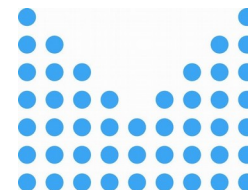


Projekt **SABU**

Sdílení a analýza bezpečnostních událostí

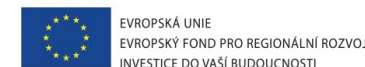
CESNET, z. s. p. o.

Andrea Kropáčová
andrea@cesnet.cz

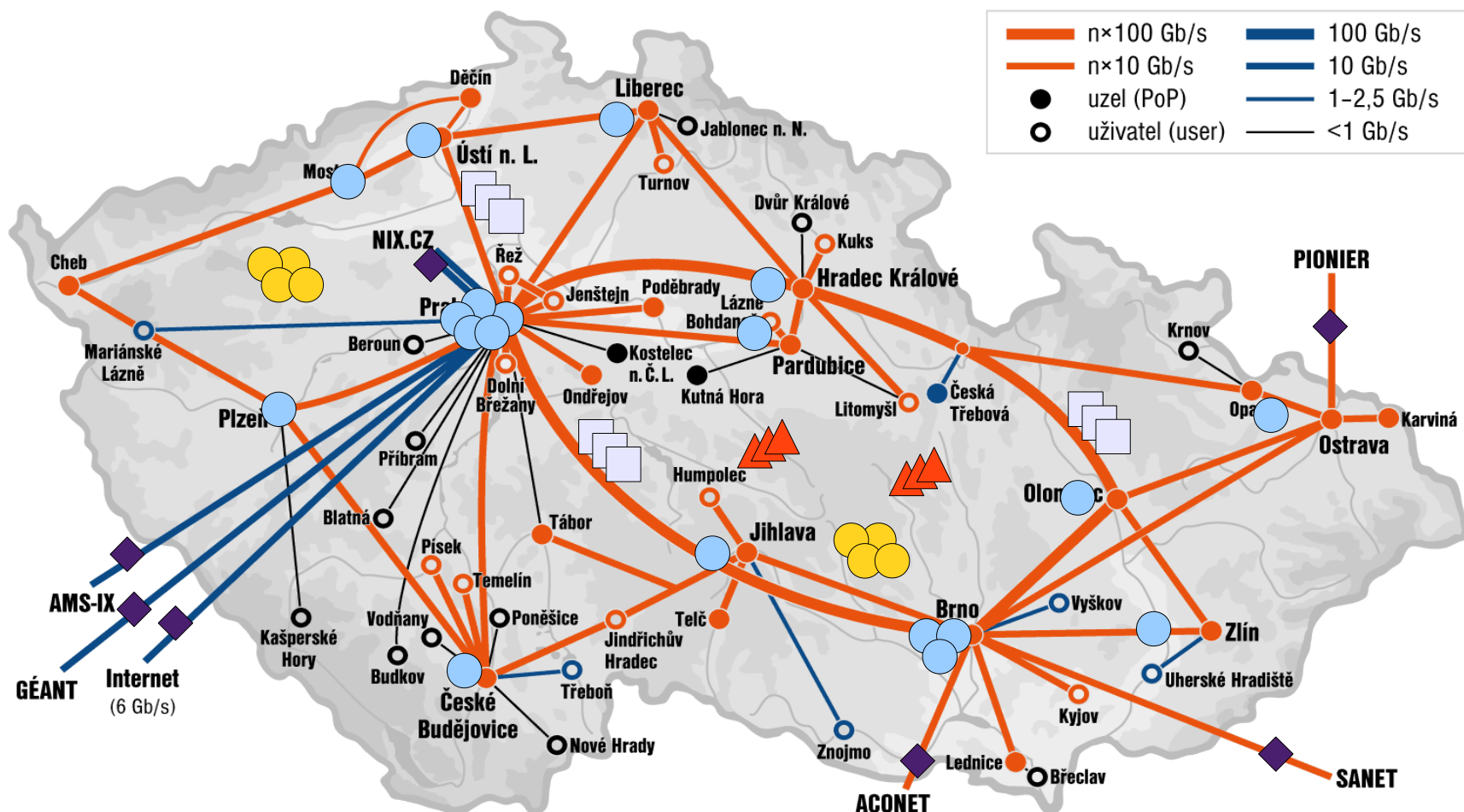


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

- 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: **Projekt E-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...

