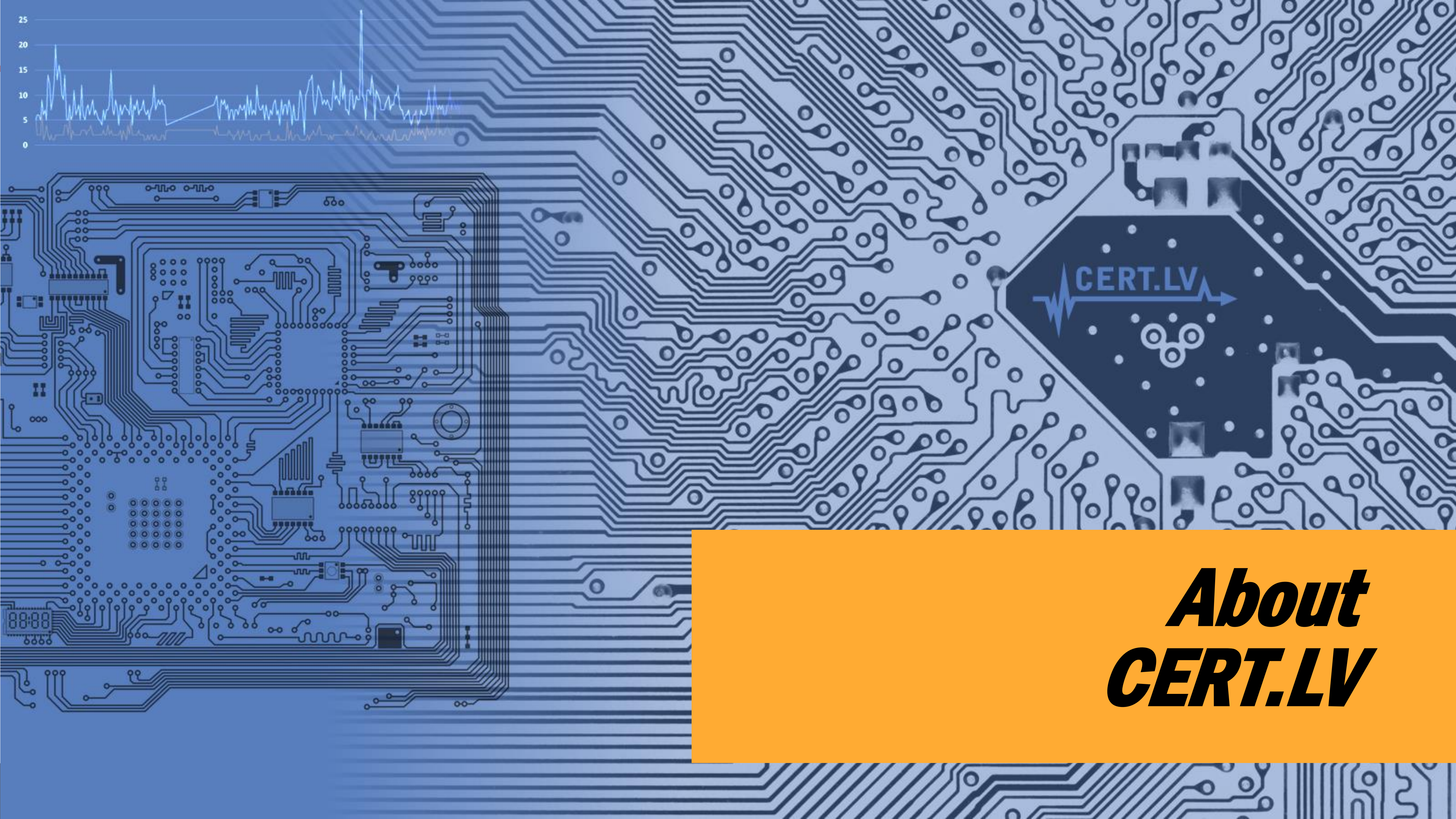
CERT.LV

Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

L4YER CAKƐ - *Hunting Malware & Sharing IOCs like a boss*

Going beyond traditional IDS

Varis Teivans & Uldis Koskins (bro)
06.10.2016.

