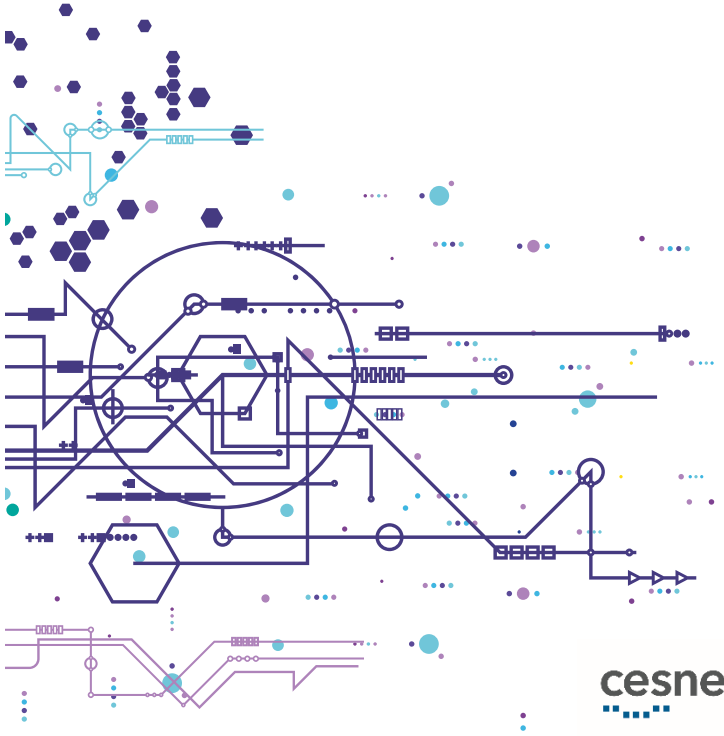
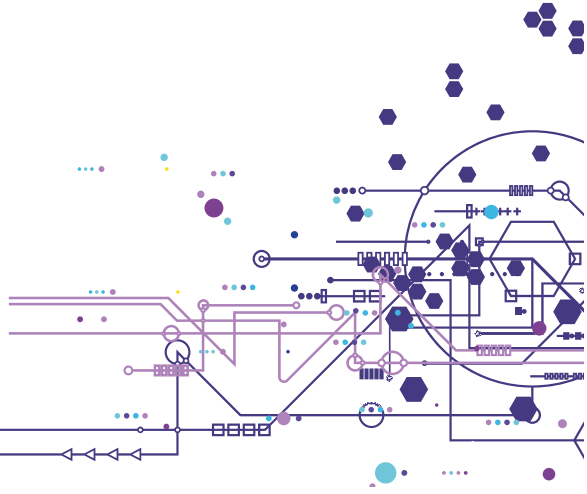
Bezpečnost

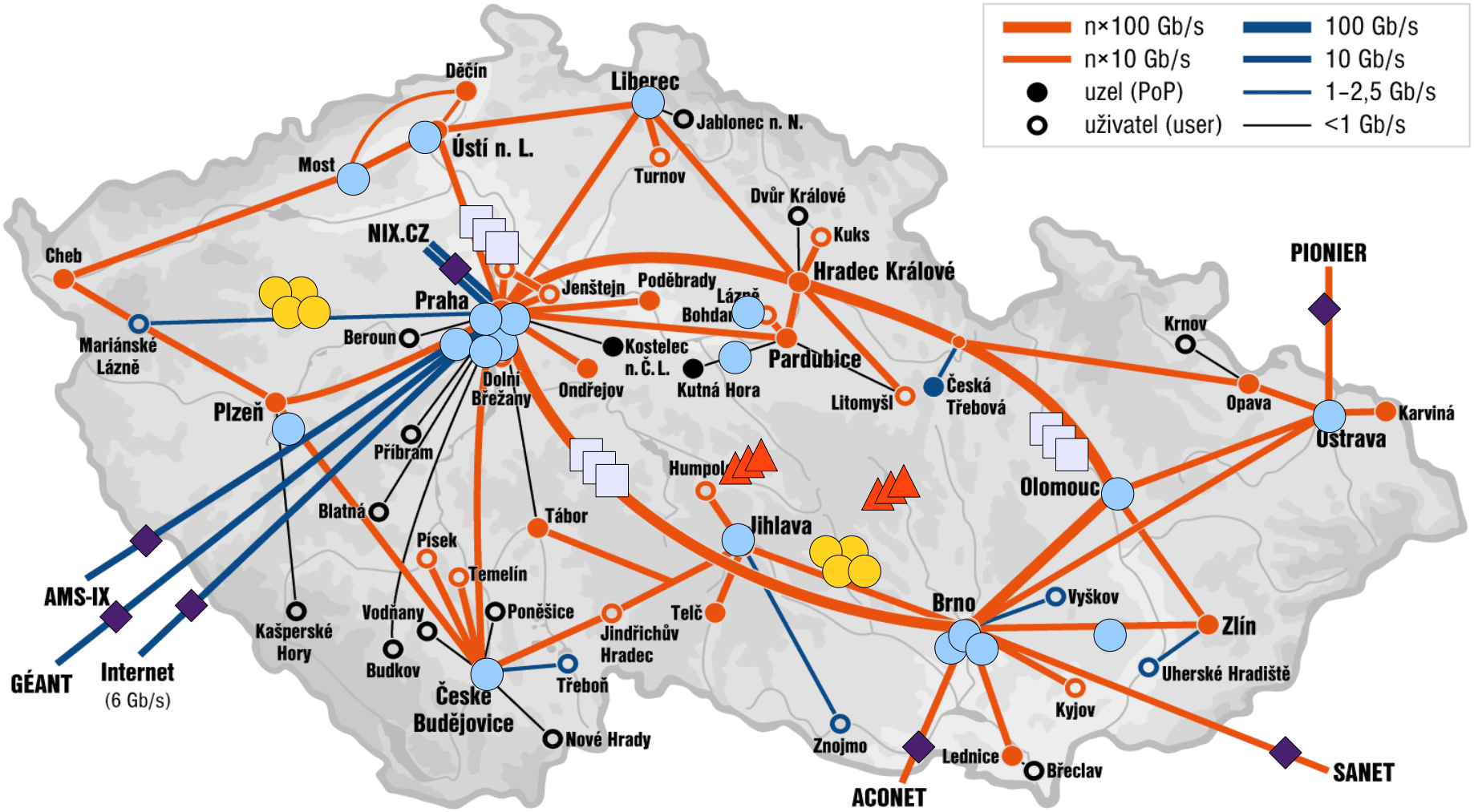
Andrea Kropáčová
andrea@cesnet.cz





- Bezpečnostní monitoring a obrana
- Sběr, zpracování a sdílení bezpečnostních událostí
- Bezpečnostní týmy a role
- Další služby v oblasti bezpečnosti