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

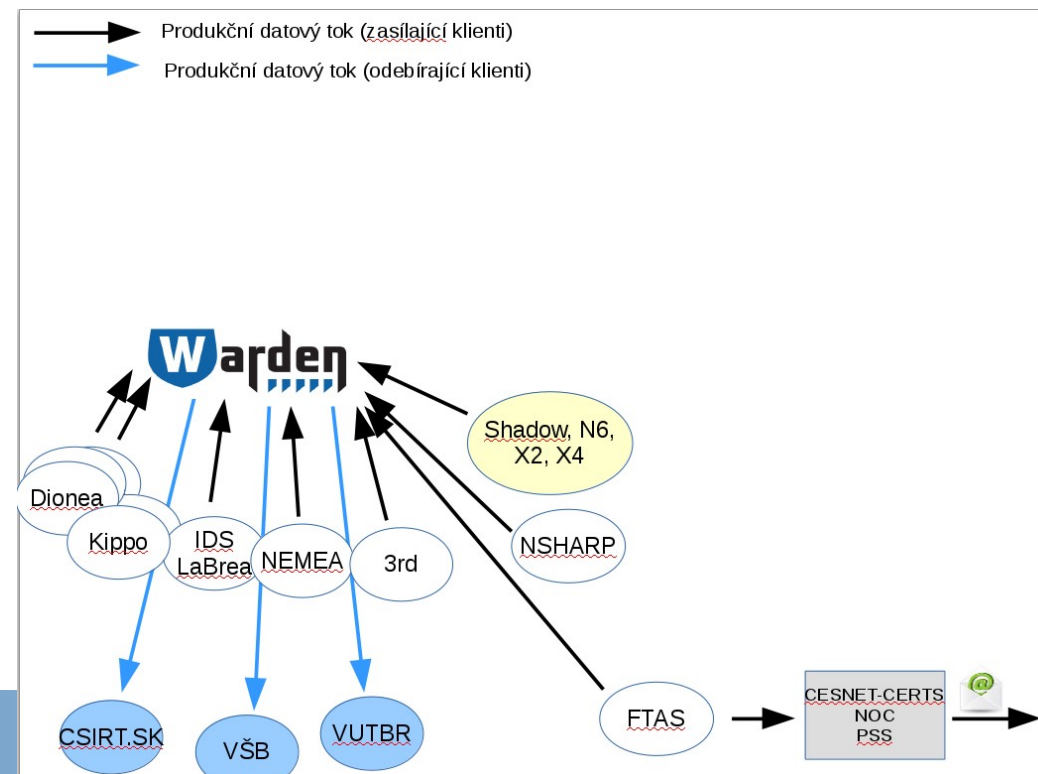
