Mentat, systém pro zpracování informací z bezpečnostních nástrojů

Jan Mach
mach@cesnet.cz

LinuxDays 2016

9.10.2016

CESNET

- Založen v roce 1996
- Členové
  - 26 českých univerzit
  - Akademie věd ČR (~ 50 organizací)
- Připojujeme ~300 menších organizací (školy, úřady, ...)
- Odhadovaný počet uživatelů ~ 450 000
- Hlavní cíle
  - Provoz a rozvoj sítě národního výzkumu a vzdělávání CESNET2
  - Podpora vědy a výzkumu v oblasti pokročilých síťových technologií a aplikací
  - Podpora a šíření vzdělanosti, kultury a poznání

www.cesnet.cz

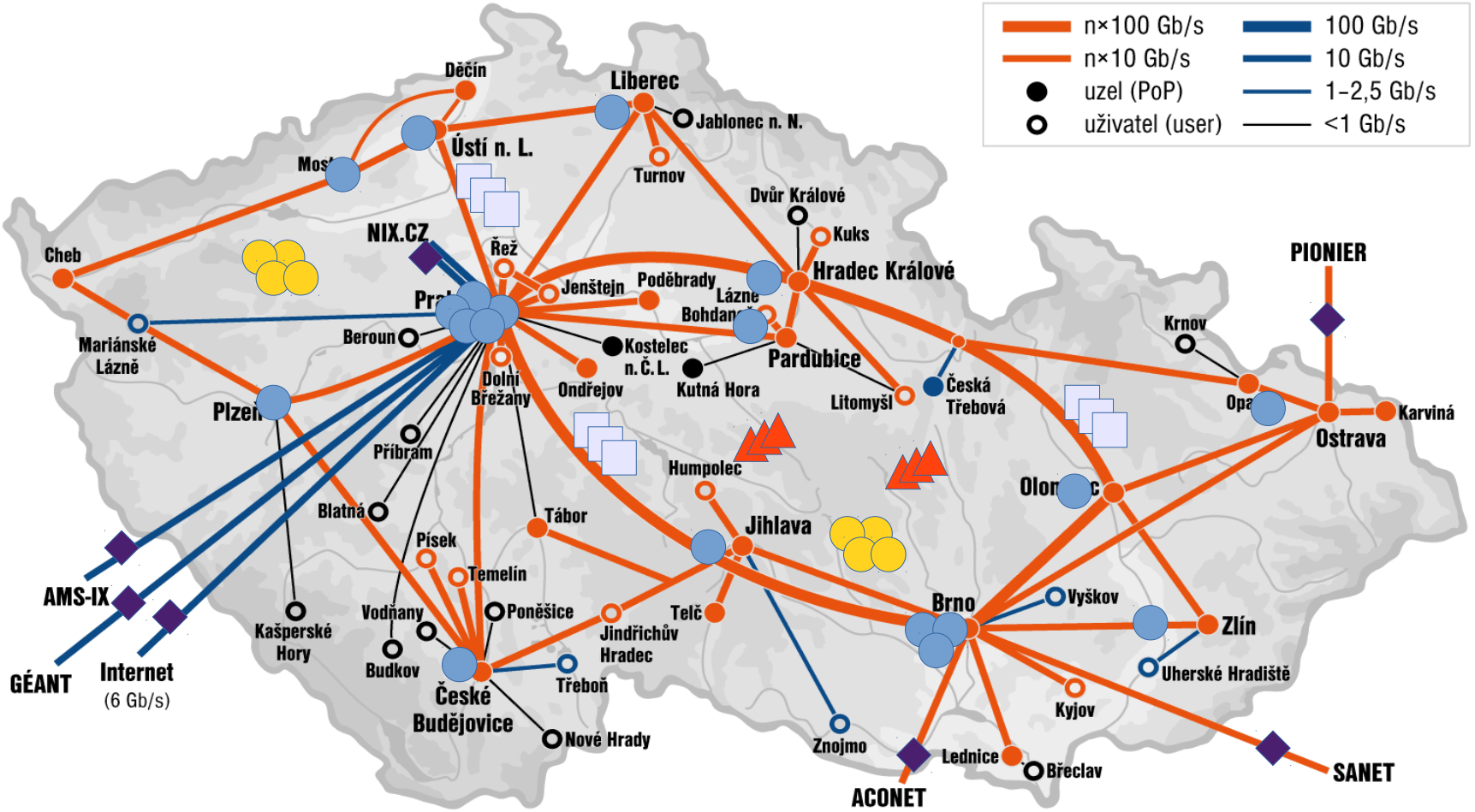
Bezpečnost

CESNET-CERTS (csirt.cesnet.cz, certs@cesnet.cz)

- Snaha o centrální a důvěryhodný kontaktní bod
- Řešení a koordinace incidentů v síti CESNET2
- Projekty pro podporu bezpečnosti
  - Forenzní laboratoř
  - Sledování provozu sítě
  - IDS, Audit, Honeypoty
  - Mentat, Warden
  - Osvěta
- Spolupráce s dalšími projekty a týmy

