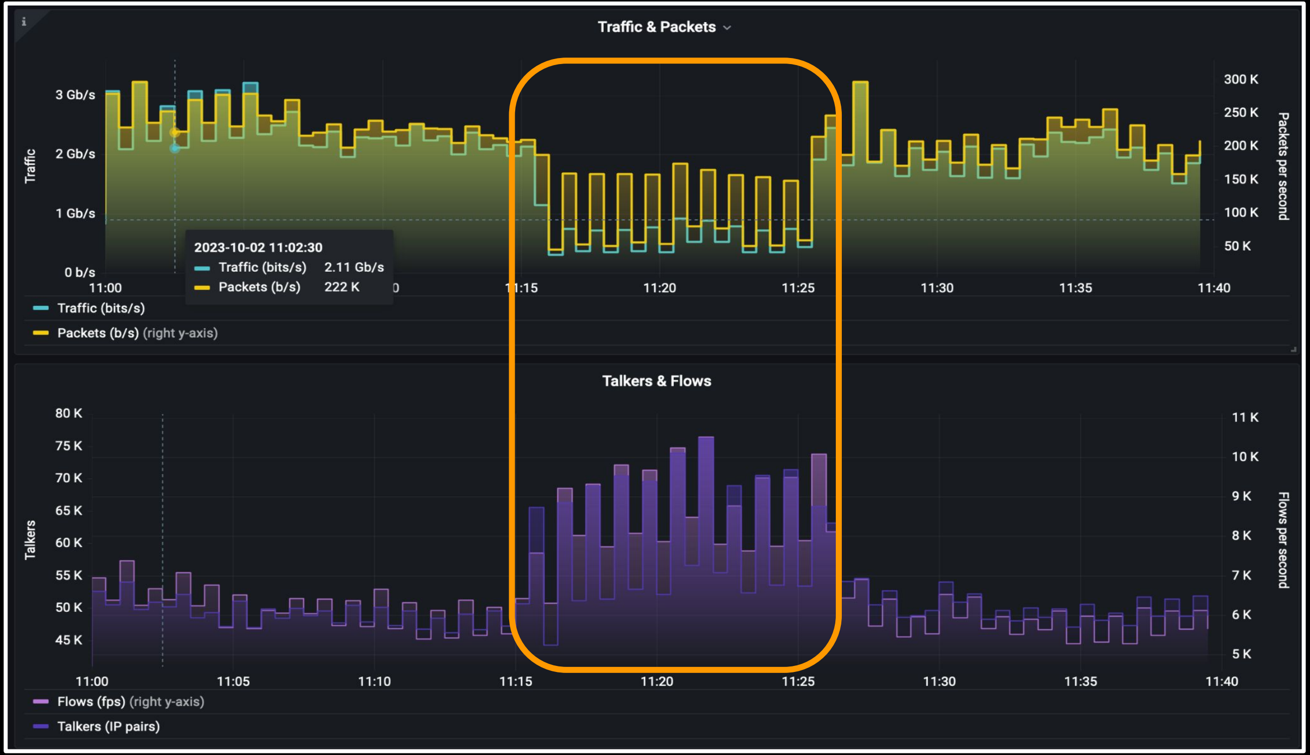
	Mean	Last *	Max
🟩 Ether1-PublicIP	127 Mib/s	330 Mib/s	396 Mib/s
🟨 Ether2-VLAN10	50.9 Mib/s	24 Mib/s	99 Mib/s
🟦 Ether3-VLAN20	48.3 Mib/s	52 Mib/s	99 Mib/s
🟧 Ether4-VLAN30	49.7 Mib/s	49 Mib/s	98 Mib/s

SNMP x Flows

- SNMP - 1D dimensional time series - what’s happening with the router
- Flows - high-cardinality big data - who is communicating with whom

Flow data

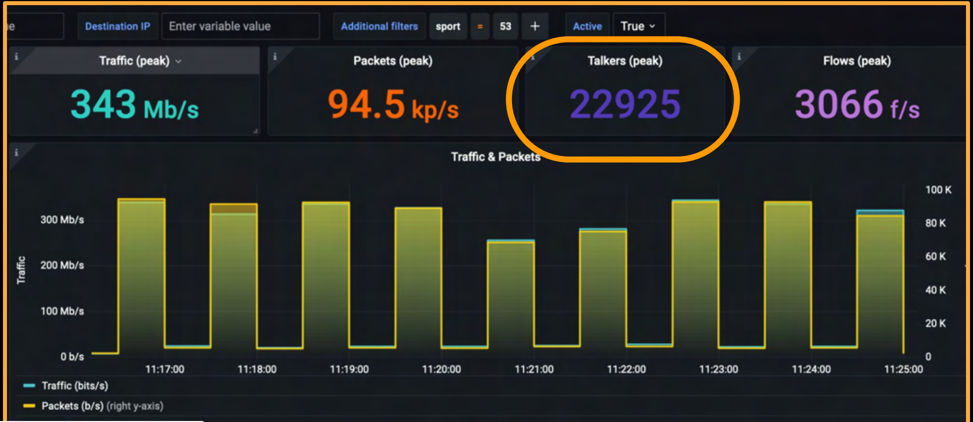
All traffic BPS, PPS, FPS, talkers



10 minutes

Before / after

During anomaly



ue | Destination IP | Enter variable value | Additional filters | sport = 53 + | Active | True

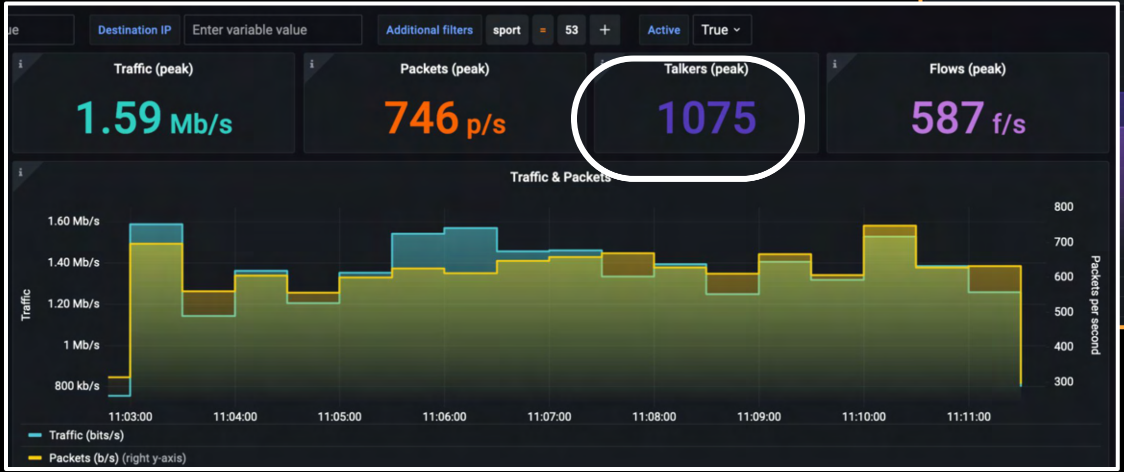
Traffic (peak): 343 Mb/s

Packets (peak): 94.5 kp/s

Talkers (peak): 22925

Flows (peak): 3066 f/s

Before anomaly



ue | Destination IP | Enter variable value | Additional filters | sport = 53 + | Active | True