X509

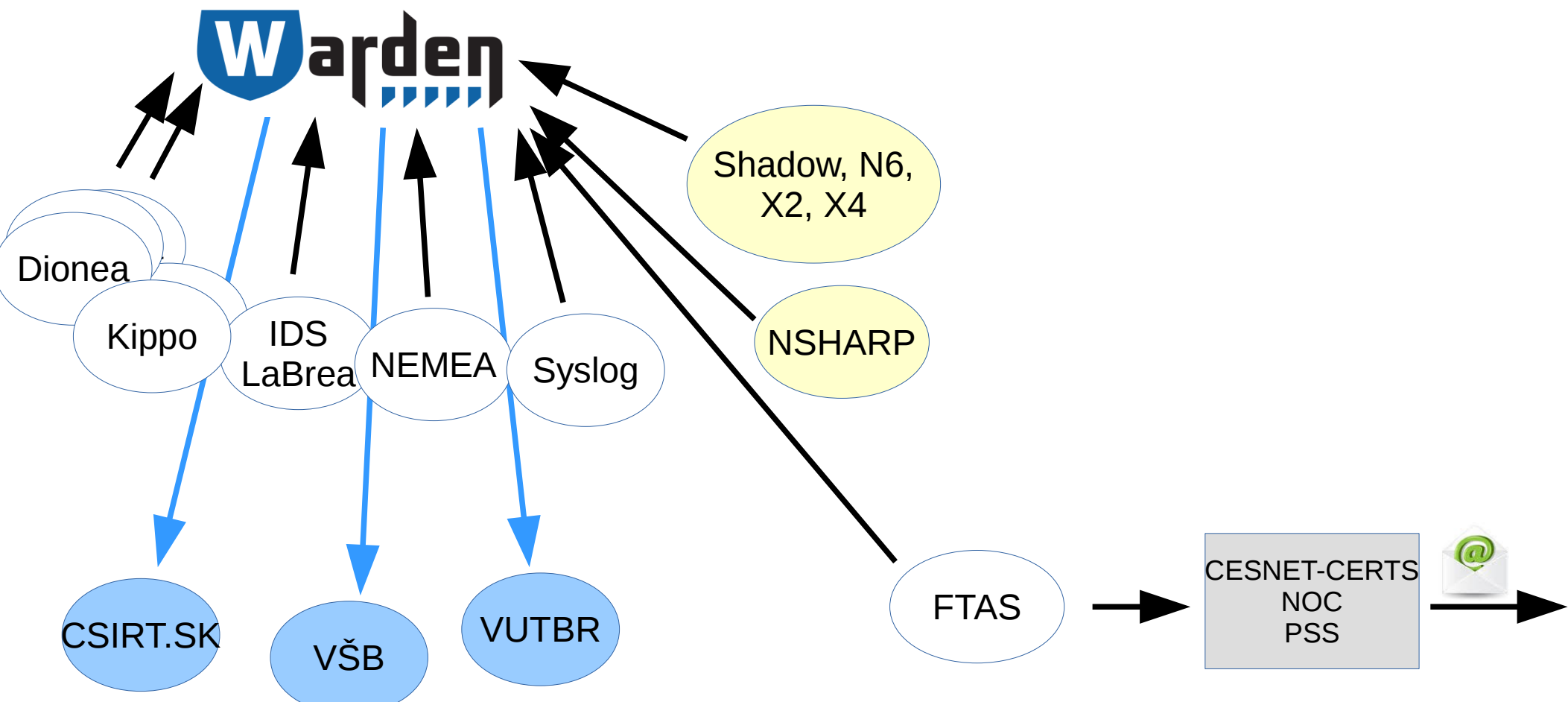
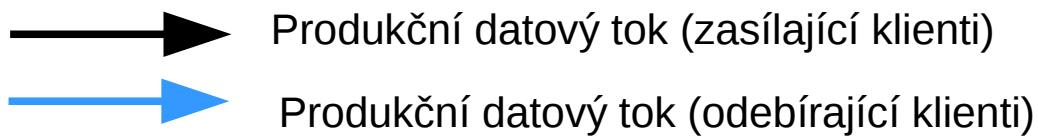
encryption