  (CSIRT.CZ, WIRT ZČU, CSIRT-MU)

Zdroje dat



- 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

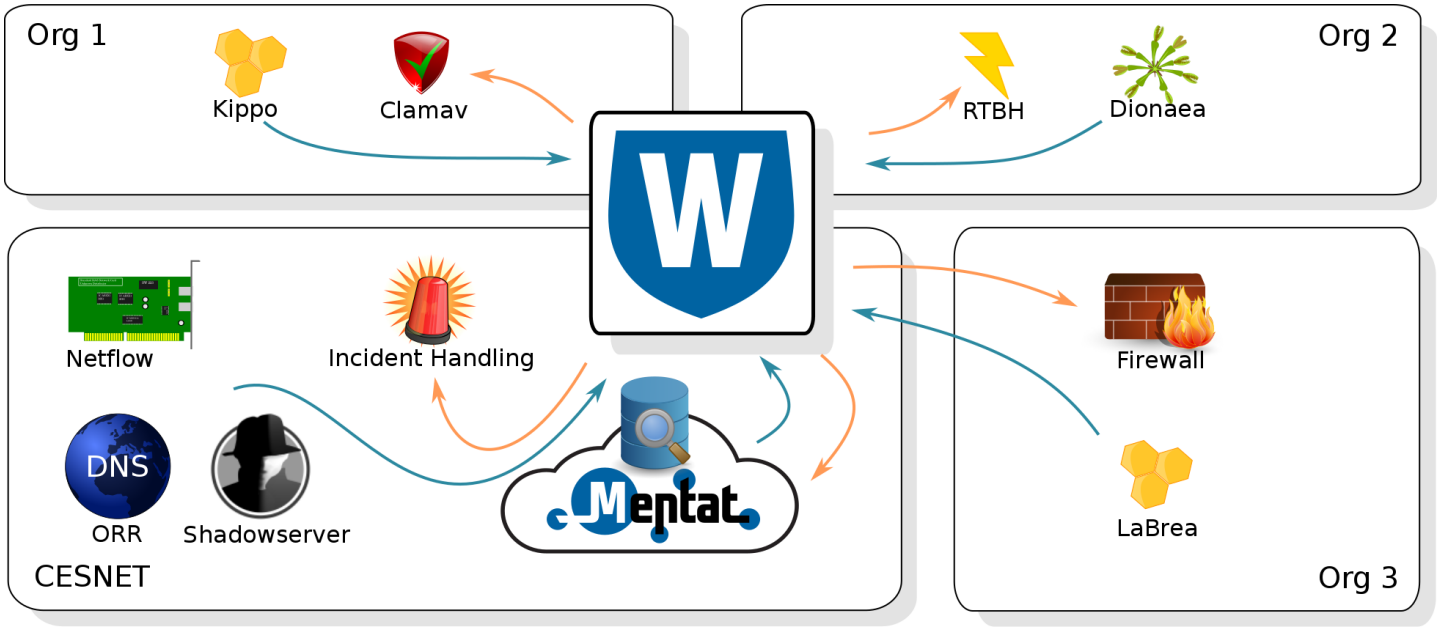
Začátky

- Neuspořádaná sbírka nekooperujících nástrojů
  - IDS, honeypoty, IPS, sondy, syslog, ...
    - Sledování stavu sítě, zdraví sítě
    - Hledání kompromitovaných zařízení
    - Detekce útoků, anomálií provozu
- Řadu z nich provozují sami správci
  (a získávají z nich data jen pro sebe – ostatní většinou zahazují)
- Dat je hodně, co s daty, pro která nemám použití
  - Zahodit?
  - Reportovat?

- Brilantní nápad: Bude výhodnější **sdílet!**

  - Méně brilantní detaily:
    Jak? Formát? Obsah? Protokol? Klasifikace? Politika?

- Systém pro efektivní **automatizované** sdílení informací o bezpečnostních incidentech
  - Client/server architektura, transportní fronta (nikoliv skladiště)
- Komunitní přístup
  - Tvá data jsou dostupná Warden komunitě
  - Data celé komunity jsou dostupná Tobě
- BSD licence, https://warden.cesnet.cz/
- Událost (event)
- IDEA formát