Traffic (peak): 1.59 Mb/s

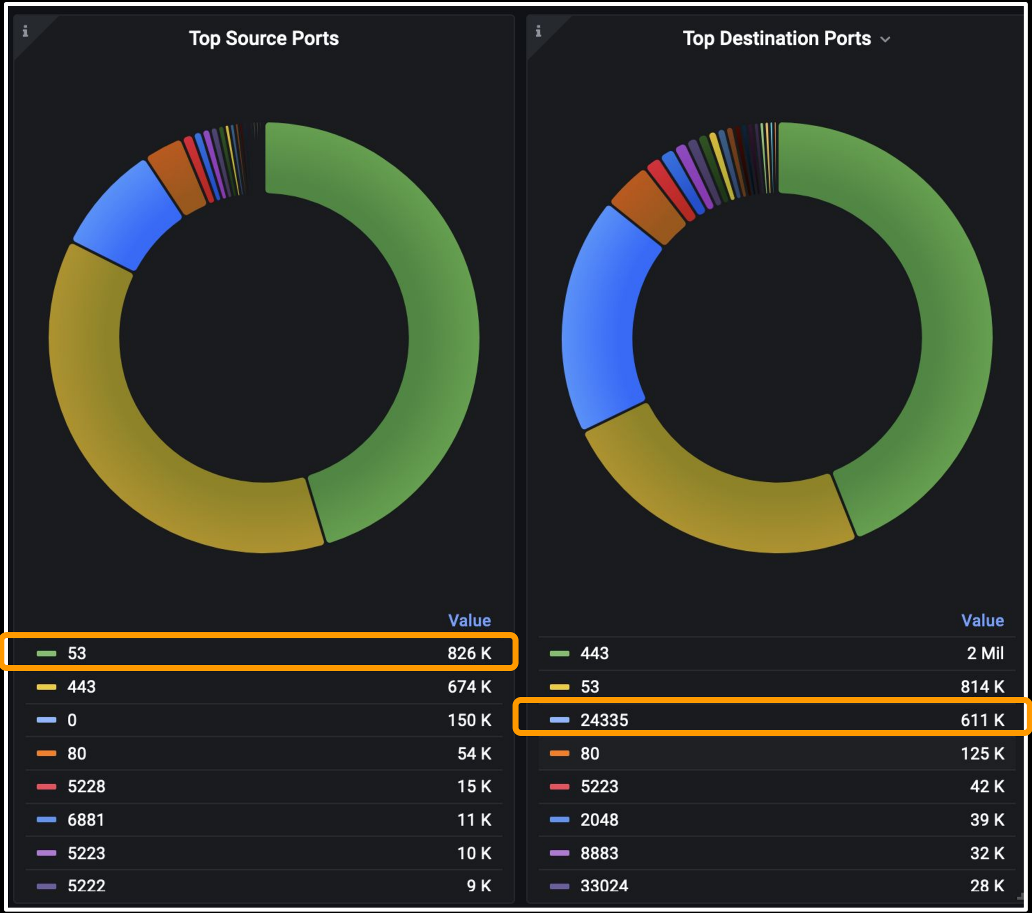
Packets (peak): 746 p/s

Talkers (peak): 1075

Flows (peak): 587 f/s

Drill down

- Source port = 53



Top Source Ports

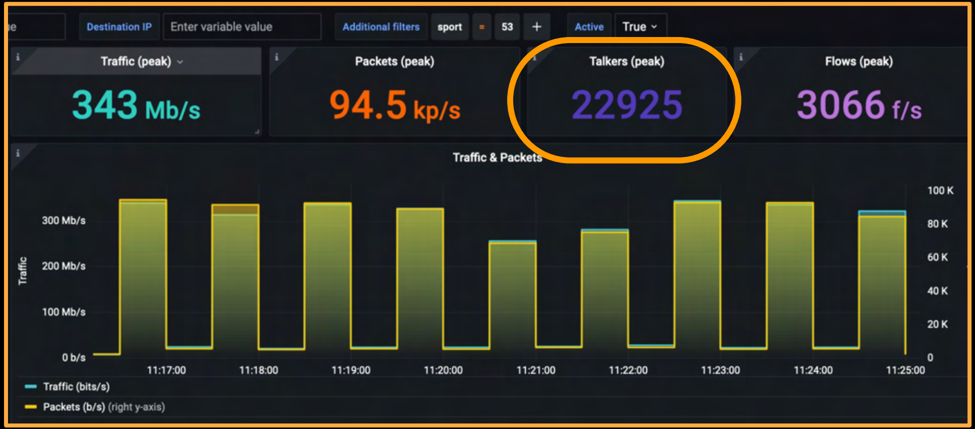
	Value
🟩 53	826 K
🟨 443	674 K
🟦 0	150 K
🟧 80	54 K
🟥 5228	15 K
🟦 6881	11 K
🟪 5223	10 K
🟪 5222	9 K

Top Destination Ports

	Value
🟩 443	2 Mil
🟨 53	814 K
🟦 24335	611 K
🟧 80	125 K
🟥 5223	42 K
🟦 2048	39 K
🟪 8883	32 K
🟪 33024	28 K

Reflection attack

- Distributed attack using open DNS ports
- Mitigated using BGP FlowSpec: Src/Dest ports = 53/24335



Destination IP: Enter variable value

Additional filters: sport = 53 +

Active: True

Traffic (peak): 343 Mb/s

Packets (peak): 94.5 kp/s

Talkers (peak): 22925

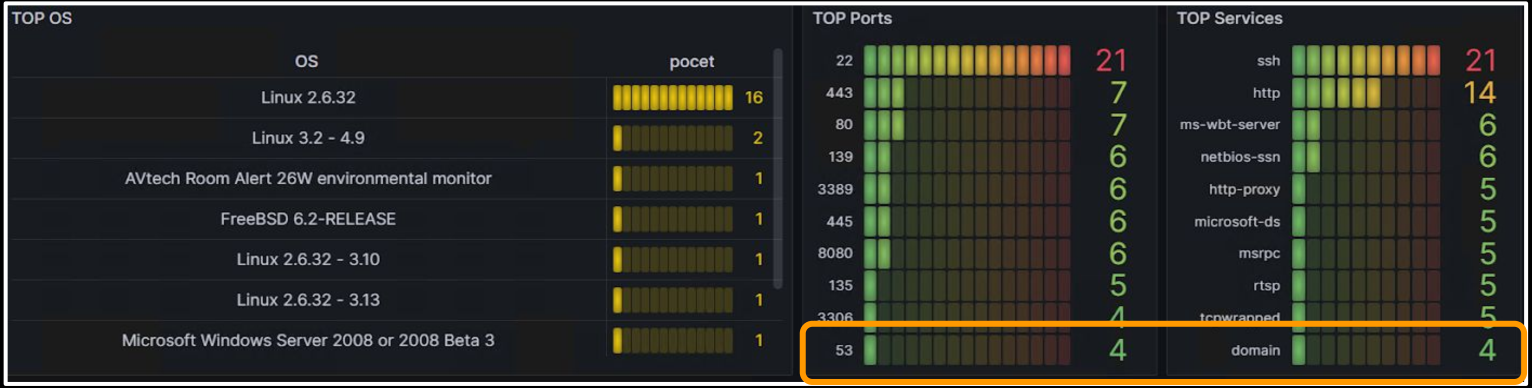
Flows (peak): 3066 f/s

Traffic & Packets

Open ports

- **Automated scan** (every night)
- **DNS port open** on SME customer’s public IP

Example screenshot (not the actual case)



TOP OS

OS	pocet
Linux 2.6.32	16
Linux 3.2 - 4.9	2
AVtech Room Alert 26W environmental monitor	1
FreeBSD 6.2-RELEASE	1
Linux 2.6.32 - 3.10	1
Linux 2.6.32 - 3.13	1
Microsoft Windows Server 2008 or 2008 Beta 3	1

TOP Ports

22	21
443	7
80	7
139	6
3389	6
445	6
8080	6
135	5
3306	4
53	4

TOP Services

ssh	21
http	14
ms-wbt-server	6
netbios-ssn	6
http-proxy	5
microsoft-ds	5
msrpc	5
rtsp	5
tcpwrapped	5
domain	4

Outcome

- ISP was able to detect anomaly and find root-cause
- ISP mitigated it before customer called.
- Open ports scan and alerting set up to spot anomaly earlier next time

Risks

- ISP could lose its customer if not resolved next day
- Other customers could be influenced

