

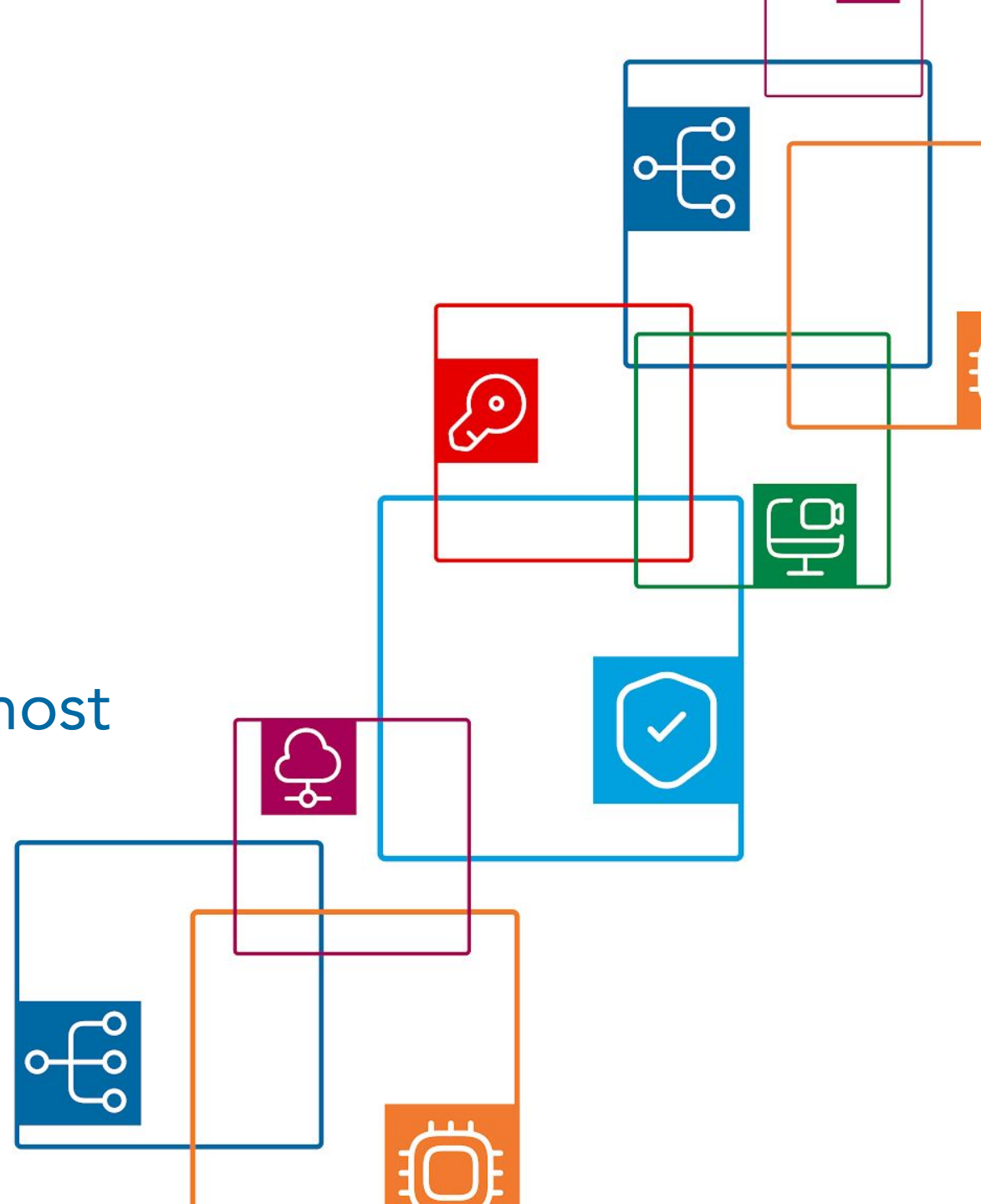


Výzkum a vývoj pro kyberbezpečnost

Tomáš Čejka,
oddělení nástrojů pro administraci a bezpečnost

Konference e-infrastruktury CESNET

30.9.-1.10.2026, Praha



- Monitorování a detekce

- Výzkum HW akcelerace
 - architektury pro SmartNIC a FPGA (viz stánek, "800G demo")
- FW, SW
- algoritmy

- Obrana

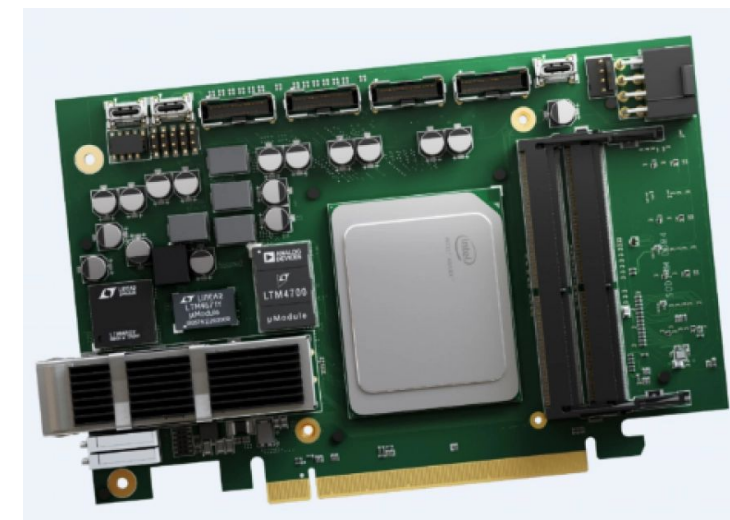
- DDoS obrana
 - 400G filtrace na komoditním HW (viz stánek, "DDoS Protector")
- NERD

- Bezpečná konfigurace

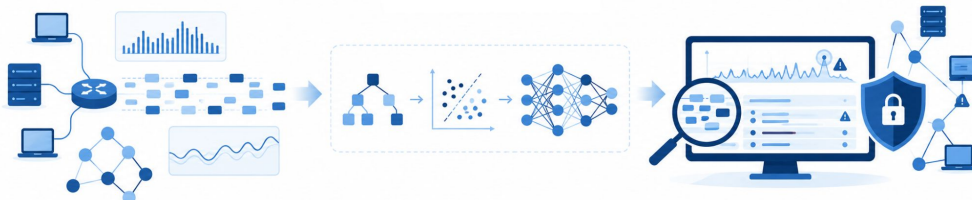
- viz prezentace Adam Piecek: "NETCONF: ovládněte svá síťová zařízení", 1.10.2026 sekce bezpečnost, od 13h