Poučení první – nejsou lidi

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

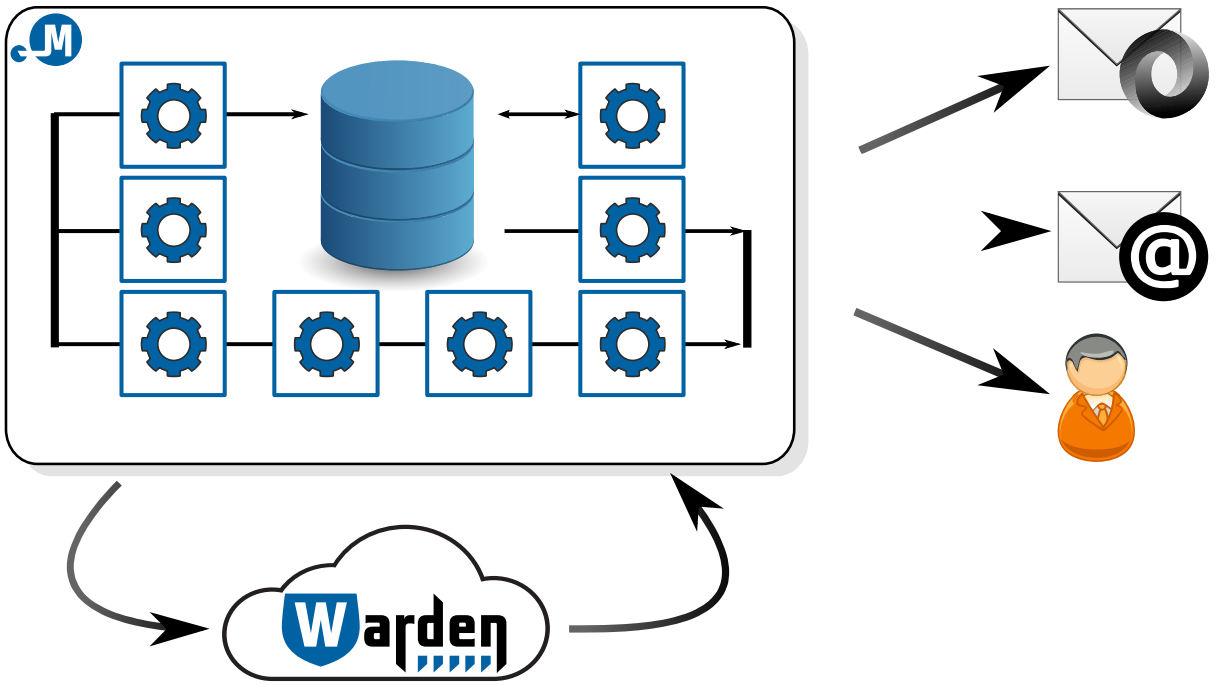
Nedokáží data odebrat a zpracovat si je.

Ale chtějí tato data získávat, data jsou užitečná

Je nutné je správcům doručit zpracovaná.

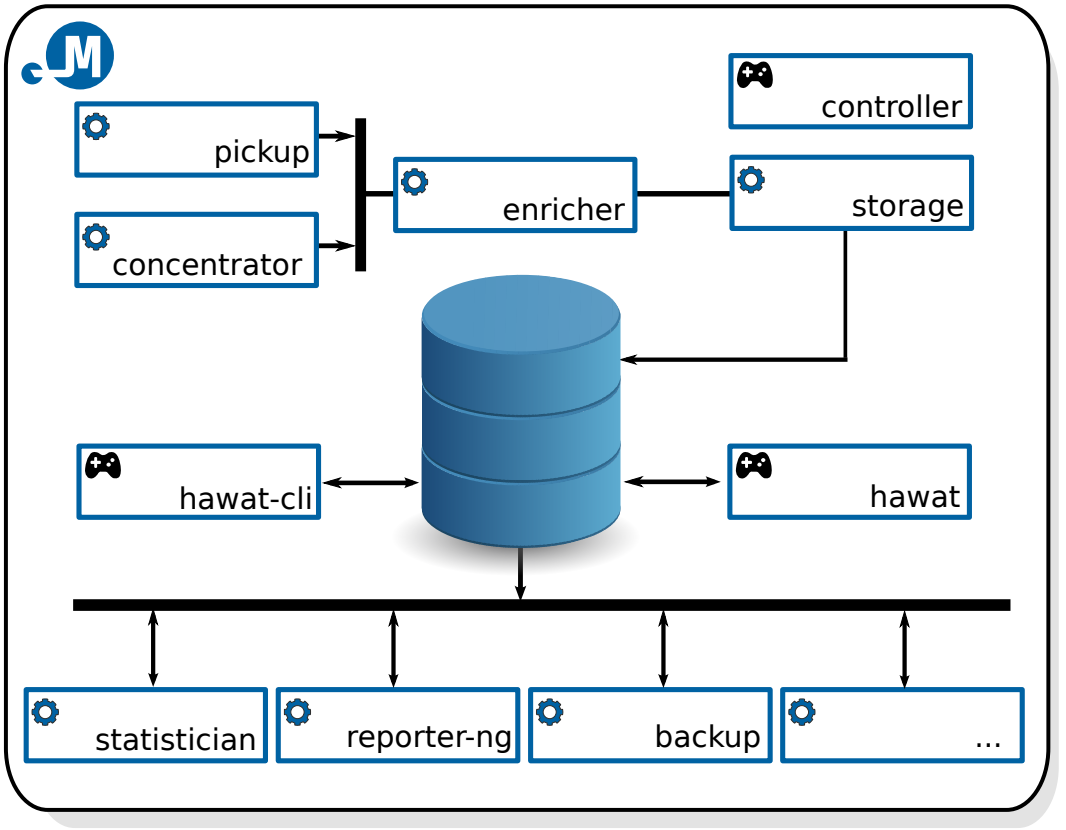
Mentat

- Z hlediska architektury systému Warden je Mentat ***odebírající klient***
- Framework a SIEM
- Podpora pro bezpečnostní tým CESNET-CERTS
  - Přístup k persistentnímu úložišti bezpečnostních událostí
  - Jednotné zpracování bezpečnostních událostí, korelace, analýzy
- + Podpora pro správce v koncových sítích
- https://mentat.cesnet.cz