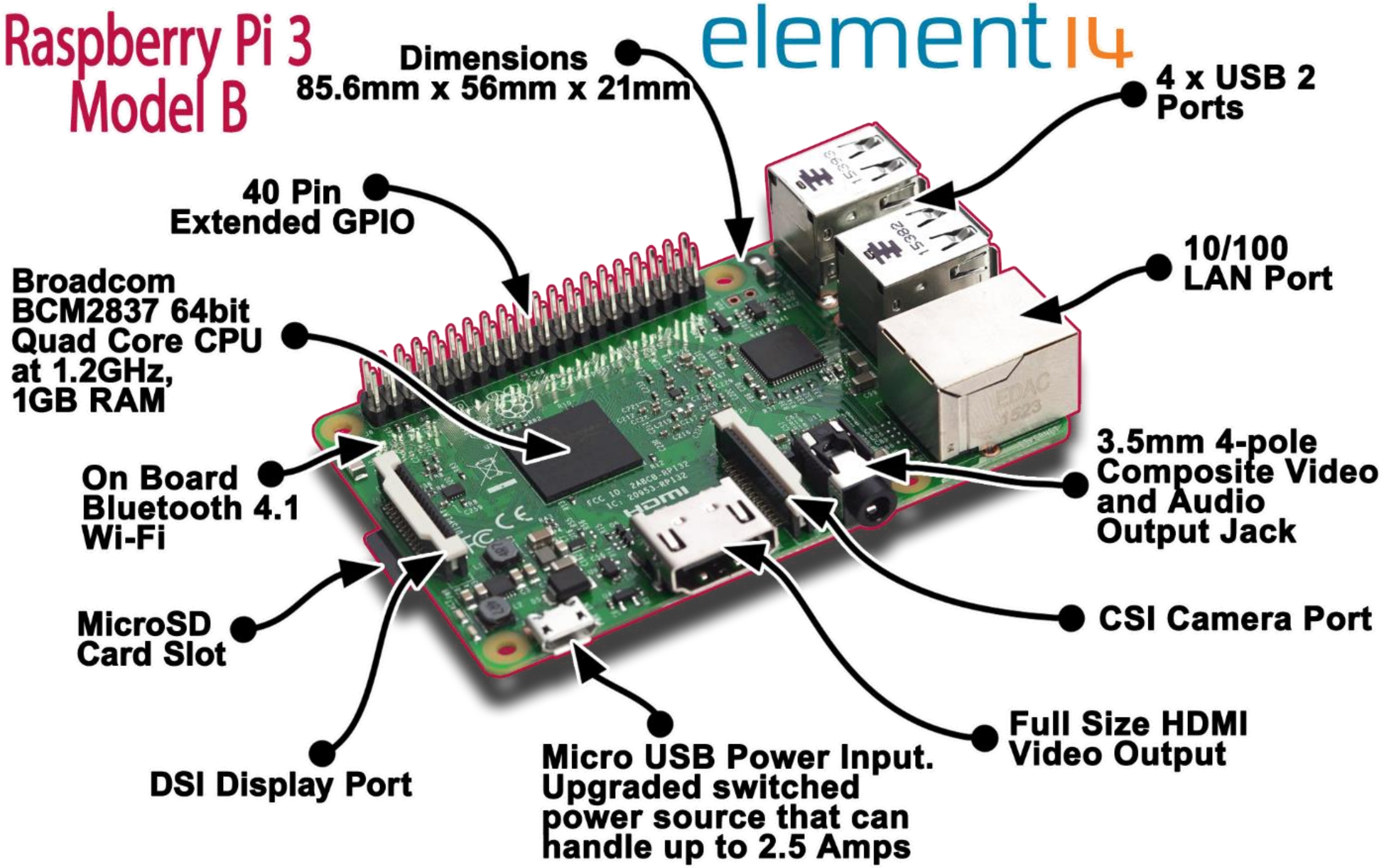


About CERT.LV

Recipe for layer cake

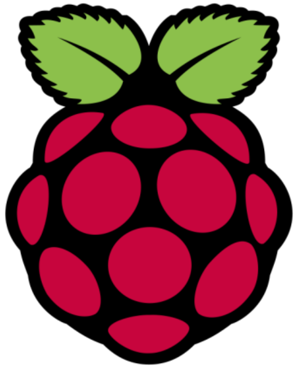
- Open source IDS
- Event monitoring & analysis
- Malware hunting & Sandbox analysis
- IOC storage, correlation and sharing capability
- Automation
- Scalability
- Low budget