Bezpečnostní monitoring



- HW accelerated probes
- large scale (backbone-wide) flow based monitoring (NetFlow data sources)
- Honey Pots
- IDS, IPS, tar pit based systems, etc..
- SNMP based monitoring

Sondy

- Celkem 8 linek
- Export IP flow data v IPFIX formátu (pomocí flowmonexp a ipfixprobe), informace o paketových statistikách, TLS spojeních, QUIC spojeních, detekci VPN
- Průměrně 120K biflow za sekundu (ipfixprobe), jednosměrných kolem 200K toků (flowmonexp)
- On-demand sběr vzorků provozu k bezpečnostní analýze/výzkumu
- Detekované události/typy provozu: např. cryptomining, bruteforce, malware, verikální skeny
- 260k událostí denně (3,0 za sekundu) ze 3 detektorů
  - kategorie: 93,4% scan, 6,2% login attempt, 0,4% (D)DoS
- Celkem je to 54% všech netestovacích zpráv ve Wardenu

Bezpečnostní monitoring

- **FTAS (Flow Trafic Analysis System)**
  - Detekce pro základní síťové útoky a anomálie (základní principy)
    - události směrem dovnitř připojené sítě – regulujeme, blokujeme, zahazujeme
      - automaticky ovládá **exaFS**
    - události mající původ uvnitř připojené sítě – notifikujeme
- **Služba exaFS** – rozhraní pro aplikaci BGPflowspec a RTBH
  - regulace provozu ***z*** nebo ***do*** prefixů připojených organizací
  - webový i-face, nebo API pro strojové ovládání
  - součástí je proškolení uživatele (správce) připojené organizace
  - sluzby@cesnet.cz
- **Služba FTAS** (3 varianty)
  - zpřístupnění dat týkající se konkrétní instituce (z hraničních boxů), uvidíte provoz, který protekl infrastrukturou, tj. provoz mezi „námi a vámi“
  - export vlastních dat do hlavní instance (exkluzivní přístup pouze v vlastním datům konkrétní připojené organizace)
  - dedikovaná instance v síti organizace (typicky velké univerzity)

Informační využití BM

Co sledujeme:

- perimetr sítě, vstup, výstup
- IP provoz v páteři
- provoz „od nás ven“
- podvrhávání zdrojových adres
- skenování portů, synflood útoky
- útoky hrubou silou na ssh, SIP, DNS tunely
- DNS amplifikace, NTP, SNMP amplifikace
- anomální datové přenosy, paketové rychlosti
- provoz vybraných prvků infrastruktury (distribuované infrastruktury, např. Datová Úložiště, Gridy)
- klíčové služby (DSN, AAI)
- ... „on-demand“ ...

Informační využití:

- informace o uskutečněném provozu
- automatická detekce anomálií
- on-the-fly detekce útoků
- odhalení podvržení adres
- verifikace, analýza bezpečnostních incidentů
- vzorky dat, ladění sítě
- obrana sítě, služeb a uživatelů
- systematické sledování provozu instituce
- náhled na provoz sítě
- zdraví, vytížení sítě
- architektura sítě, její optimalizace a rozvoj
- statistiky provozu

BM a síťová obrana

- Bezpečnostní prvky a mechanismy na bázi specifického nastavení a architektury sítě
- Pokročilý monitoring a detekce anomálií ve všech vrstvách a topologických částech sítě
  - na vnějším perimetru sítě
  - v páteřní infrastruktuře
  - na perimetru mezi páteří a připojenými institucemi
  - v koncových sítích hostujících služby

- Základní strategie a principy
  - zamezit zahlcení páteře
  - zamezit zahlcení uživatelských přípojek
  - zamezit zahlcení externích propojení tam, kde je to v principu možné
  - identifikovat a eliminovat nelegitimní provoz v síti
  - ošetřit anomální jevy na úrovni síťového transportu s minimalizací rizik spojených s potenciálním false-positive vyhodnocením jevů
  - ACL, policing, RPKI, kontrola zdrojových adres, RTBH, DoS protector, BGP flowspec

