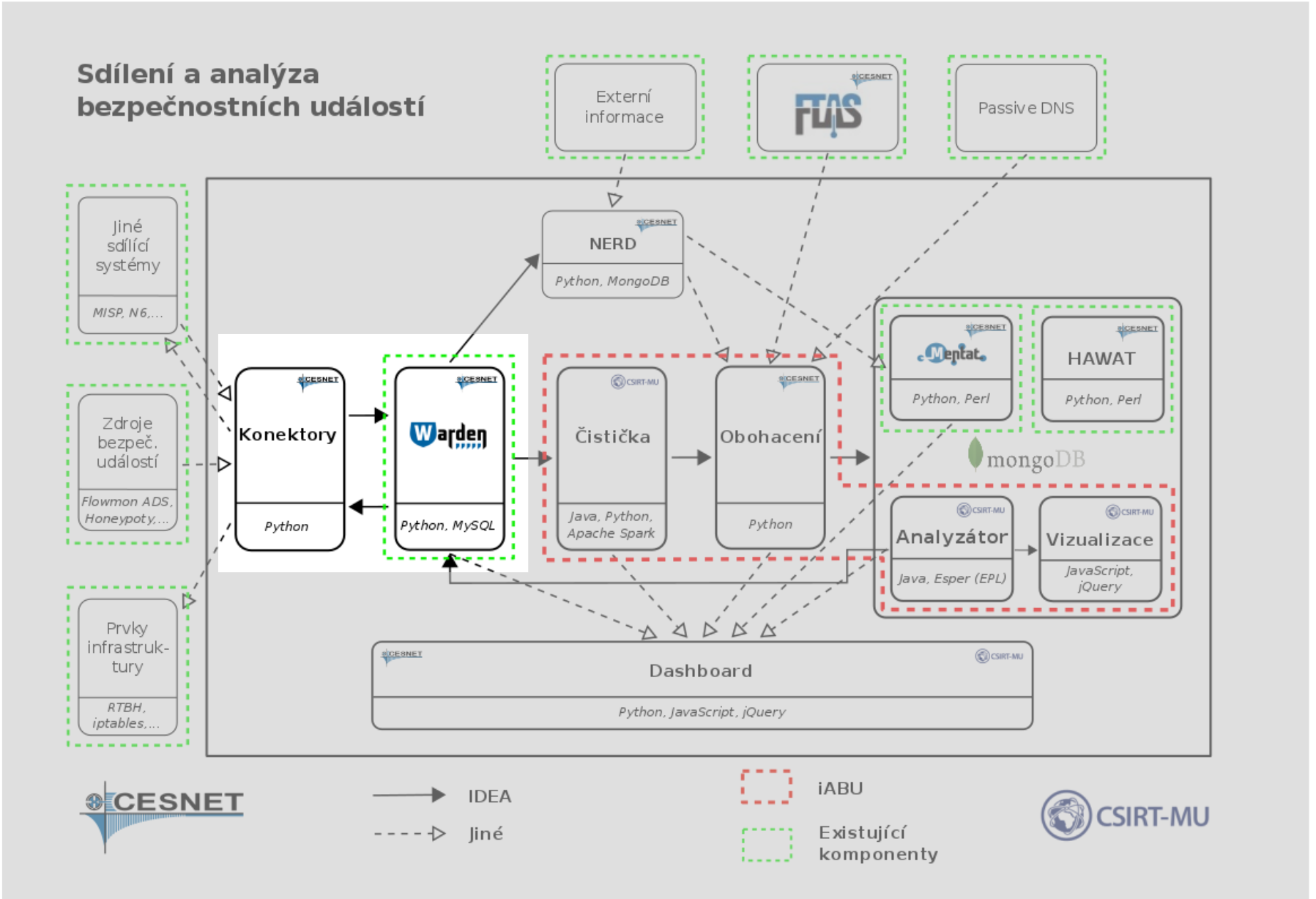
Warden & konektory

Sběr a normalizace dat SABU

Pavel Kácha
ph@cesnet.cz

Architektura



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
- Definice: https://idea.cesnet.cz

