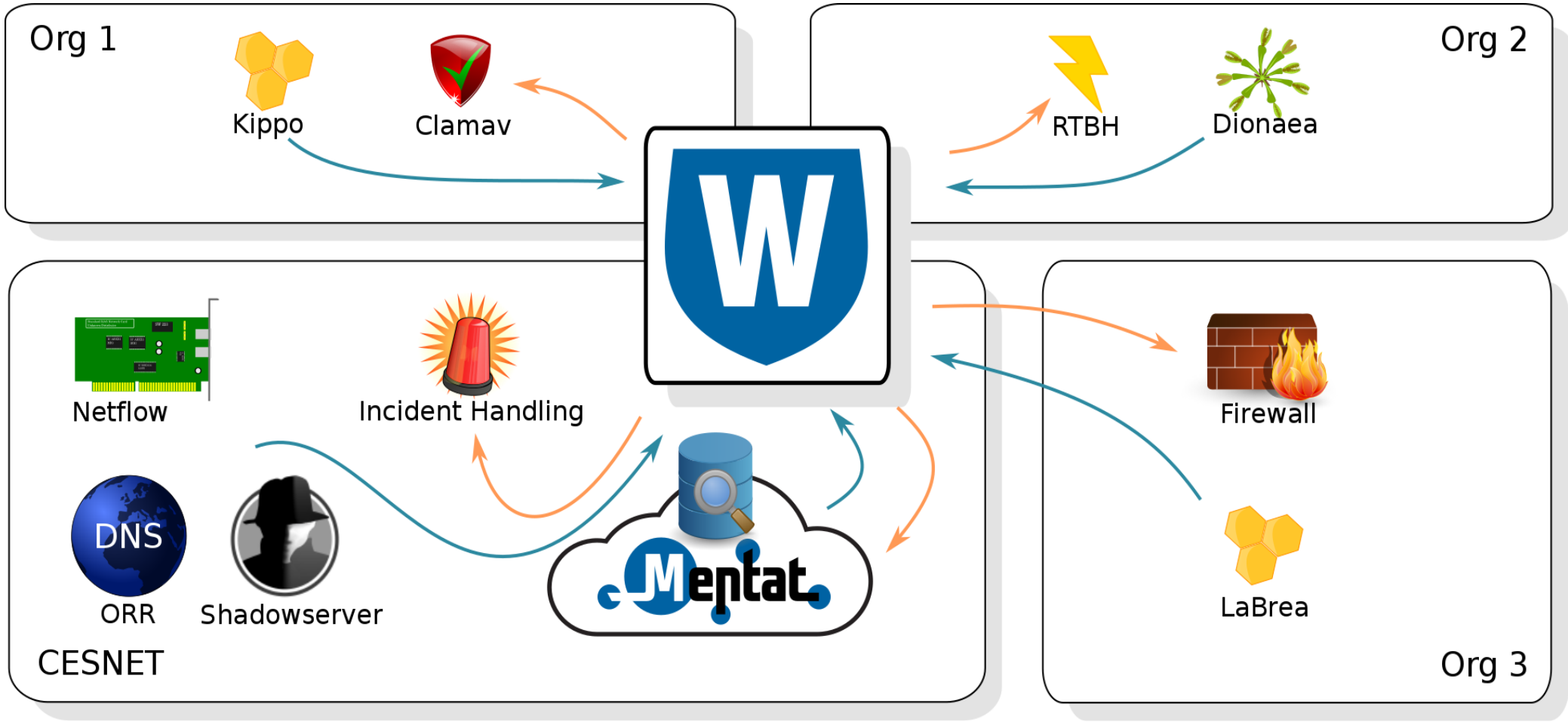
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

