



Team Info

Team Details

Constituency

Contact Information

Cryptography

Memberships

Classification

History

CSUC-CSIRT

CSUC-CSIRT: Equip de Resposta a Incidents de l'Anella Científica

Accredited
since 13 Jan 2015

Fields describing the team

Team Details

Official Name	Short Name	Country
CSUC-CSIRT: Equip de Resposta a Incidents de l'Anella Científica	CSUC-CSIRT	 Spain
Established	Host Organisation	
08 Feb 2011	Consorci de Serveis Universitaris de Catalunya (CSUC)	

Constituency

Constituency Type	Country of Constituency
Research & Education	Spain
ASNs, Domains, IP ranges	Description
13041	CSUC-CSIRT offers full service (incident handling and coordination with other IRTs as a last point of contact for emergency or high priority security matters) to all organizations connected to the Anella
15633	
43115	
49638	



Consorti de
Serveis Universitaris
de Catalunya

CSUC-CSIRT: Security services for Catalan R&E community

jordi.guijarro@csuc.cat
@jordiguijarro
@cloudadms



Poznan, 21/05/2015



Agenda

- ✓ **Introduction**
- ✓ CSUC-CSIRT Context
- ✓ Our Services
- ✓ Ecosystem of tools
- ✓ In the near future
- ✓ Q&A

New Catalan Universities services consortium (formerly known as CESCA)



Consorci de
Serveis Universitaris
de Catalunya

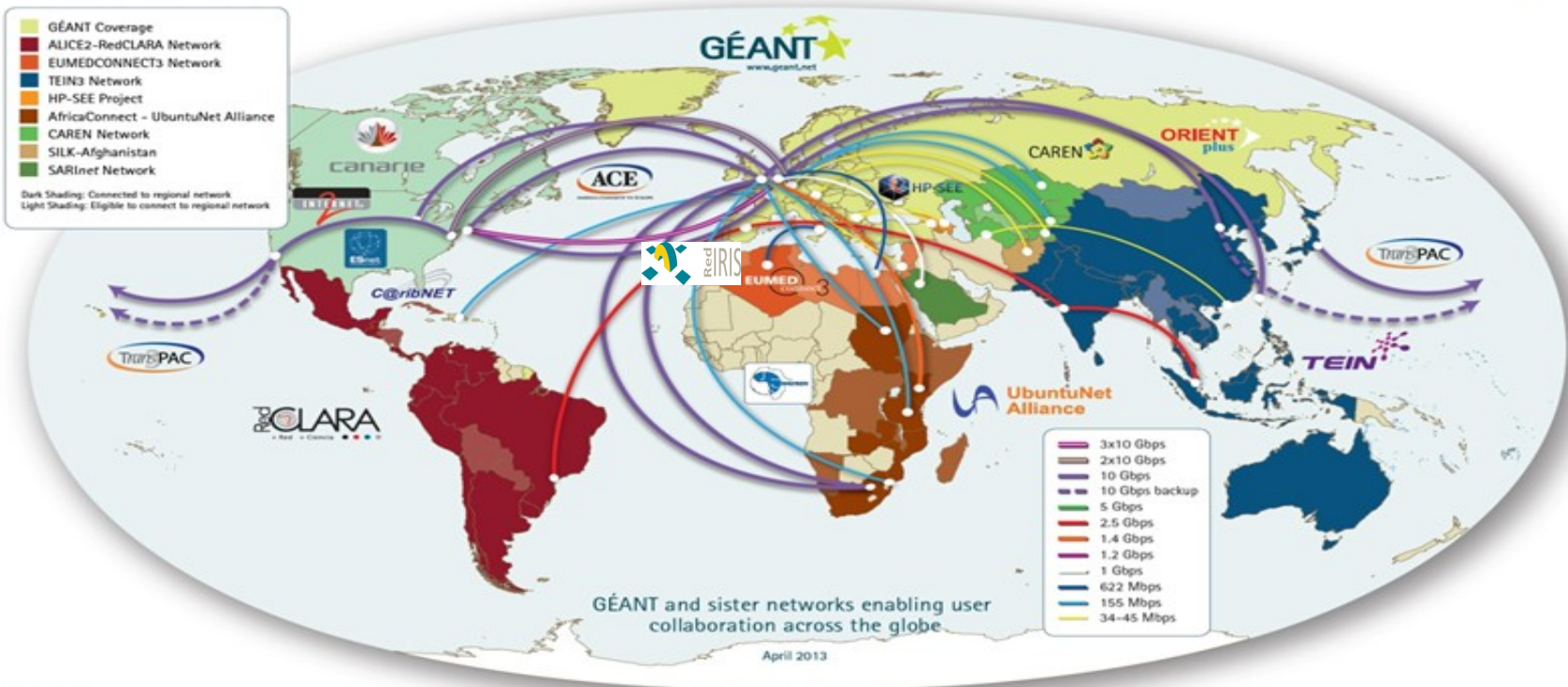


[illegible]

Focused to Research and Education agents



GÉANT At the Heart of Global Research Networking



connect • communicate • collaborate
GÉANT is co-funded by the European Union within its 7th R&D Framework Programme.
This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of DANTE and can under no circumstances be regarded as reflecting the position of the European Union.



Focused to Research and Education agents



At the H Research Networking

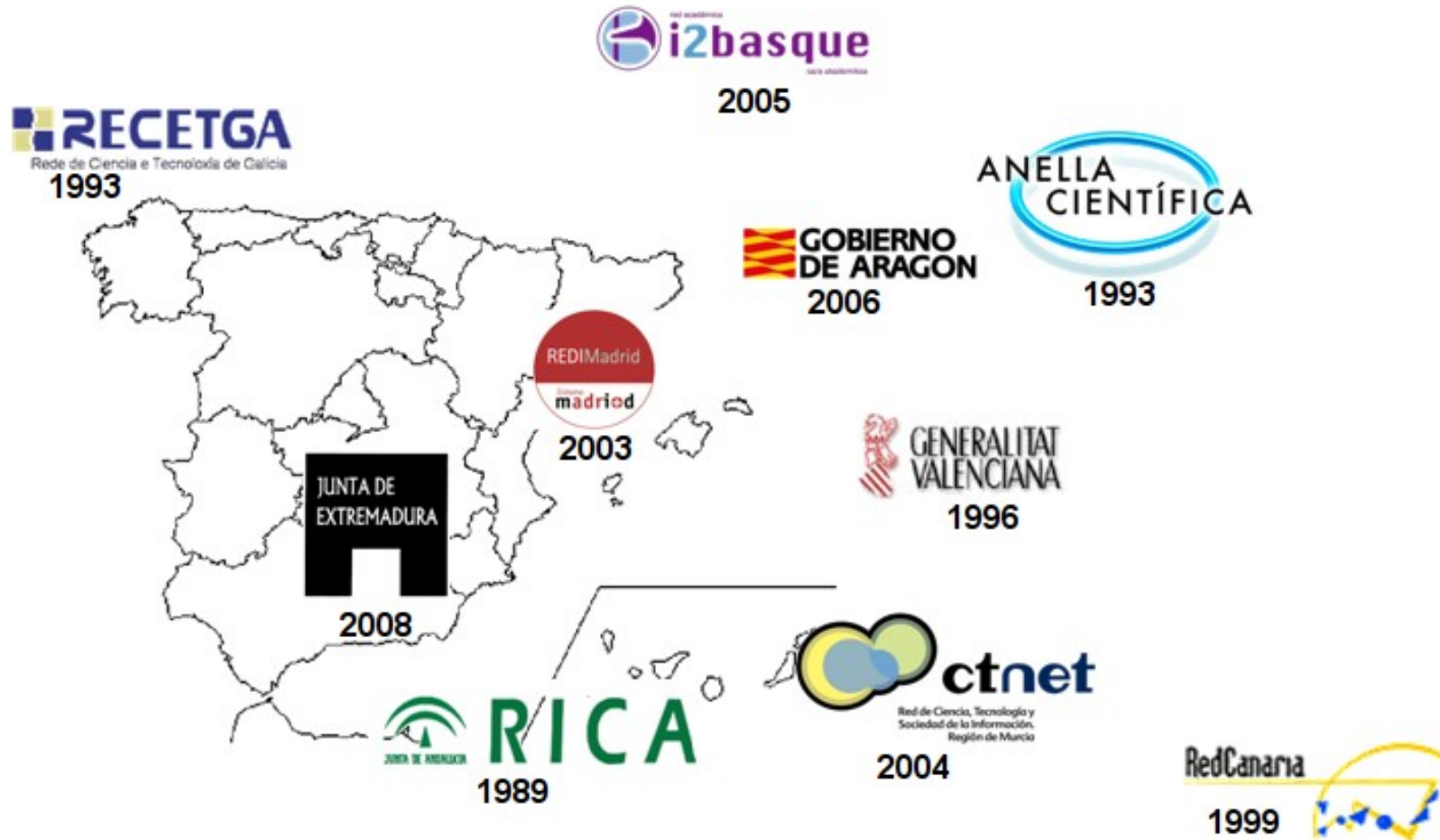


connect • communicate • collaborate

GÉANT is co-funded by the European Union within its 7th R&D Framework Programme.
This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of DANTE and can under no circumstances be regarded as reflecting the position of the European Union.