Autentizace

HTTPS + X509

- Dosud řešeno individuálně

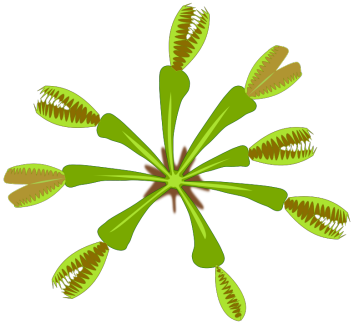
Cíl

- Jednotná certifikační autorita
- Automatizované vydání certifikátu na základě předané passphrase
- Podpora CRL
- (Certifikační politiky a směrnice)

Konektory Wardenu

Kippo/Cowrie

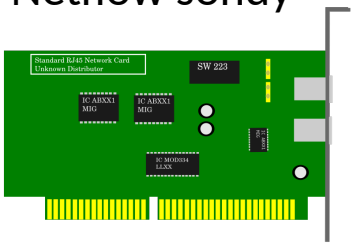
Dionaea



Fail2Ban

FTAS

Netflow sondy



LaBrea

Shadowserver

network security incident exchange

Nové konektory

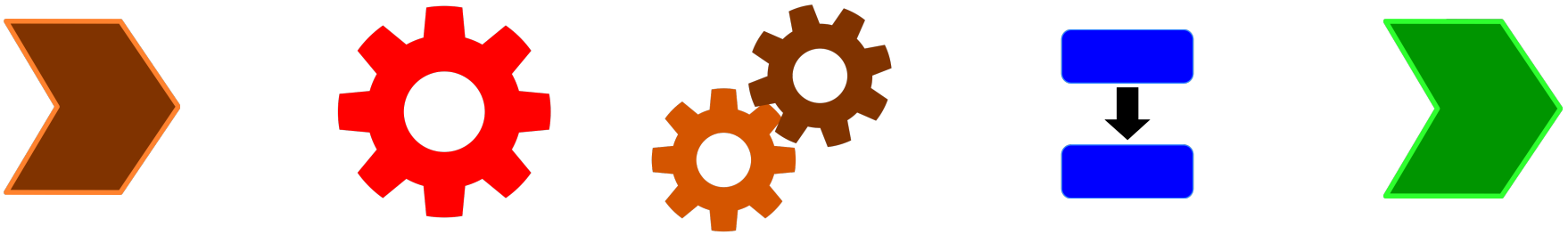
Flowmon Networks


```
{
   "Format": "IDEA0",
   "Category": ["Availability.DoS"],
   "Description": "Denial of service
      attack",
   "Note": "Current input/output packet
      ratio: 117630.00, average packet
      ratio before attack: 1810.71
      (protocol: TCP, port(s): 443,
      service: https, potential
      attackers: 69).",
   "DetectTime": "2016-06-17 18:00:00Z",
   "EventTime": "2016-06-17 17:59:12Z",
   "ID": "96d90739-10d9-475b",
   "AltNames": ["ADS-810679"],
   "Source": [{
      "Hostname": ["fr15s11.1e100.net"],
      "IP4": ["172.217.16.161"]
   }],
   "Target": [{
      "IP4": ["192.0.2.3", "192.0.2.6"],
      "Proto": ["TCP"],
      "Port": ["443"]
   }],
}
```


INTELMQ


```
{
   "Format": "IDEA0",
   "Category": ["Attempt.Login"],
   "Description": "BlockList.de: IP
      reported as having run attacks
      on Joomlas, Wordpress and other
      Web Logins with Brute-Force
      Logins",
   "DetectTime": "2016-06-17 20:10:10Z",
   "ID": "4fb702e8-4ae1-46a0",
   "Source": [{
      "IP4": ["192.0.2.55"]
   }],
   "Node": [{
      "Name":"cz.cesnet.intelmq",
      "AggrWin": "00:05:00",
      "SW": ["IntelMQ"],
      "Type": ["Relay", "External"]
   }]
}
```

