

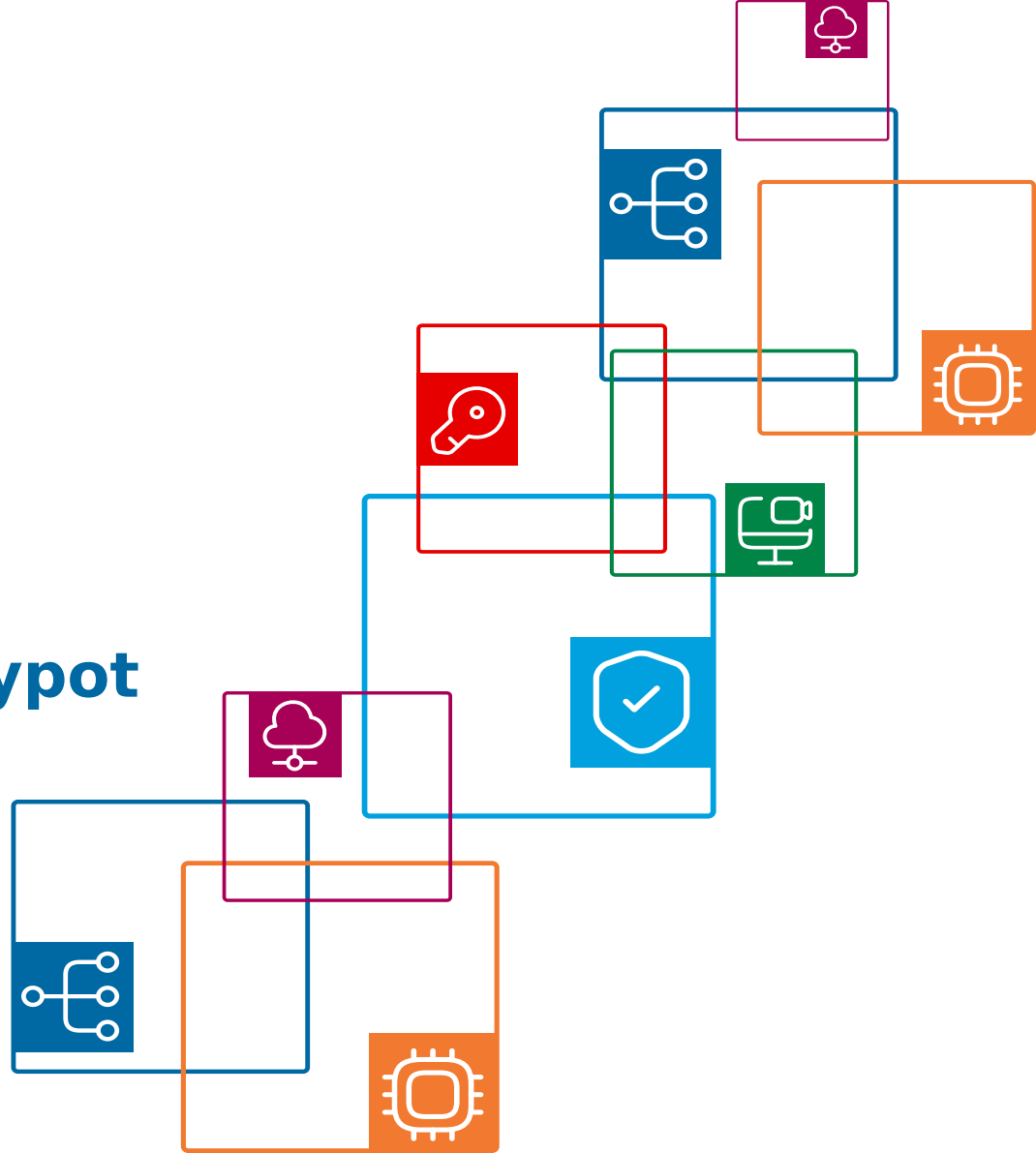


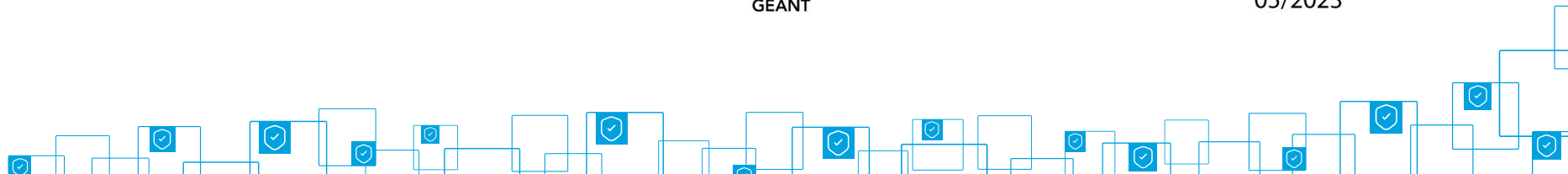
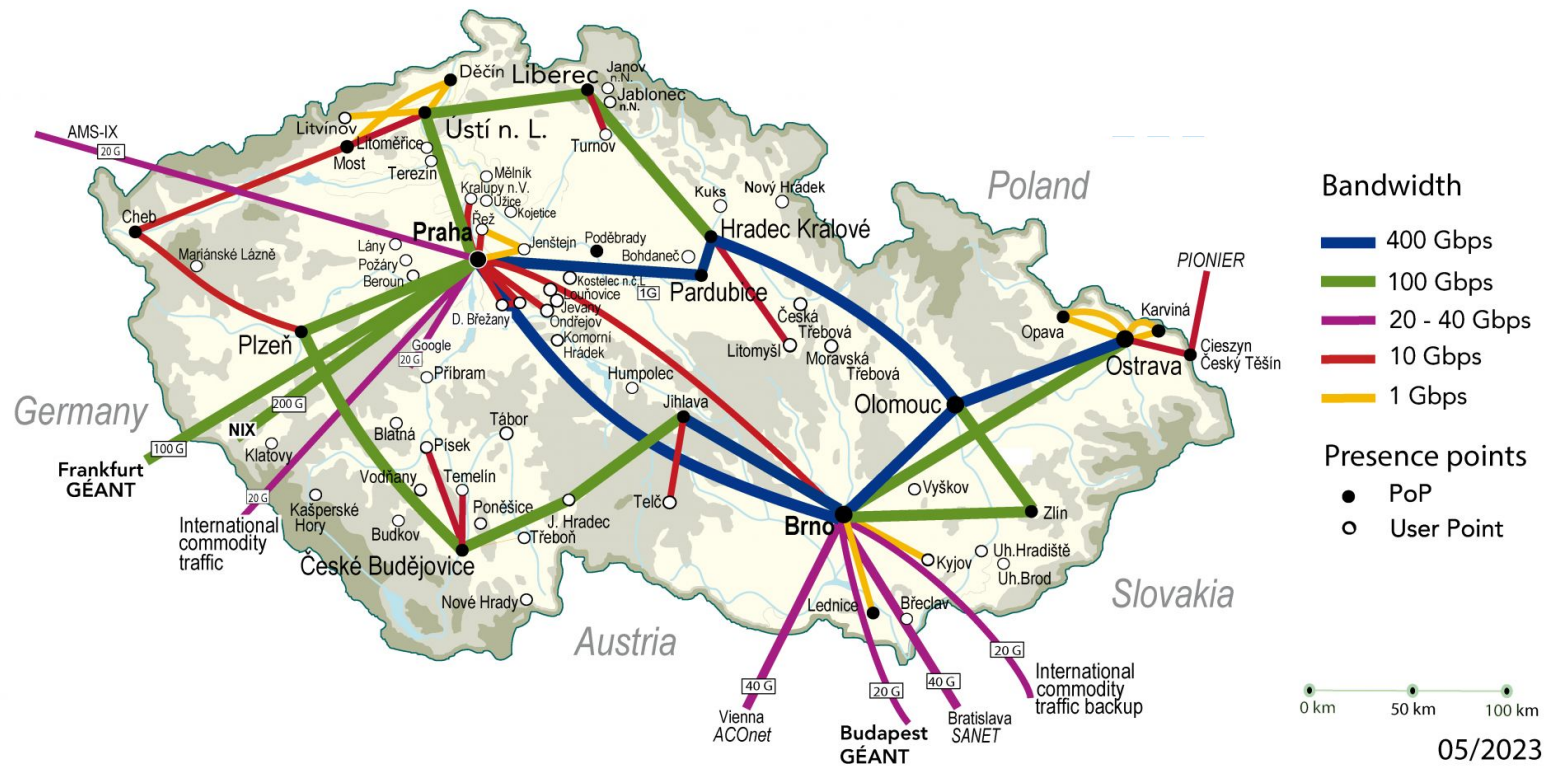
CESNET jako velký honeypot

Pavel Kácha

Konference e-infrastruktury CESNET

1. 10. 2026 Praha







60+ služeb



350+ zaměstnanců



28 řádných členů



400 Gb/s v páteřní síti



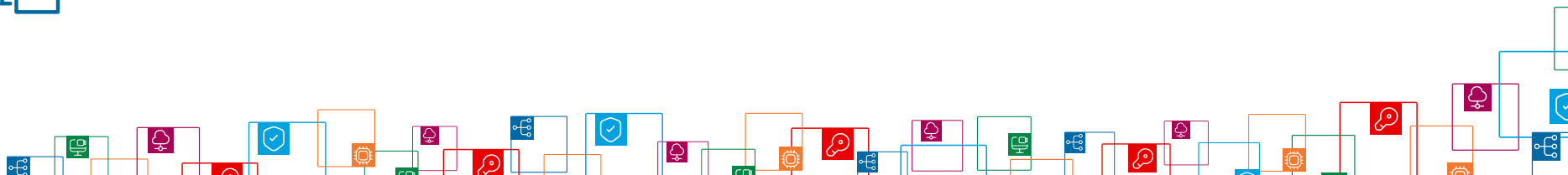
**400+ připojených
institucí**



**120+ PB datových
úložišť**



41000+ CPU





Vysoké školy
a univerzity



Výzkumné organizace,
nemocnice



Ústavy
Akademie věd



Veřejná
správa

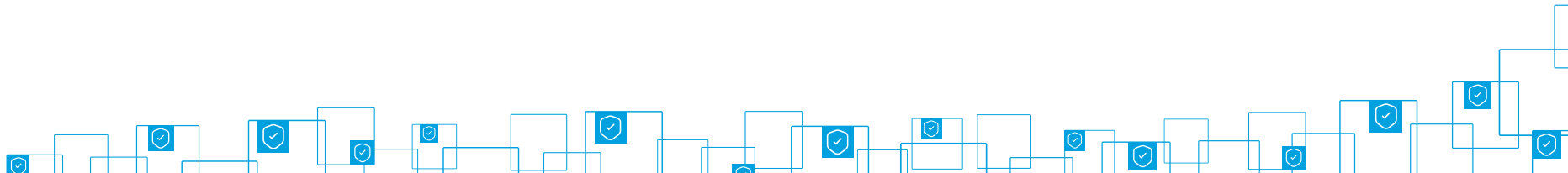
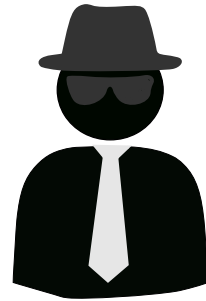