Regional R&E Networks

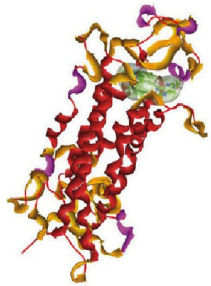


Our services

Scientific Computing

Supercomputing

Drug Design



Communications



Library Services



PUC

Portals and Repositories



e-Administration



Archiving



Certification



Registry



Voting



Logs



Signature



Interoperability



PCCD

Shared Services

Electric Energy

Content Management

Printing

SAP-FICO

Mobile

DPC

Operations and Security



Data Center



Hardware



Monitoring



CSIRT

24x7

S24x7

EC-UR

ER-CESCA

SAH

SED

Over 90 connected institutions

A.1	ESMUC	TERMCAT	ICIQ	Teknon	B.4
UB	EUSS	CTTC	IEC	IMIM	Eliepol
UAB	EUG	CTFC	IEEC	Dexeus	Crespolla
UPC	IDEC	LEITAT	IREC	VHIR	TCM
UPF	EADA	CRM			Parc UdG
UdL	WT	IFAE		B.1	PRBB
UdG	INEFC	FBM		AOCIO	
URV	A.2	I2CAT	A.4	FCRI	B.6
UOC	BSC	CMRB	CHV		RI
URL	CSUC	CREAL	CSPT	B.2	
Uvic	CIEMAT	CRESA	FCRB	BC	
UIC	CSIC	CRG	santPau	CGE	
UAO	CELLS	ICFO	FIGTP	MMB	
GSE	IRTA	IMPPC	FHAG	MACBA	
BAU	A.3	UC	IDIBELL	Liceu	
CETI	ASPB	ICS	Guttmann	MHM	
ESCI	CAR	ICGC	Puigvert	FNOB	
ELISAVA					

≥ 1,000 ≥ 100 ≥ 10 ≤ 8

“CSUC” and Security

✓ In Operation from 2003

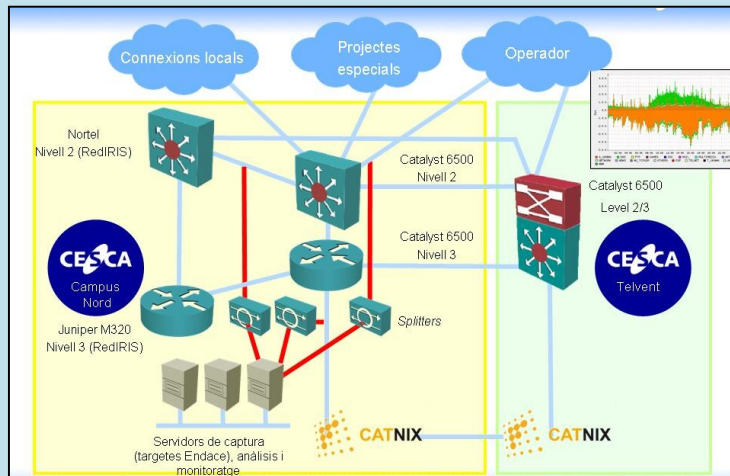
✓ Services

• Equip de Resposta a Incidents de l'Anella Científica (ERIAC)

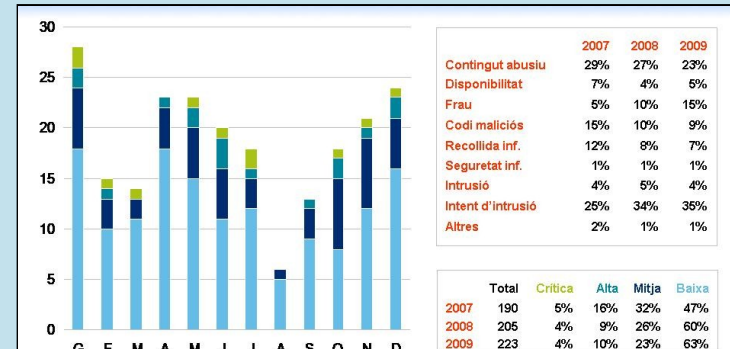
- Proactive detection
- Incident Handling
- Network focused

Listening to the NET: SMARTxAC

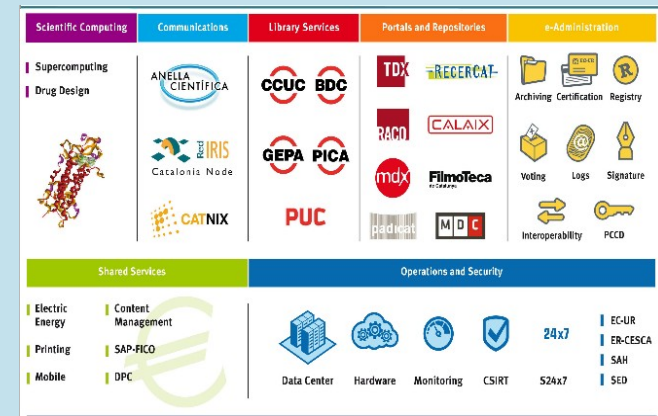
SMARTxAC



ERIAC: Security Response Team



- ✓ Usuaris com a principal objectiu i passarel·la d'atacs
- ✓ Increment del nombre d'incidents per notificacions de RedIRIS i INTECO
- ✓ Continua el creixement de incidents amb baix impacte



Security Services: CSUC-CSIRT

www.csuc.cat/en/communications/security/incident-response-team

Català | English | Castellano

CSUC

Directory | Where We Are | Contact

CSUC | Research | Communications | e-Administration | Libraries (CBUC) | Procurement and New Services

Home > Communications > Security > Incident Response Team

Incident Response Team

Print | Share

Communications

- > Anella Científica
- > Network Services
- > Eduroam
- > Security
 - Description of the Service
 - Incident Response Team
 - Collaborations with organizations
- > RedIRIS in Catalonia
- > Catalonia Neutral Internet Exchange Point: CATNIX

The Incident Response Team of the Anella Científica (CSUC-CSIRT) helps the institutions improve the security of their networks, both by detecting possible incidents and by helping once these occur.

ACCREDITED BY TRUSTED INTRODUCER

It coordinates and manages the resolution of security incidents on the Anella Científica and provides a point of contact for reporting, identifying, and analyzing the impact and the treats which occur, in addition to proposing solutions and strategies for mitigation.

CSUC-CSIRT also disseminates the critical warning notifications of imminent threats via the distribution lists and provides technical support on IT security technologies (analysis of traffic, security of the perimeter, etc.).

Related links

- IRT Ripe Object
- Incident Response Team mission

Related documents

- RFC 2350 (89.37 KB)
- Public PGP (3.05 KB)

Proactive Services

These services help to detect possible anomalies in order to protect the systems.

