Telefonica IWS CSIRT

Once upon a time…

March 10th, 2011

Telefonica International Wholesale Services
Computer Security Incidence Response Team
Telefonica Research & Development

Telefonica

Once upon a time
… who we are

Coo1

About TIWS CSIRT

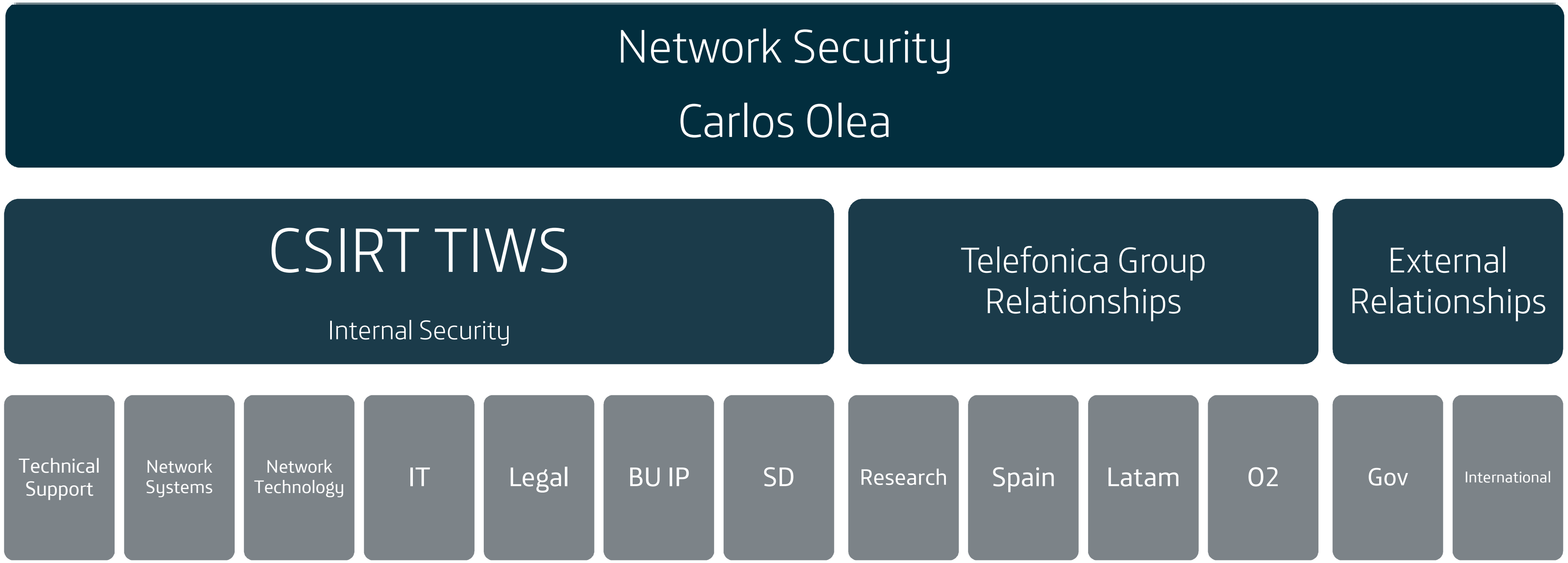
Telefonica

Carlos Olea Ortigosa
Network Area
Distrito C West 1 Building, Floor 3
carlos.olea@telefonica.com
PGP ID : 0xEEA859E0

Telefonica International Wholesale Services
Multinational Projects
Ronda de la Comunicacion s/n, 28050 Madrid, Spain
Fixed +34 914 830 061 | Cell +34 609 961 854
PGP FingerPrint : 32CD 1D58 955E 5613 8E89 9A36 0959 11EE 348E 431C

Telefonica

Santiago Rouco
CISSP
Telefonica R&D
Phone: +34913128782
Cell: +34606545061
srouco@tid.es
PGP-ID: F6C95D33
Fingerprint: 5158 272D 33C9 B998 63E8 4C51 6CA5 E5DF F6C0 5D33



Network Security

Carlos Olea

CSIRT TIWS

Internal Security

Telefonica Group Relationships

External Relationships

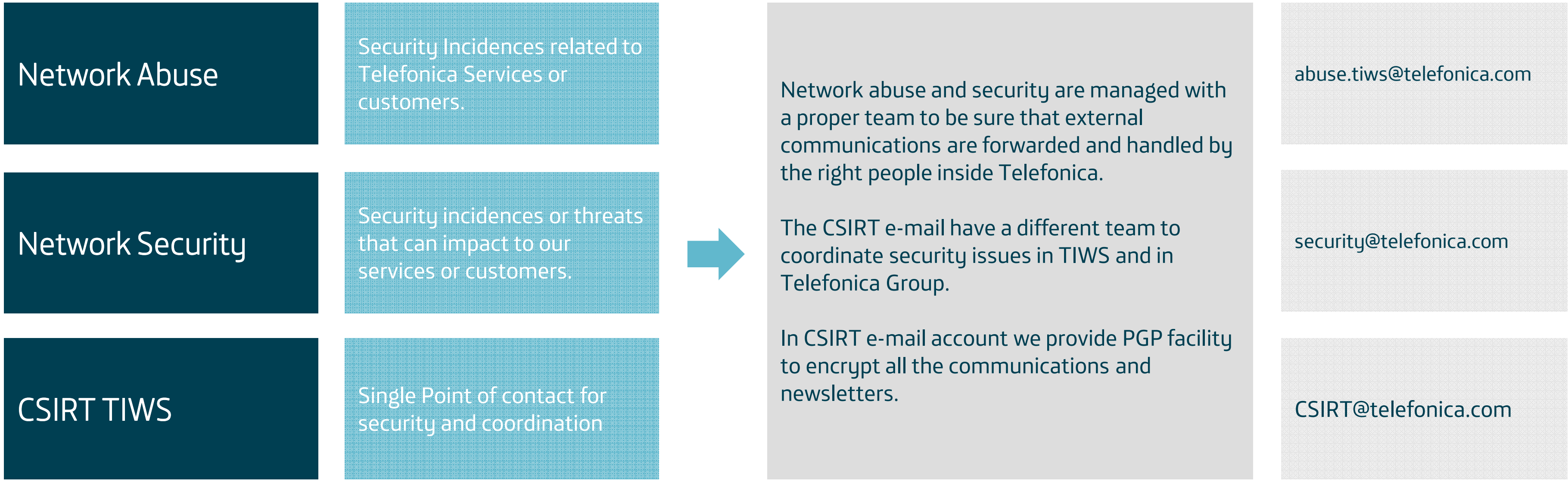
Technical Support | Network Systems | Network Technology | IT | Legal | BU IP | SD | Research | Spain | Latam | O2 | Gov | International

Diapositiva 3

Coo1 weicoo01; 28/12/2010

About TIWS CSIRT

Security Forums



Network Abuse

Security Incidences related to Telefonica Services or customers.

Network Security

Security incidences or threats that can impact to our services or customers.

CSIRT TIWS

Single Point of contact for security and coordination

Network abuse and security are managed with a proper team to be sure that external communications are forwarded and handled by the right people inside Telefonica.

The CSIRT e-mail have a different team to coordinate security issues in TIWS and in Telefonica Group.

In CSIRT e-mail account we provide PGP facility to encrypt all the communications and newsletters.

abuse.tiws@telefonica.com

security@telefonica.com

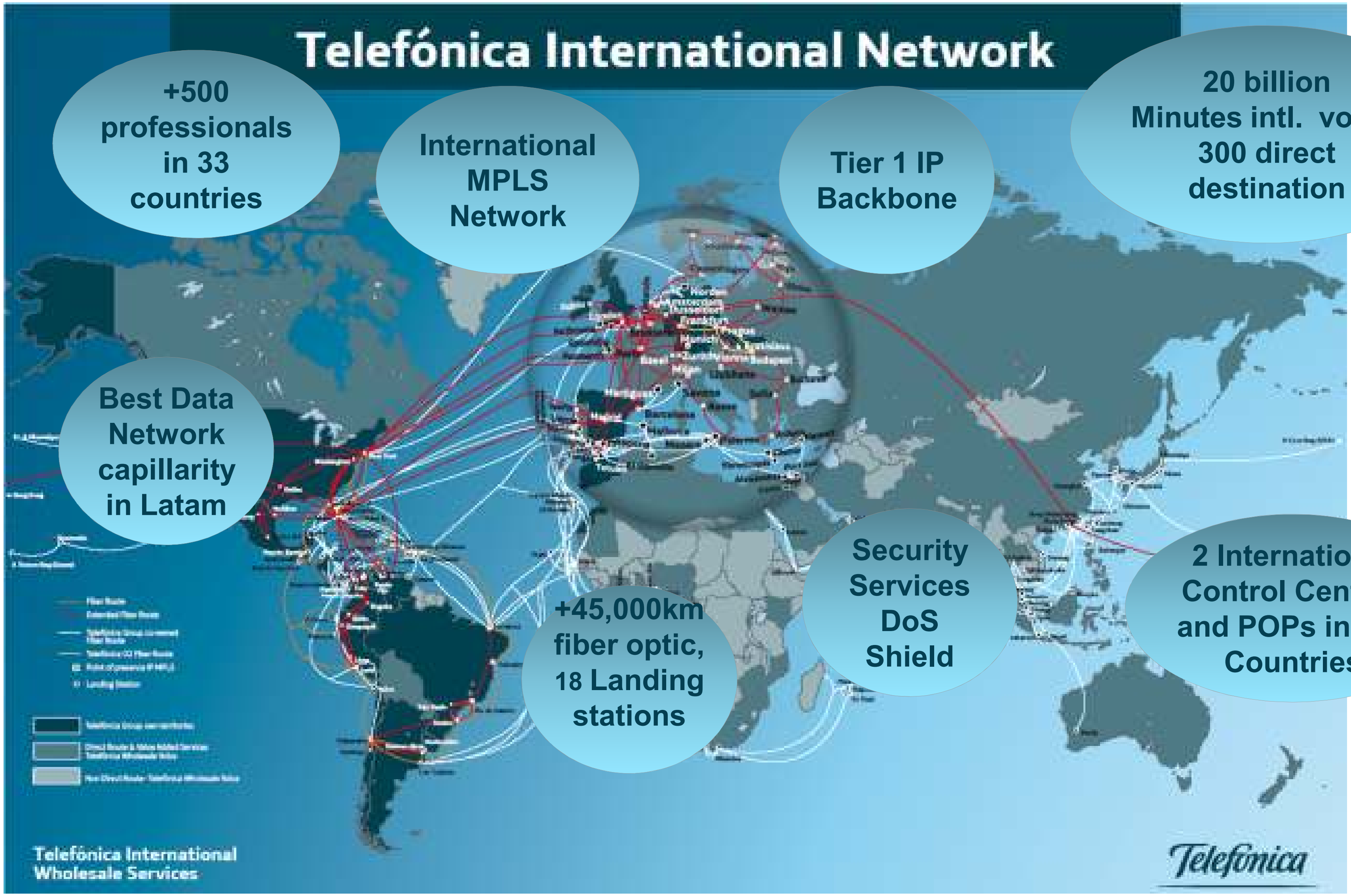
CSIRT@telefonica.com

CSIRT
Distrito C West 1 Building, 3th Floor
CSIRT@telefonica.com
PGP ID : 0xB405ED13

Telefónica Computer Security Incidence Response Team
Ronda de la Comunicación s/n, 28050 Madrid, Spain
Tel +34 914 83x xxx
PGP FingerPrint : 05E9 8A22 CA41 1341 17EA 6768 D4AB 8A99 B405 ED13

Foro ABUSES
spanish cooperation of abuse teams
APWG
Committed to Wiping Out Internet Scams and Fraud
EastWest Institute
Forging Collective Action for a Safer and Better World
enisa
European Network and Information Security Agency
FIRST
Family Online Safety Institute
etis
the global IT association for telecommunications

Telefonica Wholesale is positioned as a Tier 1 Carrier in the international arena…


Telefónica International Network
Telefónica International Wholesale Services
Telefónica

+500 professionals in 33 countries

International MPLS Network

Tier 1 IP Backbone

20 billion Minutes intl. voice, 300 direct destination

Best Data Network capillarity in Latam

+45,000km fiber optic, 18 Landing stations

Security Services DoS Shield

2 International Control Centers and POPs in +40 Countries

Telefonica is a leader in the Latin American Telco market …

Data as of December '09

● Wireline market rank
● Mobile market rank

Wireline market rank	Mobile market rank	
1	2	***Argentina**: 21.9 million*
2	1	***Brazil**: 67.0 million*
	2	***Central America**: 6.3 million*
1	2	***Colombia**: 11.2 million*
1	1	***Chile**: 10.7 million*
	2	***Ecuador**: 3.8 million*
	2	***Mexico**: 17.7 million*
1	1	***Peru**: 15.9 million*
	1	***Uruguay**: 1.6 million*
	2	***Venezuela**: 11.8 million*

movistar

+ vivo Conexão como nenhuma outra.