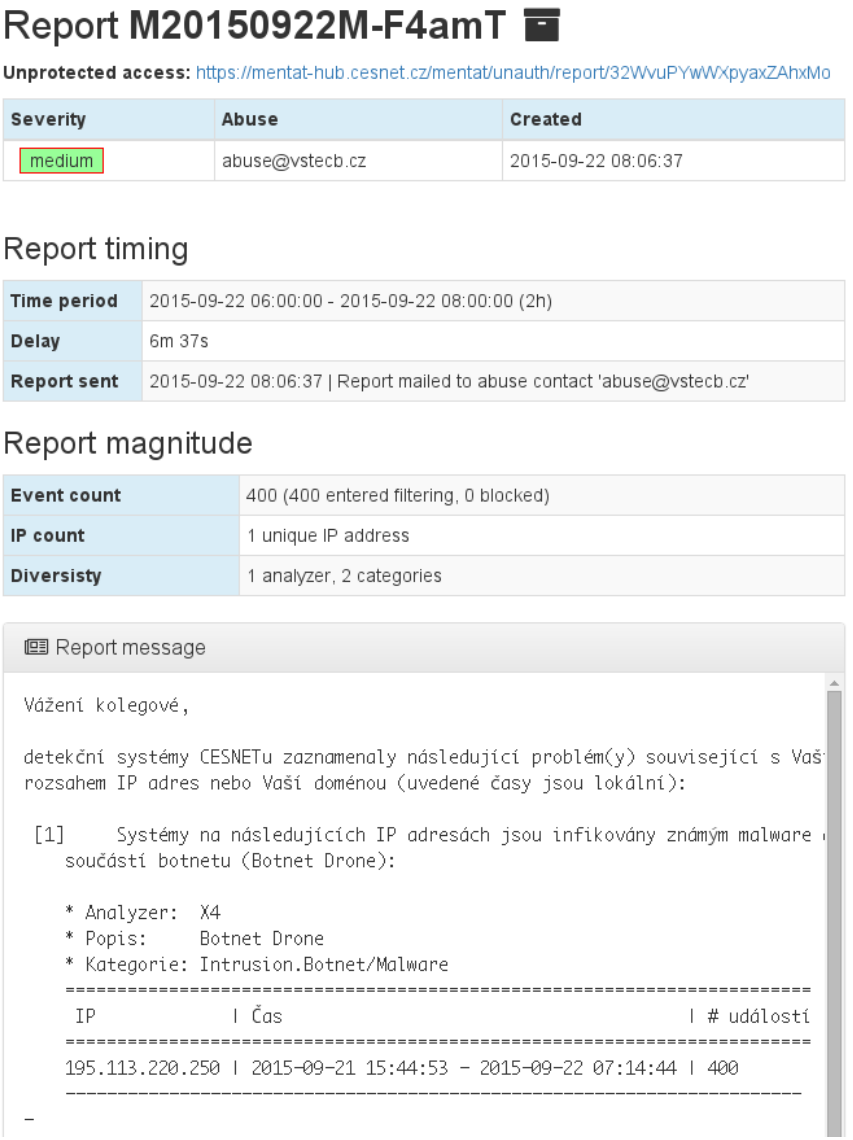
Mentat - Architektura

- Prototyp v jazyce Perl, ale postupně přecházíme na Python 3
- Design inspirován projekty Prelude SIEM a Postfix
  - Distribuovaný hierarchický systém
  - Práce rozdělena mezi více one-task démonů/procesů
  - Fronta = FS
- Datový model
  - IDEA
- Persistentní úložiště:
  - MongoDB (NoSQL)
- Více možností zpracování:
  - Realtime
  - Postprocessing
- Webové rozhraní
- Framework



Mentat – Reporter

- Učíme Mentat reportovat:
  - Sebere všechny nové události za poslední 2 hodiny
  - Události rozdělí podle příslušnosti ke koncovým sítím (vytvoří reporty)
    - Kontaktní informace získáváme z RIPE DB (www.ripe.net)
  - Reporty zasílá do koncových sítí (abuse@...)
  - K reportům se přibalí surová data ve strojově zpracovatelné podobě (CSV)