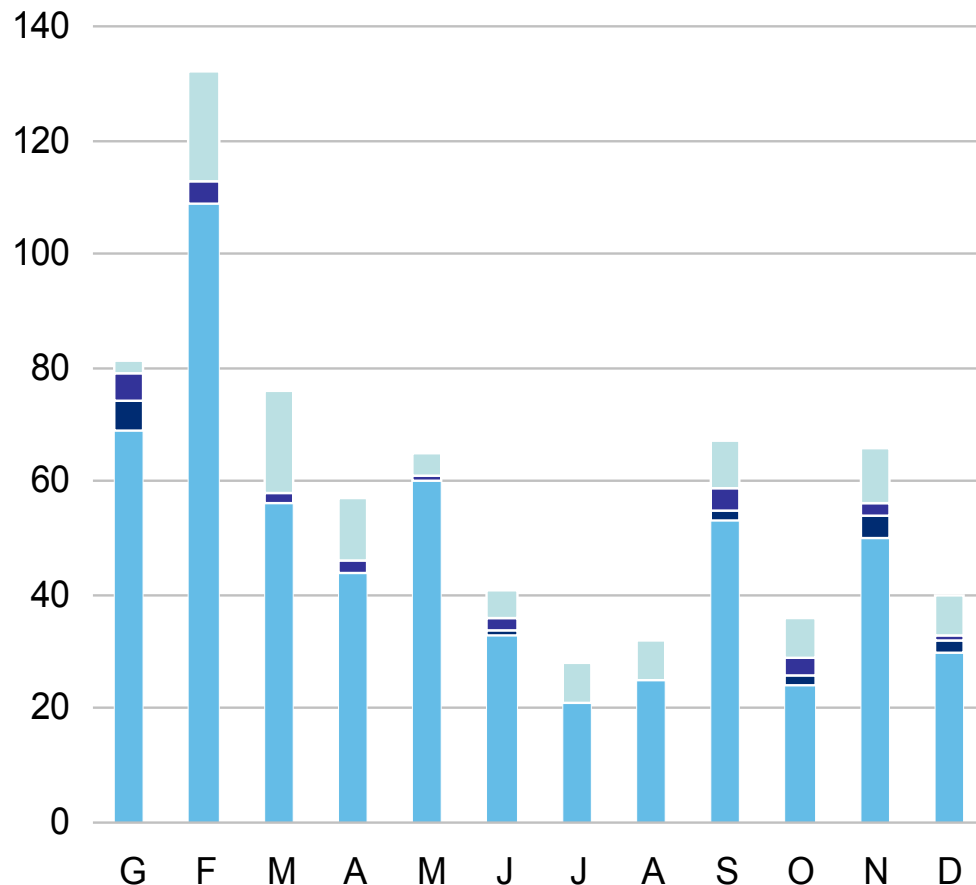
Public PGP Keys

It makes possible a secure communication with our Incident Response Team of the Anella Científica (CSUC-CSIRT)

Report an Incident

Report on security incidents through this form

Security incidents statistics



	2012	2013	2014
Abusive content	40%	20%	33%
Availability	2%	5%	6%
Fraud	7%	14%	7%
Malware	19%	27%	24%
Information rec..	4%	5%	4%
Data Security	5%	5%	2%
Intrusion	4%	2%	6%
Intrusion Attempt	16%	8%	8%
Other	3%	12%	10%

	Total	Critical	High	Medium	Low
2012	660	2%	11%	19%	68%
2013	410	3%	4%	13%	79%
2014	689	12%	2%	10%	76%

¿Inside our DNA?



Collaboration

Collaborations with organizations

The Computer Security Incident Response Team (CSUC-CSIRT) coordinates with other existing groups which respond to incidents and has established a collaborative relationship with police forces for handling security incidents at the Anella Científica.

Some of the institutions which we collaborate with include:

- **CESICAT-CERT**, the security team at the Centre de Seguretat de la Informació de Catalunya (Information Security Center of Catalonia).
- **IRIS-CERT**, the security service of RedIRIS, the national academic and research network.
- **esCERT-UPC**, the security team for the Coordination of Emergencies on Telematic Networks at the UPC.
- **CCN-CERT**, the Computer Emergency Response Team of the National Cryptology Centre (CCN), which is assigned to the National Intelligence Center.
- **INTECO-CERT**, the incident response team of the National Institute of Communication Technologies (INTECO).

NOW -> CERTSI

Collaboration

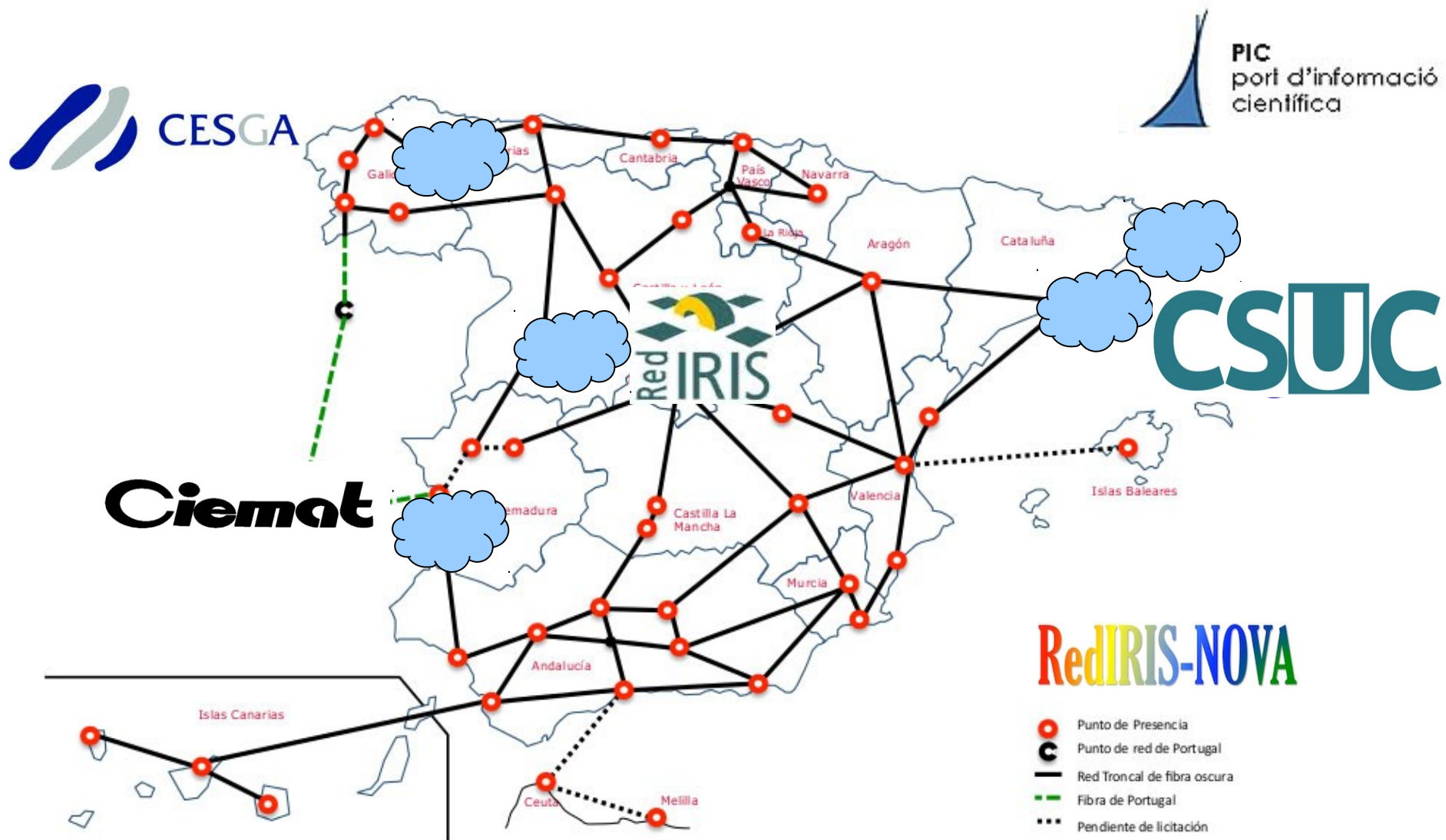
We also participate on various forums and associations for security professionals, which affords us first-hand access to information and contacts for detecting, containing, and resolving any incidents which may occur. Some of the groups we participate in include:

- **ABUSES**, which manages security incidents and disseminates reactive and proactive measures to resolve security incidents related to spam, the distribution of unauthorized content, infections of malicious code, etc.
- **TF-CSIRT**, from Terena, where the members of the computer security incident response teams (CSIRT) exchange experiences and knowledge in a trusted environment.
- **ESNOG** forum, from the Grupo de Operadores de Red Españoles (Spanish Network Operators Group).
- **Trusted Introducer** (TF-CSIRT), is a European reliable platform where **CSUC-CSIRT** is registered and validated as Incident Response Team.

