Our Incident Response Plan goes something like this...

WORKSHOP 16
17:00 - 18:00

Jordi Guijarro
and
Javier Berciano
CSUC

1 hour

CSIRT-KIT Project

CSIRT-KIT Project (CSUC-CSIRT, CERTSI [INCIBE], ES-CERT UPC) Computer Security Incident Response Teams (CSIRTs) are responsible for receiving and reviewing incident reports, and responding to them as appropriate. These services are normally performed for a defined constituency such as a corporation, institution, educational or government network, region or country, or a paid client. CSIRT services generally fall into three categories – reactive (e.g vulnerability alerts, incident handling); proactive (e.g. intrusion detection, auditing and information dissemination); and security quality management (e.g. risk analysis, disaster recovery planning, and education and training). During the session, we'll explore and "play" with a collection of CERT's daily used opensource tools for handling security incidents. (A live image will be provided where tools like RTIR, IntelMQ, Nfsen, and Pakiti are included).

Problems

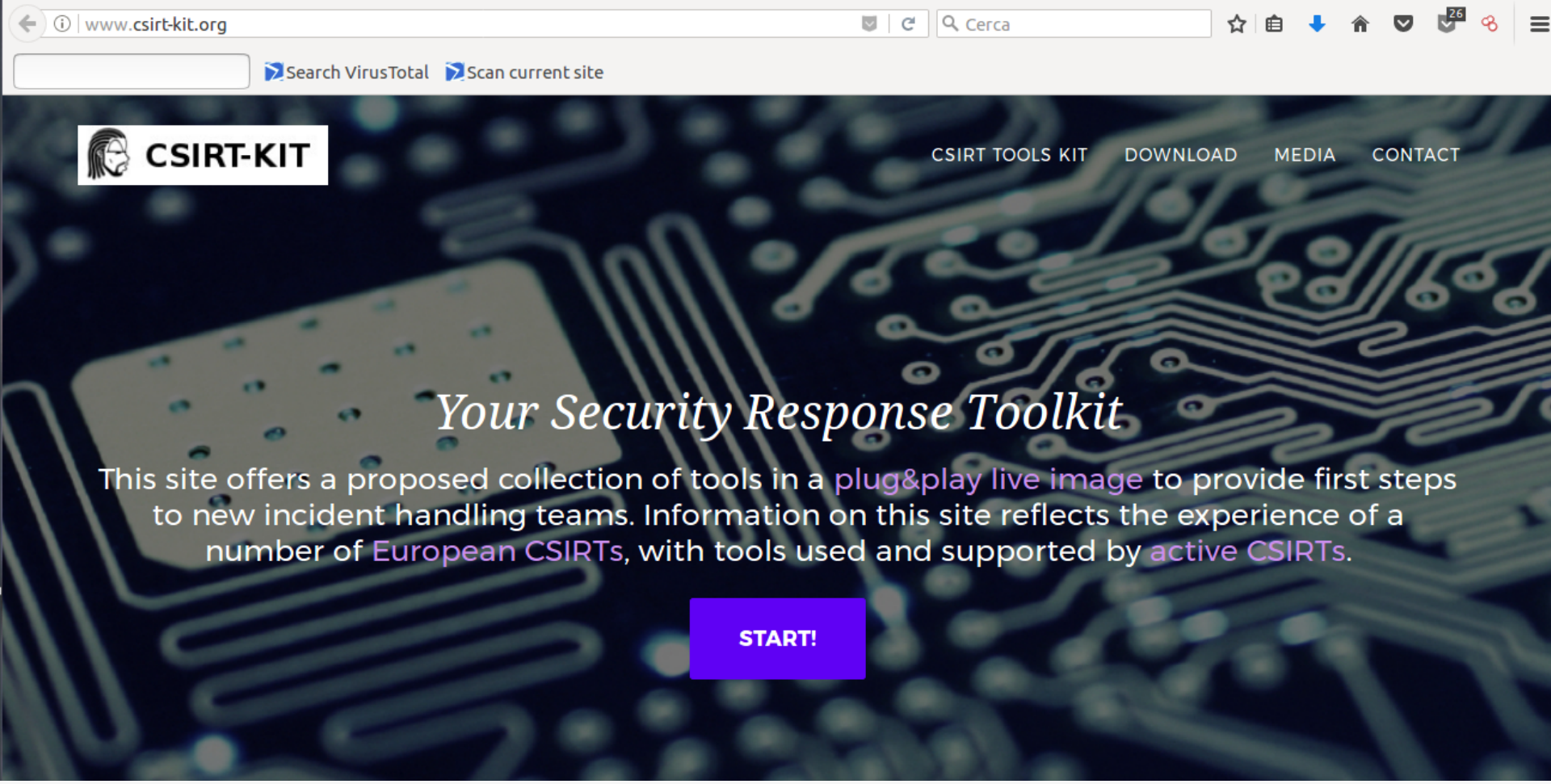
- Missing cooperation
- Incomplete monitoring
- Non-existent experience
- No emergency plan
- Very low awareness

TF-CSIRT
Trusted Introducer

TF-CSIRT Mission

The mission of TF-CSIRT is to facilitate and improve the collaboration between the European CSIRT community to make cyber space a better place.

4



CSIRT-KIT workshop

@jordiguijarro @jberciano borja.guaita@csuc.cat

WITH COLLABORATION OF

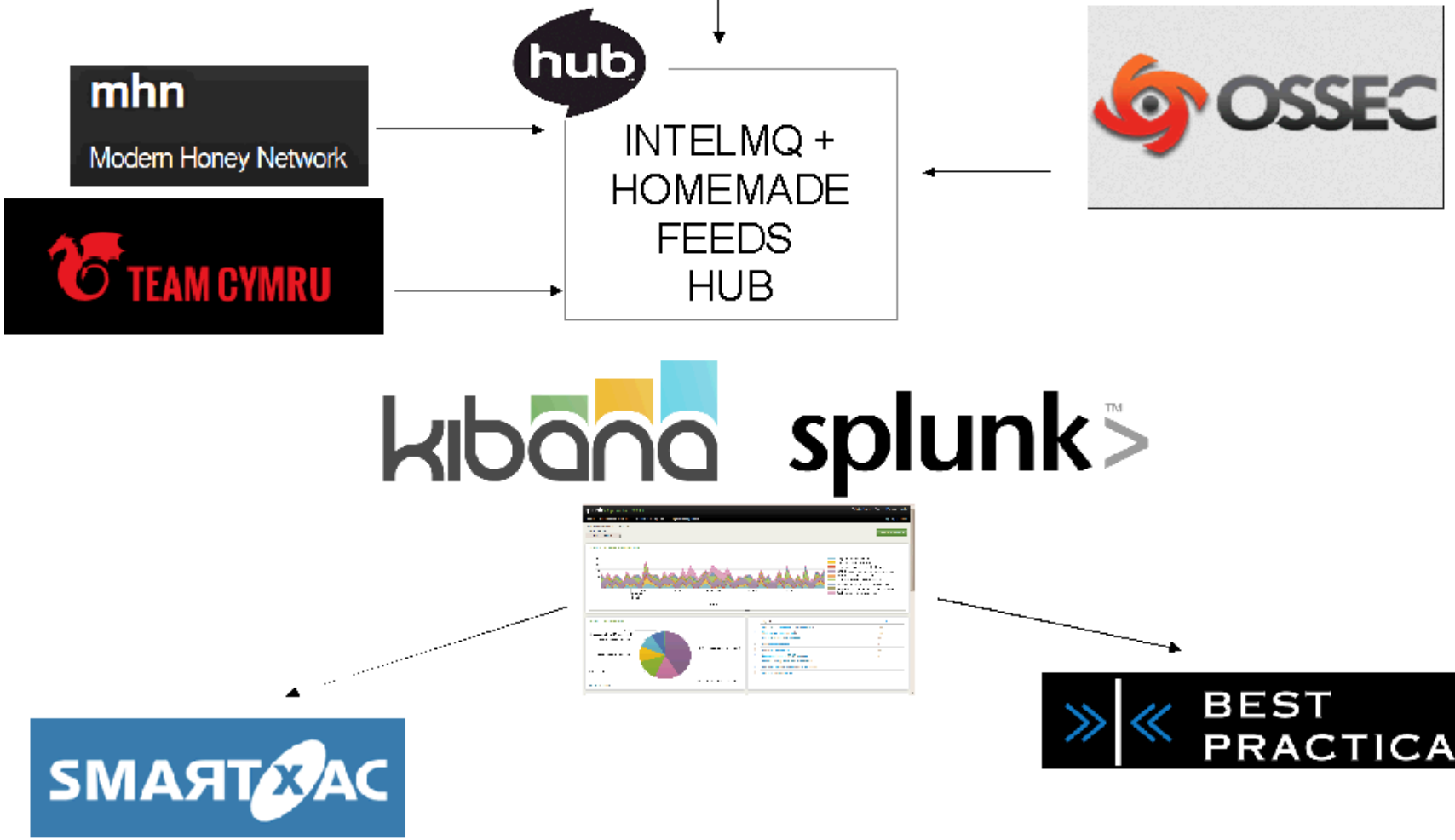
CSUC Consorci de Serveis Universitaris de Catalunya