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
    --------------------------------------------------------------------------------
-
```

Poučení druhé - kvalita dat

- Reakce příjemců:
  - Nedostatečné informace o incidentech
  - Zahlcení množstvím/opakováním (někdy i po vyřešení)
  - Nejasná závažnost incidentu (často závislá na lokální situaci)
  - Problematická data třetích stran

- Dat je stále mnoho a jsou heterogenní
  - Mají různou kvalitu,
  - a různou vypovídací hodnotu

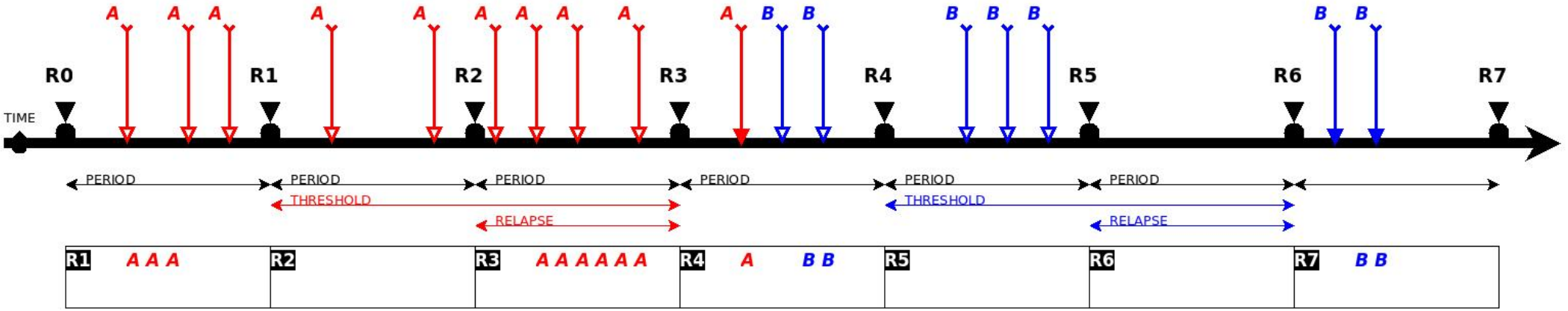
- Poučení druhé: **Nestačí je jen přebalit a rozeslat**

Mentat – Reporter NG (1)

- Klíčové vlastnosti nového reportéru vycházejí z nashromážděných připomínek:
  - Pozdržení již nahlášených problémů na určitou dobu
  - Možnost zasílání souhrnných reportů za větší časový interval (den, týden), rozdílné intervaly reportování

- Nutnost zavedení hodnocení událostí z hlediska závažnosti (velmi závažné události nelze nechat čekat týden)
- Nutný kompromis mezi co největší agregací a rozumným zpožděním při odeslání hlášení (týden stará data jsou již obvykle naprosto k ničemu)

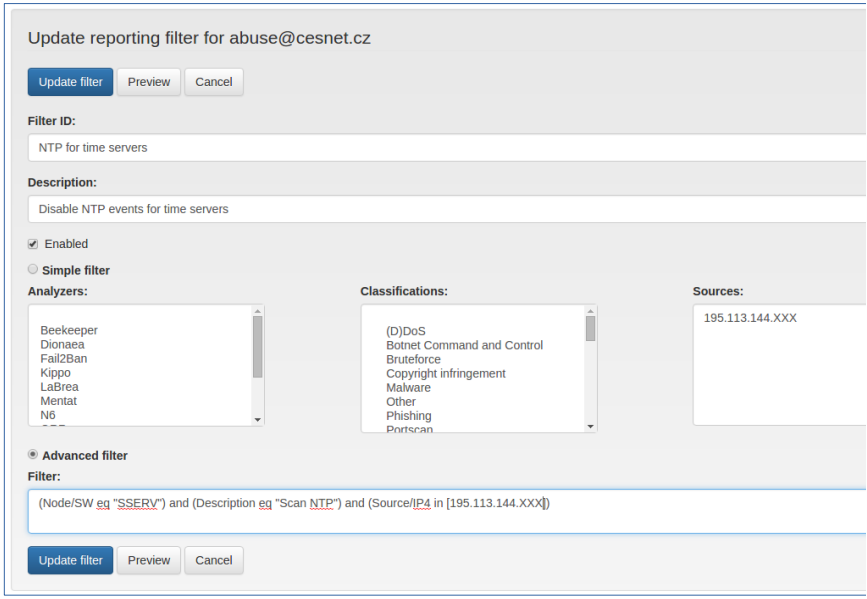
Mentat – Reporter NG (2)

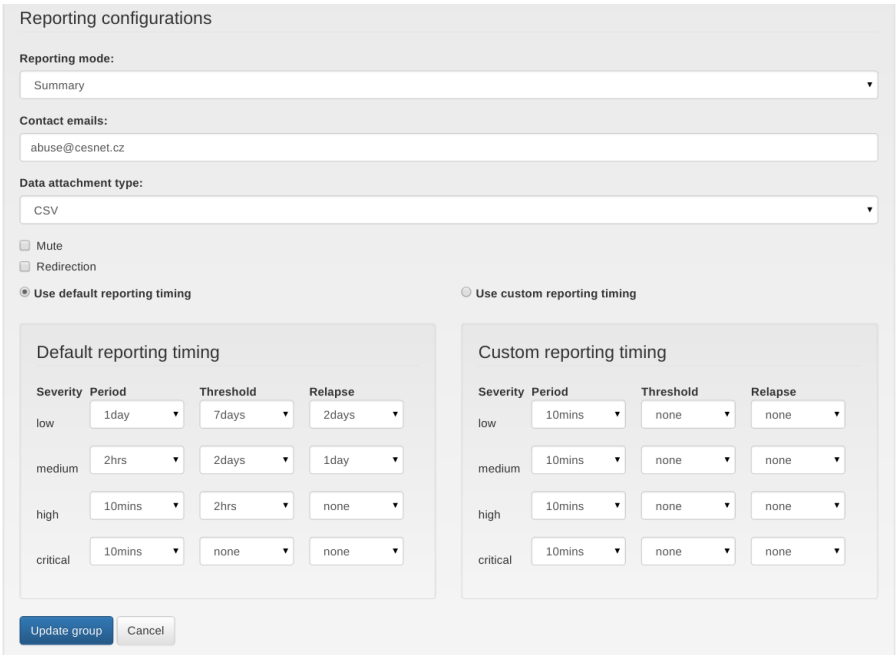


- Zpracování zpráv s každou úrovní závažnosti zvlášť
- Algoritmus je konfigurovatelný trojicí *period/threshold/relapse*
- **Period** – interval generování reportů