Total Accesses

168.6 million

Notes:
- Central America includes Guatemala, Panama, El Salvador and Nicaragua
- Total accesses figure includes Narrowband Internet accesses of Terra Brasil and Terra Colombia, and Broadband Internet accesses of Terra Brasil, Telefónica de Argentina, Terra Guatemala and Terra México.

… enjoys a significant footprint in Europe …

Data as of December '09

● Wireline market rank
● Mobile market rank

1	1	***Spain:*** 46.8 million
	1	***UK:*** 21.9 million
	4	***Germany***: 17.1 million
	2	***Ireland***: 1.7 million
1	2	***Czech Republic***: 7.8 million
	3	***Slovakia***: 0.6 million

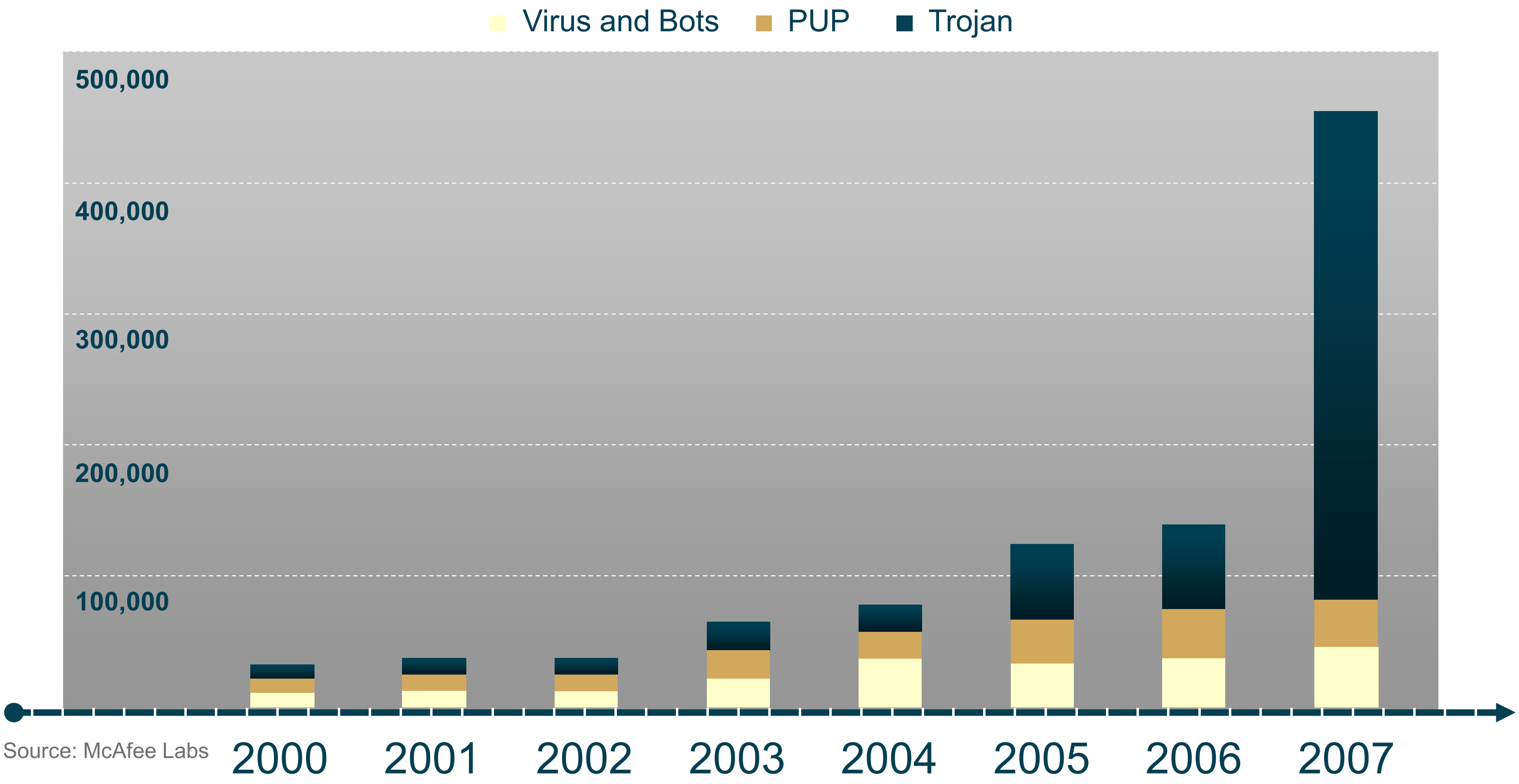
Total Accesses

96.0 million

External Activities:
... just to clarify the threat picture

External Activities

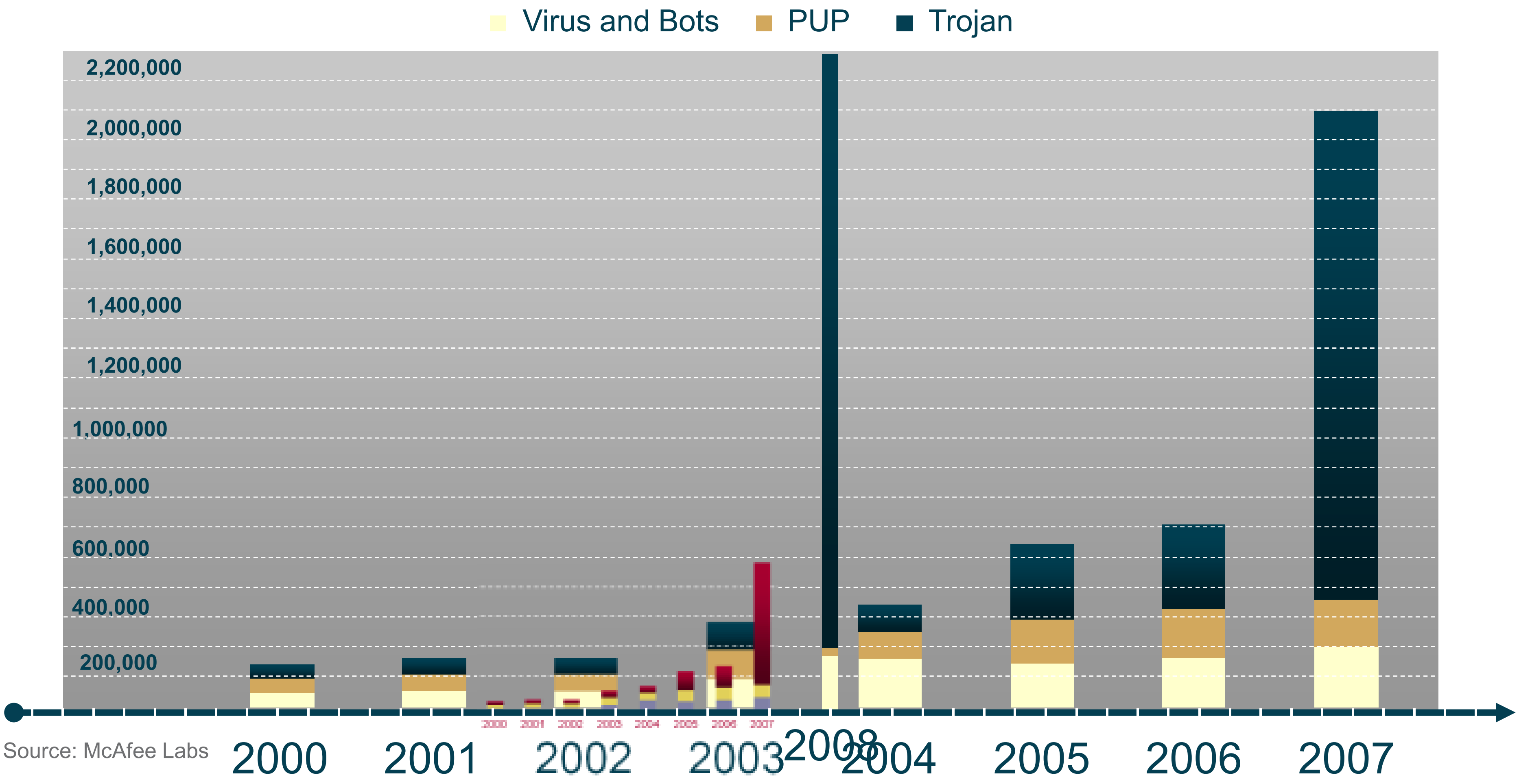
Some yearly figures I



Source: McAfee Labs

External Activities

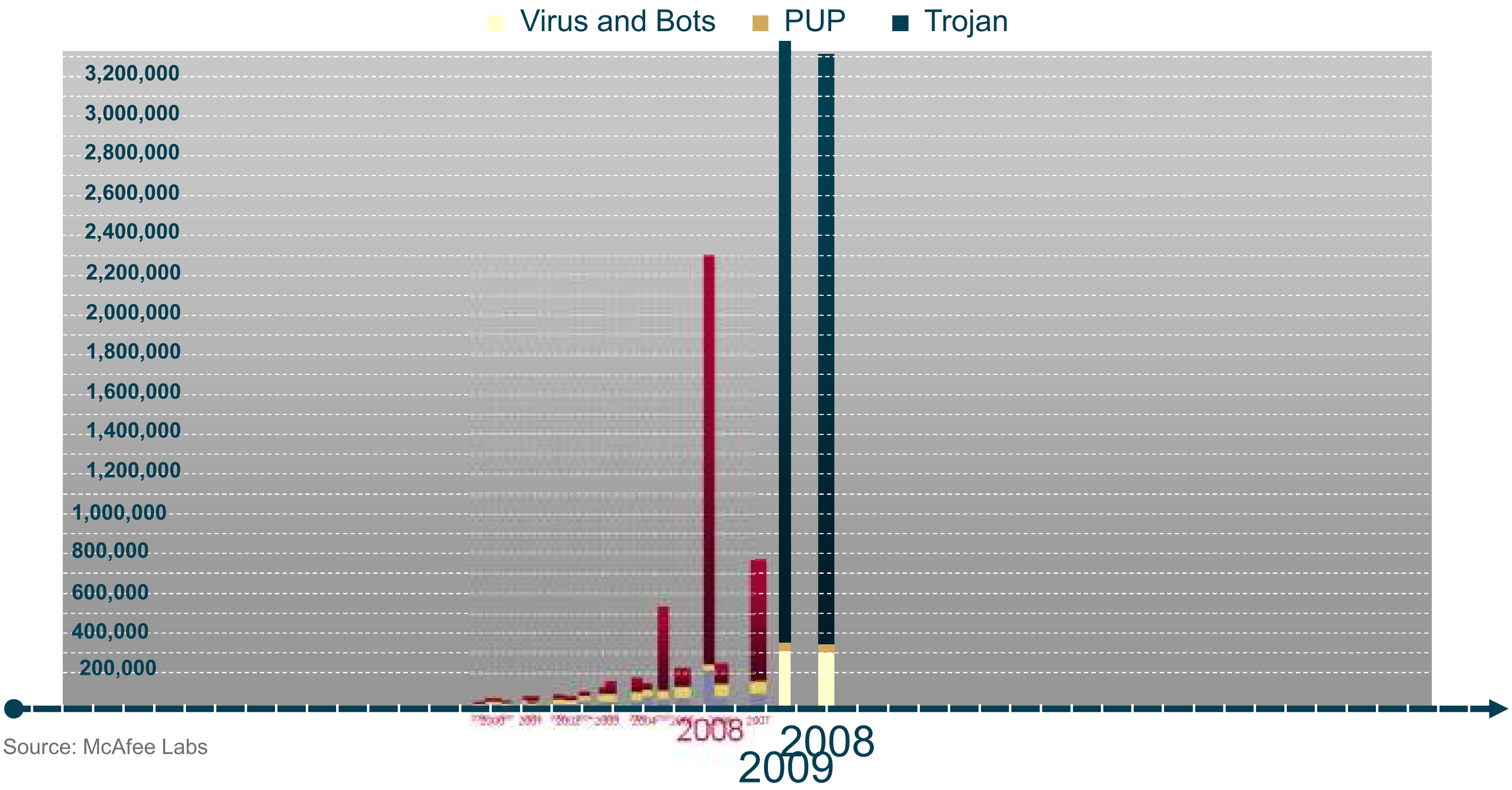
Some yearly figures II



Source: McAfee Labs

External Activities

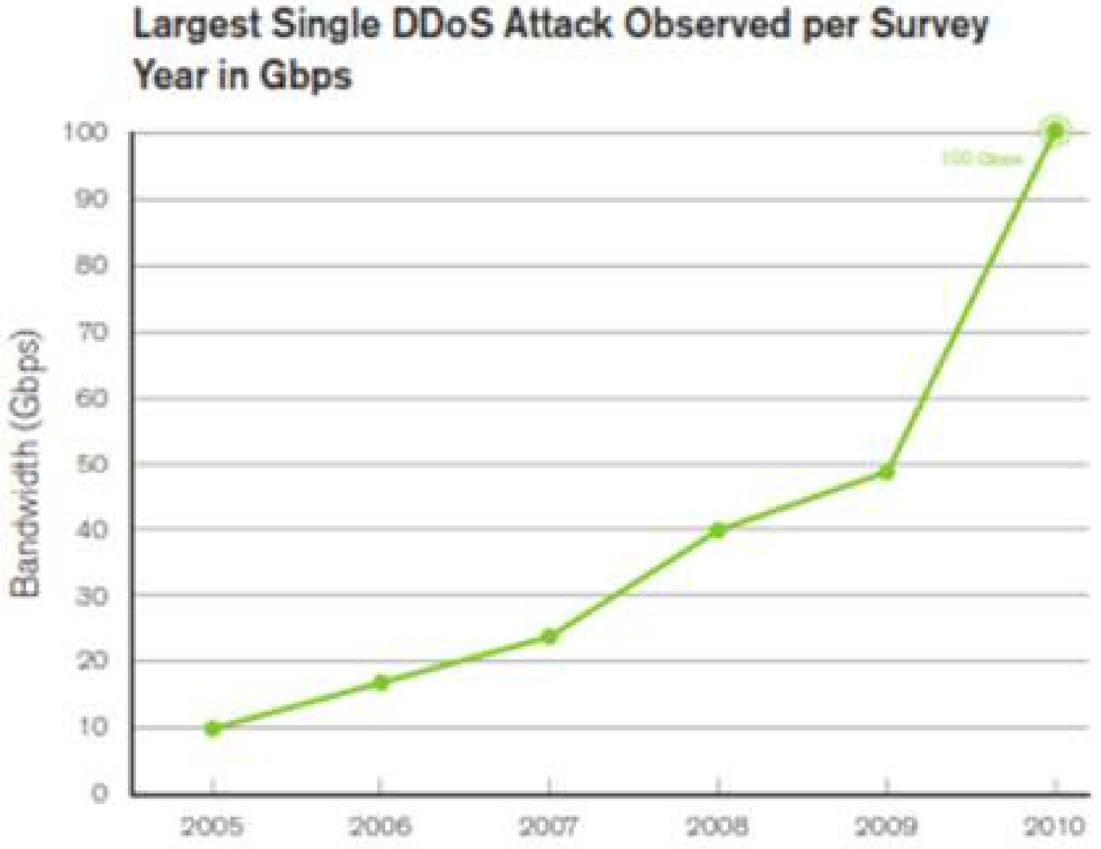
Some yearly figures III



Source: McAfee Labs

External Activities

Sometimes size matters



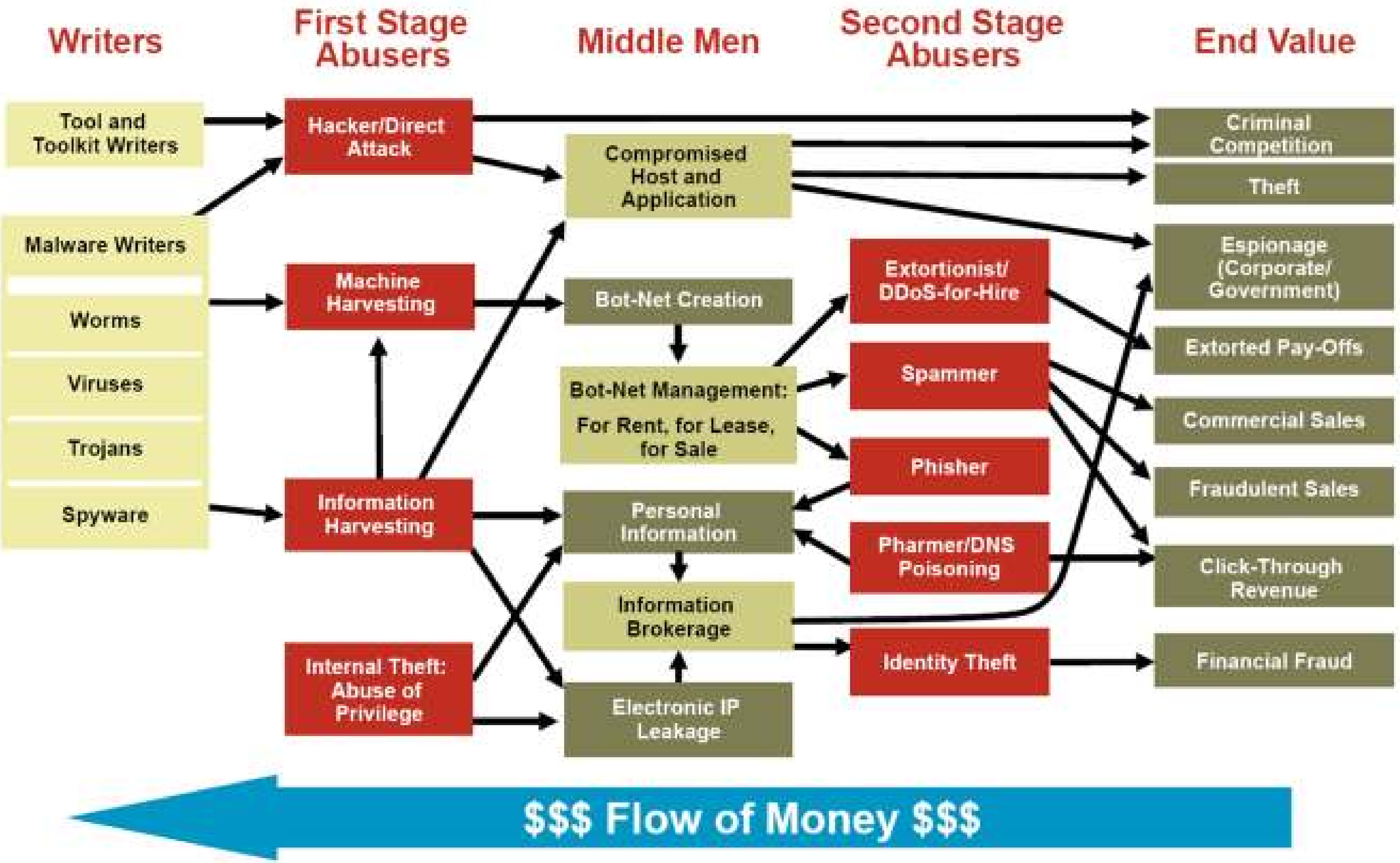
Largest Single DDoS Attack Observed per Survey Year in Gbps

Figure 1

Source: Arbor Networks, Inc.