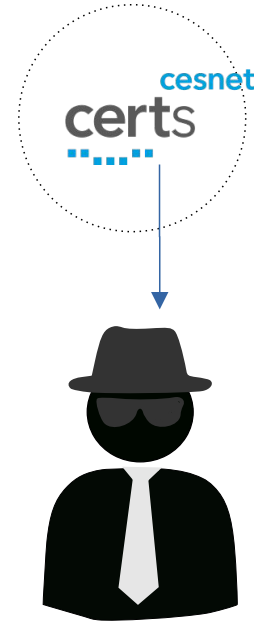
Základní, střední
a vyšší odborné školy



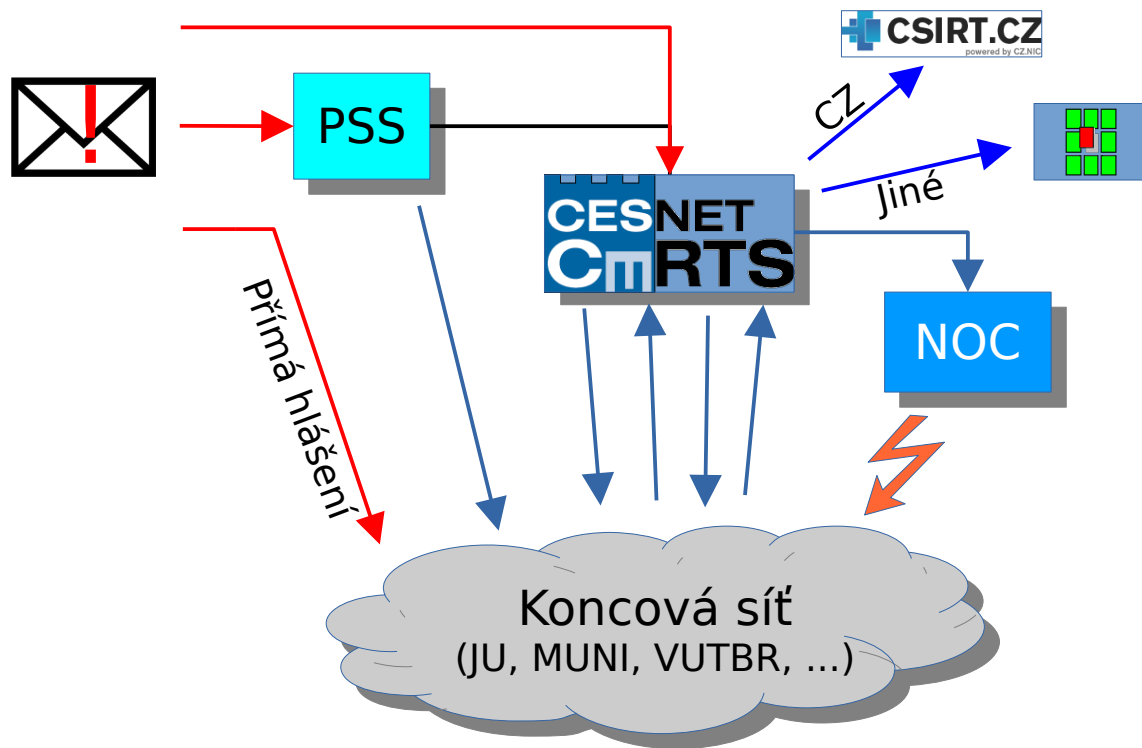
Knihovny, muzea,
galerie







- 2004* Listed – první v ČR
- 2007* Pilot CSIRT.CZ
- 2008* Accredited
- 2011* Warden
Mentat
CSIRT.CZ → CZ.NIC
- 2014* FLAB
Automatizované reporty
- 2017* Passive DNS
První The Catch
- 2021* Hugo
- 2022* SOC
CyberFeed





Skupina: abuse@cesnet.cz
Reportovací okno: 26. 9. 2026 10:00:00 - 26. 9. 2026 12:00:00 (2 hodiny)
Report vytvořen: 26. 9. 2026 12:00:06 (před 3 dny)
Report odeslán: 26. 9. 2026 12:00:06 (před 3 dny) na abuse@cesnet.cz
Počet událostí: 1 reportováno, 1 celkem v nadřazeném souhrnném reportu

Vážení kolegové,

naše detekční systémy zaznamenaly následující možné problémy související s hostitelem 195.113.147.124, který souvisí s Vaším rozsahem IP adres nebo Vaší doménou:

[1] [Stroj má otevřeně přístupnou službu SNMP s komunitou "public".](#)

Zdroj	První událost	Poslední událost	Detektory		Zprávy	
195.113.147.124 ▾	2026-09-25 05:14:34 +02:00	2026-09-25 05:14:34 +02:00	1	1	Zpětná vazba	Vyhledat události
Details from detector cz.cesnet.sabu_ext.shadowserver						
Zdrojový port:		161				
Zdrojový protokol:		snmp, udp				
Spravovat třídu událostí vulnerable-config-snmp						

Tento report obsahuje událostí se STŘEDNÍ závažností. Přezkoumejte prosím dotčené systémy, napravte zjištěné problémy a informujte nás o výsledku.

Od:
Komu: abuse@cesnet.cz
Kopie:
Příloha: [file-2](#), 1.6 KBytes
[fortianalyzer-ips-2026_09_28.log](#), 16.8 KBytes

Dobrý den,

hlásíme bezpečnostní incident týkající se skenování a pokusů IPS útok ze síťového identifikátoru v síti CESNET.

Očekáváme vaši odpověď a vyjádření k níže uvedenému provozu.

Mezi 16:15 a 16:36 CET jsme zaznamenali přes 16 000 spojení ze zdrojové IP adresy na náš cílový systém. Část z nich bezpečnostní systém FortiGate vyhodnotil jako škodlivou a zablokoval.

Může se jednat o legitimní provoz ale i o kompromitovaný stroj provádějící skenování.

Detaily a logy:

Zdrojová IP adresa: 78.128.214.225

Cílová IP adresa:

Zdrojový port: Různé (dynamické)

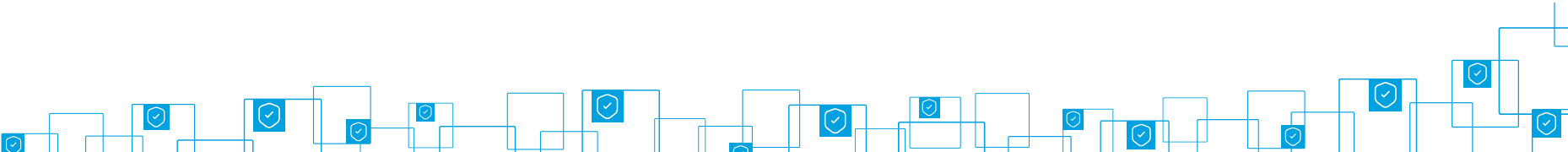
Cílový port: 8443

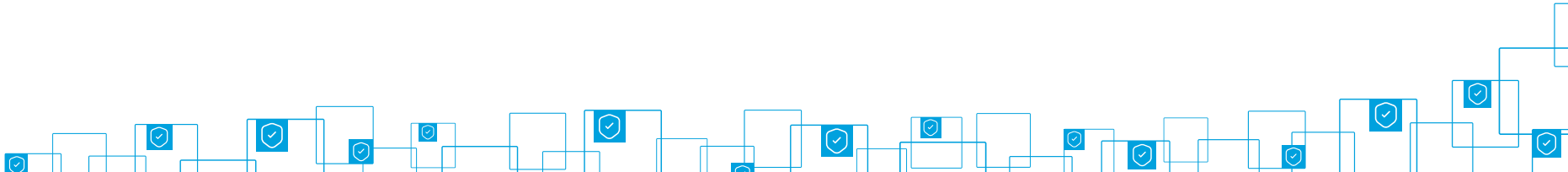
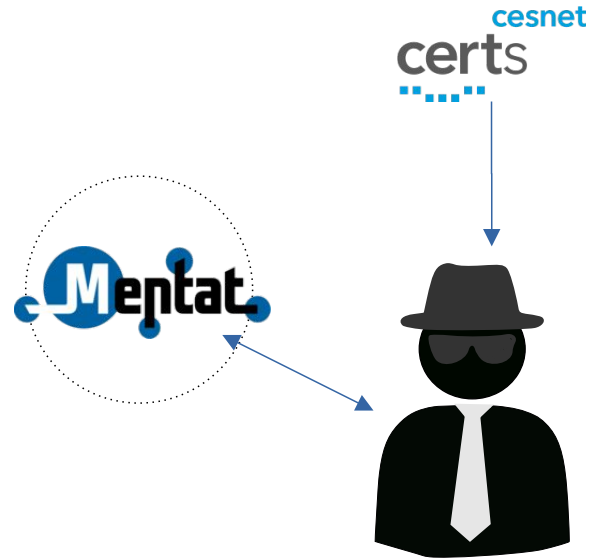
Protokol: TCP

Časové rozmezí: 16:15 až 16:36 CET.

Prosíme o ověření, očekávaný a žádoucí.

S pozdravem,





Prohledat databázi událostí

Čas detekce

Čas uložení

Zdroj

Cíl

Hostitel

Událost

Detektor

Admin

Čas detekce od:

Čas detekce do:

2025-10-06 14:00:00

2025-10-13 14:00:00

Poznámka: Zvolená časová zóna je "Europe/Prague"

Poznámka: Zvolená časová zóna je "Europe/Prague"

Adresy zdroje:

Zdrojové porty:

Typy zdroje:

195.113.134.0/24

Nic nevybráno

Nic nevybráno

Adresy cíle:

Cílové porty:

Typy cíle:

Nic nevybráno

Nic nevybráno

Nic nevybráno

Kategorie:

Protokoly:

Popis:

Nic nevybráno

Nic nevybráno

Nic nevybráno

Zdrojová skupina:

Zdrojové závažnosti:

Zdrojové třídy:

Nic nevybráno

Nic nevybráno

Nic nevybráno

Cílová skupina:

Cílové závažnosti:

Cílové třídy:

Nic nevybráno

Nic nevybráno

Nic nevybráno

Detektory:

Typy detektorů:

Nic nevybráno

Nic nevybráno

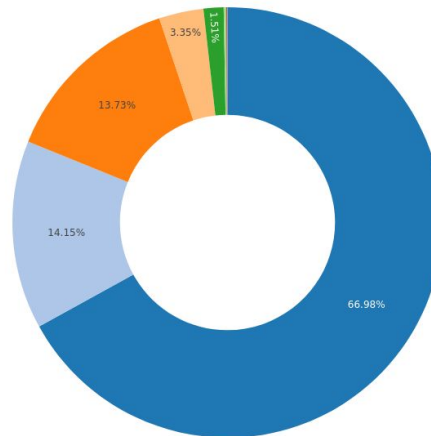
Hledat

Vymazat

Rychlé hledání

Řadit dle:

dle času detekce sestupně

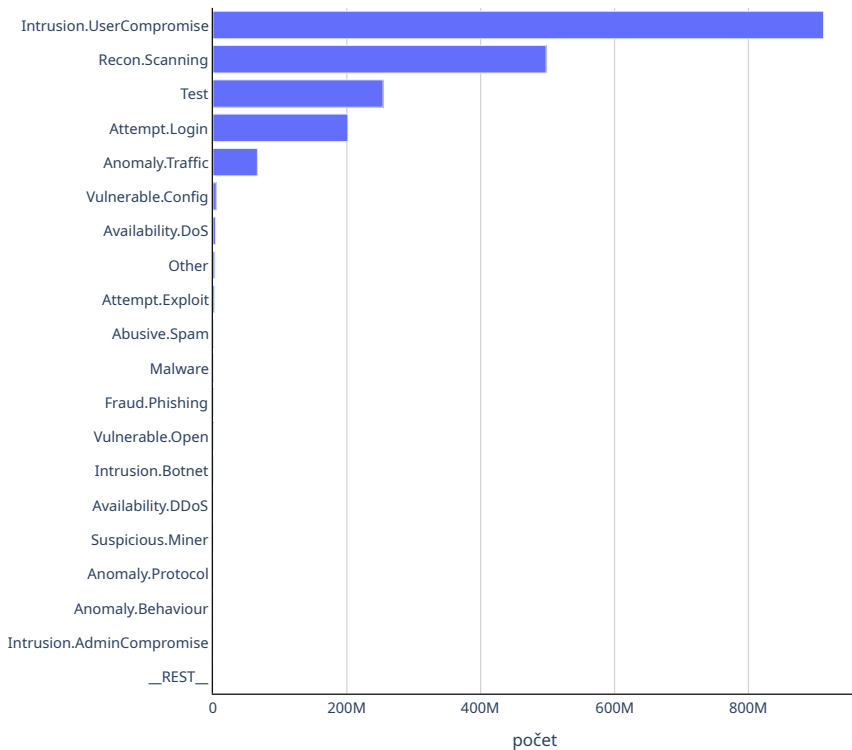


Třída události	Počet	Podíl
unknown	22 025 607	66.98%
recon-scanning	4 654 342	14.15%
attempt-login-ssh	4 516 765	13.73%
anomaly-traffic	1 100 475	3.35%
attempt-login-rdp	495 790	1.51%
avail-ddos	65 241	0.2%
attempt-login-telnet	19 796	0.06%
attempt-exploit	4 235	0.01%
vulnerable-config-tls-deprecated	2 604	0.01%
vulnerable-config-ciphers-old	378	0%
attempt-exploit-http	190	0%
vulnerable-config-ntp	163	0%
vulnerable-config-time-not-synced	103	0%
abusive-spam-spammer	85	0%
vulnerable-config-tls-old	72	0%
vulnerable-config-ssdp	21	0%
vulnerable-config-domain	13	0%
vulnerable-config-ipmi	5	0%
vulnerable-config-netbios	3	0%
anomaly-host-miner	3	0%
intrusion-botnet-bot	1	0%
vulnerable-config-snmp	1	0%