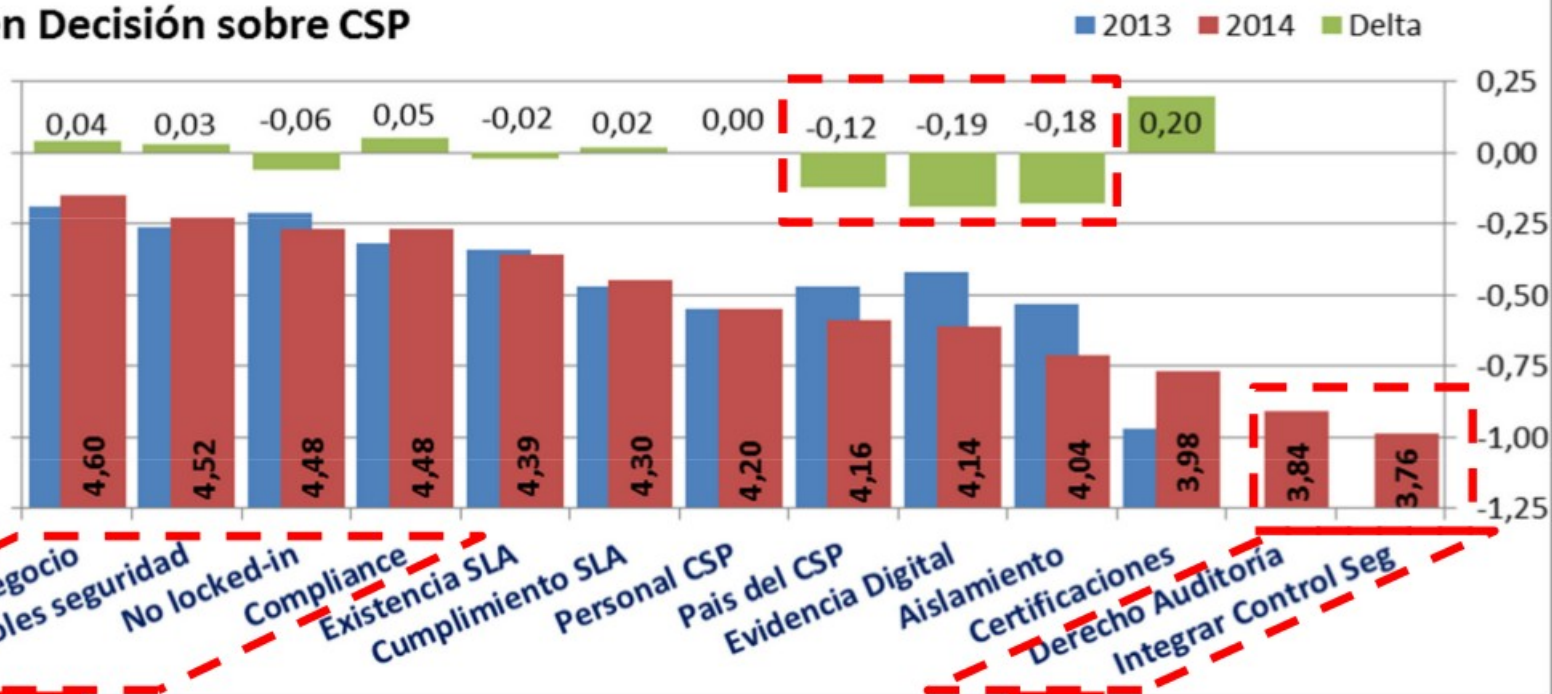


TF-CSIRT
Trusted Introducer

New challenges - “Hybrid Clouds”



Peso en Decisión sobre CSP



**Preocupación
máxima**

**Nuevos aspectos estudiados son menos
relevantes**

Ecosystem of tools



Ecosystem of tools



Nfsen + Cymru “power” -> Flow Sonar

[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)

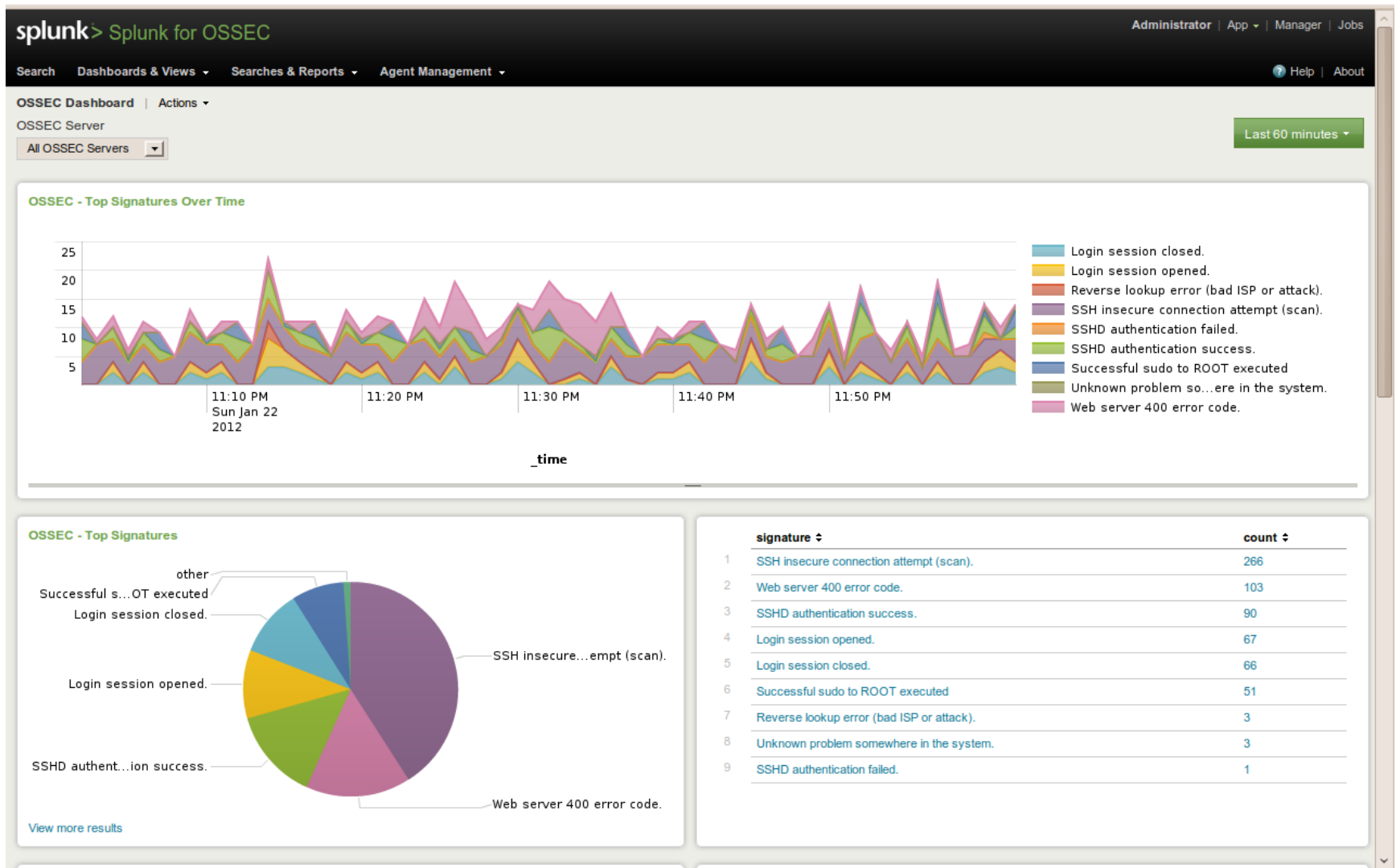
timestamp	icmp flows	icmp % diff	tcp flows	tcp % diff	udp flows	udp % diff
2013-03-12 15:50:00	259	104.44%	113442	101.88%	13230	103.77%
2013-03-12 15:45:00	248	94.3%	111350	98.76%	12749	89.54%
2013-03-12 15:40:00	263	98.13%	112743	99.73%	14238	93.83%
2013-03-12 15:35:00	268	96.4%	113050	104%	15174	109.19%
2013-03-12 15:30:00	278	94.88%	108700	99.34%	13897	100.88%
2013-03-12 15:25:00	293	110.15%	109419	99.01%	13776	108.01%