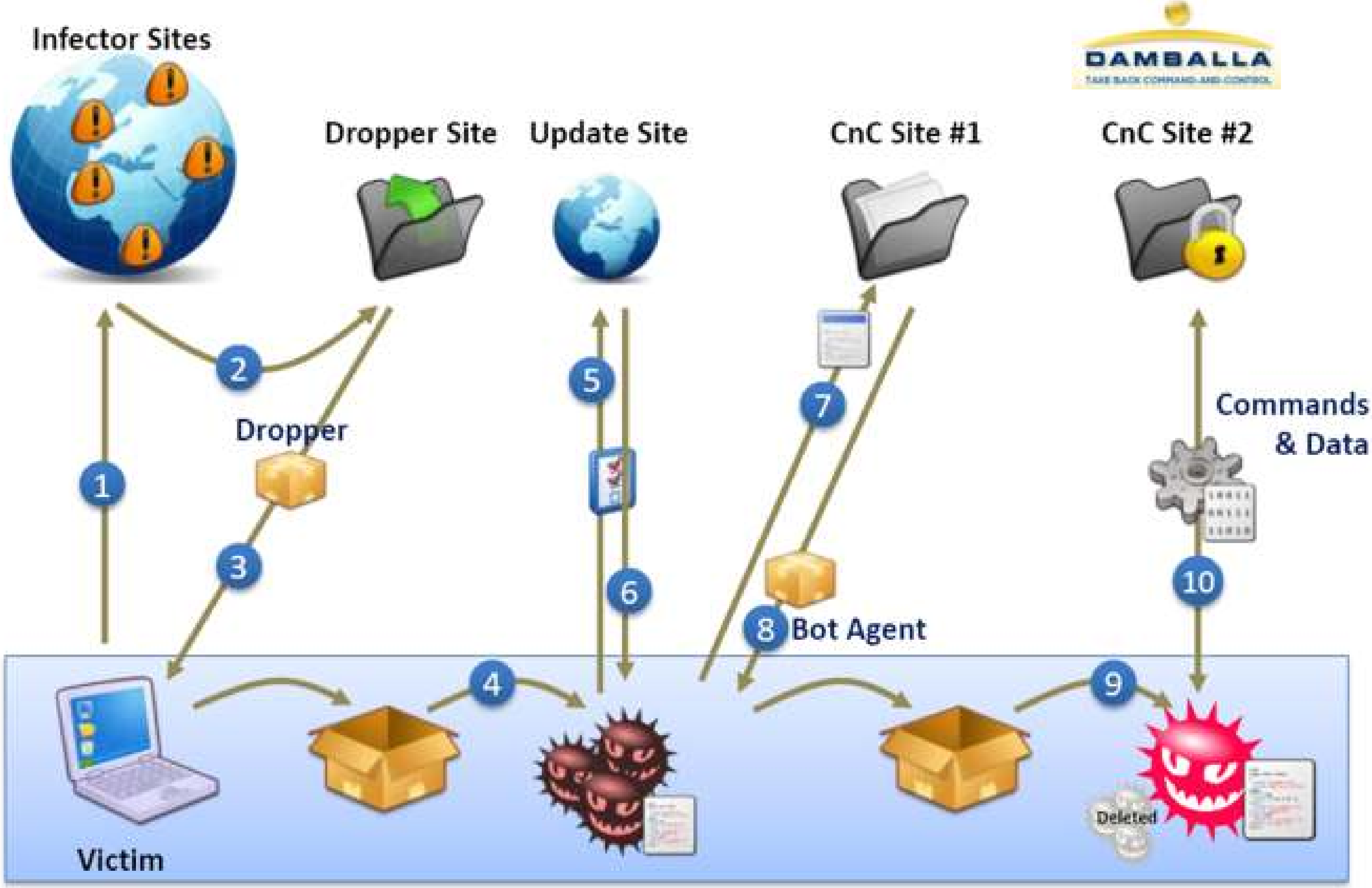
Make Money using our networks

Activities impacting our services and customers



The challenge talking about Botnets

Malware Infection Cycle, the untouchables

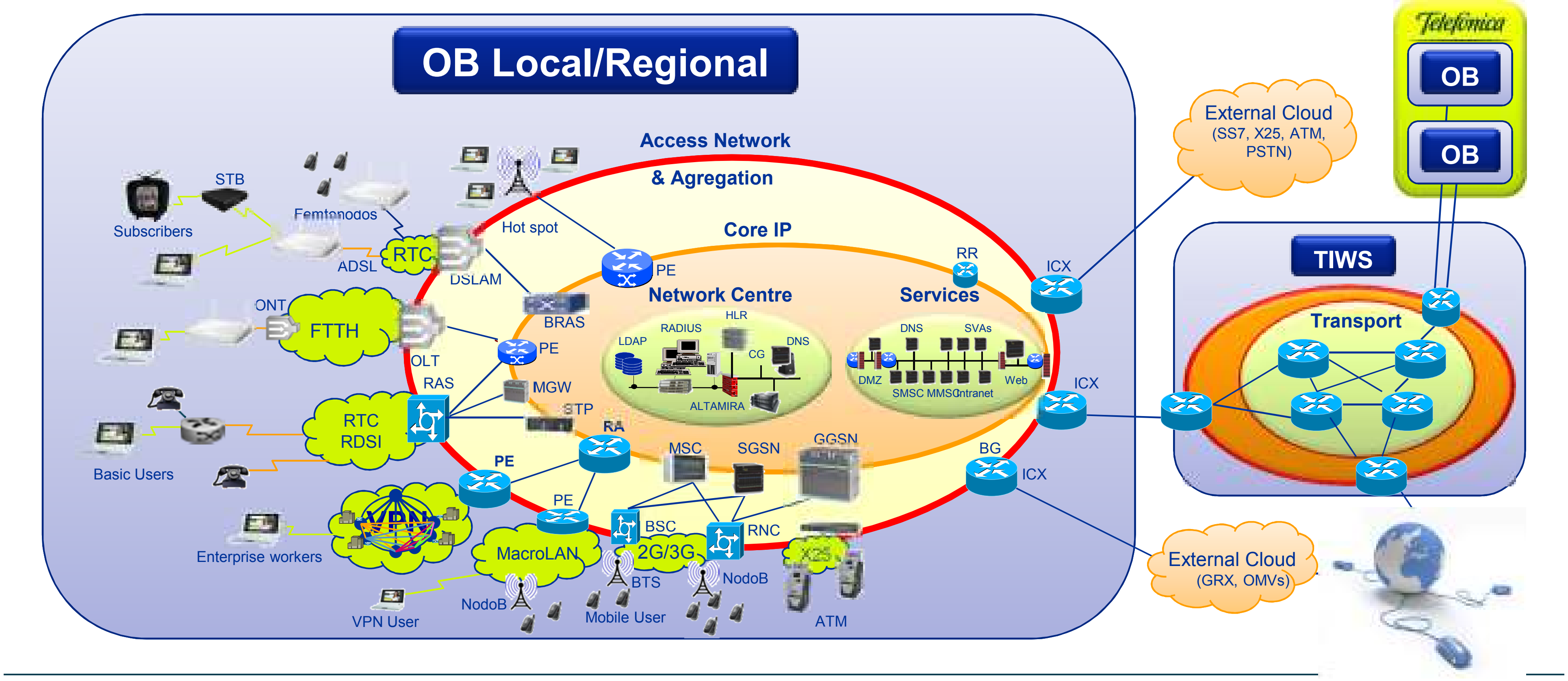


Local Activities
... just to clarify the Business

Domestic Services country basis

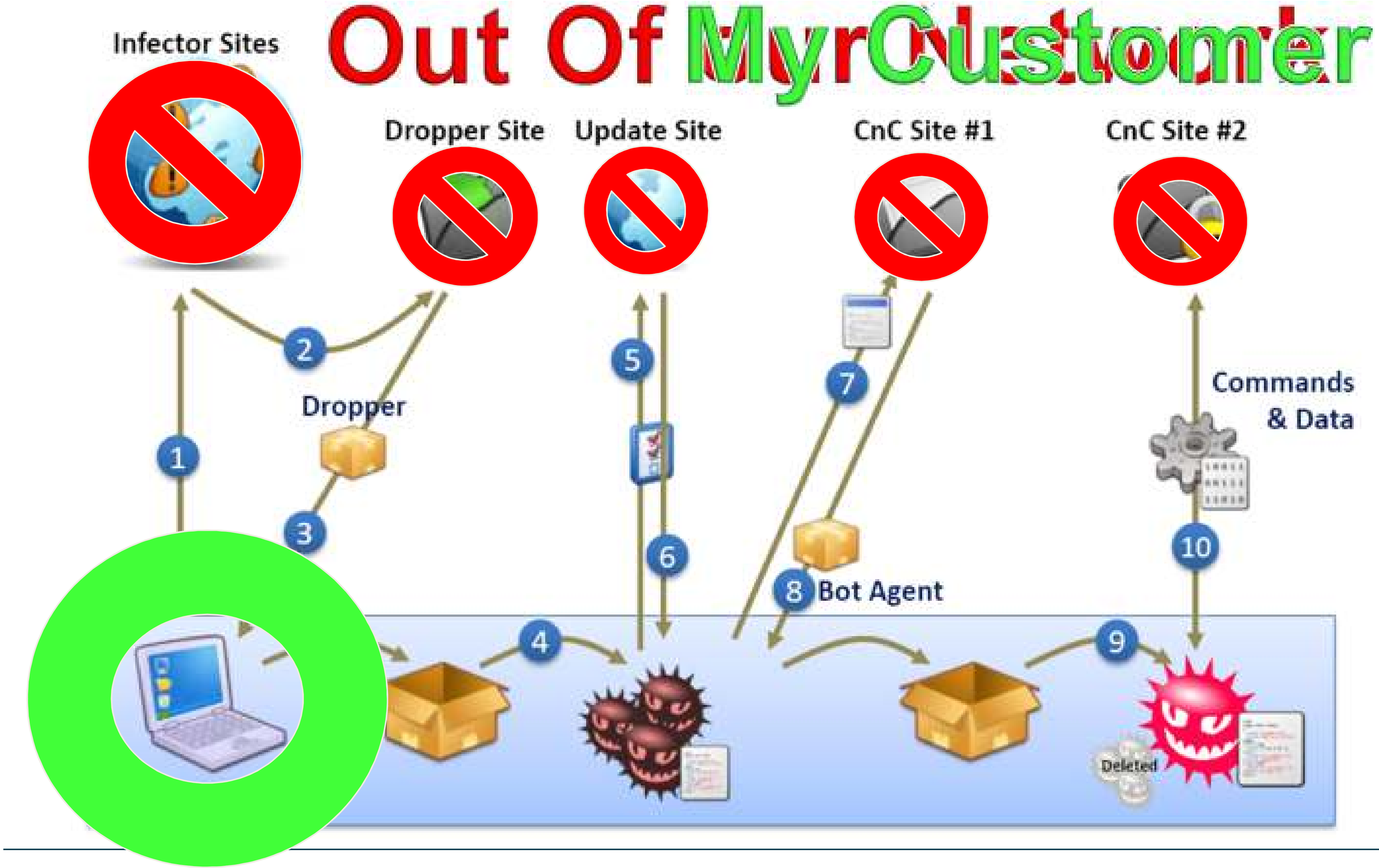
- How much money and time do you need?
- We are still fighting or resolving the root cause?
- All the problems are in your network / services?
- Who are the target for customer claims?

Spam	3.709.114
Fraud	1.604
Virus	1581
Insults, abuses	232
Hacking	20.047
Copyright violations	2.011.998