“sanity” checks

peer review

- IDEA formát







- **Zasílající klienti**

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

- **Odebírající klienti**

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

Lesson learned I

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

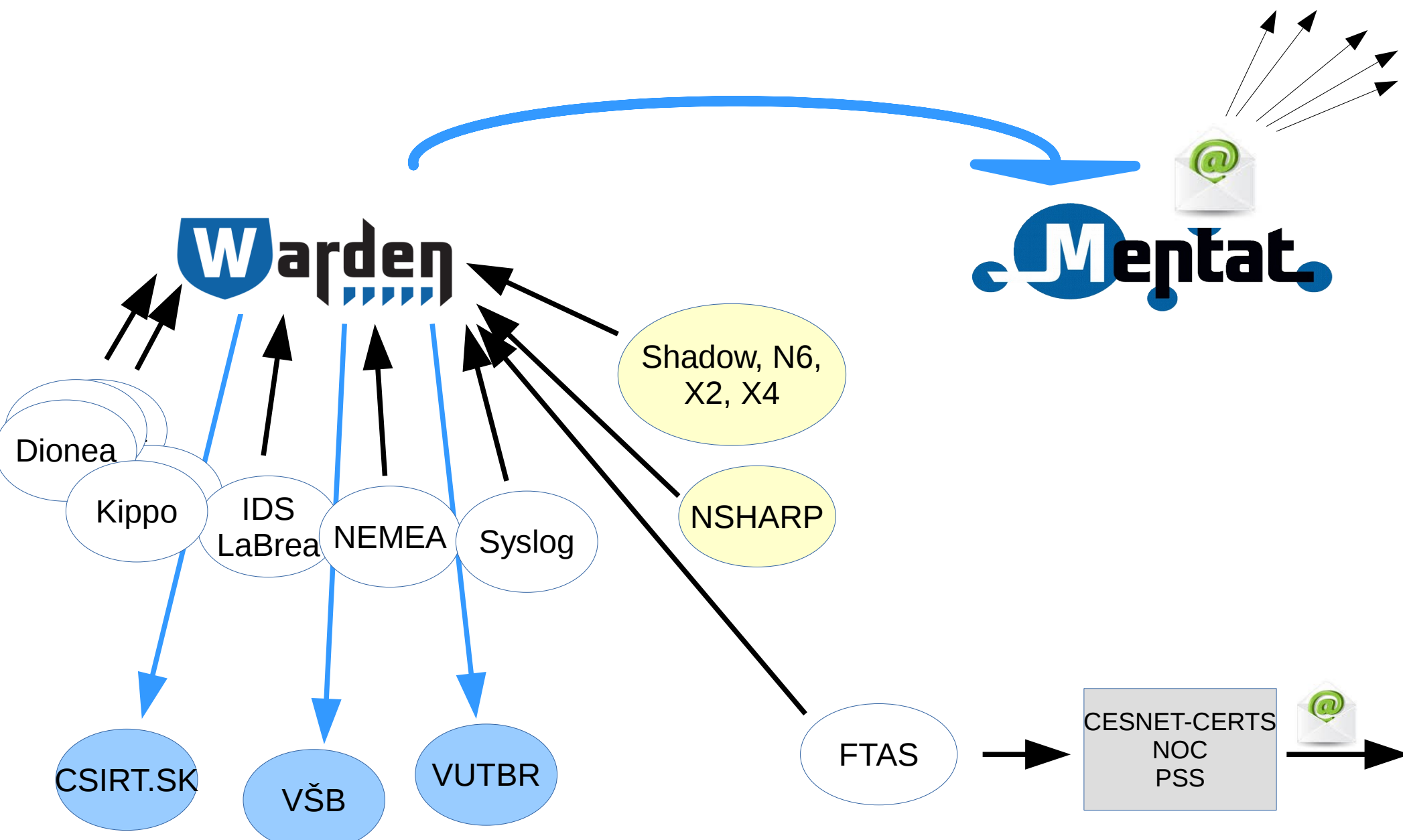
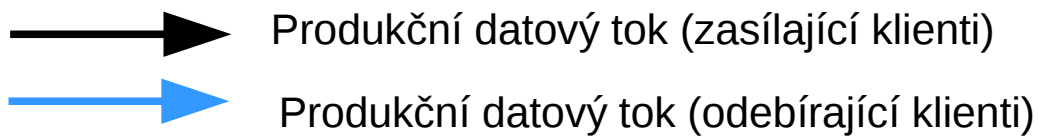
=

nedokáží data odebrat a zpracovat si je.