Recipe for layer cake



Recipe for layer cake

~45 EUR



The Bro Network Security Monitor

RSYSLOG
THE ROCKET-FAST SYSTEM FOR LOG PROCESSING

elastic & kibana

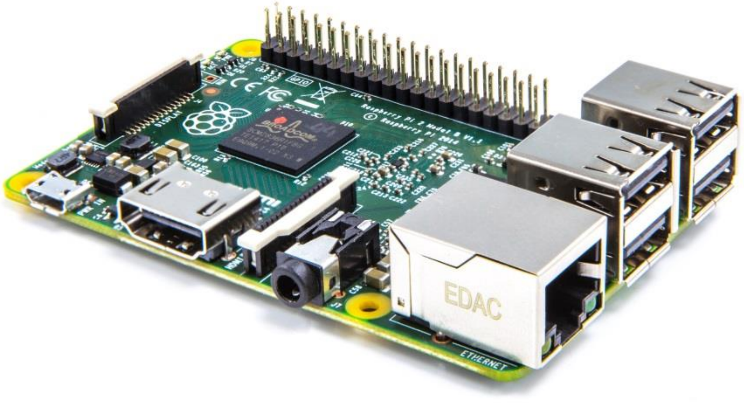
yara

300 EUR … ∞

cuckoo

MISP
Threat Sharing

Why not using sugar, spice & everything nice?



- **Raspberry PI – affordable, small, suitable for POC & real life SOHO application**
- **Start small, go big**
  - System can be:
    - Moved beyond PI
    - Beefed up & pumped with steroids

Why not using sugar, spice & everything nice?

The Bro Network Security Monitor

- Scalable to 100G networks and beyond
- US National Science Foundation funds The Bro Center of Expertise
- Bro is not restricted to any particular detection approach and does not rely on traditional signatures
- Bro scripting language
- “Bro is not about trying to tell you what's bad, it tries to tell you what's happening”
  Richard Bejtlich, TaoSecurity

Why not using sugar, spice & everything nice?