Use cases

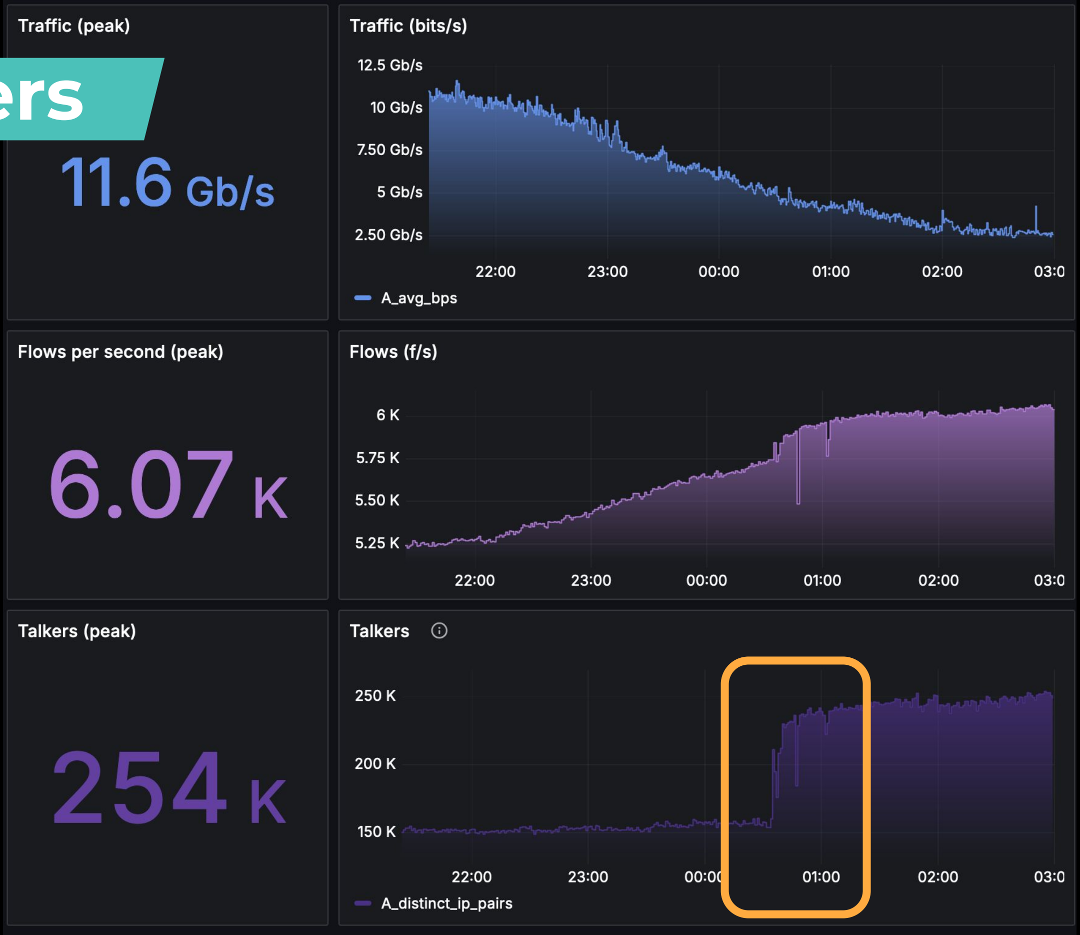
- #1 Outgoing DDoS
- #2 Hacked camera damaged /22 prefix
- #3 Hotline on steroid
- #4 Syslog
- Co si odnést

#2 case

Talkers anomaly vs IP reputation

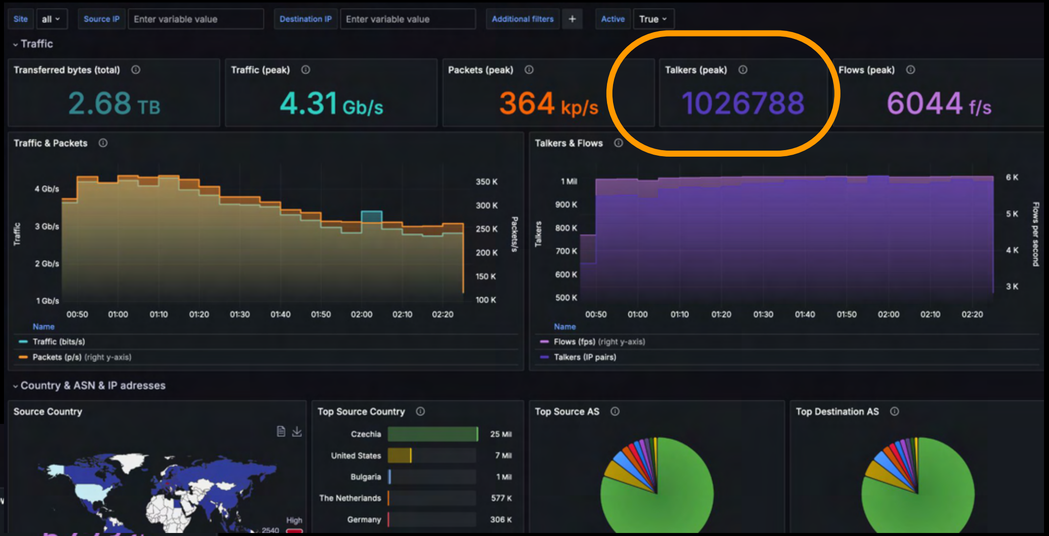
Anomaly on talkers

- Calculated on 10s interval



Before / after

During anomaly



Site all · Source IP Enter variable value · Destination IP Enter variable value · Additional filters + · Active True

Traffic

Transferred bytes (total)	Traffic (peak)	Packets (peak)	Talkers (peak)	Flows (peak)
2.68 TB	4.31 Gb/s	364 kp/s	1026788	6044 f/s

Country & ASN & IP adresses

Source Country

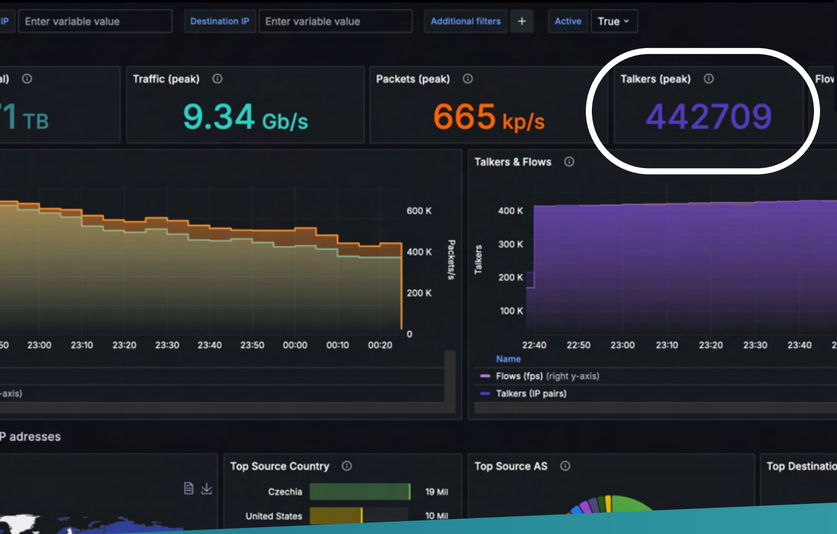
Top Source Country

Czechia	25 Mil
United States	7 Mil
Bulgaria	1 Mil
The Netherlands	577 K
Germany	306 K

Top Source AS

Top Destination AS

Before anomaly



IP Enter variable value · Destination IP Enter variable value · Additional filters + · Active True

al)	Traffic (peak)	Packets (peak)	Talkers (peak)	Flow
1 TB	9.34 Gb/s	665 kp/s	442709	5723 f/s

P adresses

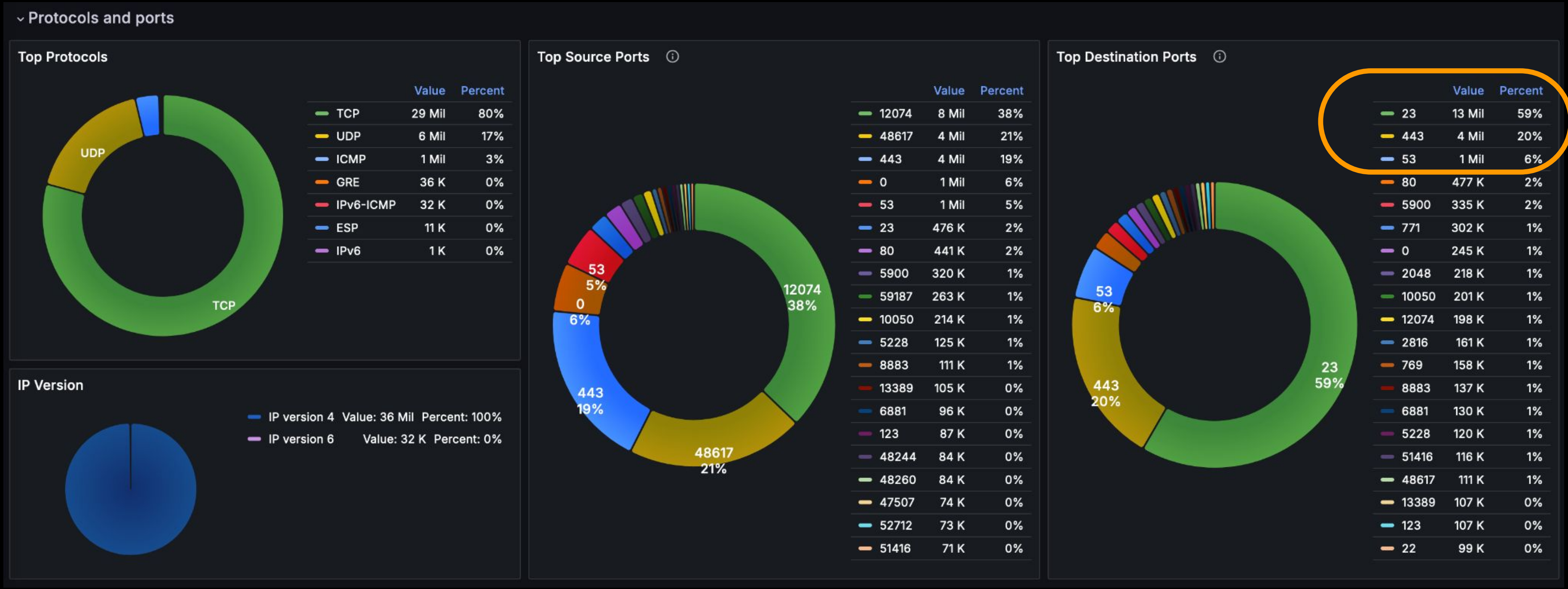
Top Source Country

Czechia	19 Mil
United States	10 Mil

Top Source AS

Top Destination AS

Anomaly on port 23



Protocols and ports

Top Protocols

	Value	Percent
TCP	29 Mil	80%
UDP	6 Mil	17%
ICMP	1 Mil	3%
GRE	36 K	0%
IPv6-ICMP	32 K	0%
ESP	11 K	0%
IPv6	1 K	0%