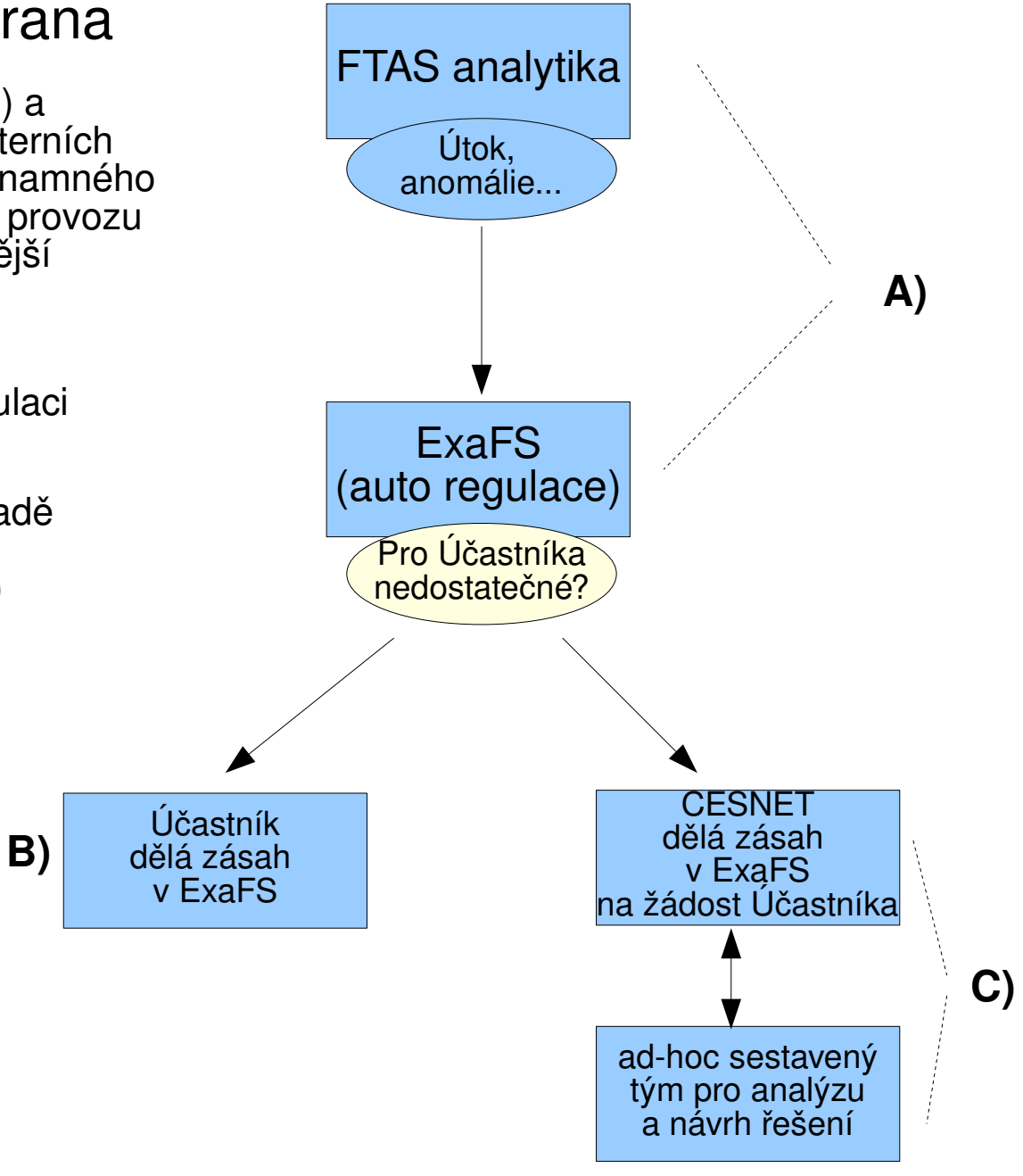
BM a síťová obrana

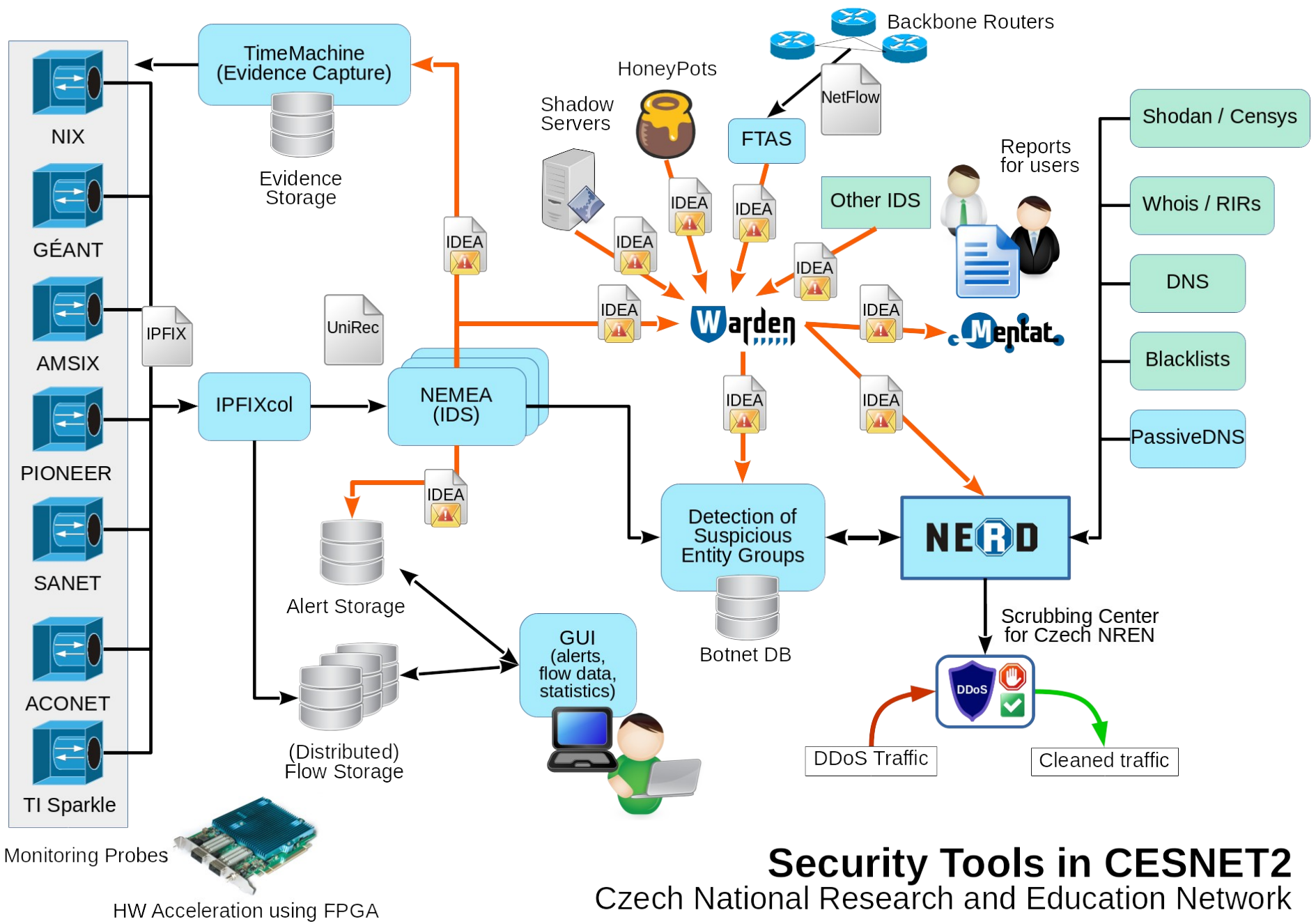
- Bezpečnostní monitoring a obrana

A) Automatická globální regulace (event driven*) a eliminace nežádoucího provozu a útoků z externích sítí (DoS volumetrické a agresivní útoky) významného objemu a dalších anomálních jevů v síťovém provozu páteřní infrastruktury (dlouhodobé / agresivnější skeny, podvržení IP adres komunity, validita oznamovaných prefixů apod.).