RSYSLOG
THE ROCKET-FAST SYSTEM FOR LOG PROCESSING

- **Way more efficient than Logstash**
  - ELK vs ERK

  http://www.rsyslog.com/

elastic & kibana

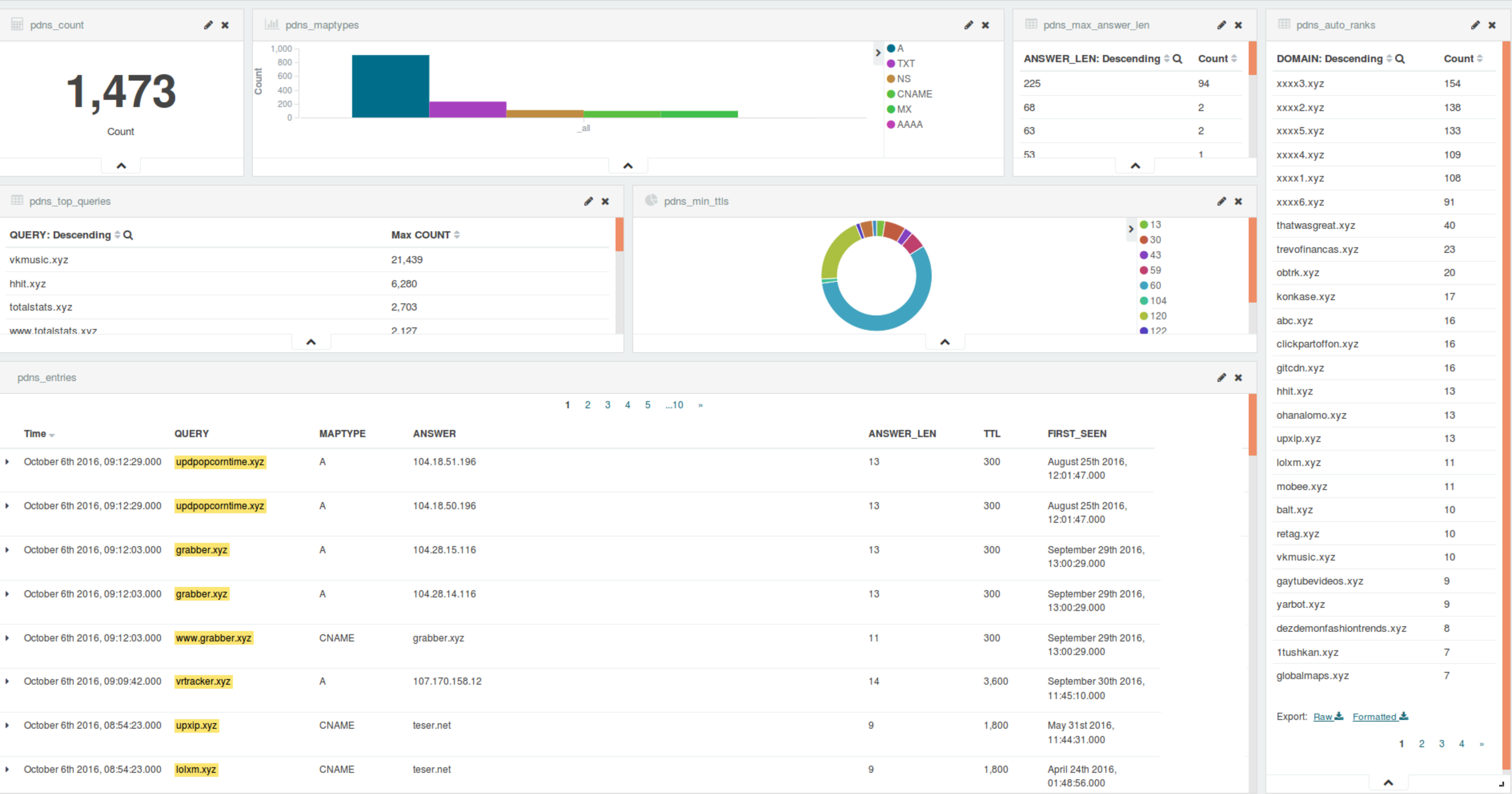
- **Elasticsearch for fast data search**
- **Kibana for analytics, pictures & graphs**

https://www.elastic.co/downloads/elasticsearch
https://www.elastic.co/downloads/kibana

yara

- **The pattern matching swiss knife for malware researchers (and everyone else)**

http://virustotal.github.io/yara/



pdns_count

1,473

Count

pdns_max_answer_len

ANSWER_LEN: Descending	Count
225	94
68	2
63	2
53	1

pdns_auto_ranks

DOMAIN: Descending	Count
xxxx3.xyz	154
xxxx2.xyz	138
xxxx5.xyz	133
xxxx4.xyz	109
xxxx1.xyz	108
xxxx6.xyz	91
thatwasgreat.xyz	40
trevofinancas.xyz	23
obtrk.xyz	20
konkase.xyz	17
abc.xyz	16
clickpartoffon.xyz	16
gitcdn.xyz	16
hhit.xyz	13
ohanalomo.xyz	13
upxip.xyz	13
lolxm.xyz	11
mobee.xyz	11
balt.xyz	10
retag.xyz	10
vkmusic.xyz	10
gaytubevideos.xyz	9
yarbot.xyz	9
dezdemonfashiontrends.xyz	8
1tushkan.xyz	7
globalmaps.xyz	7

Export: Raw Formatted

1 2 3 4 »