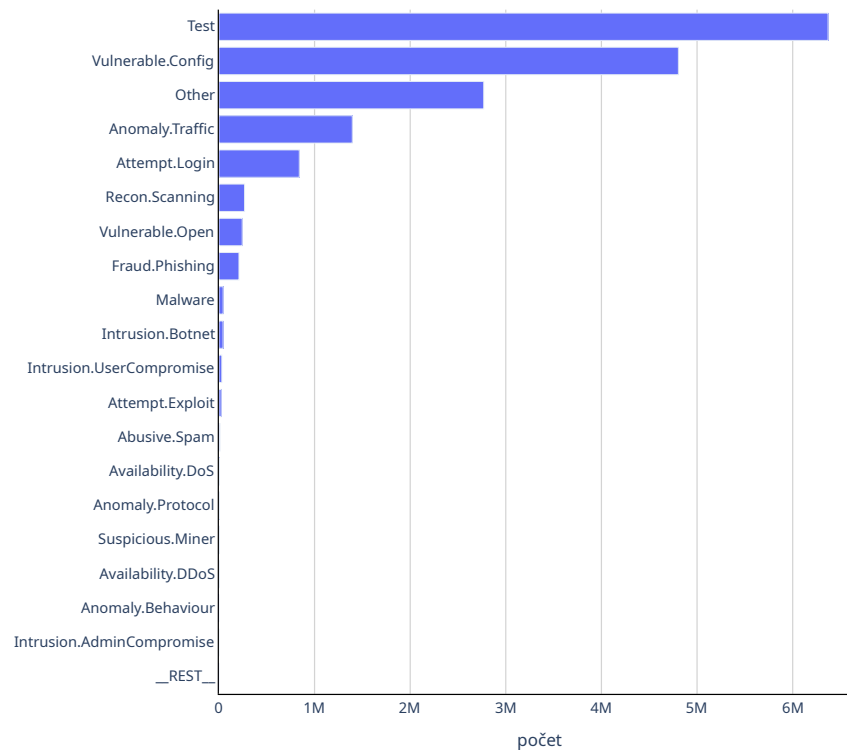
~ 20 reportů denně

<https://mentat.cesnet.cz>

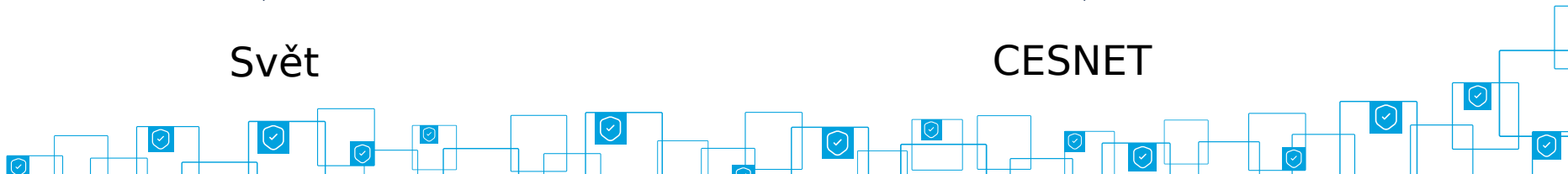


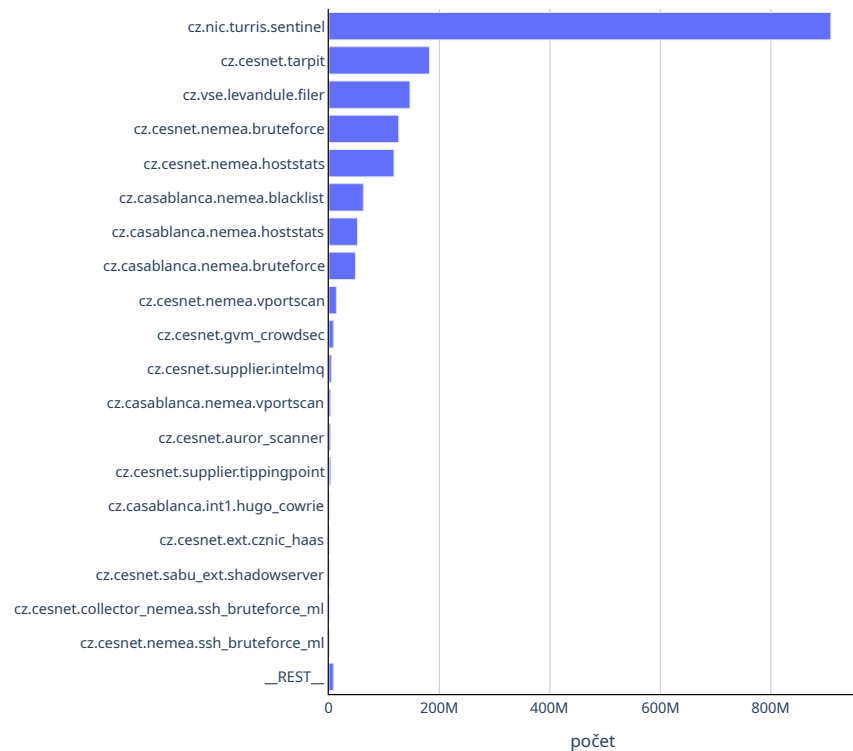


Svět

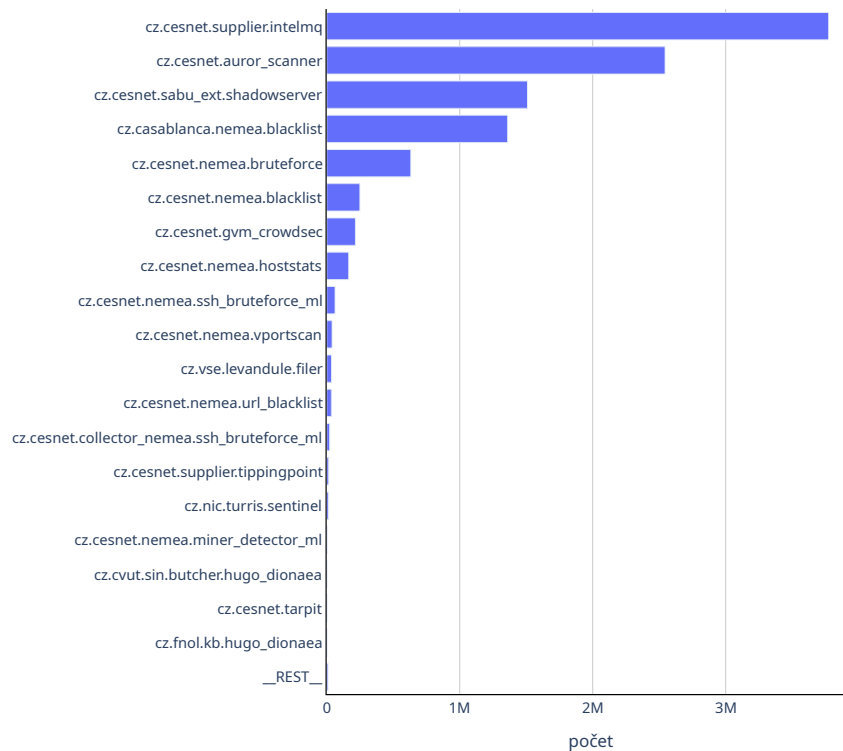


CESNET

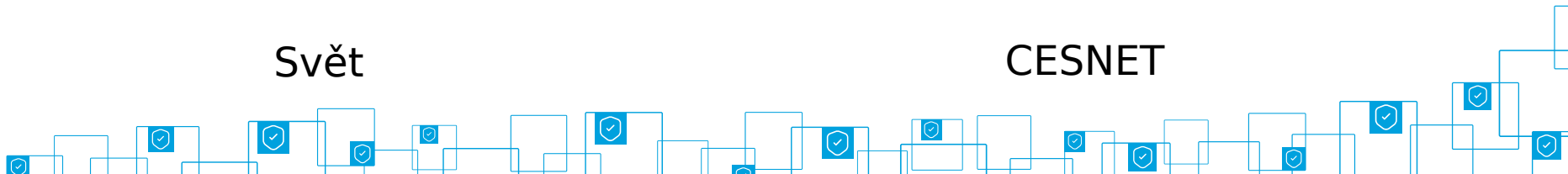


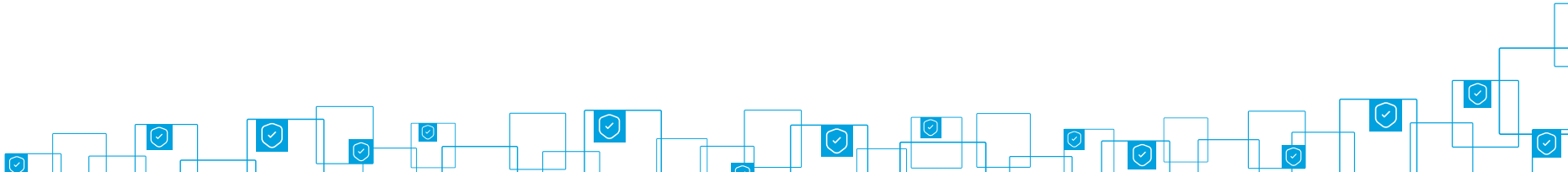
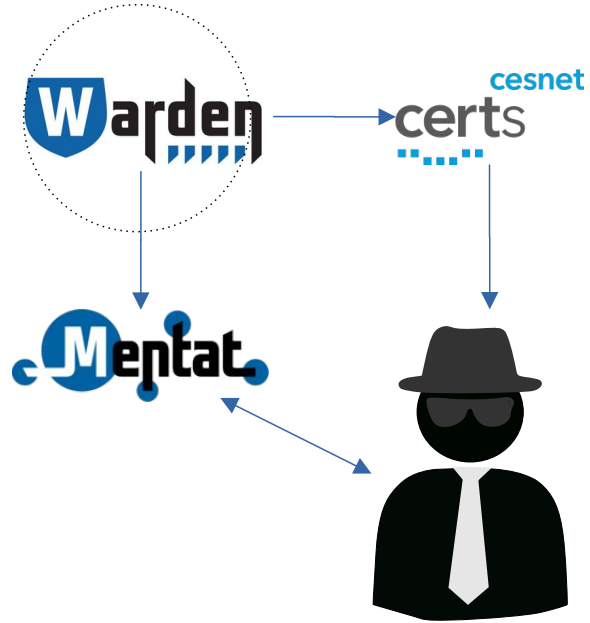


Svět



CESNET

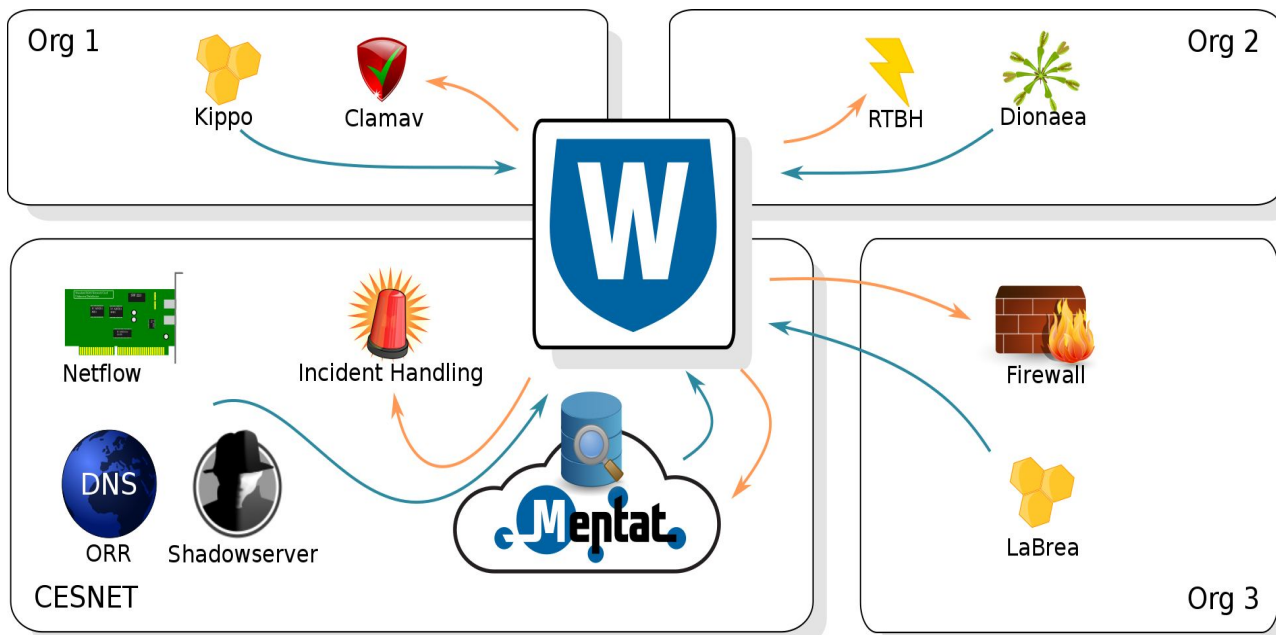




- Něco za něco
- Tvoje data jsou dostupná ostatním...
- ... a máš data celé komunity
- *Client/server* – transportní kanál
- API, knihovna, démon
- ~ 4.5 mil/den, 30 tis/den CESNET