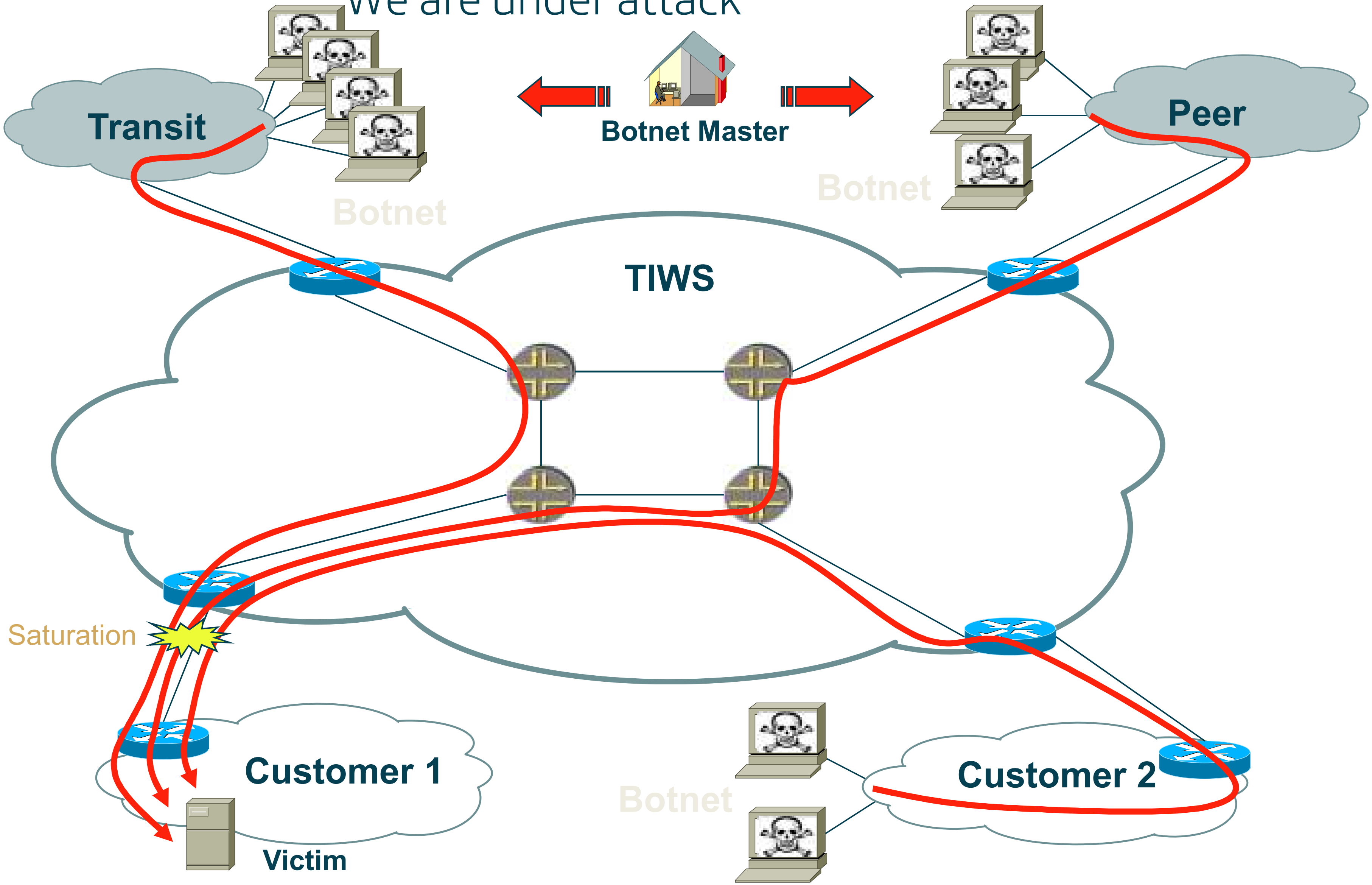
Welcome back to the Botnets

Malware Infection Cycle, the untouchables



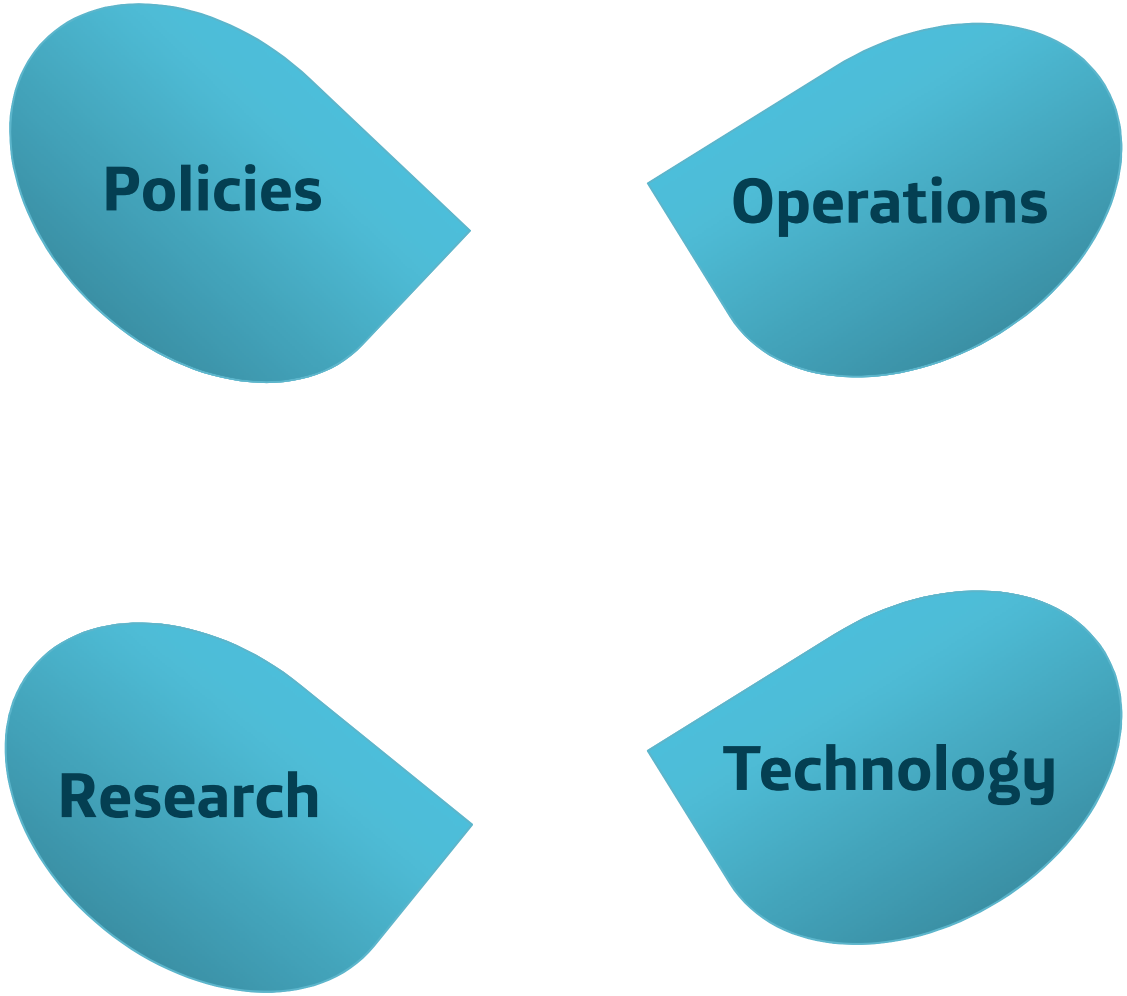
DDoS, Spam, Phising, Farming

We are under attack



What initiatives?

… Let's take a look at the framework



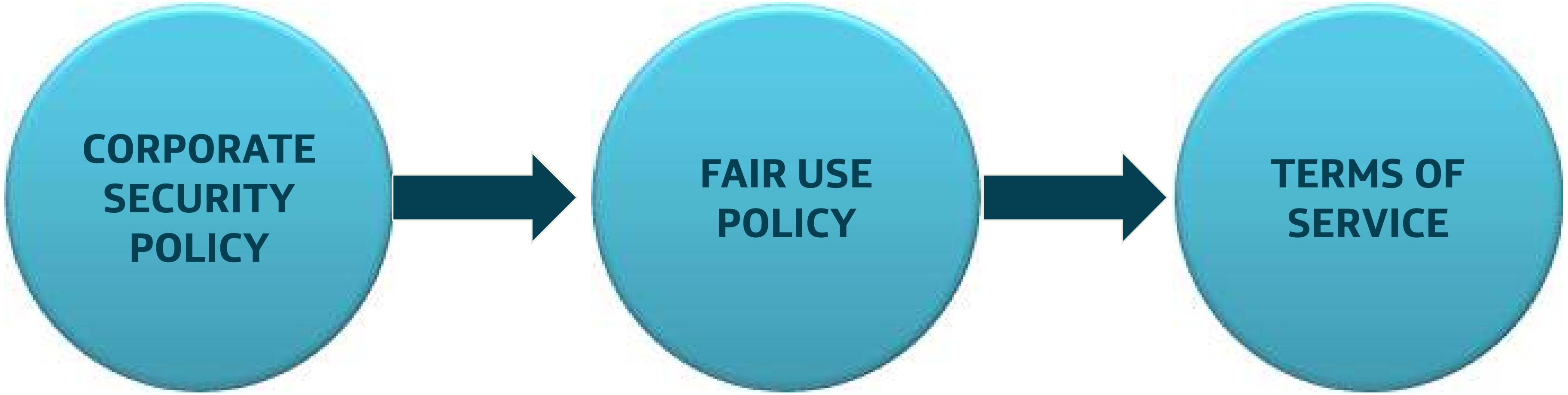
Policies

Operations

Research

Technology

Policies



CORPORATE SECURITY POLICY

FAIR USE POLICY

TERMS OF SERVICE

Illegal Activities

□Child Pornography
□Spam
□Fraud
□Intellectual Property Rights
□Hacking and similar activities
□Service disruption
•...

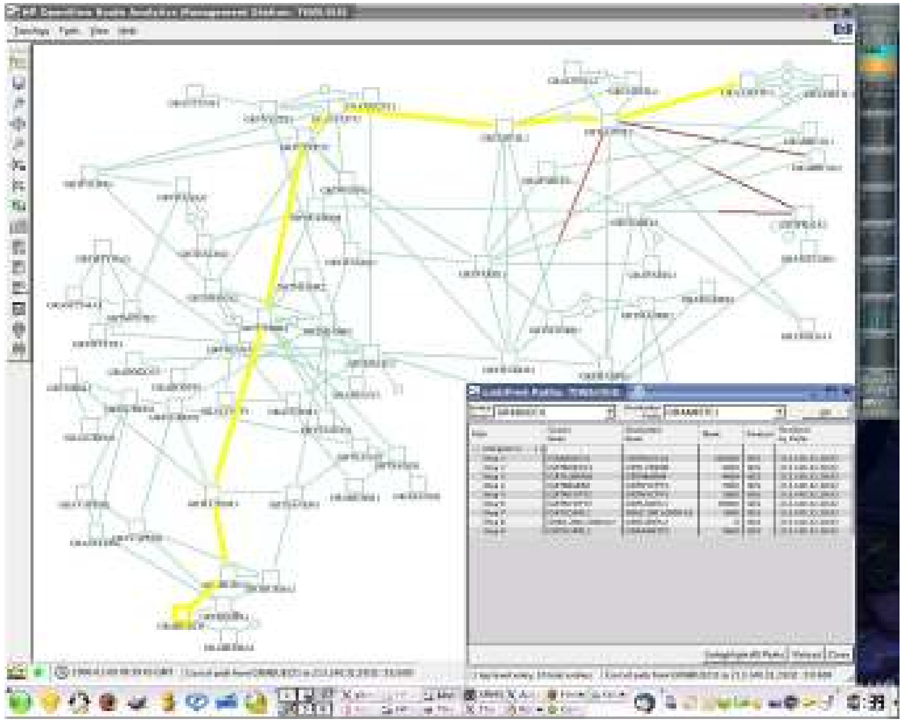
Security Commitments

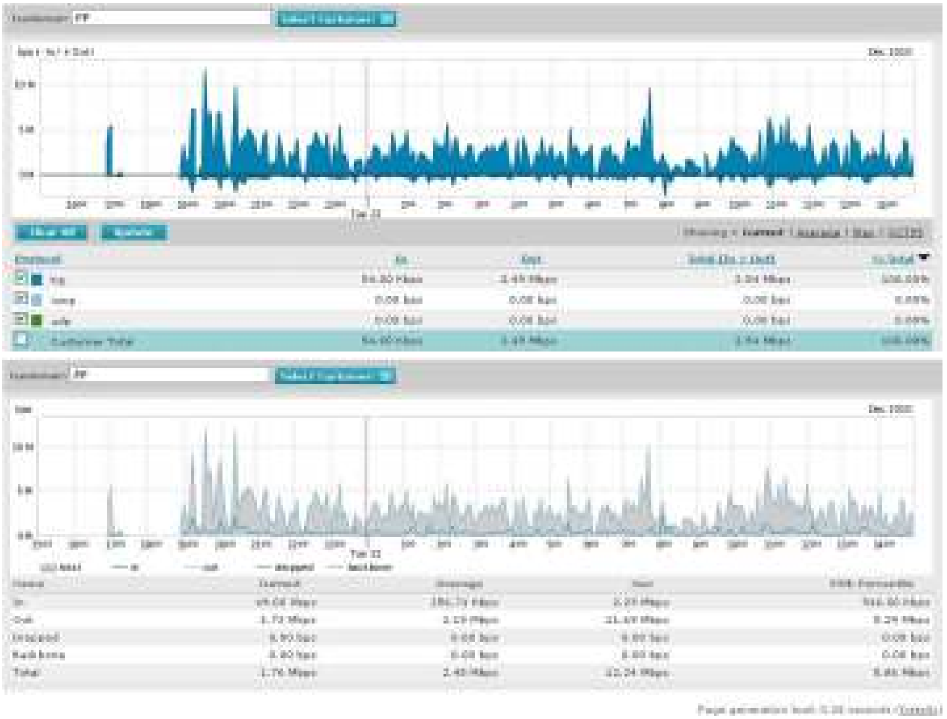
Warranties

Claim Procedures

Termination of Services

Yes, we have tools for Security

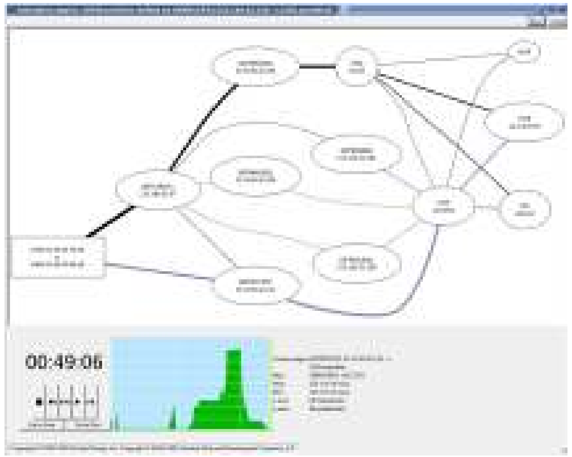


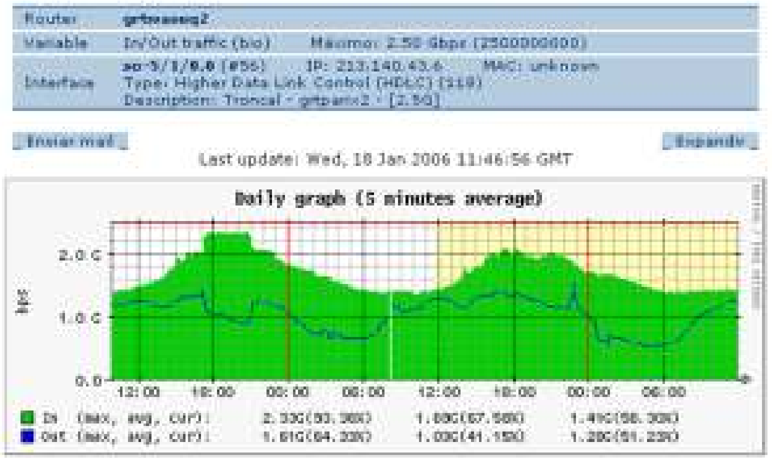


Protocol	In	Out	Total (In + Out)	% Total
☑ tcp	54.80 Mbps	3.49 Mbps	3.04 Mbps	100.00%
☑ icmp	0.00 bps	0.00 bps	0.00 bps	0.00%
☑ udp	0.00 bps	0.00 bps	0.00 bps	0.00%
□ Customer Total	54.80 Mbps	3.49 Mbps	3.04 Mbps	100.00%