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

ESCERT

Tools ecosystem : Csirt-kit inspiration!

TC Console


hub
mhn
Modern Honey Network
TEAM CYMRU
INTELMQ +
HOMEMADE
FEEDS
HUB
OSSEC
kibana
splunk>
SMARTXAC
BEST
PRACTICAL™

CSIRT-KIT

Disk Image (OVA)
ftp://ftp.csuc.cat/NCN/csirt-kit.ova

CSIRT-KIT

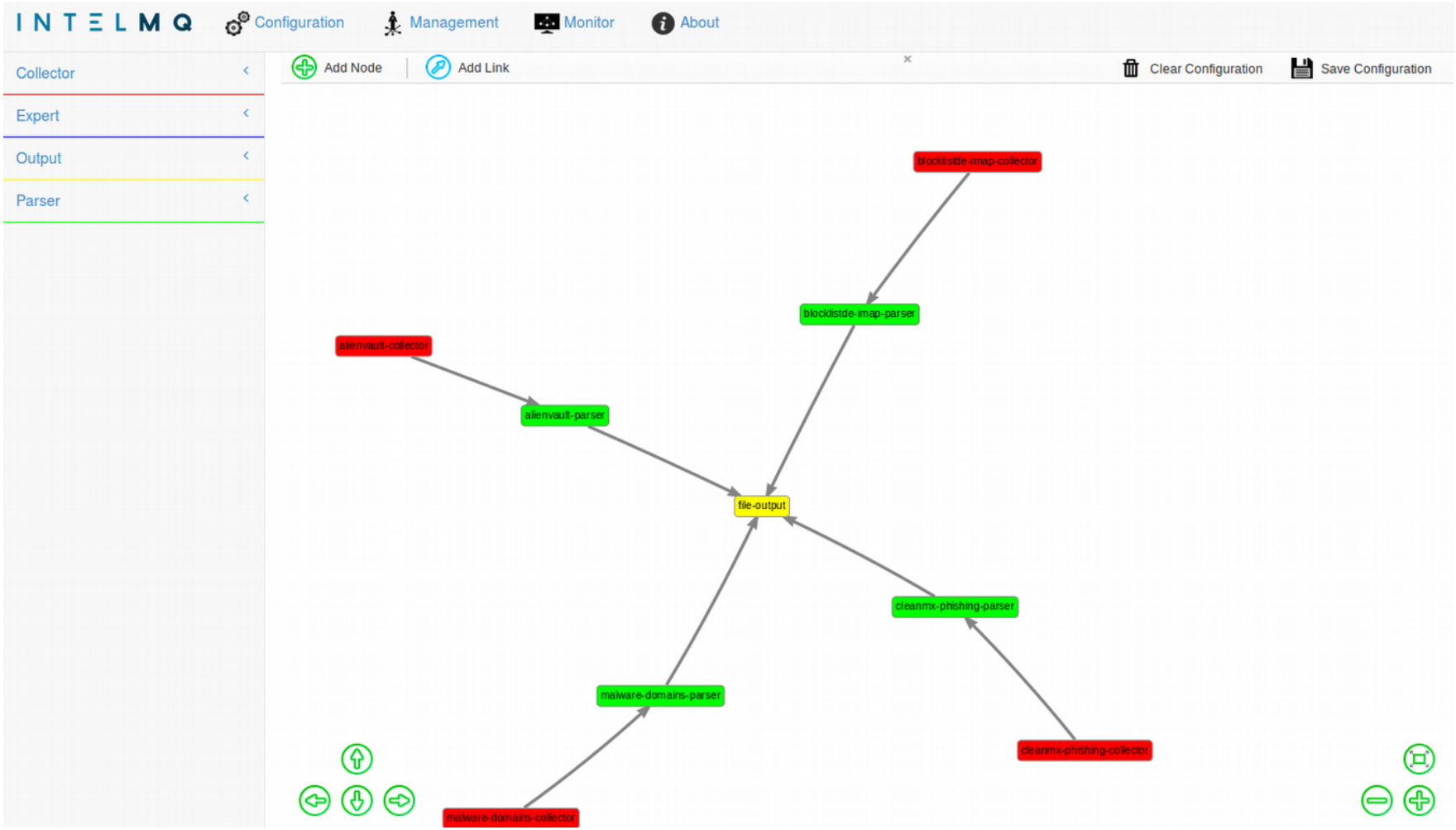
Incident handling information

IntelMQ is a solution for CERTs for collecting and processing security feeds, pastebins, tweets and log files using a message queuing protocol.

https://intelmq.org/

- Automatic feeds injection and processing
- Easy to configure and change (Python)
- GUI (IntelMQ Manager)
- Opensource
- Various output results («enrichment» with expert bots)
    - ASN lookup
    - Abuse contact
    - Whois
    - GeoIP
    - DNS lookups
    - Filters.

https://intelmq.org/



https://intelmq.org/

Malware Information Sharing Platform

http://www.misp-project.org/

Objective

- Facilitate the storage of technical and non-technical information about malware and attacks
- Create automatically relations between malware and their attributes
- Store data in a structured format (allowing automated use of the database to feed detection systems or forensic tools)
- Generate rules for Network Intrusion Detection System (NIDS) that can be imported on IDS systems (e.g. IP addresses, domain names, hashes of malicious files, pattern in memory)