IP Version

IP version 4 Value: 36 Mil Percent: 100%
IP version 6 Value: 32 K Percent: 0%

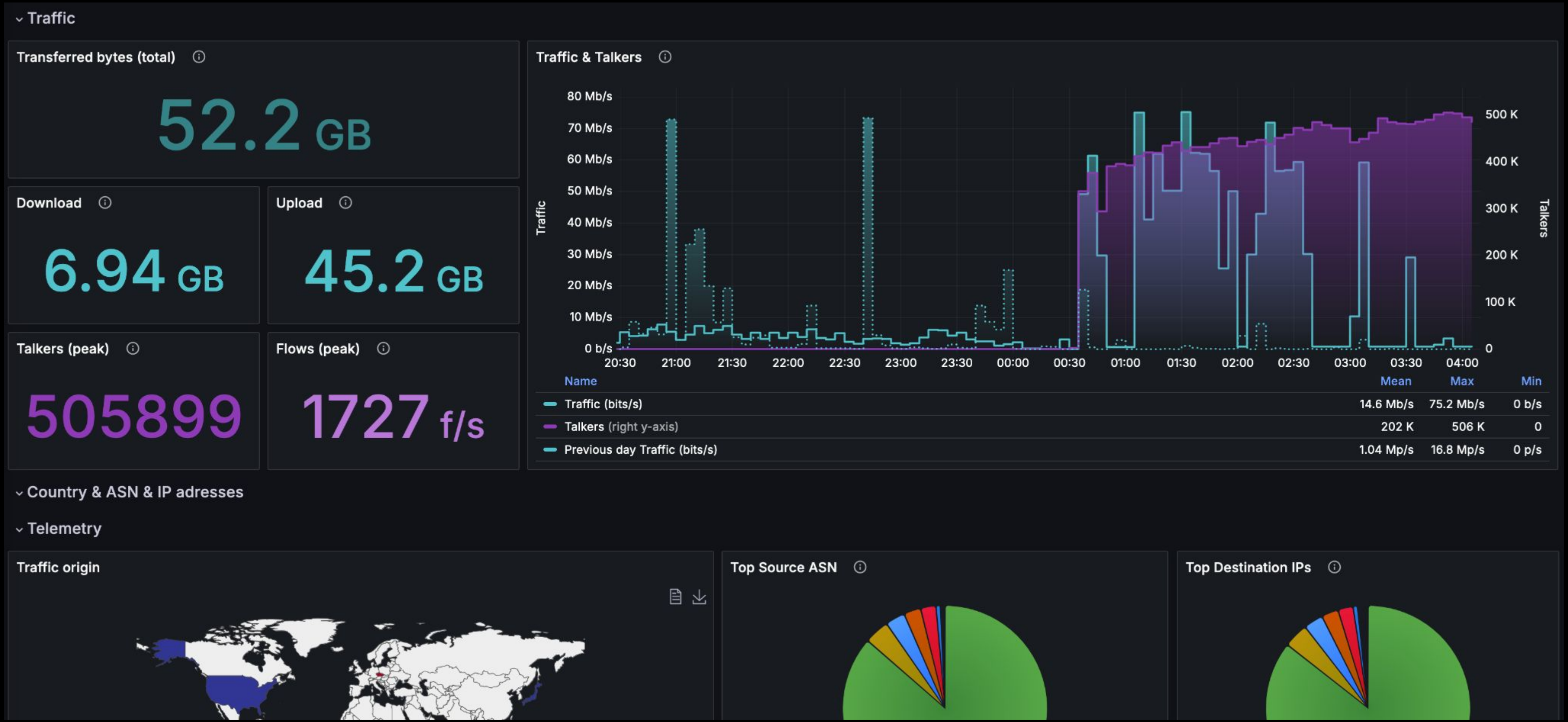
Top Source Ports

	Value	Percent
12074	8 Mil	38%
48617	4 Mil	21%
443	4 Mil	19%
0	1 Mil	6%
53	1 Mil	5%
23	476 K	2%
80	441 K	2%
5900	320 K	1%
59187	263 K	1%
10050	214 K	1%
5228	125 K	1%
8883	111 K	1%
13389	105 K	0%
6881	96 K	0%
123	87 K	0%
48244	84 K	0%
48260	84 K	0%
47507	74 K	0%
52712	73 K	0%
51416	71 K	0%

Top Destination Ports

	Value	Percent
23	13 Mil	59%
443	4 Mil	20%
53	1 Mil	6%
80	477 K	2%
5900	335 K	2%
771	302 K	1%
0	245 K	1%
2048	218 K	1%
10050	201 K	1%
12074	198 K	1%
2816	161 K	1%
769	158 K	1%
8883	137 K	1%
6881	130 K	1%
5228	120 K	1%
51416	116 K	1%
48617	111 K	1%
13389	107 K	0%
123	107 K	0%
22	99 K	0%

Single host traffic



Traffic

Transferred bytes (total)

52.2 GB

Download

6.94 GB

Upload

45.2 GB

Talkers (peak)

505899

Flows (peak)

1727 f/s

Traffic & Talkers

Name	Mean	Max	Min
Traffic (bits/s)	14.6 Mb/s	75.2 Mb/s	0 b/s
Talkers (right y-axis)	202 K	506 K	0
Previous day Traffic (bits/s)	1.04 Mp/s	16.8 Mp/s	0 p/s

Country & ASN & IP adresses

Telemetry

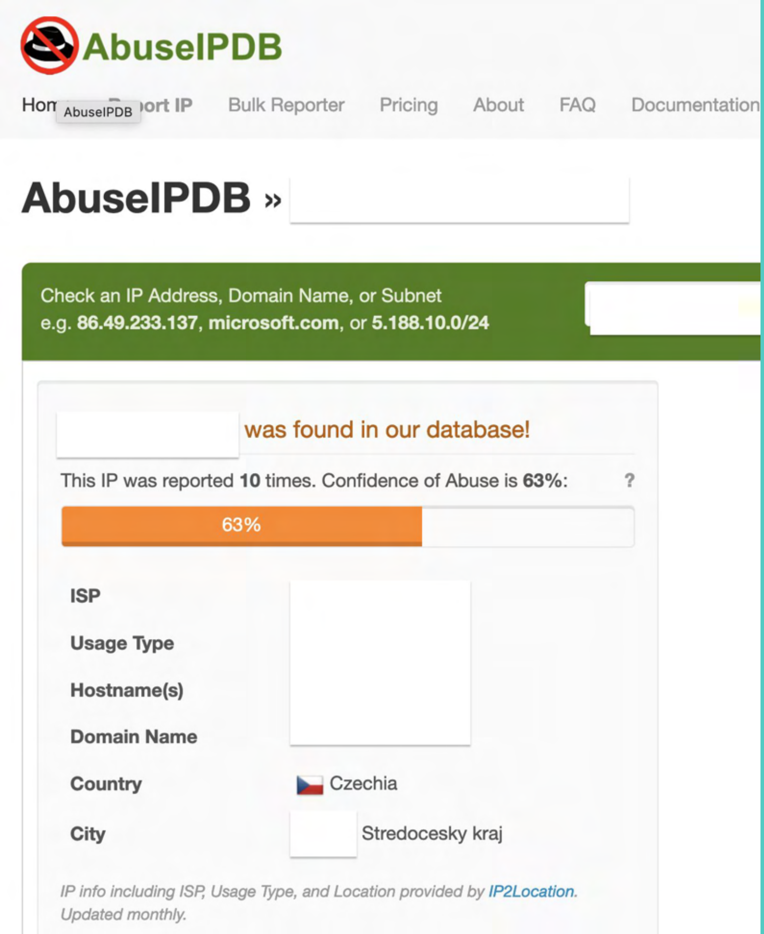
Traffic origin

Top Source ASN

Top Destination IPs

Impact

- Home camera on botnet
- IP on blacklist
- /22 IP Prefix on blacklist
- 30+ emails from ASNs
- Clean up



AbuseIPDB » [redacted]

Check an IP Address, Domain Name, or Subnet
e.g. **86.49.233.137**, **microsoft.com**, or **5.188.10.0/24**

[redacted] was found in our database!