B) Poskytnutí nástroje pro samo-obslužnou regulaci provozu Účastníkem (ExaFS)

C) Zahájení řešení provozního opatření na základě uživatelského požadavku (např. eliminace nestandardního provozu z/do sítě Účastníka)





Security Tools in CESNET2

Czech National Research and Education Network

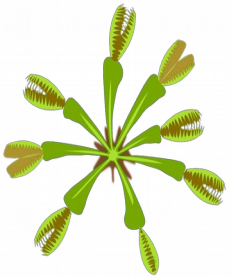
Naše zdroje… a nejen naše

ftas

Sondy + Nemea

Cowrie

Dionaea



Fail2Ban

LaBrea

Shadowserver

UCEPROTECT-NETWORK

NSHARP

NETWORK SECURITY HANDLING AND RESPONSE PROCESS

Flowmon Networks

TREND MICRO™

TEAM CYMRU

národní centrum kybernetické bezpečnosti

TippingPoint

warden

- https://warden.cesnet.cz
- Platforma pro automatizované sdílení informací o incidentech
- Zapisující konektory zasílají události do „fronty“
- Čtoucí konektory odebírají vše, co se objevilo
- Jednotný formát (https://idea.cesnet.cz)
- Kdo ostatním poskytuje data, dostane se k datům ostatních

mentat

warden-info@cesnet.cz
mentat-info@cesnet.cz

- https://mentat.cesnet.cz
- Jednotné automatizované zpracování
- Zpřístupňuje informace lidským způsobem přes GUI
- Příklad: DDoS
  - Informace dorazí přes FTAS, sondy a LaBreu do Wardenu
  - Mentat zagreguje informace z různých zdrojů
  - … a roztřídí podle zdrojů útoku
  - Jednotlivé organizace dostanou specifický report o svých IP

Reporty

Date: Mon, 19 Apr 2021 21:20:06 +0200 (CEST)
From: CESNET-CERTS Reporting <reporting@cesnet.cz>
Subject: [M20210419SL-U4TEN] Nízká - Upozornění na možné problémy ve Vaší síti
Reply-To: abuse@cesnet.cz

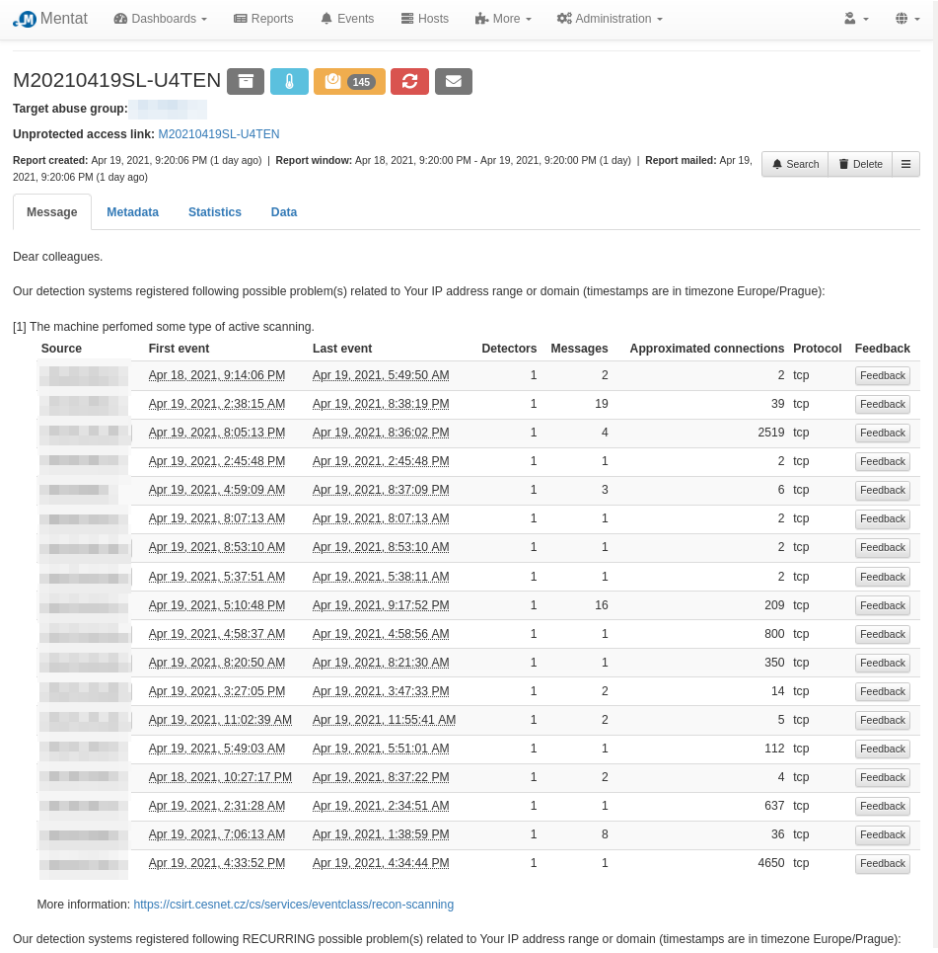
Vážení kolegové.

Naše detekční systémy zaznamenaly následující možné problém(y) související s Vaším rozsahem IP adres nebo Vaší doménou (uvedené časy jsou v časové zóně Europe/Prague):