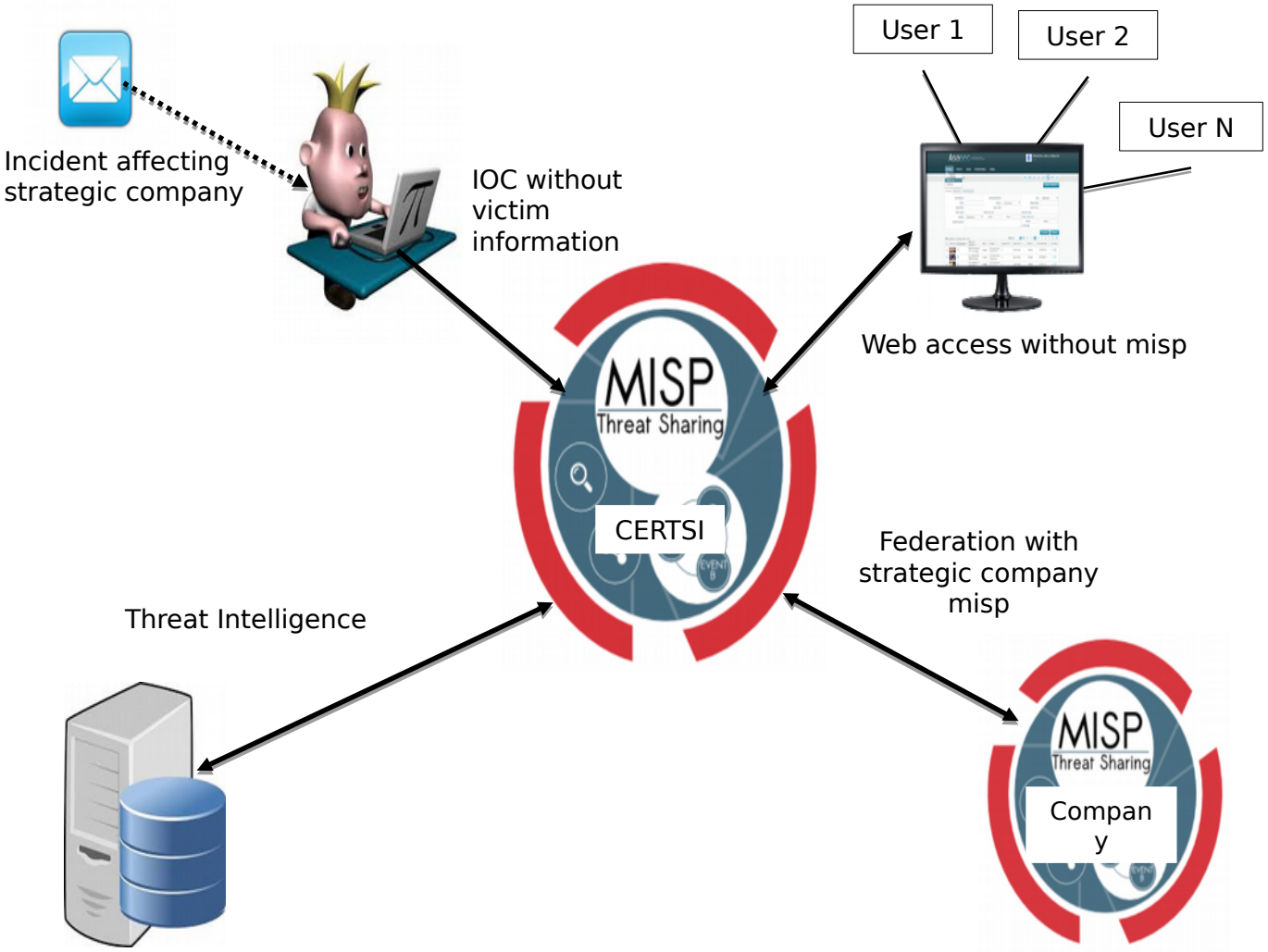
Objective

- Share malware and threat attributes with other parties and trust-groups
- Store locally all information from other instances (ensuring confidentiality on queries)
- Create a platform of trust - trusted information from trusted partners
- Improve malware detection and reversing to promote information exchange among organizations (e.g. avoiding duplicate works)

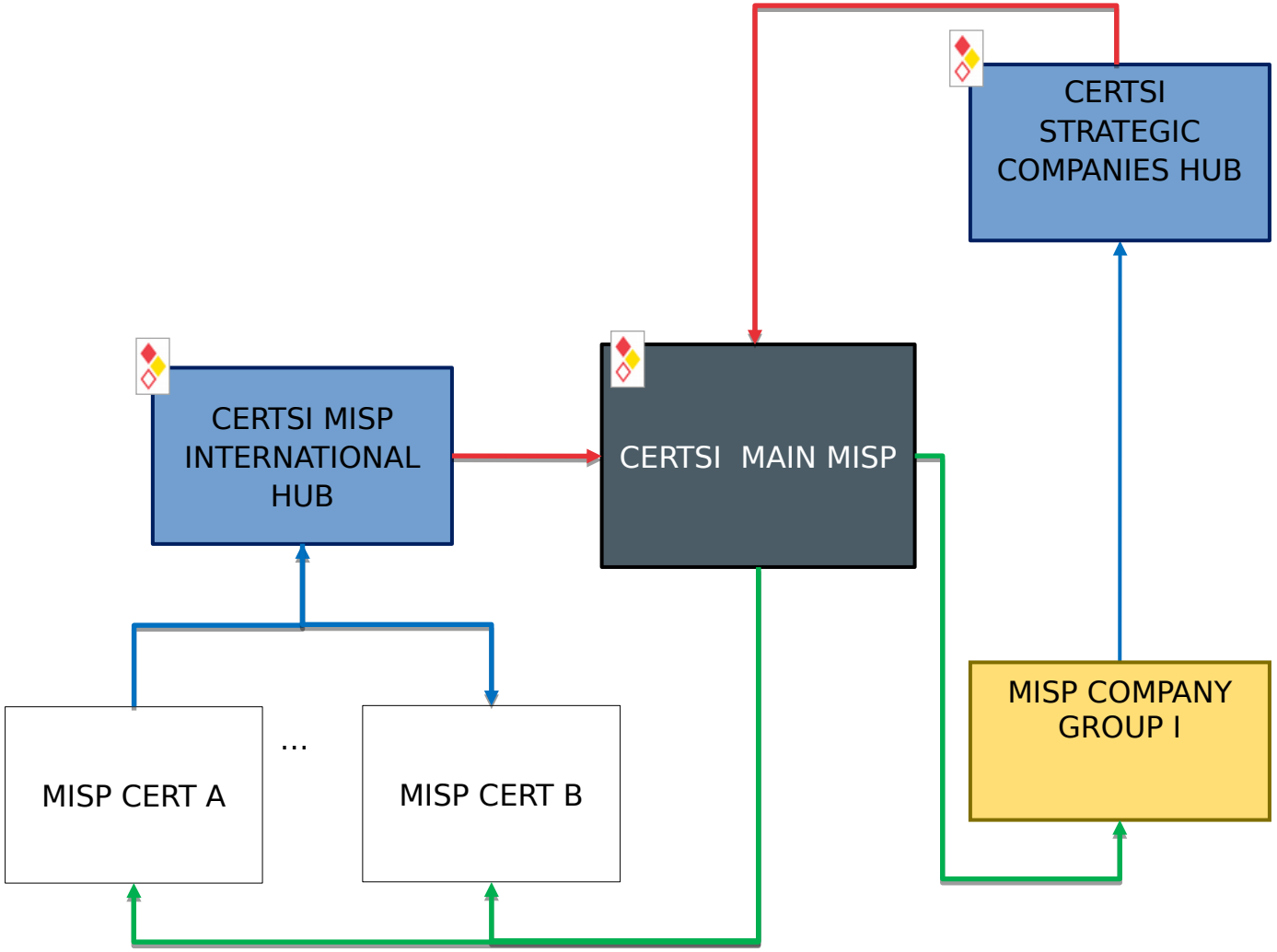
MISP (Malware information Sharing Platform)

