

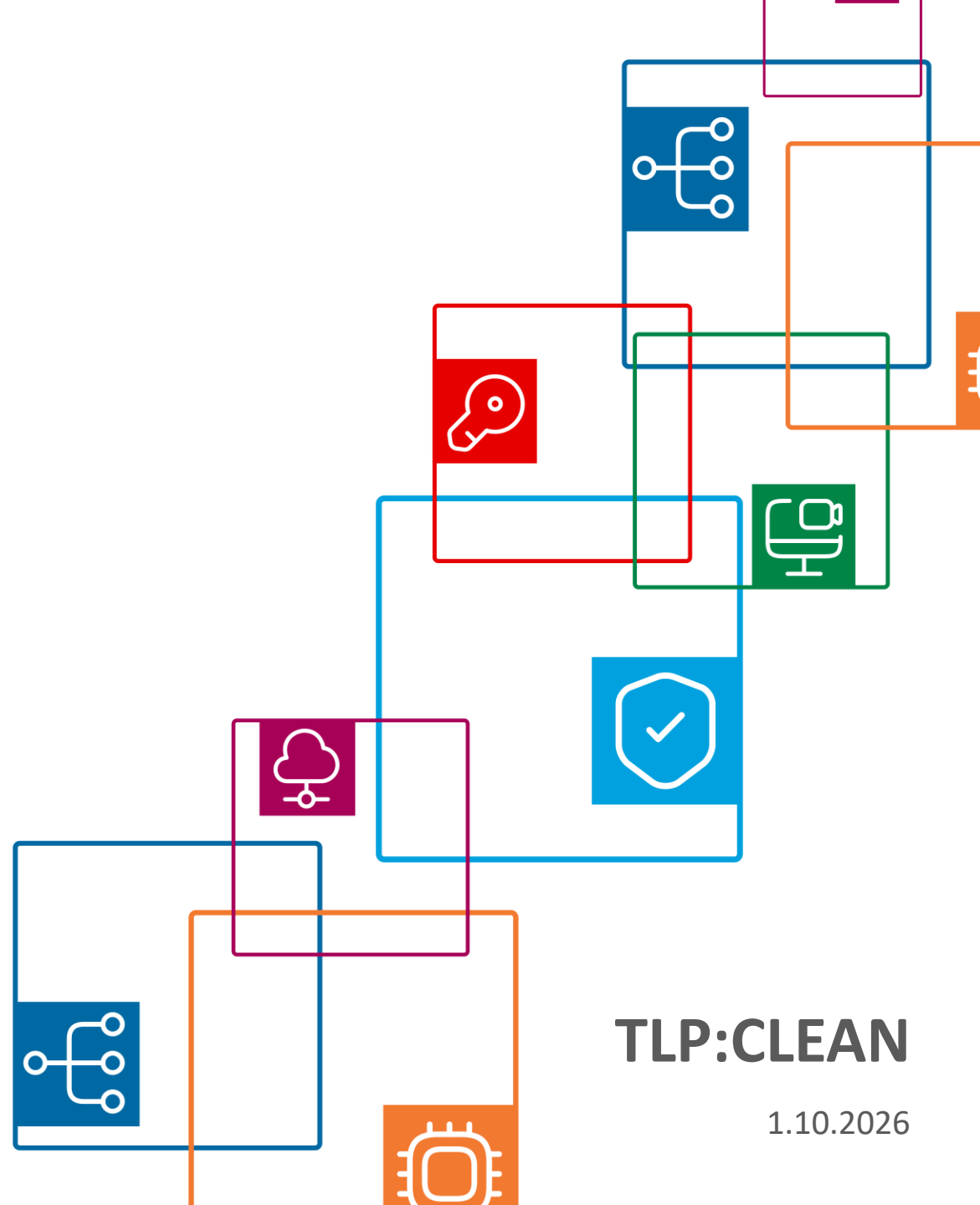


AI a bezpečnostní monitoring

Jaroslav Pešek

Praha

Oddělení 707, aktivita Traffic Analysis



TLP:CLEAN

1.10.2026

1980

Anderson: Computer Security Threat Monitoring and Surveillance

První návrh jak hledat zneužití systému v auditních záznamech

1998

Bro (dnešní Export logů

1987

Denning: An Intrusion-Detection Model

Statistické profily chování a expertní pravidla

NEW MASTER RECORDS

03/09/80

LAST TU TS
UPDATE PD ES FILES

61310 800303 1 1 CN61500 SIRSYST

```

      CRUIPSUIDSU  ITCH  ICNCT  LOGON
TOT: 241  0 1519 07414 78520  FREQUENCY
MAX: 241  0 1519 07414 78520 00-06: 0 12-18: 0
MIN: 241  0 1519 07414 78520 06-12: 1 18-24: 0
  