Name	Current	Average	Max	95th Percentile
In	[illegible]	[illegible]	[illegible]	[illegible]
Out	1.72 Mbps	2.19 Mbps	21.49 Mbps	8.24 Mbps
Dropped	0.00 bps	0.00 bps	0.00 bps	0.00 bps
Backbone	0.00 bps	0.00 bps	0.00 bps	0.00 bps
Total	1.76 Mbps	2.40 Mbps	22.24 Mbps	8.80 Mbps

Page generation took [illegible] seconds





Router:	grtbraseq2
Variable	In/Out traffic (bits) Máximo: 2.50 Gbps (2500000000)
Interface	so-3/1/0.0 (#56) IP: 213.140.43.6 MAC: unknown Type: Higher Data Link Control (HDLC) (118) Description: Troncal - grtparix2 - [2.5G]

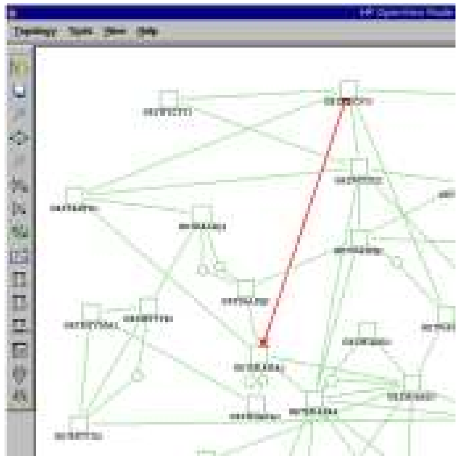
Enviar mail

Expandir

Last update: Wed, 18 Jan 2006 11:46:56 GMT

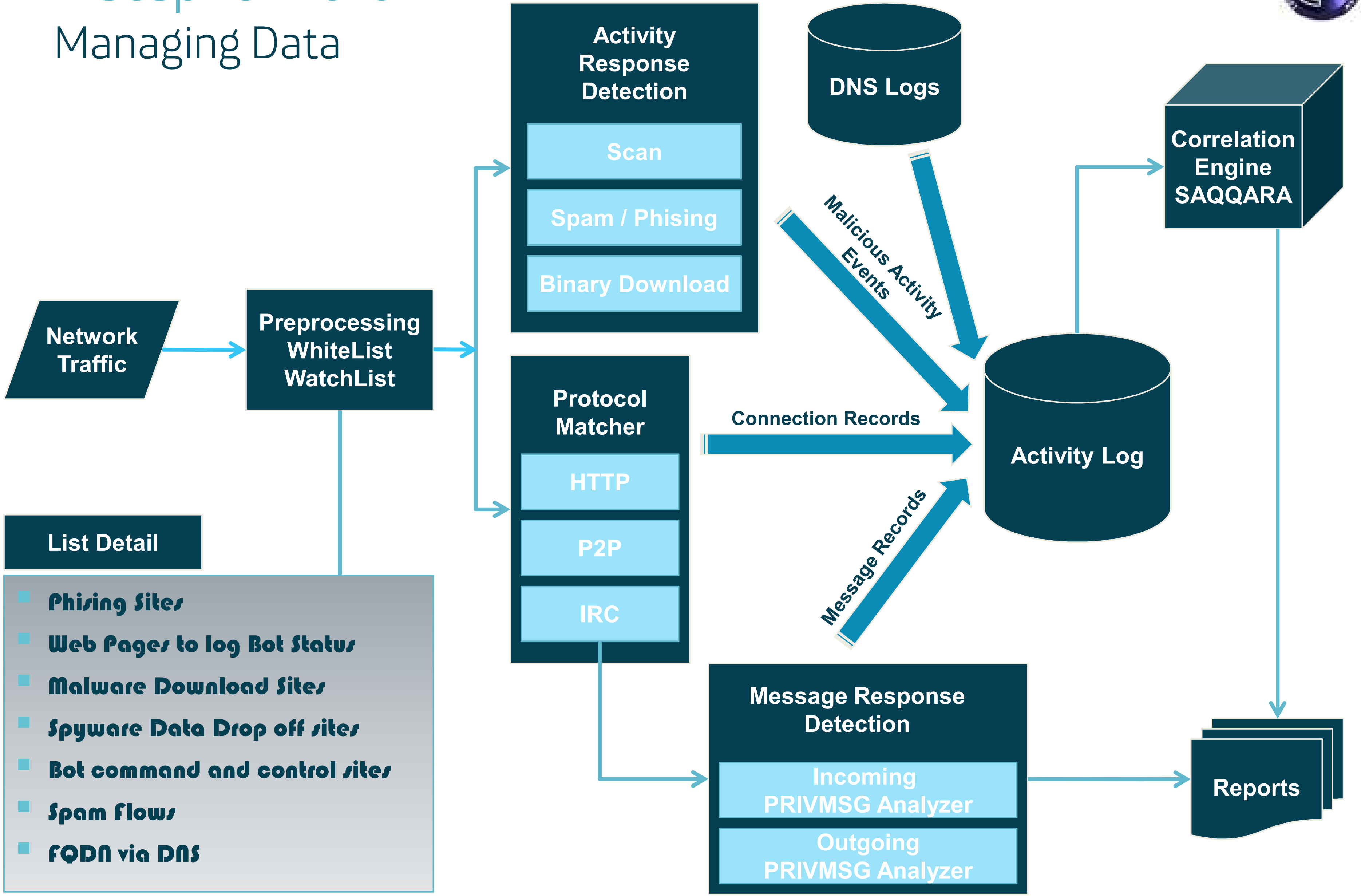
Daily graph (5 minutes average)

```
🟩 In  (max, avg, cur):   2.33G(93.38%)   1.69G(67.58%)   1.46G(58.30%)
🟦 Out (max, avg, cur):   1.61G(64.33%)   1.03G(41.15%)   1.28G(51.23%)
```



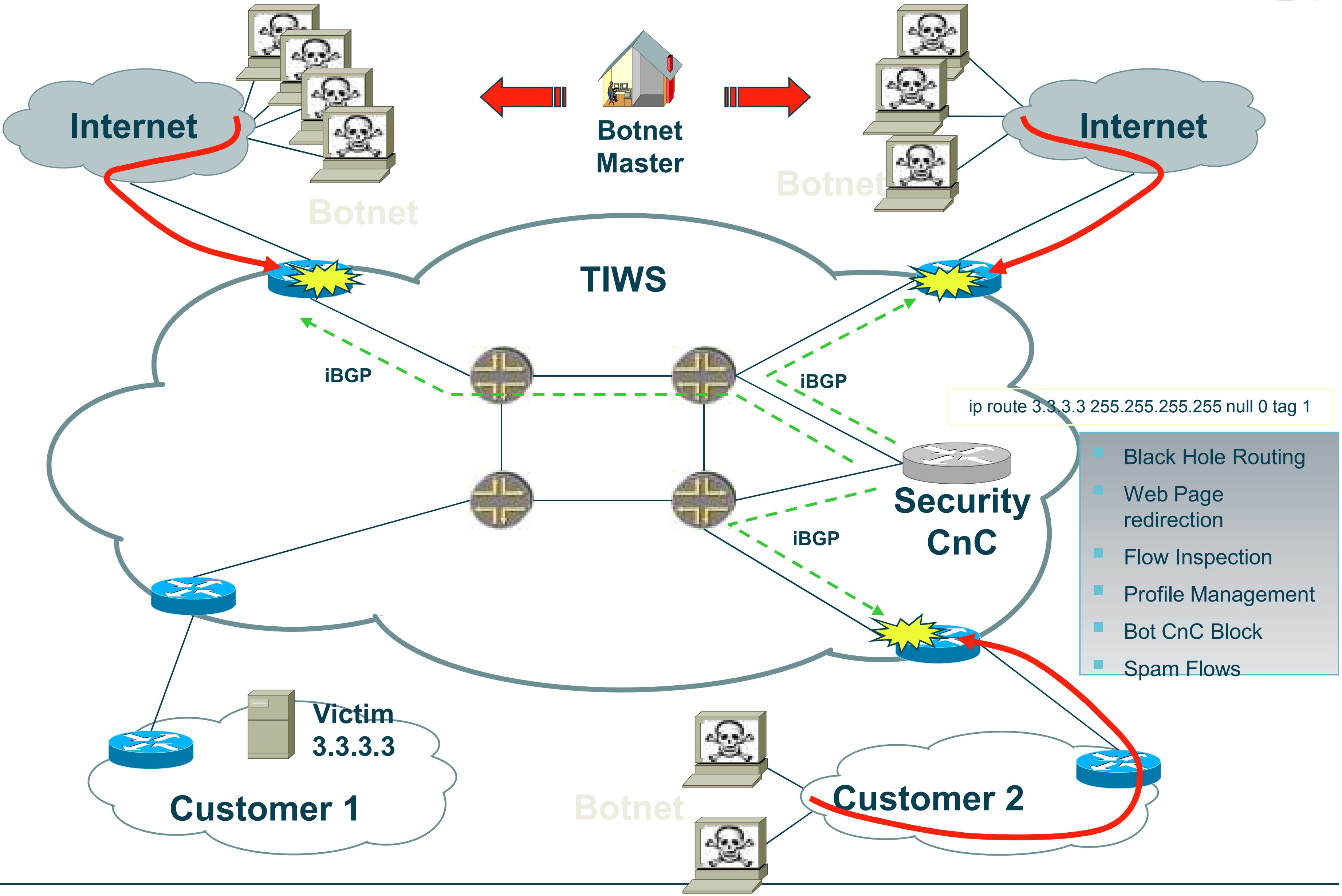
A step forward

Managing Data


Activity Response Detection
Scan
Spam / Phising
Binary Download
DNS Logs
Correlation Engine SAQQARA
Malicious Activity Events
Network Traffic
Preprocessing WhiteList WatchList
Protocol Matcher
HTTP
P2P
IRC
Connection Records
Activity Log
Message Records
Message Response Detection
Incoming PRIVMSG Analyzer
Outgoing PRIVMSG Analyzer
Reports
List Detail

- Phising Sites
- Web Pages to log Bot Status
- Malware Download Sites
- Spyware Data Drop off sites
- Bot command and control sites
- Spam Flows
- FQDN via DNS

With information take actions!