Source: http://circl.lu/services/misp-malware-information-sharing-platform/

Model


User 1
User 2
User N
Incident affecting strategic company
IOC without victim information
MISP
Threat Sharing
CERTSI
Web access without misp
Federation with strategic company misp
Threat Intelligence
MISP
Threat Sharing
Compan y

Architecture



View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from OpenIOC
Populate from ThreatConnect
Contact Reporter
Download as...
List Events
Add Event

Ransomware spread through a "Certified mail" campai...

Event ID	173
Uuid	57c57c94-ff3c-4e0f-8780-7093c0a80a8e
Org	INCIBE
Contributors	
Tags	circl:incident-classification="spam" x malware_classification:malware-category="Ransomware" x tlp:green x +
Date	2016-08-30
Threat Level	Low
Analysis	Completed
Distribution	All communities
Description	Ransomware spread through a "Certified mail" campaign impersonating Correos (Spanish national postal service)
Published	Yes

Related Events

2016-06-01 (143) 2016-04-27 (2564) 2015-02-12 (829)

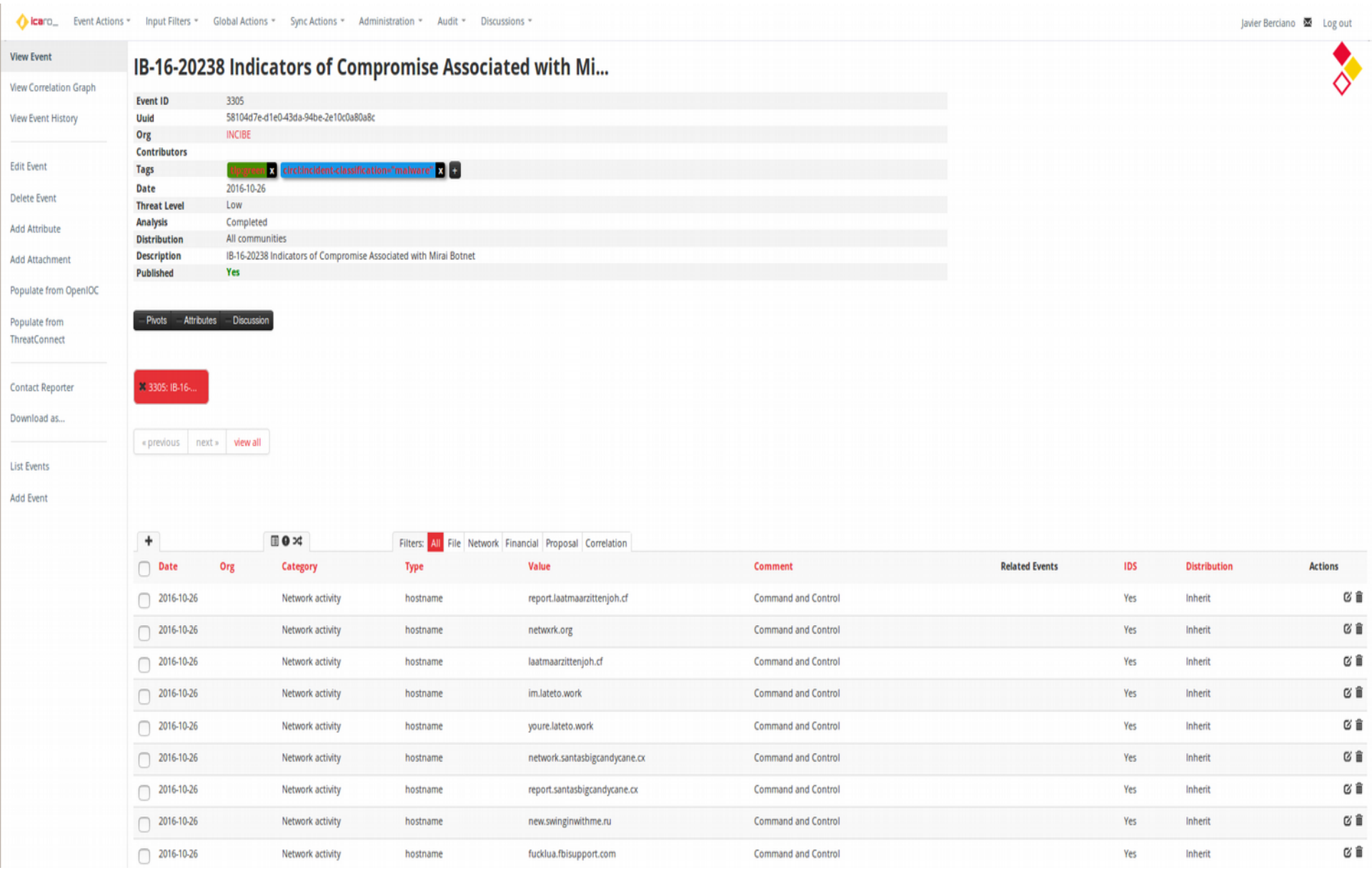
Pivots Attributes Discussion

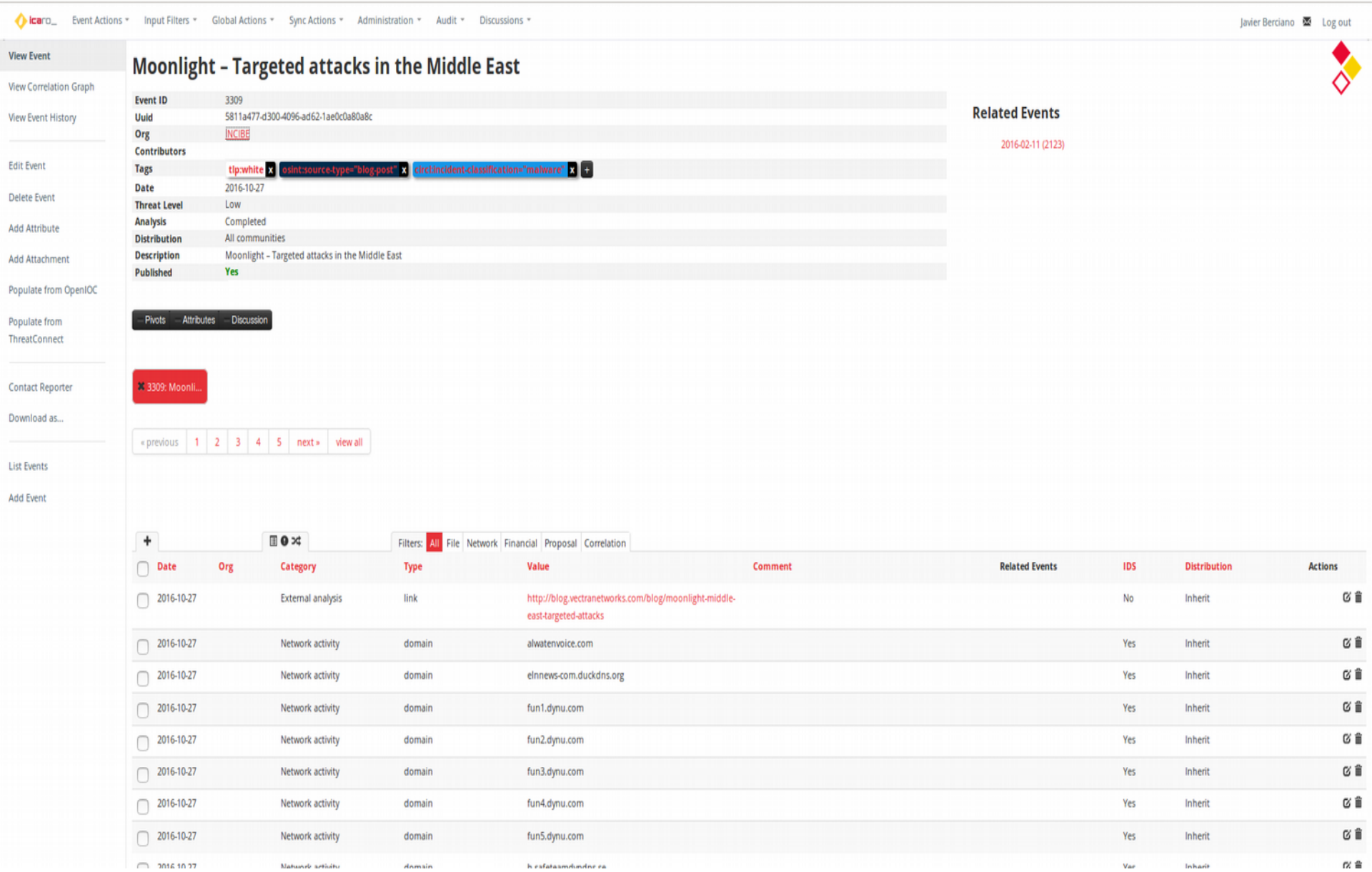
✖ 173: Ransom...

« previous 1 2 next » view all

+ Filters: All File Network Financial Proposal Correlation

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2016-08-30		External analysis	link	https://www.hybrid-analysis.com/sample/3ebb8bdabdfe55488dbecbcbd7668a7b887acfebce7963a963d6f7706fb474a6	Analysis of Carta_Certificada.js		No	Inherit	
2016-08-30		Internal reference	link	https://rtircert.inteco.es/RTIR/Search/Results.html?Query=Subject%20LIKE%20%27[CORREOS]%27%20AND%20Queue%20%3D%20%27Incidents%27%20AND%20id%20%3E=%20%271062306%27	Incidentes en rtir		No	Organisation	
2016-09-02		Internal reference	text	[CORREOS]	campaign-tag		No	Organisation	
2016-09-02		Internal reference	text	[a-z0-9]+\.([a-z0-9-]*?correos) \1	hostname-mangling		No	Organisation	
2016-08-30		Payload delivery	domain	dogus.edu.tr	Compromised domain		Yes	Inherit	
2016-08-30		Payload delivery	domain	correos-server17.org	Malicious domain registered 2016-08-30		Yes	Inherit	


icaro_
Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
Javier Berciano
Log out
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from OpenIOC
Populate from ThreatConnect
Contact Reporter
Download as...
List Events
Add Event
IB-16-20238 Indicators of Compromise Associated with Mi...
Event ID 3305
Uuid 58104d7e-d1e0-43da-94be-2e10c0a80a8c
Org INCIBE
Contributors
Tags tlp:green circl:incident-classification="malware"
Date 2016-10-26
Threat Level Low
Analysis Completed
Distribution All communities