```

61999 800303 1 1 CN61333 CN611R CN61333 LOGGER CN61500 LASTLOG
CN61500 LIST CN61500 SEND PARL IR

```

      CRUIPSUIDSU  ITCH  ICNCT  LOGON
TOT: 17 28 7 1243 307  FREQUENCY
MAX: 17 28 7 1243 307 00-06: 1 12-18: 0
MIN: 17 28 7 1243 307 06-12: 0 18-24: 0
  
```

61999 800303 1 1 CN61333 CN611R CN61333 LOGGER CN61500 LASTLOG
CN61500 LIST CN61999 POWTWO PARL IR

```

      CRUIPSUIDSU  ITCH  ICNCT  LOGON
TOT: 9 17 7 1767 280  FREQUENCY
MAX: 9 17 7 1767 280 00-06: 0 12-18: 0
MIN: 9 17 7 1767 280 06-12: 1 18-24: 0
  
```

61999 800303 1 1 CN61333 CN611R CN61333 LOGGER CN61500 LASTLOG
CN61500 LIST CN61999 DES CN61999 NUXXPRT
CN61999 REPTCNL CN61999 VALCUREV CN61999 XCPFRNT2
CN61999 XCPFRNT4 CN61999 XCPFRNT6 CN61999 XCPFRNT8
CN61999 XCPFRNT9 PARL IR

```

      CRUIPSUIDSU  ITCH  ICNCT  LOGON
TOT: 48 200 161 6859 336  FREQUENCY
MAX: 48 200 161 6859 336 00-06: 0 12-18: 0
MIN: 48 200 161 6859 336 06-12: 1 18-24: 0
  
```

O úspěchu AI v síťovém monitoringu rozhoduje datová architektura.

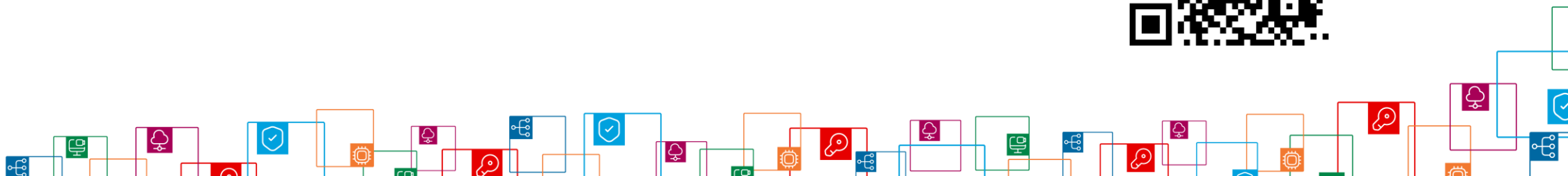
Projdeme problémy oboru a tři realistické způsoby, jak AI používáme.



- Syntetická data a vadné benchmarky
- Šifrování a viditelnost
- Chyby jsou drahé
- Síť je typicky obrovská
- Co s LLM?