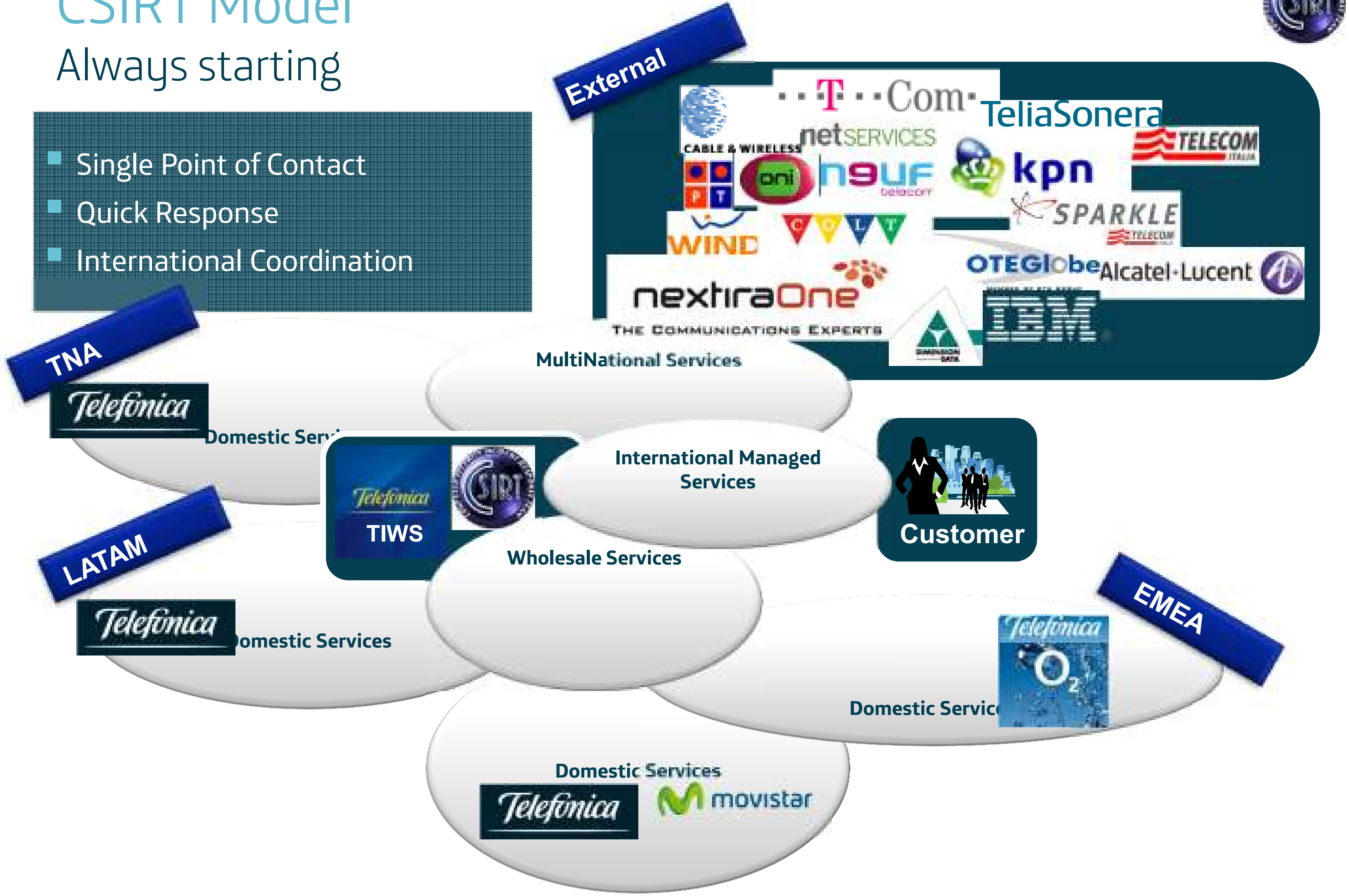
```
ip route 3.3.3.3 255.255.255.255 null 0 tag 1
```

- Black Hole Routing
- Web Page redirection
- Flow Inspection
- Profile Management
- Bot CnC Block
- Spam Flows

CSIRT Model

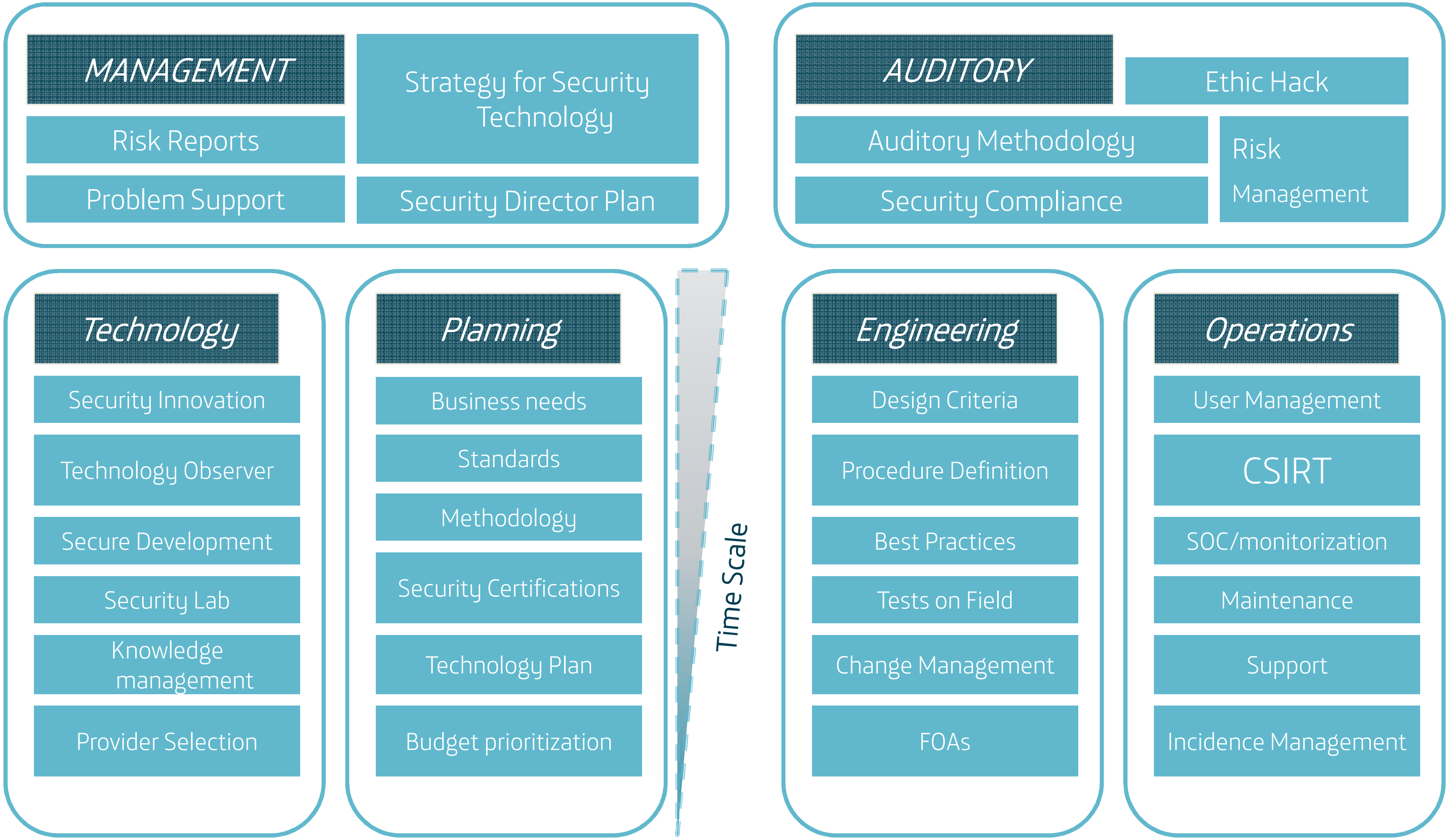
Always starting

- Single Point of Contact
- Quick Response
- International Coordination



CSIRT Scope

The mess inside



MANAGEMENT

- Risk Reports
- Problem Support
- Strategy for Security Technology
- Security Director Plan

AUDITORY

- Ethic Hack
- Auditory Methodology
- Security Compliance
- Risk Management

Technology

- Security Innovation
- Technology Observer
- Secure Development
- Security Lab
- Knowledge management
- Provider Selection

Planning

- Business needs
- Standards
- Methodology
- Security Certifications
- Technology Plan
- Budget prioritization

Time Scale

Engineering

- Design Criteria
- Procedure Definition
- Best Practices
- Tests on Field
- Change Management
- FOAs

Operations

- User Management
- CSIRT
- SOC/monitorization
- Maintenance
- Support
- Incidence Management

Research Activities
… Collaborative Security is trendy

Three ISPs working with the industry in a research project to fight botnets… in a collaborative way

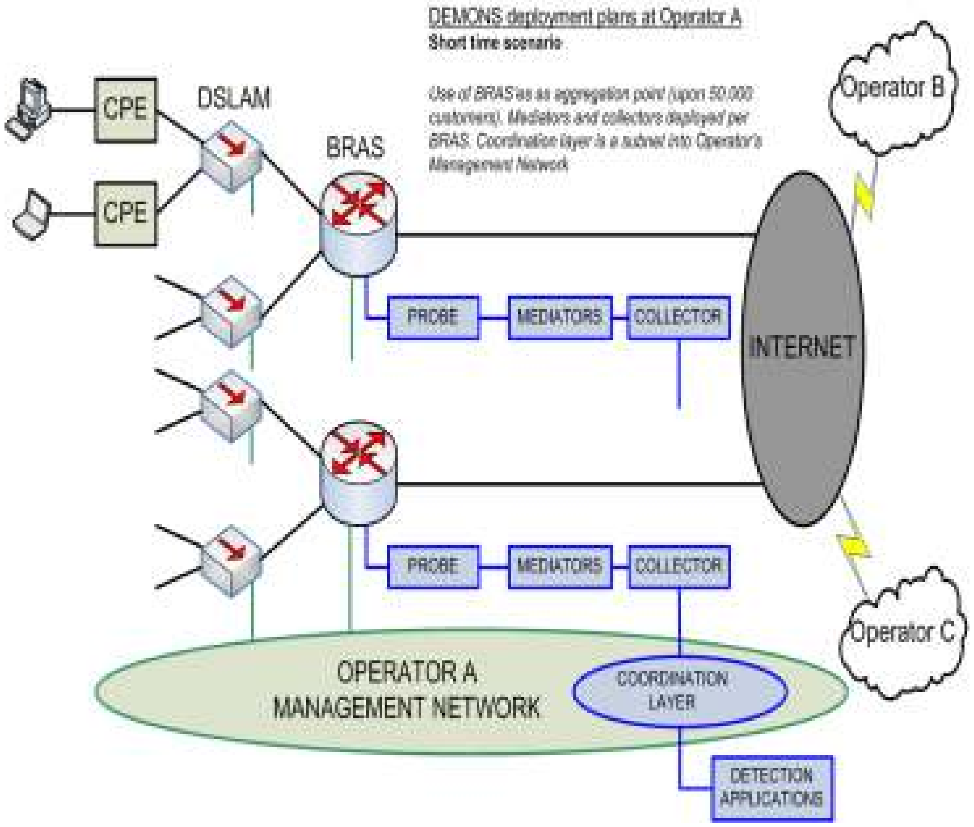
NEC
tp
invea tech
ftw
ETH
INSTITUT TELECOM
Telefónica
OPTINET
SingularLogic
ICCS