Ale chtějí tato data získávat, data jsou užitečná

=

je nutné je správcům doručit zpracovaná.



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

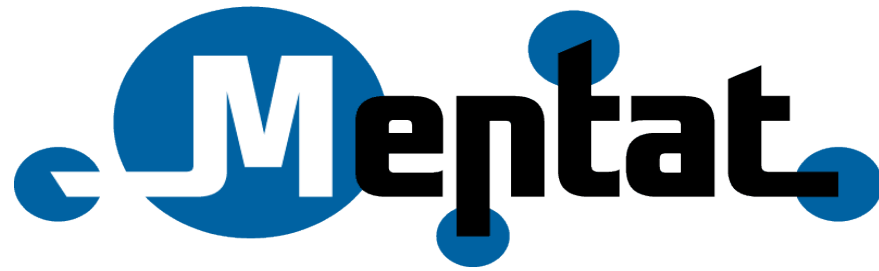
Více informací o tomto typu události lze nalézt na adrese:

<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)
 - Kontaktní informace získáváme z RIPE DB (www.ripe.net)
- Reporty zasílá do koncových sítí (abuse@...)
- <https://mentat.cesnet.cz>

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)

**Návod co dělat,
čeho se report týká**

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.

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://csirt.cesnet.cz/cs/services/x2>