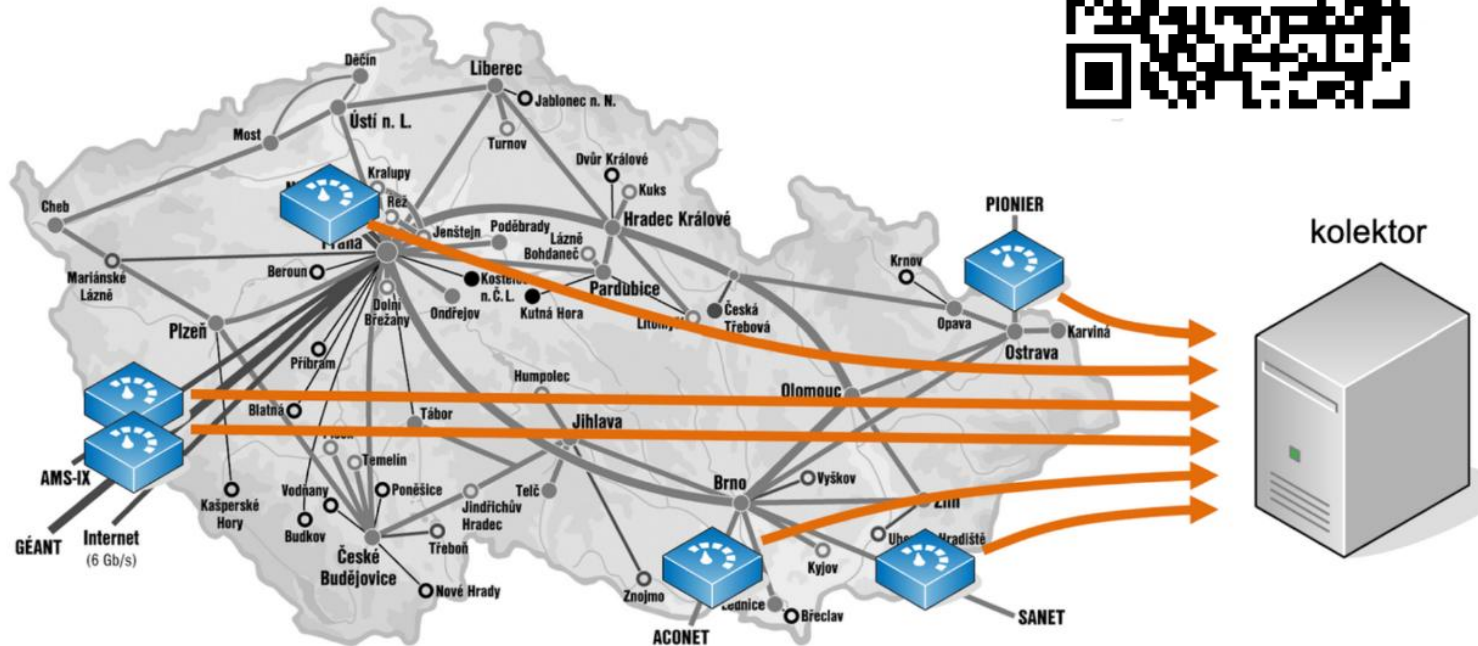


- Exportér síťových toků
- Modulární a výkonný: ověřeno na 400 Gbps
- Rozšířená data poskytují lepší sémantiku
 - NetFlow basics + statistické příznaky + dns, vpn, http, tls, quic
- Veliká škála vstupů (raw, pcap, dpdk, ...) i platform
- ipfixprobe.cesnet.cz

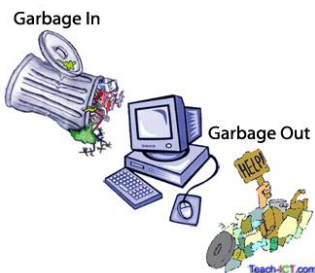


■ Kolektor dat ipfixcol2

- Vstup: NetFlow, IPFIX
- Výstup: file, json, kafka, clickhouse



- GIGO: garbage in, garbage out
- Veřejné syntetické benchmarky selhávají na reálné síti
 - CICIDS2017 obsahuje 25,9 % chybných klasifikací
 - ET-BERT: 97,5 % na benchmarku, 28 % na reálném provozu (SIGCOMM 2025)
- CESNET-DataZoo a CESNET-TsZoo, desetitisíce stažení