Description IB-16-20238 Indicators of Compromise Associated with Mirai Botnet
Published Yes
Pivots Attributes Discussion
3305: IB-16-...
« previous next » view all
Filters: All File Network Financial Proposal Correlation
Date Org Category Type Value Comment Related Events IDS Distribution Actions
2016-10-26 Network activity hostname report.laatmaarzittenjoh.cf Command and Control Yes Inherit
2016-10-26 Network activity hostname netwxrk.org Command and Control Yes Inherit
2016-10-26 Network activity hostname laatmaarzittenjoh.cf Command and Control Yes Inherit
2016-10-26 Network activity hostname im.lateto.work Command and Control Yes Inherit
2016-10-26 Network activity hostname youre.lateto.work Command and Control Yes Inherit
2016-10-26 Network activity hostname network.santasbigcandycane.cx Command and Control Yes Inherit
2016-10-26 Network activity hostname report.santasbigcandycane.cx Command and Control Yes Inherit
2016-10-26 Network activity hostname new.swinginwithme.ru Command and Control Yes Inherit
2016-10-26 Network activity hostname fucklua.fbisupport.com Command and Control Yes Inherit


Event Actions
Input Filters
Global Actions
Sync Actions
Administration
Audit
Discussions
Javier Berciano
Log out
View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Attachment
Populate from OpenIOC
Populate from ThreatConnect
Contact Reporter
Download as...
List Events
Add Event
Moonlight – Targeted attacks in the Middle East
Event ID 3309
Uuid 5811a477-d300-4096-ad62-1ae0c0a80a8c
Org NCIBF
Contributors
Tags tlp:white osint:source-type="blog-post" circl:incident-classification="malware"
Date 2016-10-27
Threat Level Low
Analysis Completed
Distribution All communities
Description Moonlight - Targeted attacks in the Middle East
Published Yes
Related Events
2016-02-11 (2123)
Pivots
Attributes
Discussion
3309: Moonli...
« previous
1
2
3
4
5
next »
view all
Filters: All File Network Financial Proposal Correlation
Date
Org
Category
Type
Value
Comment
Related Events
IDS
Distribution
Actions
2016-10-27 External analysis link http://blog.vectranetworks.com/blog/moonlight-middle-east-targeted-attacks No Inherit
2016-10-27 Network activity domain alwatenvoice.com Yes Inherit
2016-10-27 Network activity domain elnnews-com.duckdns.org Yes Inherit
2016-10-27 Network activity domain fun1.dynu.com Yes Inherit
2016-10-27 Network activity domain fun2.dynu.com Yes Inherit
2016-10-27 Network activity domain fun3.dynu.com Yes Inherit
2016-10-27 Network activity domain fun4.dynu.com Yes Inherit
2016-10-27 Network activity domain fun5.dynu.com Yes Inherit