IDEA

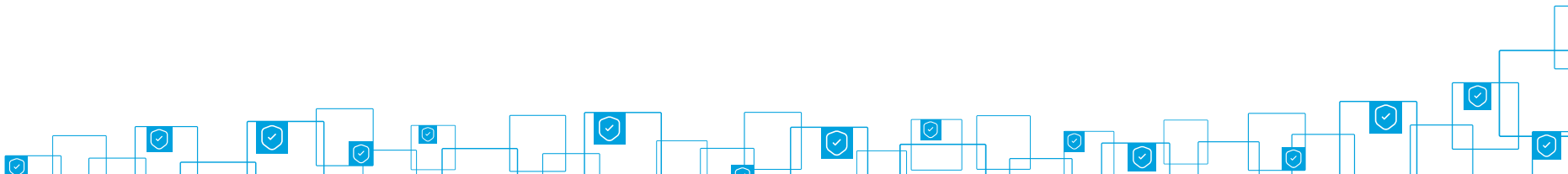
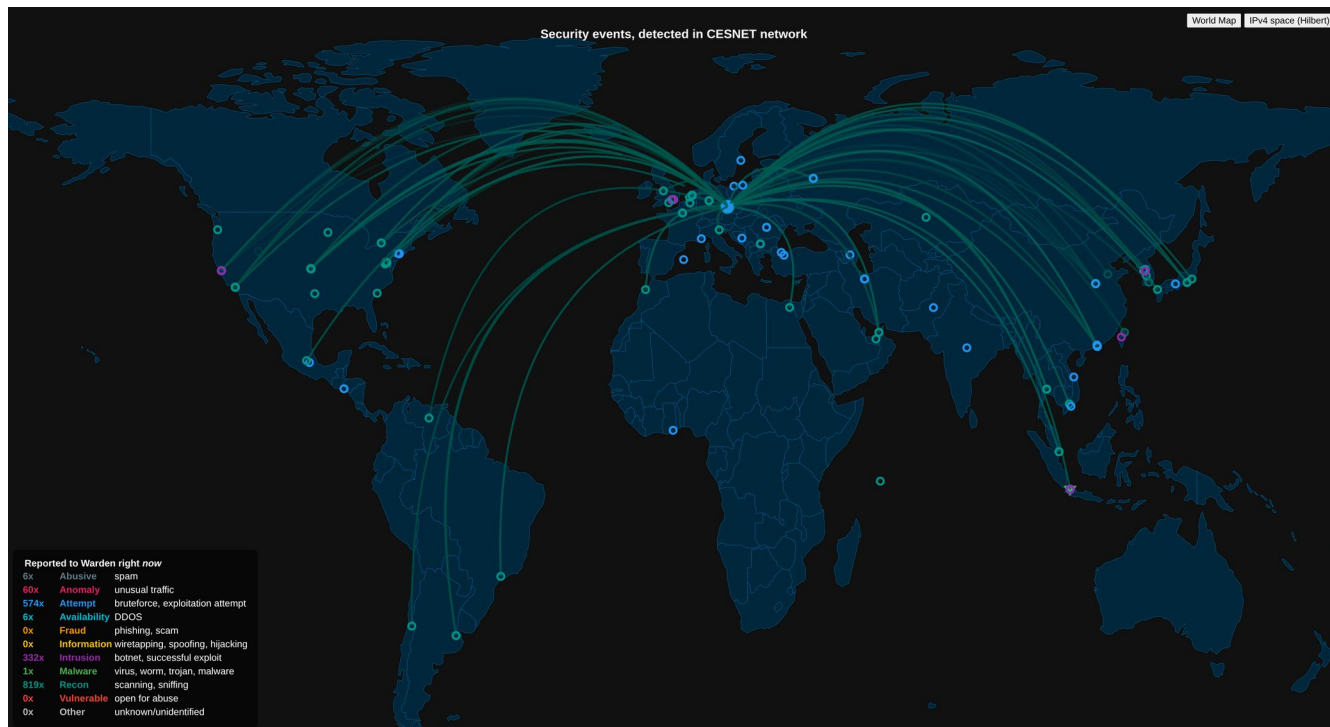
```
{
  "Format": "IDEA0",
  "ID": "cca3325c-a989-4f8c-998f-5b0e971f6ef0",
  "DetectTime": "2014-03-05T15:52:22Z",
  "Category": ["Intrusion.Botnet"],
  "Description": "Botnet Command and Control",
  "Source": [
    {
      "Type": ["Botnet", "CC"],
      "IP4": ["93.184.216.119"],
      "Proto": ["tcp", "ircu"],
      "Port": [6667]
    }
  ]
}
```

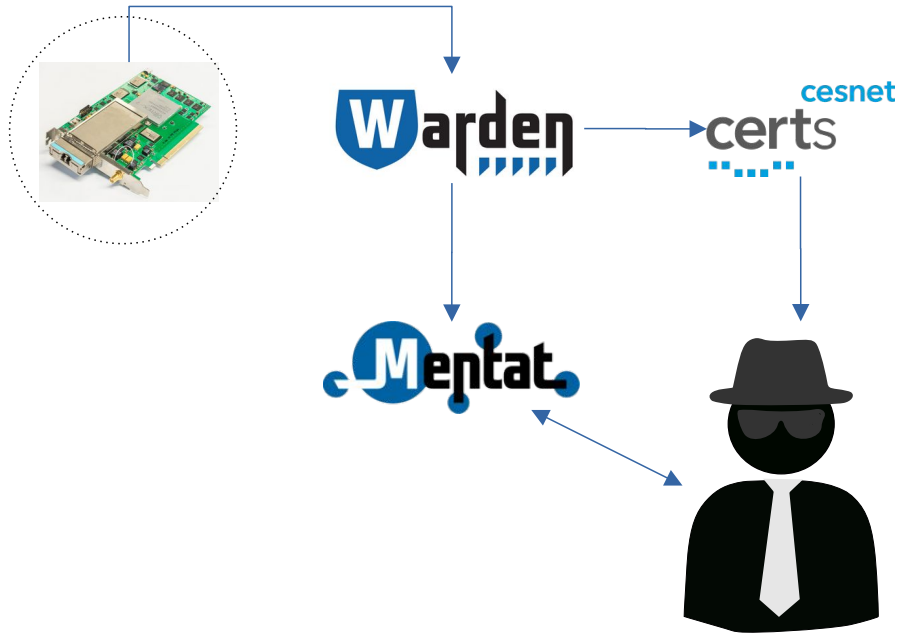


<https://warden.cesnet.cz>

<https://idea.cesnet.cz>

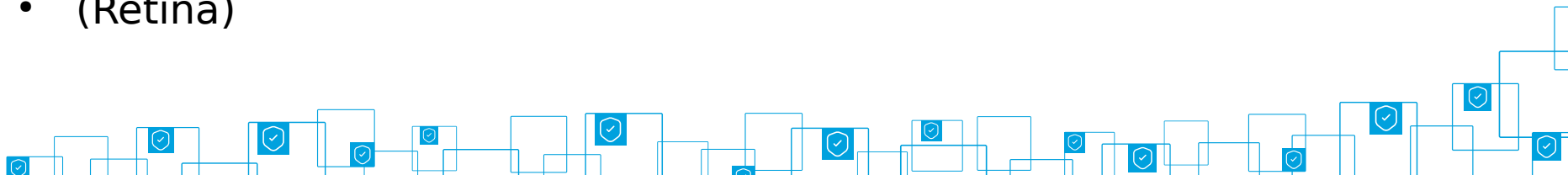
- 40 aktivních klientů
- ~3 mil. událostí za den
- ~25 mil. škodlivých IP