Cíl



Input

- Socket
- File
- Files
- Syslog
- HTTP
- Warden
- DB
- XMPP
- HPFeeds

Parse

- Mail
- CSV
- JSON
- Regex
- Normalize

Process

- Dedup
- Aggregate
- Filter

Convert

- Static
- Generator

Output

- Socket
- File
- Files
- Syslog
- SMTP
- Warden
- DB
- XMPP
- HPFeeds

Výkon

Události

(TTL 30 dní)

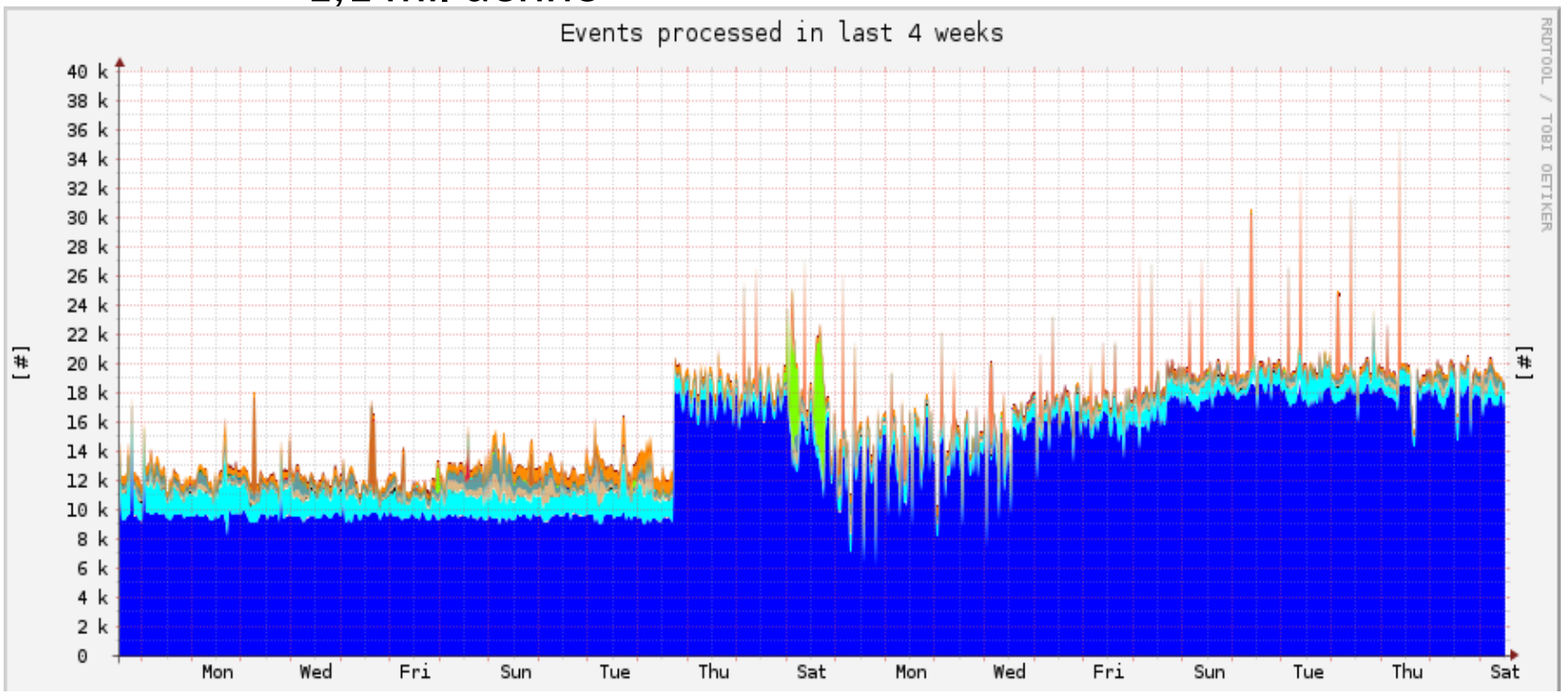
~30 GB dat

~1,1 mil denně

Reporty

(na ~320 institucí)

~60 denně



Děkuji za pozornost

GNU Terry Pratchett