Latest Flow Alerts

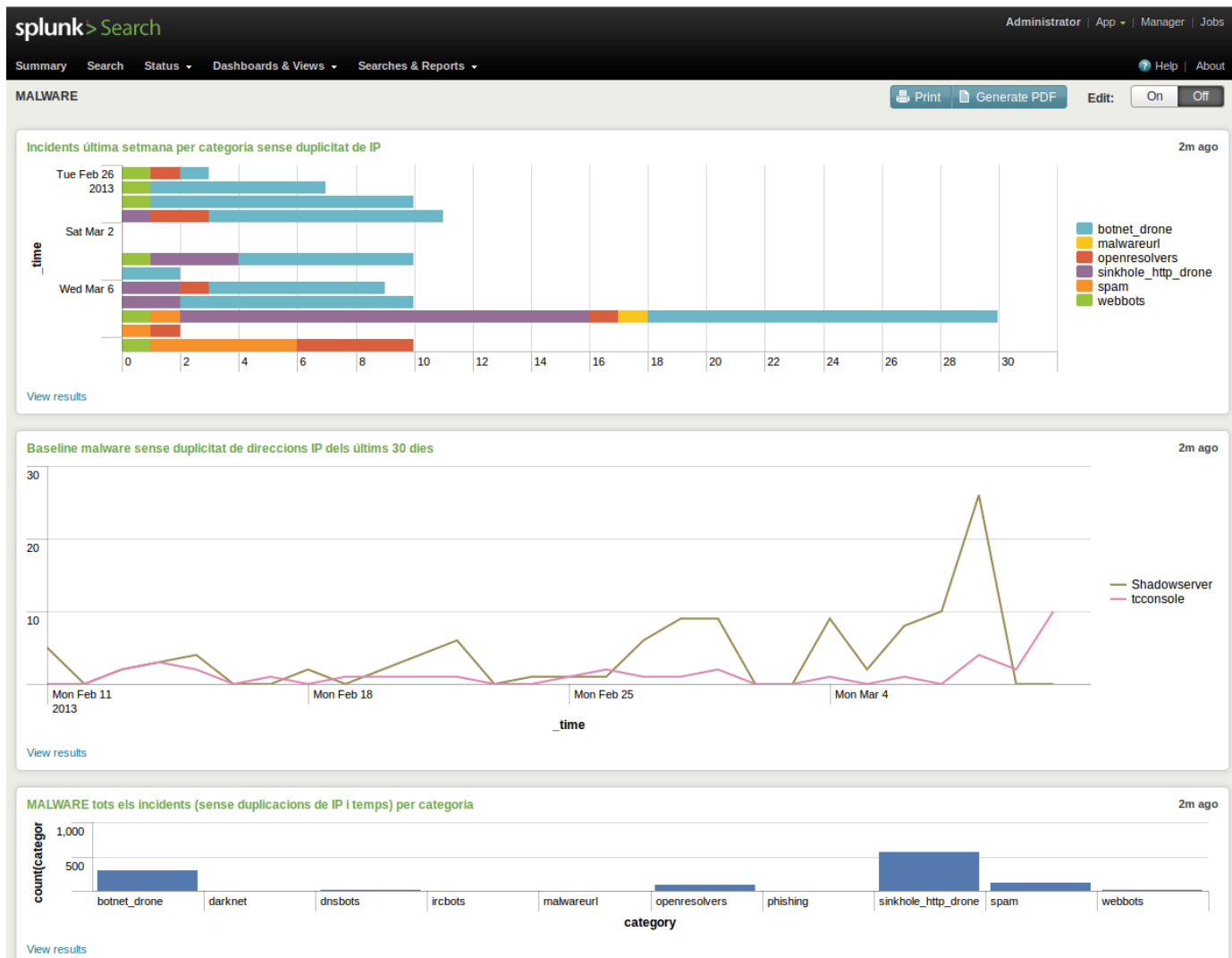
timestamp	count	src ip	src port	dst ip	dst port	protocol	alert source	type
2013-03-12 15:49:37	26		3303		57828	6	ip reputation	botnetcc
2013-03-12 15:49:21	19		57815		3303	6	ip reputation	botnetcc
2013-03-12 15:49:08	2		80		3193	6	ip reputation	bot
2013-03-12 15:28:42	1		63871		54449	6	ip reputation	bot
2013-03-12 15:19:56	1		80		60435	6	ip reputation	proxy
2013-03-12 15:15:52	1		50500		80	6	ip reputation	proxy
2013-03-12 14:59:11	1		3212		135	6	ip reputation	bot
2013-03-12 14:47:26	1		80		4584	6	ip reputation	bot
2013-03-12 14:38:43	1		80		49177	6	ip reputation	bot
2013-03-12 14:38:40	1		49177		80	6	ip reputation	bot
2013-03-12 14:36:41	1		2284		80	6	ip reputation	bot
2013-03-12 14:33:08	1		80		61564	6	ip reputation	proxy
2013-03-12 14:07:27	1		80		47256	6	ip reputation	bot