- Real-time

- Encrypted

- Traffic

work

Analysis

Flow probes až 400 Gbps



ipfixcol2



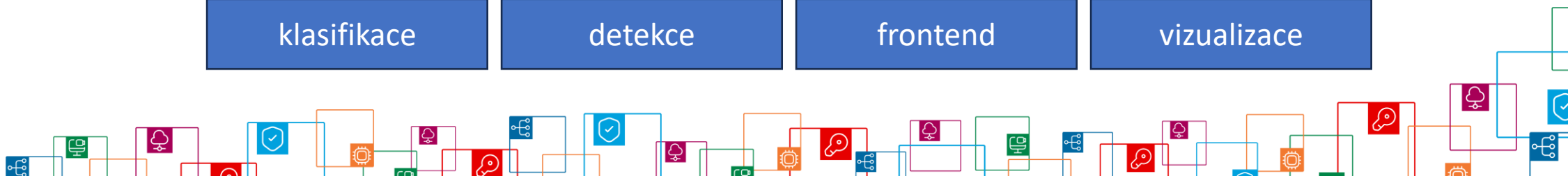
backend

klasifikace

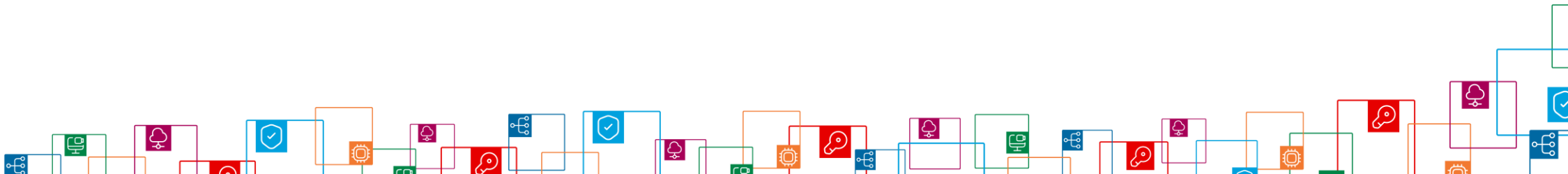
detekce

frontend

vizualizace

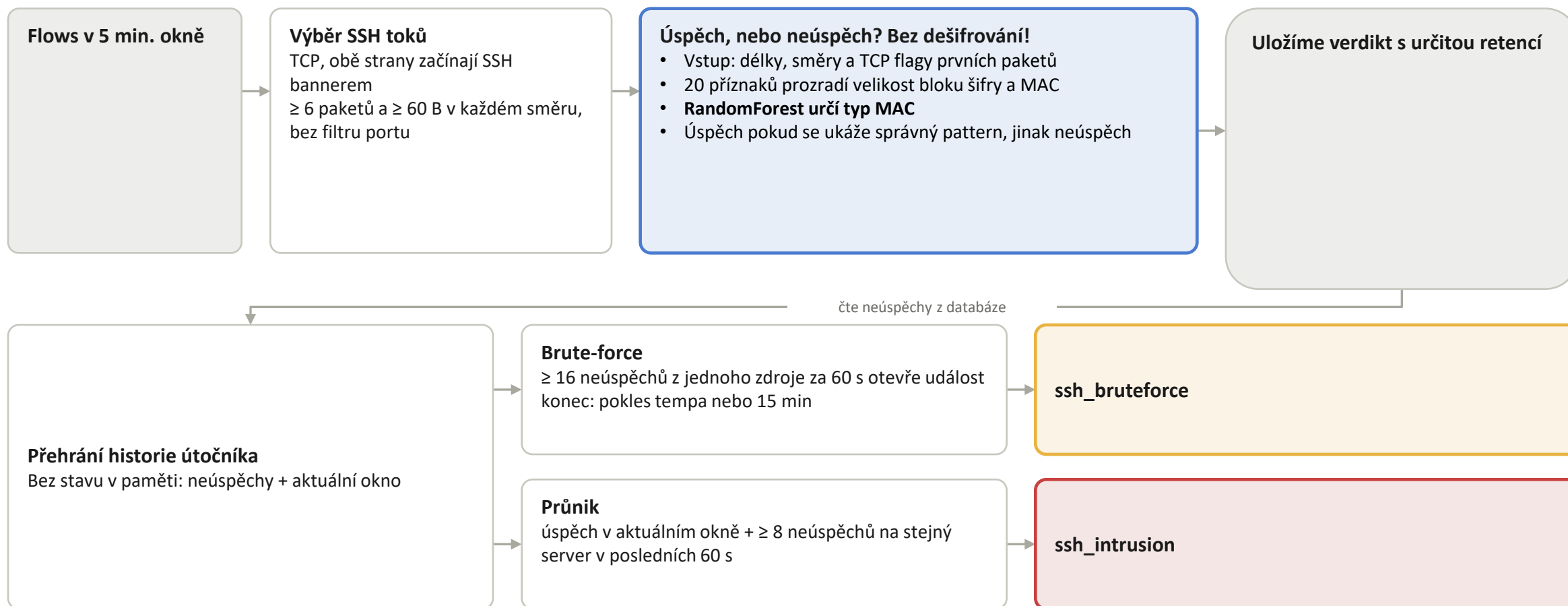


- Máme data i platformu – zatím bez AI, vše je deterministické
- **3 pilíře**
 - AI jako generalizace (pravidel)
 - AI jako automatizace
 - AI jako interakce



