

*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

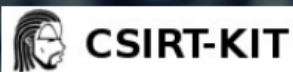


- Missing cooperation
- Incomplete monitoring
- Non-existent experience
- No emergency plan
- Very low awareness



## TF-CSIRT 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.



# Your Security Response Toolkit

This site offers a proposed collection of tools in a **plug&play live image** to provide first steps to new incident handling teams. Information on this site reflects the experience of a number of **European CSIRTs**, with tools used and supported by **active CSIRTs**.

**START!**

## CSIRT-KIT workshop (7th SIG-NOC)



@jordiguijarro

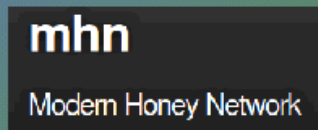
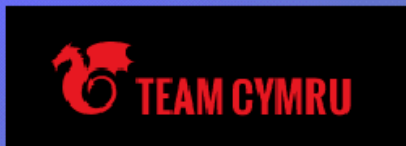
WITH COLLABORATION OF





# Tools ecosystem : Csirt-kit inspiration!

Detection

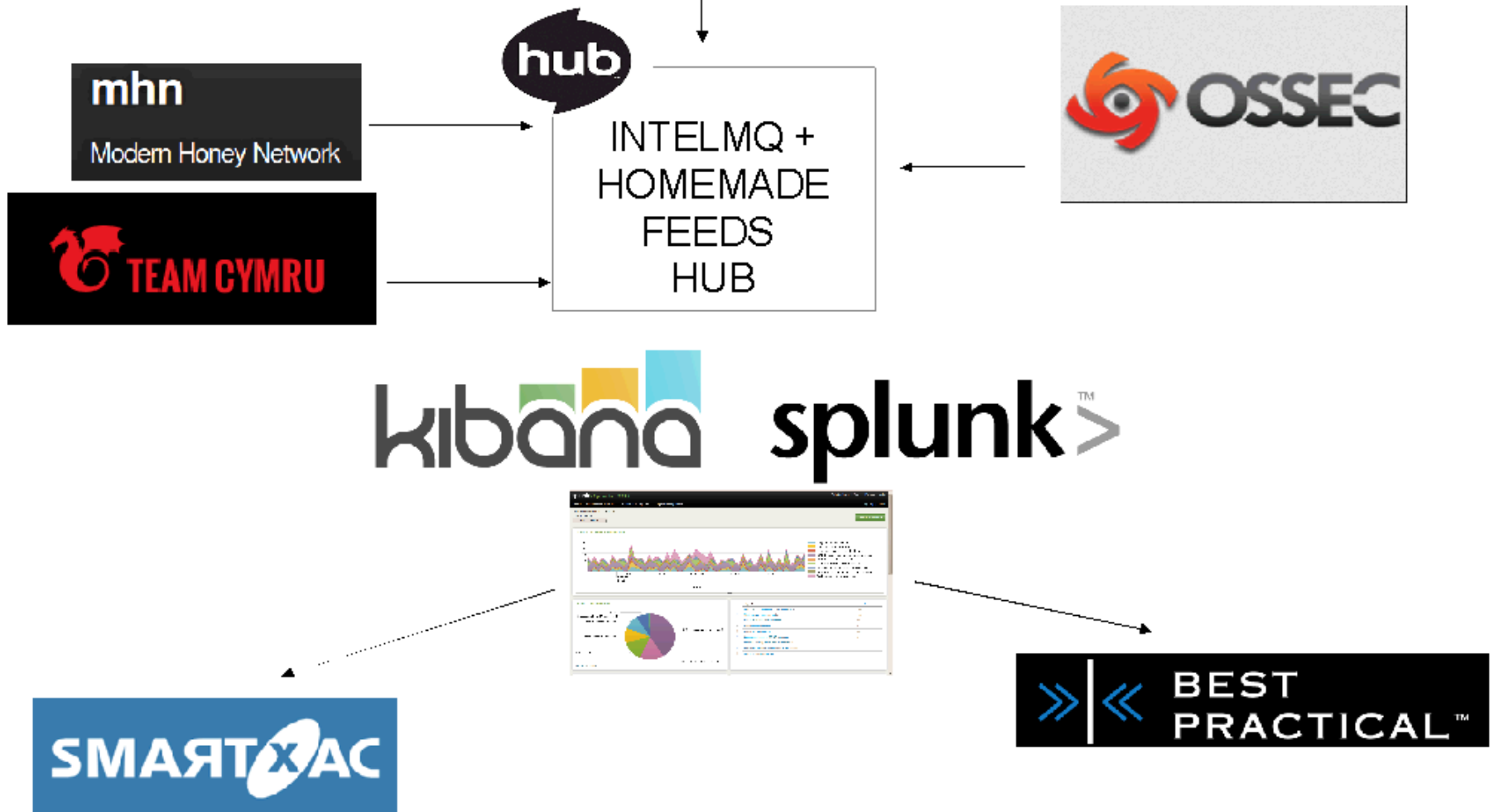


Analysis & Visualization





# TC Console





**CSIRT-KIT**

**Disk Image (OVA)**

**<ftp://ftp.csuc.cat/NCN/csirt-kit.ova>**







# *REPUTATION*



# CSIRT-KIT



INTELMQ

## 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/>



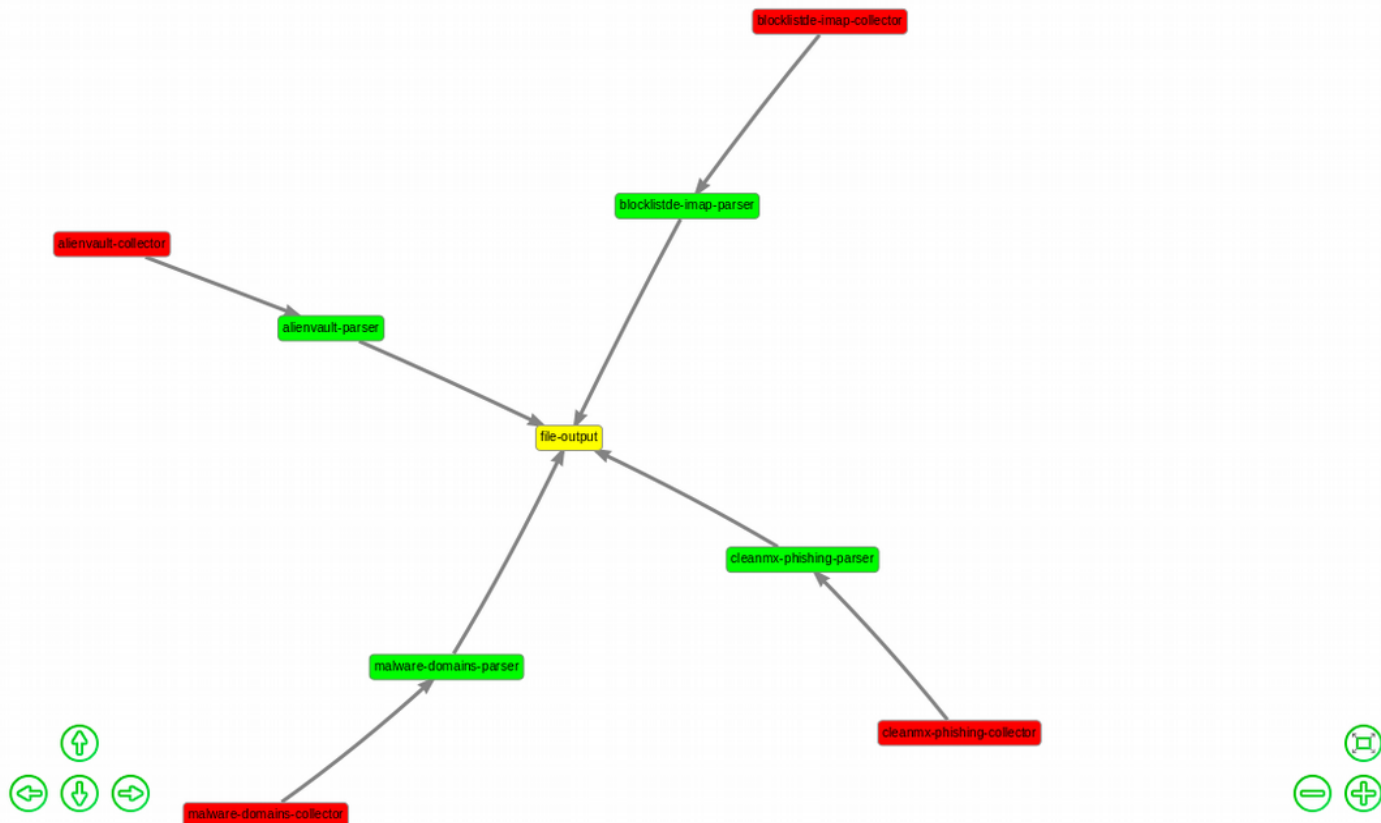
- Automatic feeds injection and processing
- Easy to configure and change (Python)
- GUI (IntelMQ Manager)
- Opensource
- Various output results («enrichment» with expert bots)
  - ASN lookup
  - Abuse contact
  - Whois
  - GeoIP
  - DNS lookups
  - Filters.