nfsen 1.3.2

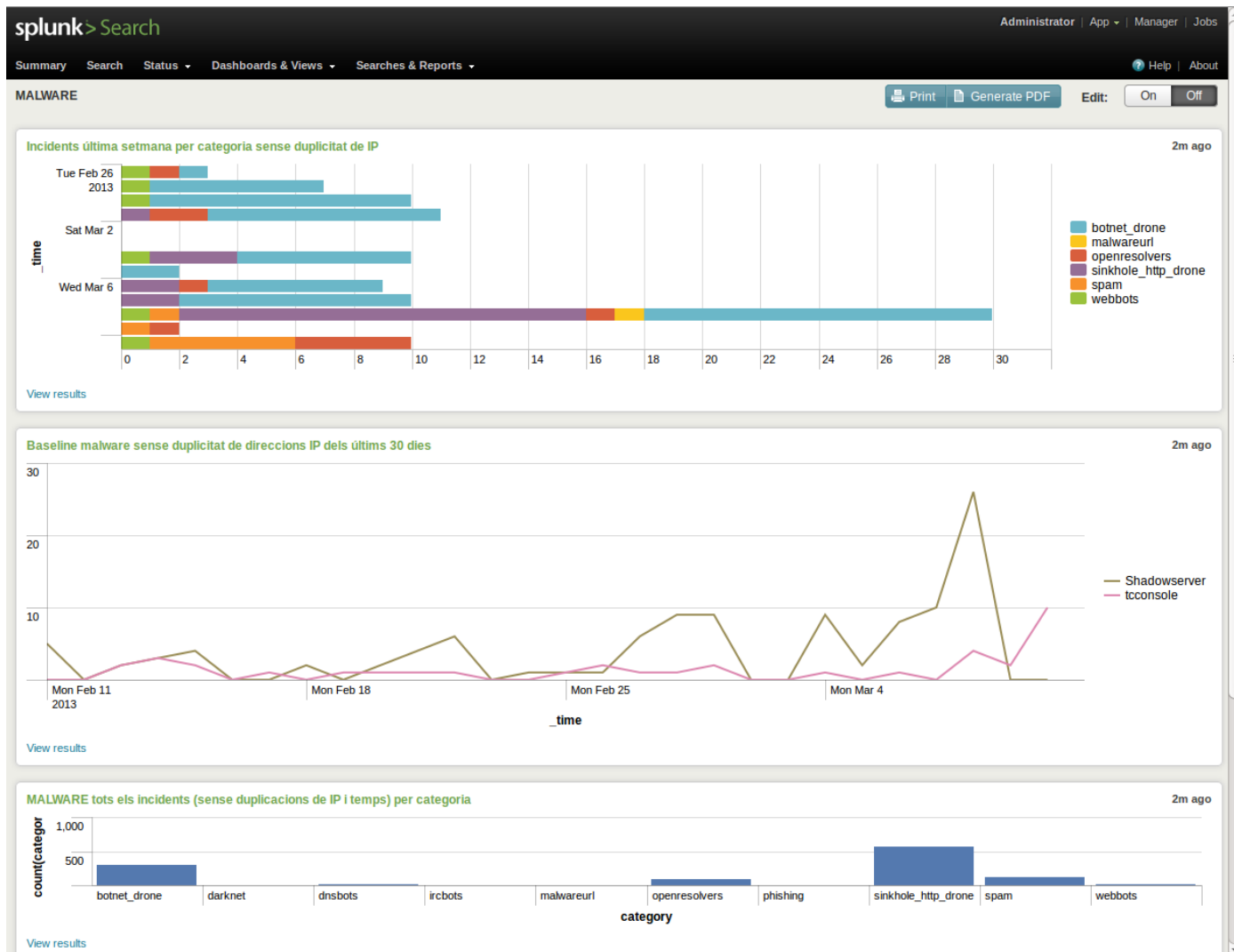
Logs correlation



External feeds placed together



External feeds placed together



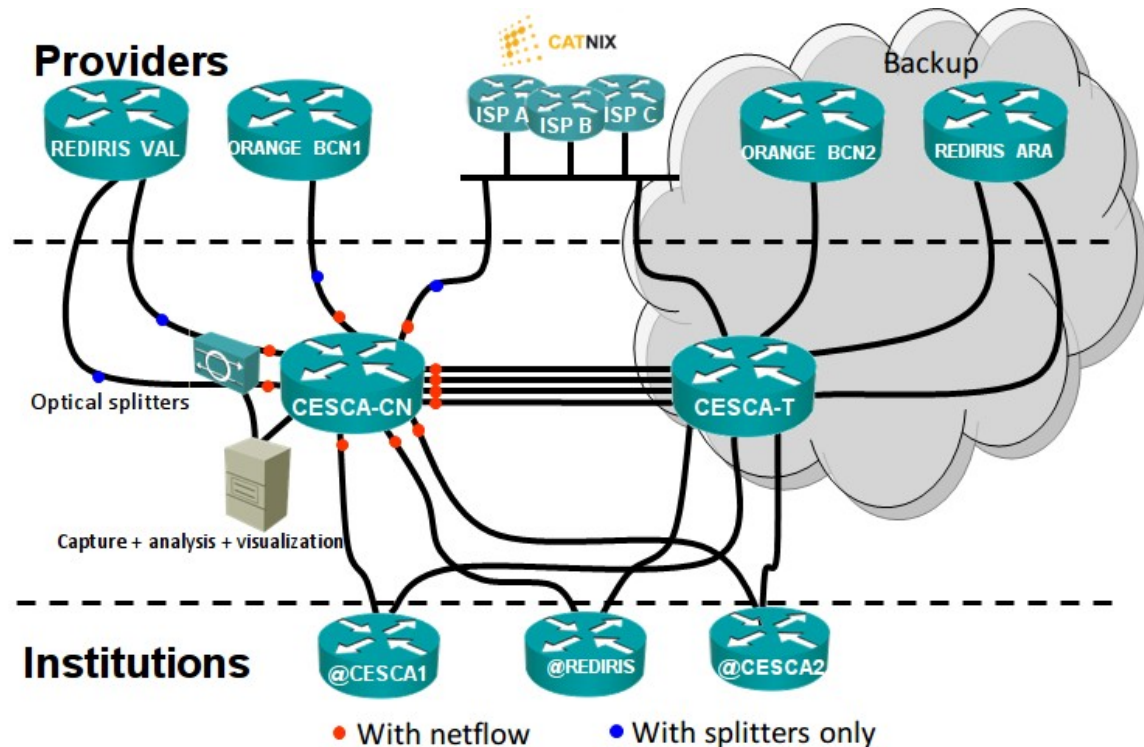
SmartxAC Platform

- ✓ SMARTxAC: Traffic Monitoring and Analysis System for Anella Científica (“Sistema de Monitoratge i Anàlisi de TRàfic per l’ Anella Científica”)
- ✓ Main objectives
 - Low-cost platform
 - Continuous monitoring of high-speed links without packet loss
 - Detection of network anomalies and irregular usage
 - Multi-user system: Network operators and Institutions

SMARTxAC is the collaboration between UPC BarcelonaTech (CCABA) and CSUC



Architecture



- ✓ The splitters are still used for the **Deep Packet Inspection (DPI)**
- ✓ All the internal and external interfaces are measured
- ✓ Offline analysis with DPI patterns, based on **Machine Learning** techniques.