- FPGA FW pro zpracování vysokorychlostního provozu (400 Gb/s)
- Monitorovací infrastruktura
 - sonda **ipfixprobe** (monitorování na 400 Gb/s linkách)
 - kolektor **IPFIXcol2**
 - analýza, detekce
- Detektor IoC
- NERD (Network Entity Reputation Database)



- Návrh a realizace architektur pro FPGA
- Strojové učení pro klasifikaci a rozpoznávání síťového provozu
 - od jednoduchých algoritmů až po DeepLearning
 - representation learning - výzkum podobnosti provozu
- Využití velkých jazykových modelů
 - interpretace výsledků
 - usnadnění analýzy a vyhledávání
 - asistent nad dokumentací a znalostní bází



- Vědecké publikace na specializovaných konferencích, články prestižních časopisech (1. kvartil / 1. decil)
- Zveřejňování datových sad



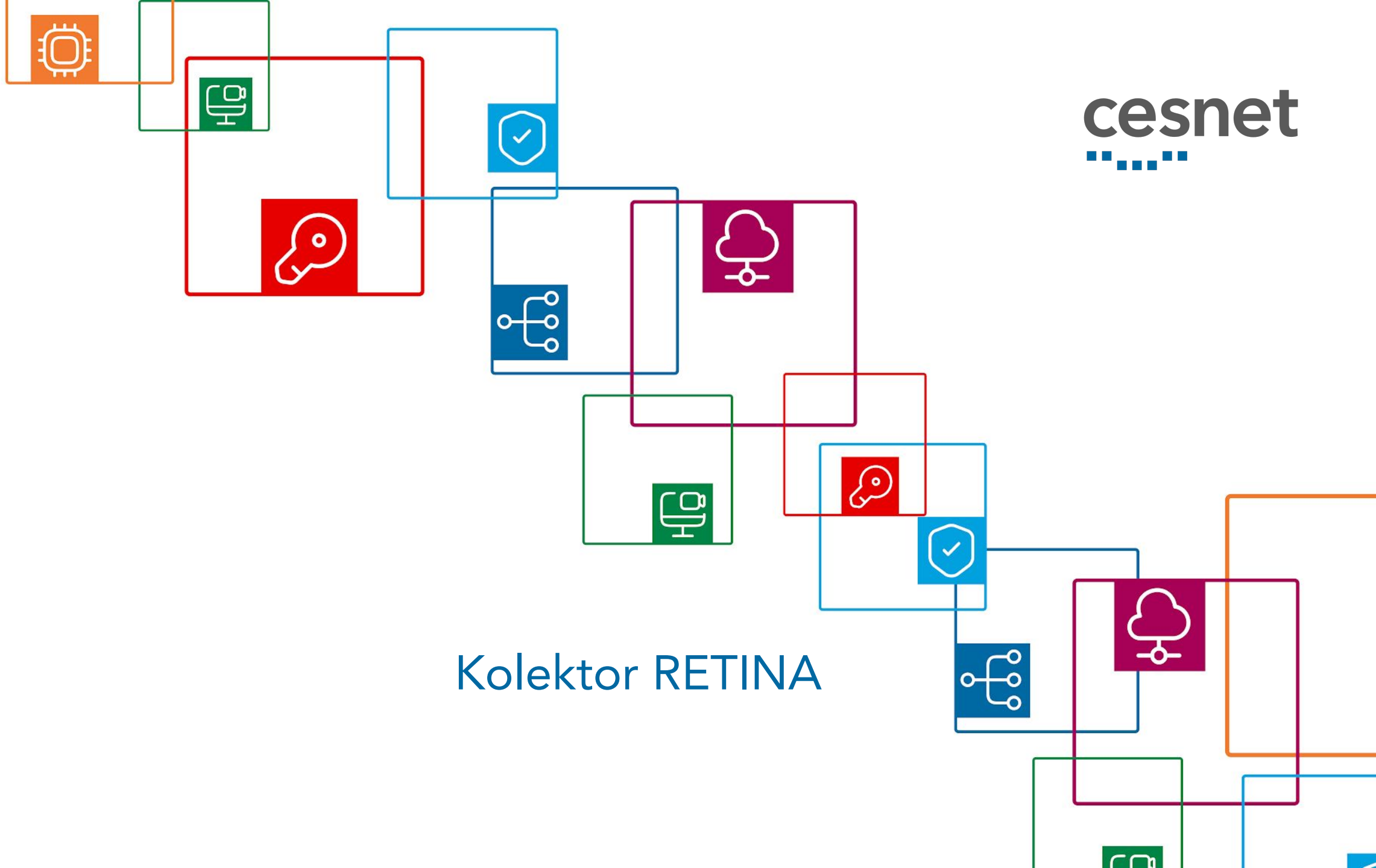
CESNET DataZoo

Důležitá zpětná vazba celosvětové vědecké komunity,
recenzní řízení!

- pracujeme na tématech, která jsou skutečně inovativní
- jsme v tom velmi úspěšní