CSIRT-KIT

Investigation Ticketing system

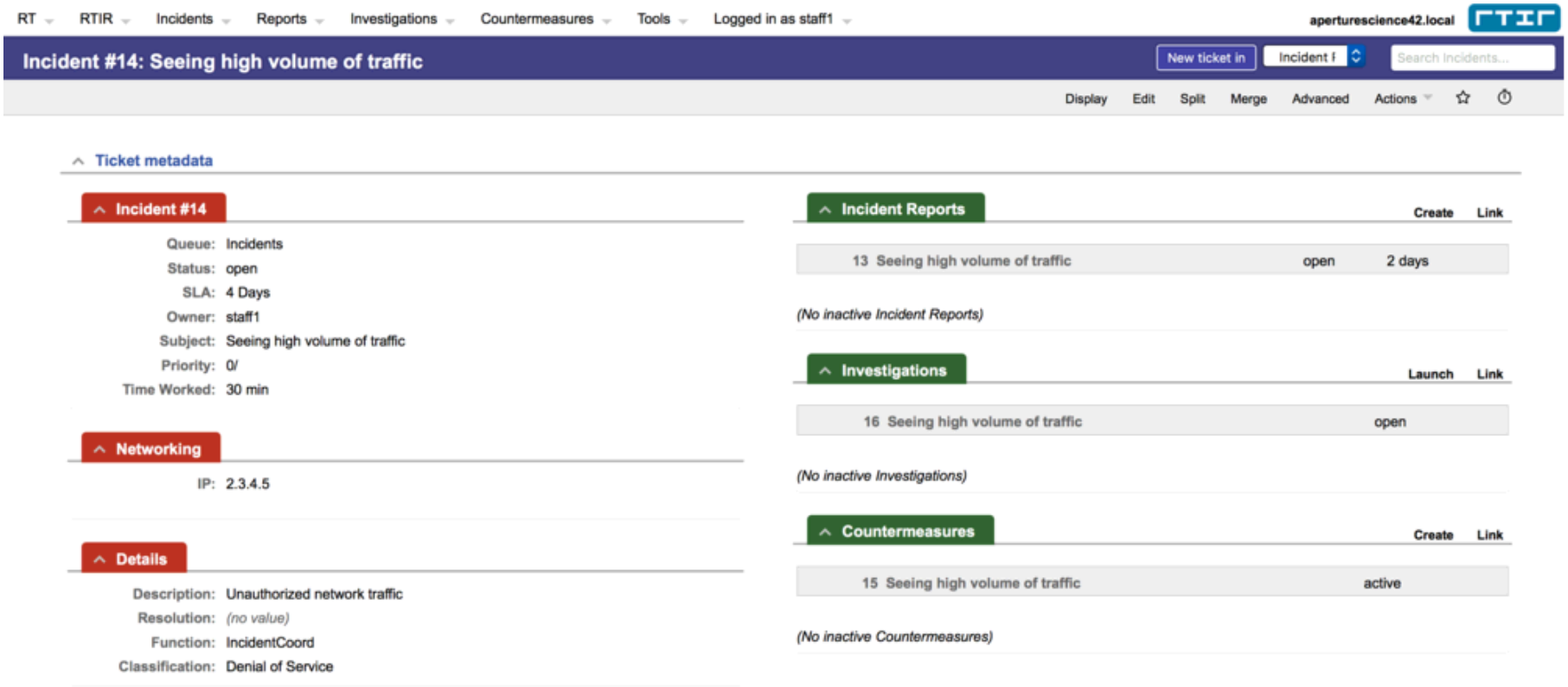
Request Tracker for Incident Response (RTIR) builds on all the features of RT and provides pre-configured queues and workflows designed for incident response.

https://bestpractical.com/rtir/

RTIR: Request tracker for Incident Response

To manage «easily»:

- Incident Requests
- Incidents
- Investigations
- Blocks



CSIRT-KIT

NfSen

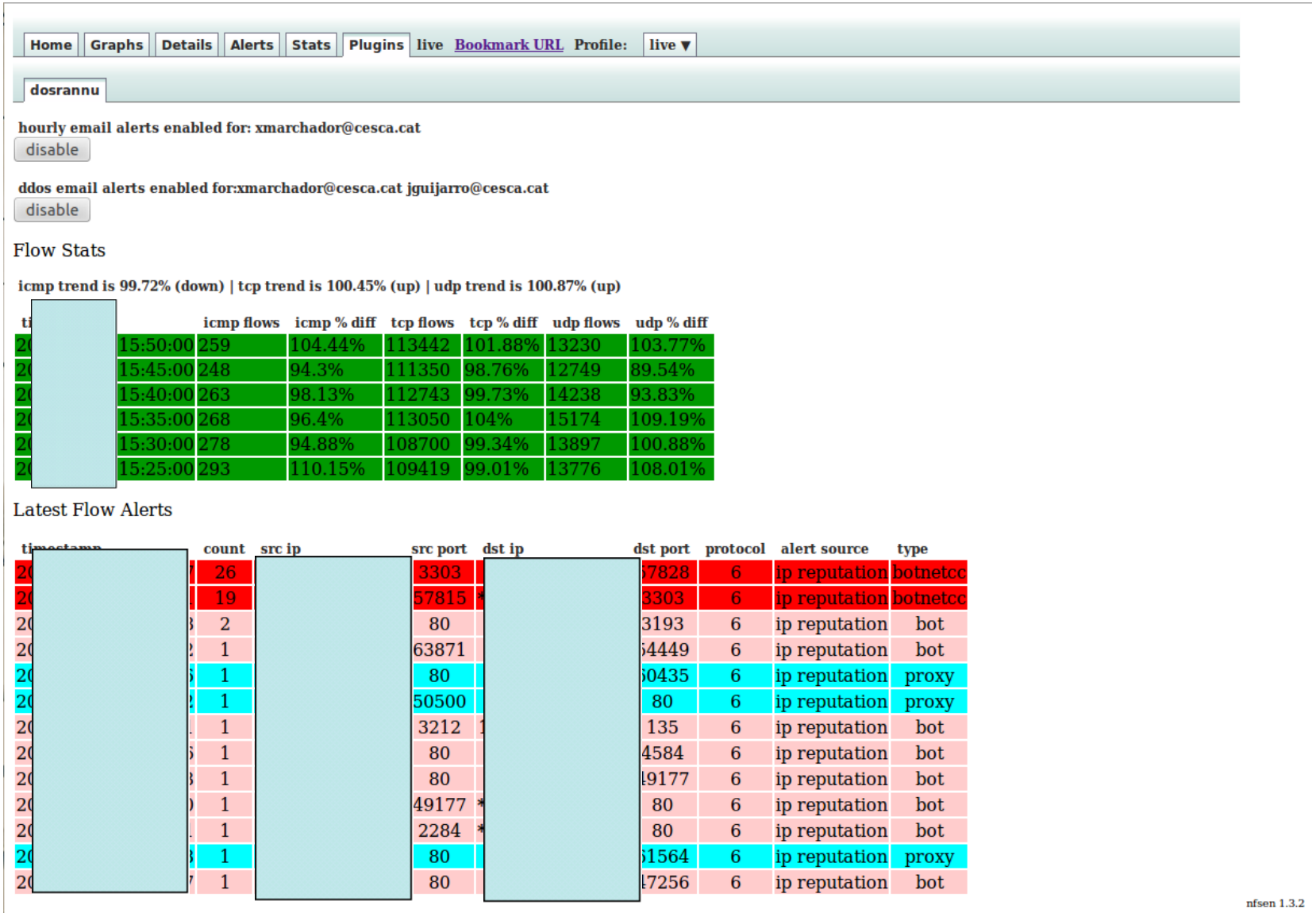
Network forensics

NfSen allows you to keep all the convenient advantages of the command line using nfdump directly and gives you also a graphical overview over your netflow data.