- **AI/ML napřímou jako detektor nefunguje**
 - ne každá odchylka je útok; chyba miliontina % toků denně není zanedbatelná
 - mnoho alertů = alert fatigue, každý stojí čas analytika
- **AI/ML dělá jen část práce klasifikátoru**
 - je jedním z indikátorů
 - odvozuje jeden z příznaků
 - vytváří reprezentaci

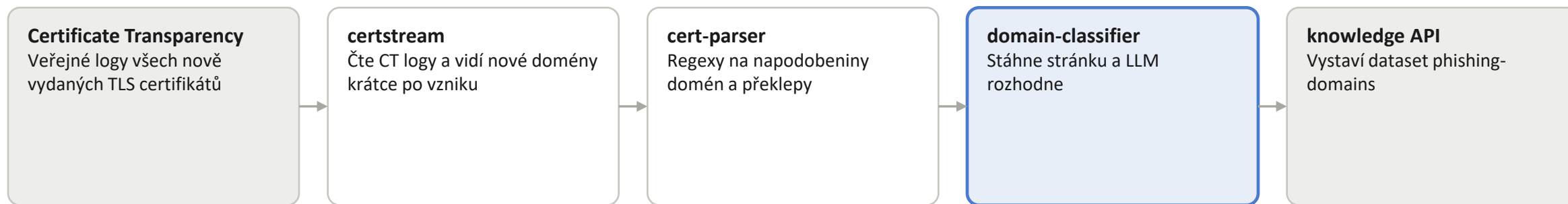




- LLM částečně přebírá rutinní práci analytika
- Dnes analytik ručně prochází podezřelé eventy
- LLM to udělá nad daty, analytik čte výsledek a rozhoduje
- Dva příklady: phishingové domény a investigace incidentů

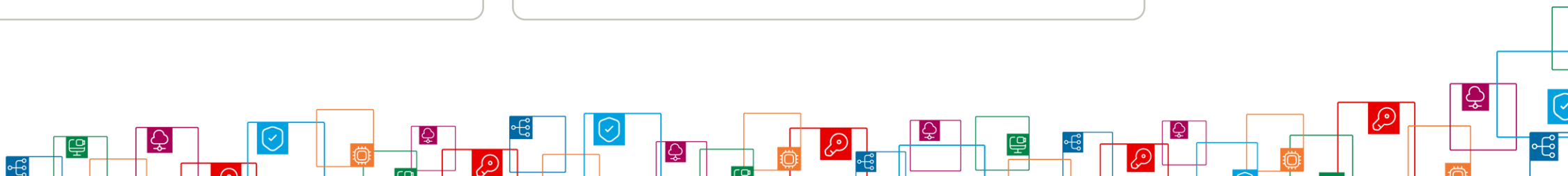
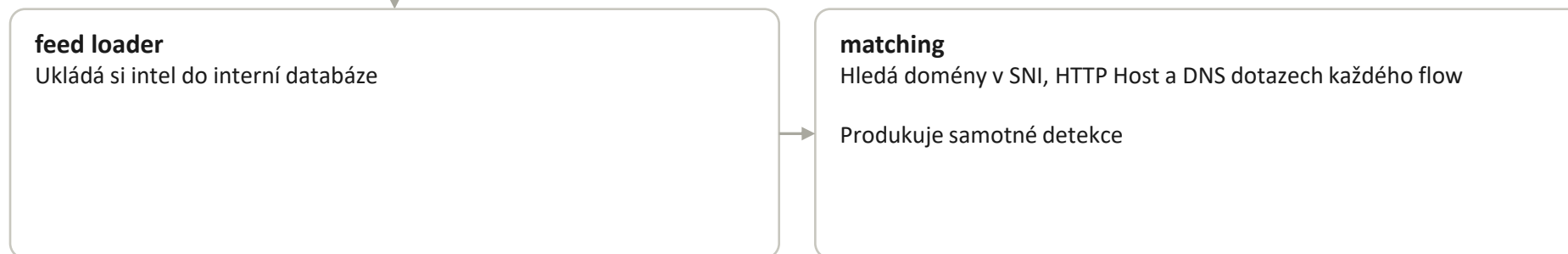