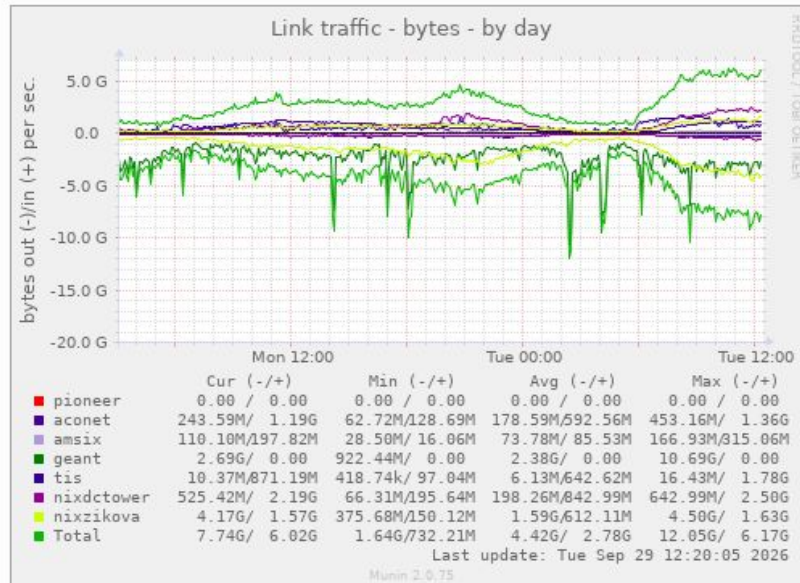


Kolektor RETINA

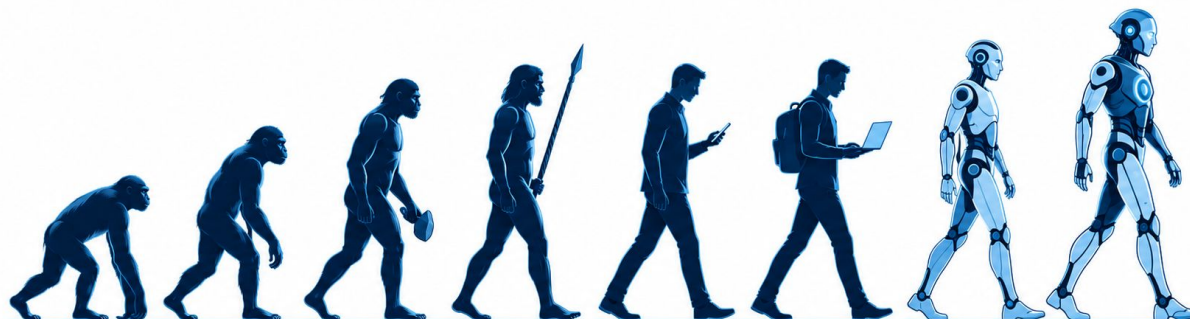
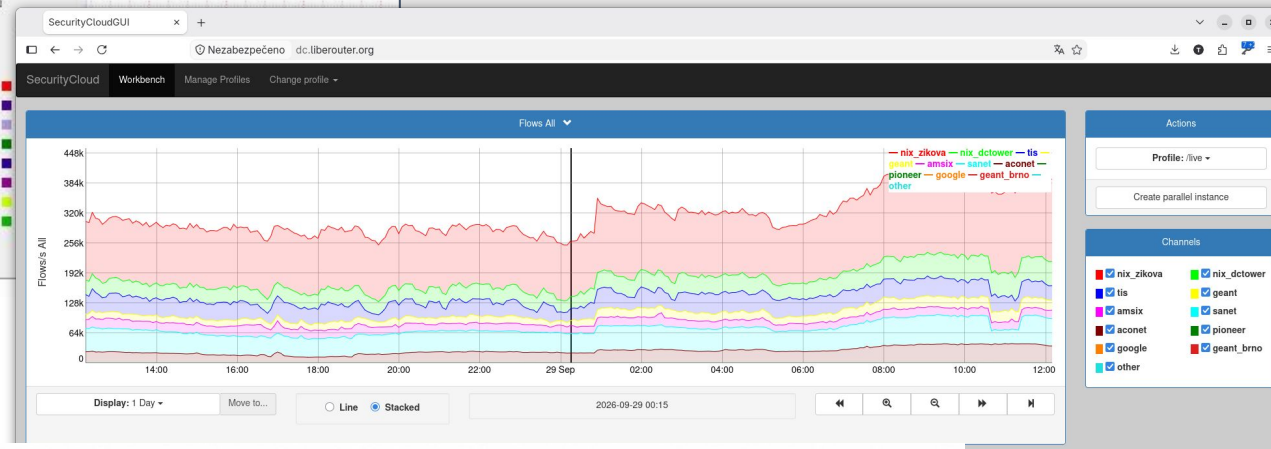


traffic-monitoring

Link traffic - bytes



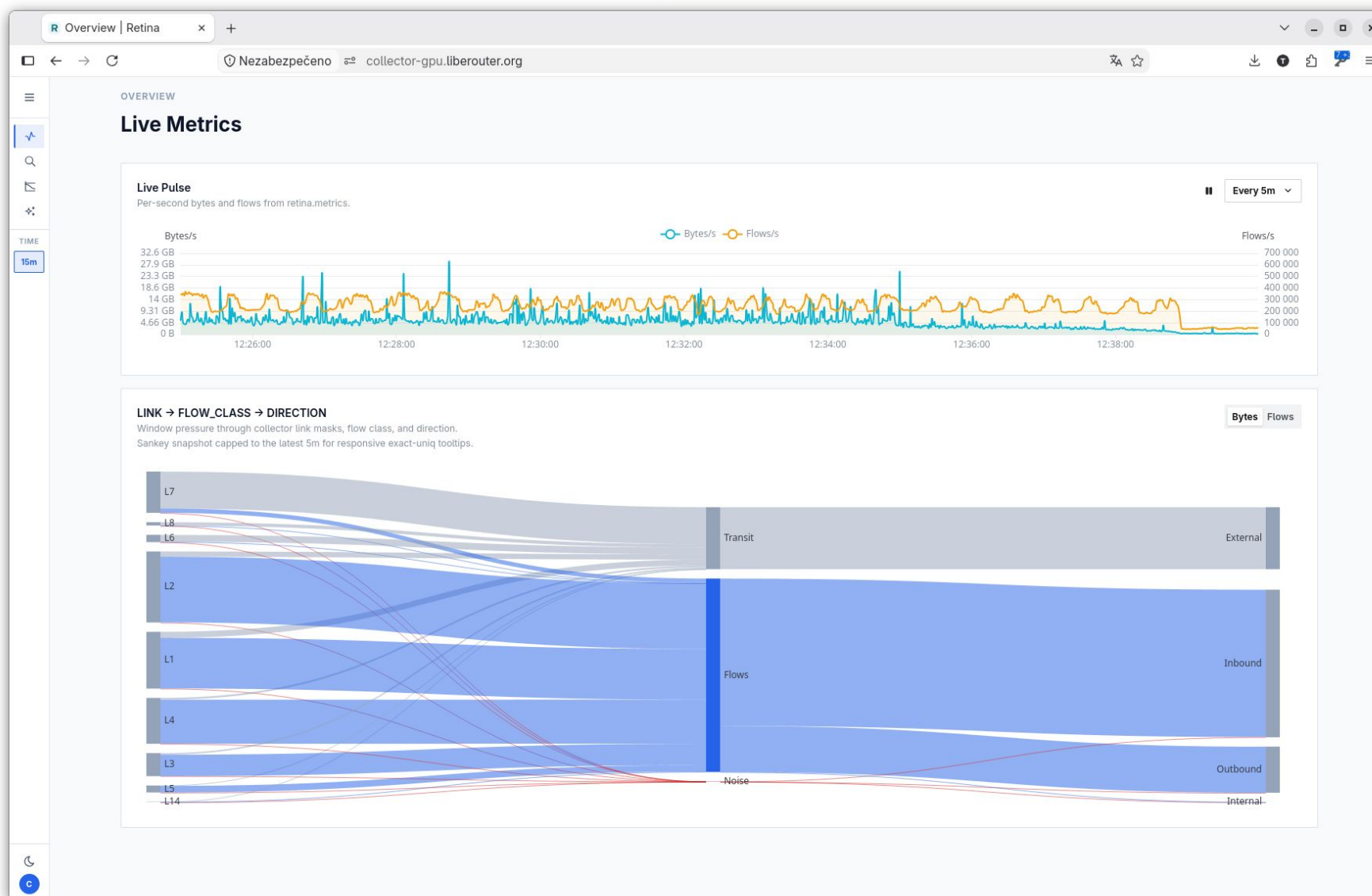
```
fdistdump-ha live/channels/nix_zikova live/channels/nix_dctower
live/channels/tis live/channels/geant live/channels/amsix
live/channels/sanet live/channels/aconet live/channels/pioneer
live/channels/google live/channels/geant_bрно
live/channels/other /usr/lib64/mpich/bin/mpirun
/usr/lib64/mpich/bin/fdistdump_mprun --num-threads 8
--output-rich-header -f 'ip 195.113.171.1 and proto tcp' -t
1790633700 -l 10 --output-format=pretty
--output-volume-conv=metric-prefix --output-items=r,p
--time-zone="Europe/Prague"
```