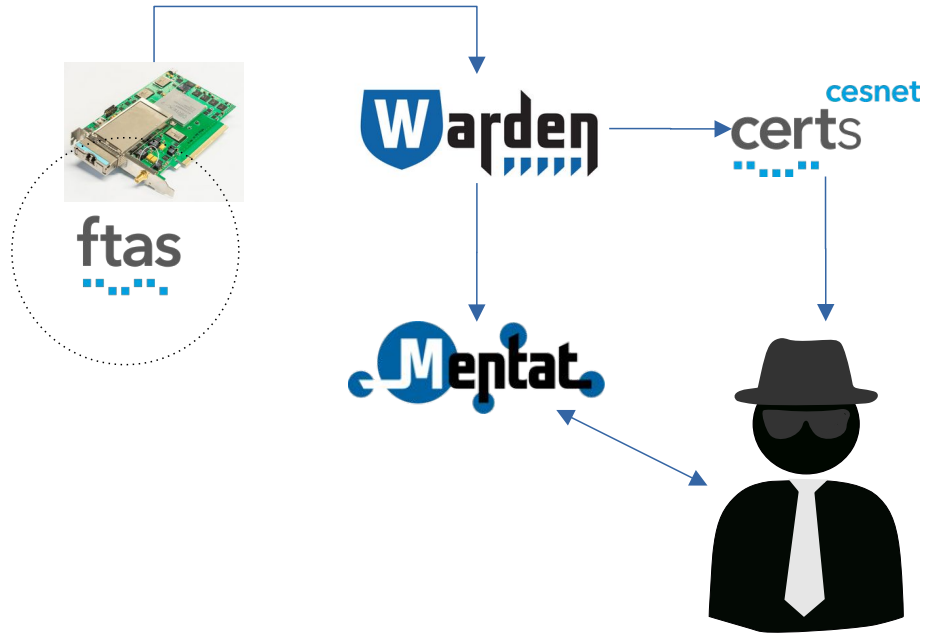




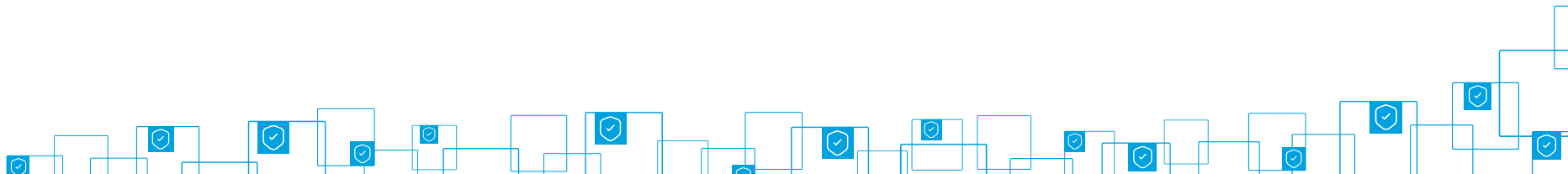
HW sondy + Nemea

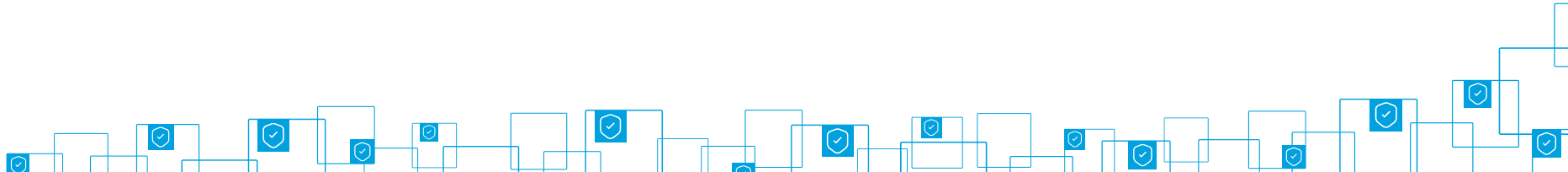
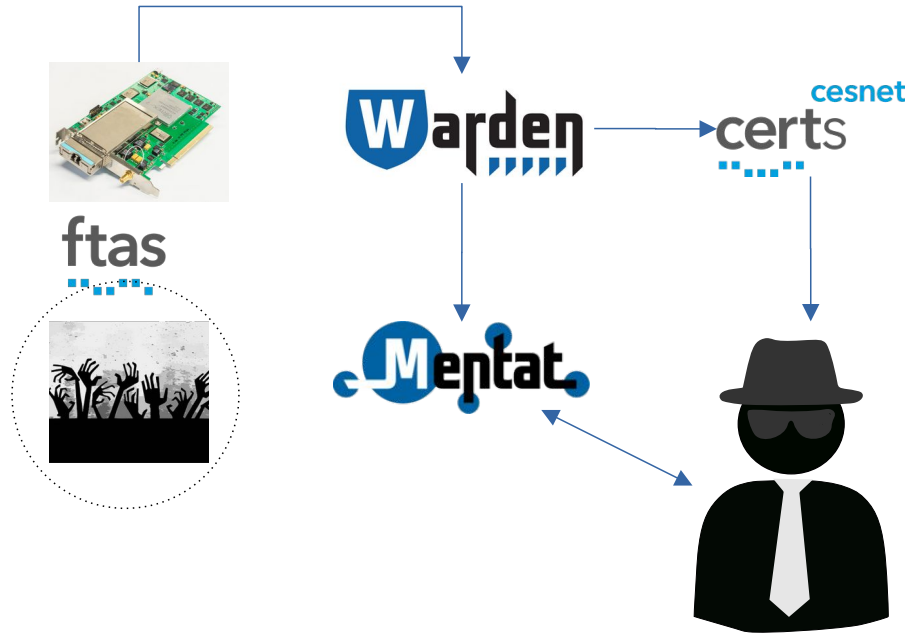
- FPGA 400 Gb/s (IPFIX)
 - 400 000 flow/s z 9 sond
- DDoS (amp) → DDoS Protector
- Skeny, slovníkové útoky
- Komunikace se stroji na blocklistech
 - C2 servery, DeepS\EEK
- Vidí i do některých protokolů
 - HeartBleed, Mining
- (Retina)





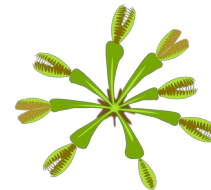
- NetFlow, IPFIX, sFLOW, ...
- DoS/DDoS amp, anomální provoz
- Statistická analýza
- Útočníci jsou automaticky blokováni (ExaFS)
- Útočníci z našich sítí jsou reportováni





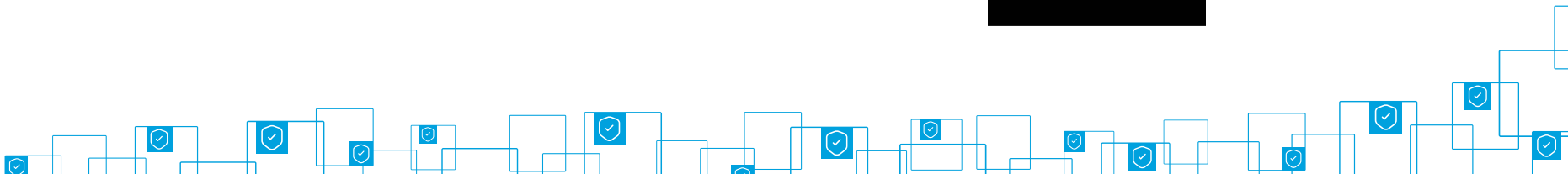
- Klasické

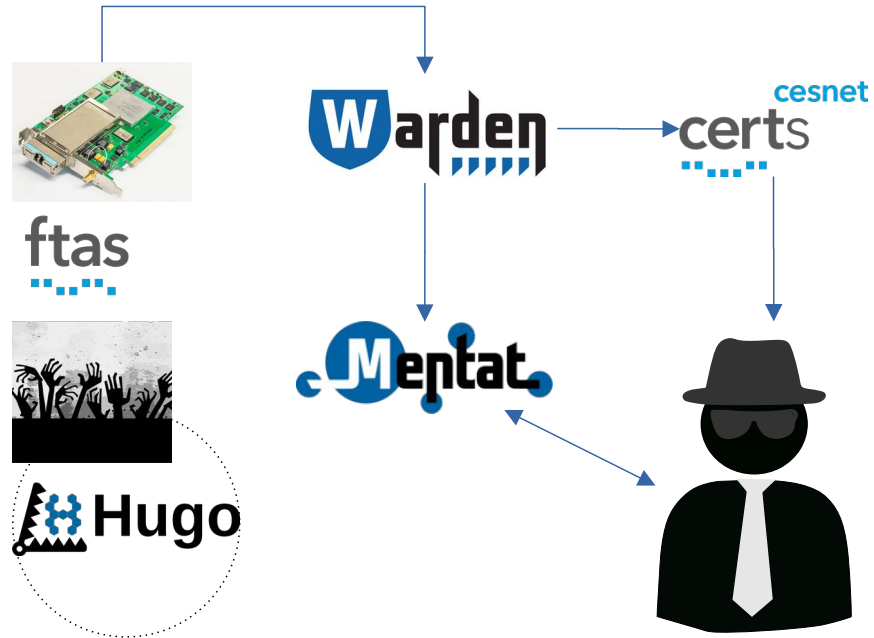
- Cowrie,
- Dionaea



- LaBrea

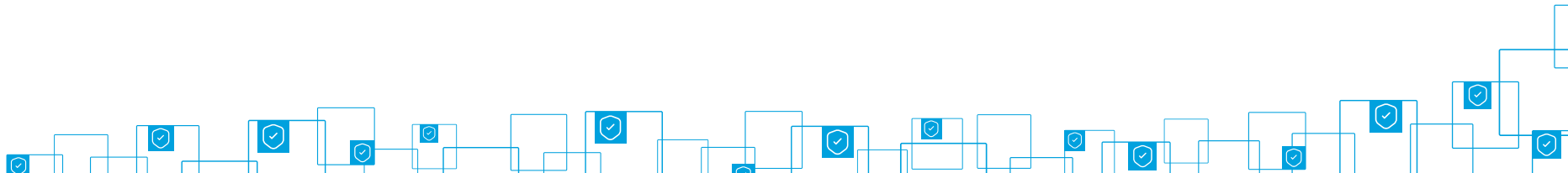
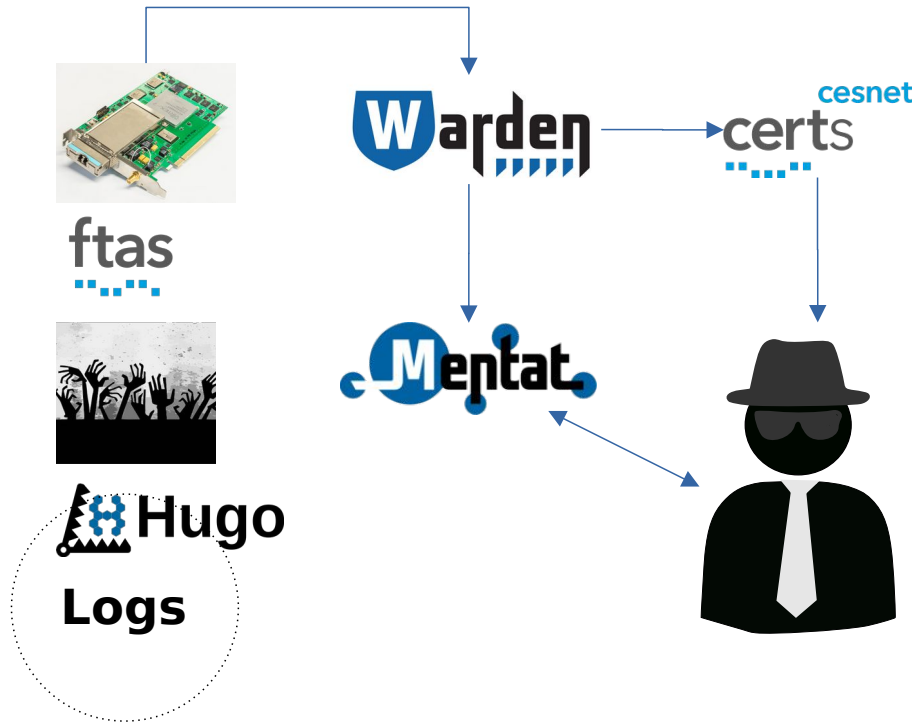
- Monitorování příchozího provozu na nikdy nepřidělených IP
- „Tarpitting“





- Honeypot as a service
 - 14 aktivních instancí
- Plug'n'play připojení do Wardenu
- (Virtualizace, docker, ...)
- Stačí nasměrovat provoz jedné/několika IP





- Aktivní systémoví démoni
(Postfix, Knot, Bind, Apache, Nginx)
- Autentizační a autorizační informace
(login, SSH, OIDC, Shibboleth, ...)
- Síťové události
(anomální provoz, zavřené porty, ...)
- Webové aplikace
(SQLi, Codei, pokusy o exploit, ...)

[06/Dec/2014:12:34:37 +0100]

195.113.134.228 grey.cesnet.cz

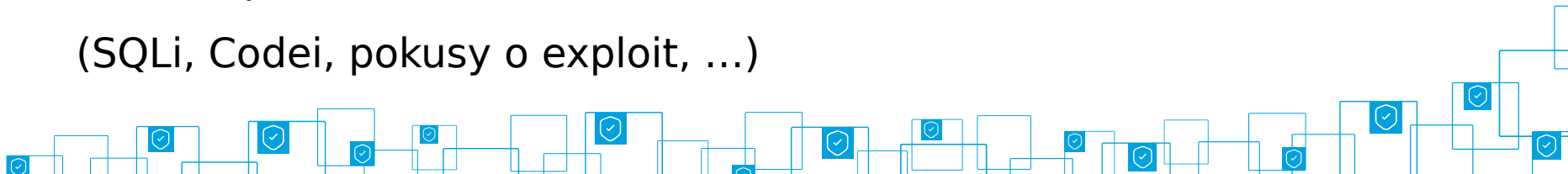
"GET /search?Gravity+free+download HTTP/1.1" 200 1986 "-"
"Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.14pre)
Gecko/20101204 Ubuntu/9.10 (karmic) Namoroka/3.6.14pre"

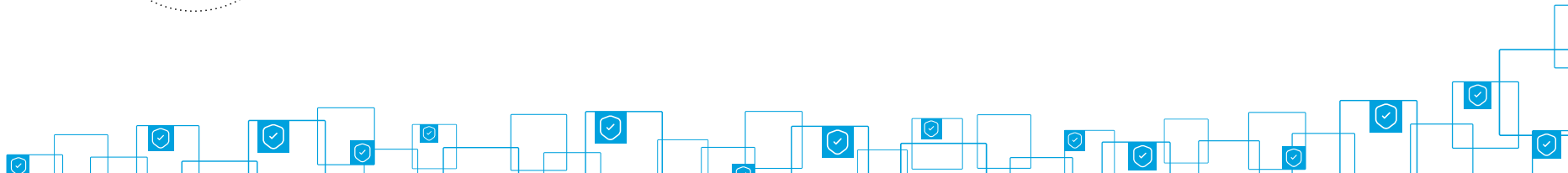
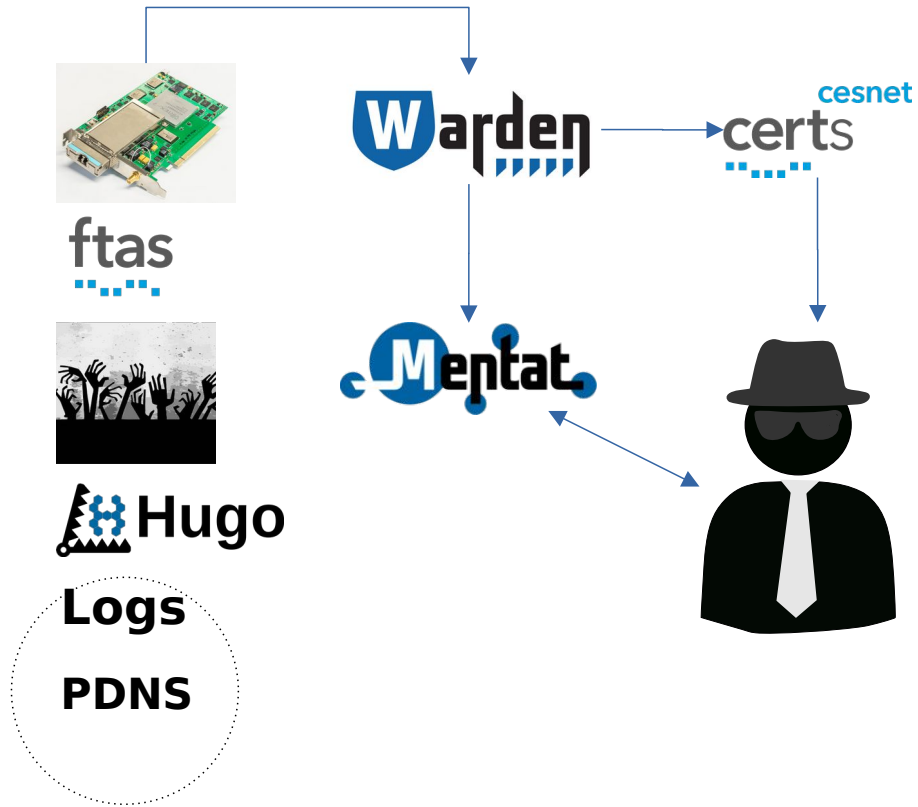
Nov 22 15:05:58 office2 postfix/smtpd[27935]: CAF18ED0073:
client=grey.cesnet.cz[2001:718:1:6::134:228],
sasl_method=LOGIN,
sasl_username=pavelk