Cloud



Doručení datasetu

Retina



Neuhradená dopravná pokuta

V súvislosti s tým, že neposkytli neuhradenú dopravnú pokutu. Lehota na úhradu končí. Pre zobrazenie sumy a úhradu

domain	first_seen ↓	subject_value
vinted-order497823402.com	2026-09-30 15:59:44	
vinted.167-233-242-108.sslip.io	2026-09-30 15:46:04	
rangerovergurdau-cz.info	2026-09-30 15:46:04	
identitaetsbestaetigung.de	2026-09-30 15:46:04	
vinted.167-233-242-108.sslip.io	2026-09-30 15:46:04	
rangerovergurdau-cz.info	2026-09-30 15:46:04	
identitaetsbestaetigung.de	2026-09-30 15:46:04	
www.idcsobsmart-cz.casa	2026-09-30 15:07:45	
idcsobsmart-cz.casa	2026-09-30 15:07:45	
www.idcsobsmart-cz.casa	2026-09-30 15:07:45	
idcsobsmart-cz.casa	2026-09-30 13:47:31	
idcsobsmart-cz.casa	2026-09-30 13:47:31	
www.idcsobsmart-cz.casa	2026-09-30 13:47:31	

výši o trovy,

a dost: rehabilitačný program a možné odobratie vodičského

tu. Pre zistenie výšky dlhu a platobných údajov sa

20,00 €

z bankovú identitu

m do internetu neodišli.

Neuhradenú pokutu je potrebné vyrovnať v stanovenej lehote. Po jej márnom uplynutí sa vec postúpi do priestupkového konania; suma sa môže navýšiť a pribudnú trovy konania.

Pri ďalšom omeškaní môže nasledovať vymáhanie súdnym exekútorom a zadržanie vodičského preukazu. Bez overenia identity nie je možné pokutu zobraziť ani uhradiť.

Prihlásiť sa

PayPal

Email address

Password

Forgot pas

Log In

Deutsch | Français | English | Español | Português | Polski |

Contact Privacy Terms of Use

International

https://paypal-identitaets.com

Investigace: RDP brute-force



Investigating RDP brute-force109.205.211.122Sep 23, 15:40-15:45MEDIUMHide evidence

Investigate this RDP brute-force signal from 109.205.211.122. Is it real, and should an operator act on it?

SchemaExamplesExecuted SQL - 1 rowExecuted SQL - 24 rowsExecuted SQL - 40 rowsExecuted SQL - 4 rowsExecuted SQL - 1 rowExecuted SQL - 100 rowsExecuted SQL - 50 rowsExecuted SQL - 100 rowsExecuted SQL - 25 rowsChartedCharted

Verdict: confirmed-suspicious — confidence high.

The signal is real and understates what is happening: 109.205.211.122 has been running a sustained RDP brute-force spray against your exposed RDP servers for over three hours, alongside at least six other source addresses in a coordinated campaign. Nothing in the flows indicates any attempt succeeded.

Did it work? No evidence of success:

- Widened anchoring read (attacker's flows on port 3389, 14:40-16:45) shows 24 hosts touched; the 7 responding victims each received 19-37 attempts whose reverse traffic is uniformly failed-attempt shaped — every flow returned at most ~1.9 KB (RDP negotiation replies), no outlier session anywhere (flows around the signal).
- No rdp_intrusion signal exists from this attacker; instead it has emitted 40 rdp_bruteForce signals today (12:25 through 15:45), all against the same 7 victims — the detector kept seeing failures, never a success (all signals from this attacker).
- The grind continues unchanged past the signal window — flows every minute from 15:45 through 15:58 — which on its own would read as continued failed logins (attacker's per-minute rhythm).

Did the victims' egress change? No. Over ±24 h around the window end, no victim shows a new outbound peer; the only traffic that appears after 15:45 is inbound RDP probing (the victims' ~1.4 KB negotiation replies to yet another brute-forcer, 87.251.64.50, which began at 15:45:09) plus the continuing grind (victim egress before/after , drilldown of the apparent new peer).

Competing readings ruled out:

- Targeted attack / scanner: ruled out. This is an opportunistic spray — 2296 flows on 3389 across 25 hosts in one day, first activity at 12:00 today, nothing on any prior day in the last 7 (attacker's day rhythm , per-day recurrence); username cookie is the single generic value 'hello', and the named victims are RDP servers answering with CredSSP negotiation (signal row). Source: ASN 201814, Azerbaijan.
- Isolated actor: ruled out. The same 7 victims are simultaneously hit by sibling addresses 109.205.211.123, 94.26.88.51, 94.26.88.52, 62.164.177.27, 62.164.177.44, and now 87.251.64.50 — a coordinated campaign against this host group (other attackers on the same victims).