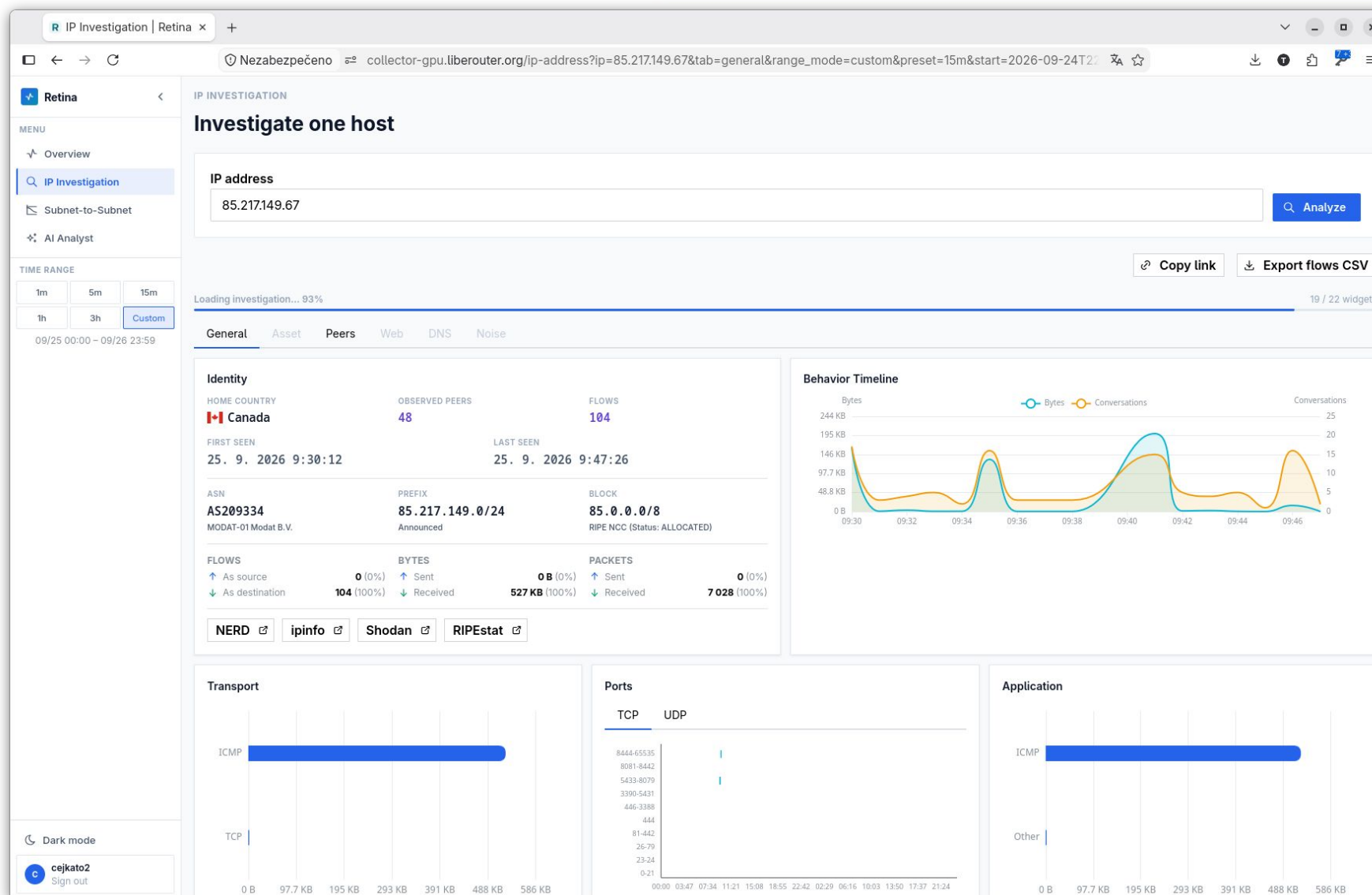




- Nová generace kolektoru!
- ClickHouse + analýza&detekce + dlouholetá expertíza
- Využití velkých jazykových modelů (LLM)
- Využití AI agentů
- Pomocník pro analytiky a bezpečnostní týmy







IP Investigation | Retina

Nezabezpečeno collector-gpu.liberouter.org/ip-address?ip=78.128.222.165&tab=asset&range_mode=preset&preset=3h

Retina

MENU

Overview

IP Investigation

Subnet-to-Subnet

AI Analyst

TIME RANGE

1m

5m

15m

1h

3h

Custom

IP INVESTIGATION

Investigate one host

IP address

78.128.222.165

Analyze

Copy link

Export flows CSV

General

Asset

Peers

Web

DNS

Noise

Asset identity

Badges cover the last 7 days, the tiles the selected range. Shares are evidence shares, not confidence; the role reads in hours held.