This IP was reported **10** times. Confidence of Abuse is **63%**: ?

63%

ISP	[redacted]
Usage Type	
Hostname(s)	
Domain Name	
Country	Czechia
City	[redacted] Stredocesky kraj

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

Use cases

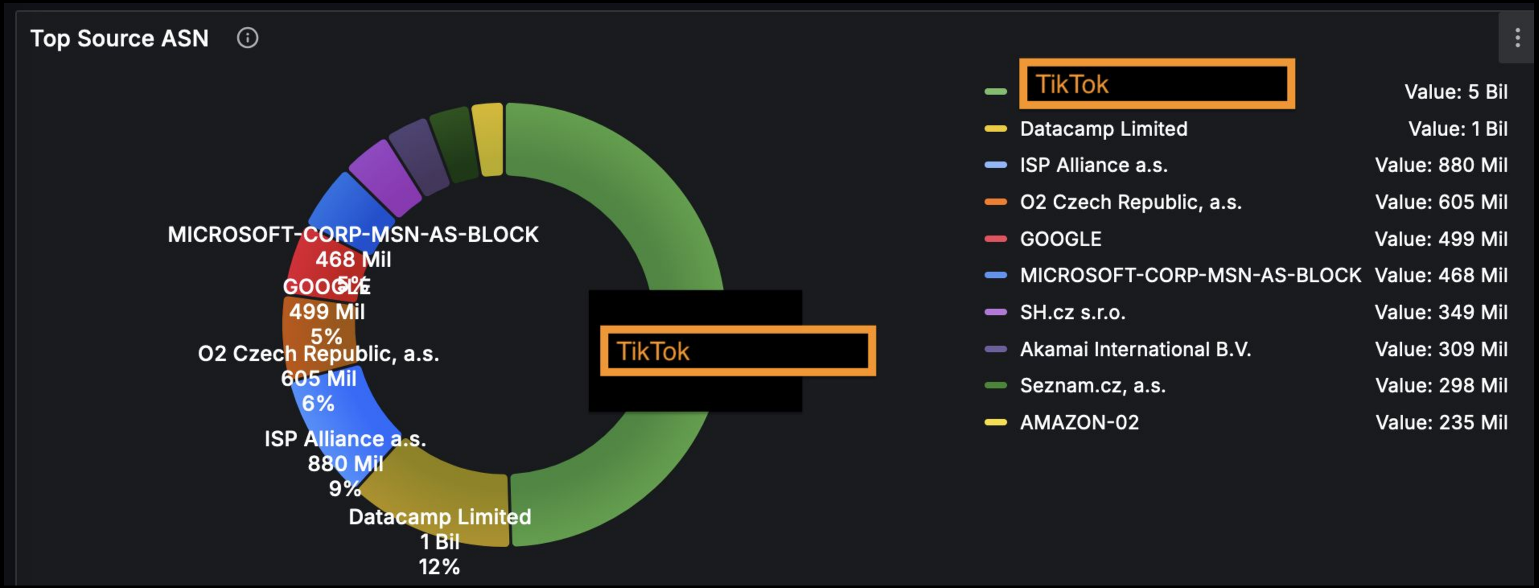
- #1 Outgoing DDoS
- #2 Hacked camera damaged /22 prefix
- #3 Hotline on steroid
- #4 Syslog
- Co si odnést