Caveats: counts are a floor — the SRC_IP pin drops inverted records and scan-shaped traffic is diverted to a noise store this layer can't see; and the post-window egress observation covers only ~11 minutes so far.

Suggested next step: block the campaign's source addresses at the edge (109.205.211.122/123, 94.26.88.51/52, 62.164.177.27/44, 87.251.64.50), and assess why seven hosts expose RDP directly to the Internet — put them behind a VPN/bastion and enable account lockout, since the grind is still active as of 15:58.

Result - 25 rowsTablechartSQLHide

flows

victims_touched

Trace

EVIDENCE - 9 RESULTS

signal row1 row

attacker's per-minute rhythm25 rows

flows around the signal24 rows

all signals from this attacker40 rows

victim egress before/after100 rows

drilldown of the apparent new peer100 rows

attacker's day rhythm4 rows

Result - 4 rowsTableSQLHide

Filter rows...

hour	flows	victims_tou
9/23/2026, 12:00:00 PM	410	25
9/23/2026, 1:00:00 PM	592	24
9/23/2026, 2:00:00 PM	638	24
9/23/2026, 3:00:00 PM	656	24

Show in conversation

per-day recurrence1 row

other attackers on the same victims50 rows

Investigace: port scan



- LLM je rozhraní k datům
- Dotaz v přirozeném jazyce
- Funguje díky předchozím krokům: reálná data, rozšířené flow záznamy, definované a schéma s danou sémantikou



What were the most frequent asns in the last hour?

Schema Examples Executed SQL · 15 rows Charted

Ranked by flow count over the last hour (2026-09-30 12:46:20 → 13:46:20), the most frequent ASNs were:

- **AS2852** dominates massively — ~352.9M flow-endpoint records across 942k active hosts (~35 TB of traffic).
- **AS198500** — ~60.7M records, but only 274 hosts, so it's a huge per-host volume (likely a CDN or infrastructure heavy-hitter).
- **AS8075** — ~58.0M records, ~59.7k hosts.
- **AS13335** — ~25.5M records, ~118.8k hosts.
- **AS16509** — ~22.6M records.

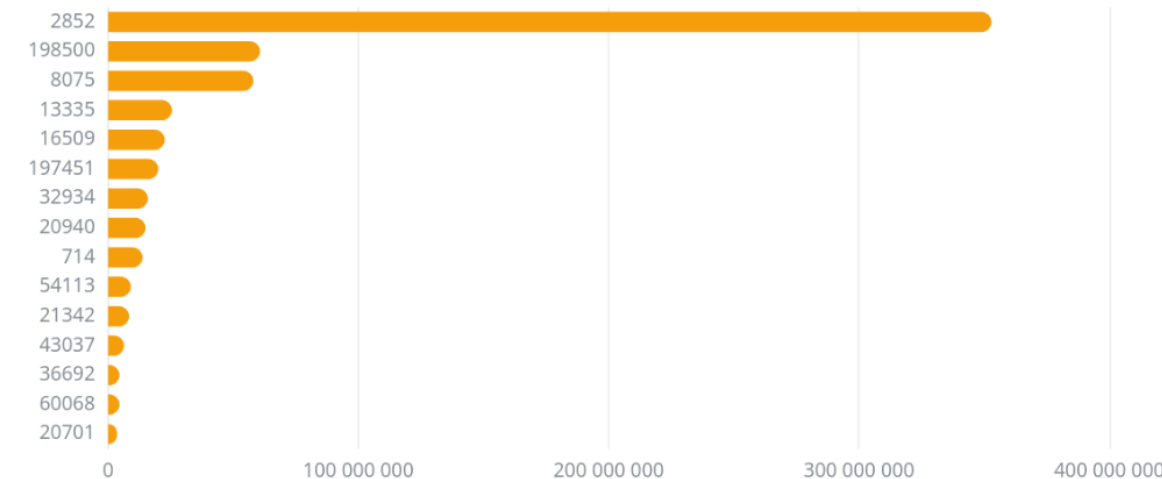
Rounding out the top 10: AS197451 (~20.0M), AS32934 (~15.8M), AS20940 (~14.9M), AS714 (~13.7M), and AS54113 (~9.0M). The full top-15 table is available above.

One measurement note: the count is per endpoint — each flow contributes one count per endpoint it has in a given ASN (a flow between two different ASNs counts once for each) — and flows with unresolved ASN (0) were excluded. AS2852's lead is so large that the ranking is the same whether you rank by flows, hosts, or bytes.