SEVENTH FRAMEWORK PROGRAMME

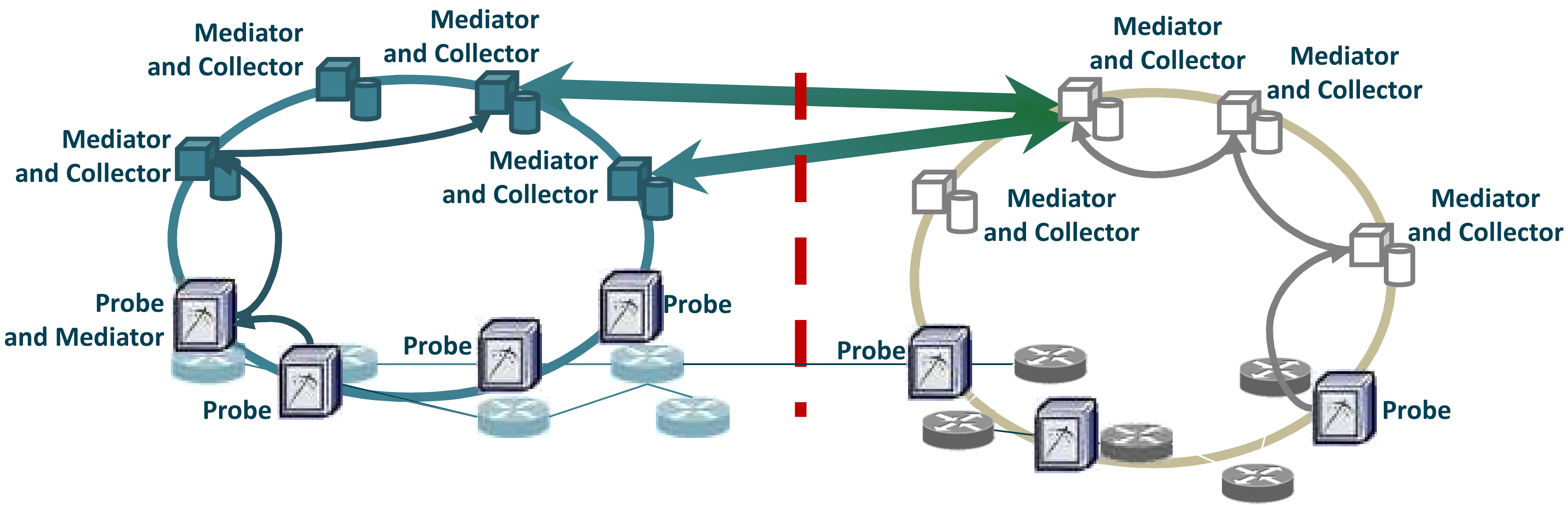
Demons

Our Research trend: Collaborative Security

- GOAL: to share security information to enhance the detection and the mitigation
- How to do that?
  - Placing the monitoring activity close to the network edge
  - Advanced applications to let us detect more complex, distributed attacks. For instance: advanced correlation engines.
  - Collaborative Security Services: such as collectors sharing their alarms and using imported alarms from to draw a wider picture of the threats.
  - Inter-domain information sharing: proposing controlled security information sharing with other Operators/ISPs
- Ongoing project: FP7 DEMONS (co-funded by the EC)


DEMONS deployment plans at Operator A
Short time scenario
Use of BRAS as an aggregation point (upon 50.000 customers). Mediators and collectors deployed per BRAS. Coordination layer is a subnet into Operator's Management Network
CPE
CPE
DSLAM
BRAS
Operator B
INTERNET
PROBE
MEDIATORS
COLLECTOR
PROBE
MEDIATORS
COLLECTOR
Operator C
OPERATOR A
MANAGEMENT NETWORK
COORDINATION
LAYER
DETECTION
APPLICATIONS

DEMONS VISION



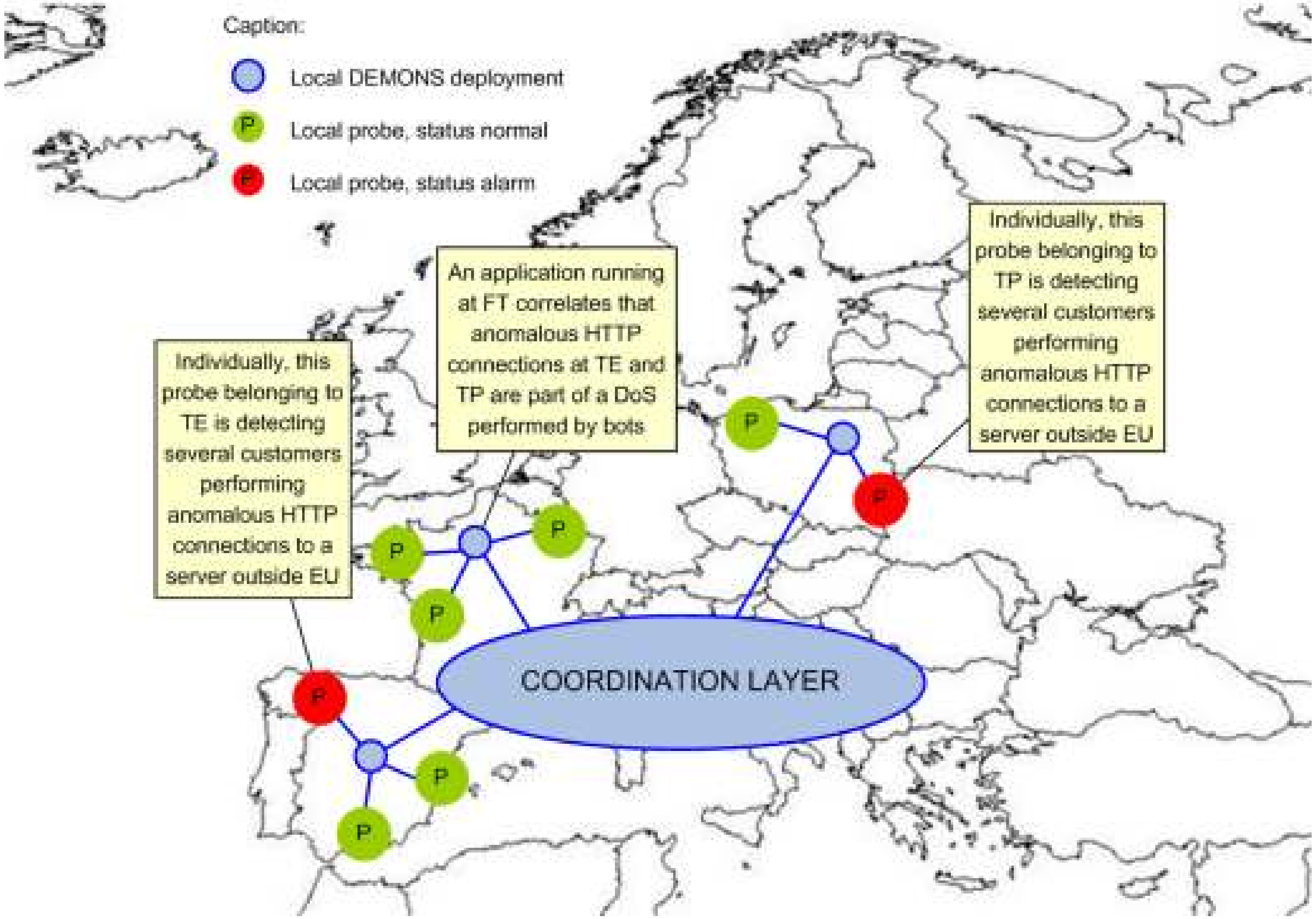
Overlay of in-network monitoring devices

From data-gathering probes to collaborative P2P computing and filtering devices

Innovation pillars
In-network processing and distributed intelligence
Application-tailored data reduction and protection
Resilient autonomic monitoring overlay
Cross-domain interworking

Target Impact
Scalability
Privacy preservation
Flexibility and resilience
Cross-domain threat detection and mitigation

A SAMPLE OF DEMONS COLLABORATIVE APPROACH

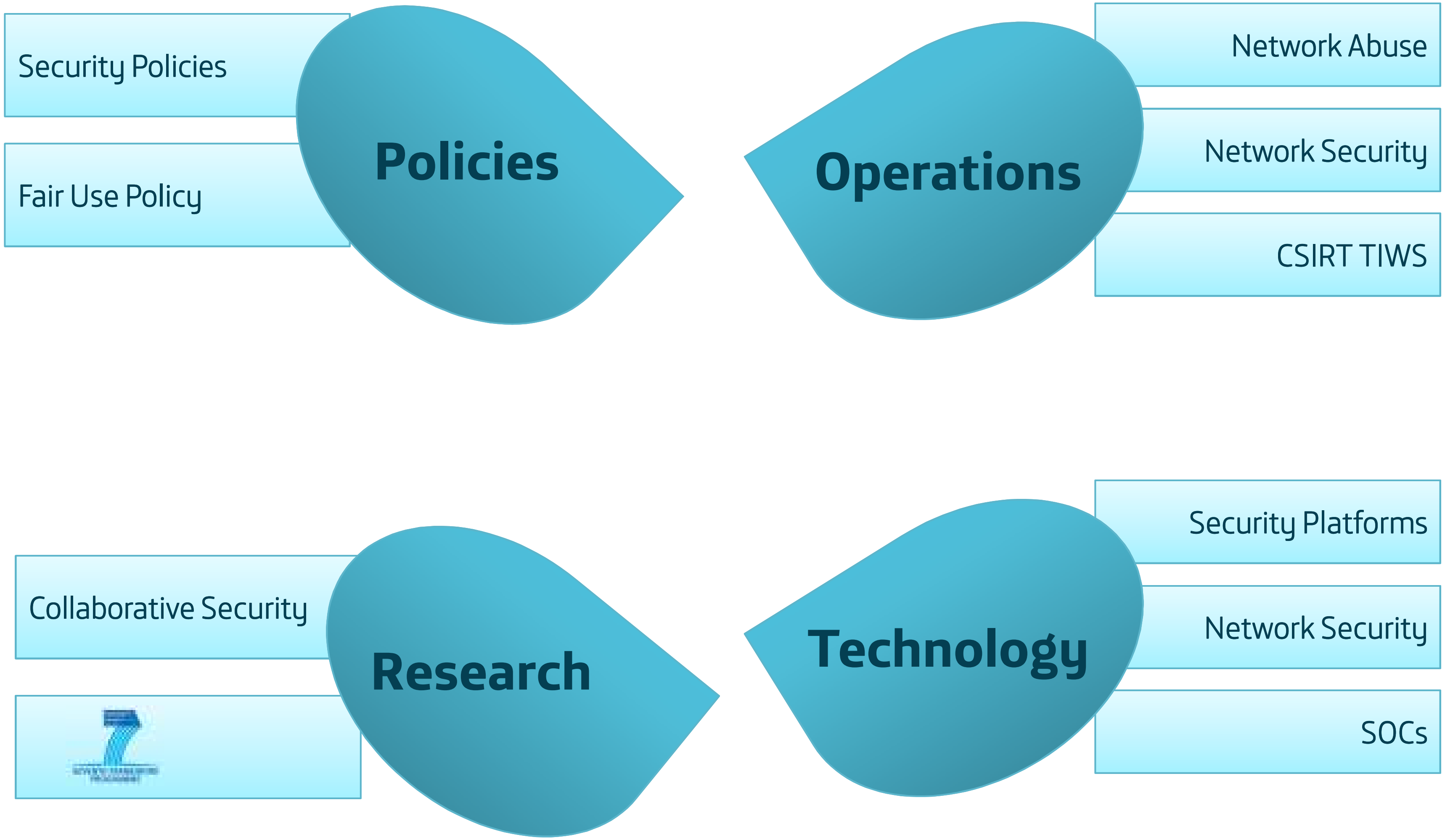


Individually, this probe belonging to TE is detecting several customers performing anomalous HTTP connections to a server outside EU

An application running at FT correlates that anomalous HTTP connections at TE and TP are part of a DoS performed by bots

Individually, this probe belonging to TP is detecting several customers performing anomalous HTTP connections to a server outside EU

… let's look again at what we are doing



Policies

- Security Policies
- Fair Use Policy

Operations

- Network Abuse
- Network Security
- CSIRT TIWS

Research

- Collaborative Security

Technology

- Security Platforms
- Network Security
- SOCs

And a call to action

…Collaborative Security

Telefonica