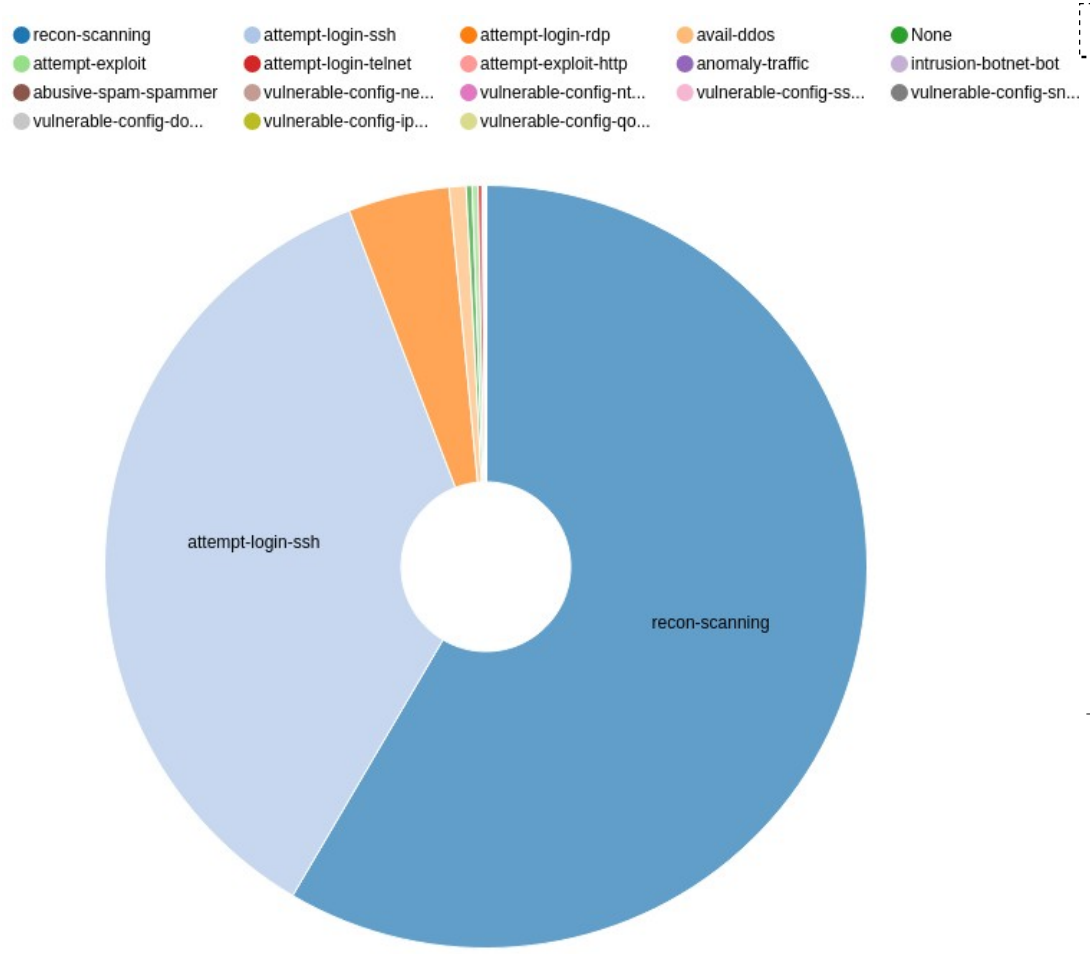
[1] Stroj se pokoušel o nějakou formu aktivního skenování.

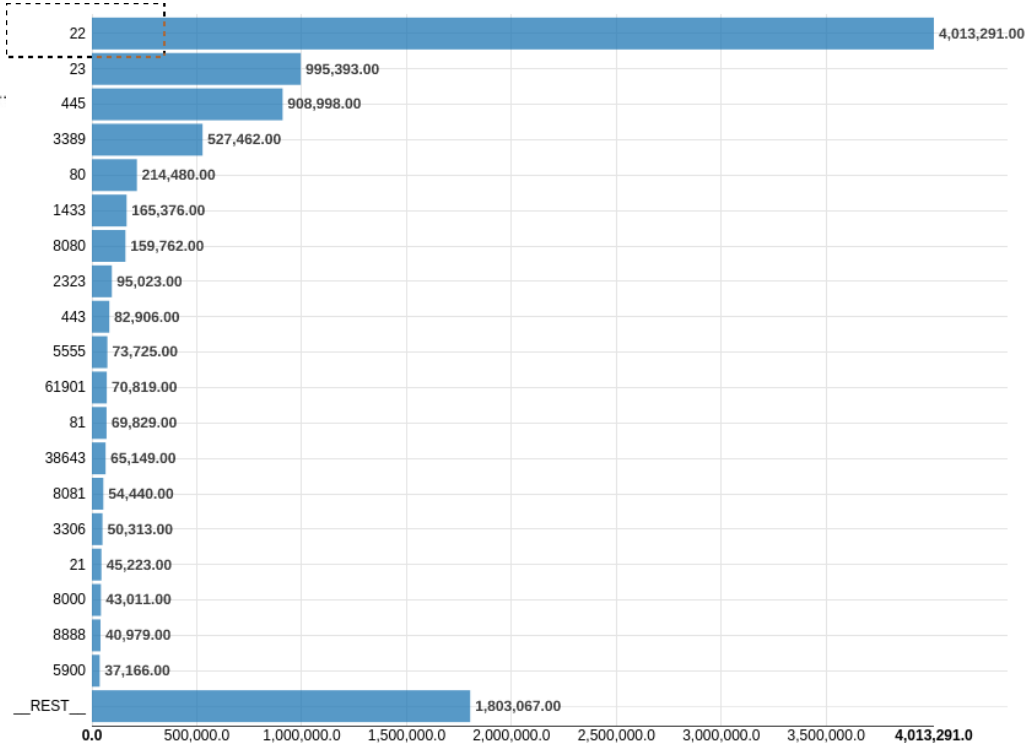
Zdroj	První událost	Poslední událost	Detekt	Zpráv	Protokol
[redacted]	18.04. 21:14:06	19.04. 05:49:50	1	2	tcp
	19.04. 02:38:15	19.04. 20:38:19	1	19	tcp
	19.04. 20:05:13	19.04. 20:36:02	1	4	tcp
	19.04. 14:45:48	19.04. 14:45:48	1	1	tcp
	19.04. 04:59:09	19.04. 20:37:09	1	3	tcp
	19.04. 08:07:13	19.04. 08:07:13	1	1	tcp
	19.04. 08:53:10	19.04. 08:53:10	1	1	tcp
	19.04. 05:37:51	19.04. 05:38:11	1	1	tcp
	19.04. 17:10:48	19.04. 21:17:52	1	16	tcp
	19.04. 04:58:37	19.04. 04:58:56	1	1	tcp
	19.04. 08:20:50	19.04. 08:21:30	1	1	tcp
	19.04. 15:27:05	19.04. 15:47:33	1	2	tcp
	19.04. 11:02:39	19.04. 11:55:41	1	2	tcp
	19.04. 05:49:03	19.04. 05:51:01	1	1	tcp
	18.04. 22:27:17	19.04. 20:37:22	1	2	tcp
	19.04. 02:31:28	19.04. 02:34:51	1	1	tcp
	19.04. 07:06:13	19.04. 13:38:59	1	8	tcp
	19.04. 16:33:52	19.04. 16:34:44	1	1	tcp

Více informací: https://csirt.cesnet.cz/cs/services/eventclass/recon-scanning



Zdraví sítě


recon-scanning
attempt-login-ssh
attempt-login-rdp
avail-ddos
None
attempt-exploit
attempt-login-telnet
attempt-exploit-http
anomaly-traffic
intrusion-botnet-bot
abusive-spam-spammer
vulnerable-config-ne...
vulnerable-config-nt...
vulnerable-config-ss...
vulnerable-config-sn...
vulnerable-config-do...
vulnerable-config-ip...
vulnerable-config-qo...
attempt-login-ssh
recon-scanning