(Více pro

UPOZORNĚNÍ: U

(zejména exte

událostech i

Kompletní dos

v příslušných

V závislosti 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
```

**Strojově
zpracovatelný formát
přidaný k e-mailovému
reportu**

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.

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:
NTP for time servers

Description:
Disable NTP events for time servers

☒ 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 eg "SSERV") and (Description eg "Scan NTP") and (Source/IP4 in [195.113.144.XXX])

Browse » List of 2387 objects

**Negistry umožňuje
jemněji naškálovat reportování
pro velké sítě se spojitým adresovým
rozsahem /16.**

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

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

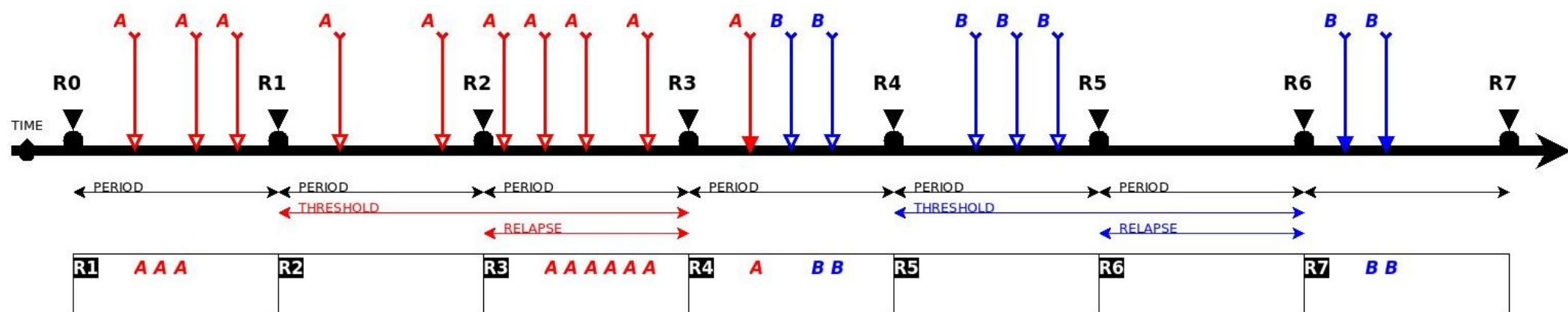
inetnum 147.32.101.0 – 147.32.150.255
netname CVUT-TCZ
descr Praha 10
remarks Report network abuse --> abuse@p10.cvut.cz

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

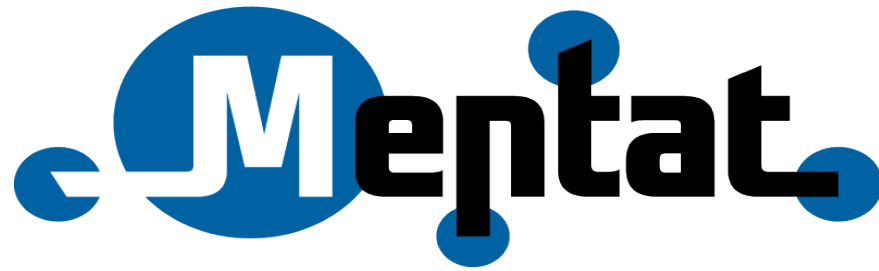
inetnum 147.32.160.0 – 147.32.180.255
netname CVUT-TCZ
descr Praha 8
remarks Report network abuse --> abuse@p8.cvut.cz

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