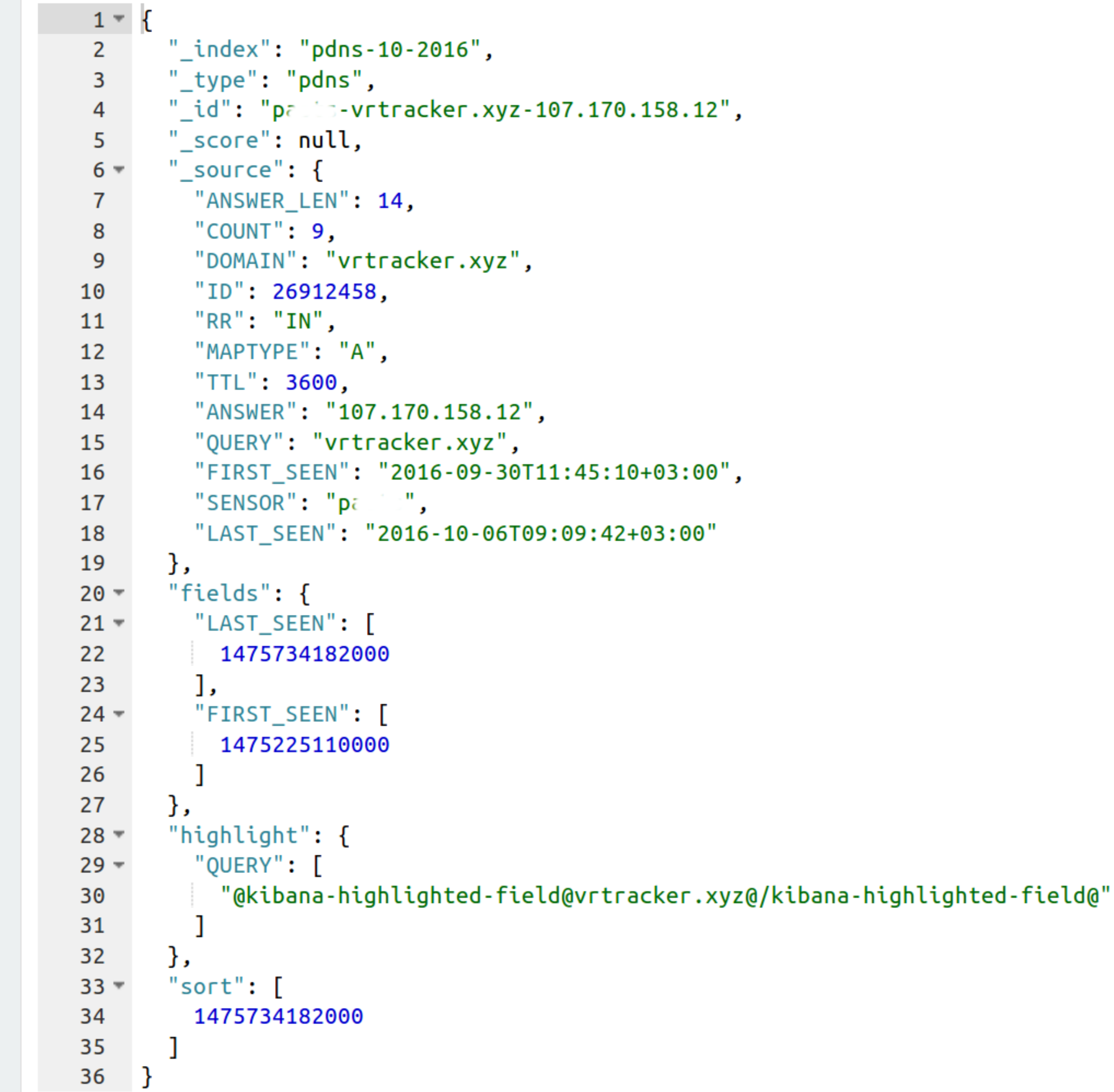
pdns_top_queries

QUERY: Descending	Max COUNT
vkmusic.xyz	21,439
hhit.xyz	6,280
totalstats.xyz	2,703
www.totalstats.xyz	2,127