Case #3

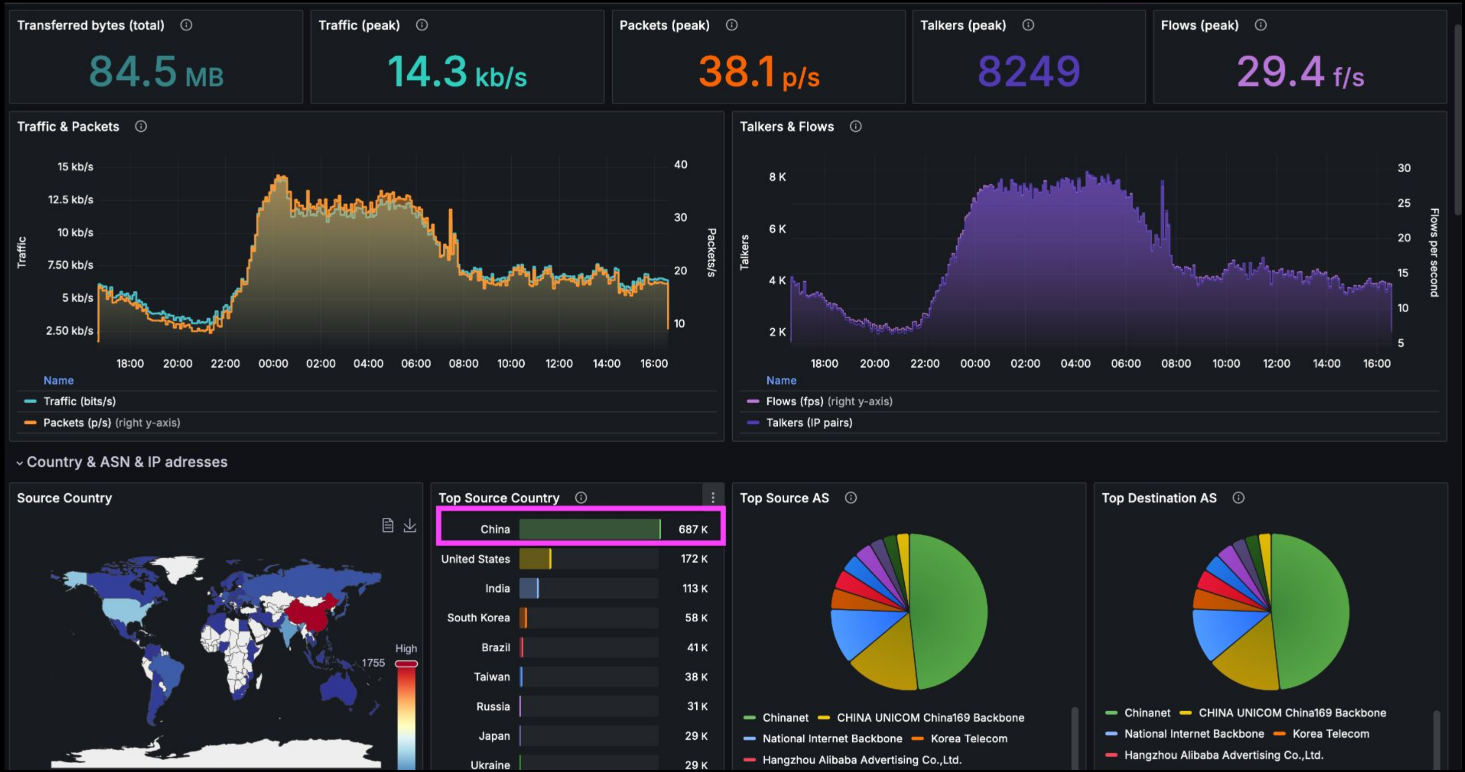
Hotline operator on steroids

FLOWCUTTER

ASN enrichment



Src/Dst Country



Transferred bytes (total) 84.5 MB

Traffic (peak) 14.3 kb/s

Packets (peak) 38.1 p/s

Talkers (peak) 8249

Flows (peak) 29.4 f/s

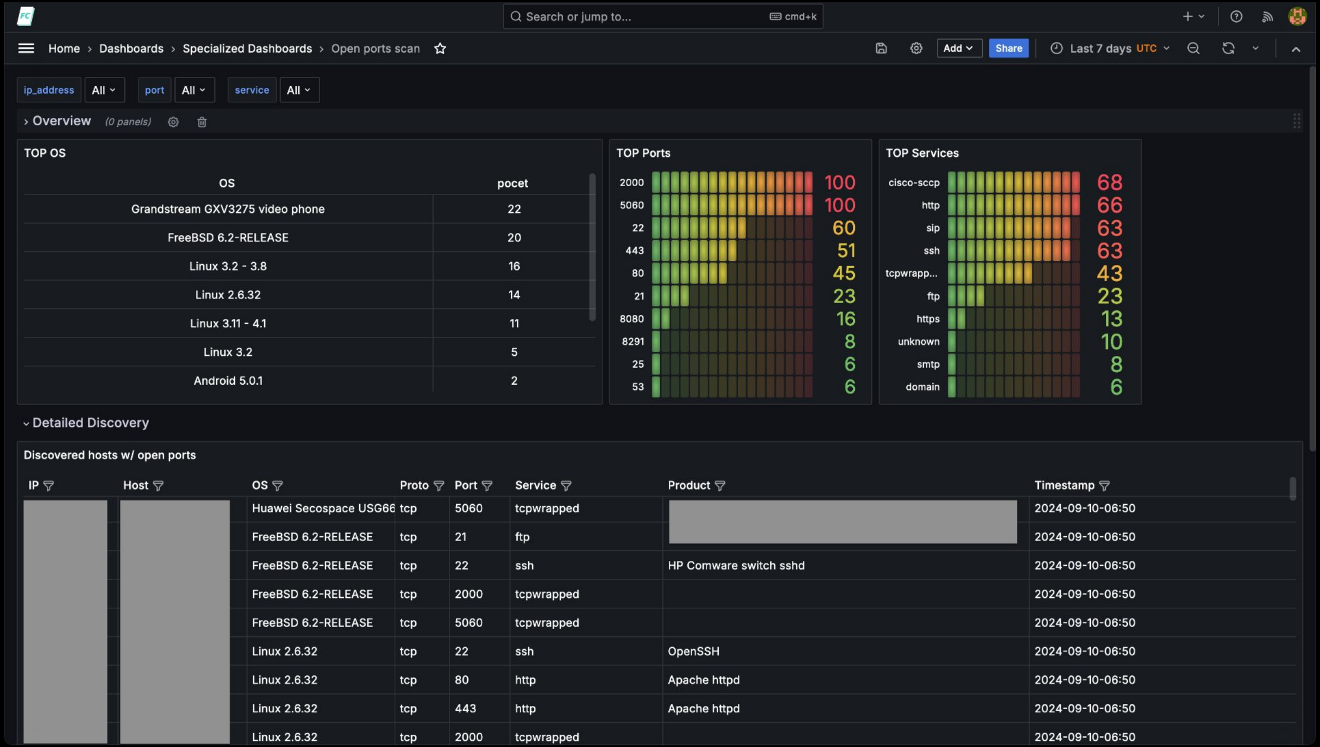
Country & ASN & IP adresses

Top Source Country

China	687 K
United States	172 K
India	113 K
South Korea	58 K
Brazil	41 K
Taiwan	38 K
Russia	31 K
Japan	29 K
Ukraine	29 K

Top Source AS
Chinanet
CHINA UNICOM China169 Backbone
National Internet Backbone
Korea Telecom
Hangzhou Alibaba Advertising Co.,Ltd.
Top Destination AS
Chinanet
CHINA UNICOM China169 Backbone
National Internet Backbone
Korea Telecom
Hangzhou Alibaba Advertising Co.,Ltd.

Open ports



Home › Dashboards › Specialized Dashboards › Open ports scan

Last 7 days UTC

ip_address All · port All · service All

› Overview (0 panels)

TOP OS

OS	pocet
Grandstream GXV3275 video phone	22
FreeBSD 6.2-RELEASE	20
Linux 3.2 - 3.8	16
Linux 2.6.32	14
Linux 3.11 - 4.1	11
Linux 3.2	5
Android 5.0.1	2

TOP Ports

2000	100
5060	100
22	60
443	51
80	45
21	23
8080	16
8291	8
25	6
53	6

TOP Services

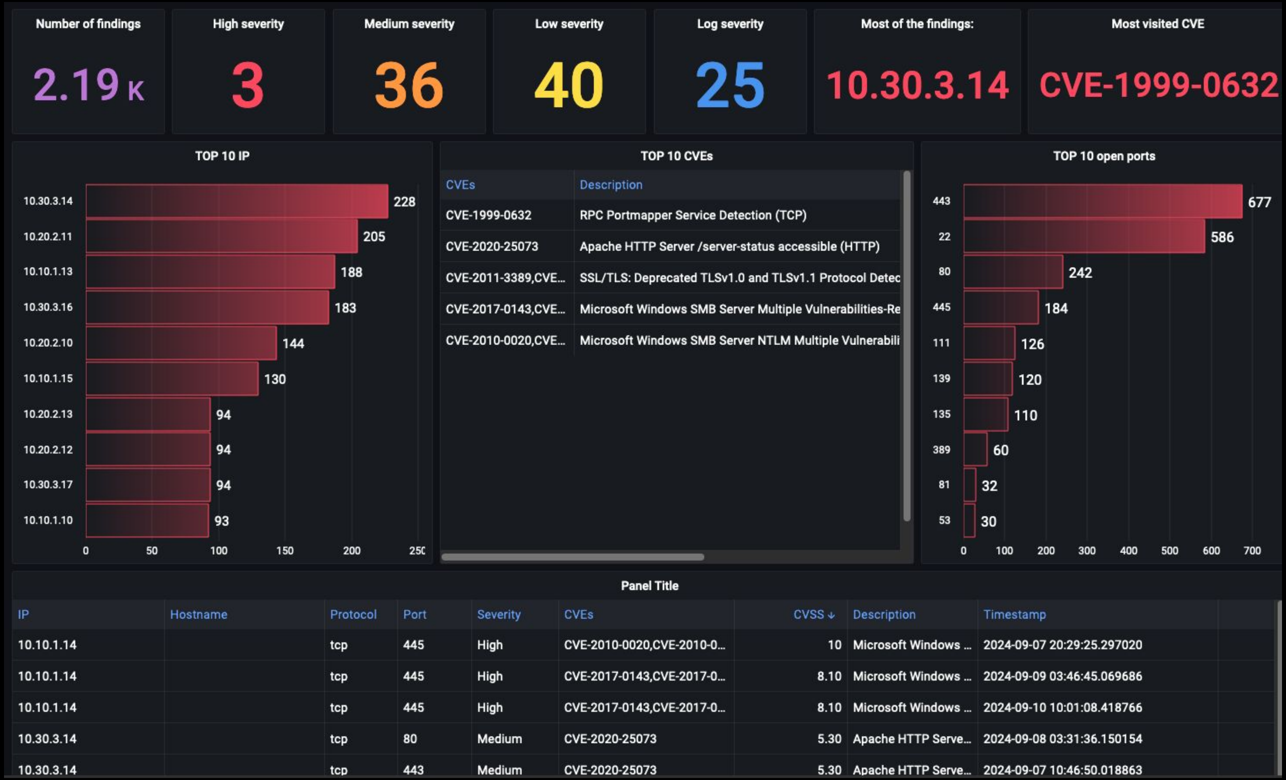
cisco-sccp	68
http	66
sip	63
ssh	63
tcpwrapp...	43
ftp	23
https	13
unknown	10
smtp	8
domain	6

⌄ Detailed Discovery

Discovered hosts w/ open ports

IP	Host	OS	Proto	Port	Service	Product	Timestamp
[redacted]	[redacted]	Huawei Secospace USG66	tcp	5060	tcpwrapped	[redacted]	2024-09-10-06:50
[redacted]	[redacted]	FreeBSD 6.2-RELEASE	tcp	21	ftp	[redacted]	2024-09-10-06:50
[redacted]	[redacted]	FreeBSD 6.2-RELEASE	tcp	22	ssh	HP Comware switch sshd	2024-09-10-06:50
[redacted]	[redacted]	FreeBSD 6.2-RELEASE	tcp	2000	tcpwrapped		2024-09-10-06:50
[redacted]	[redacted]	FreeBSD 6.2-RELEASE	tcp	5060	tcpwrapped		2024-09-10-06:50
[redacted]	[redacted]	Linux 2.6.32	tcp	22	ssh	OpenSSH	2024-09-10-06:50
[redacted]	[redacted]	Linux 2.6.32	tcp	80	http	Apache httpd	2024-09-10-06:50
[redacted]	[redacted]	Linux 2.6.32	tcp	443	http	Apache httpd	2024-09-10-06:50
[redacted]	[redacted]	Linux 2.6.32	tcp	2000	tcpwrapped		2024-09-10-06:50

Vulnerabilities



Number of findings	High severity	Medium severity	Low severity	Log severity	Most of the findings:	Most visited CVE
2.19 K	3	36	40	25	10.30.3.14	CVE-1999-0632

TOP 10 IP

TOP 10 CVEs

CVEs	Description
CVE-1999-0632	RPC Portmapper Service Detection (TCP)
CVE-2020-25073	Apache HTTP Server /server-status accessible (HTTP)
CVE-2011-3389,CVE...	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detec
CVE-2017-0143,CVE...	Microsoft Windows SMB Server Multiple Vulnerabilities-Re
CVE-2010-0020,CVE...	Microsoft Windows SMB Server NTLM Multiple Vulnerabili