- **Threshold** – doba, po kterou budou již hlášené události týkající se konkrétní IP adresy “zamlčeny”
- **Relapse** – heuristika, která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

Mentat – Reporter NG (3)

- Konfigurovatelné filtry pro úplné vyřazení určitých událostí z reportování
- Konfigurovatelné atributy PERIOD/THRESHOLD/RELAPSE pro každou úroveň závažnosti událostí (v rámci vymezených hranic)
- Nastavení zasílaných emailů:
  - Přesměrování na jiné cílové emailové adresy
  - Volba typu hlášení (summary, extra, obojí)
  - Volba typu příloh (CSV, JSON, obojí)
  - Volba zipování/nezipování příloh





Mentat – Reporter NG (4)

- TEST: Zpětné zpracování dat za období **2015-05-14 00:00 - 2015-05-24 06:00 (~10 dní)**

	Legacy	NG
# reportů	955	255

Výsledek: Pokles počtu odeslaných emailů cca o **2/3**

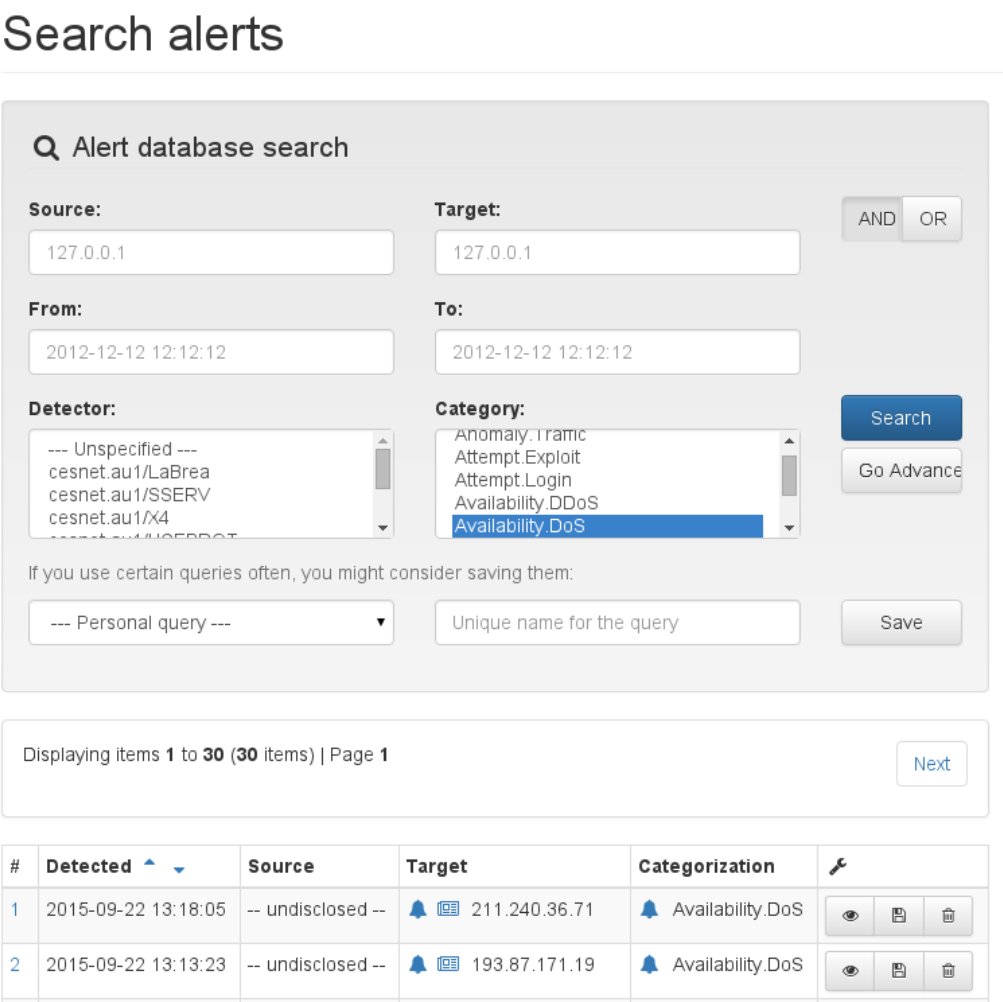
Beze ztráty informační hodnoty!

Mentat – Webové rozhraní Hawat

- Podpůrný nástroj pro nejen bezpečnostní tým CESNET-CERTS, ale i WWW rozhraní pro správce z koncových sítí
  - Přístup k databázi událostí
  - Přístup k databázi reportů, konfigurace reportů
  - Globální dahsboardy
  - Statistiky
- Autorizace a konfigurace na základě abuse skupin

Hawat – Databáze událostí

- ~ 2 miliony událostí denně
- ~ 500GB databáze
- Retence dat
  - Kompletní data za poslední 4 týdny
  - Interní data za posledních 6 měsíců
  - Smazaná data se uchovávají v agregované formě