CESNET

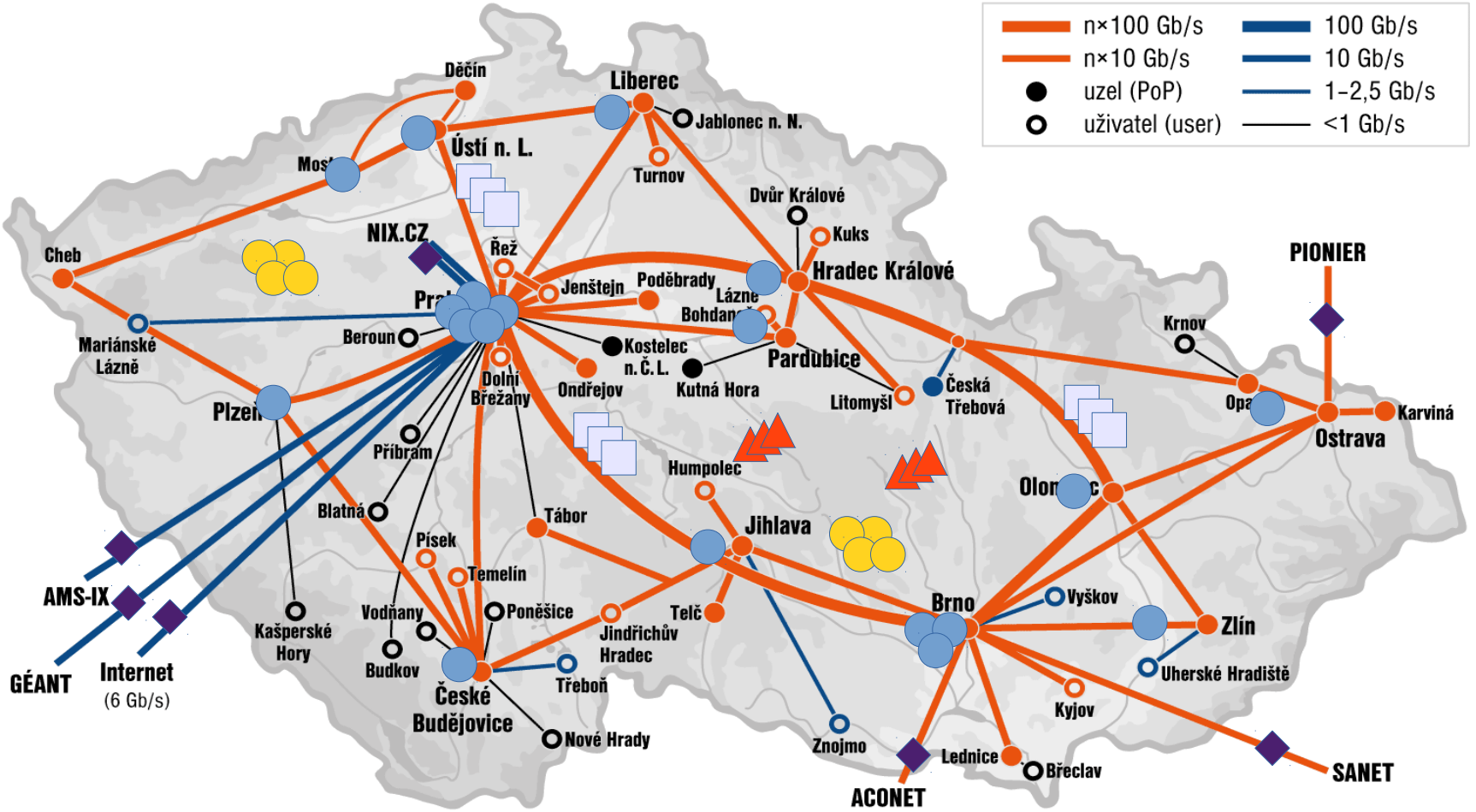
SABU & Warden

Pavel Kácha
ph@cesnet.cz

Architecture



Data sources



- 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

Format – 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]
    }
  ]
}
```

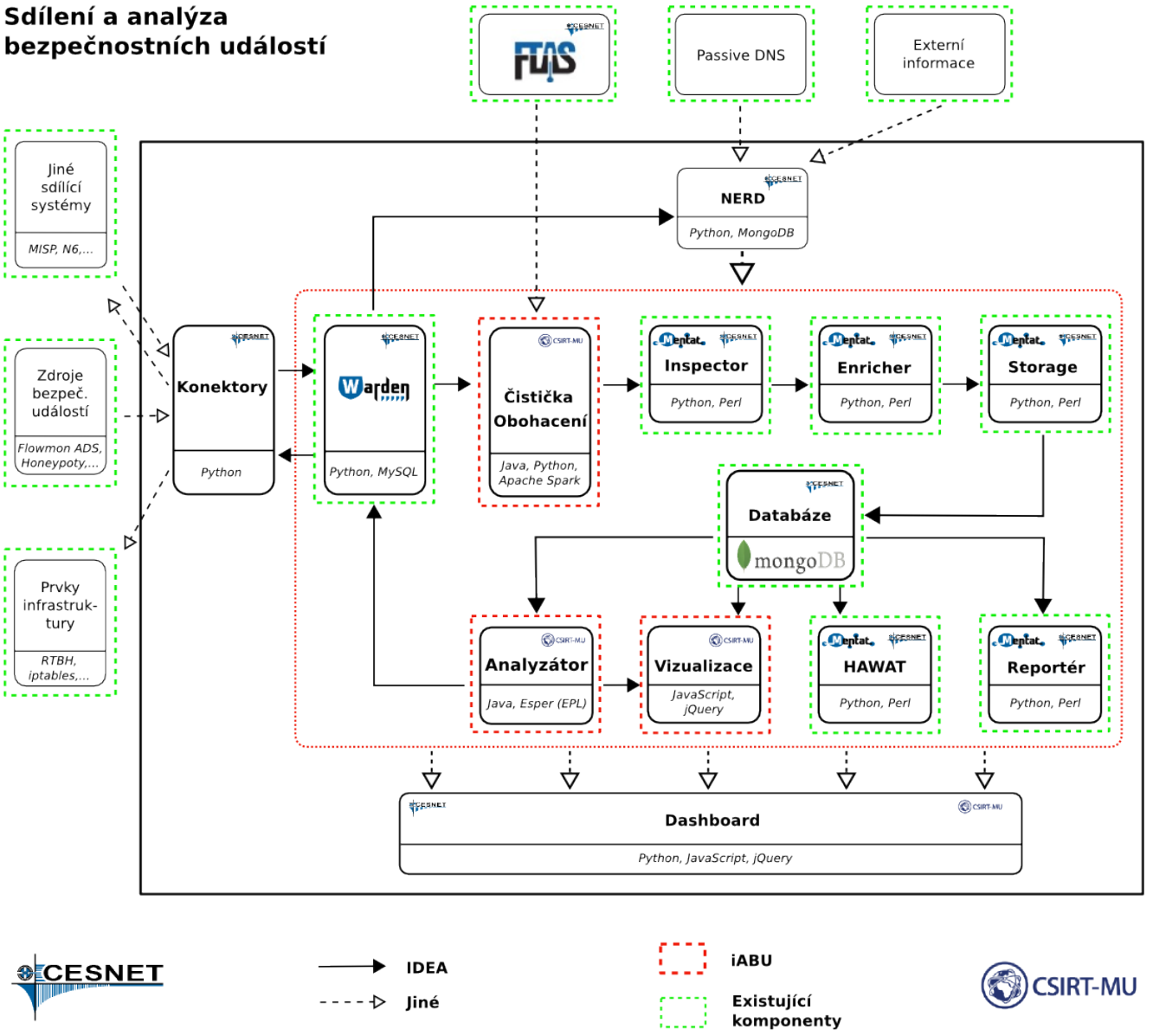

- Simple, extensible format
- Once defined keys and types do not change
- We are able to differentiate bitween primary, aggregated, correlated data
- Supports anonymisation and imprecision
- Definition, JSON schema: https://idea.cesnet.cz

How much?

	Name	#	%
1	cz.cesnet.labrea	2,256,169	91.09
2	cz.cesnet.hoststats	104,554	4.22
3	cz.cesnet.supplier.intelmq	38,196	1.54
4	cz.cesnet.nemea.hoststats	33,069	1.34
5	cz.cesnet.nemea.bruteforce	12,624	0.51
6	cz.tul.ward.dionaea	7,511	0.3
7	cz.vsb.kippo	5,546	0.22
8	cz.cesnet.nemea.vportscan	5,240	0.21
9	cz.uhk.apate.dionaea	2,561	0.1
10	cz.nic.dionaea1	1,513	0.06
11	cz.cesnet.kryten.dionaea	1,406	0.06
12	cz.nic.dionaea2	1,335	0.05