Nov 22 15:05:58 office2 postfix/cleanup[30693]: CAF18ED0073:
message-id=<20131122140558.GC1700@cesnet.cz>

Nov 22 15:05:59 office2 postfix/qmgr[2599]: CAF18ED0073:
from=<ph@cesnet.cz>, size=7206, nrcpt=1 (queue active)

Nov 22 15:06:00 office2 postfix/smtp[31597]: CAF18ED0073:
to=<oleg@cesnet.cz>,
relay=postino.cesnet.cz[195.113.144.242]:25,
delay=2.1, delays=1/0/1/0.11, dsn=2.0.0,
status=sent (250 2.0.0 rAME5x59029798 Accepted for delivery)





- Historie DNS záznamů

- Z DNS transakcí na resolverech

- Příklady

- Jaký A záznam ukazuje na adresu a.b.c.d?
- Jaké záznamy existují v *cesnet.cz*?
- Jak se záznam měnil v čase?
Možná fastflux?
- Podobné jinému jménu?
Možná phishing?

[Search](#) [Match](#) [Analytics](#) [Phishing](#) [REST API](#)

[Logout](#)

PassiveDNS Search

Query:

78.128.211.46

Query type:

☒ IP ☐ domain

☐ domain & subdomains

Date limit:

Since: dd . mm . rrrr

Until: dd . mm . rrrr

[Search](#)

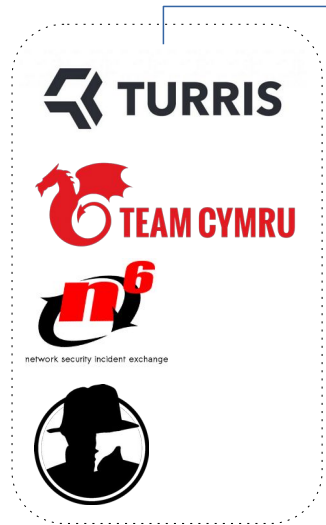
Elapsed time: 0.040385s

Page 1

IP	Domain	RTYPE	First seen	Last seen	Count	Details
78.128.211.46	vyzkumne-infrastruktury.cz	A	2021-06-07 13:21:33.157842	2022-05-03 09:22:11.964581	112	i
78.128.211.46	nren.cz	A	2022-02-14 10:59:54.483857	2022-04-08 09:05:02.337680	10	i
78.128.211.46	research-infrastructures.cz	A	2021-06-07 13:21:33.163023	2022-04-27 08:02:41.262069	29	i
78.128.211.46	30letinternetu.cz	A	2022-01-20 10:05:37.853247	2022-06-06 09:19:51.230190	203	i
78.128.211.46	www.cesnet.cz	A	2021-06-07 13:21:33.157842	2022-05-03 09:22:11.964581	112	i
78.128.211.46	cesnet.cz	A	2021-06-07 13:21:33.157842	2022-05-03 09:22:11.964581	112	i
46.211.128.78.in-addr.arpa	www.cesnet.cz	PTR	2021-06-07 13:21:33.157842	2022-05-03 09:22:11.964581	112	i
NODATA	46.211.128.78.in-addr.arpa	A	2021-06-07 13:21:33.157842	2022-05-03 09:22:11.964581	112	i
NODATA	46.211.128.78.in-addr.arpa	PTR	2021-06-07 13:21:33.157842	2022-05-03 09:22:11.964581	112	i

<https://passivedns.cesnet.cz>





ftas



Hugo

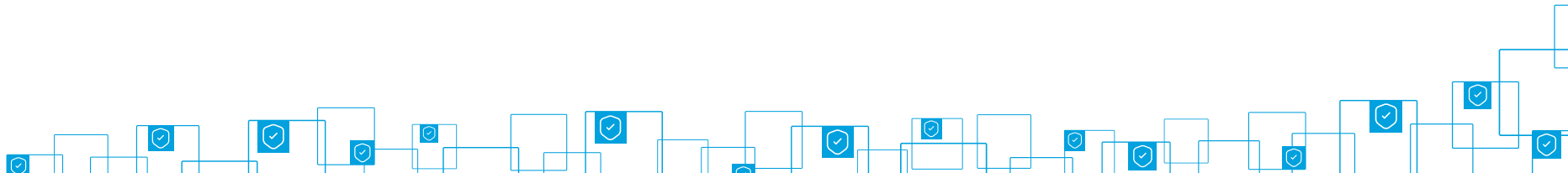
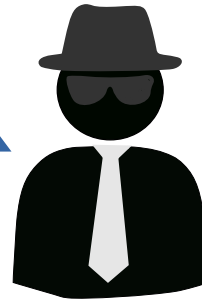
Logs