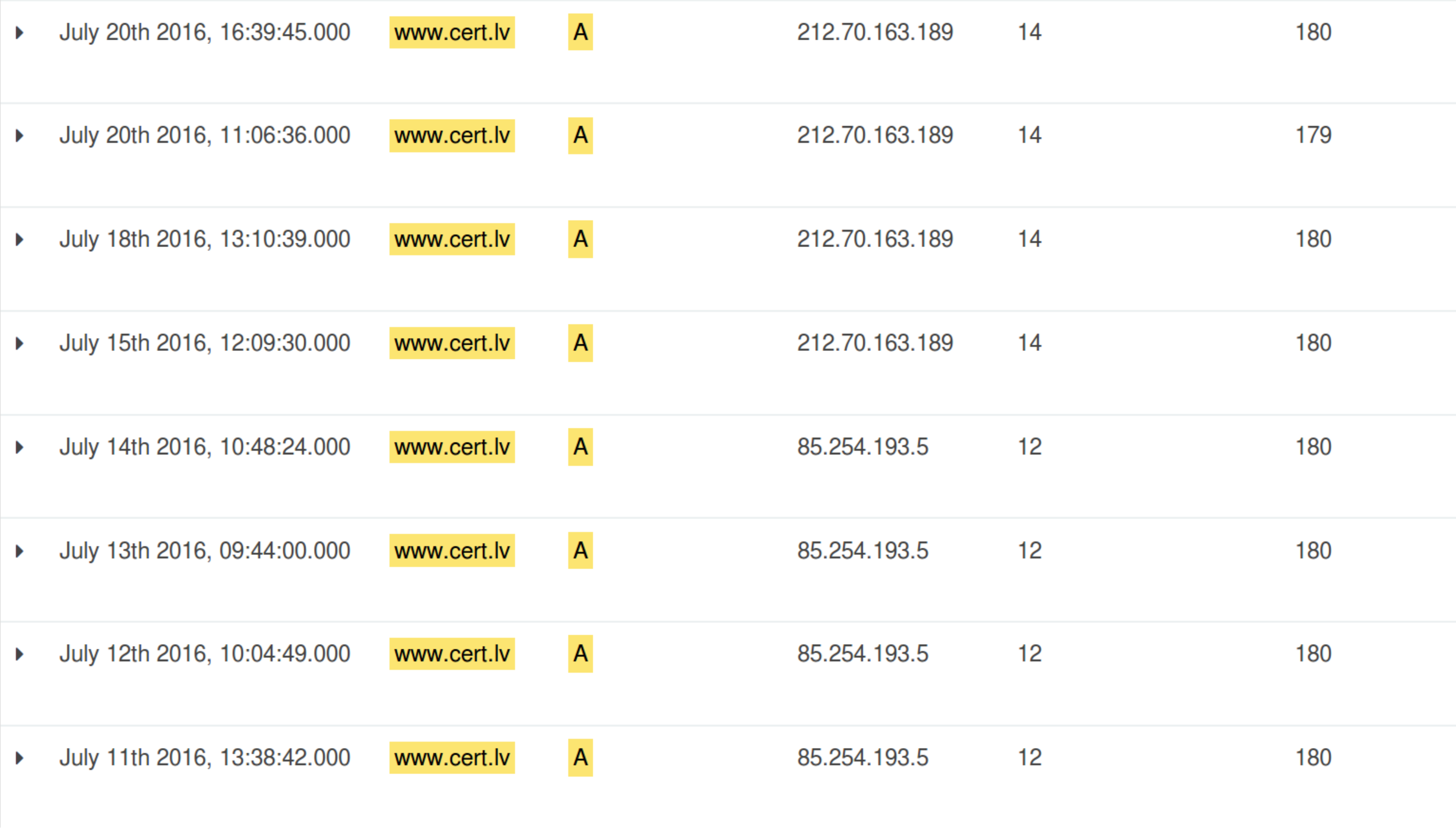
pdns_entries

1 2 3 4 5 ...10 »