- NFDUMP Graphical interface
- BSD license

http://nfsen.sourceforge.net/

NFSEN



Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: | live ▼

dosrannu

hourly email alerts enabled for: xmarchador@cesca.cat

disable

ddos email alerts enabled for:xmarchador@cesca.cat jguijarro@cesca.cat

disable

Flow Stats

icmp trend is 99.72% (down) | tcp trend is 100.45% (up) | udp trend is 100.87% (up)

ti		icmp flows	icmp % diff	tcp flows	tcp % diff	udp flows	udp % diff
20	15:50:00	259	104.44%	113442	101.88%	13230	103.77%
20	15:45:00	248	94.3%	111350	98.76%	12749	89.54%
20	15:40:00	263	98.13%	112743	99.73%	14238	93.83%
20	15:35:00	268	96.4%	113050	104%	15174	109.19%
20	15:30:00	278	94.88%	108700	99.34%	13897	100.88%
20	15:25:00	293	110.15%	109419	99.01%	13776	108.01%

Latest Flow Alerts

timestamp	count	src ip	src port	dst ip	dst port	protocol	alert source	type
20	26		3303		7828	6	ip reputation	botnetcc
20	19		57815	*	3303	6	ip reputation	botnetcc
20	2		80		3193	6	ip reputation	bot
20	1		63871		4449	6	ip reputation	bot
20	1		80		0435	6	ip reputation	proxy
20	1		50500		80	6	ip reputation	proxy
20	1		3212		135	6	ip reputation	bot
20	1		80		4584	6	ip reputation	bot
20	1		80		9177	6	ip reputation	bot
20	1		49177	*	80	6	ip reputation	bot
20	1		2284	*	80	6	ip reputation	bot
20	1		80		1564	6	ip reputation	proxy
20	1		80		7256	6	ip reputation	bot

nfsen 1.3.2

NFSEN - Stat TopN “proto udp”

Netflow Processing

Source: netflows — All Sources

Filter: proto UDP — and <none>

Options:

- List Flows / Stat TopN
- Top: 10
- Stat: Flow Records order by flows
- Aggregate: proto; srcPort srcIP; dstPort dstIP
- Limit: Packets > 0
- Output: long / IPv6 long

Clear Form | process

```
** nfdump -M /opt/nfsen/profiles-data/live/netflows -T -R 2015/11/30/nfcapd.201511301215:2015/11/30/nfcapd.201511301620 -n 10 -s record/flows -A prot
nfdump filter:
proto UDP
Aggregated flows 473543
Top 10 flows ordered by flows:
Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes Flows
2015-11-30 12:15:00.289 14869.705 UDP                    :24687 ->                  :514    ......    0   979200  479.4 M   258
2015-11-30 12:12:54.864 15020.563 UDP                    :4500  ->                  :7242   ......    0   724800  382.7 M   226
2015-11-30 12:14:21.050 14975.689 UDP                    :60504 ->                  :1024   ......    0     3.7 M    3.8 G   192
2015-11-30 12:14:56.064 14912.933 UDP                    :4500  ->                  :4500   ......    0     9.4 M    1.2 G   147
2015-11-30 12:15:10.148 14960.192 UDP                    :33001 ->                  :38276  ......    0     3.7 M    5.6 G   143
2015-11-30 12:13:54.800 15037.516 UDP                    :33001 ->                  :50590  ......    0     1.4 M    2.1 G   138
2015-11-30 12:15:40.024 14927.471 UDP                    :33001 ->                  :52736  ......    0     1.5 M    2.1 G   137
2015-11-30 12:14:01.138 15045.077 UDP                    :33001 ->                  :42942  ......    0     1.4 M    2.1 G   134
2015-11-30 12:14:48.985 14973.522 UDP                    :33001 ->                  :54354  ......    0     1.4 M    2.1 G   134
2015-11-30 12:14:06.933 14957.230 UDP                    :20785 ->                  :38092  ......    0     1.7 M   97.6 M   132
Summary: total flows: 1157243, total bytes: 2842765995600, total packets: 4332609600, avg bps: 1471178148, avg pps: 280274, avg bpp: 656
Time window: 2015-11-30 12:01:42 - 2015-11-30 16:24:58
Total flows processed: 9163755, Blocks skipped: 0, Bytes read: 879770224
Sys: 1.970s flows/second: 4650002.4  Wall: 11.670s flows/second: 785235.4
```

nfsen 1.3.2

CSIRT-KIT

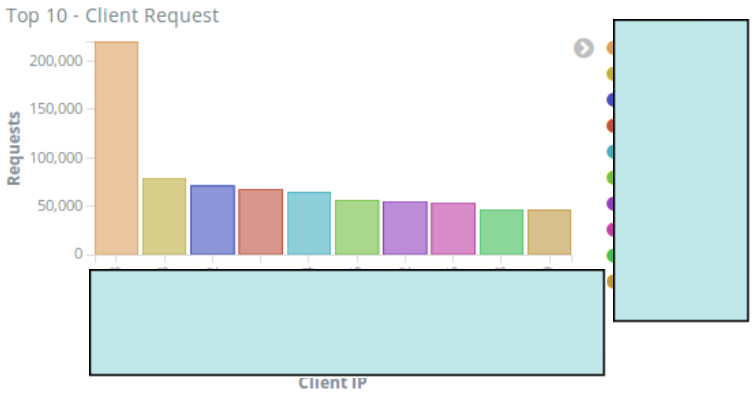
elastic

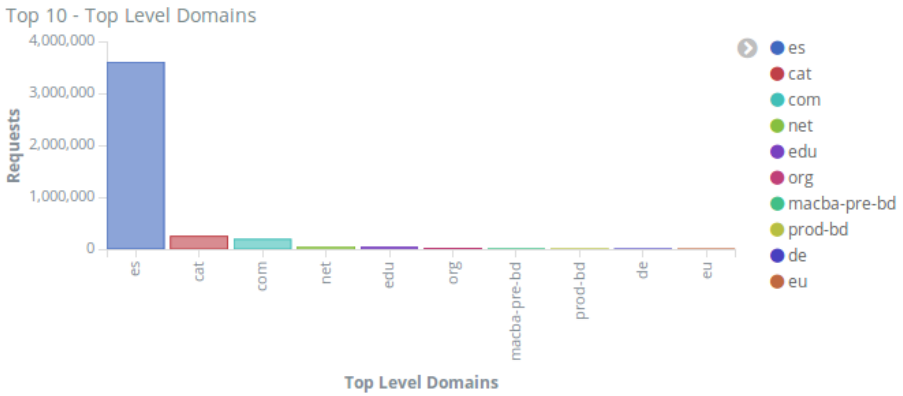
Operational intelligence

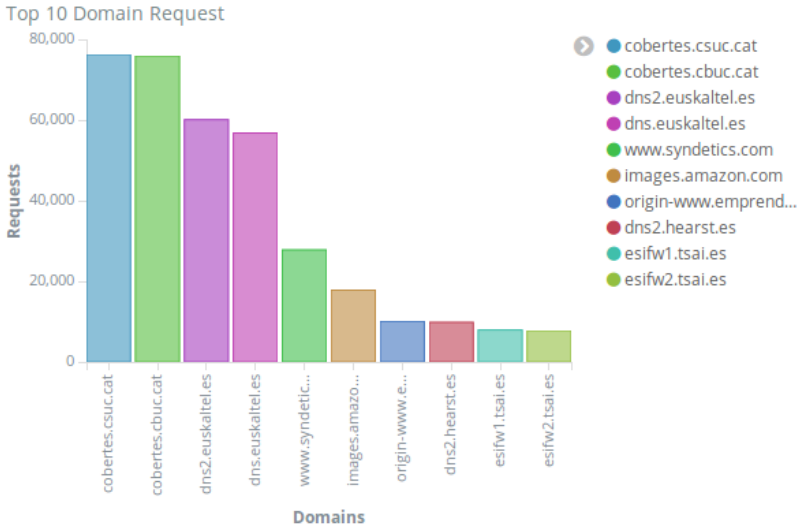
Use **Elastic** to search, monitor, analyze and visualize machine data.

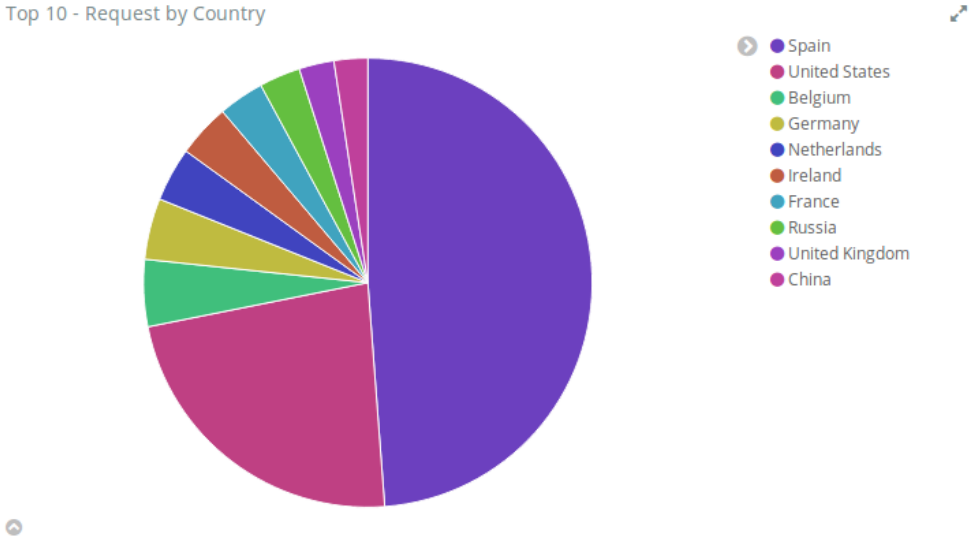
https://www.elastic.co/

ELK and DNS

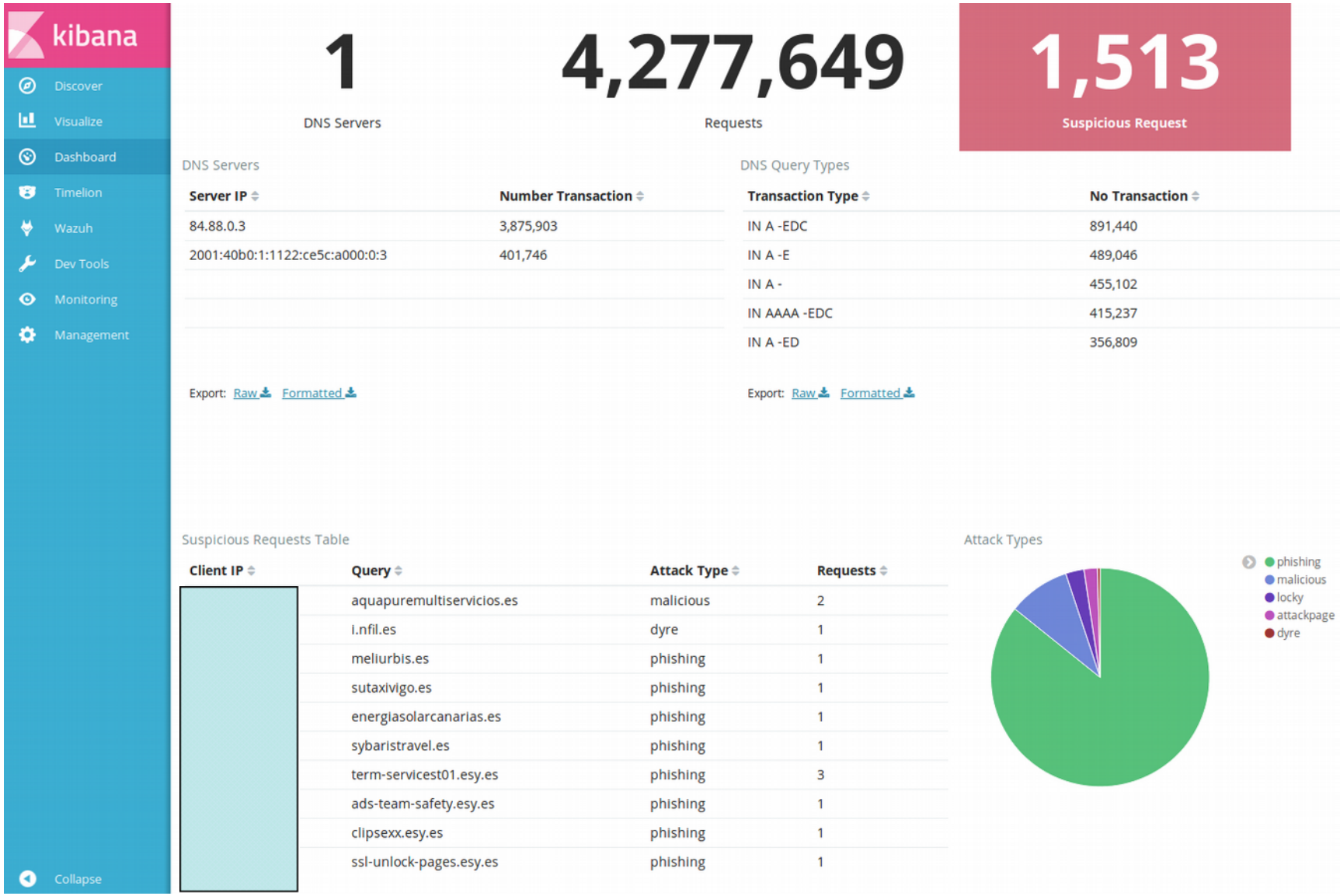

Top 10 - Client Request
200,000
150,000
100,000
50,000
0
Requests
Client IP


Top 10 - Top Level Domains
4,000,000
3,000,000
2,000,000
1,000,000
0
Requests
es
cat
com
net
edu
org
macba-pre-bd
prod-bd
de
eu
Top Level Domains


Top 10 Domain Request
80,000
60,000
40,000
20,000
0
Requests
cobertes.csuc.cat
cobertes.cbuc.cat
dns2.euskaltel.es
dns.euskaltel.es
www.syndetic...
images.amazo...
origin-www.e...
dns2.hearst.es
esifw1.tsai.es
esifw2.tsai.es
Domains


Top 10 - Request by Country
Spain
United States
Belgium
Germany
Netherlands
Ireland
France
Russia
United Kingdom
China

Intel and external sources



Q&A

Thanks!

https://www.csirt-kit.org