PDNS

Warden

Mentat

cesnet
certs

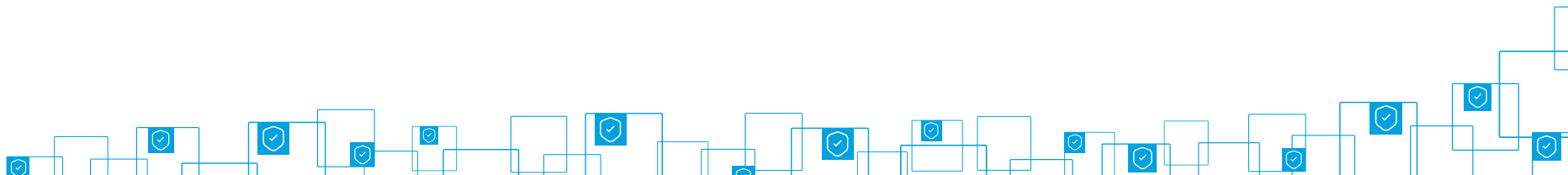


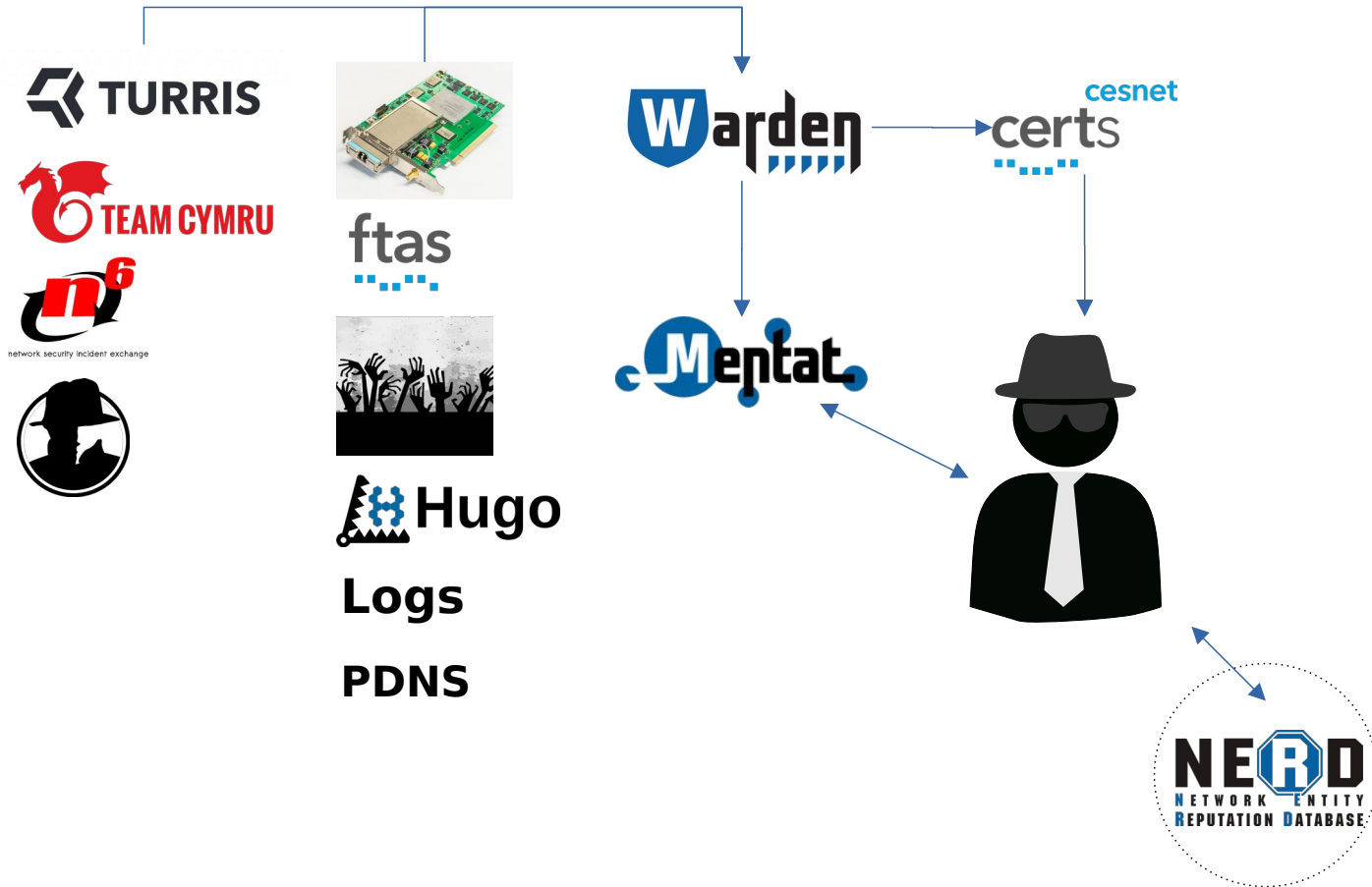


network security incident exchange



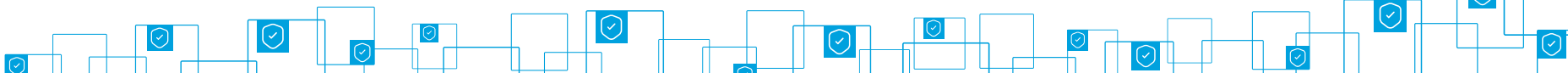
Shadowserver

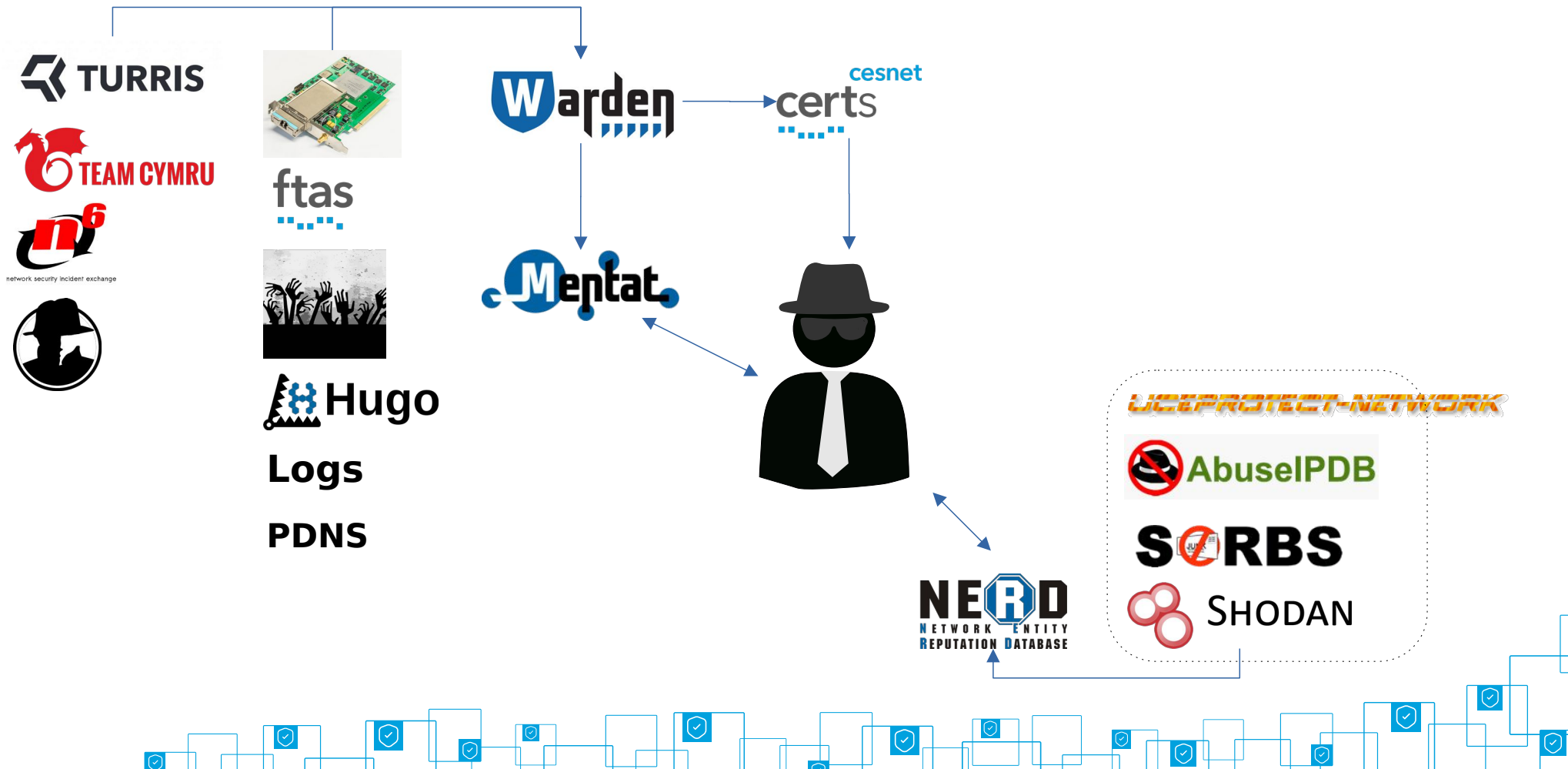




- Primární zdroje – Warden, MISP
- Data obohacená o externí zdroje
 - Speciálně ty, které nejdu stahovat hromadně
- Přepočítáno (ML) do reputačního skóre
 - Což je měřítko nebezpečnosti pro další den

IP address	Hostname	ASN	Country	Events	Rep. ^(?)	Other properties
193.46.255.83	hostingmailto236.statics.servermail.org	AS47890	 RO	5667 5 2 + 107496 DShield reports	0.501	4 blacklists Scanner 22, 111 scanner
196.251.72.53	--	AS401120	 SC	952 10 5 + 68344 DShield reports	0.492	7 blacklists Login attempts Scanner Malware 3389 self-signed
52.8.37.72	ec2-52-8-37-72.us-west-1.compute.amazonaws.com	AS16509	 US	297 5 2 + 4734 DShield reports	0.458	1 blacklist IP in hostname Scanner
93.123.109.163	--	AS48090 AS401116	 BG	271 4 2 + 4776 DShield reports	0.451	4 blacklists Scanner 22
176.65.148.238	chernobyl.network	AS51396	 NL	3471 6 3 + 18690 DShield reports	0.447	9 blacklists Scanner 22
88.210.63.67	--	AS211736	 UA	15211 6 4 + 17591 DShield reports + 3 OTX pulses	0.442	8 blacklists Scanner
146.190.174.211	--	AS14061	 US	1888 8 4 + 11612 DShield reports	0.441	4 blacklists Scanner Login attempts 22, 80, 443 cloud, open-dir
20.169.85.114	azpdweq95i0h.stretchoid.com	AS8075	 US	408 4 2 + 4132 DShield reports + 1 OTX pulses	0.435	3 blacklists Scanner
152.32.206.51	--	AS135377	 US	2297 4 2 + 9757 DShield reports	0.434	11 blacklists Scanner 22 scanner
91.199.163.52	--	AS16276 AS209272	 LT	28516 5 2 + 33580 DShield reports	0.428	2 blacklists Scanner
78.128.112.74	ip-112-74.4vendeta.com	AS202325 AS208637	 BG	7711 15 4 + 249791 DShield reports	0.427	8 blacklists IP in hostname Login attempts Scanner 22 scanner
45.135.232.24	--	AS198953	 RU	88911 12 2 + 2009579 DShield reports + 1 OTX pulses	0.426	4 blacklists Login attempts 135, 137, 139, 5985







www.blocklist.de



Exit nodes



DSshield



SHODAN



AbuseIPDB



censys



GeoIP
whois

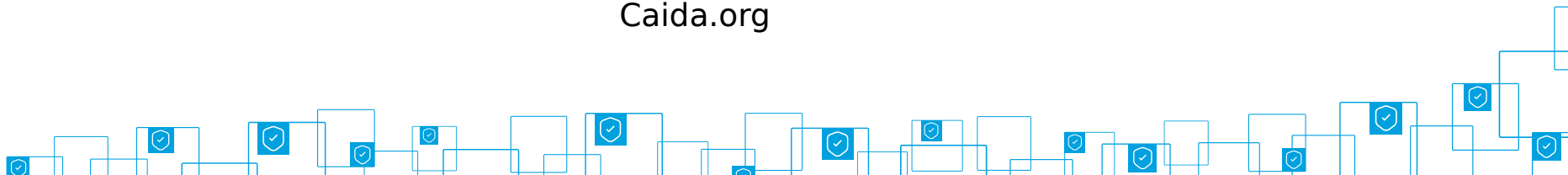
BGP+ASN



CIRCL
BGP Ranking

spamcop.net

Caida.org



- SNER (Slow Network Reconnaissance)

- Paralelní NMAP
- Nuclei
- Nessus
- ...

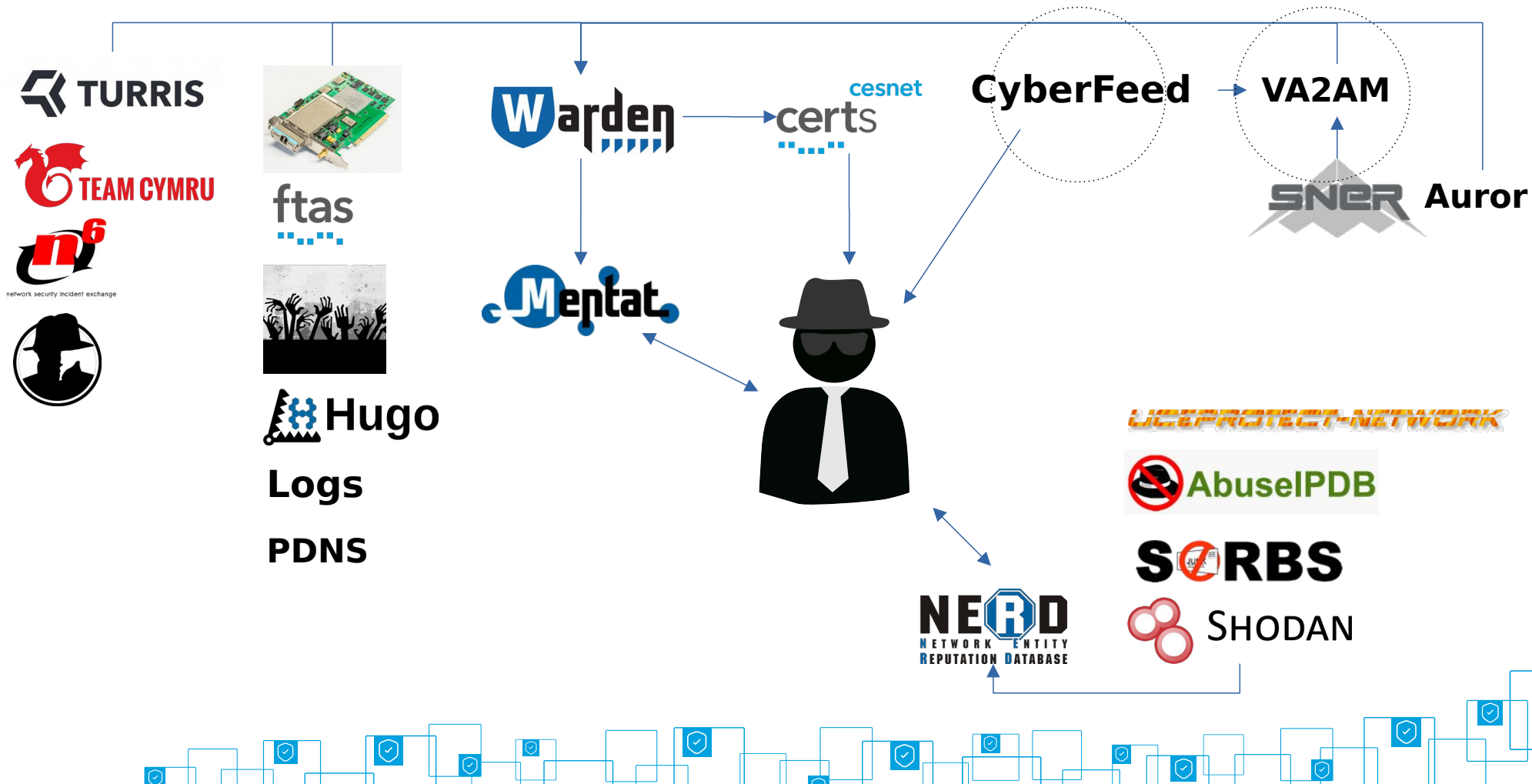
- 29187 hostů
60040 services

- Auror

- testssl.sh
- security.txt
- DNS

Search Network		Add Network		Table View		
Search network		Add network		Add	Expand All	Collapse All
Subnet (78.128.210.0/25)		sner/basic		auror		sner/nuclei
→ 78.128.210.0/25	   	✓		X		✓
Subnet (78.128.211.0/24)		sner/basic		auror		sner/nuclei
→ 78.128.211.0/24	   	✓		X		✓
Subnet (78.128.212.0/26)		sner/basic		auror		sner/nuclei
→ 78.128.212.0/26	  	✓		X		✓
Subnet (78.128.212.64/26)		sner/basic		auror		sner/nuclei
→ 78.128.212.64/26	EXPAND   	✓		X		✓
↳ 78.128.212.92/32	   	✓		X		✓