DEVICE WORKSTATION/SERVER · 100 %

OS LINUX · 52 %

TUNNEL SSA · 67 %

Flows

832

Bytes

5.39 MB

Distinct peers

88

Hours observed

3

rollup hours in range

First seen

29. 9. 2026 9:06:51

Last seen

29. 9. 2026 12:03:18

Asset timeline

One cell per hour over the selected range. Roles and the NAT hint are per-hour verdicts; OS family is the hour's dominant label; signal lanes mark windows.

Activity flows/h

OS family dominant

Activity (darker = more flows)

OS: Linux

empty cell = no evidence that hour

Classification

One row per dimension: the winning label, its evidence share, what else was seen, and which rollup arms feed it.

DIMENSION	VERDICT	SHARE · OBS	ALSO SEEN	SOURCE
Device type	Workstation/Server	28 obs 100 %	—	names · User-Agent · ports
OS family	Linux	45 obs 100 %	—	names · User-Agent · banner
OS label	Linux	28 obs 62 %	Fedora 38 %	names · User-Agent · banner

Services

What this asset serves. Payload rows are proven by the reply the asset sends back; src-port rows come from the port table and are marked as such.

SERVICE	SHARE · OBS	SOURCE
http	39 obs 95 %	PAYLOAD
tls	2 obs 5 %	PAYLOAD

Listen ports

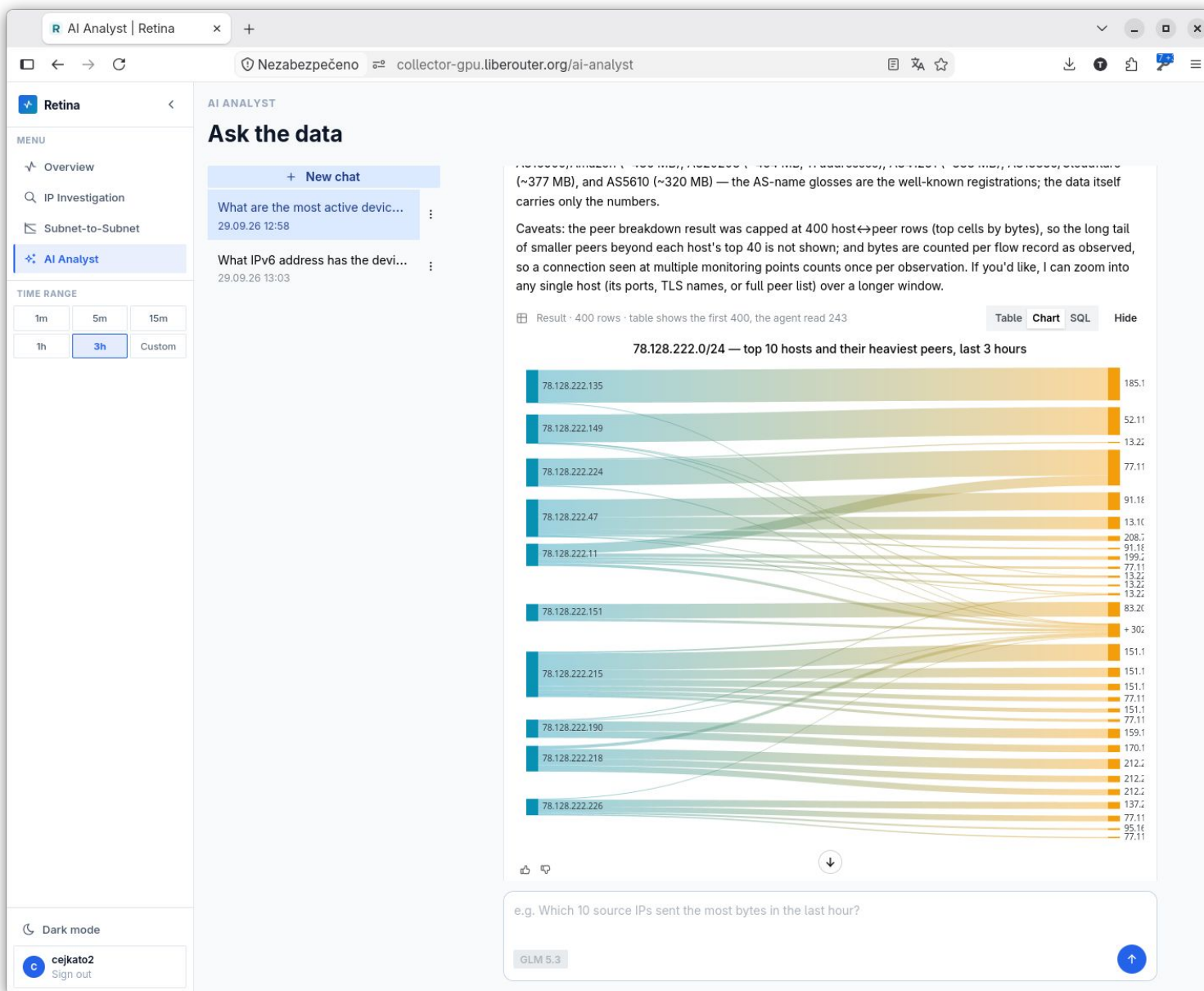
19 · 22 · 53 · 80 · 123 · 443 · 500 · 623 · 873 · 1015 · 1434 · 1645 · 2059 · 2152 · 2361 · 3391 · 3445 · 3702 · 4488 · 5060 · 5351 · 5353 · 5683 · 10074 · 10161 · 11211 · 12438 · 12646 · 15446 · 17185 · 18216 · 33031 · 33106 · 33152 · 33254 · 33548 · 34038 · 34044 · 34046 · 34054 · 34208 · 34222 · 34308 · 34370 · 34460 · 34500 · 34582 · 34616 · 34777 · 34825 · 35201 · 35300 · 35328 · 35774 · 35806 · 36056 · 36066 · 36090 · 36184 · 36372 · 36378 · 36658 · 36674 · 36824

Client ports

32843 · 33006 · 33031 · 33085 · 33106 · 33152 · 33164 · 33184 · 33227 · 33348 · 33534

Dark mode

cejkato2 Sign out



"What are the most active devices in 78.128.222.0/24 and with whom do they communicate?"