- Možnost uložení často používaných dotazů



Hawat – Group dashboard

Group dashboard for abuse@cesnet.cz

From: 2016-04-21 02:00:00 **To:** YYYY-MM-DD HH:MM:SS View

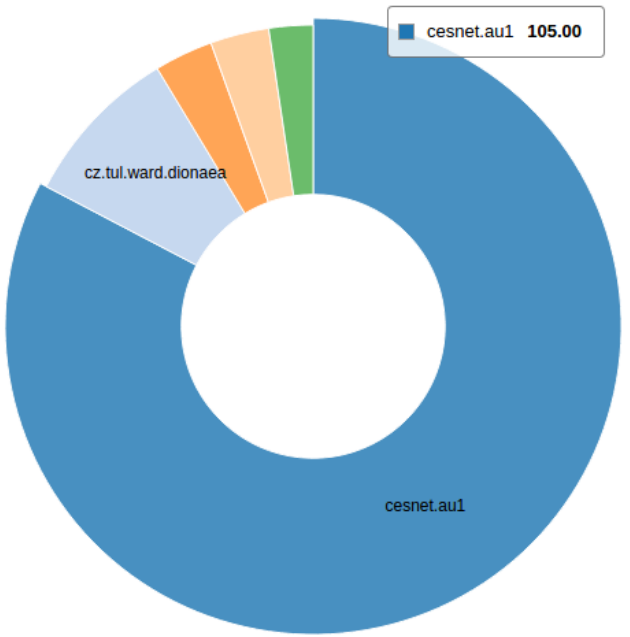
View the related reports (50)

Reporting statistics

Actual data period: 2016-04-20 02:00:00 - 2016-05-05 10:00:00 (15d 8h)

per report | # per detector | # per category set | # per analyzer | # per category | # per IP

per detector



Search:

	Name	#	%
1	cesnet.au1	105	82.68
2	cz.tul.ward.dionaea	11	8.66
3	cz.cesnet.gc15	4	3.15
4	cz.cesnet.ext.nsharp	4	3.15
5	cz.cesnet.ext.uceprot	3	2.36
	Sum	**127**	**100**

Showing 1 to 5 of 5 entries

Min	3
Max	105
Sum	127
Cnt	5
Avg	25.4
Med	4

Hawat – databáze reportů

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 **19,032** total) | Page **1** of **635**

1 2 3 4 5 6 7 › »

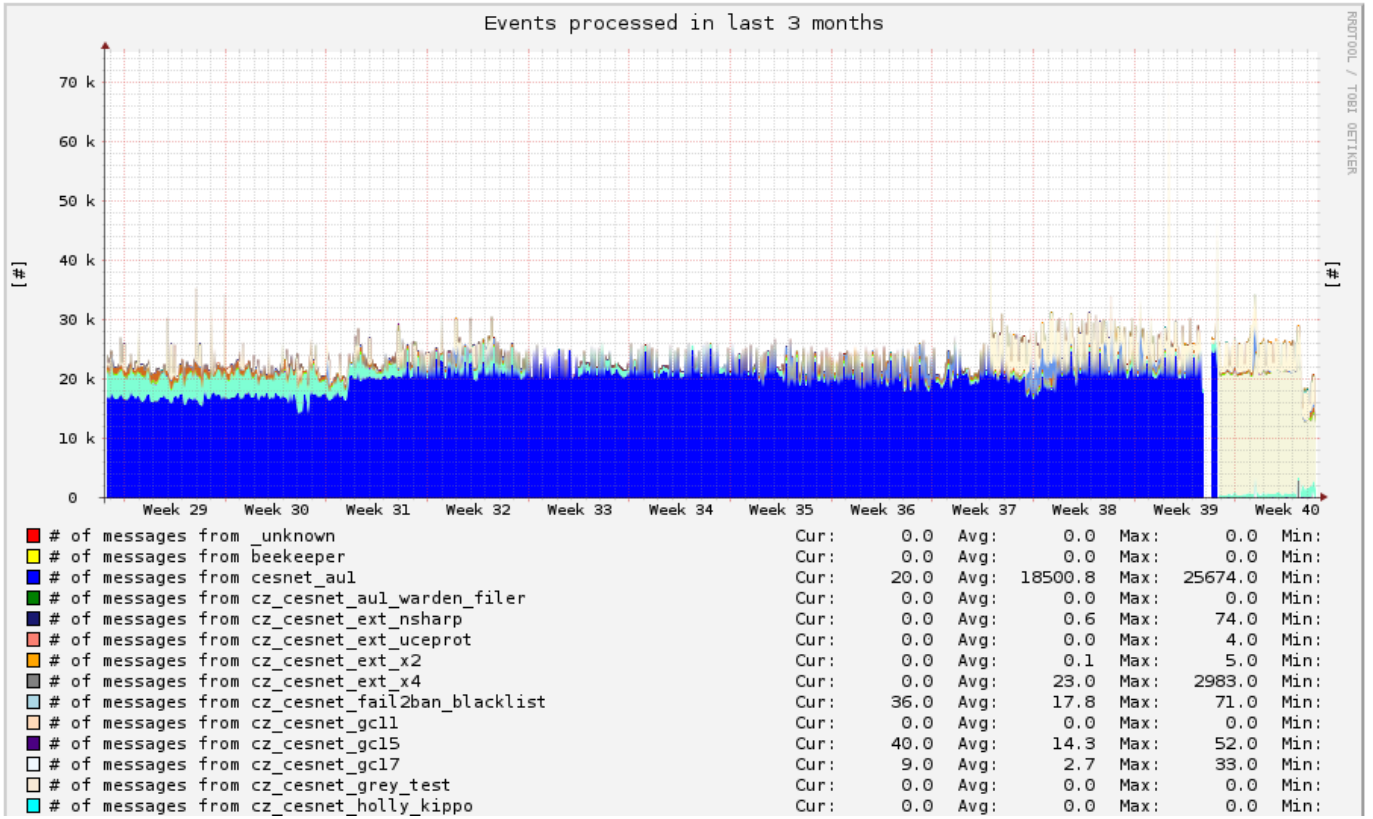
#	?	Time period	Report ID	Abuse contact	Node	ECNT | UNIQ | ACNT | CCNT	Delay
1	H	2016-05-05 09:50:00 -	M20160505SH-JtfEl	abuse@[redacted]	[redacted]202.9 (9 total)	**9** 9 1 1	12m 50s
2	H	2016-05-05 10:10:00	M20160505SH-wlWu7	abuse@[redacted]	[redacted]201.56 (2 total)	**2** 2 1 1	12m 49s
3	H		M20160505SH-HeAj7	abuse@[redacted]	[redacted]206.44 (2 total)	**2** 2 1 1	12m 48s
4	H		M20160505SH-MHoRV	abuse@[redacted]	[redacted]34.41 (32 total)	**32** 32 1 1	12m 43s