Time	QUERY	MAPTYPE	ANSWER	ANSWER_LEN	TTL	FIRST_SEEN
October 6th 2016, 09:12:29.000	updpopcorntime.xyz	A	104.18.51.196	13	300	August 25th 2016, 12:01:47.000
October 6th 2016, 09:12:29.000	updpopcorntime.xyz	A	104.18.50.196	13	300	August 25th 2016, 12:01:47.000
October 6th 2016, 09:12:03.000	grabber.xyz	A	104.28.15.116	13	300	September 29th 2016, 13:00:29.000
October 6th 2016, 09:12:03.000	grabber.xyz	A	104.28.14.116	13	300	September 29th 2016, 13:00:29.000
October 6th 2016, 09:12:03.000	www.grabber.xyz	CNAME	grabber.xyz	11	300	September 29th 2016, 13:00:29.000
October 6th 2016, 09:09:42.000	vrtracker.xyz	A	107.170.158.12	14	3,600	September 30th 2016, 11:45:10.000
October 6th 2016, 08:54:23.000	upxip.xyz	CNAME	teser.net	9	1,800	May 31st 2016, 11:44:31.000
October 6th 2016, 08:54:23.000	lolxm.xyz	CNAME	teser.net	9	1,800	April 24th 2016, 01:48:56.000



```
{
  "_index": "pdns-10-2016",
  "_type": "pdns",
  "_id": "pa[redacted]-vrtracker.xyz-107.170.158.12",
  "_score": null,
  "_source": {
    "ANSWER_LEN": 14,
    "COUNT": 9,
    "DOMAIN": "vrtracker.xyz",
    "ID": 26912458,
    "RR": "IN",
    "MAPTYPE": "A",
    "TTL": 3600,
    "ANSWER": "107.170.158.12",
    "QUERY": "vrtracker.xyz",
    "FIRST_SEEN": "2016-09-30T11:45:10+03:00",
    "SENSOR": "pa[redacted]",
    "LAST_SEEN": "2016-10-06T09:09:42+03:00"
  },
  "fields": {
    "LAST_SEEN": [
      1475734182000
    ],
    "FIRST_SEEN": [
      1475225110000
    ]
  },
  "highlight": {
    "QUERY": [
      "@kibana-highlighted-field@vrtracker.xyz@/kibana-highlighted-field@"
    ]
  },
  "sort": [
    1475734182000
  ]
}
```



▸	July 20th 2016, 16:39:45.000	www.cert.lv	A	212.70.163.189	14	180
▸	July 20th 2016, 11:06:36.000	www.cert.lv	A	212.70.163.189	14	179
▸	July 18th 2016, 13:10:39.000	www.cert.lv	A	212.70.163.189	14	180
▸	July 15th 2016, 12:09:30.000	www.cert.lv	A	212.70.163.189	14	180
▸	July 14th 2016, 10:48:24.000	www.cert.lv	A	85.254.193.5	12	180
▸	July 13th 2016, 09:44:00.000	www.cert.lv	A	85.254.193.5	12	180
▸	July 12th 2016, 10:04:49.000	www.cert.lv	A	85.254.193.5	12	180
▸	July 11th 2016, 13:38:42.000	www.cert.lv	A	85.254.193.5	12	180

Why not using sugar, spice & everything nice?

- Open source automated malware analysis system
  https://github.com/cuckoosandbox/cuckoo
- Highly customizable
- Branch for Android – CuckooDroid
- Integration with MISP

Why not using sugar, spice & everything nice?

MISP
Threat Sharing

- **Malware Information Sharing Platform**
  - There is hardly any reason for keeping the commercial malware IOCs private
  - Criminals share more efficiently than good guys do. This has to be changed…

    https://github.com/MISP/MISP
- **Common taxonomy & format set []**
- **API & PyMISP for automation**
- **Integration with [Cuckoo, Virustotal, Viper, your-custom-module]**

DEMO

- **Demonstration of automated malware hunting & IOC collection**

Takeaways..

- **CERT.LV sandbox will be publicly available in 2nd quarter 2017**
  - https://sandbox.cert.lv
- **Raspberry PI image will be available if there will be interest in this project**
- **CERT.LV MISP instance is available to participants of CERT.LV Sensor network project (government)**
  - Anyone else interested have to contact cert@cert.lv with subject “CERT.LV MISP” explaining the use case & motivation
- **Network forensics & monitoring course**
  - When – 3d quarter of 2017 (follow CERT.LV news)

Takeaways..

- You can have your home-brewed IDS for less than 50 EUR
- You can have your home-brewed MALWARE hunting lab for less than 400 EUR with threat intelligence capability

…

Participate in making the Internet a safer place!

Thank you!

https://www.cert.lv
varis.teivans@cert.lv
Varis Teivans & Uldis Koskins (bro)