Result · 15 rows

Table Chart SQL Hide

Most frequent ASNs by flow count, last hour (2026-09-30 12:46–13:46)



Trace

What TLS domains carried the most volume in the last two hours? Which IPs communicated with these domains? Give me sankey with client IP - domain - server IP.

Schema Examples Executed SQL · 10 rows Executed SQL · 400 rows Charted

Over the last two hours (2026-09-30 11:51:40 → 13:51:40 local), the heaviest TLS domains by total volume were:

1. belle2-webdav-analysis-data.cc.kek.jp — 435.4 GB (Belle II physics data at KEK, Japan)
2. res.public.onecdn.static.microsoft — 279.6 GB (Microsoft CDN)
3. cache11-vie1.steamcontent.com — 260.2 GB, plus cache10 (250.9 GB), cache9 (236.0 GB) and cache12 (198.4 GB) — Steam content servers in Vienna
4. fe1.dhr.cesnet.cz — 209.4 GB (CESNET data host)
5. oneclient.sfx.ms — 189.9 GB, updates.cdn-apple.com — 165.4 GB, dcbldoor.sdcc.bnl.gov — 163.3 GB (Brookhaven)

The sankey above maps client IP → domain → server IP for these ten domains. What stands out in the paths:

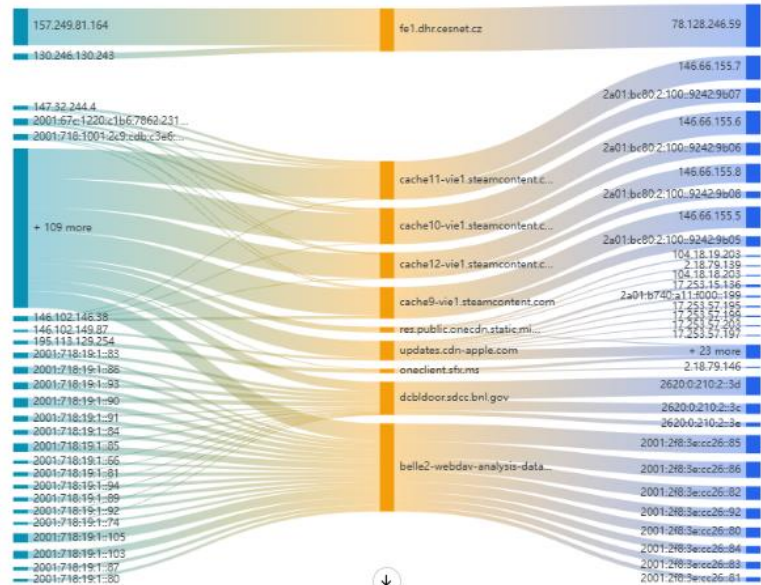
- One dominant transfer: 157.249.81.164 pulling from fe1.dhr.cesnet.cz at 78.128.246.59 accounts for ~179.7 GB on its own — the single heaviest client→server path.
- Physics data movement: the KEK and BNL domains are served to a whole cluster of IPv6 clients in 2001:718:19:1::/64 — KEK from servers 2001:2f8:3ecc26:80–92, BNL from 2620:0:210:2::3c–3e — dozens of parallel multi-GB transfers, typical of a grid data replication job.
- Steam traffic is many-client: a long tail of local clients (195.113.213.189, 195.178.92.59, the 147.32.244.x and 147.229.186.x hosts, and IPv6 clients) pulling from cache servers 146.66.155.5–8 and 2a01:bc80:2:100:9242:9b05–08.
- Apple/Microsoft CDN: updates.cdn-apple.com fans out to 17.253.x.x and 2a01:b740:... servers; the Microsoft names go to Akamai (2.18.79.139/144) and 104.18.19.203.

Two notes on reading the chart: the stages are oriented by keeping only records where the destination is the server end (inverted records excluded), so per-domain totals in the sankey run slightly below the ranking above; and the result is capped at the 400 heaviest client-domain-server triples, so very small tails are cut.

Result · 400 rows · table shows the first 400, the agent read 143

Table Chart SQL Hide

Client IP → TLS domain → server IP, last 2 hours



1. Na jakých datech byl trénován a testován?
2. Co vidí v šifrovaném provozu?
3. Zvládne vaši propustnost?
4. Co smí LLM číst a co smí spustit?



Paying Attention Is All You Need

Děkuji za pozornost. Dotazy?