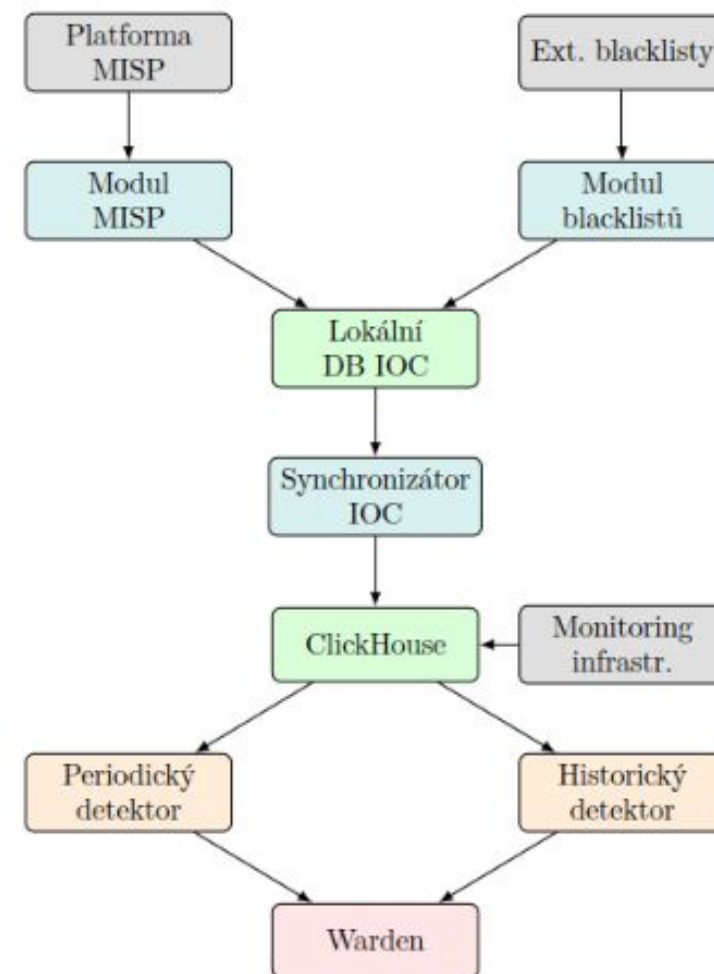
1. Viz prezentace v sekci Bezpečnost — Jaroslav Pešek!
Zítra 1.10. 2026 od 9:45
“AI a bezpečnostní monitoring - kolektor RETINA”
2. Dále viz stánek!
3. Více na semináři BSS 2027 → plánujeme workshop!



Detekce IoC na perimetru

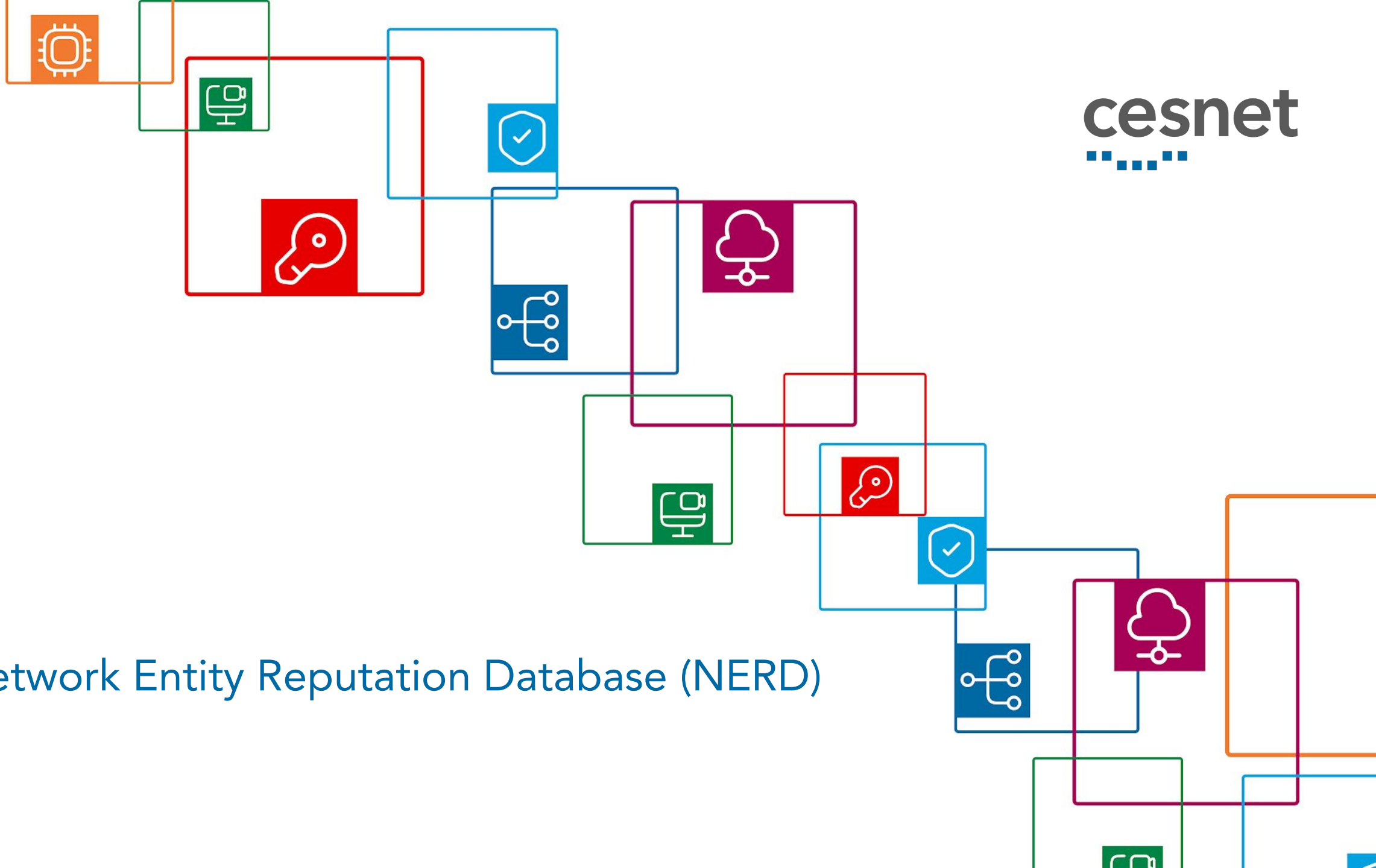


- Sběr IOCs (IP, IP:port, domain, URL) z MISP a blacklistů
- Detekce nad rozšířenými flow daty na perimetru
 - využití vlastních sond / kolektoru
 - hlášení detekovaných podezřelých událostí do Wardenu