<https://intelmq.org/>

- Collector <
- Expert <
- Output <
- Parser <

Add Node Add Link

Clear Configuration Save Configuration



<https://intelmq.org/>



**LEARN TO USE  
THE CRITICISM  
AS FUEL  
& YOU WILL NEVER  
RUN OUT OF  
ENERGY**

**ORRIN WOODWARD**

rennyjogers





# 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

The screenshot displays the RTIR web interface. At the top, there is a navigation bar with menu items: RT, RTIR, Incidents, Reports, Investigations, Countermeasures, Tools, and Logged in as staff1. The current page title is 'Incident #14: Seeing high volume of traffic'. A search bar on the right contains 'Incident f' and a search button. Below the navigation bar, there are action buttons: 'New ticket in', 'Incident f', and 'Search Incidents...'. A secondary bar contains 'Display', 'Edit', 'Split', 'Merge', 'Advanced', 'Actions', and icons for a star and a refresh.

The main content area is divided into two columns. The left column contains three sections: 'Ticket metadata', 'Networking', and 'Details'. The right column contains three sections: 'Incident Reports', 'Investigations', and 'Countermeasures'. Each section has a header with an expand/collapse arrow and a title. The 'Incident Reports' section shows one report with ID 13, status 'open', and '2 days' remaining. The 'Investigations' section shows one investigation with ID 16, status 'open'. The 'Countermeasures' section shows one countermeasure with ID 15, status 'active'. Each section also has 'Create' and 'Link' buttons.

**Ticket metadata**

- Incident #14
- Queue: Incidents
- Status: open
- SLA: 4 Days
- Owner: staff1
- Subject: Seeing high volume of traffic
- Priority: 0/
- Time Worked: 30 min

**Networking**

- IP: 2.3.4.5

**Details**

- Description: Unauthorized network traffic
- Resolution: (no value)
- Function: IncidentCoord
- Classification: Denial of Service

**Incident Reports**

ID	Description	Status	Time
13	Seeing high volume of traffic	open	2 days

(No inactive Incident Reports)

**Investigations**

ID	Description	Status
16	Seeing high volume of traffic	open

(No inactive Investigations)

**Countermeasures**

ID	Description	Status
15	Seeing high volume of traffic	active

(No inactive Countermeasures)

**WHEN THE TEACHER CALLS ON YOU**

**AND YOU DON'T KNOW WHAT THE  
QUESTION WAS**



# 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 - Stat TopN "proto udp"

## Netflow Processing

Source: netflows Filter: proto UDP

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 proto
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

Home Graphs Details Alerts Stats Plugins live [Bookmark URL](#) Profile: live ▼

dosrannu

hourly email alerts enabled for: xmarchador@cesca.cat

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

## Flow Stats

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

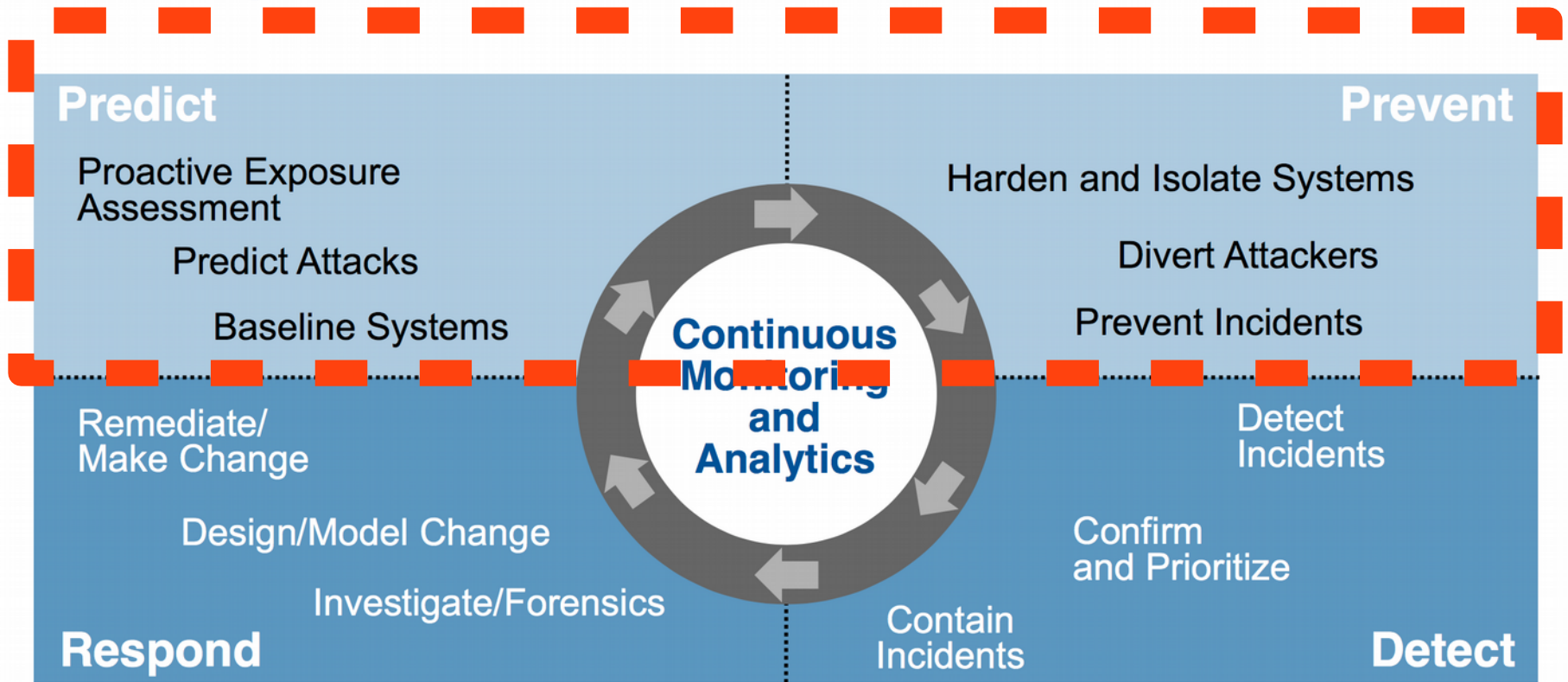
time	icmp flows	icmp % diff	tcp flows	tcp % diff	udp flows	udp % diff
2015-05-01 15:50:00	259	104.44%	113442	101.88%	13230	103.77%
2015-05-01 15:45:00	248	94.3%	111350	98.76%	12749	89.54%
2015-05-01 15:40:00	263	98.13%	112743	99.73%	14238	93.83%
2015-05-01 15:35:00	268	96.4%	113050	104%	15174	109.19%
2015-05-01 15:30:00	278	94.88%	108700	99.34%	13897	100.88%
2015-05-01 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
2015-05-01 15:50:00	26		3303		7828	6	ip reputation	botnetcc
2015-05-01 15:45:00	19		57815		3303	6	ip reputation	botnetcc
2015-05-01 15:40:00	2		80		3193	6	ip reputation	bot
2015-05-01 15:35:00	1		63871		4449	6	ip reputation	bot
2015-05-01 15:30:00	1		80		0435	6	ip reputation	proxy
2015-05-01 15:25:00	1		50500		80	6	ip reputation	proxy
2015-05-01 15:20:00	1		3212		135	6	ip reputation	bot
2015-05-01 15:15:00	1		80		4584	6	ip reputation	bot
2015-05-01 15:10:00	1		80		9177	6	ip reputation	bot
2015-05-01 15:05:00	1		49177		80	6	ip reputation	bot
2015-05-01 15:00:00	1		2284		80	6	ip reputation	bot
2015-05-01 14:55:00	1		80		1564	6	ip reputation	proxy
2015-05-01 14:50:00	1		80		7256	6	ip reputation	bot



# The Adaptive Security Architecture



Gartner



# CSIRT-KIT



elastic

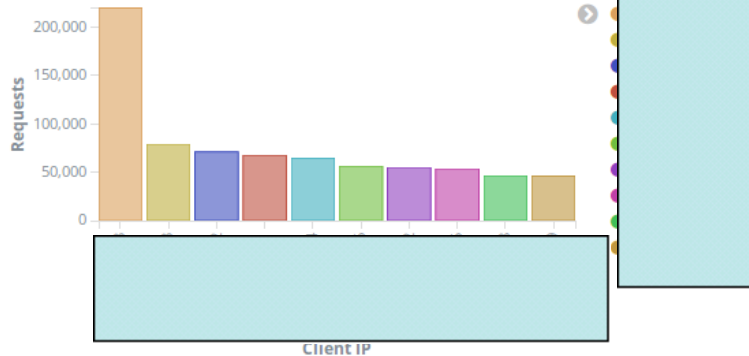
## **Operational intelligence**

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

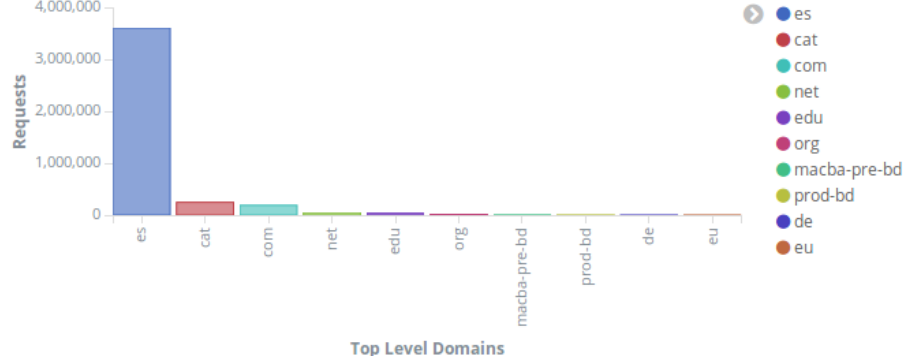
<https://www.elastic.co/>

# ELK and DNS

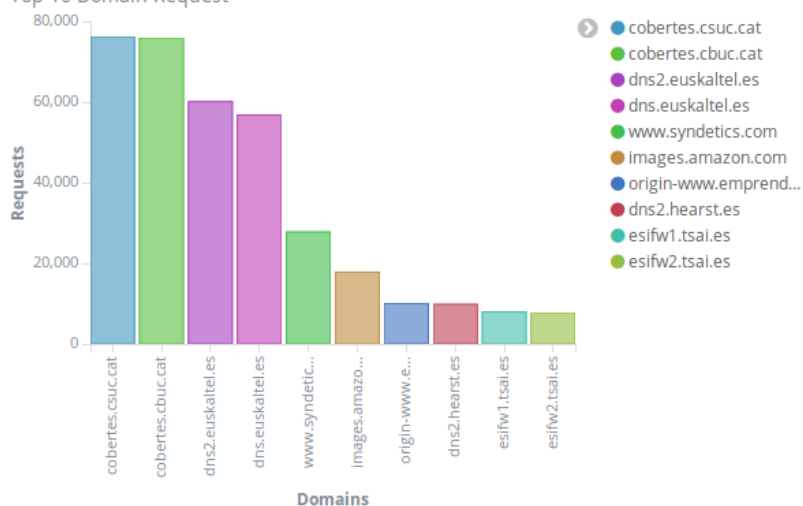
Top 10 - Client Request



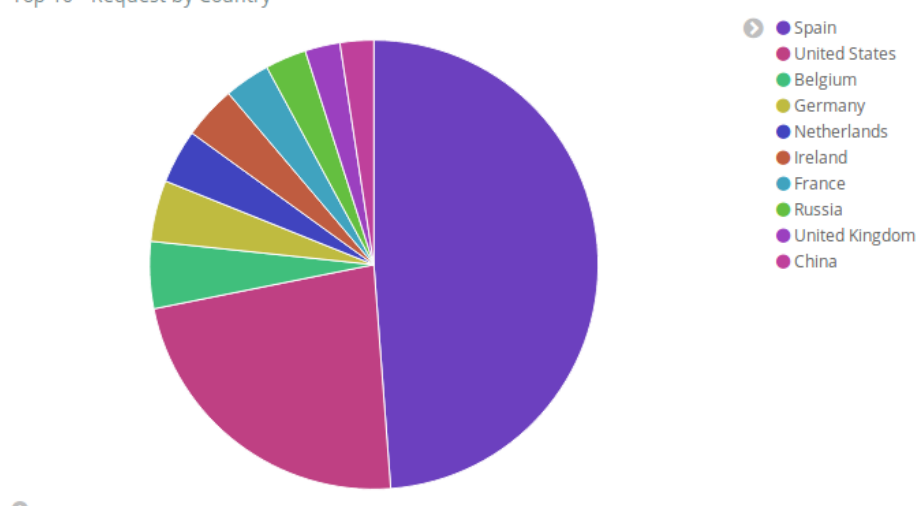
Top 10 - Top Level Domains



Top 10 Domain Request



Top 10 - Request by Country



# Intel and external sources

**kibana**

- Discover
- Visualize
- Dashboard
- Timeline
- Wazuh
- Dev Tools
- Monitoring
- Management

Collapse

# 1

DNS Servers

DNS Servers

Server IP	Number Transaction
84.88.0.3	3,875,903
2001:40b0:1:1122:ce5c:a000:0:3	401,746

Export: [Raw](#) [Formatted](#)

# 4,277,649

Requests

DNS Query Types

Transaction Type	No Transaction
IN A -EDC	891,440
IN A -E	489,046
IN A -	455,102
IN AAAA -EDC	415,237
IN A -ED	356,809

Export: [Raw](#) [Formatted](#)

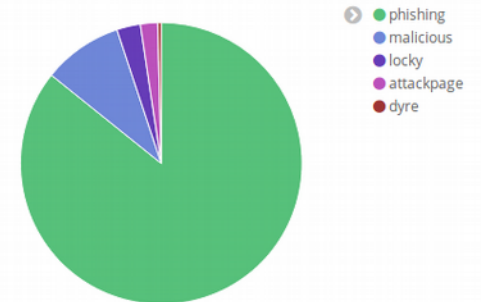
# 1,513

Suspicious Request

Suspicious Requests Table

Client IP	Query	Attack Type	Requests
	aquapuremultiservicios.es	malicious	2
	i.nfil.es	dyre	1
	meliurbis.es	phishing	1
	sutaxivigo.es	phishing	1
	energiasolarcanarias.es	phishing	1
	sybaristravel.es	phishing	1
	term-servicest01.esy.es	phishing	3
	ads-team-safety.esy.es	phishing	1
	clipsex.esy.es	phishing	1
	ssl-unlock-pages.esy.es	phishing	1

Attack Types



Q&A

Thanks!

<http://www.csirt-kit.org>  
@jordiguijarro