Apps detection



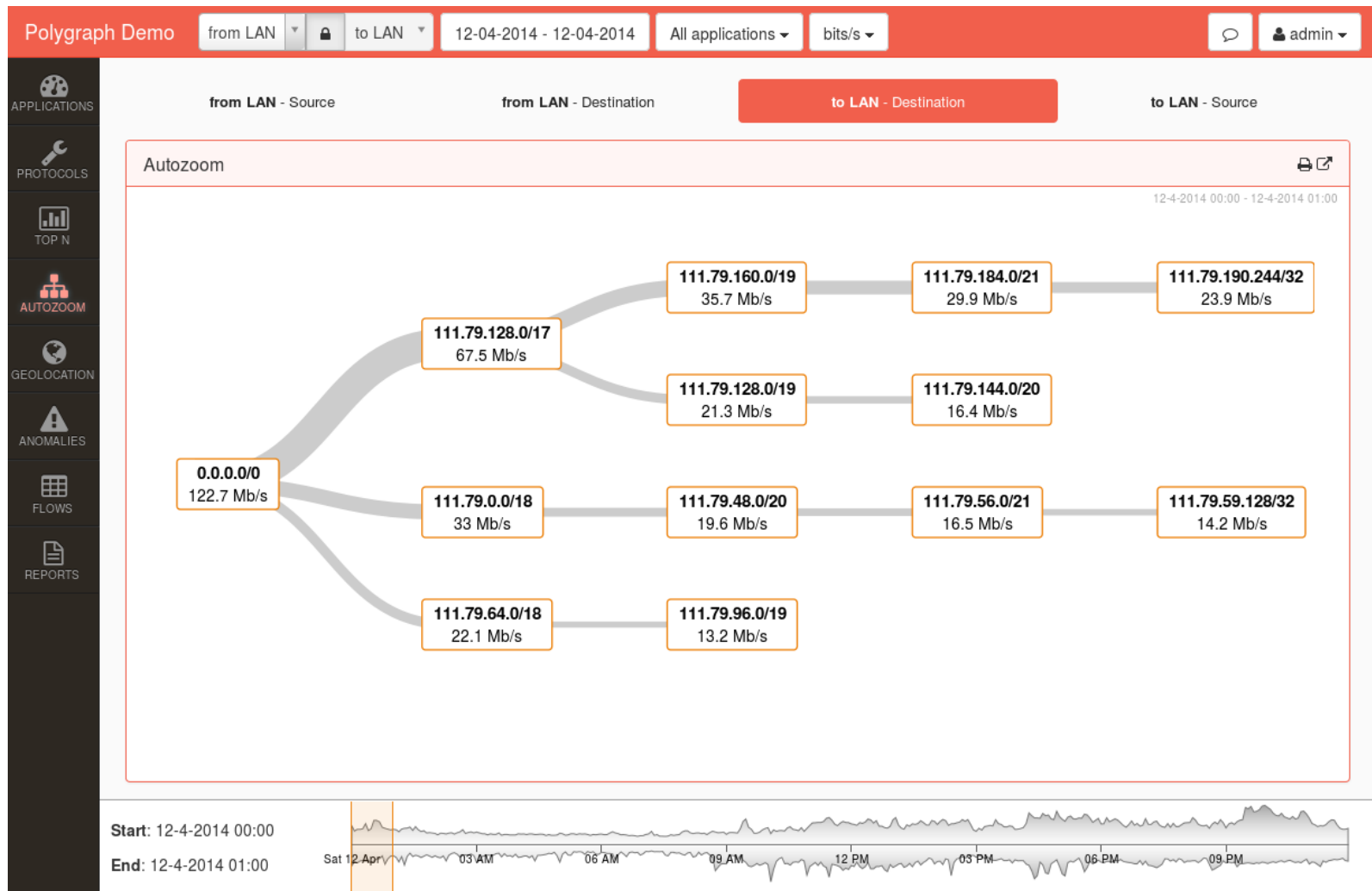
Apps Classification



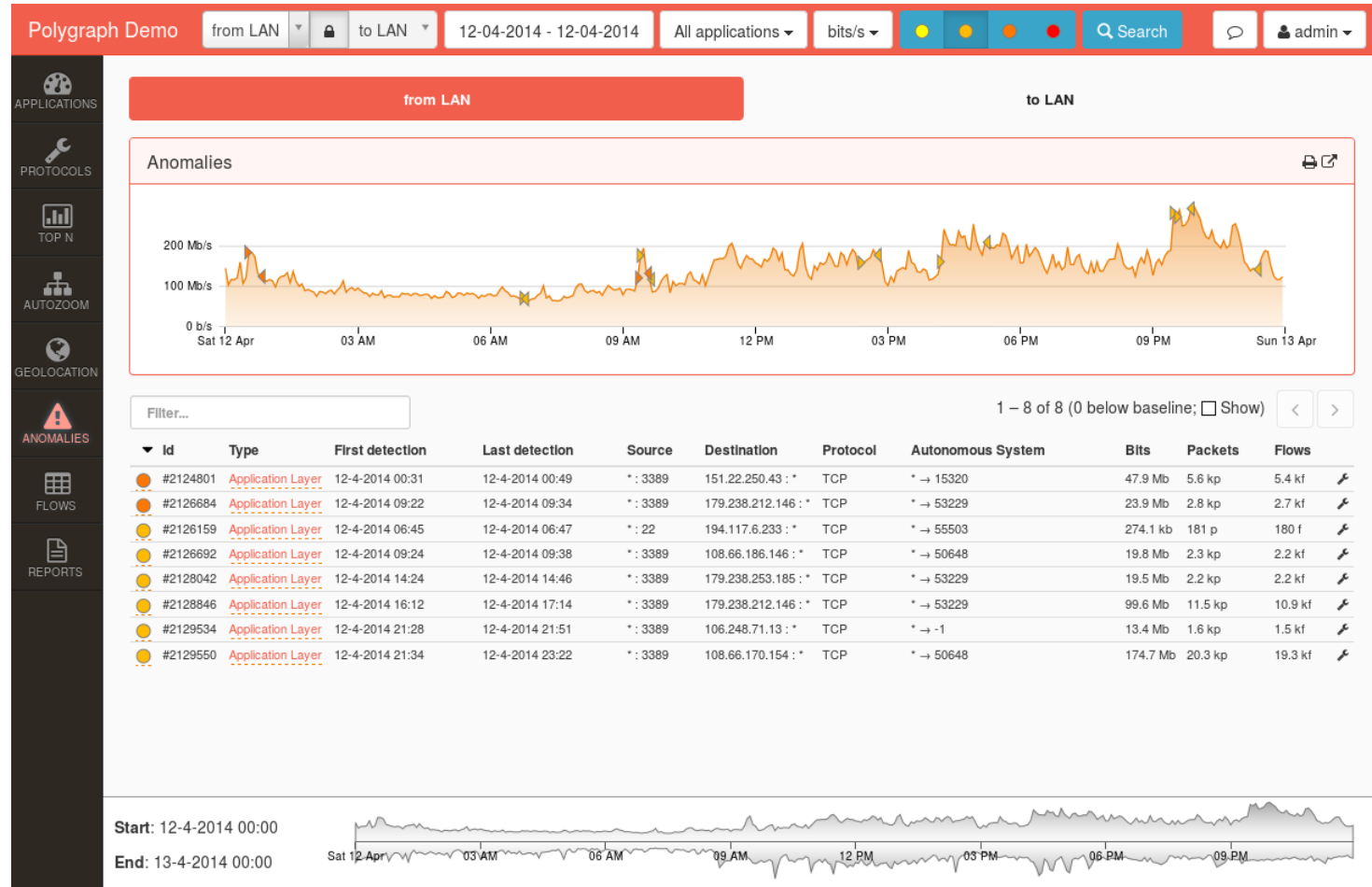
Top N



Autozoom



Security anomalies detection



Flows search

Polygraph Demofrom LANto LAN12-04-2014 - 12-04-2014All applicationsbits/sSearch

Search flowsInterval: 12-4-2014 00:00 - 13-4-2014 00:00Views: from LANApplication: All applications

Retrieved more than 1000 flows from 2,017,325 in 1.653 secondsDownload (1000 flows)