13	cz.cesnet.gc15	1,287	0.05
14	cz.cesnet.metacentrum.nemea.bruteforce	1,177	0.05
15	cz.uhk.apate.cowrie	1,133	0.05
16	cz.cesnet.gc17	891	0.04
17	cz.tul.ward.kippo	775	0.03
18	cz.cesnet.fail2ban.blacklist	646	0.03
19	cz.cesnet.metacentrum.nemea.hoststats	370	0.01
20	-- Rest (9)	822	0.03
	Sum	**2,476,825**	**100**

	Name	#	%
1	Recon.Scanning	2,405,553	97.12
2	Other/Test	22,614	0.91
3	Attempt.Login/Test	14,061	0.57
4	Attempt.Login	7,769	0.31
5	Attempt.Exploit/Test	7,233	0.29
6	Intrusion.Botnet/Test	7,087	0.29
7	Recon.Scanning/Test	5,621	0.23
8	Anomaly.Traffic	2,178	0.09
9	Attempt.Exploit	1,770	0.07
10	Abusive.Spam	648	0.03
11	Fraud.Phishing/Test	501	0.02
12	Availability.DoS	461	0.02
13	Intrusion.Botnet/Malware	364	0.01
14	Abusive.Spam/Test	321	0.01
15	Malware/Test	250	0.01
16	Vulnerable.Config	248	0.01
17	Attempt.Exploit/Malware	83	0
18	Availability.DoS/Test	23	0
19	Availability.DDoS	20	0
20	-- Rest (3)	20	0
	Sum	**2,476,825**	**100**

Architecture – SABU



https://sabu.cesnet.cz/en/

Questions?