TOP 10 open ports

Panel Title

IP	Hostname	Protocol	Port	Severity	CVEs	CVSS ↓	Description	Timestamp
10.10.1.14		tcp	445	High	CVE-2010-0020,CVE-2010-0...	10	Microsoft Windows ...	2024-09-07 20:29:25.297020
10.10.1.14		tcp	445	High	CVE-2017-0143,CVE-2017-0...	8.10	Microsoft Windows ...	2024-09-09 03:46:45.069686
10.10.1.14		tcp	445	High	CVE-2017-0143,CVE-2017-0...	8.10	Microsoft Windows ...	2024-09-10 10:01:08.418766
10.30.3.14		tcp	80	Medium	CVE-2020-25073	5.30	Apache HTTP Serve...	2024-09-08 03:31:36.150154
10.30.3.14		tcp	443	Medium	CVE-2020-25073	5.30	Apache HTTP Serve...	2024-09-07 10:46:50.018863

Benefits

- ISP was able to quickly respond to customer complaints on hotline
- Technical support can easily rule out operator’s fault
- In some case junior support person can answer

Risks

- Spending valuable time of technical stuff on trivial issues
- Not being able to prove SLA to enterprise clients

Use cases

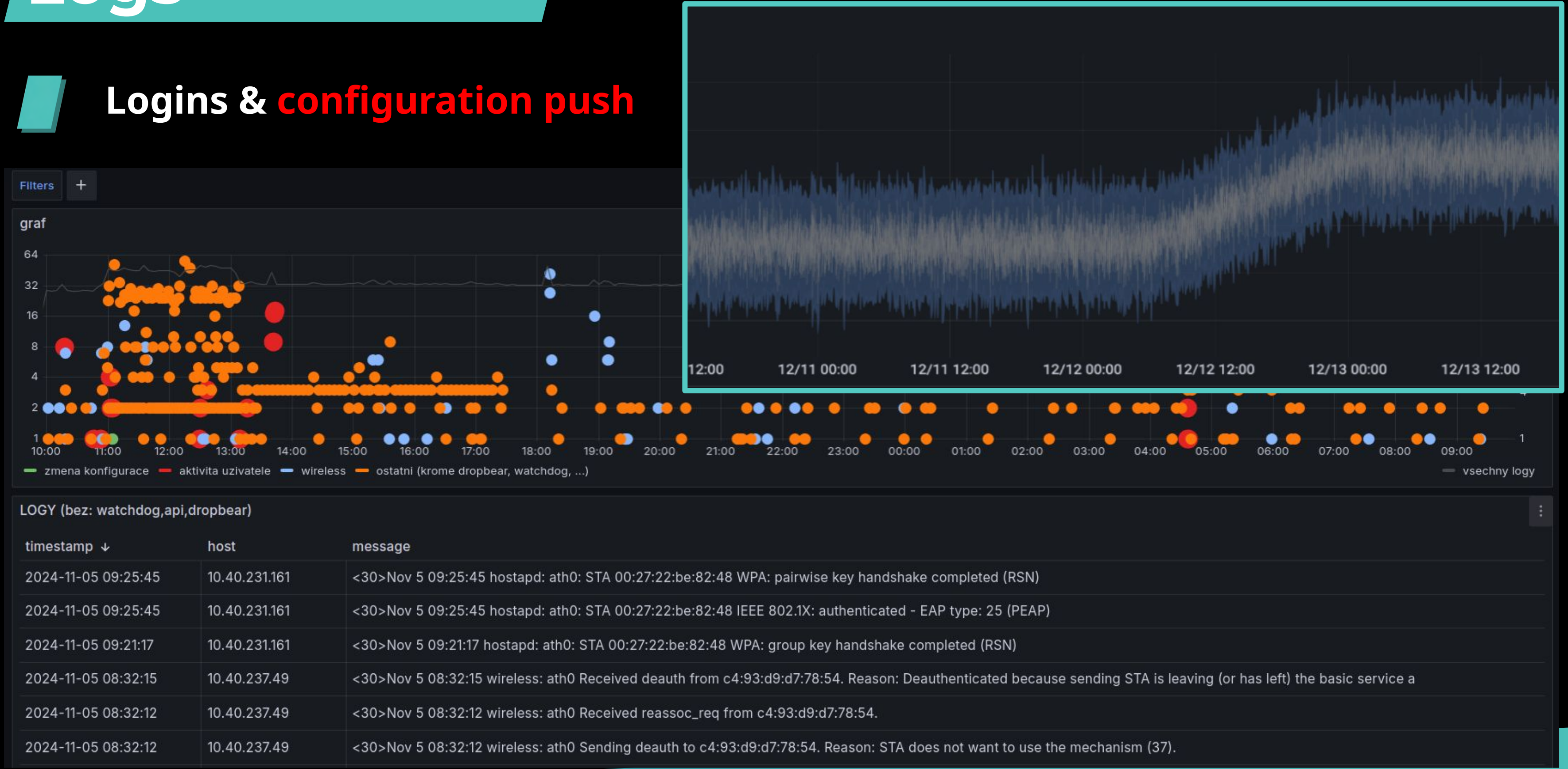
- #1 Outgoing DDoS
- #2 Hacked camera damaged /22 prefix
- #3 Hotline on steroid
- #4 Syslog
- Co si odnést

Case #4

Syslog for troubleshooting

Logs

Logins & configuration push



LOGY (bez: watchdog,api,dropbear)

timestamp ↓	host	message
2024-11-05 09:25:45	10.40.231.161	<30>Nov 5 09:25:45 hostapd: ath0: STA 00:27:22:be:82:48 WPA: pairwise key handshake completed (RSN)
2024-11-05 09:25:45	10.40.231.161	<30>Nov 5 09:25:45 hostapd: ath0: STA 00:27:22:be:82:48 IEEE 802.1X: authenticated - EAP type: 25 (PEAP)
2024-11-05 09:21:17	10.40.231.161	<30>Nov 5 09:21:17 hostapd: ath0: STA 00:27:22:be:82:48 WPA: group key handshake completed (RSN)
2024-11-05 08:32:15	10.40.237.49	<30>Nov 5 08:32:15 wireless: ath0 Received deauth from c4:93:d9:d7:78:54. Reason: Deauthenticated because sending STA is leaving (or has left) the basic service a
2024-11-05 08:32:12	10.40.237.49	<30>Nov 5 08:32:12 wireless: ath0 Received reassoc_req from c4:93:d9:d7:78:54.
2024-11-05 08:32:12	10.40.237.49	<30>Nov 5 08:32:12 wireless: ath0 Sending deauth to c4:93:d9:d7:78:54. Reason: STA does not want to use the mechanism (37).

Use cases

- #1 Outgoing DDoS
- #2 Hacked camera damaged /22 prefix
- #3 Hotline on steroid
- #4 Syslog
- Co si odnést

Shrnutí

Závěr

- Čas techniků je drahý
- Troubleshooting je na problémy,

  kt je levnější řešit hned a nečekat na důsledky
- ???
- ???

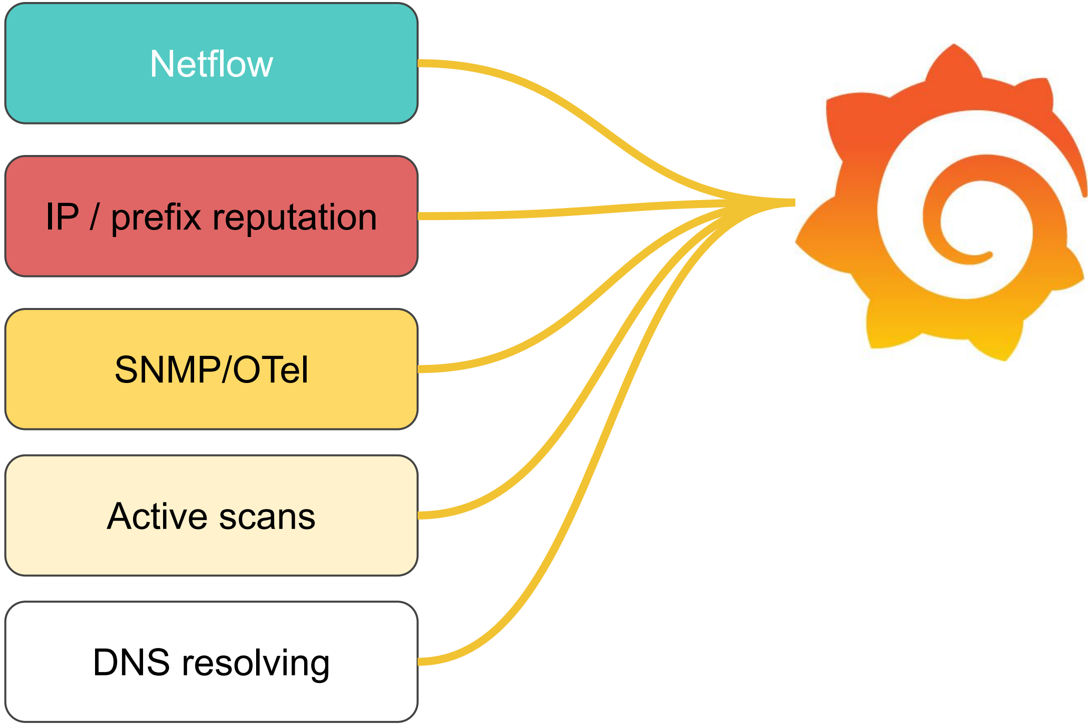
Závěr

- Čas techniků je drahý
- Troubleshooting je na problémy,

  kt je levnější řešit hned a nečekat na důsledky
- Používejte více zdrojů dat, vč netflow
- ???