22
4,013,291.00
23
995,393.00
445
908,998.00
3389
527,462.00
80
214,480.00
1433
165,376.00
8080
159,762.00
2323
95,023.00
443
82,906.00
5555
73,725.00
61901
70,819.00
81
69,829.00
38643
65,149.00
8081
54,440.00
3306
50,313.00
21
45,223.00
8000
43,011.00
8888
40,979.00
5900
37,166.00
__REST__
1,803,067.00
0.0
500,000.0
1,000,000.0
1,500,000.0
2,000,000.0
2,500,000.0
3,000,000.0
3,500,000.0
4,013,291.0

NERD
NETWORK ENTITY REPUTATION DATABASE

- https://nerd.cesnet.cz
- Databáze síťových entit (IP adresy, sítě, domény, …)
- Seznam nám známých zdrojů škodlivých aktivit
  … a všeho, co o nich víme
- Primární zdroj – Warden, MISP. Data jsou obohacena o další informace z externích zdrojů
- Shrnutí všech informací do reputačního skóre, predikce míry hrozby entity pro následující den (strojové učení z dostupných dat)

PassiveDNS

- DNS odráží okamžitý stav – Passive DNS udržuje historii
- Sleduje DNS transakce a staví databázi
- Příklady využití
  - Jaké všechny jmenné záznamy ukazují na IP a.b.c.d?
  - Jaké záznamy známe v doméně example.org?
  - Jak se měnilo doménové jméno v čase? Není to fast-flux?
  - Není příliš podobné existujícímu jménu? Nejde o phishing?

Known IP addresses

IP prefix & Hostname suffix & Country code & ASN

Event category

Blacklist & Tag Min tag confidence 0.5

Sort by Reputation score Ascending

Max number of addresses 20

Submit Query

Results (≥20)

IP address	Hostname	ASN	Country	Events	Rep.	Other properties	Time added	Last event	Links
194.165.16.67	--	AS48721	MC	5839 8 3	0.992	Scanner blocklist_de-ssh abuseipdb	2021-03-19 06:48:57	2021-04-21 13:24:05	
194.165.16.42	--	AS48721	MC	11536 8 4	0.982	Scanner	2021-02-16 18:57:15	2021-04-21 13:19:31	
81.161.63.253	--	AS202984	CN	3061 6 4	0.961	Scanner Login attempts DShield uceprotect blocklist_de-ssh abuseipdb ciarmy	2020-11-07 14:01:19	2021-04-21 11:50:17	
171.67.71.100	research.esrg.stanford.edu	AS32	US	19689 6 2	0.953	Scanner ciarmy abuseipdb	2021-03-05 19:07:44	2021-04-21 14:00:50	
156.96.113.109	--	AS46664	US	1333 5 2	0.944	Scanner spamhaus-sbl spamhaus-drop spamhaus-pbl-isp abuseipdb	2021-03-09 00:28:14	2021-04-20 06:48:05	
89.248.165.134	recyber.net	AS202425	GB	30588 5 2	0.943	Scanner dshield ciarmy abuseipdb	2021-03-02 20:34:25	2021-04-21 13:59:28	
23.148.145.7	--	AS46664	US	4145 5 2	0.942	Scanner ciarmy	2021-03-01 17:21:55	2021-04-21 03:33:44	
81.161.63.100	--	AS202984	CN	3567 6 4	0.942	Scanner DShield Login attempts uceprotect blocklist_de-ssh abuseipdb ciarmy bruteforceblocker	2020-11-09 17:41:05	2 hours ago 13:28:51	
89.248.168.176	security.criminalip.com	AS29073 AS202425	NL	5821 5 2	0.937	Scanner DShield Research scanner dshield ciarmy abuseipdb	2019-05-21 07:09:03	2021-04-21 11:51:08	
221.181.185.19	--	AS56046	CN	3806 7 3	0.937	Scanner Login attempts DShield blocklist_de-ssh abuseipdb spamhaus-xbl-cbl uceprotect	2020-12-07 14:28:54	2021-04-21 08:22:25	
222.187.232.205	--	AS4134	CN	2038 4 2	0.937	Login attempts Scanner spamhaus-pbl sorbs-dul uceprotect blocklist_de-ssh abuseipdb spamhaus-xbl-cbl	2021-03-10 10:23:46	2021-04-21 13:56:49	
221.181.185.135	--	AS56046	CN	4370 7 3	0.937	Login attempts Scanner DShield blocklist_de-ssh abuseipdb spamhaus-xbl-cbl uceprotect	2020-12-07 14:46:24	2021-04-21 07:26:24	
81.161.63.103	--	AS202984	CN	2368 5 3	0.937	Scanner DShield Login attempts blocklist_de-ssh uceprotect bruteforceblocker abuseipdb ciarmy	2020-11-09 13:38:08	2021-04-21 12:21:59	
221.181.185.153	--	AS56046	CN	1271 4 2	0.937	Scanner Login attempts uceprotect blocklist_de-ssh abuseipdb spamhaus-xbl-cbl	2021-03-26 04:05:03	2021-04-21 07:31:33	
45.148.10.50	--	AS48090	NL	2743 6 4	0.937	Scanner abuseipdb ciarmy uceprotect spamhaus-xbl-cbl	2021-04-07 13:14:25	2021-04-21 14:00:03	
118.126.65.27	--	AS45090	CN	2863 5 2	0.936	Scanner ciarmy uceprotect	2021-02-05 09:12:49	2021-04-21 14:00:19	
209.141.45.200	joseph.kreed.org	AS53667	US	5016 7 3	0.935	Scanner abuseipdb ciarmy spamhaus-xbl-cbl uceprotect bruteforceblocker	2021-04-06 19:43:35	2021-04-20 17:03:36	
89.248.169.12	security.criminalip.com	AS202425	NL	2958 5 2	0.934	Scanner DShield Research scanner uceprotect ciarmy spamhaus-xbl-cbl	2019-05-10 09:15:28	2021-04-21 10:16:08	
92.63.197.71	--	AS60307 AS12695 AS204655 AS44446	RU	18353 5 2	0.933	Scanner DShield ciarmy dshield abuseipdb	2020-07-27 18:33:29	2021-04-21 13:57:29	
222.187.239.109	--	AS4134	CN	1142 4 2	0.932	Login attempts Scanner spamhaus-pbl sorbs-dul uceprotect blocklist_de-ssh abuseipdb spamhaus-xbl-cbl	2021-03-26 03:50:03	2021-04-21 12:27:12	