5	H		M20160505SH-QFGfi	abuse@[redacted]	[redacted]228.84	**1** 1 1 1	12m 41s
6	M	2016-05-05 08:00:00 -	M20160505SM-wOUhZ	abuse@[redacted]cz	[redacted]149.222	**1** 1 1 1	22m 51s
7	M	2016-05-05 10:00:00	M20160505SM-sGNEj	abuse@[redacted]	[redacted]161.198	**1** 1 1 1	22m 50s
8	M		M20160505SM-t5mD2	abuse@[redacted]	[redacted]79.50	**1** 1 1 1	22m 50s
9	M		M20160505SM-6ivBe	abuse@[redacted]	[redacted]153.8	**1** 1 1 1	22m 50s
10	M		M20160505SM-3vd2o	abuse@[redacted]	[redacted]80.1	**1** 1 1 1	22m 50s
11	M		M20160505SM-Qh34n	abuse@[redacted]	[redacted]171.181	**1** 1 1 1	22m 50s
12	M		M20160505SM-ichm9	abuse@[redacted]	[redacted]184.150	**1** 1 1 1	22m 50s
13	H	2016-02-01 15:20:00 - 2016-02-02 14:10:00	M20160202EH-dJZ0E	abuse@[redacted]	[redacted]53.91	**1** 1 1 1	4m 15s

Hawat – Provozní statistiky

Overview by node name

6 hours | 24 hours | Week | 4 weeks | 3 months | 6 months | 12 months

Statistics by node name for last 3 months



System statistics

- Overview by node name
- Totals by node name
- Overview by node SW
- Totals by node SW
- Overview by event category
- Totals by event category

Pro srovnání

Události

~2,1 mil denně

~66 GB dat

(TTL 30 dní)

Události

~2,1 mil denně

~500 GB dat

(TTL 4 týdny/6 měsíců)

Reporty

(Na ~300 institucí)

~100 denně

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
- Další projekty:
  - SABU
  - NERD
  - PassiveDNS

Děkuji za pozornost

GNU Terry Pratchett