Correlate multiple data sources

- Technici
- Nástroje
- **Zdroje dat**
- Orchestra



Netflow

IP / prefix reputation

SNMP/OTel

Active scans

DNS resolving

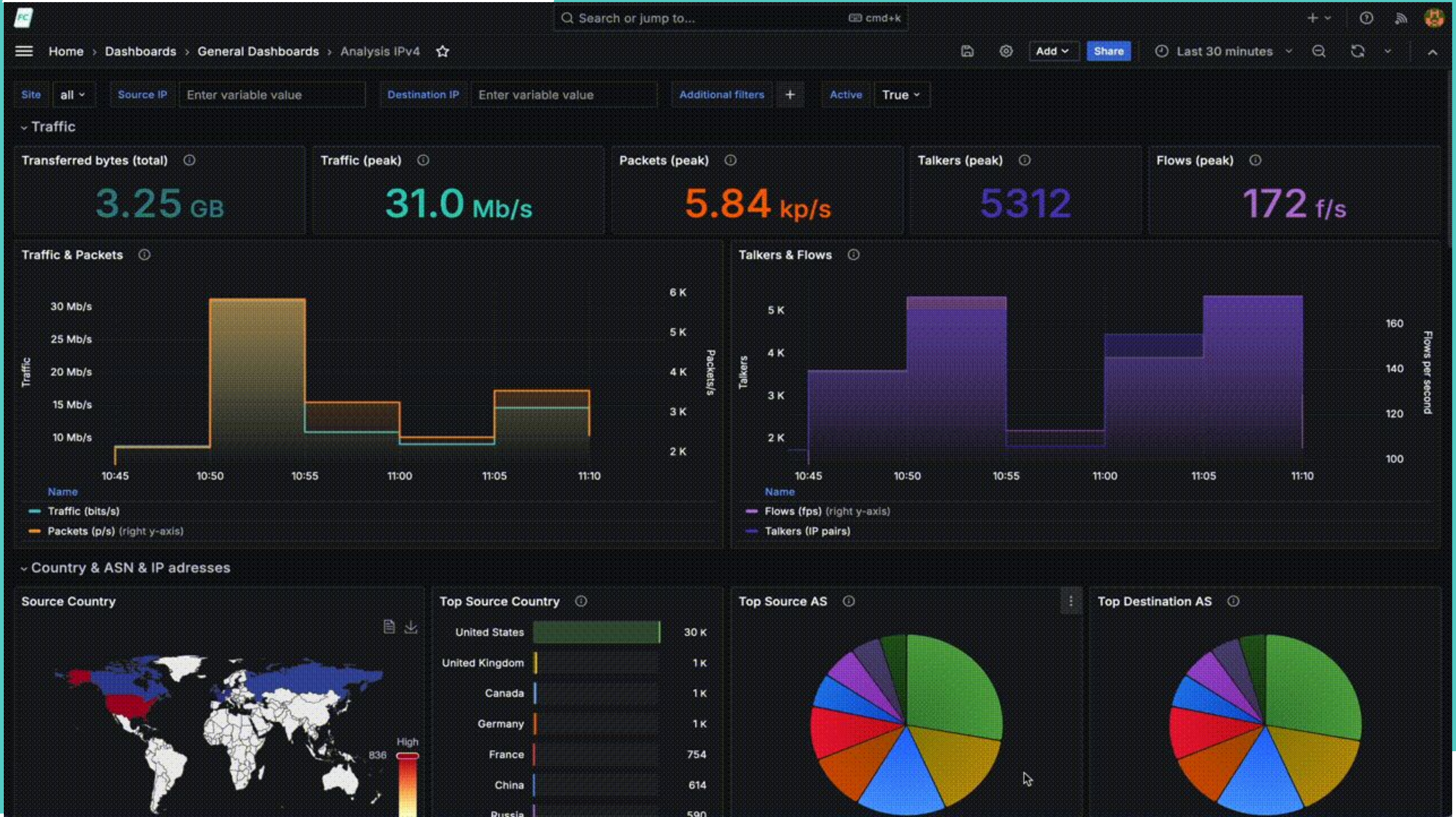
Závěr

- Čas techniků je drahý
- Troubleshooting je na problémy,

  kt je levnější řešit hned a nečekat na důsledky
- Používejte více zdrojů dat, vč netflow
- Používejte ⬡ kt jsou efektivní

Ad hoc queries

https://www.youtube.com/watch?v=cycMnXpbIpU



Transferred bytes (total): 3.25 GB

Traffic (peak): 31.0 Mb/s

Packets (peak): 5.84 kp/s

Talkers (peak): 5312

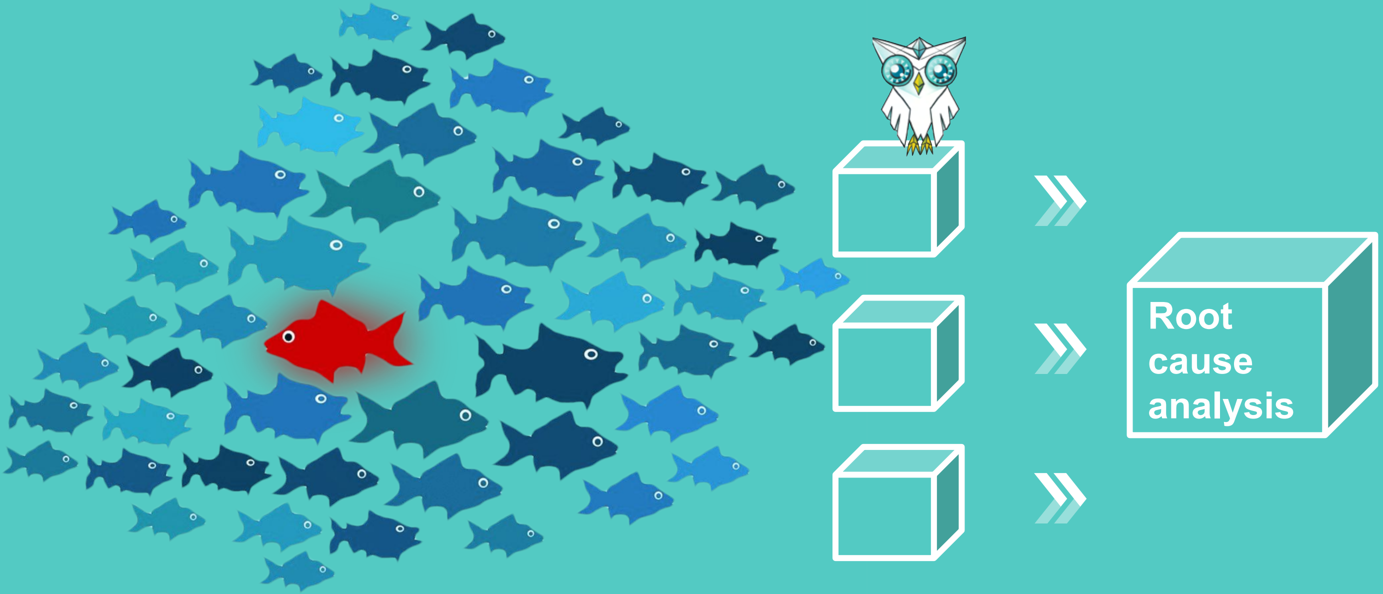
Flows (peak): 172 f/s

Top Source Country

United States	30 K
United Kingdom	1 K
Canada	1 K
Germany	1 K
France	754
China	614
Russia	590

Photo from thedatascientist.com/

Děkuji



Root cause analysis

FLOWCUTTER