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

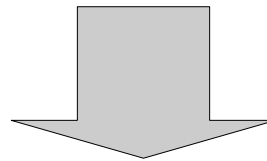


- SIEM
- Skladiště informací
- Zpracovává data (události) z Warden a od třetích stran (N6, ShadowServer, ...)
- Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
- Reporty zasílá do koncových sítí (abuse@...)
- Podpůrný nástroj CESNET-CERTS a bezpečnostní týmy připojených organizací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

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)

Lesson learned III

... současnost & budoucnost ...

- Nestačí

- **Sdílet pouze primární data** – příliš mnoho, pro les nevidíme stromy
- **Sdílet jen na úrovni jedné sítě** – o řadě problémů se nedozvíme
- **Sdílet jen data pro cílovou síť** – chybí souvislosti, vidíme les, ale ne krajinu

- Motivace

- Sítě jsou přirozeně nezávislé a řeší bezpečnost odděleně
- Sdílení informací a jejich využití je v plenkách
- V době útoku má každá síť **pouze část informace** a to ztěžuje rozhodnutí, co dělat → chybí adekvátní reakce
- Sdílení, obohacení a inteligentnější analýza umožní **efektivnější reakci**

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**
- **Inteligentní analýzy, korelace**
- Sdílení dat a informací na národní a mezinárodní úrovni