<https://sner.flab.cesnet.cz>





- **TARANIS** NG



GitLab opravuje 11 zranitelností

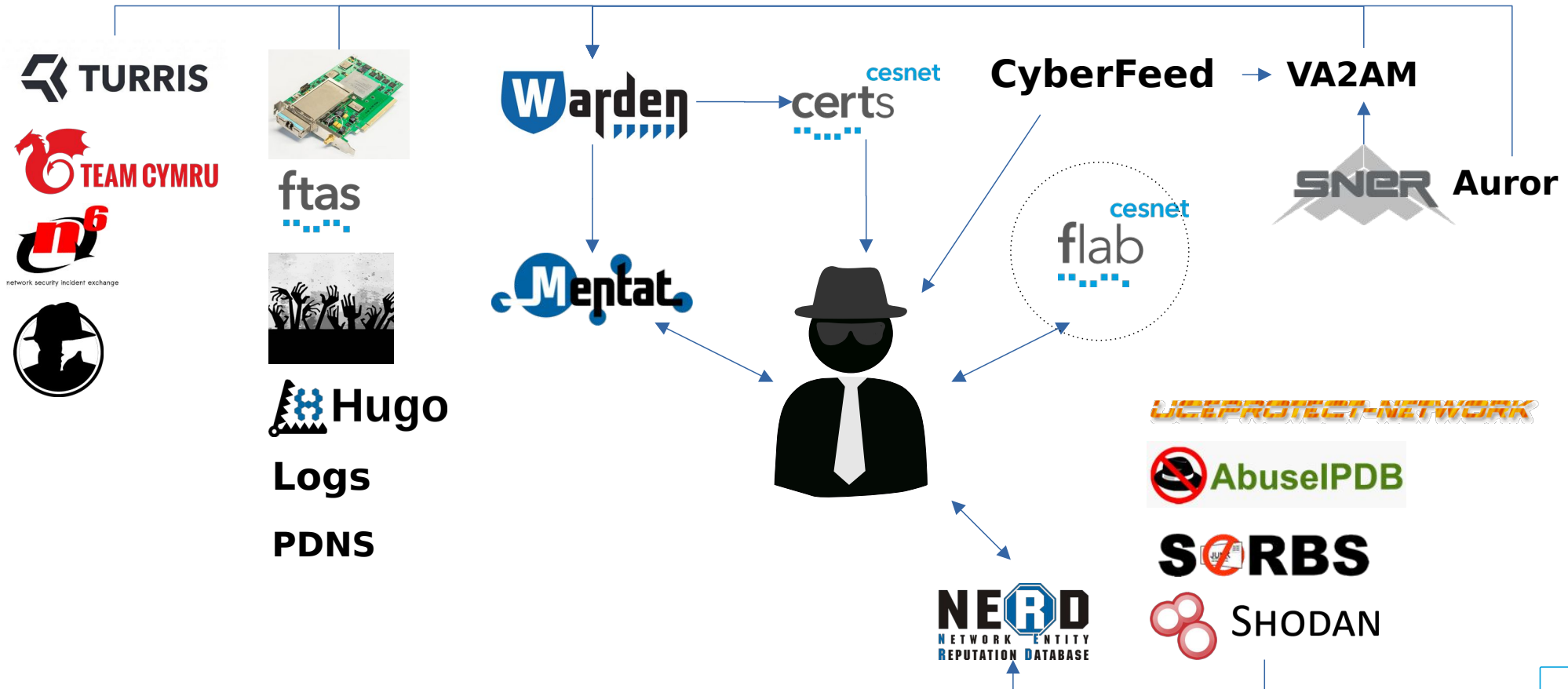
Max CVSS 9.9 (Critical)

Publikované dňa 24. 9. 2026.

- Sledování zdrojů o zranitelnostech
- Prioritizace, kompletace, zhodnocení
- Web, Mail, RSS – ~ 400 reportů a ~ 800 CVE za rok
- VA2AM
 - Hledání zranitelných verzí ve výsledcích skenování
 - Warden → Mentat → Reporting

<https://cyberfeed.cesnet.cz>

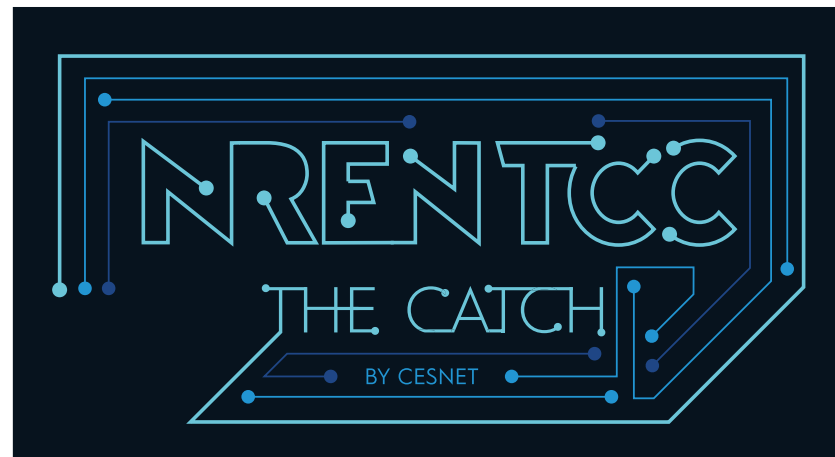




- Forenzní laboratoř
- Penetrační testy (5 FTE pentesterů)
- Sociální inženýrství
- Phishingator
 - 26 instancí, 75 tis. emailů za 2025
 - ~ 3 testy na klíč ročně
- The Catch – 5. 10. 12:00:00 UTC
 - 10. ročník, 30 let CESNETU → téma NREN
 - Loni 522 registrovaných, 19 dohrálo
- Školení
- (Čerstvě medaile ze SANS)

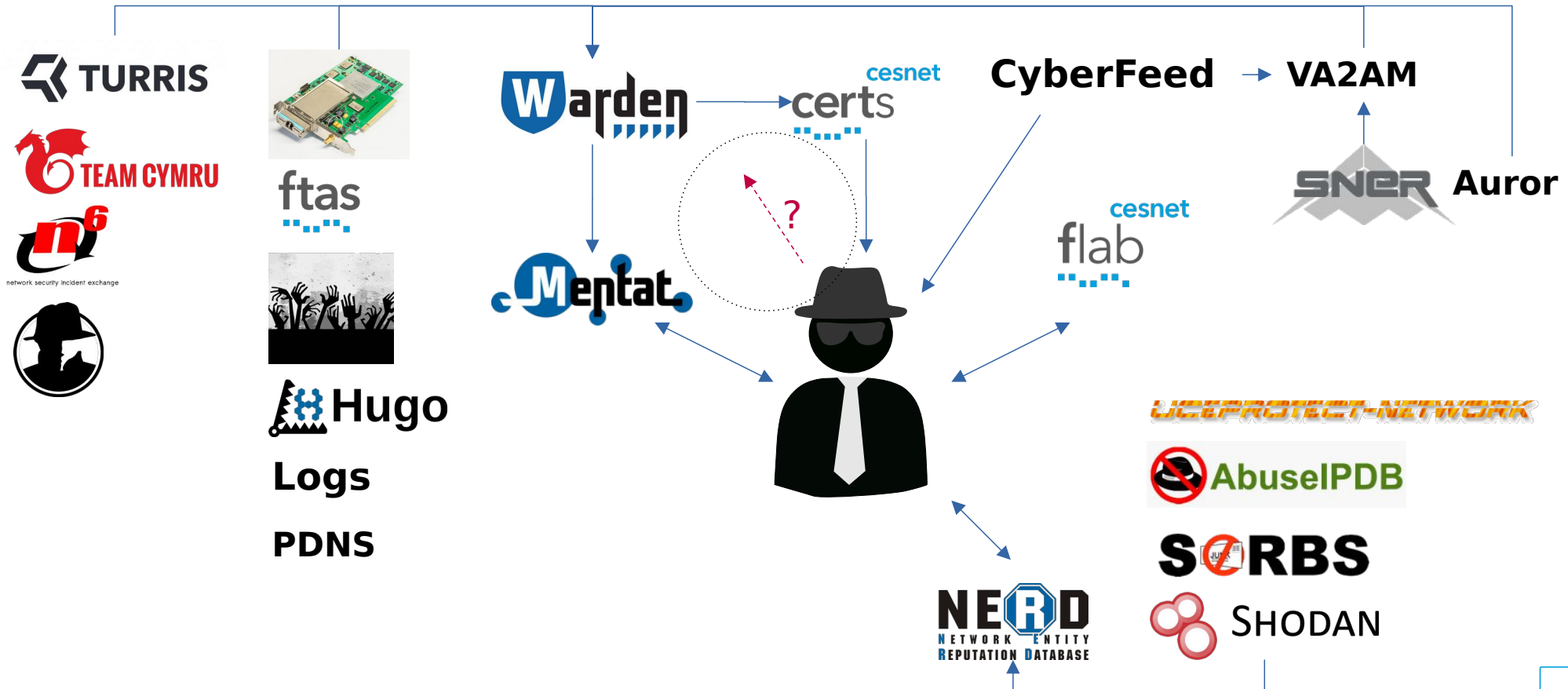
<https://flab.cesnet.cz>

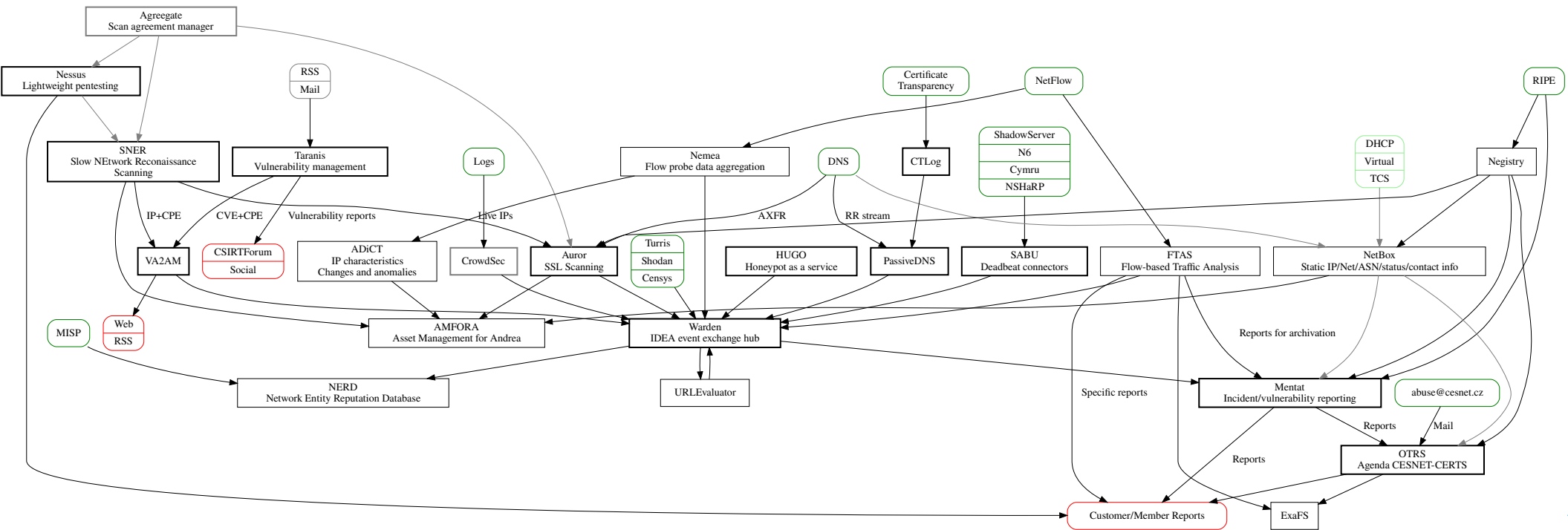
<https://phishingator.cesnet.cz>

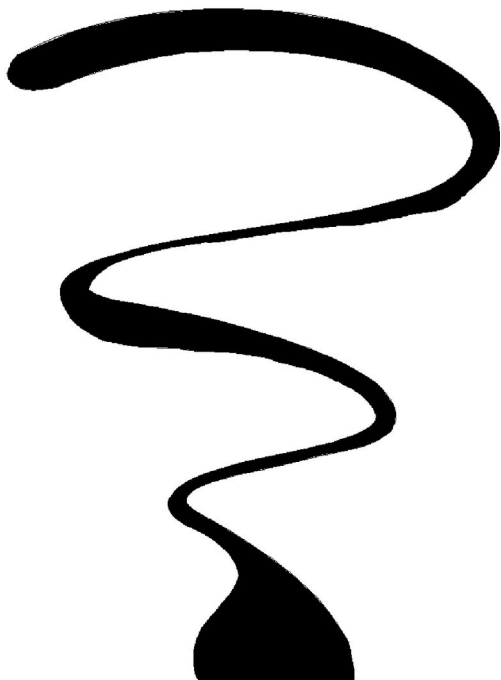


<https://thecatch.cz>









Warden:	https://warden.cesnet.cz
IDEA:	https://idea.cesnet.cz
Mentat:	https://mentat.cesnet.cz
HUGO	https://hugo.cesnet.cz
FLAB:	https://flab.cesnet.cz
Phishingator:	https://phishingator.cesnet.cz
TheCatch:	https://thecatch.cz
SNER:	https://sner.flab.cesnet.cz
CyberFeed:	https://cyberfeed.cesnet.cz
PassiveDNS:	https://passivedns.cesnet.cz
NERD:	https://nerd.cesnet.cz
Nemea:	https://nemea.liberrouter.org

sec-op@cesnet.cz