Network Entity Reputation Database (NERD)



IP search - Network Enti x

nerd.cesnet.cz/nerd/ips

Timezone: local

Log in using: Local account EduGAIN

Search IP addresses by ...

Criteria Match

List of IPs

IP prefix

Hostname suffix

ASN

Country

a.b.c.d/x

.example.org

ASxxx

Any

Source

Event category

Blacklist

Tag

Any

Any

Any

Any

Threat category

Role

Category

Subcategory

Confidence

Any

Any

--

=

0.5

Sorting options

Sort by

Order

Max. number of addresses

Reputation score

DESC ASC

20

SEARCH

Results (220)

Download as csv

- Automatické zpracování bezp. událostí (z Wardenu)
- Sběr relevantních informací z OSINT
- Modelování "reputace" IP adres
- Historie škodlivých/podezřelých adres





NERD2

IP Addresses Domains URLs IP:ports Glossary

UTC Local

NERD2

Network Entity Reputation Database

Q IP address or prefix Search →

Browse all indexed IPs →

EXAMPLE QUERIES

IPv4 addresses

85.217.149.67 117.89.254.46 176.65.134.121 3.147.122.184

IPv6 addresses

2602:f71d:200::30

IPv6/64 prefixes

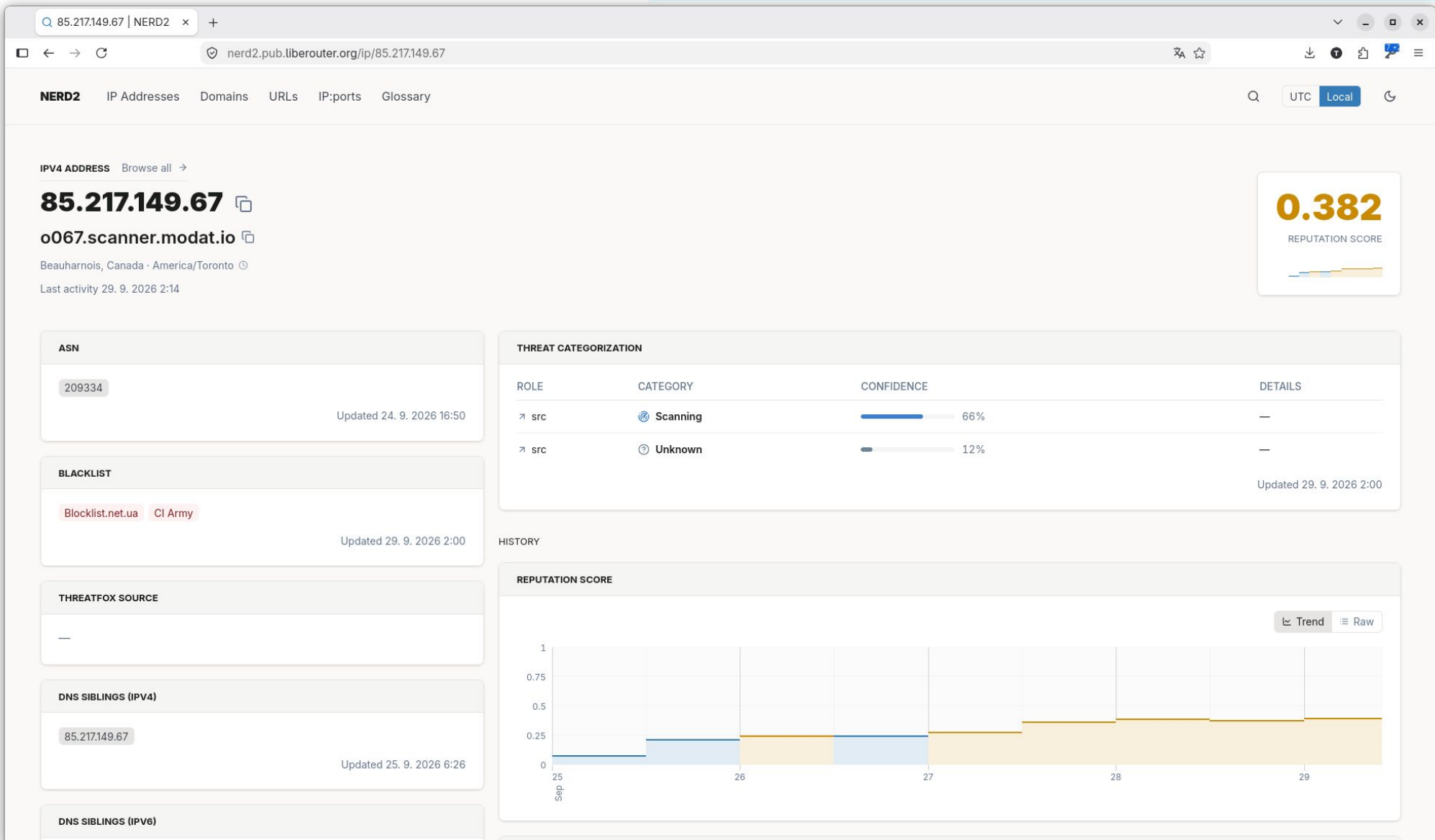
2607:ff10:c8:594::/64 2001:41d0:33a:a00::/64

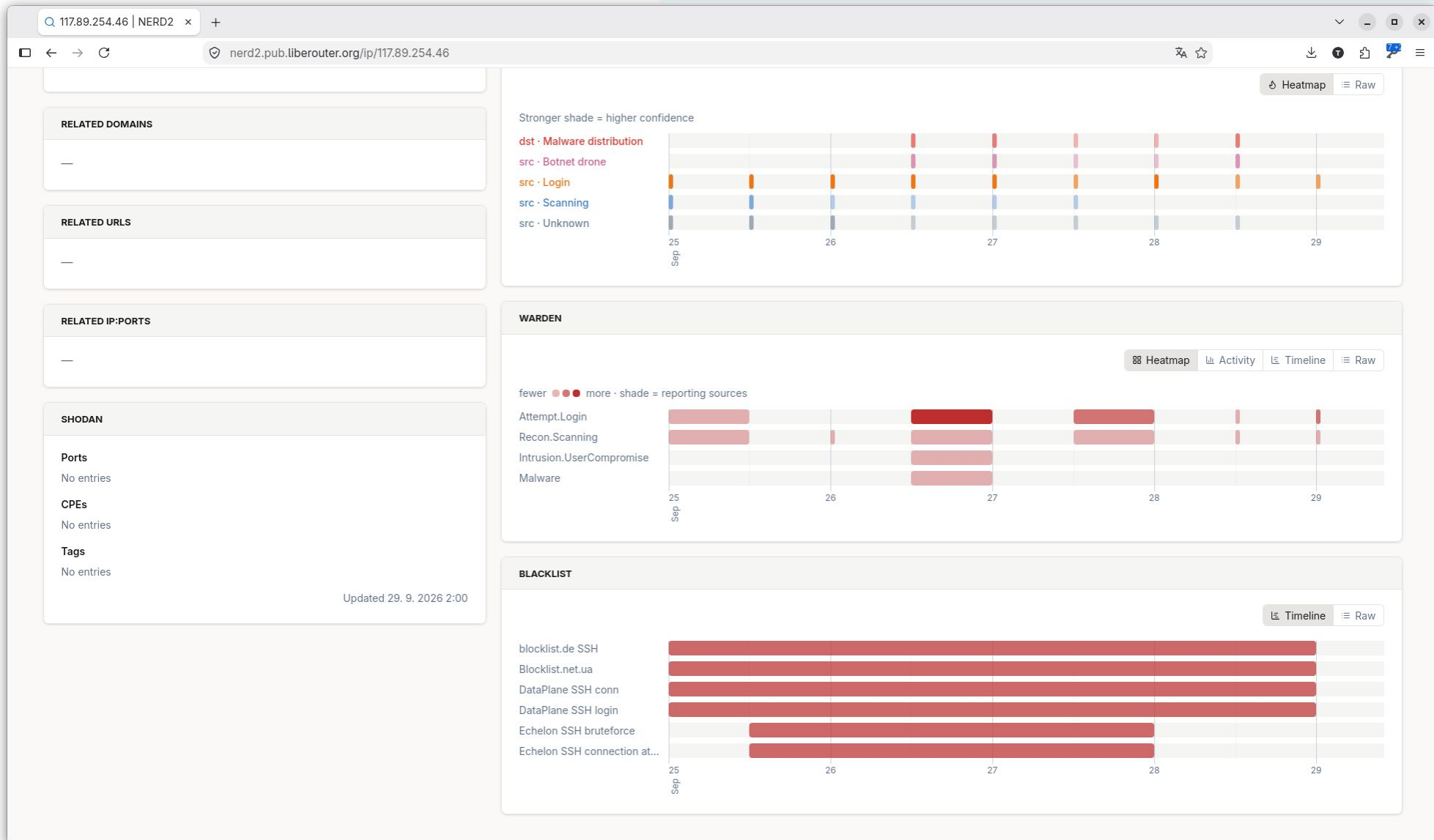
Domains

general.agency

NERD2

Service provided by CESNET.







general.agency | NERD2x

nerd2.pub.liberouter.org/domain/general.agency

NERD2 IP Addresses Domains URLs IP:ports Glossary

DOMAIN Browse all →

general.agency

Top-level domain: agency

BLACKLIST

CERT Polska Warning List

Updated 29. 9. 2026 2:00

THREATFOX SOURCE

—

THREAT CATEGORIZATION

ROLE	CATEGORY	CONFIDENCE	DETAILS
dst	Phishing site	48%	—

Updated 29. 9. 2026 2:00

HISTORY

THREAT CATEGORIZATION

Stronger shade = higher confidence

dst - Phishing site

Heatmap Raw

BLACKLIST

CERT Polska Warning List

Timeline Raw



2607:ff10:c8:594::/64

nerd2.pub.liberouter.org/prefix/2607:ff10:c8:594::%2F64

NERD2 IP Addresses Domains URLs IP:ports Glossary

UTC Local

IPV6/64 PREFIX Browse all →

2607:ff10:c8:594::/64

United States · America/Chicago

Last activity 29. 9. 2026 2:04

ADDRESSES

2607:ff10:c8:594::

2607:ff10:c8:594::4

2607:ff10:c8:594::5

2607:ff10:c8:594::6

2607:ff10:c8:594::8

2607:ff10:c8:594::9

2607:ff10:c8:594::a

2607:ff10:c8:594::b

2607:ff10:c8:594::c

2607:ff10:c8:594::d

Show more (+1)

Updated 29. 9. 2026 2:00

THREAT CATEGORIZATION

ROLE	CATEGORY	CONFIDENCE	DETAILS
src	Login	90%	protocol: TCP, TELNET port: 23
src	Scanning	95%	port: 0, 21, 22, 23, 26, 53, 80, 81, 82, 83 (+253 more)
src	Unknown	48%	—

Updated 29. 9. 2026 2:00

ASN

10439

Updated 29. 9. 2026 2:00

HOSTNAMES

No entries

Updated 29. 9. 2026 2:00

BLACKLIST

DataPlane SSH conn Turris greylist

HISTORY

THREAT CATEGORIZATION

Heatmap Raw

Stronger shade = higher confidence

src · Login

src · Scanning

src · Unknown

25

26

27

28

29

Sep

WARDEN

- Redesign + rework
- Nové grafy
- Podpora doménových jmen
- Podpora IPv6
- Nové zdroje

<https://nerd2.cesnet.cz/>
(<https://nerd2.pub.liberrouter.org/>)

Více na semináři BSS 2027!





Děkuji za pozornost

cejkat@cesnet.cz

<https://www.linkedin.com/in/cejkatomas/>

#PROPOJUJEME VĚDU