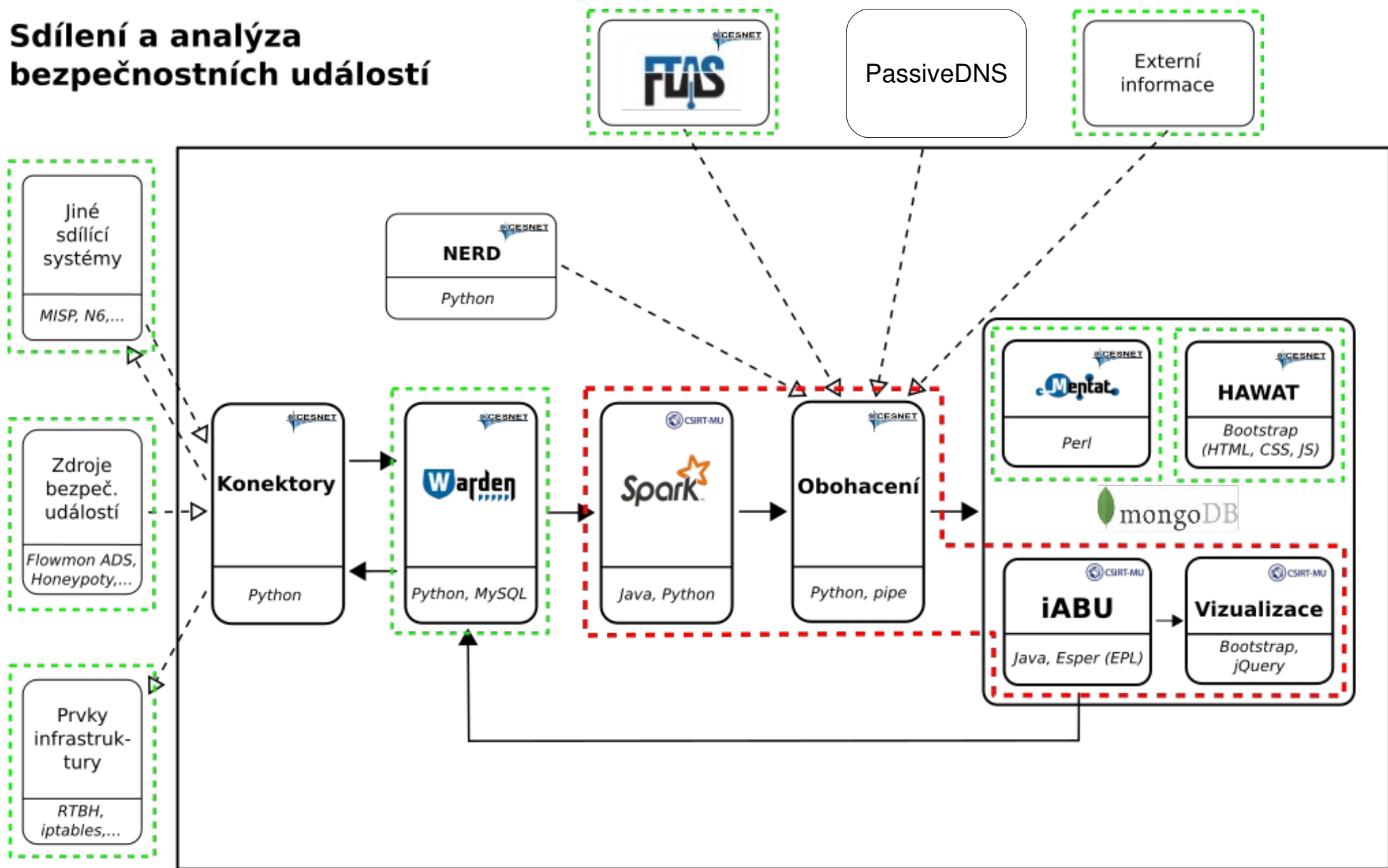
„ ... více, rychleji, kvalitněji ...“

SABU

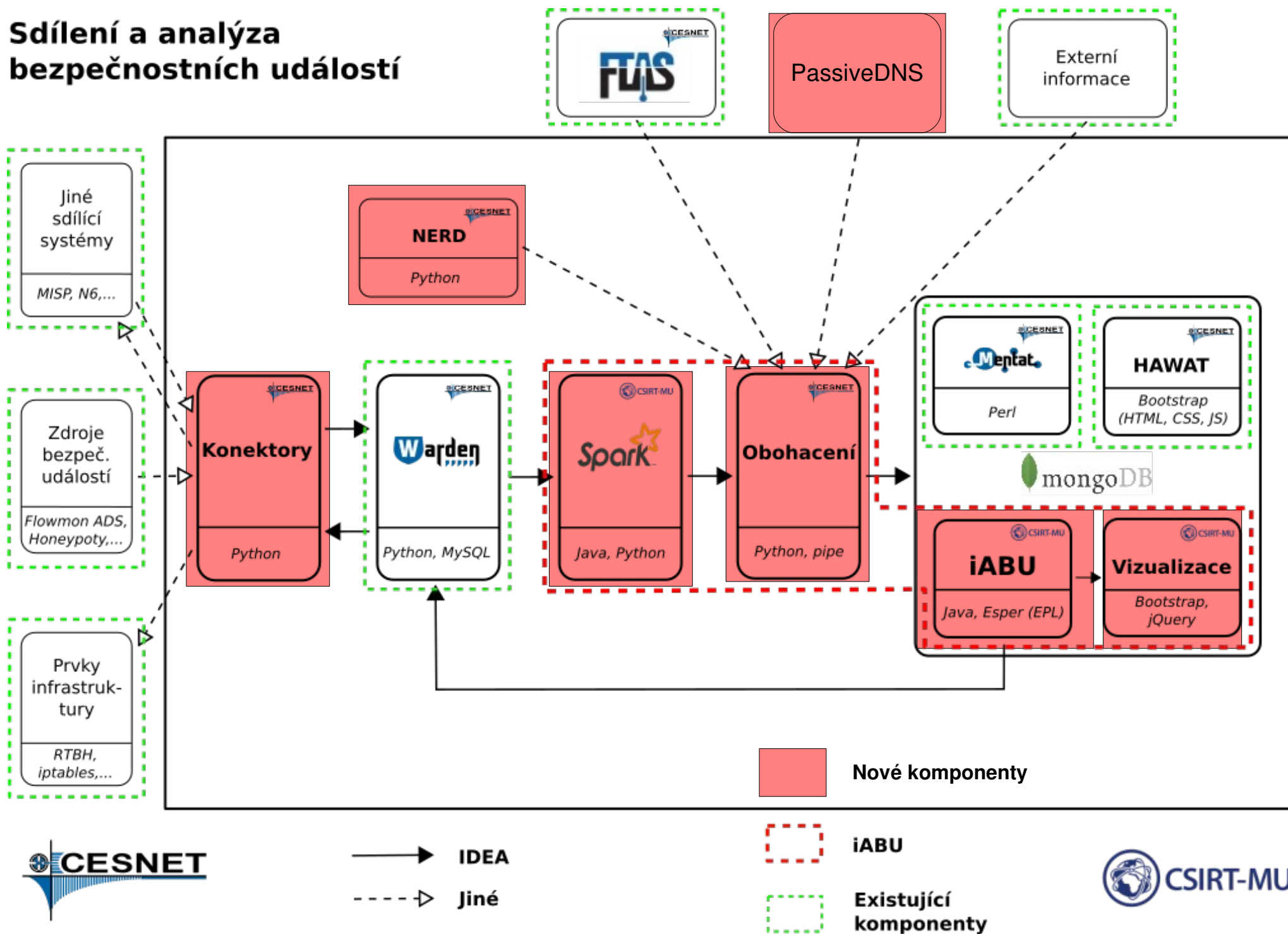
- **S**dílení a **A**nalýza **B**ezpečnostních **U**dálostí
- 2016 – 2020, Projekt Ministerstva vnitra ČR
- Řešitelé: CESNET, Masarykova univerzita
- <https://sabu.cesnet.cz> – stránky jsou ve výstavbě
- sabu-info@cesnet.cz – kontaktní e-mail

- Partneři:
 - CSIRT.SK
 - ISP
 - Bankovní sektor
 - Invea Technologies

Sdílení a analýza bezpečnostních událostí



Sdílení a analýza bezpečnostních událostí



Harmonogram

- 2011 - první idea vytvoření systému pro sdílení informací (Warden)
- 2012-2015 - vývoj a pilotní běh na CESNETu (Warden, Mentat)
- 2014/15 - příprava návrhu projektu SABU, oslovení partnerů
- 2016 – specifikace, analýzy, návrh a začátek implementace
 - Q2 – napojení zainteresovaných partnerů na mailový reporting
 - Q3 – zhodnocení testovacího provozu
 - Q4 – příprava konektorů pro partnery
 - Q4 – propojení SABU a PROKI
- 2017 – testovací nasazení SABU, spolupráce s partnery
- 2018 – vyhodnocení a zapracování připomínek od partnerů
- 2019 – produkční nasazení

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

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