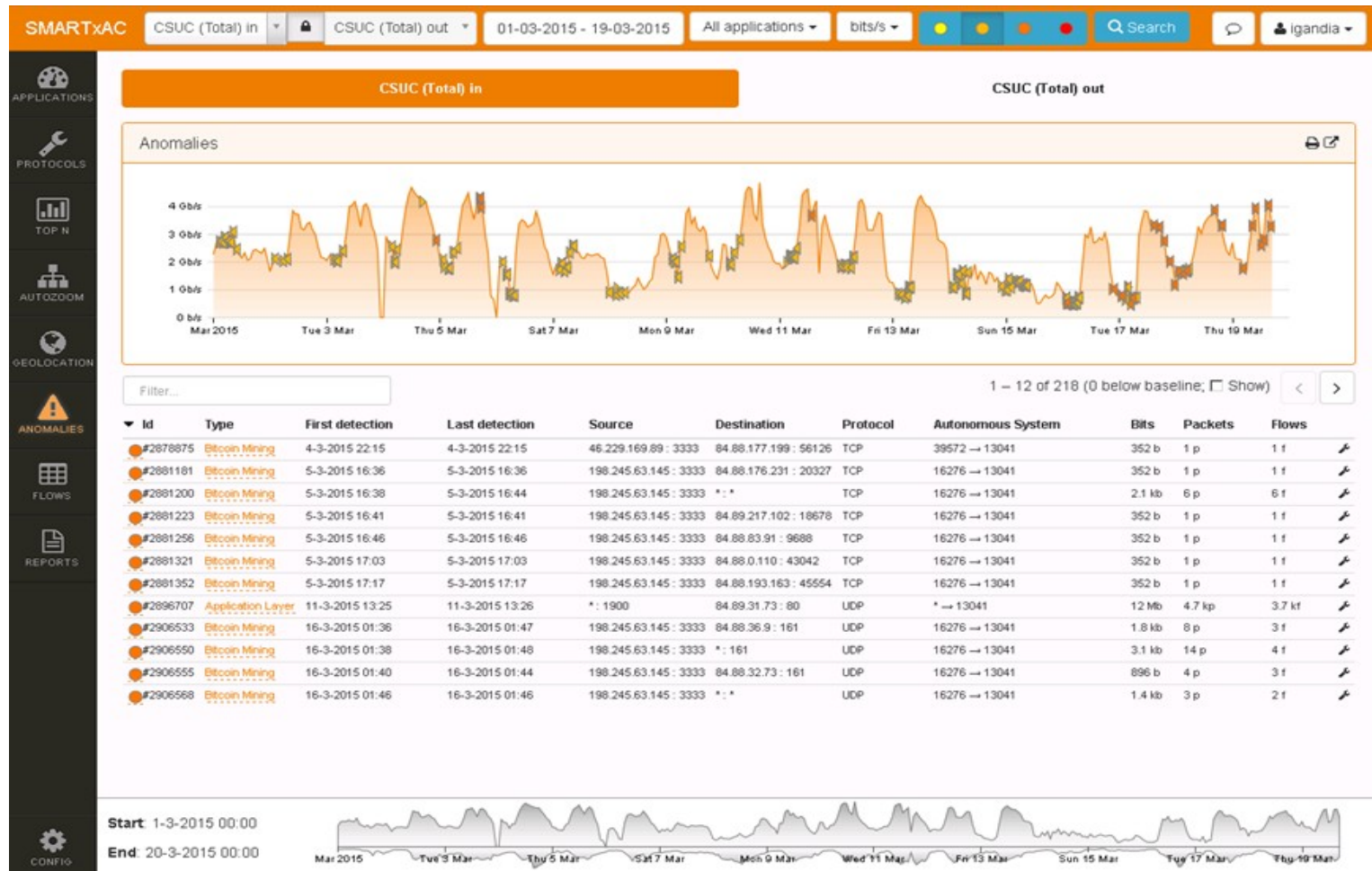
Filter...11 – 20 of 1,000

Start	End	Src Addr	S. Port	Dst Addr	D. Port	Protocol	Src ASN	Dst ASN	Bytes	Packets	Flags	Application	Exporter
2014-4-11 23:59:14.279	2014-4-12 00:00:11.720	111.79.9.113	6970	157.22.230.111	2726	UDP	197518	53064	8.3 Mb	6 kp	_____	BitTorrent	84.8.215.18
2014-4-11 23:59:16.625	2014-4-12 00:00:13.056	111.79.190.244	8338	116.28.166.133	10537	UDP	197518	13697	1.1 Mb	6 kp	_____	Skype	84.8.215.18
2014-4-11 23:59:17.466	2014-4-12 00:00:24.920	111.79.132.156	15243	148.244.7.118	46795	UDP	197518	4719	532.8 kb	3.6 kp	_____	Skype	84.8.215.18
2014-4-11 23:59:19.865	2014-4-12 00:00:24.911	111.79.40.17	5060	67.149.223.58	5528	UDP	197518	17061	3.7 Mb	7.2 kp	_____	BitTorrent	84.8.215.18
2014-4-11 23:59:19.888	2014-4-12 00:00:29.762	111.79.59.128	58322	9.150.252.133	443	TCP	197518	30407	374.4 kb	7.2 kp	___A_	SSL	84.8.215.18
2014-4-11 23:59:20.030	2014-4-12 00:00:26.282	111.79.190.244	51584	170.11.37.254	20247	TCP	197518	51656	7.2 Mb	4.8 kp	___A_	BitTorrent	84.8.215.18
2014-4-11 23:59:20.421	2014-4-12 00:00:08.917	111.79.55.227	80	154.57.64.72	63767	TCP	197518	21753	10.8 Mb	7.2 kp	___A_	HTTP	84.8.215.18
2014-4-11 23:59:21.332	2014-4-12 00:00:24.401	111.79.97.107	0	1.99.213.80	0	ICMP	197518	42988	124.8 kb	2.4 kp	_____	ICMP	84.8.215.18
2014-4-11 23:59:21.834	2014-4-12 00:00:03.345	111.79.27.65	63010	157.31.207.93	60176	UDP	197518	53064	499.2 kb	2.4 kp	_____	Skype	84.8.215.18
2014-4-11 23:59:26.213	2014-4-12 00:00:09.286	111.79.132.156	15243	143.189.158.171	4172	UDP	197518	53064	680.4 kb	4.8 kp	_____	Skype	84.8.215.18

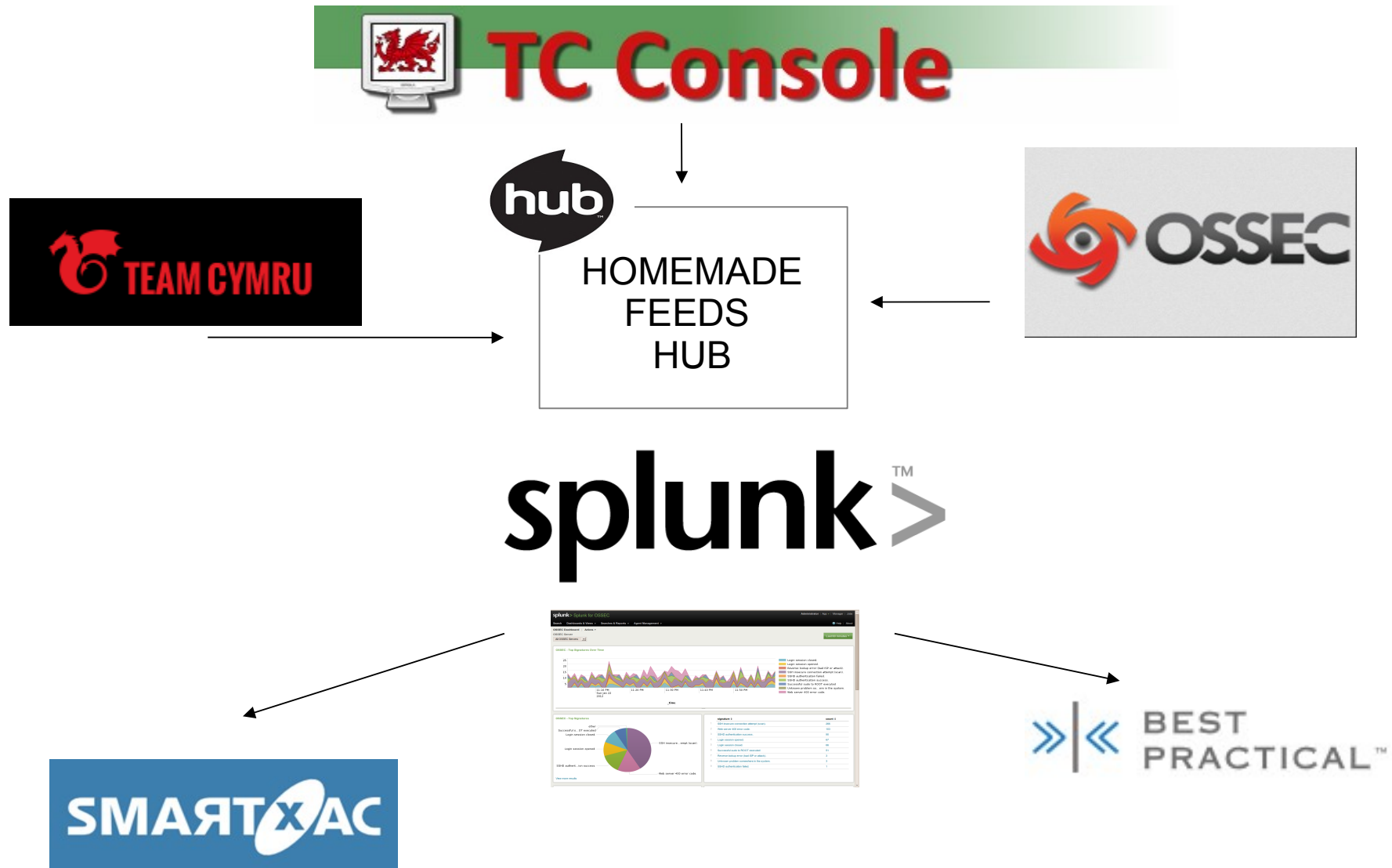
Start: 12-4-2014 00:00End: 13-4-2014 00:00

Sat 12 Apr 03 AM06 AM09 AM12 PM03 PM06 PM09 PM

Eyes for our constituency



Proactive monitoring workflow and tools



Close to University (be viral!)



Master in Security Technologies



Near Future

- ✓ **New Audit Services**
- ✓ RT → RTIR
- ✓ More focus to DNS
- ✓ DDOS 'headache'



And continuously listening the
NET ;-)

Q & A time

Dziękuję!
Thanks!
Gracias!
Gràcies!

jordi.guijarro@csuc.cat
CSUC-CSIRT (eriac@csuc.cat)

Note: ERI -> CSIRT in Catalan

