Mentat

Zpracování dat z bezpečnostních nástrojů

CESNET, z. s. p. o.

Andrea Kropáčová & Mentat team
andrea@cesnet.cz

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

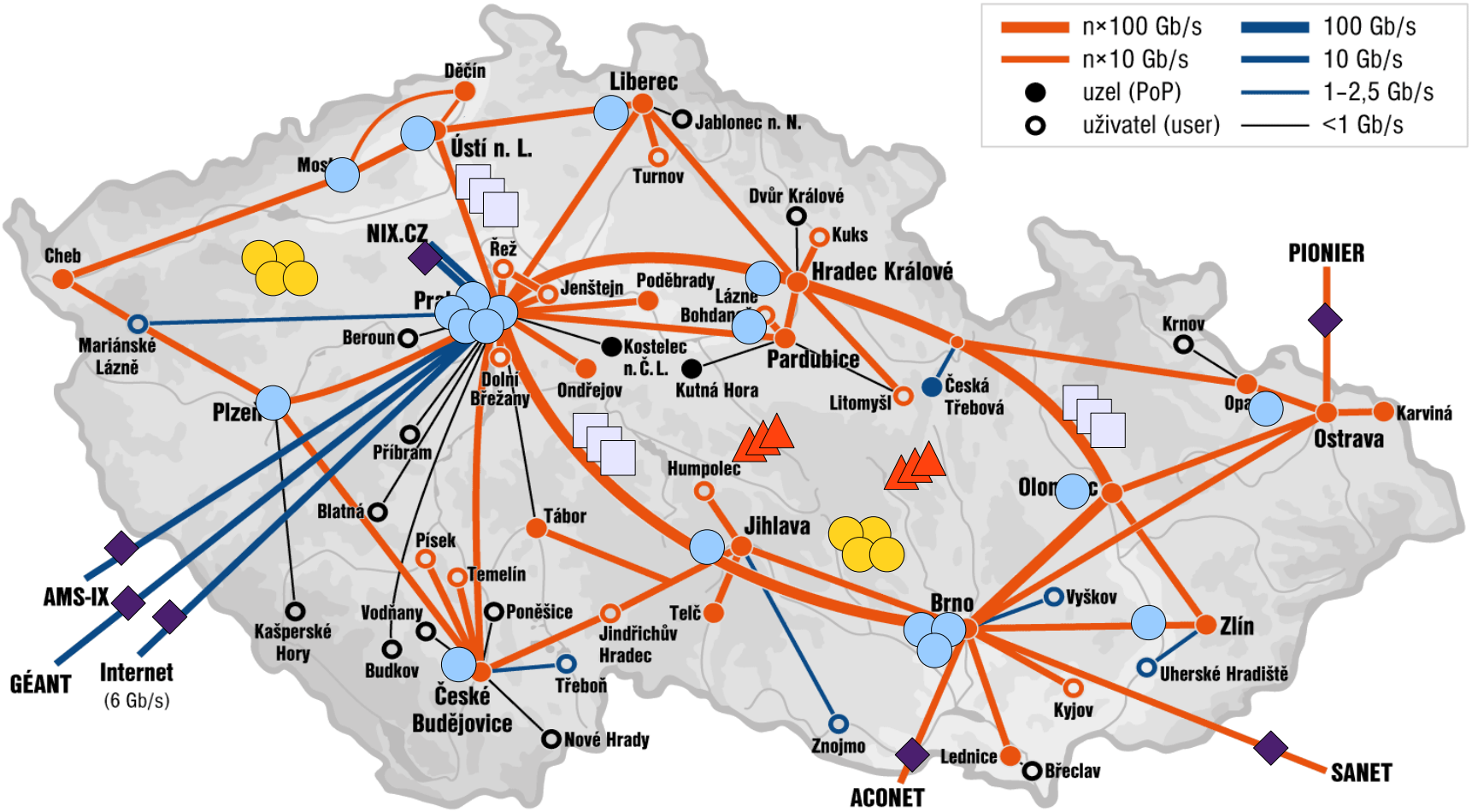
- Provozuje síť národního výzkumu a vzdělávání CESNET2
- Založen v roce 1996
- Připojeno 27 členů (české VŠ, AV ČR) a cca 280 dalších organizací
- K e-infrastruktuře CESNET se mohou připojit instituce, které se zabývají
  - vědou, výzkumem, vývojem včetně uplatnění jejich výsledků v praxi
  - experimentálním vývojem nebo inovacemi v průmyslu i jiných oborech
  - šířením vzdělanosti, kultury a prosperity
  - vybrané sítě veřejné správy
- Hlavní cíle:
  - výzkum a vývoj informačních a komunikačních technologií
  - budování a rozvoj e-infrastruktury CESNET určené pro výzkum a vzdělávání
  - podpora a šíření vzdělanosti, kultury a poznání
- 2011 – 2015
  - ***Projekt Velká infrastruktura CESNET***

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

CESNET a CESNET2

- Externí propojení
  - Sdílená IP
    - 30 Gbps GÉANT
    - 91 Gbps IX a partneři
      - 40 Gbps NIX.CZ
      - 10 Gbps ACONET (VIX)
      - 10 Gbps SANET (SIX)
      - 10 Gbps PIONIER
      - 10 Gbps AMS-IX
      - 10 Gbps Google
      - 1 Gbps TWAREN
    - 6 Gbps Tier 1 (Telia)
  - E2E pro výzkum
    - 4x10 Gbps GÉANT
    - Nx10 CBF - ACONET, SANET, PIONIER
    - 10 Gbps GLIF
- Člen sdružení CZ.NIC, NIX.CZ, projektu Fenix
- Cca 400tis uživatelů

CESNET2



- 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

Dilema

- Správci provozují řadu bezpečnostních nástrojů (IDS, honeypot, IPS, sondy, syslog, netflow ...)
  - Sledování stavu sítě, zdraví sítě
  - Detekce útoků, anomálií provozu
  - Ochrana uživatelů, hledání kompromitovaných zařízení
- Co s daty, pro která nemám použití?
  - Zahodit?
  - Reportovat?

Dilema

- Správci provozují řadu bezpečnostních nástrojů (IDS, honeypot, IPS, sondy, syslog, netflow ...)
  - Sledování stavu sítě, zdraví sítě
  - Detekce útoků, anomálií provozu
  - Ochrana uživatelů, hledání kompromitovaných zařízení
- Co s daty, pro která nemám použití?
  - Zahodit?
  - Reportovat?

Sdílet!

Dilema

- Správci provozují řadu bezpečnostních nástrojů (IDS, honeypot, IPS, sondy, syslog, netflow ...)
  - Sledování stavu sítě, zdraví sítě
  - Detekce útoků, anomálií provozu
  - Ochrana uživatelů, hledání kompromitovaných zařízení
- Co s daty, pro která nemám použití?
  - Zahodit?
  - Reportovat?

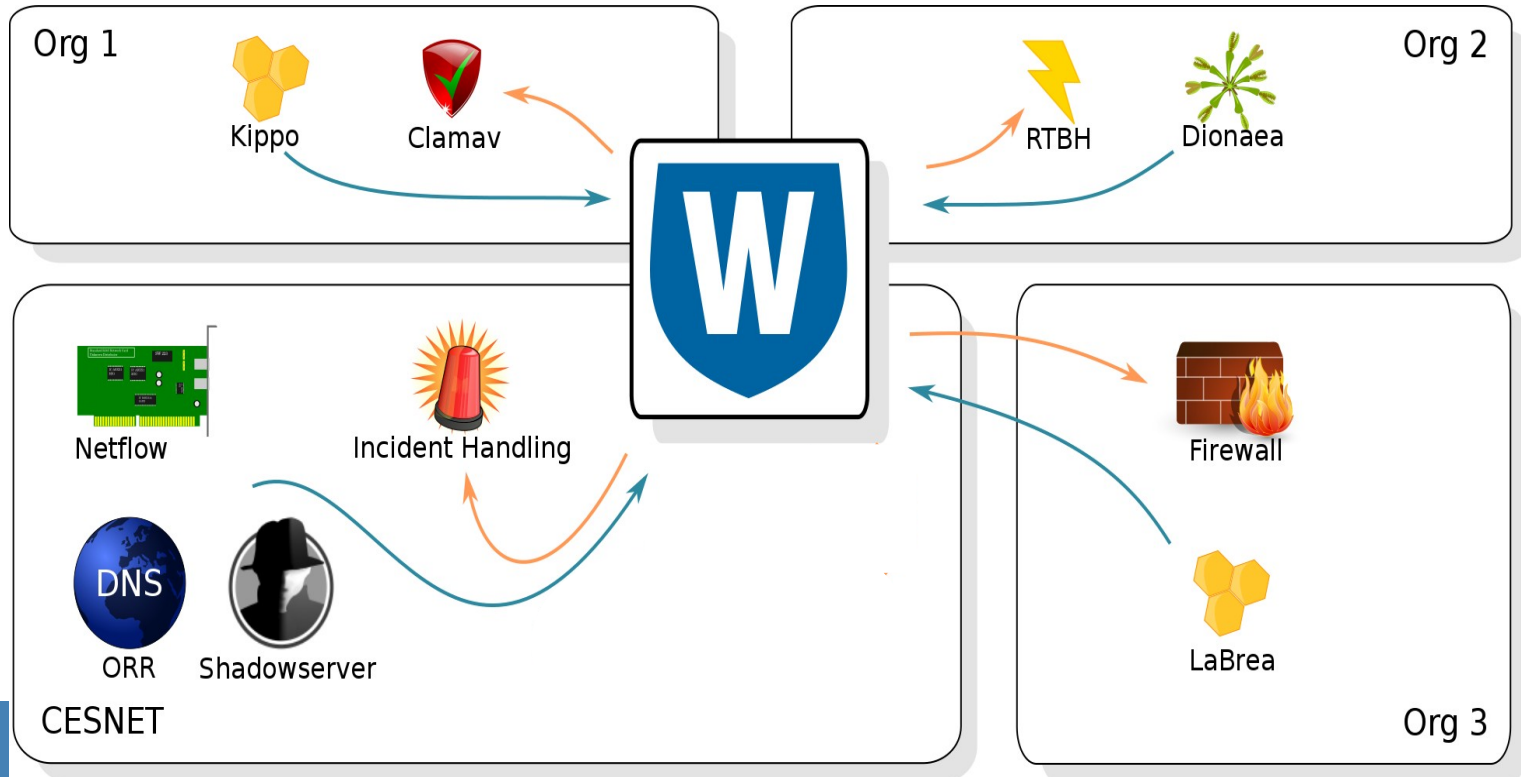
Sdílet!

- Ale – jak? A co formát? Obsah? Protokol? Klasifikace? Politika?

Warden

- Systém pro efektivní sdílení informací o bezpečnosních incidentech
- Client/server ("glorifikovaná fronta", transport, ne naskladnění dat)
- Komunitní přístup
  - Tvoje data jsou dostupná celé Warden komunitě
  - Data celé komunity jsou dostupná Tobě
- Událost (event)
- Bezpečnost

  X509
  encryption
  “sanity” checks
  peer review



Lesson learned

Připojené organizace nemají dostatek lidských zdrojů na využití otevřeného komunitního přístupu k systému Warden

=

nedokáží data odebrat a zpracovat si je.

Lesson learned

Připojené organizace nemají dostatek lidských zdrojů na využití otevřeného komunitního přístupu k systému Warden

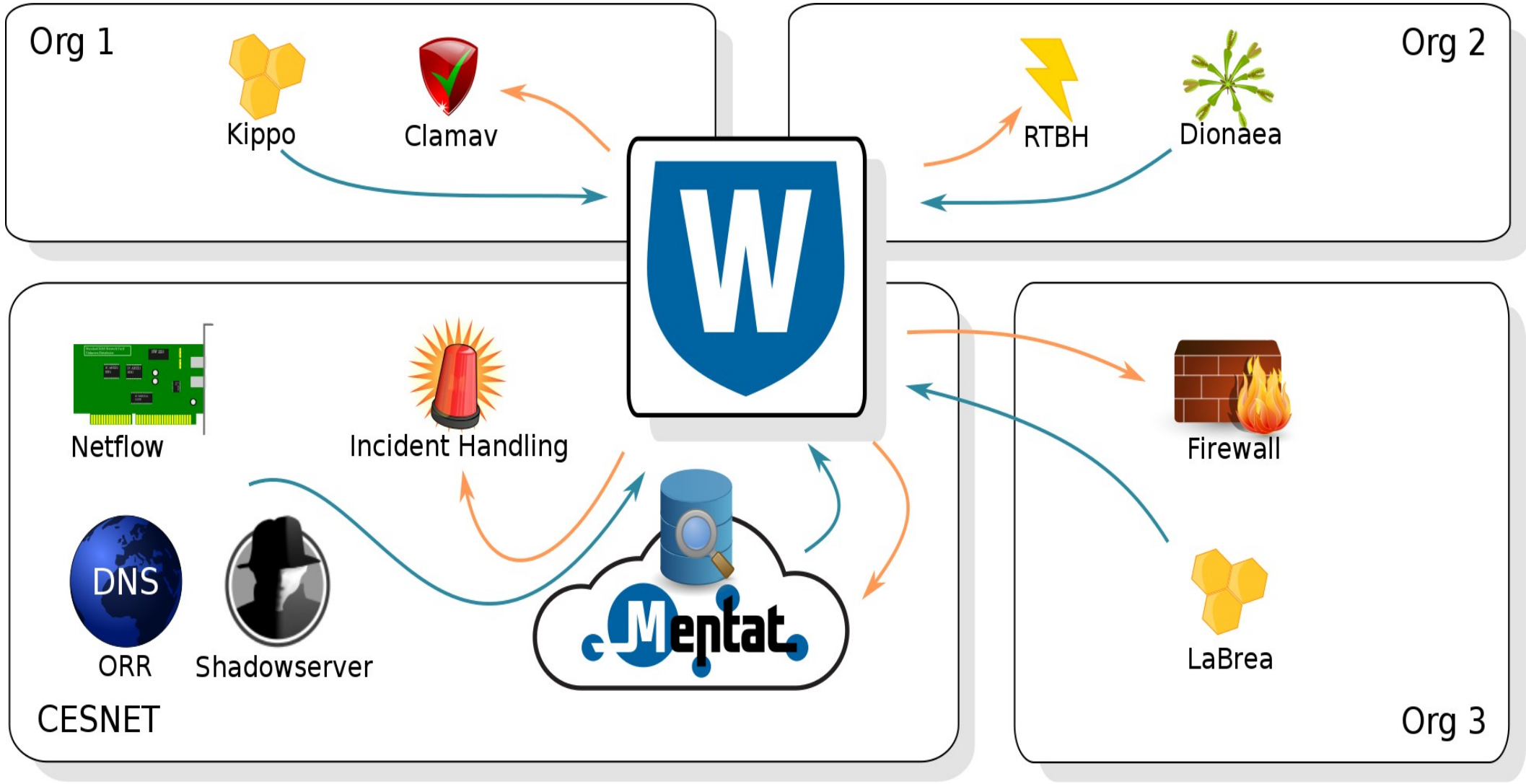
=

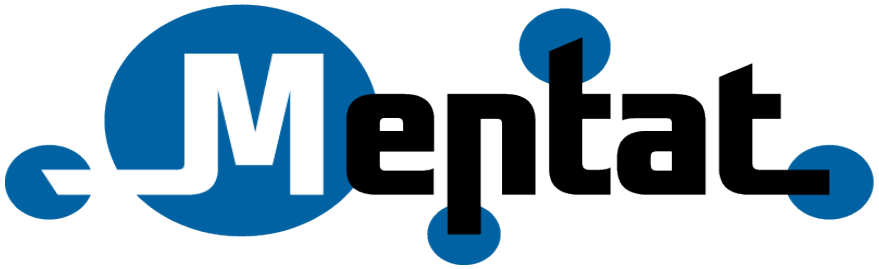
nedokáží data odebrat a zpracovat si je.

Ale chtějí tato data získávat, data jsou užitečná

=

je nutné je doručit správcům.


Org 1
Kippo
Clamav
Org 2
RTBH
Dionaea
Netflow
Incident Handling
Firewall
DNS
ORR
Shadowserver
Mentat
LaBrea
CESNET
Org 3



- SIEM
- Skladiště informací
- Zpracovává data (události) z Warden a od třetích stran (N6, ShadowServer, ...)
- Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
- Reporty zasílá do koncových sítí (abuse@...)

Report message

```
Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) související s Vaším
rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

 [1]     Stroje na následujících IP adresách fungují jako otevřené DNS resolvery a
    mohou být zneužity pro masivní DDoS útoky (Open DNS Resolver):

    * Analyzer:  X2
    * Popis:     Open DNS Resolver
    * Kategorie: Vulnerable.Config
    ================================================================================
     IP             | Čas                                           | # událostí
    ================================================================================
    158.194.189.46  | 2015-11-11 13:20:35 - 2015-11-13 03:29:49 | 1
    --------------------------------------------------------------------------------
    * Celkem 1 událost, 1 unikátní IP adresa

    Více informací o tomto typu události lze nalézt na adrese:
        https://csirt.cesnet.cz/cs/services/x2

    (Více provozních informací lze nalézt v příslušné části přiloženého souboru)


UPOZORNĚNÍ: Uvedené časy jsou okamžiky údajné detekce. Některé služby a systémy
(zejména externí, jako např. ShadowServer) bohužel občas posílají informace o
událostech i s několikadenním zpožděním.

Kompletní dostupné provozní informace k jednotlivým událostem lze nalézt
v příslušných částech jednoho z přiložených strojově zpracovatelných souborů.
V závisloti na Vašich preferencích můžete použít formát JSON, nebo CSV.
Doporučujeme použít formát JSON, protože data v něm obsažená jsou úplná.
```

Lesson learned 2

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme udělat.
- Nechci report mailem, chci to umět strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Toto nechceme vůbec, odebíráme to přímo od zdroje.
- Data od třetích stran mají různou kvalitu
  - **Nechci!** Co si počít s informací, že IP a.b.c.d je na blacklistu X?
  - **Chci!** Informace, že IP a.b.c.d. je na blacklistu X je užitečná.
- NAT, FW, DHCP …
- Velké sítě (s vlastními PI bloky)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to zase reportujete? Včera jsem to spravil.

Lesson learned 2

... reakce od příjemců reportů ...

- **Málo informací, nevíme co s tím máme udělat.**
- Nechci report mailem, chci to umět strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Toto nechceme vůbec, odebíráme to přímo od zdroje.
- Data od třetích stran mají různou kvalitu
  - **Nechci!** Co si počít s informací, že IP a.b.c.d je na blacklistu X?
  - **Chci!** Informace, že IP a.b.c.d. je na blacklistu X je užitečná.
- NAT, FW, DHCP …
- Velké sítě (s vlastními PI bloky)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to zase reportujete? Včera jsem to spravil.

Report message

Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) související s Vaším rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

[1] Stroje na následujících IP adresách fungují jako otevřené DNS resolvery a mohou být zneužity pro masivní DDoS útoky (Open DNS Resolver):

* Analyzer: X2
* Popis: Open DNS Resolver
* Kategorie: Vulnerable.Config

IP	Čas	# událostí
158.194.189.46	2015-11-11 13:20:35 - 2015-11-13 03:29:49	1

* Celkem 1 událost, 1 unikátní IP adresa

Více informací o tomto typu události lze nalézt na adrese:
https://csirt.cesnet.cz/cs/services/x2

(Více provozních informací lze nalézt v příslušné části přiloženého souboru)

UPOZORNĚNÍ: Uvedené časy jsou okamžiky údajné detekce. Některé služby a systémy (zejména externí, jako např. ShadowServer) bohužel občas posílají informace o událostech i s několikadenním zpožděním.

Kompletní dostupné provozní informace k jednotlivým událostem lze nalézt v příslušných částech jednoho z přiložených strojově zpracovatelných souborů. V závislosti na Vašich preferencích můžete použít formát JSON, nebo CSV. Doporučujeme použít formát JSON, protože data v něm obsažená jsou úplná.

Lesson learned 2

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme udělat.
- **Nechci report mailem, chci to umět strojově zpracovat.**
- Spěchá to? Jakou to má závažnost?
- Toto nechceme vůbec, odebíráme to přímo od zdroje.
- Data od třetích stran mají různou kvalitu
  - **Nechci!** Co si počít s informací, že IP a.b.c.d je na blacklistu X?
  - **Chci!** Informace, že IP a.b.c.d. je na blacklistu X je užitečná.
- NAT, FW, DHCP …
- Velké sítě (s vlastními PI bloky)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to zase reportujete? Včera jsem to spravil.

Report message

```
Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) související s Vaším
rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

 [1]     Stroje na následujících IP adresách fungují jako otevřené DNS resolvery a
    mohou být zneužity pro masivní DDoS útoky (Open DNS Resolver):

    * Analyzer:  X2
    * Popis:     Open DNS Resolver
    * Kategorie: Vulnerable.Config
    ================================================================================
     IP             | Čas                                             | # událostí
    ================================================================================
    158.194.189.46  | 2015-11-11 13:20:35 - 2015-11-13 03:29:49 | 1
    --------------------------------------------------------------------------------
    * Celkem 1 událost, 1 unikátní IP adresa

    Více info
        https

    (Více pro

UPOZORNĚNÍ: U
(zejména exte
událostech i

Kompletní dos
v příslušných
V závisloti n
Doporučujeme
```

```
#
# SECTION 1
#
#  Analyzer    | X2
#  Detector    | cesnet.au1
#  Description | Open DNS Resolver
#  Categories  | Vulnerable.Config
#  Reference   | https://csirt.cesnet.cz/cs/services/x2
#
##date_gmt;detected_gmt;analyzer;detector;classification;categories;src_ip;src_h
ost;src_port;tgt_port;src_proto;tgt_proto;con_cnt;date_ts;detected_ts;note;impac
t
2015-11-13 02:29:49Z;2015-11-11 12:20:35Z;X2;cesnet.au1;Open DNS Resolver;Vulner
able.Config;158.194.189.46;189-46.kolejnet.upol.cz;-;-;udp/dns;-;-;1447381789;14
47244435;-;System 158.194.189.46 is ORR and can be misused to DDoS attacks
```

Lesson learned 2

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme udělat.
- Nechci report mailem, chci to umět strojově zpracovat.
- **Spěchá to? Jakou to má závažnost?**
- Toto nechceme vůbec, odebíráme to přímo od zdroje.
- Data od třetích stran mají různou kvalitu
  - **Nechci!** Co si počít s informací, že IP a.b.c.d je na blacklistu X?
  - **Chci!** Informace, že IP a.b.c.d. je na blacklistu X je užitečná.
- NAT, FW, DHCP …
- Velké sítě (s vlastními PI bloky)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to zase reportujete? Včera jsem to spravil.

Report message

Report M20151113M-KFrDb

Severity	Abuse	Created
medium	abuse@upol.cz	2015-11-13 05:05:51

Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) souvise
rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

[1] Stroje na následujících IP adresách fungují jako otevřené DNS resolvery a mohou být zneužity pro masivní DDoS útoky (Open DNS Resolver):

* Analyzer: X2
* Popis: Open DNS Resolver
* Kategorie: Vulnerable.Config

IP	Čas	# událostí
158.194.189.46	2015-11-11 13:20:35 - 2015-11-13 03:29:49	1

* Celkem 1 událost, 1 unikátní IP adresa

Více informací o tomto typu události lze nalézt na adrese:
https://csirt.cesnet.cz/cs/services/x2

(Více provozních informací lze nalézt v příslušné části přiloženého souboru)

UPOZORNĚNÍ: Uvedené časy jsou okamžiky údajné detekce. Některé služby a systémy (zejména externí, jako např. ShadowServer) bohužel občas posílají informace o událostech i s několikadenním zpožděním.

Kompletní dostupné provozní informace k jednotlivým událostem lze nalézt v příslušných částech jednoho z přiložených strojově zpracovatelných souborů. V závisloti na Vašich preferencích můžete použít formát JSON, nebo CSV. Doporučujeme použít formát JSON, protože data v něm obsažená jsou úplná.

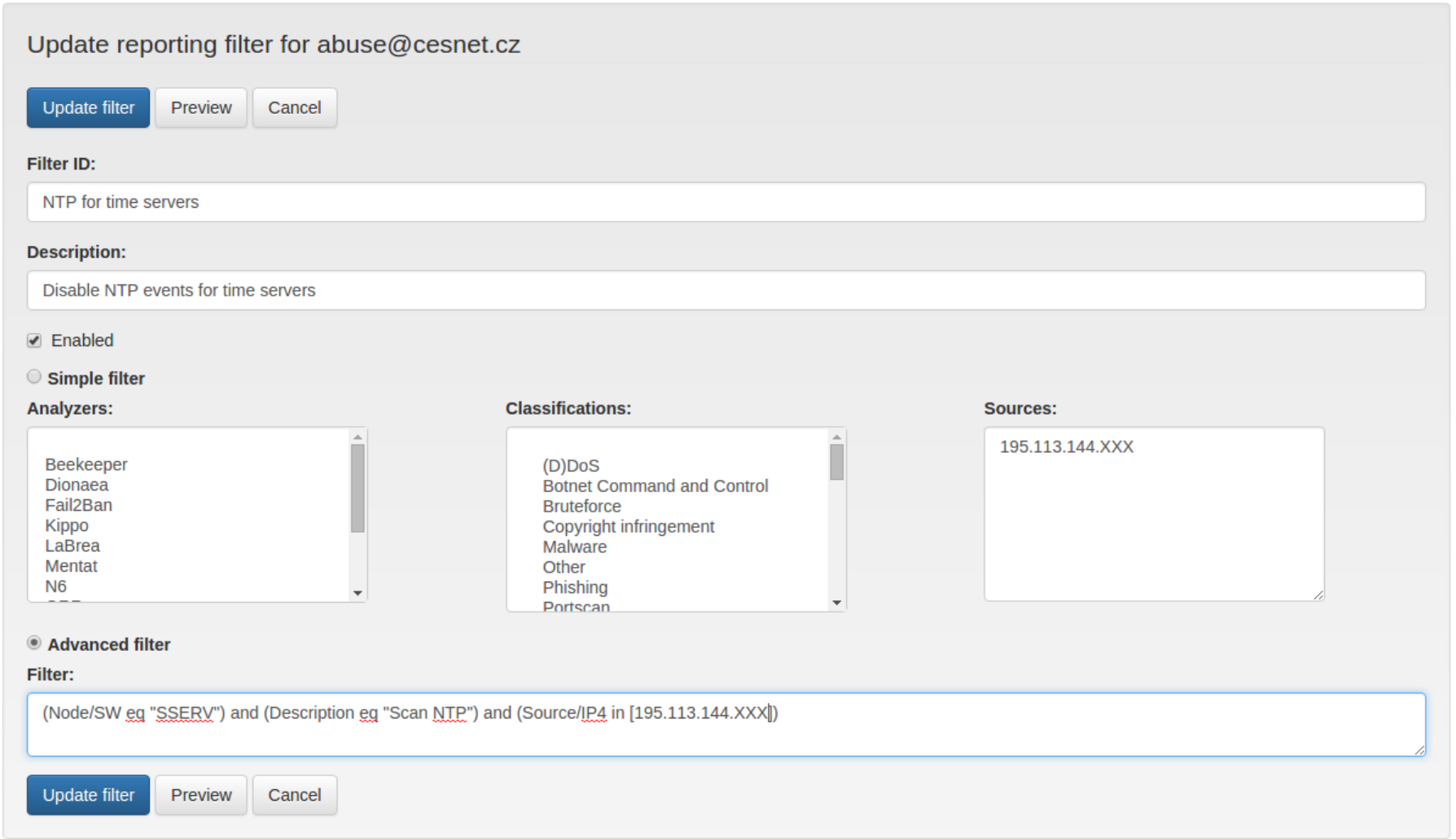
Lesson learned 2

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme udělat.
- Nechci report mailem, chci to umět strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- **Toto nechceme vůbec, odebíráme to přímo od zdroje.**
- **Data od třetích stran mají různou kvalitu**
  - **Nechci! Co si počít s informací, že IP a.b.c.d je na blacklistu X?**
  - **Chci! Informace, že IP a.b.c.d. je na blacklistu X je užitečná.**
- **NAT, FW, DHCP …**
- Velké sítě (s vlastními PI bloky)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to zase reportujete? Včera jsem to spravil.

Filtrování

- Možnost nehlásit některé sety událostí
  - Např. pro jednu IP adresu, která komunikuje nestandardně
  - Nepřijímat jeden zdroj (protože ho odebírám přímo)
  - Nepřijímat některé typy událostí



Lesson learned 2

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme udělat.
- Nechci report mailem, chci to umět strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Toto nechceme vůbec, odebíráme to přímo od zdroje.
- Data od třetích stran mají různou kvalitu
  - **Nechci!** Co si počít s informací, že IP a.b.c.d je na blacklistu X?
  - **Chci!** Informace, že IP a.b.c.d. je na blacklistu X je užitečná.
- NAT, FW, DHCP …
- **Velké sítě (s vlastními PI bloky)**
  - **Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.**
- Proč mi to zase reportujete? Včera jsem to spravil.

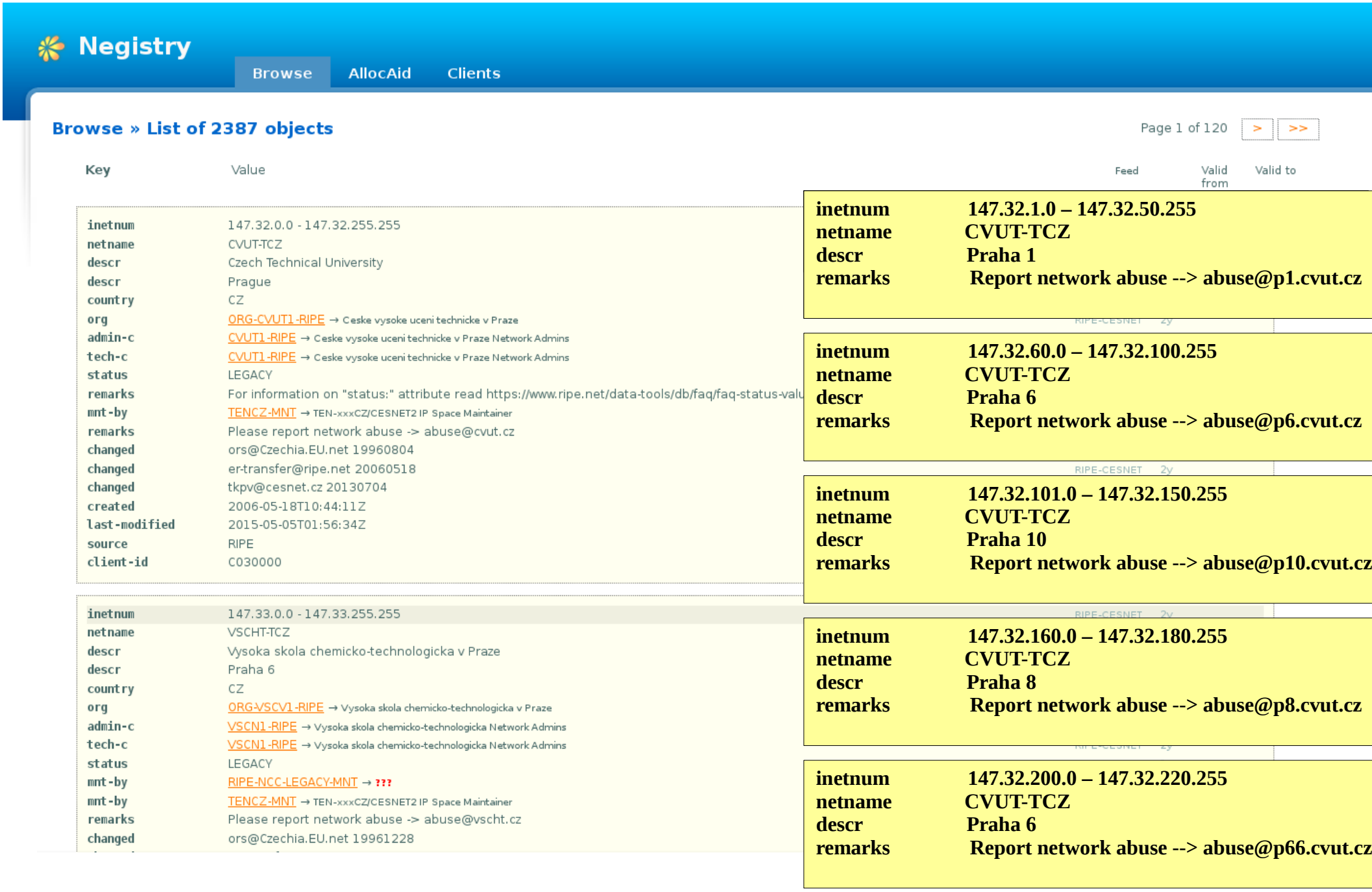
Negistry

Browse | AllocAid | Clients

Browse » List of 2387 objects

Page 1 of 120 > >>

Key	Value	Feed	Valid from	Valid to
inetnum	147.32.0.0 - 147.32.255.255	RIPE-CESNET	2y	
netname	CVUT-TCZ	RIPE-CESNET	2y	
descr	Czech Technical University	RIPE-CESNET	2y	
descr	Prague	RIPE-CESNET	2y	
country	CZ	RIPE-CESNET	2y	
org	ORG-CVUT1-RIPE → Ceske vysoke uceni technicke v Praze	RIPE-CESNET	2y	
admin-c	CVUT1-RIPE → Ceske vysoke uceni technicke v Praze Network Admins	RIPE-CESNET	2y	
tech-c	CVUT1-RIPE → Ceske vysoke uceni technicke v Praze Network Admins	RIPE-CESNET	2y	
status	LEGACY	RIPE-CESNET	1y	
remarks	For information on "status:" attribute read https://www.ripe.net/data-tools/db/faq/faq-status-values-legacy-resources	RIPE-CESNET	1y	
mnt-by	TENCZ-MNT → TEN-xxxCZ/CESNET2 IP Space Maintainer	RIPE-CESNET	2y	
remarks	Please report network abuse -> abuse@cvut.cz	RIPE-CESNET	2y	
changed	ors@Czechia.EU.net 19960804	RIPE-CESNET	2y	
changed	er-transfer@ripe.net 20060518	RIPE-CESNET	2y	
changed	tkpv@cesnet.cz 20130704	RIPE-CESNET	2y	
created	2006-05-18T10:44:11Z	RIPE-CESNET	6mo	
last-modified	2015-05-05T01:56:34Z	RIPE-CESNET	6mo	
source	RIPE	RIPE-CESNET	2y	
client-id	C030000	CESNET-CLIENTS	2y	
inetnum	147.33.0.0 - 147.33.255.255	RIPE-CESNET	2y	
netname	VSCHT-TCZ	RIPE-CESNET	2y	
descr	Vysoka skola chemicko-technologicka v Praze	RIPE-CESNET	1w	
descr	Praha 6	RIPE-CESNET	2y	
country	CZ	RIPE-CESNET	2y	
org	ORG-VSCV1-RIPE → Vysoka skola chemicko-technologicka v Praze	RIPE-CESNET	2y	
admin-c	VSCN1-RIPE → Vysoka skola chemicko-technologicka Network Admins	RIPE-CESNET	2y	
tech-c	VSCN1-RIPE → Vysoka skola chemicko-technologicka Network Admins	RIPE-CESNET	2y	
status	LEGACY	RIPE-CESNET	1y	
mnt-by	RIPE-NCC-LEGACY-MNT → ???	RIPE-CESNET	1w	
mnt-by	TENCZ-MNT → TEN-xxxCZ/CESNET2 IP Space Maintainer	RIPE-CESNET	2y	
remarks	Please report network abuse -> abuse@vscht.cz	RIPE-CESNET	2y	
changed	ors@Czechia.EU.net 19961228	RIPE-CESNET	2y	



inetnum 147.32.1.0 – 147.32.50.255
netname CVUT-TCZ
descr Praha 1
remarks Report network abuse --> abuse@p1.cvut.cz

inetnum 147.32.60.0 – 147.32.100.255
netname CVUT-TCZ
descr Praha 6
remarks Report network abuse --> abuse@p6.cvut.cz

inetnum 147.32.101.0 – 147.32.150.255
netname CVUT-TCZ
descr Praha 10
remarks Report network abuse --> abuse@p10.cvut.cz

inetnum 147.32.160.0 – 147.32.180.255
netname CVUT-TCZ
descr Praha 8
remarks Report network abuse --> abuse@p8.cvut.cz

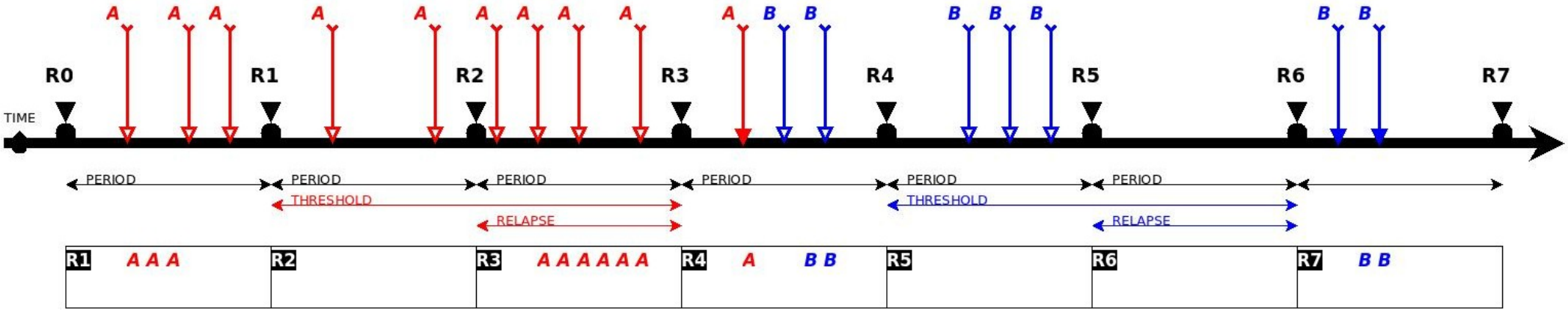
inetnum 147.32.200.0 – 147.32.220.255
netname CVUT-TCZ
descr Praha 6
remarks Report network abuse --> abuse@p66.cvut.cz

Lesson learned 2

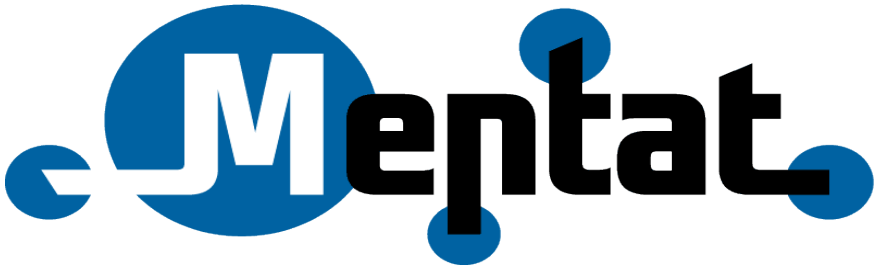
... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme udělat.
- Nechci report mailem, chci to umět strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Toto nechceme vůbec, odebíráme to přímo od zdroje.
- Data od třetích stran mají různou kvalitu
  - **Nechci!** Co si počít s informací, že IP a.b.c.d je na blacklistu X?
  - **Chci!** Informace, že IP a.b.c.d. je na blacklistu X je užitečná.
- NAT, FW, DHCP …
- Velké sítě (s vlastními PI bloky)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- **Proč mi to zase reportujete? Včera jsem to spravil.**

Reportér nové generace



- Zpracování zpráv s každou úrovní závažnosti zvlášť
- Algoritmus je konfigurovatelný trojicí *period/threshold/relapse*
- **Period** – interval generování reportů
- **Threshold** – doba, po kterou budou již hlášené události týkající se konkrétní IP adresy “zamlčeny”
- **Relapse** – heuristika, která v případě nevyřešení problému zajistí odeslání “zamlčených” událostí



- SIEM
- Skladiště informací
- Zpracovává data (události) z Warden a od třetích stran (N6, ShadowServer, ...)
- Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
- Reporty zasílá do koncových sítí (abuse@...)
- Podpůrný nástroj CESNET-CERTS a bezpečnostní týmy připojených organizací
- **WWW rozhraní pro správce z koncových sítí**
  - **Možnost ovlivnit jak a kdy reporty dostávat a co chci dostávat**
  - **Detaily reportů**
  - **Globální dahsboardy**
  - **Statistiky**

Mentat SIEM

Search alerts

Alert database search

Source: 127.0.0.1 **Target:** 127.0.0.1 AND OR

From: 2012-12-12 12:12:12 **To:** 2012-12-12 12:12:12

Detector:
--- Unspecified ---
cesnet.au1/LaBrea
cesnet.au1/SSERV
cesnet.au1/X4

Category:
Anomaly.Traffic
Attempt.Exploit
Attempt.Login
Availability.DDoS
Availability.DoS

Search
Go Advance

If you use certain queries often, you might consider saving them:

--- Personal query --- Unique name for the query Save

Displaying items **1** to **30** (**30** items) | Page **1** Next

#	Detected	Source	Target	Categorization	
1	2015-09-22 13:18:05	-- undisclosed --	211.240.36.71	Availability.DoS	
2	2015-09-22 13:13:23	-- undisclosed --	193.87.171.19	Availability.DoS	

Report M20150922M-F4amT

Unprotected access: https://mentat-hub.cesnet.cz/mentat/unauth/report/32WvuPYwWXpyaxZAhxMo

Severity	Abuse	Created
medium	abuse@vstecb.cz	2015-09-22 08:06:37

Report timing

Time period	2015-09-22 06:00:00 - 2015-09-22 08:00:00 (2h)
Delay	6m 37s
Report sent	2015-09-22 08:06:37 | Report mailed to abuse contact 'abuse@vstecb.cz'

Report magnitude

Event count	400 (400 entered filtering, 0 blocked)
IP count	1 unique IP address
Diversisty	1 analyzer, 2 categories

Report message

```
Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) související s Vaš
rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

 [1]     Systémy na následujících IP adresách jsou infikovány známým malware
    součástí botnetu (Botnet Drone):

    * Analyzer:  X4
    * Popis:     Botnet Drone
    * Kategorie: Intrusion.Botnet/Malware
    ================================================================================
     IP             | Čas                                          | # událostí
    ================================================================================
    195.113.220.250 | 2015-09-21 15:44:53 - 2015-09-22 07:14:44 | 400
    --------------------------------------------------------------------------------
-
```


CESNET

Home
Group dashboards
Reports
Alerts
Event library
Whois
Statistics
Briefs
Group management
Administration

Report detail

Home / Reports / Detail

Report **M20151113M-KFrDb**

Unprotected access: https://mentat-hub.cesnet.cz/mentat/unauth/report/3lul5Np7yiRqkTcvdSXp

Severity	Abuse	Created
medium	abuse@upol.cz	2015-11-13 05:05:51

Report timing

Time period	2015-11-13 03:00:00 - 2015-11-13 05:00:00 (2h)
Delay	5m 51s
Report sent	2015-11-13 05:05:51 | Report mailed to abuse contact 'abuse@upol.cz'

Report magnitude

Event count	1 (1 entered filtering, 0 blocked)
IP count	1 unique IP address
Diversity	1 analyzer, 1 category

Report message

```
Vážení kolegové,

detekční systémy CESNETu zaznamenaly následující problém(y) související s Vaším
rozsahem IP adres nebo Vaší doménou (uvedené časy jsou lokální):

 [1]     Stroje na následujících IP adresách fungují jako otevřené DNS resolvery a
    mohou být zneužity pro masivní DDoS útoky (Open DNS Resolver):

    * Analyzer:  X2
    * Popis:     Open DNS Resolver
    * Kategorie: Vulnerable.Config
    ================================================================================
     IP             | Čas                                          | # událostí
    ================================================================================
    158.194.189.46  | 2015-11-11 13:20:35 - 2015-11-13 03:29:49 | 1
    --------------------------------------------------------------------------------
    * Celkem 1 událost, 1 unikátní IP adresa
```

Home
Group dashboards
abuse@cesnet.cz
eduroam-abuse@cesnet.cz
VS@cesnet.cz
Reports
Alerts
Event library
Whois
Statistics
Briefs
Group management
Administration

Group dashboard

abuse@cesnet.cz

From: YYYY-MM-DD HH:MM:SS **To:** YYYY-MM-DD HH:MM:SS View

Last reports (limited to 50) 50

- **M20151111M-iL9Kp** (2015-11-11 11:05:46 | **10** | 1 | 1 |)
- **M20151111H-f8xVn** (2015-11-11 10:45:56 | **3** | 1 | 1 |)
- **M20151111H-KQGWy** (2015-11-11 09:55:57 | **1** | 1 | 1 |)
- **M20151111M-vXTC9** (2015-11-11 09:06:03 | **2** | 1 | 1 |)
- **M20151111L-c6Up6** (2015-11-11 01:06:07 | **3** | 3 | 1 |)

Reporting statistics

Result size:	50			
Result period:	2015-11-01 13:20:00 - 2015-11-11 11:00:00 (9d 21h 40m)			
Delay time:	⌄ 3m 57s (79.63%)	⌃ 6m 7s (123.3%)	✖	⊙ 4m 57s
Total event count:	⌄ 1 (29.41%)	⌃ 12 (352.94%)	✚ 170	⊙ 3.4
Unique IP count:	⌄ 1 (56.82%)	⌃ 4 (227.27%)	✚ 88	⊙ 1.76
Analyzer count:	⌄ 1 (78.13%)	⌃ 3 (234.38%)	✚ 64	⊙ 1.28
Category count:	⌄ 1 (100%)	⌃ 1 (100%)	✚ 50	⊙ 1

Charts

Delay # per report # per abuse # per analyzer # per category # per IP @ per abuse

@ per address

Home
Group dashboards
Reports
Alerts
Event library
Whois
Statistics
Briefs
Group management
Administration

Alert detail

Home / Alerts / Detail

Alert 2196b984-8fa1-42af-b41e-9add8a753884

Severity	Event
unknown	unknown

Actions
- Download alert in JSON
- Delete alert

General alert attributes

Alert ID	2196b984-8fa1-42af-b41e-9add8a753884
Detected At	2015-11-11 16:24:47 (2015-11-11 15:24:47Z)
Created At	-- undefined --
Stored At	2015-11-11 16:26:33 (2015-11-11 15:26:33Z)
Creation delay	-- undefined --
Storage delay	-- undefined --
Categories	Attempt.Exploit
Resolved Abuses	-- none --

Source nodes

IPv4s	208.100.26.231
Ports	60730

Target nodes

IPv4s	147.230.185.94
Ports	3306
Protocols	tcp

Attachments

This alert does not disclose any atachments

Analyzer nodes

Name	cz.cesnet.mentat.warden_filer
Detection SW	Mentat warden_filer-receiver
Type	Relay

Name	cz.tul.ward.dionaea
Detection SW	Dionaea

Alert walkthrough

- **Category[1]:** Attempt.Exploit
- **ConnCount:** 2
- **DetectTime:** 2015-11-11 15:24:47Z
- **Format:** IDEA0
- **ID:** 2196b984-8fa1-42af-b41e-9add8a753884
- **Node[1]/Name:** cz.cesnet.mentat.warden_filer
- **Node[1]/SW[1]:** Mentat

Mentat

mach@cesnet.cz | Logout | Help

- Home
- Group dashboards
- Reports
- Alerts
- Event library
- Whois
- Statistics
- Briefs
- Group management
- Administration

Reports

Report ID or type, abuse contact or IP **From:** YYYY-MM-DD HH:MM:SS **To:** YYYY-MM-DD HH:MM:SS Search

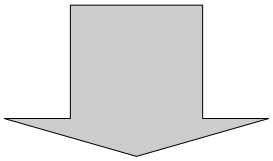
Displaying items **1** to **30** (**30** items of **7,359** total) | Page **1** of **246**

1 2 3 4 5 6 7 › »

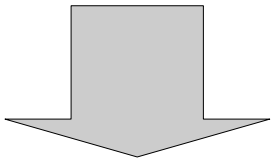
#	?	Time period	Report ID	Abuse contact	Node	ECNT | UNIQ | ACNT | CCNT	Delay
1	M	2015-11-11 11:00:00 - 2015-11-11 13:00:00	M20151111M-2JBFO	abuse@casablanca.cz	81.0.198.123	1 1 1 1	5m 44s
2	M		M20151111M-iq1mn	abuse@cuni.cz	78.128.178.251	0 1 1 1	5m 44s
3	M		M20151111M-0ICcE	abuse@cuni.cz	78.128.178.251	1 1 1 1	5m 44s
4	M	2015-11-11 09:00:00 - 2015-11-11 11:00:00	M20151111M-thhw1	abuse@czu.cz	193.84.36.83	3 1 1 1	5m 49s
5	M		M20151111M-ysEqz	abuse@ultimum.io	195.113.161.198	1 1 1 1	5m 48s
6	M		M20151111M-q3Mg6	abuse@vfn.cz	195.113.70.110	1 1 1 1	5m 47s
7	M		M20151111M-YT5NW	abuse@avu.cz	195.113.80.1	1 1 1 1	5m 47s
8	M		M20151111M-7Vcrs	abuse@vsb.cz	158.196.99.73 (5 total)	5 5 1 1	5m 47s
9	M		M20151111M-OLUik	abuse@kerio.cz	195.113.184.20	1 1 1 1	5m 47s
10	M		M20151111M-a3pUp	abuse@osanet.cz	195.113.113.114	1 1 1 1	5m 47s
11	M		M20151111M-J2UBE	abuse@techlib.cz	195.113.242.122 (2 total)	2 2 1 1	5m 47s
12	M		M20151111M-MJElY	abuse@cvut.cz	147.32.62.186 (5 total)	5 5 1 1	5m 46s
13	M		M20151111M-iL9Kp	abuse@cesnet.cz	195.113.151.161 (3 total)	10 3 1 1	5m 46s
14	M		M20151111M-MwoCn	abuse@vutbr.cz	147.229.206.218	0 1 1 1	5m 46s
15	M		M20151111M-LXjwG	abuse@vutbr.cz	147.229.206.218	1 1 1 1	5m 46s
16	M		M20151111M-39BGm	abuse@upol.cz	158.194.108.30 (9 total)	9 9 1 1	5m 46s

Statistiky

- FTAS
  - sběr informací o provozu z páteřních prvků a připojených sítí
  - 50 primárních zdrojů, 20 z páteře, 30 z koncových sítí
  - 400 core, ~180TB dat, TTL dat >= 62 dní



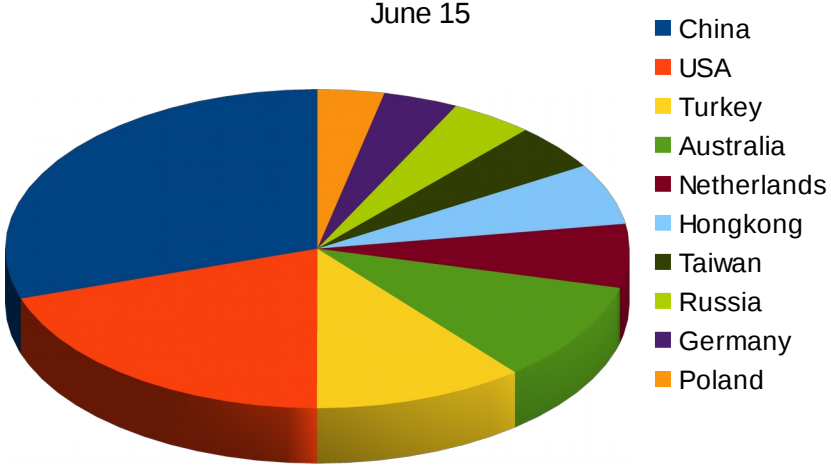
- Warden
  - cca 1,1 mil událostí za den



- Mentat
  - cca 60 reportů denně, cca 300 týdně (na cca 320 připojených organizací)

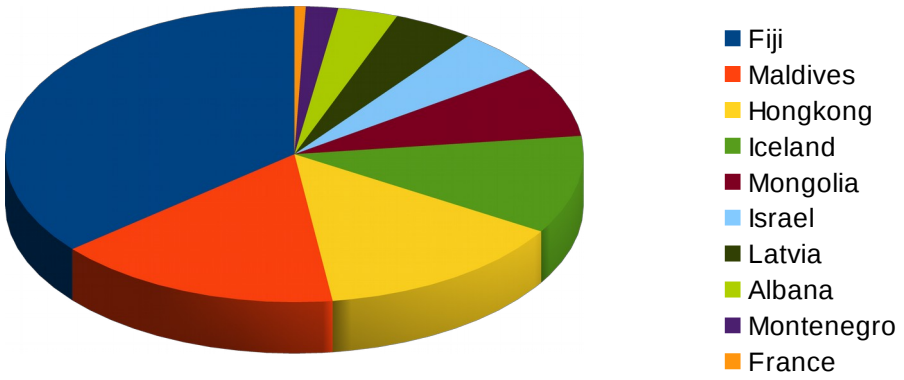
Incident TOP10 share by country

June 15



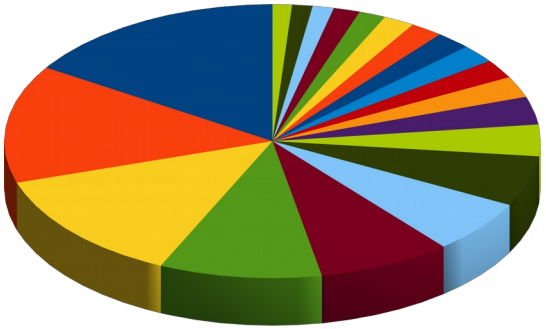
Incident TOP10 share

according to number of incidents
per one IP in the country
June 2015



TOP 20 incident share by AS

June 2015

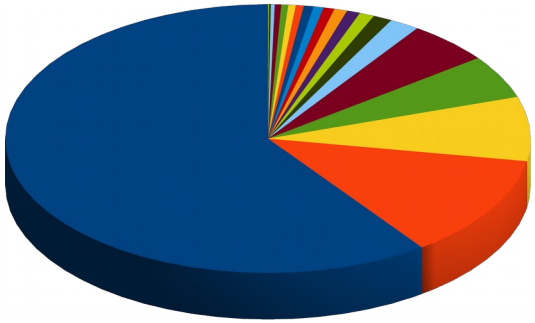


- Chinanet CN
- Turk Telekomunikasyon Anonim Sirketi TR
- SoftLayer Technologies Inc. AU
- CNCGROUP China169 Backbone CN
- CHINANET jiangsu province backbone CN
- Ecatel LTD NL
- Data Communication Business Group TW
- CariNet, Inc. US
- SoftLayer Technologies Inc. HK
- Hurricane Electric, Inc. US
- HOT NET LIMITED HK
- PlusServer AG DE
- University of Michigan US
- Jazz Telecom S.A. ES
- Biznes-Host.pl sp. z o.o. PL
- MCI Communications Services, Inc. d/b/a Verizon Business US
- 013 NetVision Ltd. IL
- Contabo GmbH DE
- CNCGROUP IP network China169 Beijing Province Network CN
- Abovenet Communications, Inc US

TOP 20 incident share by AS

according to number of incidents per one IP from AS

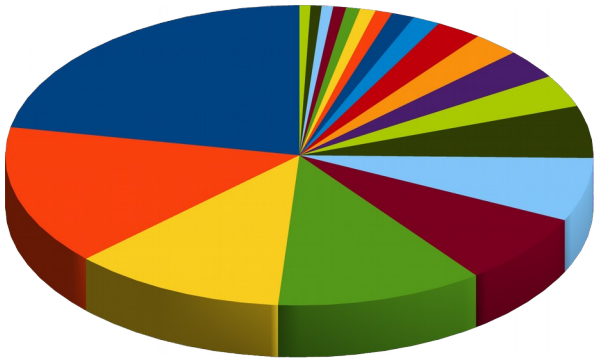
June 2015



- HOT NET LIMITED
- Przedsiebiorstwo Uslug Specjalistycznych ELAN mgr inz.
- Nikultsev Aleksandr Nikolaevich
- Ecatel LTD
- DELORIAN Internet Services Artur Grabowski
- Nagravision SA
- DataClub S.A.
- PE Voronov Evgen Sergiyovich
- Livenet Sp, z o.o.
- WEDOS Internet, a.s.
- Storm Systems LLC
- MediaServicePlus Ltd.
- Black Fox Limited
- CariNet, Inc.
- Iradeum Trading Ltd.
- DataWagon LLC
- DDNET SOLUTIONS SRL
- HOSTKEY B.V.
- Hosting Solution Ltd.

Incident TOP20 share by Czech ISP

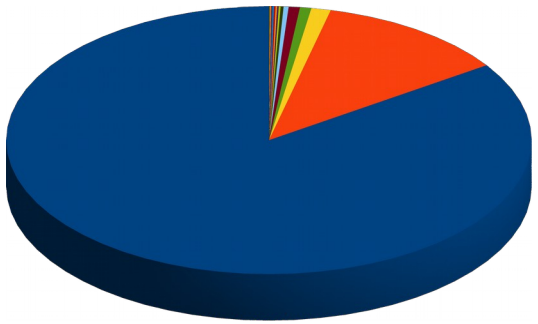
June 2015



- WEDOS Internet, a.s.
- FDCservers.net
- O2 Czech Republic, a.s.
- OVH SAS
- Liberty Global Operations B.V. (UPC ČR)
- CESNET z.s.p.o.
- METRONET s.r.o.
- Media a.s.
- itself s.r.o.
- Vodafone Czech Republic a.s.
- PODA a.s.
- T-Mobile Czech Republic a.s.
- CD-Telematika a.s.
- Starnet s.r.o.
- T-Mobile Czech Republic a.s.
- CoProSys a.s.
- ISP Alliance a.s.
- WIA spol. s.r.o.

Incident TOP20 share by Czech ISP

according to number of incidents
per one IP address from AS
June 2015



- WEDOS Internet, a.s.
- FDCservers.net
- Pe3ny Net s.r.o.
- Ladislav Rudolf
- MAXTEL s.r.o.
- Vodafone Czech Republic a.s.
- Druzstvo EUROSIGNAL
- FreeTel, s.r.o.
- Brno University of Technology
- Futurenet ISP s.r.o.
- CoProSys a.s.
- Tlapnet s.r.o.
- Humlnet s.r.o.
- Marek Smutny
- WMS s.r.o.
- CESNET z.s.p.o.
- Dial Telecom, a.s.
- TTNET Czech Republic
- INTERNET CZ, a.s.
- VSHosting s.r.o.

Závěr

- Umíme data dostat na jedno místo, zpracovat a využít.

- CESNET2
  - významný zdroj primárních dat (bezpečnostní událost)

- Další rozvoj Warden a Mentat
  - nové a další zdroje primárních dat
  - obohacení dat
  - korelace

!Sdílení a výměna dat na národní a mezinárodní úrovni!

Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz