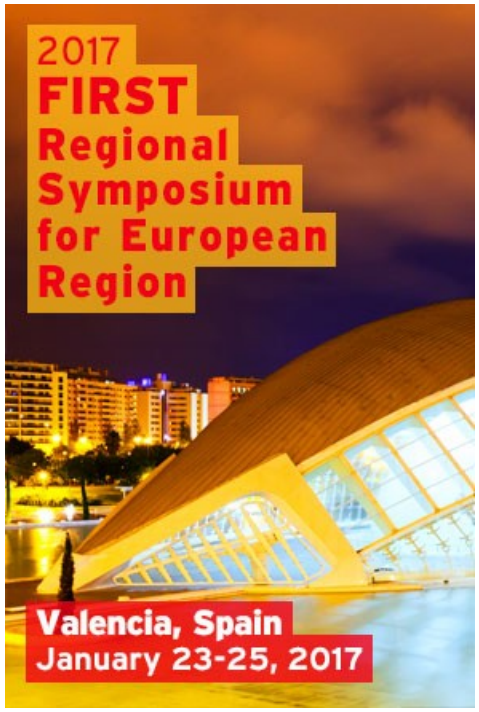
GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

certsi_
SECURITY AND INDUSTRY CERT

incibe_
SPANISH NATIONAL CYBERSECURITY INSTITUTE

Incident Response dealing with the whole country



Javier Berciano
Head of incident response

What is **INCIBE**?

certsi_
SECURITY AND INDUSTRY CERT

Leading company in **cybersecurity and digital trust development** for:

The public

Companies, especially those in **strategic sectors**

The academic research network in Spain (RedIRIS)

It leads different cybersecurity **interventions at a national and international level**

CERTSI (Security and Industry CERT)

certsi_
SECURITY AND INDUSTRY CERT

Year 2012 → Partnership Framework Agreement:

CERTSI (Security and Industry CERT)

certsi_
SECURITY AND INDUSTRY CERT

certsi_
SECURITY AND INDUSTRY CERT

A benchmark for the **technical resolution of cybersecurity incidents** that affect essential services

Prevention

Mitigation

Response

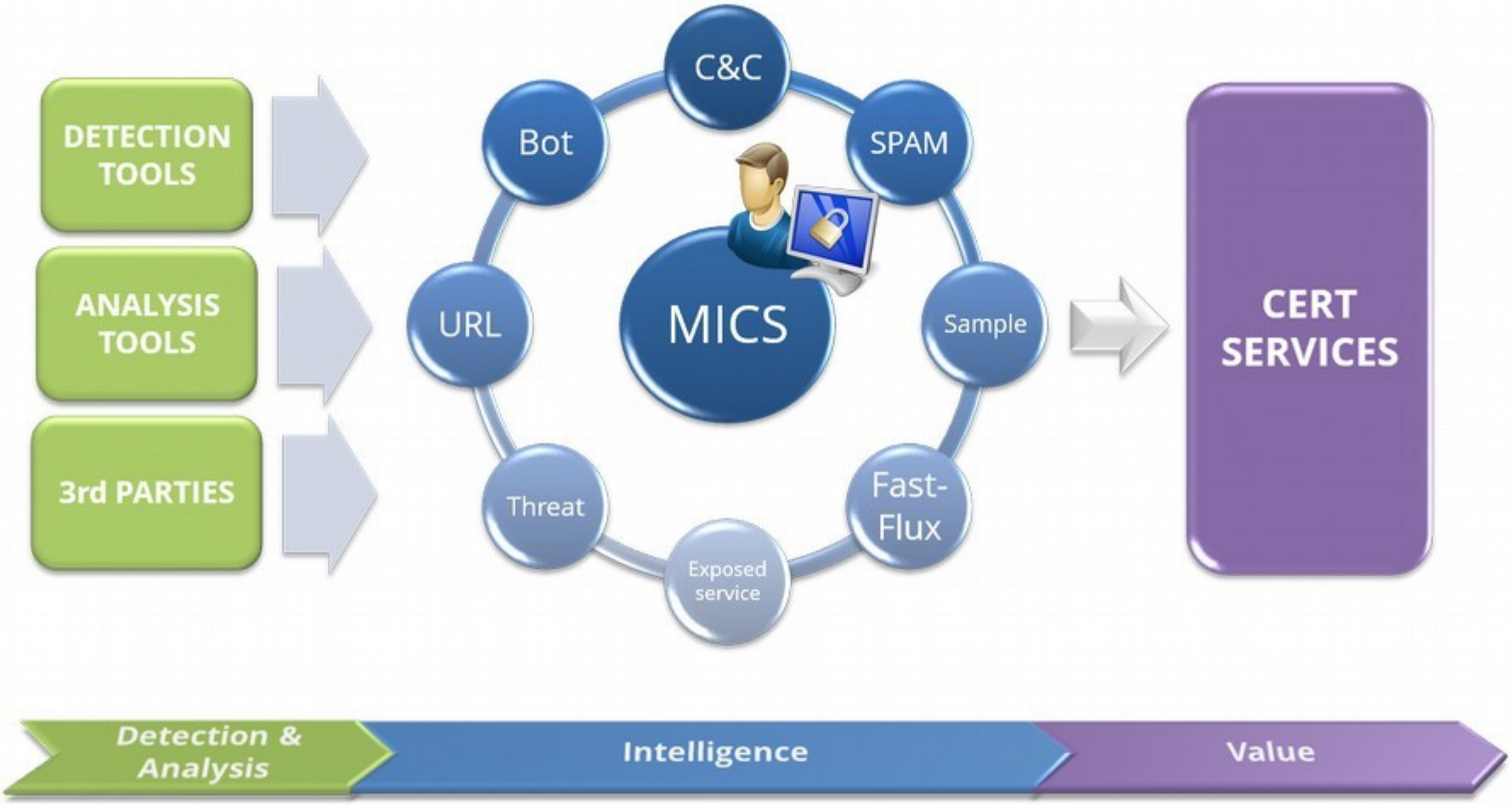
individuals

companies

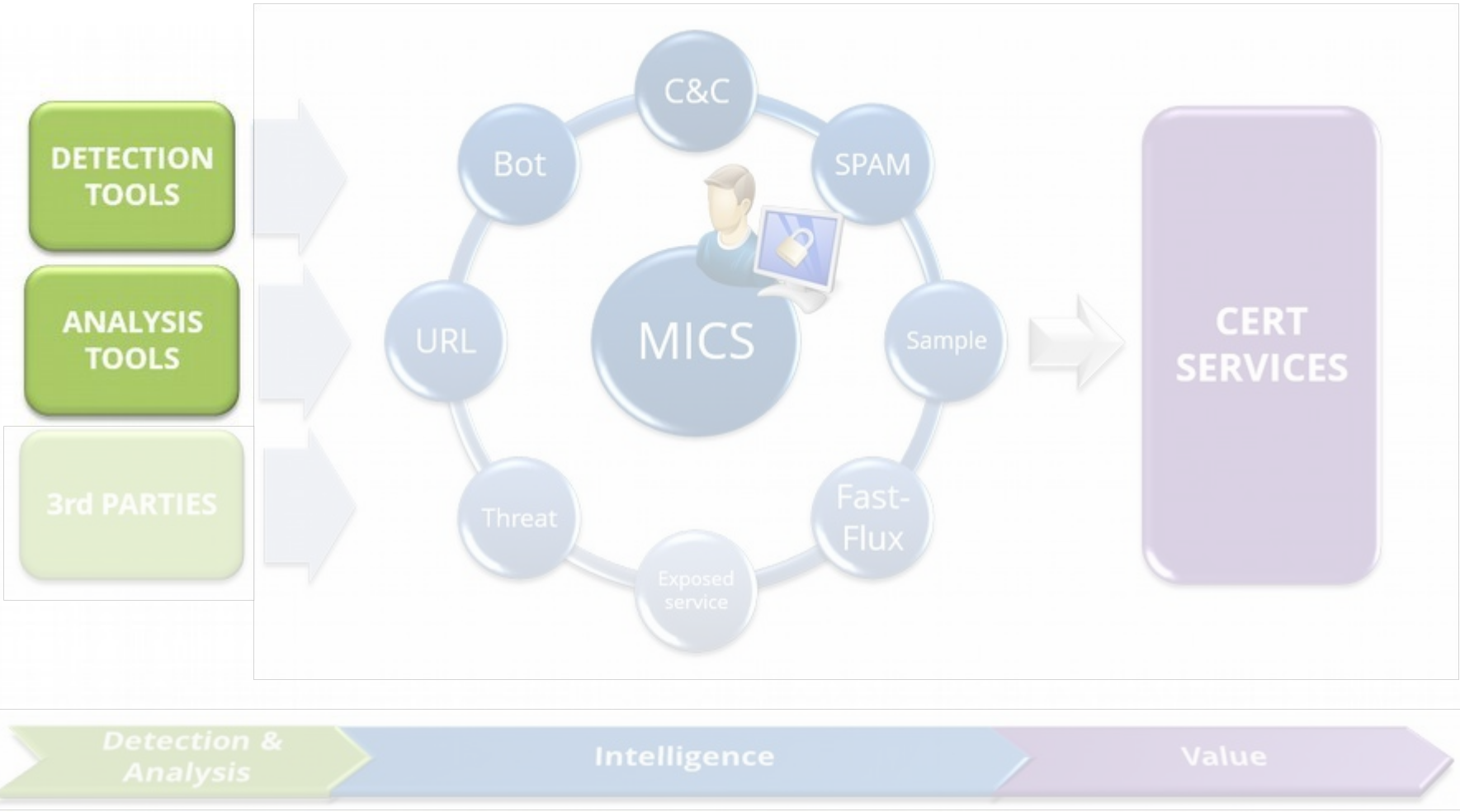
critical infrastructure operators

academic and research network

MICS


DETECTION TOOLS
ANALYSIS TOOLS
3rd PARTIES
C&C
Bot
SPAM
URL
MICS
Sample
Threat
Fast-Flux
Exposed service
CERT SERVICES
Detection & Analysis
Intelligence
Value

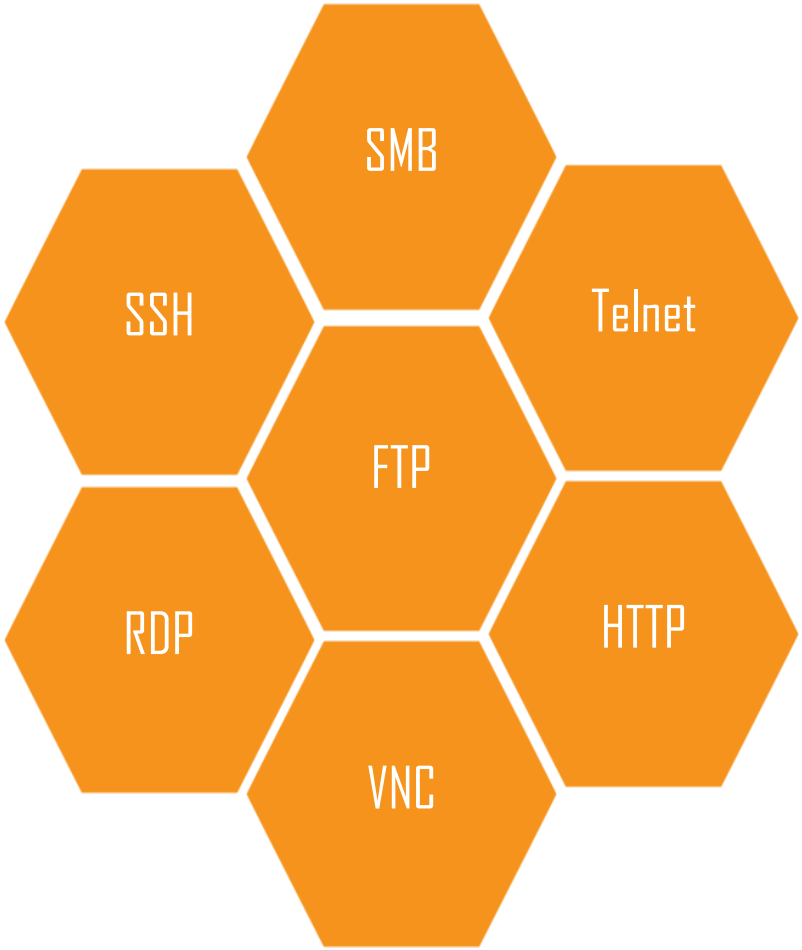
MICS

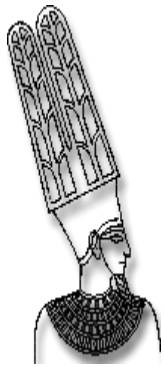

DETECTION TOOLS
ANALYSIS TOOLS
3rd PARTIES
C&C
Bot
SPAM
URL
MICS
Sample
Threat
Fast-Flux
Exposed service
CERT SERVICES
Detection & Analysis
Intelligence
Value

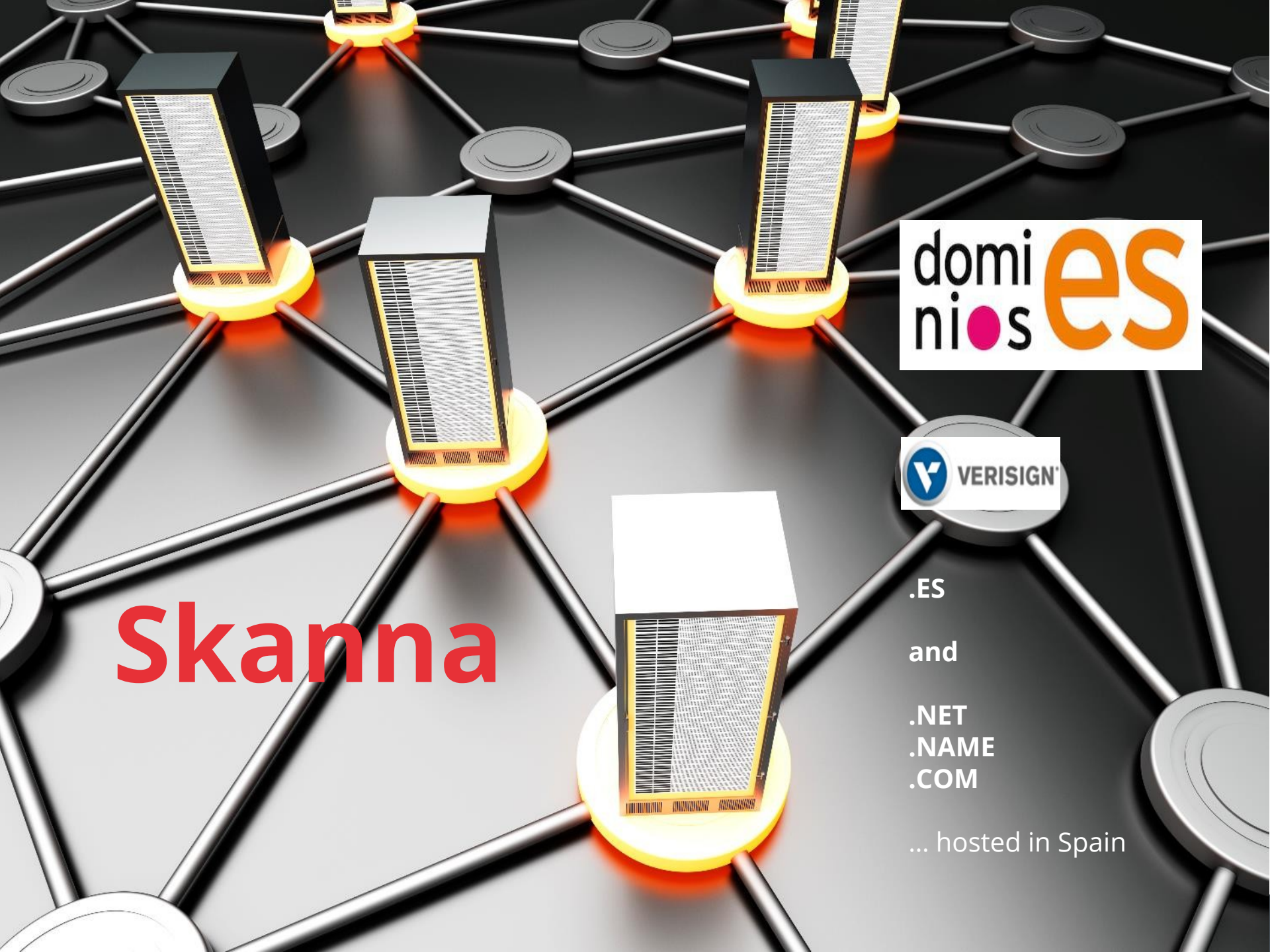
Spamtraps

RedIRIS

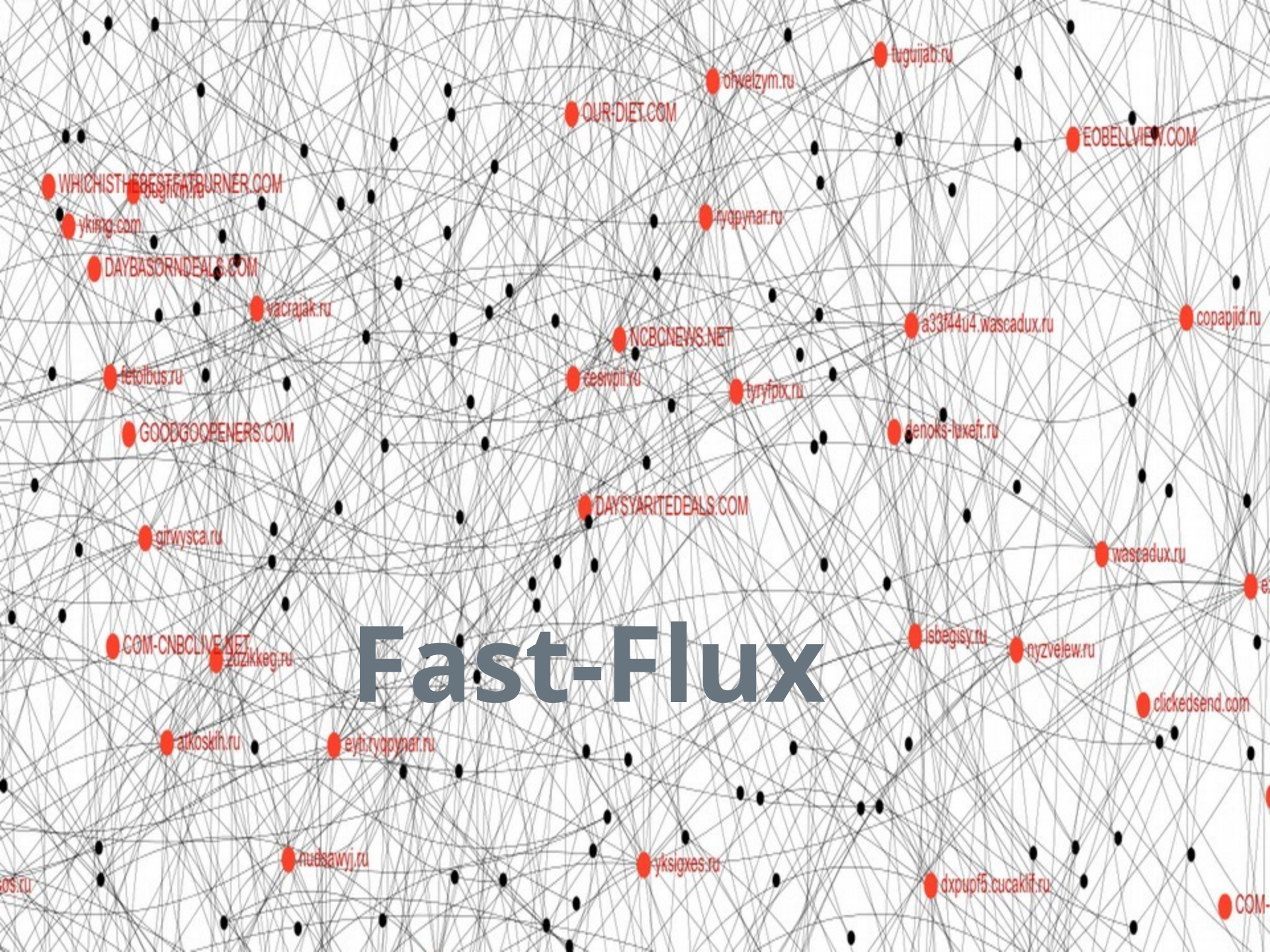
Honeypots



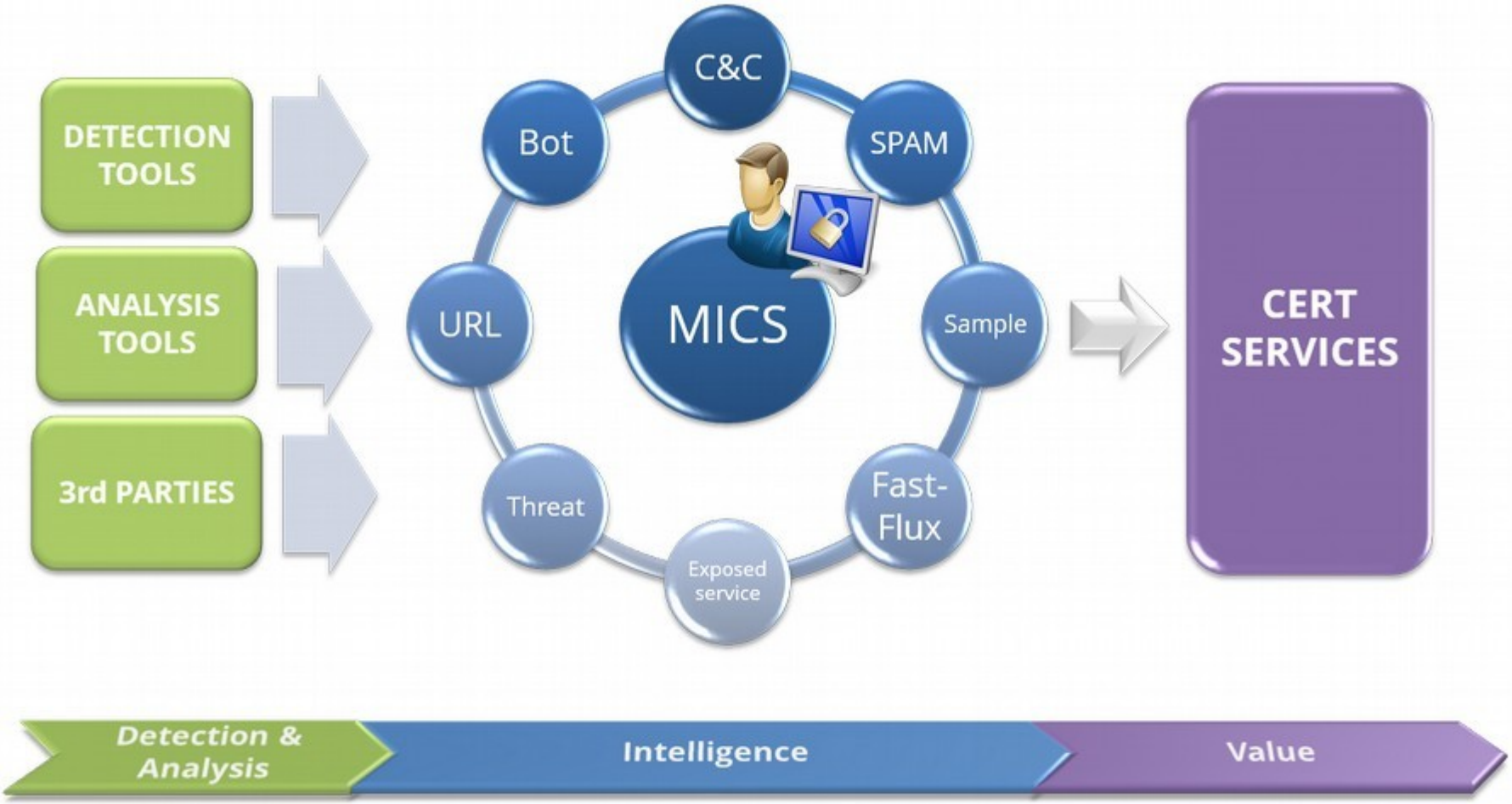



dominios es
VERISIGN
Skanna
.ES
and
.NET
.NAME
.COM
... hosted in Spain

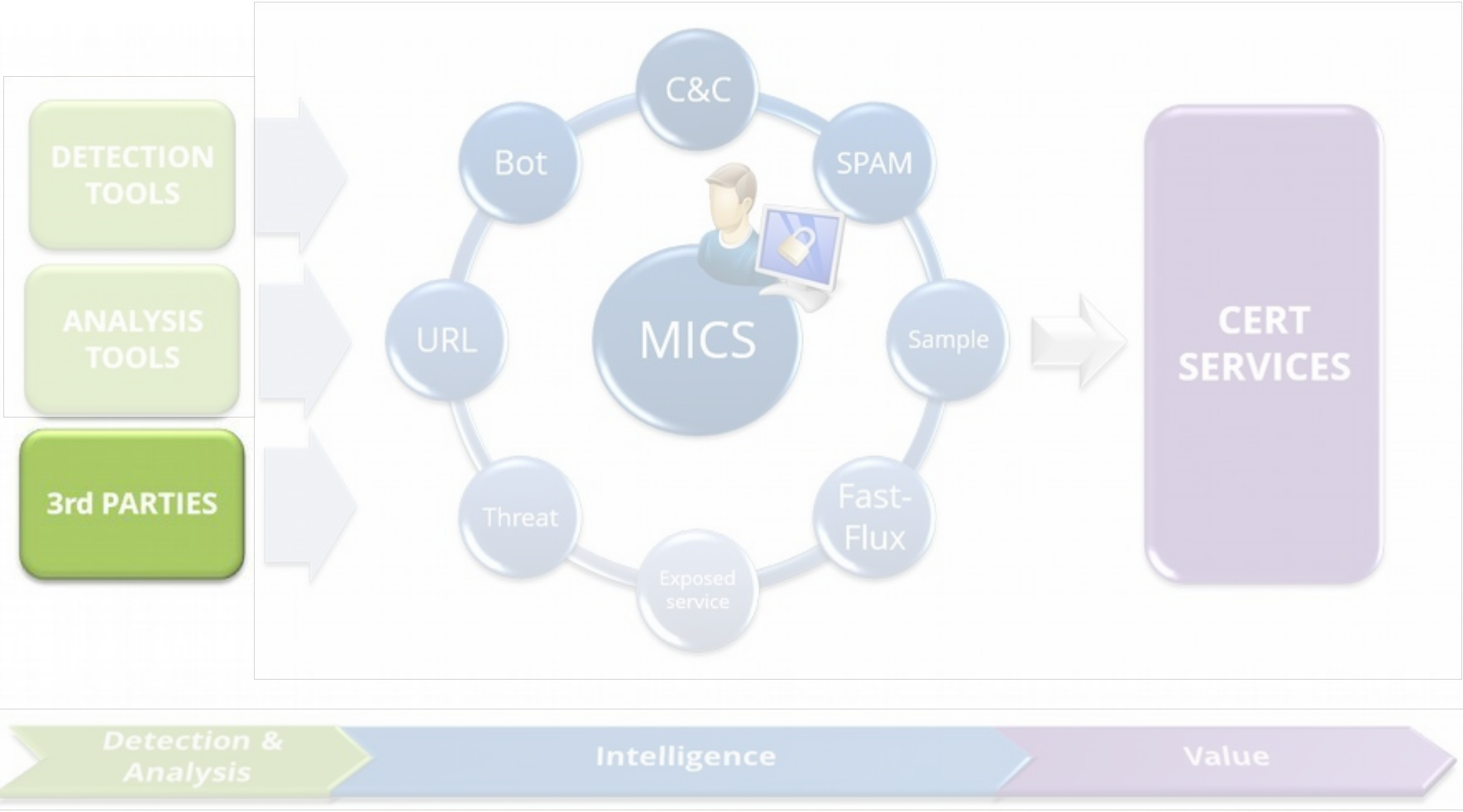

cuckoo
FireEye
virustotal
Jennings


tugujijab.ru
ohwelzym.ru
OUR-DIET.COM
EOBELLVIEW.COM
WHICHISTHEBESTFATBURNER.COM
yking.com
ryqpynar.ru
DAYBASORNDEALS.COM
vacrajak.ru
a33f44u4.wascadux.ru
copapijd.ru
NCBCNEWS.NET
fetolbus.ru
zeswpil.ru
tyryfpix.ru
GOODGOOPENERS.COM
denoks-luxefr.ru
DAYSYARITEDEALS.COM
girwysca.ru
wascadux.ru
COM-CNBCLIVE.NET
isbegisy.ru
nyzvelew.ru
clickedsend.com
atkoskih.ru
eyti.ryqpynar.ru
nudsawyj.ru
yksigxes.ru
dxpupf5.cucakif.ru
Fast-Flux

MICS


DETECTION TOOLS
ANALYSIS TOOLS
3rd PARTIES
C&C
Bot
SPAM
URL
MICS
Sample
Threat
Fast-Flux
Exposed service
CERT SERVICES
Detection & Analysis
Intelligence
Value

MICS

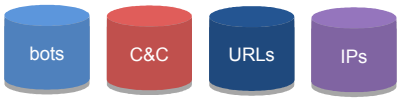

DETECTION TOOLS
ANALYSIS TOOLS
3rd PARTIES
C&C
Bot
SPAM
URL
MICS
Sample
Threat
Fast-Flux
Exposed service
CERT SERVICES
Detection & Analysis
Intelligence
Value

Information feeds

certsi_
SECURITY AND INDUSTRY CERT

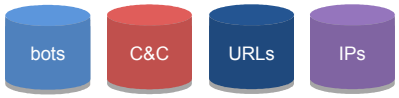
Microsoft Digital Crimes Unit

Symantec.

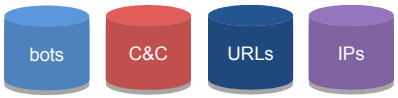


anubisnetworks™
a BITSIGHT company

shadowserver



TEAM CYMRU



SPAMHAUS

Information feeds

certsi_
SECURITY AND INDUSTRY CERT

Information feeds

URLs

URLs

URLs

C&C

URLs

Domains DGA

Domains DGA

Domains DGA

Information feeds

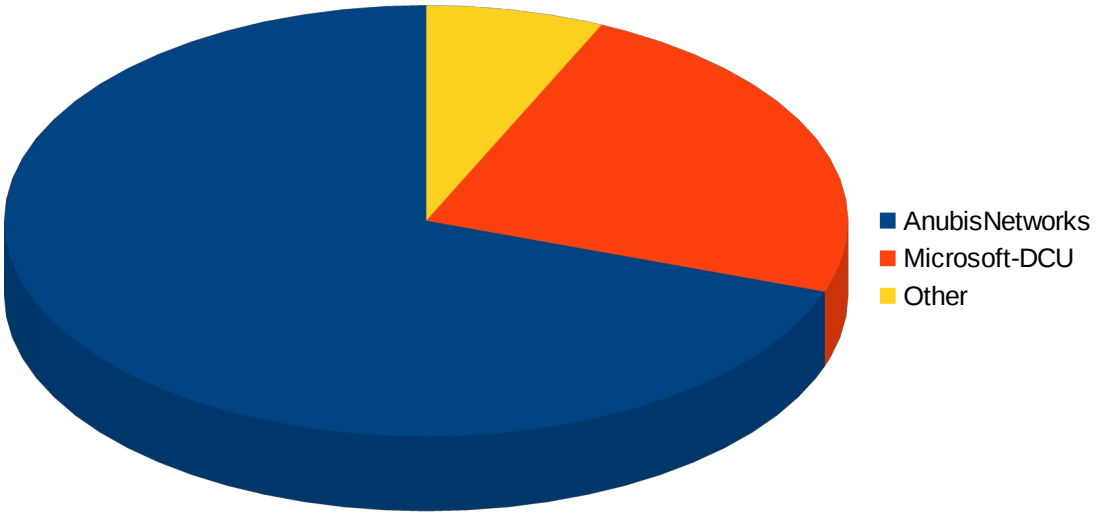
certsi_
SECURITY AND INDUSTRY CERT

More than **10,000,000** events per day

92% bot infections

Two main sources Anubis Networks and Microsoft-DCU

Both provide all connections to a C2 as evidence




Challenge

Servicio ANTIBOTNET

certsi_
SECURITY AND INDUSTRY CERT

AntiBotnet service

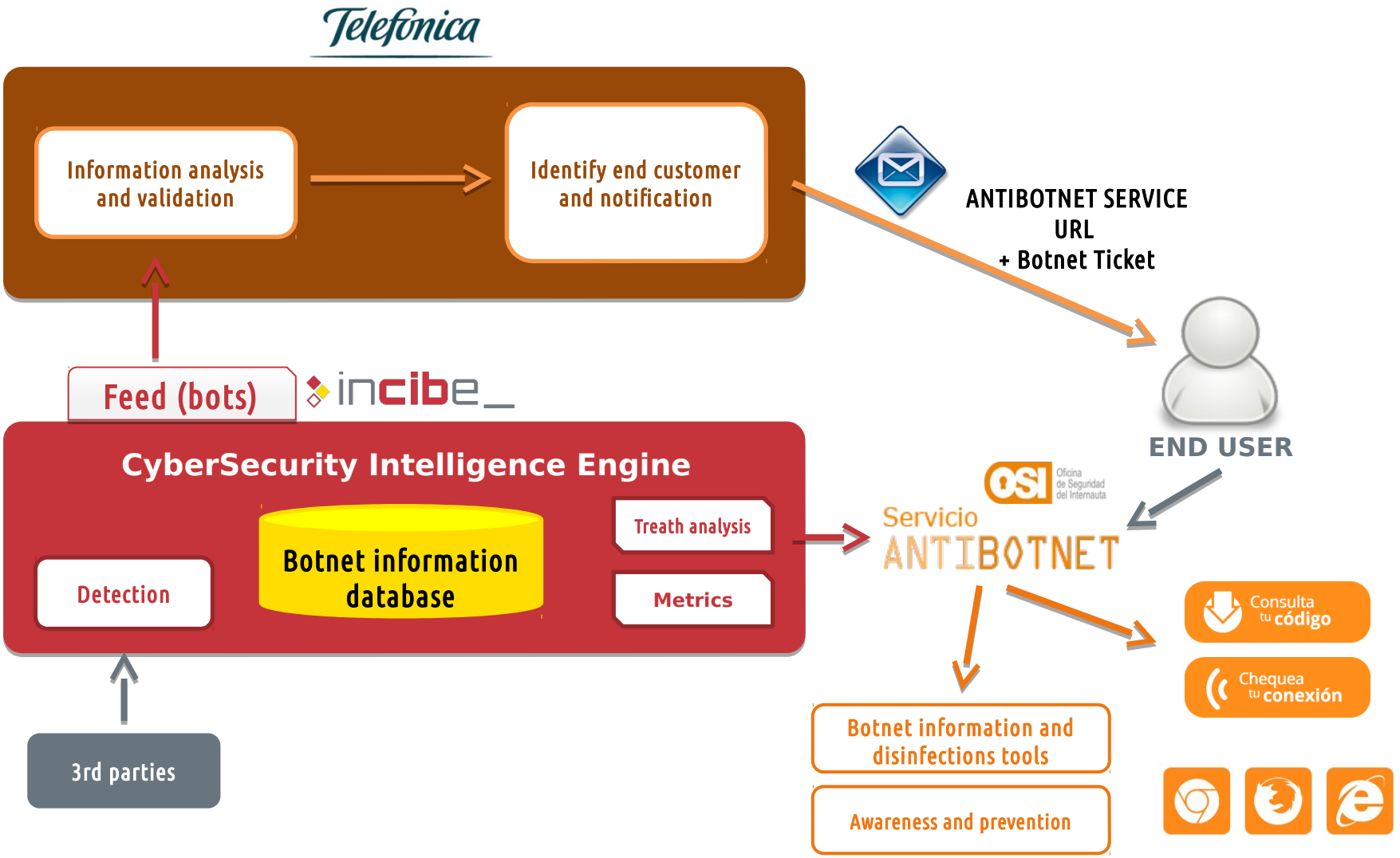
The **objetive** of the Antibotnet Service is the mitigation of botnets from the point of view of the **disinfection** of the users' devices infected: **bots**. Also the service is way to inform and aware users about this problems.

This service is a result of the work developed day to day by INCIBE in collaboration with other national and international entities in fighting against botnets:

- An average of **9,2 million evidences of botnet connections** from Spain daily.
- An average of **59.500 unique IPs affected** daily in Spain.
- Data from close to **900 external sinkholes**, which correspond approximately with **129 families** of botnets.

Spain is pioneer in this kind of initiative alongside countries such Germany, Japan or Sweden.

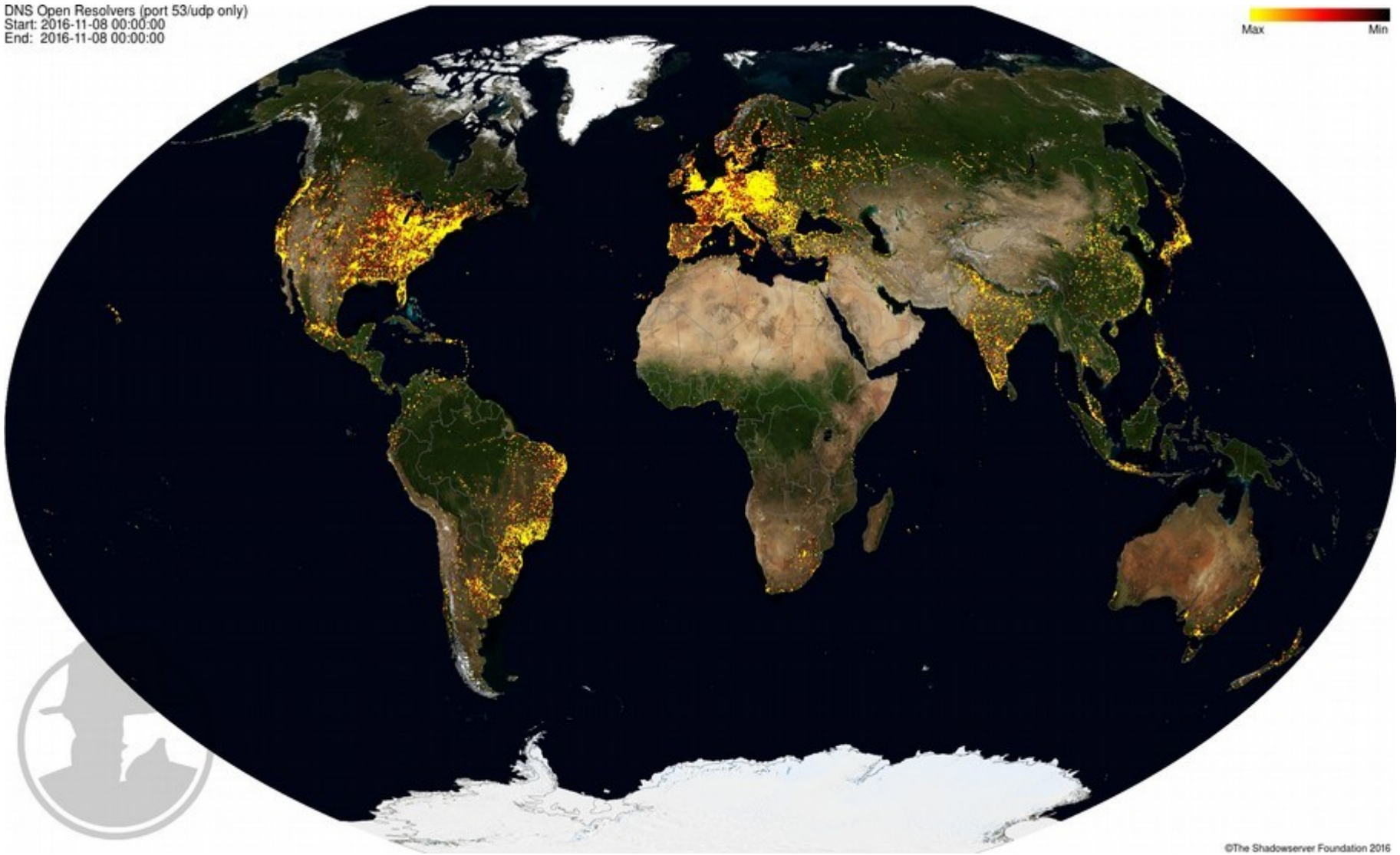
AntiBotnet service



AntiBotnet service

Antibotnet Service is offered to end-users through **five different ways**:

- **Online Service:** End-users can check online if their public IP is involved in botnet activity.
- **Plugin Service:** Plugin available for Google Chrome, Firefox and Internet Explorer to check the IP periodically and automatically, in order to alert the end-user in case of a positive is detected.
- **CONAN Mobile:** Application for Android devices, which helps to check the level of security of mobile devices developed by INCIBE. This app integrates the functionality of the Antibotnet Service, giving botnet alerts in case a positive is detected on wifi networks.
- **ISP Notification:** The Spanish ISP Telefónica collaborates with us notifying end-users by email about botnet related incidents that affect their internet connection. INCIBE gives to Telefónica every day a feed containing bot evidences related to their ASNs. With this information, Telefónica can identify end-user lines affected and therefore notify.
- **API for companies:** API that allows IT personal to integrate the service in their network monitoring systems. This service is oriented to companies


DNS Open Resolvers (port 53/udp only)
Start: 2016-11-08 00:00:00
End: 2016-11-08 00:00:00
Max
Min
©The Shadowserver Foundation 2016

Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/19)
- DNS (UDP/53) (Open Resolver Project)
- Kad (UDP/6429)
- MS-SQL (UDP/1434)
- NetBIOS (UDP 137 to 139)
- NTP Mode 6 (UDP/123) (Open NTP Project)
- NTP Mode 7 (UDP/123)
- QOTD (UDP/17)
- Quake Network Protocol (UDP/26000 and UDP/27960)
- SNMPv2 (UDP/161) (Open SNMP Project)
- SSDP (UDP/1900) (Open SSDP Project)
- Steam Protocol (Many – UDP/27015)

Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/1
- DNS (UDP/53) (O
- Kad (UDP/6429)
- MS-SQL (UDP/14
- NetBIOS (UDP 13
- NTP Mode 6 (UDI
- NTP Mode 7 (UDI
- QOTD (UDP/17)
- Quake Network P
- SNMPv2 (UDP/16
- SSDP (UDP/1900)
- Steam Protocol (

Protocols That Should not be Exposed:

- DB2 (UDP/523)
- Elastic Search (TCP/9200)
- HDFS (TCP/50070, TCP/50075, TCP/50090, TCP/50105, TCP/50030, TCP/50060)
- IPMI (UDP/623)
- LDAP (UDP/389)
- mDNS (UDP/5353)
- MemCached (TCP/11211)
- MongoDB (TCP/27017, TCP/27018, TCP/27019, TCP/28017)
- NAT-PMP (UDP/5351)
- NetBIOS (TCP/137 to 139)
- Portmapper (UDP/111)
- RDP (TCP/3389 and UDP/3389)
- REDIS (TCP/6379)
- rlogin (TCP/451)
- SSDP (TCP/1900)
- TFTP (UDP/69)
- telnet (TCP/23)
- XDMCP (UDP/177)

Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/1
- DNS (UDP/53) (O
- Kad (UDP/6429)
- MS-SQL (UDP/14
- NetBIOS (UDP 13
- NTP Mode 6 (UDI
- NTP Mode 7 (UDI
- QOTD (UDP/17)
- Quake Network F
- SNMPv2 (UDP/16
- SSDP (UDP/1900)
- Steam Protocol (

Protocols That Should not be Exposed:

- DB2 (UDP/523)
- Elastic Search (TCP/9200)
- HDFS (TCP/50070, TCP/50075, TCP/50090, TCP/50105, TCP/50030, TCP/50060)
- IPMI (UDP/623)
- LDAP (UDP/389)
- mDNS (UDP/5353)
- MemCached (TCP/11211)
- MongoDB (TCP/27017, TCP/27018, TCP/27019, TCP/28017)
- NAT-PMP (UDP/5351)
- NetBIOS (TCP/137 to 139)
- Portmapper (UDP/111)
- RDP (TCP/3389 and UDP/3389)
- REDIS (TCP/6379)
- rlogin (TCP/451)
- SSDP (TCP/1900)
- TFTP (UDP/69)
- telnet (TCP/23)
- XDMCP (UDP/177)

Protocols That are Vulnerable:

- ISAKMP (UDP/500)
- Netcore/Netis Router (UDP/53413)
- SSL/FREAK (TCP/443)
- SSLv3 (TCP/443)
- Synful Knock (TCP/80)

Amplification Protocols:

- BitTorrent (any)
- CharGEN (UDP/1
- DNS (UDP/53) (O
- Kad (UDP/6429)
- MS-SQL (UDP/14
- NetBIOS (UDP 13
- NTP Mode 6 (UDI
- NTP Mode 7 (UDI
- QOTD (UDP/17)
- Quake Network F
- SNMPv2 (UDP/16
- SSDP (UDP/1900)
- Steam Protocol (

Protocols That Sh

- DB2 (UDP/523)
- Elastic Search (TCI
- HDFS (TCP/50070,
- IPMI (UDP/623)
- LDAP (UDP/389)
- mDNS (UDP/5353)
- MemCached (TCP/
- MongoDB (TCP/270
- NAT-PMP (UDP/535
- NetBIOS (TCP/137
- Portmapper (UDP/
- RDP (TCP/3389 and
- REDIS (TCP/6379)
- rlogin (TCP/451)
- SSDP (TCP/1900)
- TFTP (UDP/69)
- telnet (TCP/23)
- XDMCP (UDP/177)

- UPDATED: 2016-11-02 – Added LDAP
- UPDATED: 2016-09-22 – Added RDP
- UPDATED: 2016-09-21 – Added ISAKMP
- UPDATED: 2016-05-18 – Added XDMCP
- UPDATED: 2016-05-18 – Added DB2
- UPDATED: 2016-03-09 – Added TFTP
- UPDATED: 2016-02-17 – Added mDNS
- UPDATED: 2015-09-20 – Added Synful Knock
- UPDATED: 2015-09-15 – Added Portmapper
- UPDATED: 2015-06-01 – Added Elastic Search
- UPDATED: 2015-03-09 – Added SSL/FREAK
- UPDATED: 2015-02-13 – Added MongoDB
- UPDATED: 2015-02-08 – Added Open SSDP and Open SNMP project links
- UPDATED: 2015-01-29 – Added MS-SQL
- UPDATED: 2015-01-23 – Added MemCached
- UPDATED: 2015-01-21 – Added REDIS
- UPDATED: 2015-01-07 – Added NAT-PMP
- UPDATED: 2014-11-17 – Added SSLv3
- UPDATED: 2014-08-28 – Added Netcore/Netis
- UPDATED: 2014-07-01 – Added Quake and Steam
- UPDATED: 2014-06-26 – Added IPMI and Gameover Zeus
- UPDATED: 2014-06-12 – Added port numbers
- UPDATED: 2014-03-26 – Added NetBIOS
- UPDATED: 2014-03-06 – Added SSDP

PyRTIR

certsi_
SECURITY AND INDUSTRY CERT

Uses the 1.0 Request Tracker REST API

Main goal is to complement and improve our day to day incident handling

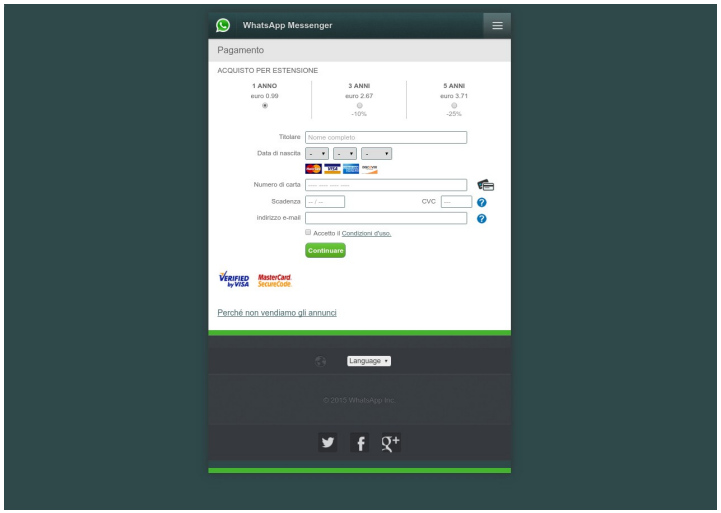
Easily expandable. It is structured in plugins, and each of them performs a different work into RTIR.

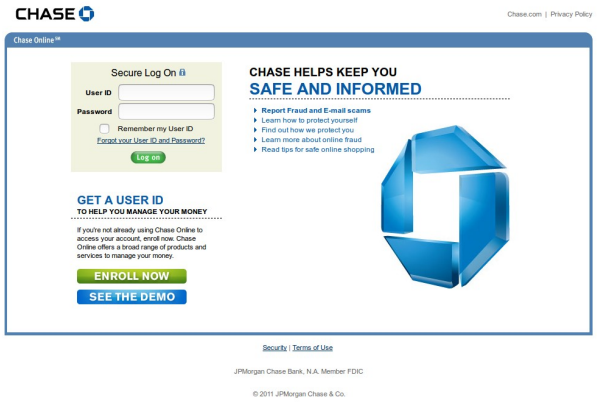
Plugins:

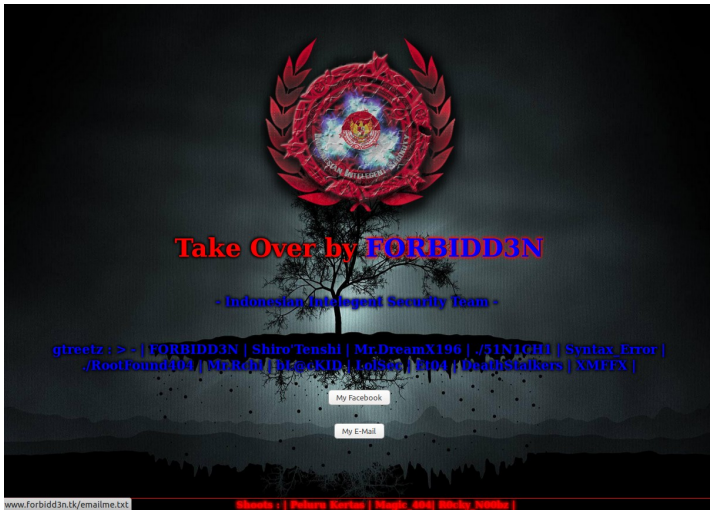
- Phishing
- Defacement
- StealRAT
- XSS
- Stats

Whois data and yara rules

Yara detected websites: Examples







RTIR Custom Actions

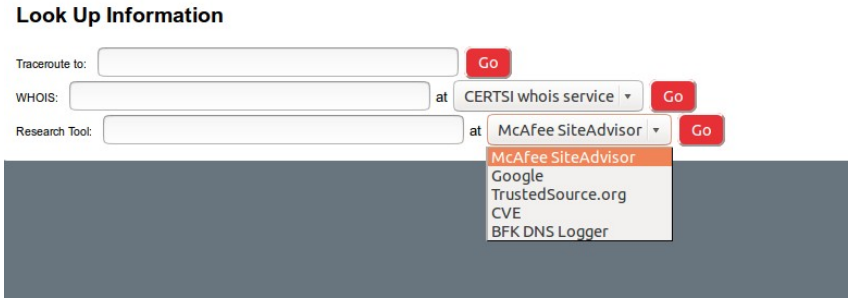
certsi_
SECURITY AND INDUSTRY CERT

On create action for Incident Reports, get URL, extract domains and IP (IPv4, IPv6) and set values in custom fields if it's not listed in the blacklist.

On conditional action for Incidents, push data from Incident into JSON and:

- Put Incident metadata into SIEM.
- Post metadata in JSON to ElasticSearch

Custom forms



Unify access to another internal party tools in RTIR.
Examples:

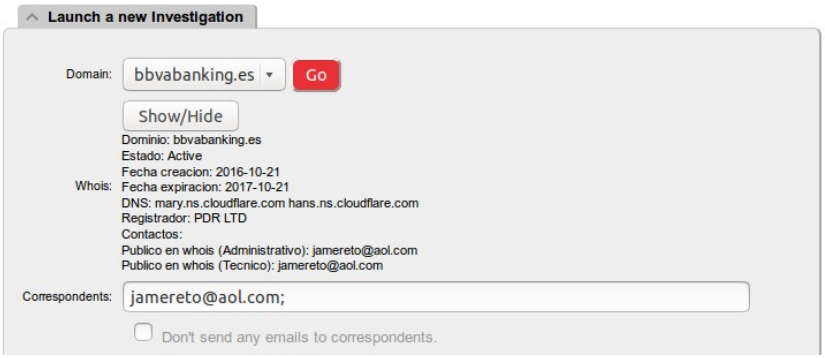
- Internal WHOIS.
- GPG public keys management.
- SIEM integration

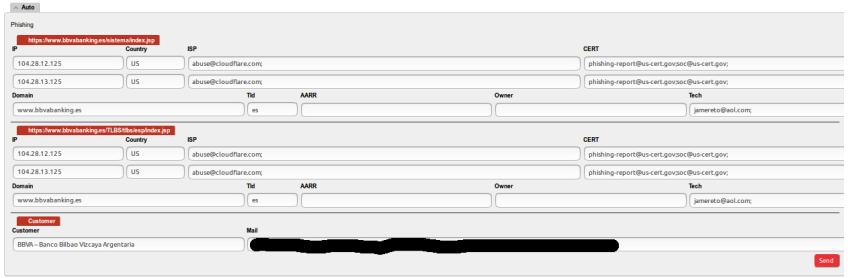
Easy life for operator

certsi_
SECURITY AND INDUSTRY CERT

Several options to launch Investigations:

- domain or IP: get WHOIS data and parse email contacts.
- automatic: based on category of the Incident, get a template and parse it, get emails from WHOIS query and create Investigations by URL.





10 incibe_ 2005-2015 TRABAJANDO POR LA CONFIANZA DIGITAL

CNPIC CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Export data

certsi_
SECURITY AND INDUSTRY CERT

Feedback for SIEM
Executive indicators
Cyber Security Situational Awareness

JSON format
- By email
- POST to ElasticSearch

Executive indicators

certsi_
SECURITY AND INDUSTRY CERT

Indicadores_

2016-01-01 00:00 | 2016-12-31 23:59 | Empresas/ciudadanos | RedIRIS | IICC | Filtrar

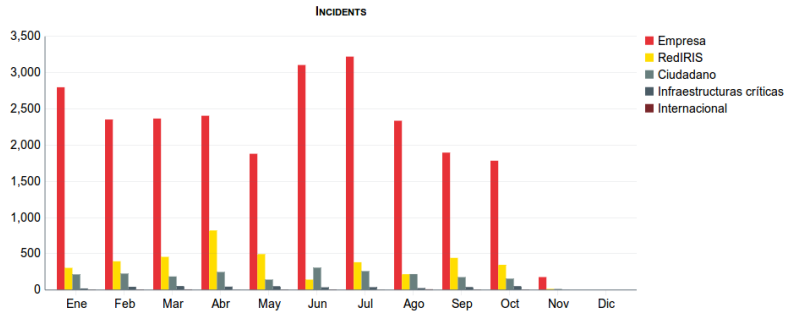
- Resumen
- Incidents
- Incident Reports
- Investigations
- Otras notificaciones
- Consultas
- Exportar

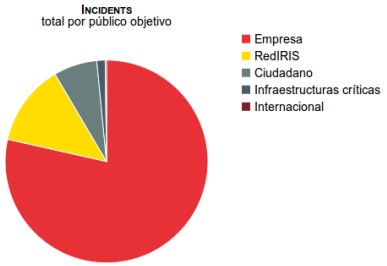
Resumen

certsi_

Público objetivo | Tipología | Estado

	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	Total
Empresa	2.798	2.353	2.366	2.405	1.880	3.105	3.221	2.336	1.896	1.784	178	-	24.322
RedIRIS	305	396	457	822	495	143	383	218	443	347	15	-	4.024
Ciudadano	215	226	186	248	143	308	260	219	177	156	14	-	2.152
Infraestructuras críticas	21	44	54	46	52	37	39	26	41	53	2	-	415
Internacional	6	8	9	2	6	8	3	10	6	6	-	-	64
	3.345	3.027	3.072	3.523	2.576	3.601	3.906	2.809	2.563	2.346	209	-	30.977





10 incibe_ 2005-2015 TRABAJANDO POR LA CONFIANZA DIGITAL

CNPIC CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Cyber Security Situational Awareness

certsi_
SECURITY AND INDUSTRY CERT

Information Sharing with strategic companies, universities and National CERT/CSIRT

ICARO: goals

certsi_
SECURITY AND INDUSTRY CERT

- Share knowledge with strategic companies
- Increase detection capabilities on private sector
- Define a neutral Spanish hub
- Increase automation in early warning

MISP (Malware information Sharing Platform)

certsi_
SECURITY AND INDUSTRY CERT

MISP
Threat Sharing

Thank you!

Javier Berciano
javier.berciano@incibe.es

www.incibe.es www.certsi.es
@certsi_

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
SPANISH NATIONAL CYBERSECURITY INSTITUTE