NERD
NETWORK ENTITY REPUTATION DATABASE

- https://nerd.cesnet.cz
- Databáze síťových entit (IP adresy, sítě, domény, …)
- Seznam nám známých zdrojů škodlivých aktivit
  … a všeho, co o nich víme
- Primární zdroj – Warden, MISP. Data jsou obohacena o další informace z externích zdrojů
- Shrnutí všech informací do reputačního skóre, predikce míry hrozby entity pro následující den (strojové učení z dostupných dat)

PassiveDNS

- DNS odráží okamžitý stav – Passive DNS udržuje historii
- Sleduje DNS transakce a staví databázi
- Příklady využití
  - Jaké všechny jmenné záznamy ukazují na IP a.b.c.d?
  - Jaké záznamy známe v doméně example.org?
  - Jak se měnilo doménové jméno v čase? Není to fast-flux?
  - Není příliš podobné existujícímu jménu? Nejde o phishing?

PassiveDNS Search

Query:

78.128.211.46

Query type: IP domain domain & subdomains

Date limit:

Since: 03 / 29 / 2021

Until: 03 / 30 / 2021

Search

Elapsed time: 0.039217s

Page 1

IP	Domain	RTYPE	First seen	Last seen	Count	Source
78.128.211.46	www.cesnet.cz	A	2021-03-29 00:10:02.344920	2021-03-29 23:55:02.227642	256	ns.ces.net
78.128.211.46	www.cesnet.cz	A	2021-03-29 00:03:44.595298	2021-03-29 23:44:05.743237	170	adns2.cesnet.cz
78.128.211.46	www.cesnet.cz	A	2021-03-29 00:08:23.365356	2021-03-29 23:59:32.152469	202	adns1.cesnet.cz
78.128.211.46	cesnet.cz	A	2021-03-29 00:05:03.948795	2021-03-29 23:55:03.869946	157	adns1.cesnet.cz
78.128.211.46	cesnet.cz	A	2021-03-29 01:57:39.927095	2021-03-29 21:14:09.949594	20	ns.ces.net
78.128.211.46	cesnet.cz	A	2021-03-29 10:45:44.954685	2021-03-29 22:48:07.111438	6	adns2.cesnet.cz
46.211.128.78.in-addr.arpa	www.cesnet.cz	PTR	2021-03-29 00:52:25.640564	2021-03-29 22:32:58.246510	25	adns1.cesnet.cz
46.211.128.78.in-addr.arpa	www.cesnet.cz	PTR	2021-03-29 00:56:14.486300	2021-03-29 23:30:15.149114	15	adns2.cesnet.cz
NODATA	46.211.128.78.in-addr.arpa	A	2021-03-29 00:56:14.485409	2021-03-29 21:41:20.626957	10	adns2.cesnet.cz
NODATA	46.211.128.78.in-addr.arpa	A	2021-03-29 00:52:25.640190	2021-03-29 23:27:03.394540	16	adns1.cesnet.cz

Sběr, analýza a sdílení dat ...
... trocha čísel

- **Warden**
  - ~ **1.6** milionu událostí za den
  - (pouze **0.4 %** CESNET + partneři)
  - **26** zdrojů

- **NERD**
  - ~ **800 000** IP
  - ~ **115 000** BGP
  - ~ **16 000** ASN
  - ~ **38 000** CIDR
  - ~ **16 000** organizací

- **Mentat**
  - ~ **30** reportů za týden
  - pro ~ **300** organizací

- **PassiveDNS**
  - ~ **129** milionů záznamů za den

Pro Vás

- Většina služeb je dostupná veřejně
  - Některé jen pro členy bezpečnostních týmů (Mentat)
  - Některé s podmínkami („dejte, dáme“ :)) (Warden)
- Většina dat je také přístupná přes API
- Rádi pohovoříme o požadavcích, zvážíme zakomponování úprav, nebojte se ozvat

Pro nás

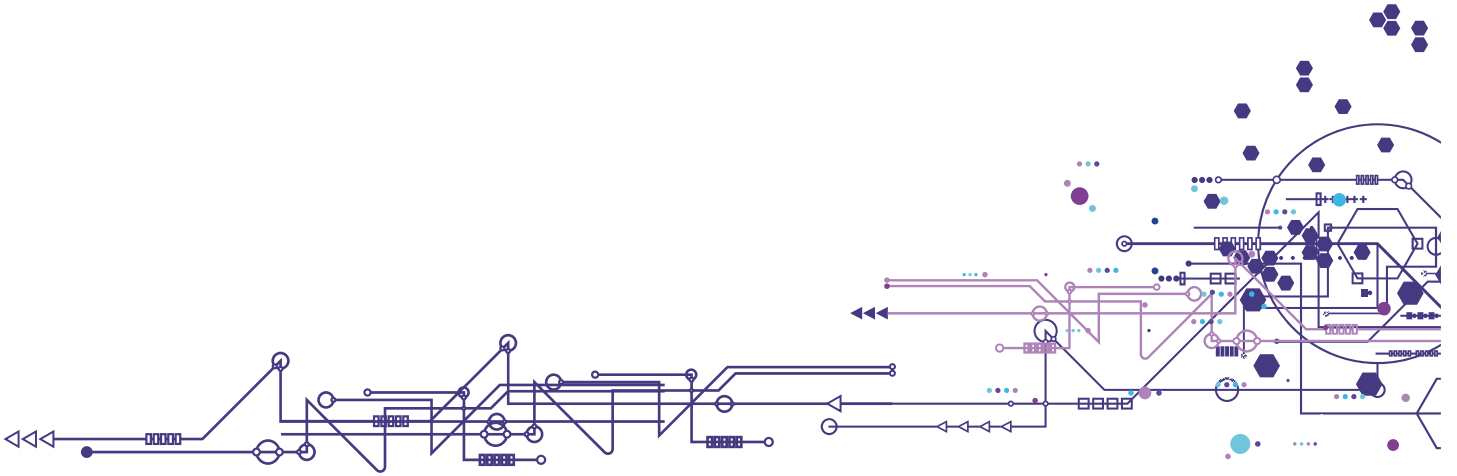
- **Zapojte se do Wardenu**

- Máte honepot? IDS/IPS?
- Máte logy a fail2ban?

- Podívejte se na https://warden.cesnet.cz a ozvěte se na warden-info@cesnet.cz

Bezpečnost ...

... a kdo je za tím?



Náš tým ...

SOC

- **NOC**

  - správci páteřní infrastruktury

  - řeší provozní a bezpečnostní problémy e-infrastruktury CESNET

  - 24/7, v nočních hodinách „on phone“

- **FLAB**

  - řešení závažných bezpečnostních incidentů

  - analýzy, scanování, ...

- **Správci sond umístěných na perimetru**
- **Správci služeb ...**

- **Monitoring a detekce**
  - **FTAS**
  - **ExaFS**

- **CESNET-CERTS**

  - řešení a koordinace řešení bezpečnostních incidentů (reponse)

  - bezpečnostní tým, constituency = AS2852, 9:00 – 17:00

  - csirt.cesnet.cz, abuse@cesnet.cz

- **PSS, Pracoviště stálé služby**

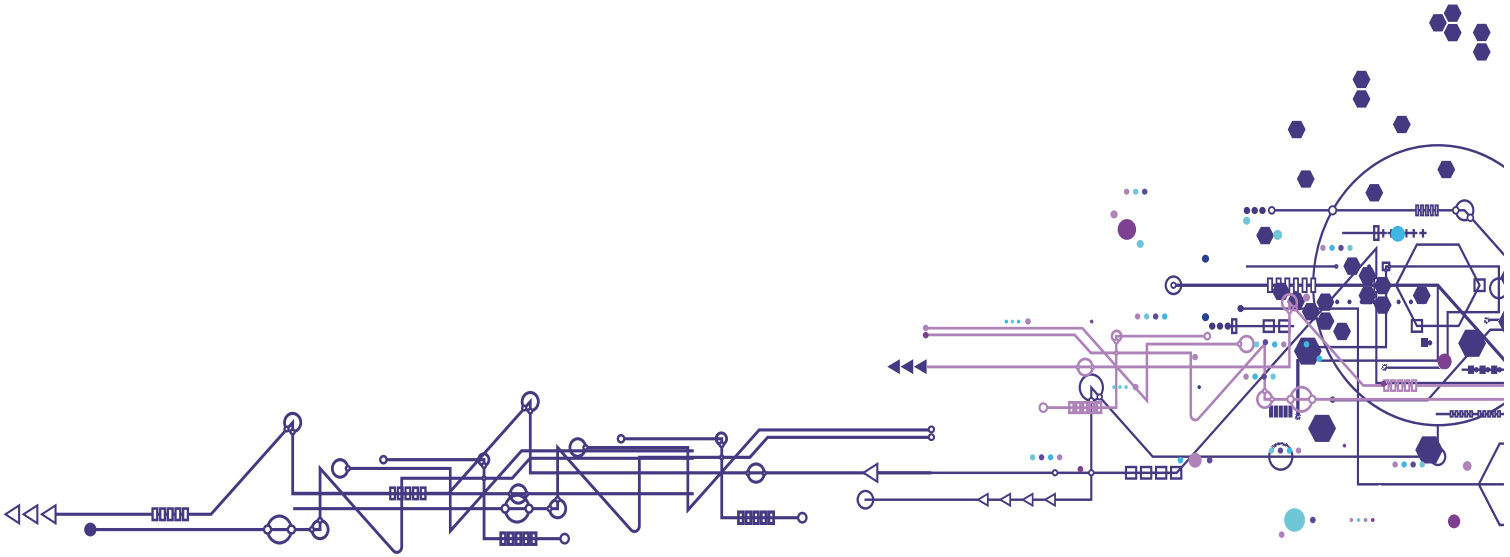
  - dohledové centrum, 24/7

  - dohled nad e-infrastrukturou CESNET a službami

  - POC, koordinační role

  - www.cesnet.cz --> kontakty

Další služby v oblasti bezpečnosti



Služby Forenzní laboratoře

- Analýza událostí **https://flab.cesnet.cz**
- Plošné testy e-infrastruktury na zranitelnosti
  - heartbleed, memcached, shellshock ...

- Penetrační testy
- Zátěžové testy
- Testy sociálního inženýrství („phishingové testy“)
  - na míru zákazníkovi

- Zadání --> Testy --> Zpracování --> Závěrečná zpráva & workshop
  - přehled provedených testů
  - zhodnocení výsledků (nálezů)
  - doporučení nápravných opatření
  - školení pro uživatele

CESNET audit system

- https://csirt.cesnet.cz/cs/services/audit
- csirt.cesnet.cz --> Služby
- Vlastní otestování zabezpečení jednotlivých strojů, podsítí nebo celých rozsáhlých sítí
- Založeno na použití nástroje Nessus (síťový scanner)

- Podoba služby
  - instalace Nessus na stroj v cílové síti [zajišťuje instituce]
  - získání aktivačního kódu od CESNET [zajišťuje CESNET]
  - provedení testů [zajišťuje instituce]
  - zpracování výsledků [zajišťuje instituce]

Osvěta, vzdělávání ...

- Seminář o bezpečnosti
  - každý rok leden/únor
- Seminář o IPv6
  - červen
- Pracovní skupiny (restart praxe pracovních skupin)
  - červen 2022 – téma „bezpečnostní události“

- Školení Forenzní trénink 1 (aka FA1)
- Školení Forenzní trénink 2 (aka FA2)
- The Catch

FA1/FA2 training

- Hands-on školení v laboratoři pod vedením zkušených školitelů (by FLAB)
- Základy forenzní analýzy digitálních dat
- 2 dny, plus Forensic Night@CESNET

- FA1
  - *Zajišťování dat, vytváření časové osy ze souborového systému, následná analýza, identifikování jednotlivých stopy vedoucích k vytvoření komplexního obrazu analyzovaného incidentu. Prezentování výsledků jako součást tréninku.*
- FA2
  - *Analýza síťového provozu, teoretický úvod do problematiky, seznámení s postupy pro zajištění podkladů, analýzou toků v sítích (netflow) a analýzou částečného i plného záznamu provozu (packet capture). Součástí školení je také seznámení s jednotlivými nástroji používanými pro analýzu.*

Kontakty

- www.cesnet.cz
- https://www.cesnet.cz/sluzby/
- www.cesnet.cz/enews - e-mail Newsletter
- **sluzby**@cesnet.cz
- support@cesnet.cz
- **certs**@cesnet.cz

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz