

The logo for Warden, with the letter "W" inside a blue shield shape, followed by the word "arden" in a bold, black, sans-serif font. Below the letters "a", "r", and "d" are four small blue vertical bars of varying heights.

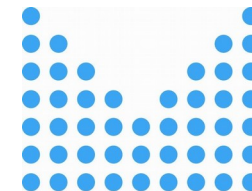
Efektivní sdílení informací

The logo for Mentat, with the letter "M" inside a blue circle, followed by the word "entat" in a bold, black, sans-serif font. The letters "e", "n", and "t" have blue circular accents at their bottom ends.

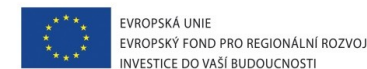
Zpracování dat z bezpečnostních nástrojů  
& reporting

CESNET, z. s. p. o.

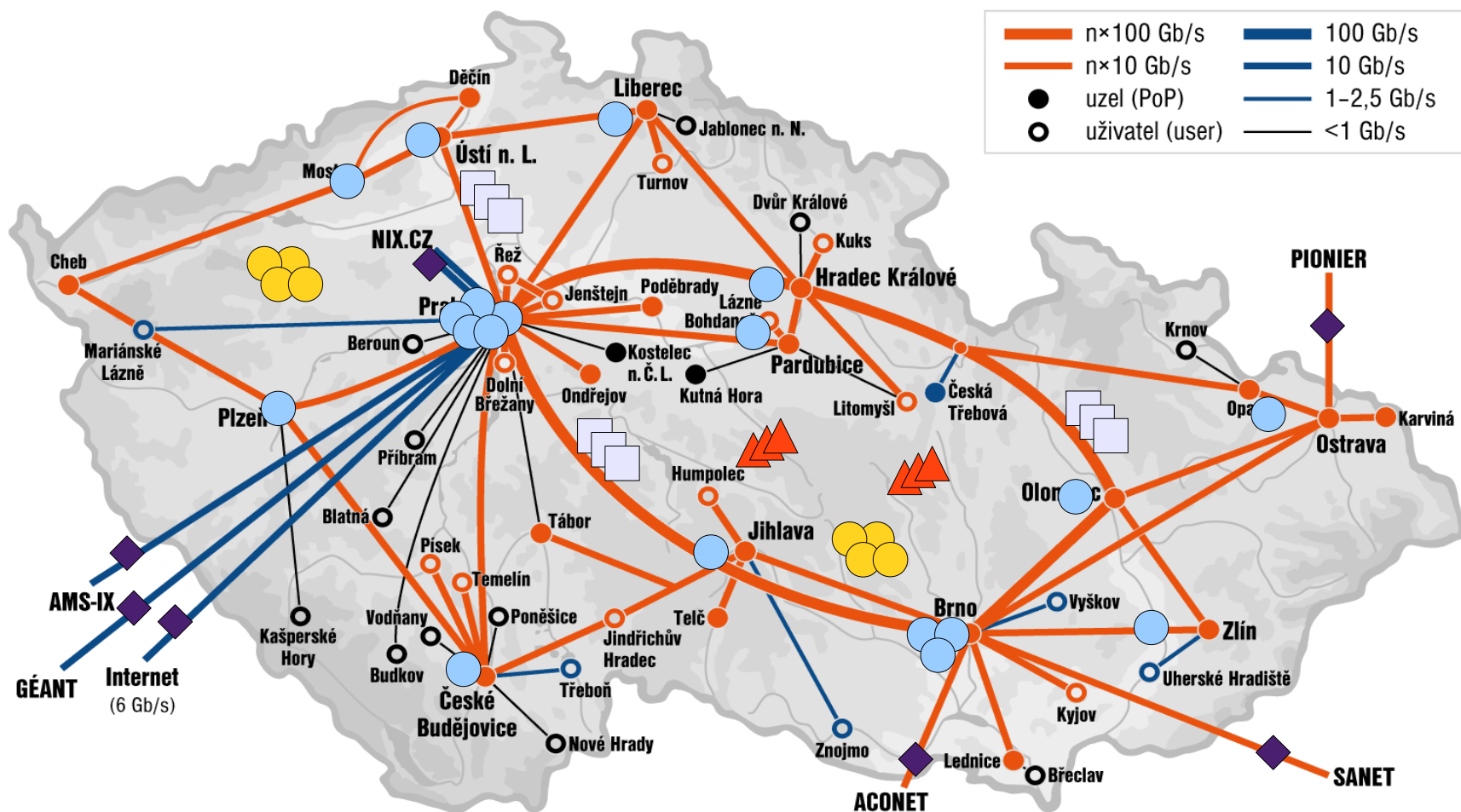
Andrea Kropáčová  
andrea@cesnet.cz



- Provozuje síť národního výzkumu a vzdělávání CESNET2
- Připojeno 27 členů (české VŠ, Akademie věd 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**
- 2016 – 2020: *pokračování projektu Velká infrastruktura CESNET*
- Člen TF-CSIRT, Pracovní skupiny CSIRT.CZ, projektu Fenix



# 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

# Začátky ...

- Správci v připojených sítích provozují bezpečnostní nástroje
  - IDS, honeypoty, IPS, sondy, syslog, ...
    - Sledování stavu sítě, zdraví sítě
    - Hledání kompromitovaných zařízení
    - Detekce útoků, anomálií provozu
- DILEMA – Co s daty, pro která nemám použití?
  - Zahodit?
    - To je škoda a plýtvání
  - Reportovat?
    - To je zase moc pracné, s potenciálem přejít do diskuse, dožadování se pomoci, dalších informací atd...

# Začátky ...

- Správci v připojených sítích provozují bezpečnostní nástroje
  - IDS, honeypoty, IPS, sondy, syslog, ...
    - Sledování stavu sítě, zdraví sítě
    - Hledání kompromitovaných zařízení
    - Detekce útoků, anomálií provozu
- DILEMA – Co s daty, pro která nemám použití?
  - Zahodit?
    - To je škoda a plýtvání
  - Reportovat?
    - To je zase moc pracné, s potenciálem přejít do diskuse, dožadování se pomoci, dalších informací atd...

## Sdílet!

- Jak? A co formát? Obsah? Protokol? Klasifikace? Politika?



- Systém pro efektivní sdílení informací o bezpečnostních incidentech
- Client/server architektura (**transport**, ne naskladnění dat)
- Komunitní přístup (aka „budujme bezpečnost společně“)
  - Tvoje data jsou dostupná celé Warden komunitě
  - Data celé komunity jsou dostupná Tobě

- **Zasílající a odebírající klienti**

- Událost (event)

- Bezpečnost

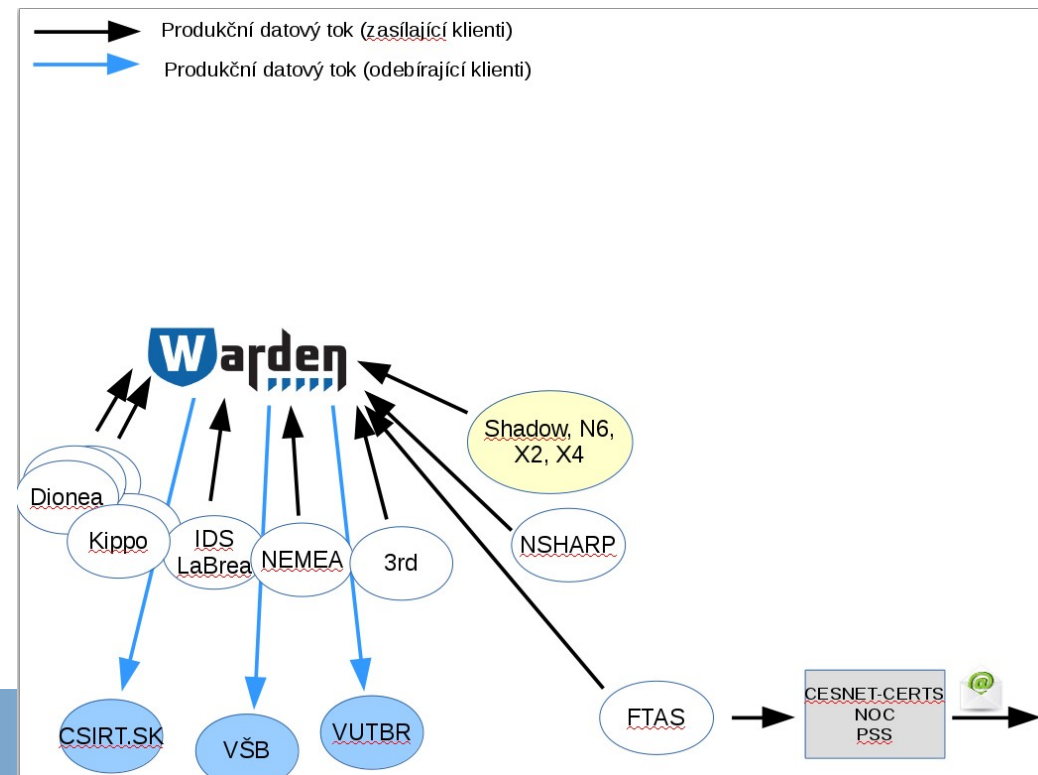
  - X509

  - encryption

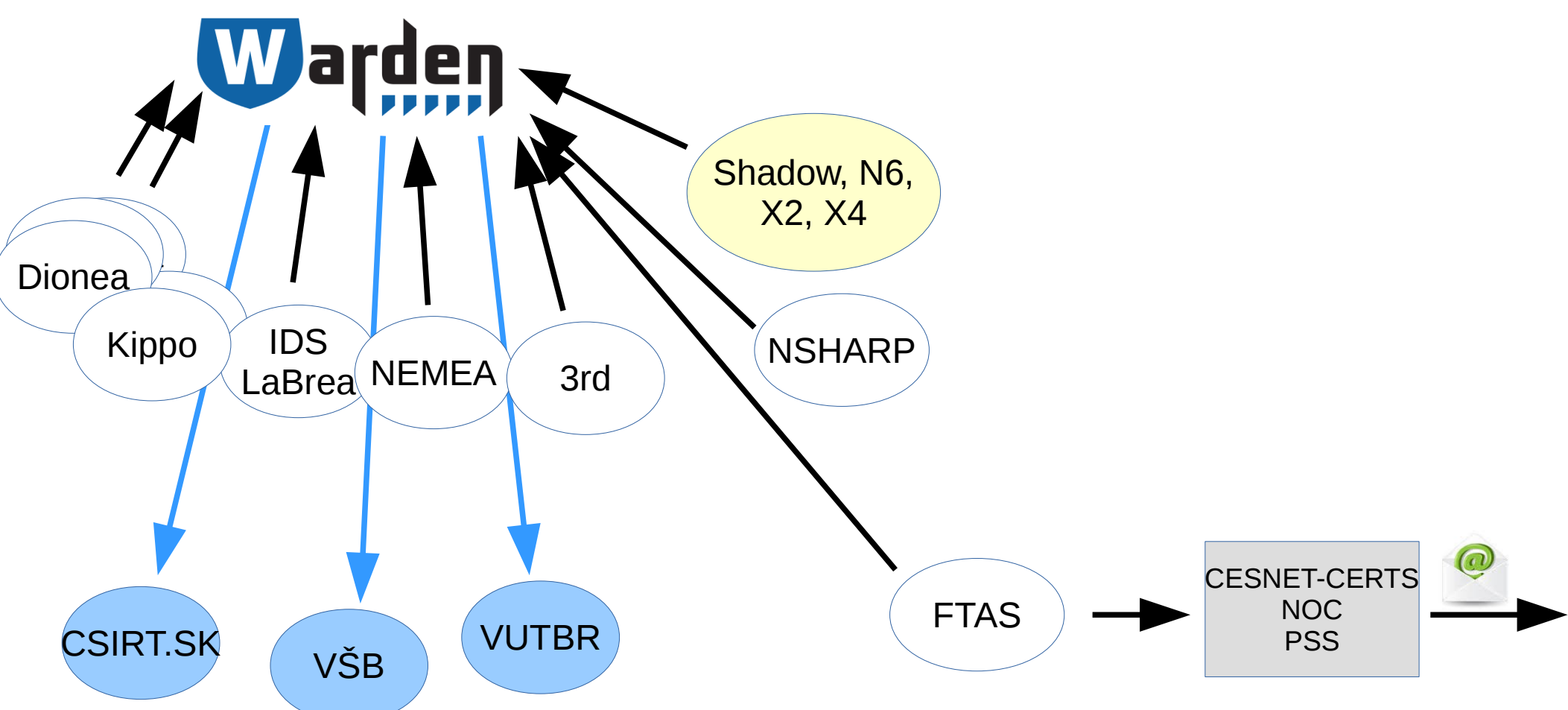
  - “sanity” checks

  - peer review

- IDEA formát



→ Produkční datový tok (zasílající klienti)  
→ Produkční datový tok (odebírající klienti)





- Systém pro efektivní sdílení informací o bezpečnostních incidentech
- Client/server architektura (**transport**, ne naskladnění dat)
- Komunitní přístup (aka „budujme bezpečnost společně“)
  - Tvoje data jsou dostupná celé Warden komunitě
  - Data celé komunity jsou dostupná Tobě

- **Zasílající a odebírající klienti**

- Událost (event)

- Bezpečnost

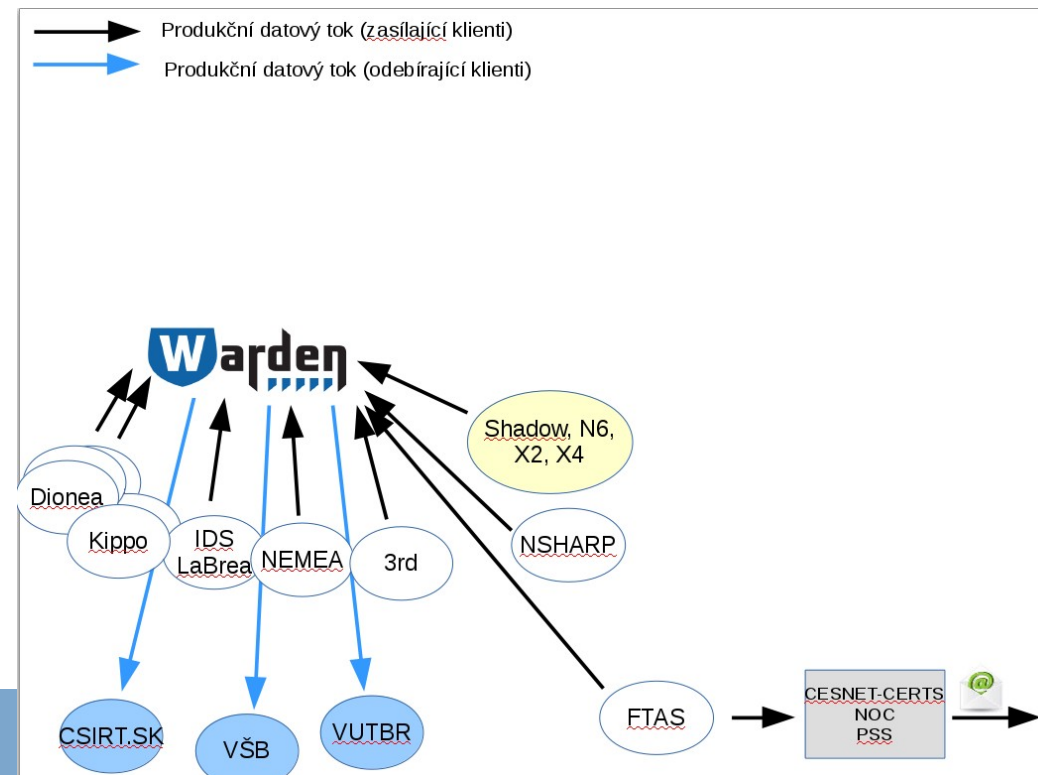
  - X509

  - encryption

  - “sanity” checks

  - peer review

- IDEA formát







- **Zasílající klienti**

- IDS, IPS, honeypoty (Kippo, Dionea), logy, sondy ...
- 22 klientů z 6 členských sítí (univerzit)
- Cca 1,5 mil událostí

- **Odebírající klienti**

- TT, FW, Antispam obrana, filtry, QoS
- Mentat systém provozovaný CESNET

# Formát IDEA

## Botnet C&C


```
{
  "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]
    }
  ]
}
```

## Honeypot

```
{
  "Format": "IDEA0",
  "ID": "2E4A3926-B1B9-41E3-89AE-B6B474EB0A54",
  "DetectTime": "2014-03-22T10:12:31Z",
  "Category": ["Recon.Scanning"],
  "ConnCount": 633,
  "Description": "EPMAPPER exploitation attempt",
  "Ref": ["cve:CVE-2003-0605"],
  "Source": [
    {
      "IP4": ["93.184.216.119"],
      "Proto": ["tcp", "epmap"],
      "Port": [24508]
    }
  ],
  "Target": [
    {
      "Port": [135]
    }
  ]
}
```

- JSON
- Jednoduchý, rozšiřitelný formát
- Jednou definované klíče a typy se ale nemění
- Dokážeme rozlišit primární data, agregovaná data, korelovaná data
- <https://idea.cesnet.cz>


# Lesson learned I

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

=

nedokáží data odebrat a zpracovat si je.

# Lesson learned I

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

=

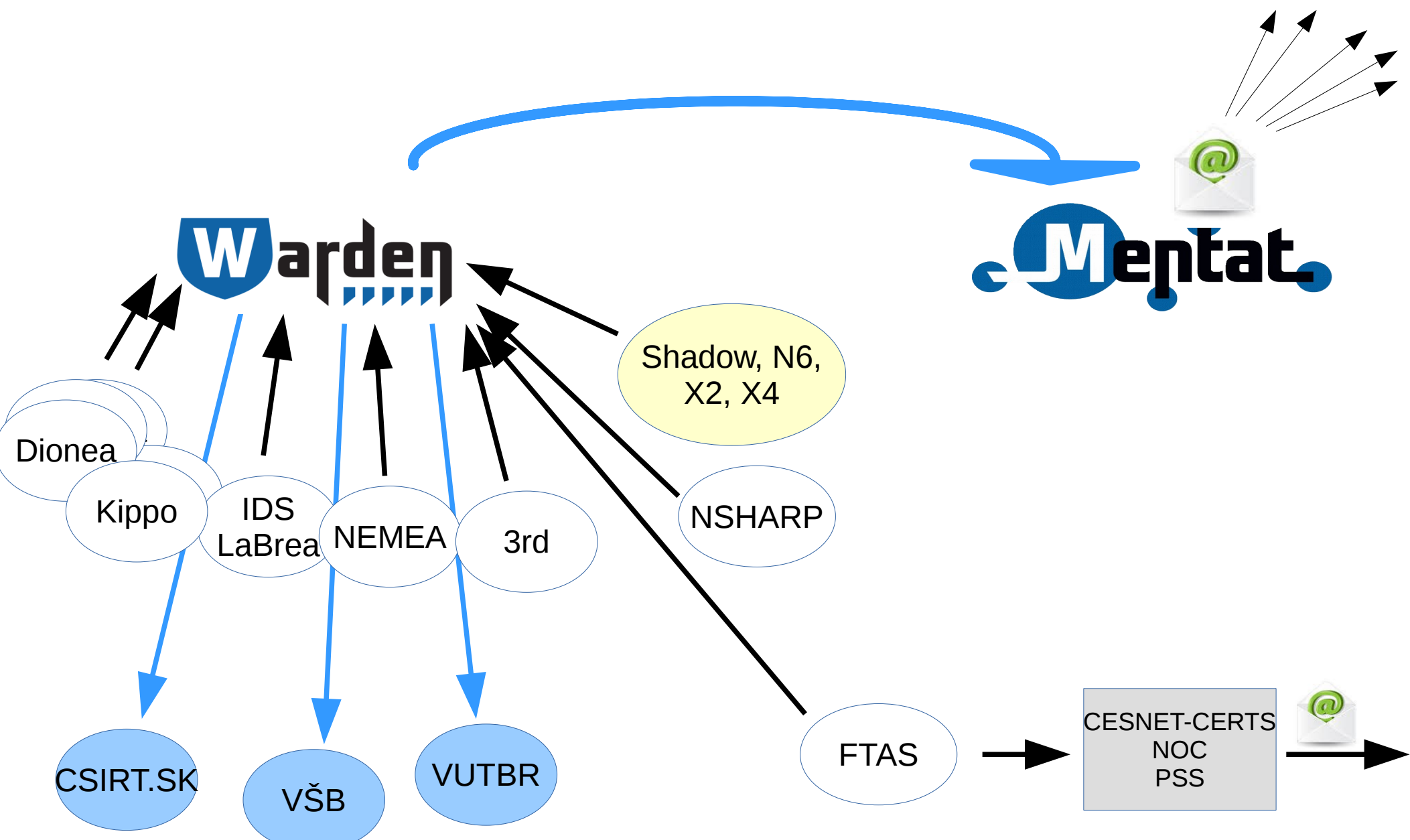
nedokáží data odebrat a zpracovat si je.

**Ale chtějí tato data získávat, data jsou užitečná**

=

**je nutné je správcům doručit zpracovaná.**

→ Produkční datový tok (zasílající klienti)  
→ Produkční datový tok (odebírající klienti)



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 resolvers 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

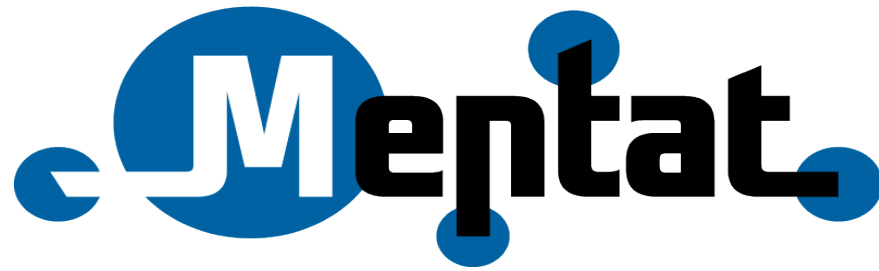
Více informací o tomto typu události lze nalézt na adrese:

<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.



- Z hlediska architektury Warden je Mentat **odebírající klient**
- SIEM
- Skladiště informací
- Zpracovává data (události) z Warden a od třetích stran (N6, ShadowServer, ...)
- Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
  - opřeno o RIPE DB
- Reporty zasílá do koncových sítí (abuse@...)

# Lesson learned II

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme dělat.
- Chci mít možnost report strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Tyto informace nechceme vůbec, odebíráme je 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 hierarchií správy (Uni → Fakulta → Katedra → Pracoviště)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to reportujete znova? Včera jsem to vyřešil.



# Lesson learned II

... reakce od příjemců reportů ...

- **Málo informací, nevíme co s tím máme dělat.**
- Chci mít možnost report strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Tyto informace nechceme vůbec, odebíráme je 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 hierarchií správy (Uni → Fakulta → Katedra → Pracoviště)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to reportujete znova? Včera jsem to vyřešil.

# Formát IDEA

## Botnet C&C

```
{
  "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]
    }
  ]
}
```

## Honeypot

```
{
  "Format": "IDEA0",
  "ID": "2E4A3926-B1B9-41E3-89AE-B6B474EB0A54",
  "DetectTime": "2014-03-22T10:12:31Z",
  "Category": ["Recon.Scanning"],
  "ConnCount": 633,
  "Description": "EPMAPPER exploitation attempt",
  "Ref": ["cve:CVE-2003-0605"],
  "Source": [
    {
      "IP4": ["93.184.216.119"],
      "Proto": ["tcp", "epmap"],
      "Port": [24508]
    }
  ],
  "Target": [
    {
      "Port": [135]
    }
  ]
}
```

- JSON
- Jednoduchý, rozšiřitelný formát
- Jednou definované klíče a typy se ale nemění
- Dokážeme rozlišit primární data, agregovaná data, korelovaná data
- <https://idea.cesnet.cz>

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 resolvers 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 II

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme dělat.
- **Chci mít možnost report strojově zpracovat.**
- Spěchá to? Jakou to má závažnost?
- Tyto informace nechceme vůbec, odebíráme je 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 hierarchií správy (Uni → Fakulta → Katedra → Pracoviště)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to reportujete znova? Včera jsem to vyřešil.

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 resolvers 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 # SECTION 1
#
(Více pro # Analyzer | X2
# Detector | cesnet.au1
# Description | Open DNS Resolver
UPOZORNĚNÍ: U # Categories | Vulnerable.Config
(zejména exte # Reference | https://csirt.cesnet.cz/cs/services/x2
#
# událostech i ##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
Kompletní dos t
v příslušných 2015-11-13 02:29:49Z;2015-11-11 12:20:35Z;X2;cesnet.au1;Open DNS Resolver;Vulner
V závislosti n able.Config;158.194.189.46;189-46.kolejnet.upol.cz;-;-;udp/dns;-;-;1447381789;14
Doporučujeme 47244435;-;System 158.194.189.46 is ORR and can be misused to DDoS attacks
```

# Lesson learned II

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme dělat.
- Chci mít možnost report strojově zpracovat.
- **Spěchá to? Jakou to má závažnost?**
- Tyto informace nechceme vůbec, odebíráme je 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 hierarchií správy (Uni → Fakulta → Katedra → Pracoviště)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to reportujete znova? Včera jsem to vyřešil.

## Report M20151113M-KFrDb

Vážený kolegové,

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

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

- [1] Stroje na následujících IP adresách fungují jako otevřené DNS resolvers 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 II

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme dělat.
- Chci mít možnost report strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- **Tyto informace nechceme vůbec, odebíráme je 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 hierarchií správy (Uni → Fakulta → Katedra → Pracoviště)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- Proč mi to reportujete znova? Včera jsem to vyřešil.



# 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

Update reporting filter for abuse@cesnet.cz

**Filter ID:**

**Description:**

Enabled  
 Simple filter

**Analyzers:**

- Beekeeper
- Dionaea
- Fail2Ban
- Kippo
- LaBrea
- Mentat
- N6

**Classifications:**

- (D)DoS
- Botnet Command and Control
- Bruteforce
- Copyright infringement
- Malware
- Other
- Phishing
- Portscan

**Sources:**

195.113.144.XXX

Advanced filter

**Filter:**

(Node/SW eq "SSERV") and (Description eq "Scan NTP") and (Source/IP4 in [195.113.144.XXX])

# Lesson learned II

... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme dělat.
- Chci mít možnost report strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Tyto informace nechceme vůbec, odebíráme je 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 hierarchií správy** (Uni → Fakulta → Katedra → Pracoviště)
  - **Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.**
- Proč mi to reportujete znova? Včera jsem to vyřešil.

**Browse » List of 2387 objects**

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

**Browse » List of 2387 objects**

Key	Value
inetnum	147.32.0.0 - 147.32.255.255
netname	CVUT-TCZ
descr	Czech Technical University
descr	Prague
country	CZ
org	<a href="#">ORG-CVUT1-RIPE</a> → Ceske vysoke uceni technicke v Praze
admin-c	<a href="#">CVUT1-RIPE</a> → Ceske vysoke uceni technicke v Praze Network Admins
tech-c	<a href="#">CVUT1-RIPE</a> → Ceske vysoke uceni technicke v Praze Network Admins
status	LEGACY
remarks	For information on "status:" attribute read <a href="https://www.ripe.net/data-tools/db/faq/faq-status-val">https://www.ripe.net/data-tools/db/faq/faq-status-val</a>
mnt-by	<a href="#">TENCZ-MNT</a> → TEN-xxxCZ/CESNET2 IP Space Maintainer
remarks	Please report network abuse -> <a href="mailto:abuse@cvut.cz">abuse@cvut.cz</a>
changed	<a href="mailto:ors@Czechia.EU.net">ors@Czechia.EU.net</a> 19960804
changed	<a href="mailto:er-transfer@ripe.net">er-transfer@ripe.net</a> 20060518
changed	<a href="mailto:tkpv@cesnet.cz">tkpv@cesnet.cz</a> 20130704
created	2006-05-18T10:44:11Z
last-modified	2015-05-05T01:56:34Z
source	RIPE
client-id	C030000

<b>inetnum</b>	<b>147.32.1.0 – 147.32.50.255</b>
<b>netname</b>	<b>CVUT-TCZ</b>
<b>descr</b>	<b>Praha 1</b>
<b>remarks</b>	<b>Report network abuse --&gt; <a href="mailto:abuse@p1.cvut.cz">abuse@p1.cvut.cz</a></b>

<b>inetnum</b>	<b>147.32.60.0 – 147.32.100.255</b>
<b>netname</b>	<b>CVUT-TCZ</b>
<b>descr</b>	<b>Praha 6</b>
<b>remarks</b>	<b>Report network abuse --&gt; <a href="mailto:abuse@p6.cvut.cz">abuse@p6.cvut.cz</a></b>

<b>inetnum</b>	<b>147.32.101.0 – 147.32.150.255</b>
<b>netname</b>	<b>CVUT-TCZ</b>
<b>descr</b>	<b>Praha 10</b>
<b>remarks</b>	<b>Report network abuse --&gt; <a href="mailto:abuse@p10.cvut.cz">abuse@p10.cvut.cz</a></b>

inetnum	147.33.0.0 - 147.33.255.255
netname	VSCHT-TCZ
descr	Vysoka skola chemicko-technologicka v Praze
descr	Praha 6
country	CZ
org	<a href="#">ORG-VSCV1-RIPE</a> → Vysoka skola chemicko-technologicka v Praze
admin-c	<a href="#">VSCN1-RIPE</a> → Vysoka skola chemicko-technologicka Network Admins
tech-c	<a href="#">VSCN1-RIPE</a> → Vysoka skola chemicko-technologicka Network Admins
status	LEGACY
mnt-by	<a href="#">RIPE-NCC-LEGACY-MNT</a> → ???
mnt-by	<a href="#">TENCZ-MNT</a> → TEN-xxxCZ/CESNET2 IP Space Maintainer
remarks	Please report network abuse -> <a href="mailto:abuse@vscht.cz">abuse@vscht.cz</a>
changed	<a href="mailto:ors@Czechia.EU.net">ors@Czechia.EU.net</a> 19961228

<b>inetnum</b>	<b>147.32.160.0 – 147.32.180.255</b>
<b>netname</b>	<b>CVUT-TCZ</b>
<b>descr</b>	<b>Praha 8</b>
<b>remarks</b>	<b>Report network abuse --&gt; <a href="mailto:abuse@p8.cvut.cz">abuse@p8.cvut.cz</a></b>

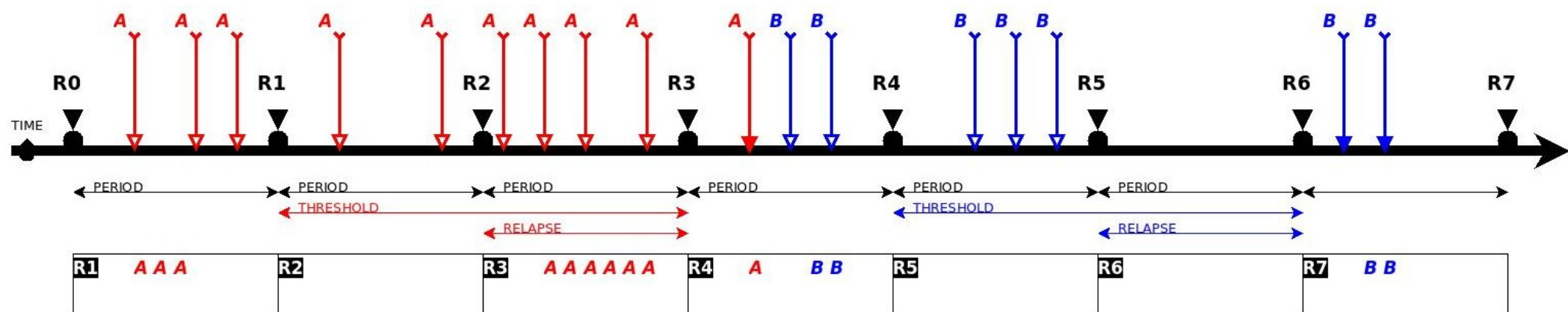
<b>inetnum</b>	<b>147.32.200.0 – 147.32.220.255</b>
<b>netname</b>	<b>CVUT-TCZ</b>
<b>descr</b>	<b>Praha 6</b>
<b>remarks</b>	<b>Report network abuse --&gt; <a href="mailto:abuse@p66.cvut.cz">abuse@p66.cvut.cz</a></b>

# Lesson learned II

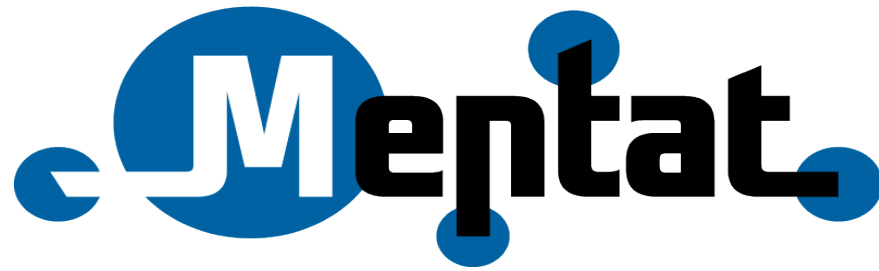
... reakce od příjemců reportů ...

- Málo informací, nevíme co s tím máme dělat.
- Chci mít možnost report strojově zpracovat.
- Spěchá to? Jakou to má závažnost?
- Tyto informace nechceme vůbec, odebíráme je 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 hierarchií správy (Uni → Fakulta → Katedra → Pracoviště)
  - Příjemce musí report rozebrat, přebalíčkovat a poslat do podsítí.
- **Proč mi to reportujete znova? Včera jsem to vyřešil.**

# 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

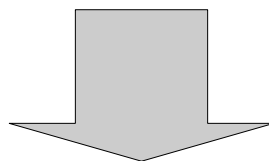


- SIEM
- Skladiště informací
- Zpracovává data (události) z Warden a od třetích stran (N6, ShadowServer, ...)
- Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
- Reporty zasílá do koncových sítí (abuse@...)
- Podpůrný nástroj CESNET-CERTS a bezpečnostní týmy připojených organizací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

# Statistiky

- **Warden**

- 22 zasílajících klientů (zdrojů dat typu “bezpečnostní událost”)
- cca 1,5 mil událostí za den



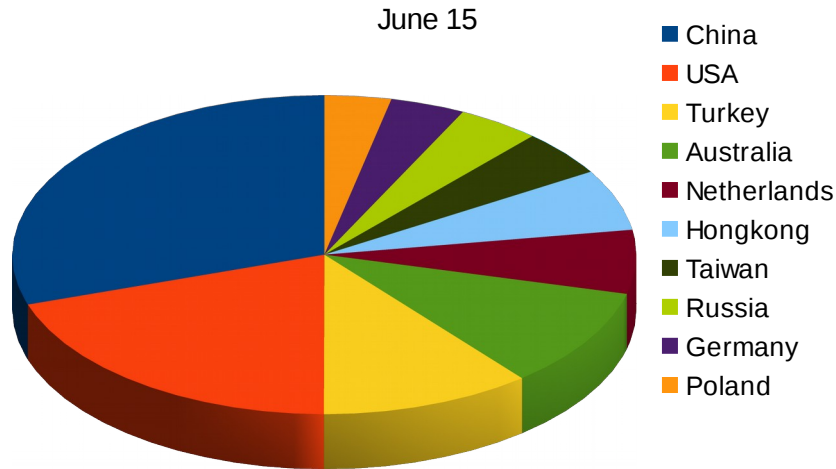
- **Mepstat**

- cca 80 reportů denně, cca 360 týdně (na cca 320 připojených organizací)

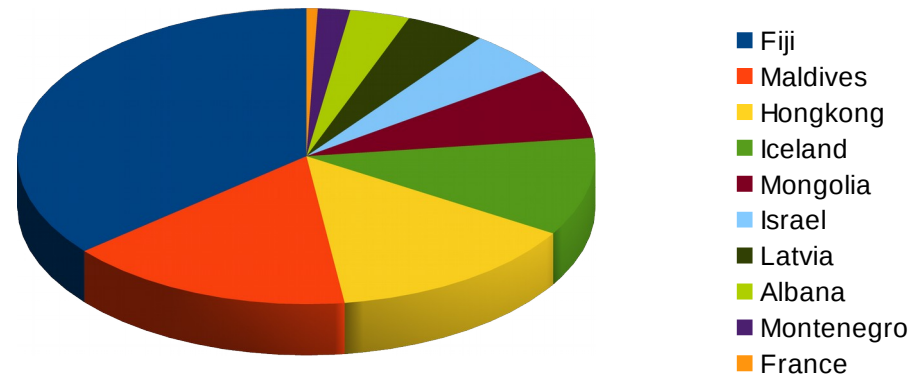


# Statistiky

Incident TOP10 share by country

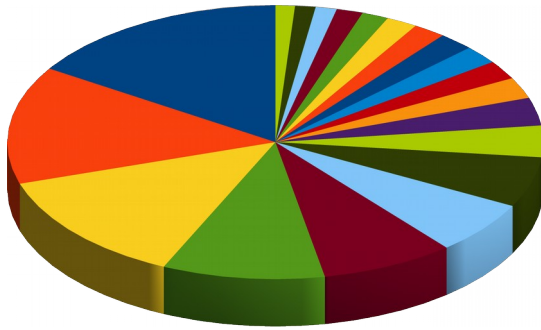


Incident TOP10 share  
according to number of incidents  
per one IP in the country  
June 2015



## TOP 20 incident share by AS

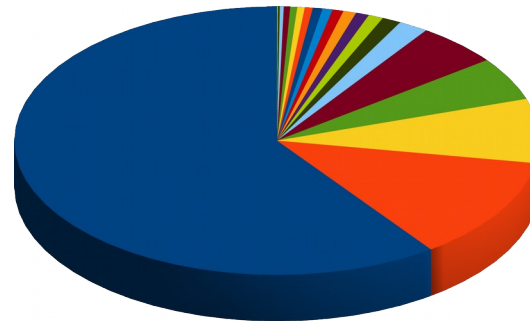
June 2015



- 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

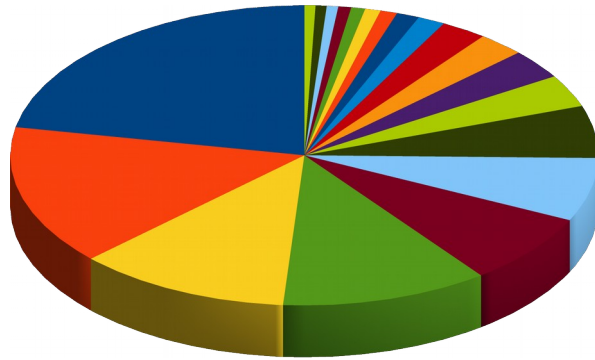
according to number of incidents  
per one IP from AS  
June 2015



- HOT NET LIMITED
- Przedsiębiorstwo Usług Specjalistycznych ELAN mgr inż.
- 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

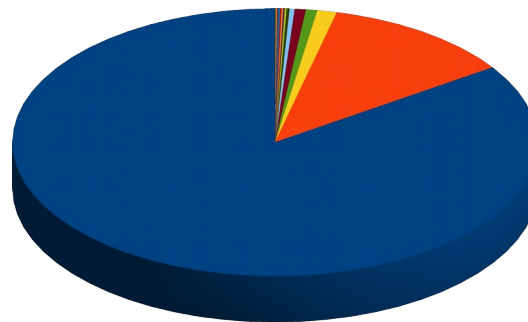
June 2015



- 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.

# Lesson learned III

... současnost & budoucnost ...

- Umíme data dostat na jedno místo, zpracovat a doručit.
- **ALE!**
  - Sdílet syrová *primární* data nestačí!
  - Data získaná z bezpečnostních nástrojů jedné sítě nestačí!
  - Sdílet na úrovni jedné sítě (ISP/organizace) nestačí!

# Lesson learned III

... současnost & budoucnost ...

- Umíme data dostat na jedno místo, zpracovat a doručit.
- **ALE!**
  - Sdílet syrová *primární* data nestačí!
  - Data získaná z bezpečnostních nástrojů jedné sítě nestačí!
  - Sdílet na úrovni jedné sítě (ISP/organizace) nestačí!
- **Proč?**
  - Primárních dat je moc a mají různou vypovídací hodnotu.
  - Některé problémy nemusíme zaznamenat.
  - Chybí souvislosti, nevidíme celkový obraz.

# Co dál ...

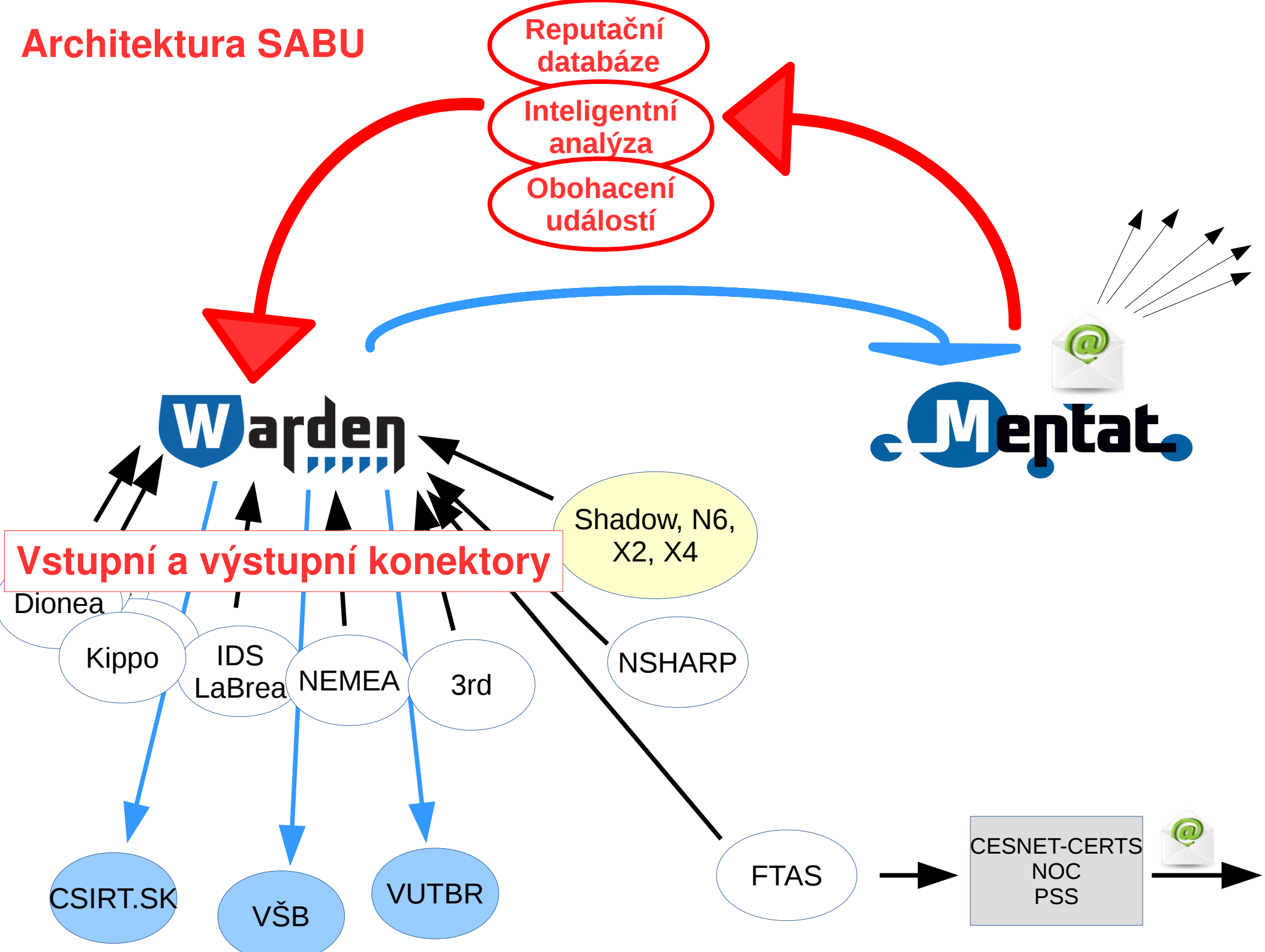
- Nové a další zdroje primárních dat v síti CESNET2
- Nové a další zdroje primárních dat mimo síť CESNET2
- Nové zdroje od tzv. třetích stran
- **Obohacení dat**
- **Lepší validace a klasifikace dat**
- **Intelligentní analýzy, korelace**
- **Reputační databáze** („historie ke konkrétní IP adrese/síti“)
- Sdílení dat a informací na národní a mezinárodní úrovni

*„ ... více, rychleji, kvalitněji ... “*

# SABU

- Sdílení a Analýza Bezpečnostních Událostí
- 2016 – 2020, Projekt Ministerstva vnitra ČR
- Řešitelé: CESNET, Masarykova univerzita
- <https://sabu.cesnet.cz> – stránky jsou ve výstavbě
  
- Partneri:
  - CSIRT.SK
  - ISP
  - Bankovní sektor
  - Invea Technologies

# Architektura SABU





# Přínosy

- Podpora a rozvoj spolupráce
- Vysoká kvalita sdílených dat (čištění) a informací
- Standardizace kanálu pro předávání dat mezi bezpečnostními týmy (povinnými osobami dle zákona o kybernetické bezpečnosti)
  
- Více informací
- Lepší ochrana sítě
- Zefektivnění reakce na incidenty
- Prevence

# Zpojení partnerů

# Zapojení partnerů

- Zasílání dat

- Provozujete bezpečnostní nástroj a jste ochotní data sdílet?
  - Jaká data?
  - Za jakých podmínek? Částečná anonymizace? Jen data relevantní pro CESNET2?
- Máte vhodné místo v síti pro umístění nějakého bezp. Nástroje?

- Odebírání dat

- Přímo (konektor, vlastní zpracování, naskladnění a využití)
- Formou e-mail reportu
  - Ze systému Mentat
  - Data příslušející Vaší organizaci
  - Bezpečnostní události, kde zdrojem je IP adresa z Vaší sítě

Děkuji za pozornost.

Andrea Kropáčová, [andrea@cesnet.cz](mailto:andrea@cesnet.cz)



- [warden.cesnet.cz](http://warden.cesnet.cz), [idea.cesnet.cz](http://idea.cesnet.cz)
- Python
- Server
  - db schéma, skripty, certifikáty, Apache, filer
- Klienti
  - klientská knihovna
  - klienti pro Kippo, Dionea, fail2ban, *FlowMon*
- Kalibrace serveru
  - 2x CPU po 12 jádrech
  - 32 GB paměti (8 GB je ok)
  - Ne thready, procesy
  - 37GB DB = měsíc naskladněných událostí