



Real World Information Exchange Challenges and Insights

Munich 2016 FIRST TC

February 2016

Frédéric Garnier
(frederic.garnier@ec.europa.eu)



- EU Institutions' own CERT
- Operational support for the internal IT teams
- Supports 60+ entities
- Defense against targeted cyber threats



- Around 60 organisations
- From 40 – 40.000 users
- Seperate, heterogenous networks
- Cross-sectoral
 - Government, foreign policy, embassies
 - Banking, energy, pharmaceutical, chemical, food, telecom
 - Maritime, rail and aviation safety
 - Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
 - Research, hi-tech, satellite navigation (GALILEO), defence (EUMS, EDA)
- High-value targets



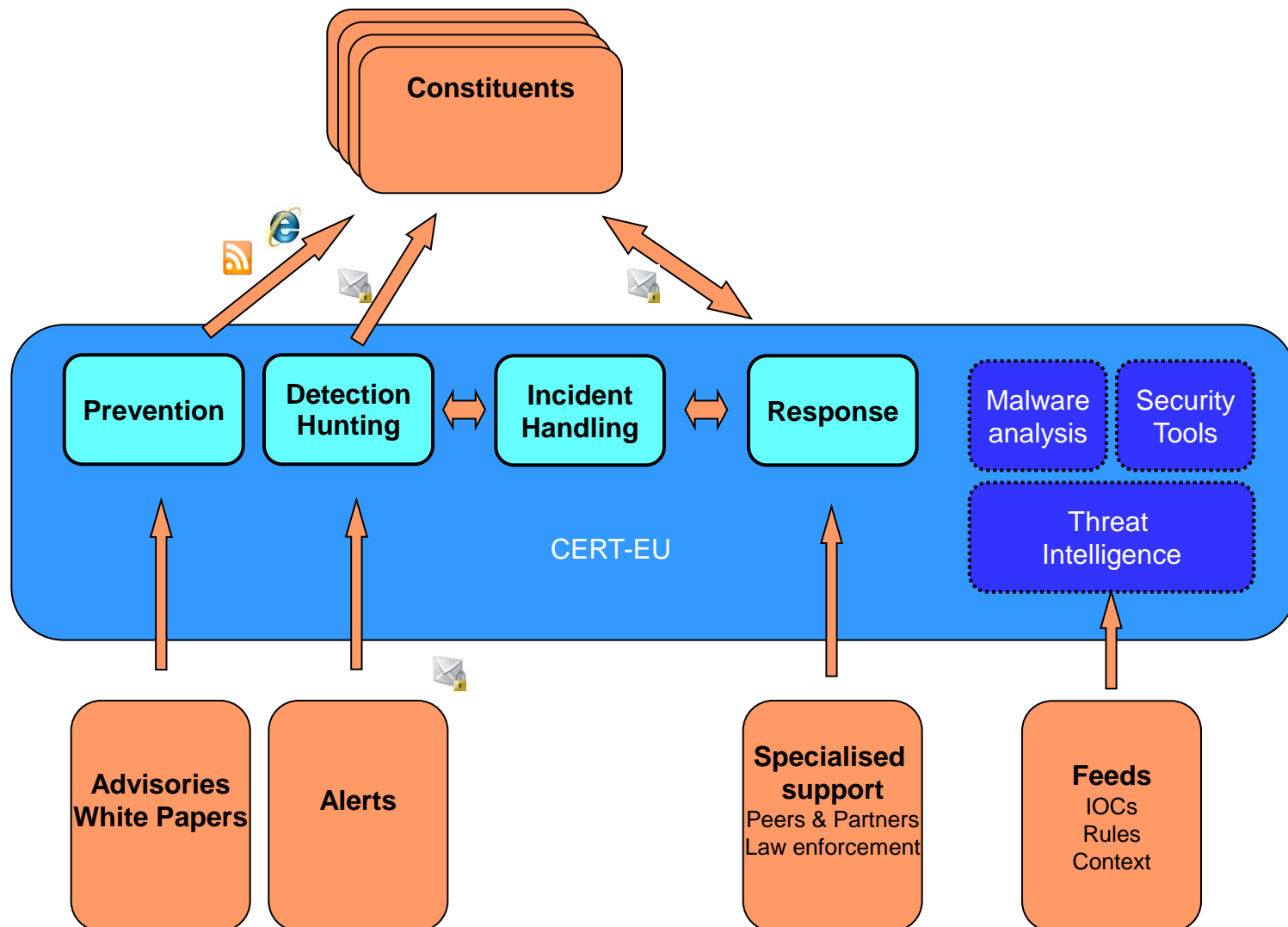


computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

Peers - Partners







Key questions

- What?



- Who?



- Why?

- How?



- When?



- Where?

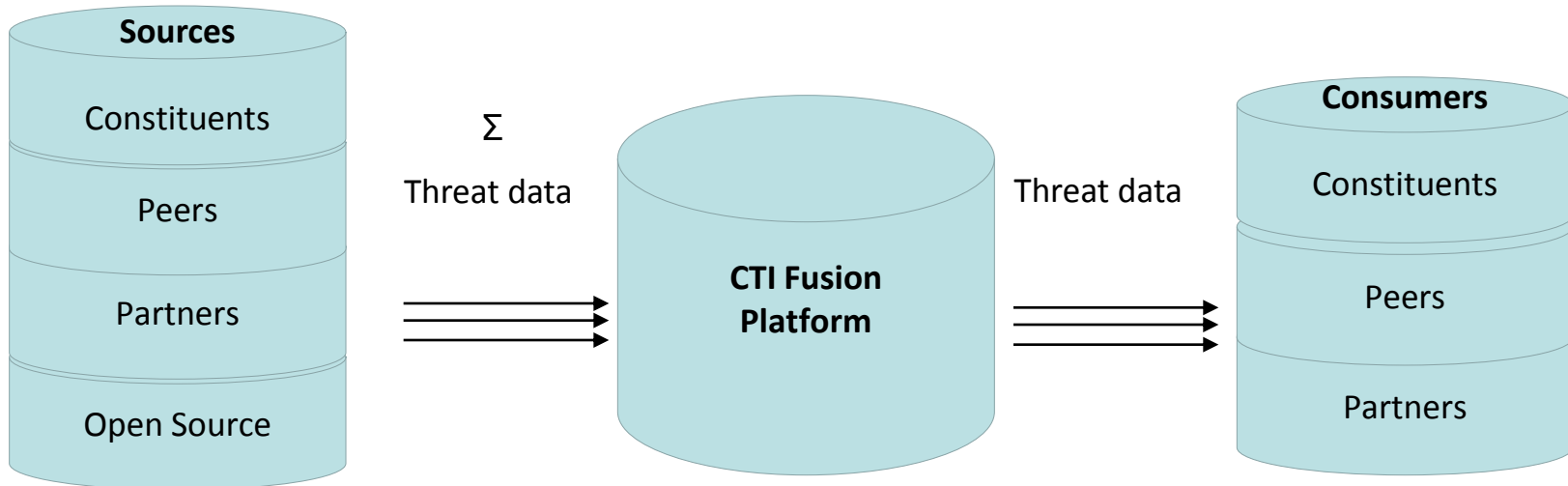


Risk management

- Intelligence needs to serve a purpose
- Not all risks are equal
- Situation is not static



Let's Gather All Badness



Technical intelligence Data flow oriented



✓ IOCs

- Raw value
- Types

✓ Context

- Timing
- Sighting
- Killchain

✓ Accuracy

- FP / TP feedback
- Checks
- Time-To-Live

✓ Detection mechanisms

- YARA
- SNORT

Tactical intelligence Knowledge Basis oriented



✓ 5 Motives

- Cyber-Crime
- Cyber-War
- Cyber-Espionage
- Hacktivism
- Jihadism
- ✓ Country
- ✓ Type
- ✓ Activities
- ✓ First seen / Last seen

✓ 6 Categories

- Malware (families)
- Exploits
- Tools
- Infrastructures
- Attack Patterns (S) & (G)
- ✓ Intended Effect
- ✓ Kill Chain
- ✓ First seen / Last seen

✓ 3 Classes

- Surveillance
- Operations
- Cases
- ✓ Targeted Domains
- ✓ Targeted Sectors
- ✓ Time Period
- ✓ Intent
- ✓ First seen / Last seen



STIX – TTP Data Model

STIX – TTP Data Model		CERT-EU – TTP Implementation
ID		YES
TIMING		YES (First Seen / Last Seen)
TITLE / DESCRIPTION		YES
INTENDED EFFECT		YES
BEHAVIOR	ATTACK PATTERNS	(Generic) – KB1
		(Specific) – KB2
	MALWARE	KB3
	EXPLOITS	KB4
RESOURCES	TOOLS	KB5
	INFRASTRUCTURES	KB6
	PERSONAS	Not used
VICTIM TARGETING	IDENTITY	YES (Org / Country / Sector level not structured yet)
	TARGETED SYSTEM	Not used
	TARGETED INFO	Not used
	TARGETED TECH DETAILS	Not used
EXPLOIT TARGETS		Not used
RELATED TTPs		YES
KILL CHAIN		YES
INFORMATION SOURCE		YES



KB1 - Attack Patterns (G)

Web Appl. Scanning, Social Media
Intell Collection, Malicious Office docs,
Phishing, SWC, Spoofed Websites,
DoS, Defacement, Doxing, etc

- Common techniques used by attackers
- Only for trends / basic profiling
- Useless for attribution

Started: November 2015

Entries: 10+

KB2 - Attack Patterns (S)

Malicious Tor exit nodes, DGA, Single
hit, trojanised software (TrueCrypt),
stalling code, COM object hijacking,
desktop shortcuts redirection, satellite
links hijacking, etc

- Special techniques not accessible to any attacker
- May be used for attribution and characterisation of malware.

Started: mid 2015

Entries: 30+

KB3 - Malware

RAT / backdoor (BlackEnergy, PlugX,
njRAT, Snake, Sofacy, xxxDuke, ...),
ransomware/ banking trojan
(TeslaCrypt, CryptoWall, GPCode,
Dridex, Shifu, Dyre, ...), etc

- Malware family level
- Focus on malware used in targeted attacks
- Importance of Detection Mechanisms

Started: mid 2013

Entries: 600+

KB4 - Exploits

Exploit Kits, CVE (?)

- Symmetrical to CVE / Exploit Target ?

Started: Jan 2016

Entries: 30+

KB5 - Tools

Legitimate tools re-purposed or
customised for malicious use: Shell,
port scanners, web vulnerability
scanners, sql injection tools, key
loggers, password cracking etc,.

- Understanding TTP supply chain

Started: Nov 2015

Entries: 60+

KB6 - Infrastructures

Delivery infra (phishing, watering hole,
etc), C2 infra, bots, forums, malware
sites, darknets, etc

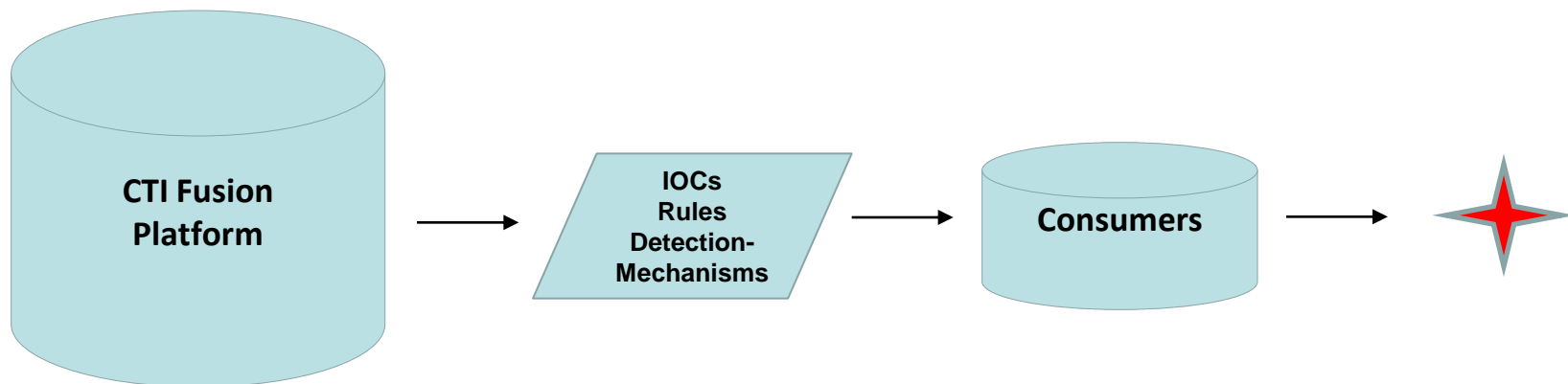
- Pivoting for attribution

Started: Nov 2015

Entries: 30+



Let's Use it to Detect Stuff

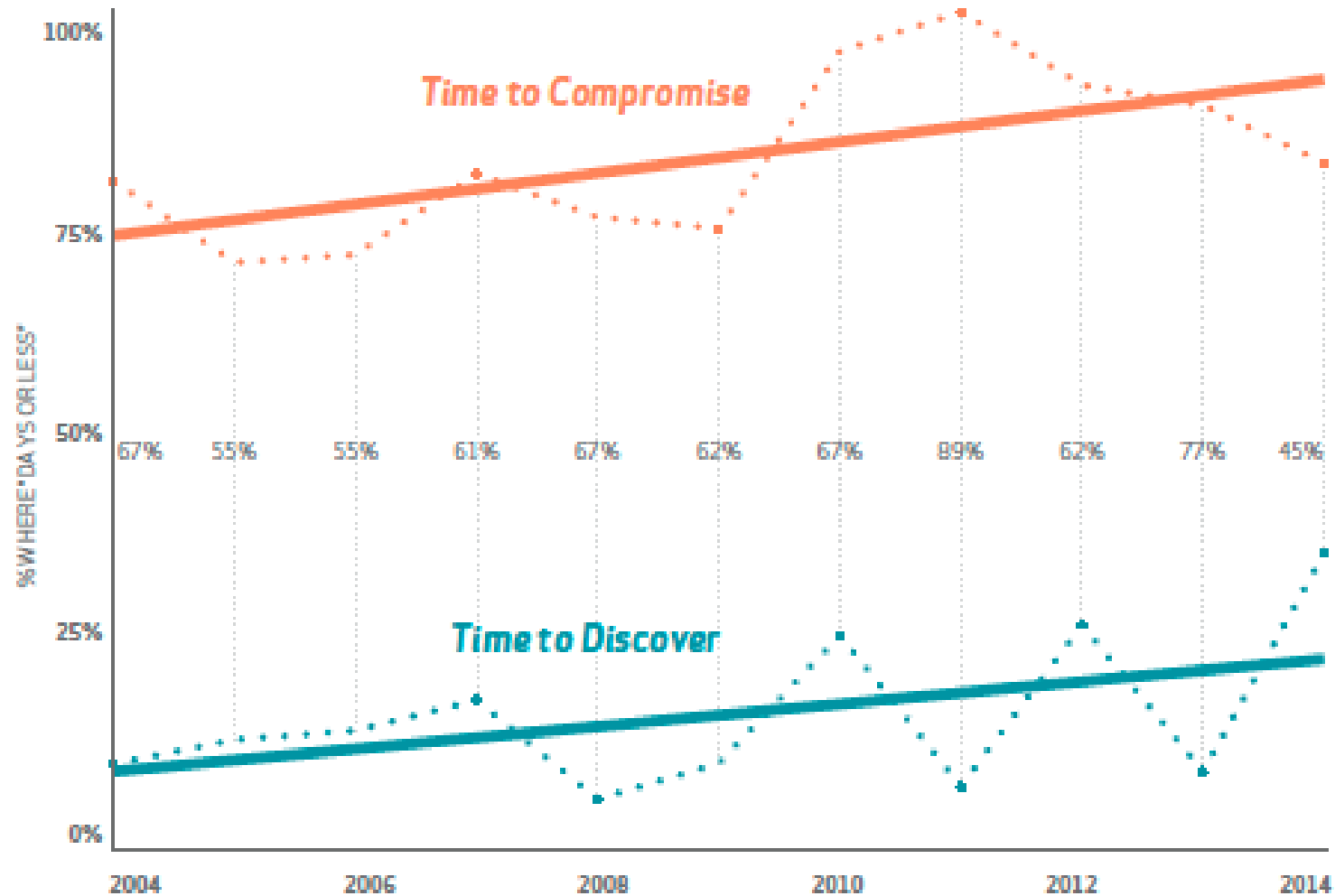




- 60% of attacks don't use malware
- 3% overlap of indicators
- Most indicators have a lifetime of only 1 day
- 60% of organisations compromised within minutes
- Very few breaches are detected using IOCs



Race





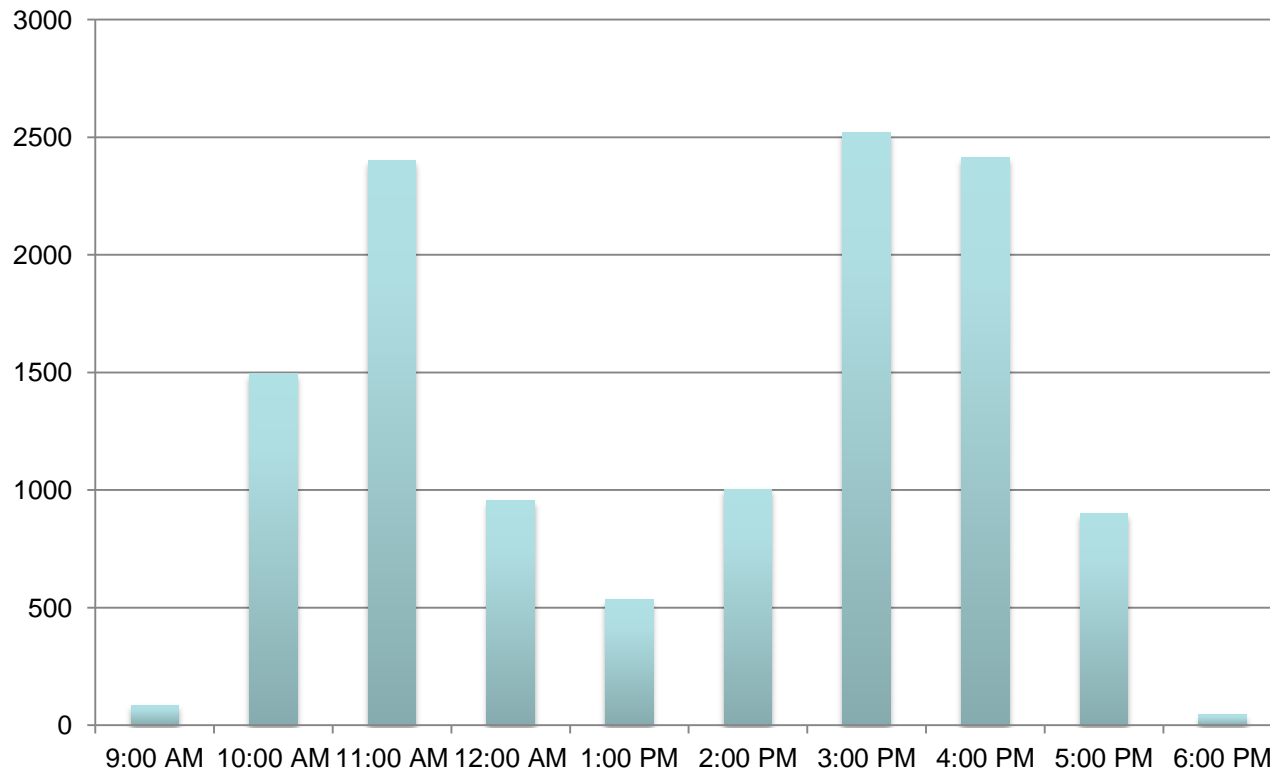
- Technical indicators of compromise very short-lived
 - Domains: Very high number of domains, freshly registered
 - IPs: Changing: active, parking, legit
 - MD5: Victim-specific signatures
 - Email metadata: changing on a daily basis
- Blending in with the user
 - User agent
 - Proxy credentials
 - Legitimate accounts (also admins)
 - Timing / batch processing
 - Legitimate domains as C&C



	Teleramafr.com	Lemondebe.org	istafrica2013	belgiquede.com	belgabe.com
26-Apr-13	198.100.113.60				
26-Apr-13	None				
8-May-13	198.100.113.60				
14-May-13			193.43.125.242		
20-May-13	65.55.57.21		65.55.57.29		
21-May-13				192.69.237.25	
30-May-13	192.69.237.25	216.158.76.216	216.158.76.216	93.46.8.89	142.4.40.230
12-Jun-13	193.191.245.4	68.232.45.233	193.43.125.242		93.94.105.162
6-Jul-13	108.62.206.68		108.62.206.68		
19-Jul-13	193.43.125.242		193.43.125.242		
31-Jul-13				122.10.83.51	
25-Aug-13		198.100.114.14			
6-Sep-13		122.10.83.51			
30-Sep-13		103.246.244.196		103.246.244.196	103.246.244.196
24-Oct-13					93.94.105.162
14-Dec-13		203.84.187.111		62.116.182.44	
30-Dec-13	None		None		
18-Mar-14				192.69.236.176	
31-Mar-14	137.175.36.18	137.175.36.18	137.175.36.18	137.175.36.18	137.175.36.18
28-Apr-14		50.118.255.47		50.118.255.47	
14-May-14	65.19.157.196		65.19.157.196		
19-May-14		69.46.84.51			
22-May-14		None			
3-Jun-13		50.117.115.84			
15-Jun-14		None			None
27-Jun-14	None		None	59.24.3.173	
21-Jul-14				50.118.255.47	
2-Aug-14				173.193.106.11	
1-Feb-15	For sale	Sinkholed	For sale	192.199.250.138	For sale



Connections



May 2014

Sept 2015

TOUTE l'Europe .EU

DOSSIER SPÉCIAL

ÉLECTIONS EUROPÉENNES
RÉSULTATS & ANALYSES

En ce moment
Elections européennes 2014 | Commission 2014-2019 | Ukraine

L'Union européenne | Les Etats membres | Les politiques européennes

A LA UNE
Elections européennes :
Les estimations des résultats en France

WakeNet3-Europe
A network on Aircraft Wake Turbulence

WakeNet-Europe

Home |

WakeNet
NEW: Research Needs Rep
Workshop 2015
Workshop 2014
Workshop 2013
WNSE Partners
WNSE Task Groups
WNSE Workshops
Previous WakeNets
Wake Vortex Projects
Publications
Contact
Sitemap
Login/Logout

Welcome to WakeNet Europe!

This website is dedicated to the topic of aircraft wake turbulence and has been created as part of the WakeNet3-Europe Coordination Action project. After having served the community for more than four years between April 2008 and July 2012, the WakeNet3-Europe project is now terminated.

As of today, no project in succession has been funded. But despite the funded project no longer

State Border Guard Service of Ukraine

Hotline
+38 (044) 527-63-63

ABOUT AGENCY | ACTIVITY | PUBLIC APPEALS | ACCESS TO PUBLIC INFORMATION | CONTACTS

Management | Main tasks | Structure | Symbolics | History

14 January 2016
In the framework of bribery control the State Border Guard Service of Ukraine is being actively reformed and prevents corruption in the SBGS

11 November 2015
The situation in checkpoints of entry and exit on the line of demarcation in the area of ATO

09 November 2015
Two citizens of Uzbekistan attempted to bribe border guards at "Boryspil" airport

20 August 2015
Border guards caught four violators in Zakarpattia

Actual News

Border guards detained 4 citizens of Somalia in Bukovyna

18 August 2015
Within the "Frontier-2015" joint operation yesterday the border guards and the representatives of the Security Service of Ukraine have detained four illegal migrants in Bukovyna.

Nov 2015

State Border Guard Service of Ukraine

Hotline
+38 (044) 527-63-63

ABOUT AGENCY | ACTIVITY | PUBLIC APPEALS | ACCESS TO PUBLIC INFORMATION | CONTACTS

Management | Main tasks | Structure | Symbolics | History

14 January 2016
In the framework of bribery control the State Border Guard Service of Ukraine is being actively reformed and prevents corruption in the SBGS

11 November 2015
The situation in checkpoints of entry and exit on the line of demarcation in the area of ATO

09 November 2015
Two citizens of Uzbekistan attempted to bribe border guards at "Boryspil" airport

20 August 2015
Border guards caught four violators in Zakarpattia

Actual News

Border guards detained 4 citizens of Somalia in Bukovyna

18 August 2015
Within the "Frontier-2015" joint operation yesterday the border guards and the representatives of the Security Service of Ukraine have detained four illegal migrants in Bukovyna.

KОРДОН On-Line





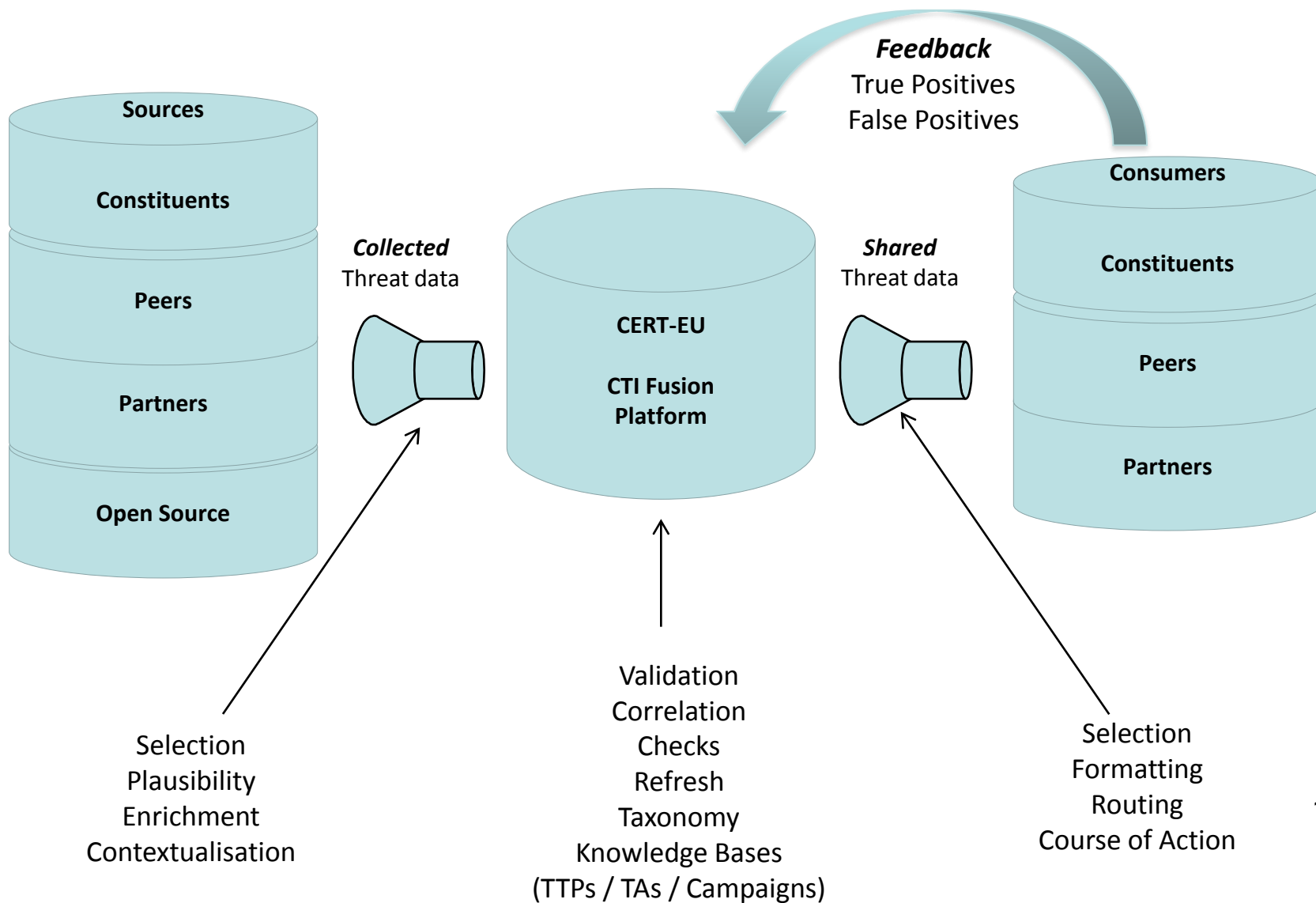
- Large diversity of information sources
- Formatted, unformatted, PDF
- Massive overload of information
- Overwhelming amount of irrelevant information
- Accuracy not guaranteed
- Unclear timing
- Unclear sighting or targeting
- Large number of false positives
- Difficult prioritisation
- **Drowning the real positives**



- Limited human resources
 - Specific IT security tools
 - Limited capacity for the implementation of detection rules
 - Specific security policies
-
- Automation / Routing
 - Minimise false-positives (in fact they prefer no positives...)
 - Prioritisation on alerts
 - Actionable context when needed



Workflow





Technical checks (automated)

- Constituent & Partners ranges
- TLD/SLD check
- Alexa ranking
- YARA validator

Contextualisation

- Timing
- Targeting
- Kill chain

Source

- Reliability
- Redundancy

Correlations

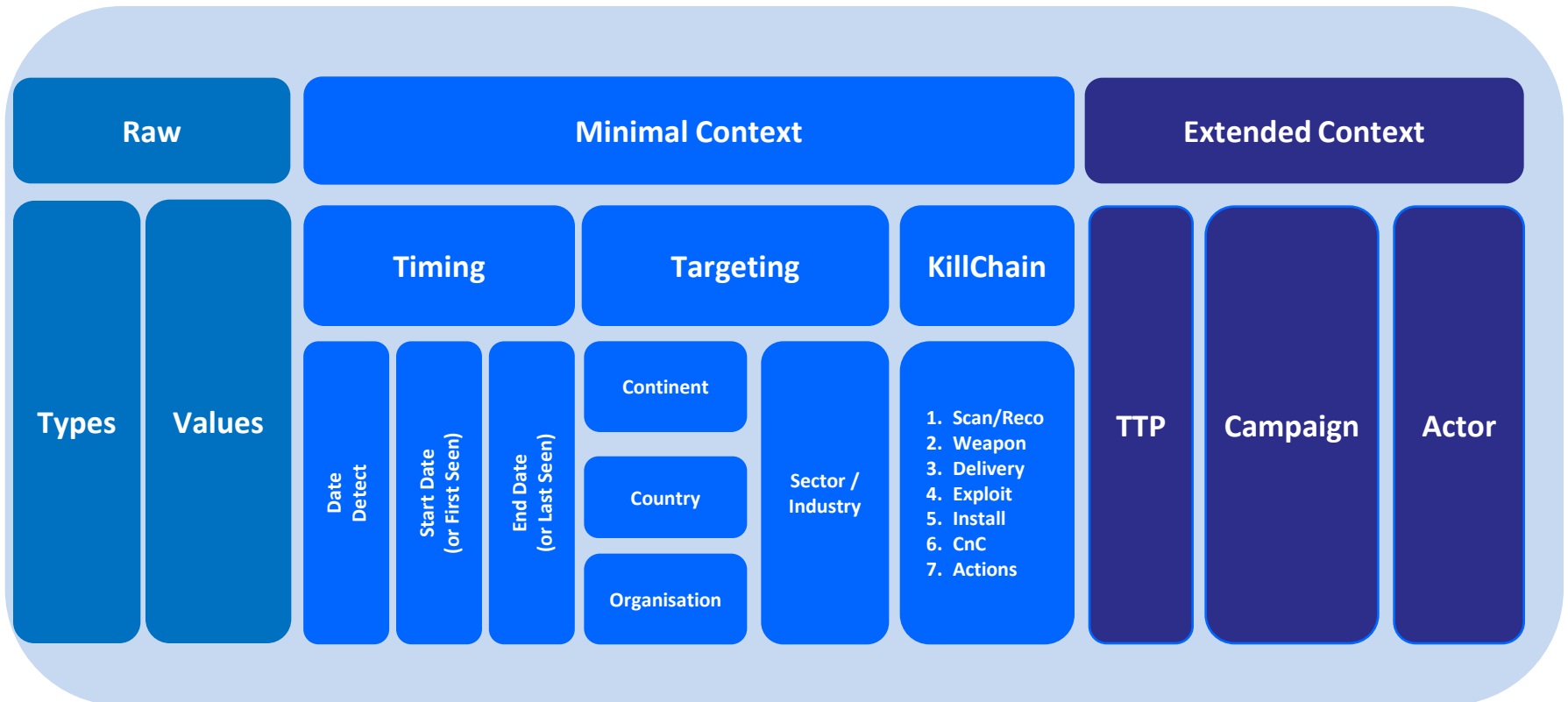
- Provided
- Detected
- Researched

Risk

- Targeting / promixity
- Threat level



Contextualisation





Minimal Context : Poor

```
csdns.com Domain
cs.com Domain
analytics.dynaliacs.com Domain
lash.js URL
48.222 IP Address
51.43 IP Address
41.175 IP Address
8.196 IP Address
mg.ca Domain
mg.ca Domain
mg.ca Domain
ymg.ca Domain
rg.tw Domain
ymg.ca Domain
yandexru.com Domain
yandexru.com Domain
124.56 IP Address
55.122 IP Address
120.16 IP Address
privacy_security.htm URL
/news/dochunter.asp?hostid= URL
stid= URL
online.asp?hostname= URL
48.125 IP Address
216.124 IP Address
```

Contextualisation

Timing	✗
Detect_date	
First seen	
Last seen	
KillChain	✗
Targeting	✗
Geoloc	
Sector	

- Block traffic to the following domains:

- arabooks.ch
- artas.org
- tsoftonline.com
- www.eamtm.com
- news.grouptumbler.com

- Block traffic to the following IPs:

- 200.63.46.23
- 194.38.160.153
- 95.128.72.24
- 72.34.47.186
- 188.40.99.143
- 85.95.236.114

Contextualisation

Timing	✗
Detect_date	
First seen	
Last seen	
KillChain	✗
Targeting	✗
Geoloc	
Sector	



Exploit files

First seen (YYYY-MM-DD)	Filename	SHA1	Size
2013-11-04	-	353540c6619f2bba2351babad736599811d3392e	946124
2014-03-20	nota.pdf	5295b09592d5a651ca3f748f0e6401bd48fe7bda	917093
2014-03-14	dip.mail march.pdf	c671786abd87d214a28d136b6bafd4e33ee66951	919914
2014-03-11	Bulletin-PISM-No-31-(625)-March-10-2014.pdf	65681390d203871e9c21c68075dbf38944e782e8	917093
2014-03-05	March.pdf	8949c1d82dda5c2ead0a73b532c4b2e1fbb58a0e	908285
2013-07-01	paper_format.pdf	74bc93107b1bbae2d98fca6d819c2f0bbe8c9f8a	917093

Droppers

First seen (YYYY-MM-DD)	Filename	SHA1	Compiled (All times in UTC)	Size
2014-04-27	rcs.DSC_1365527283.jpg	f621ec1b363e13dd60474fcfab374b8570ede4de	Fri Aug 2 10:50:12 2013	430080
2014-03-18	rcs.18.jpg	7631fdb92e61504596790057ce674ee90570755	Fri Aug 2 10:50:12 2013	811008
2014-03-13	rcs.Ukraine-Gas-Pipelines-Security-Report-March-2014.pdf	5a199a75411047903b7ba7851bf705ec545f6da9	Fri Aug 2 10:50:12 2013	942080
2013-11-11	rcs.3aka3.doc	0e5f55676e01d8e41d77cdc43489da8381b68086	Fri Aug 2 10:50:12 2013	405504

Contextualisation

Timing	✓
Detect_date	✓
First seen	✓
Last seen	✓
KillChain	✓
Targeting	✗
Geoloc	
Sector	



SECURELIST

THREATS ▾

CATEGORIES ▾

TAGS ▾

The Banking Trojan Emotet: Detailed Analysis

By [Alexey Shulmin](#) on April 9, 2015. 2:00 pm

hxxp://200.210.10.110
hxxp://88.80.187.139
hxxp://188.93.174.136
hxxp://130.133.3.7
hxxp://100.111.70.100

Contextualisation

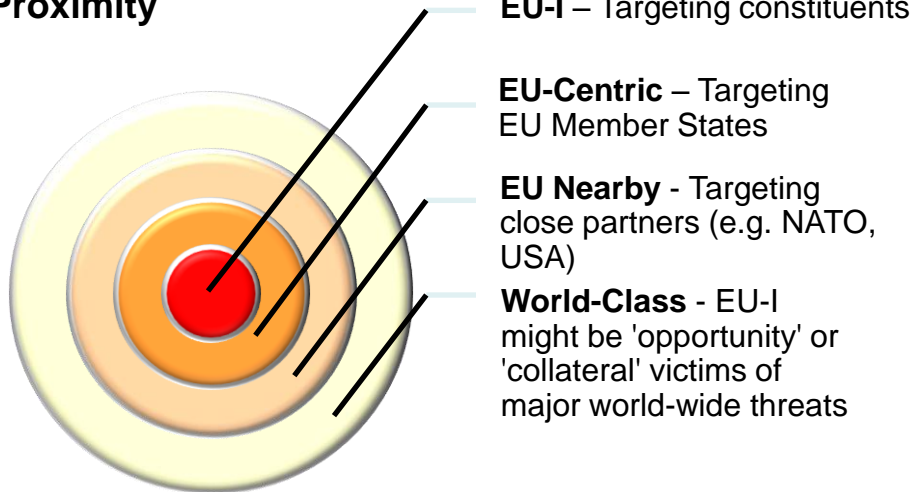
Timing	✓
Detect_date	
First seen	✓
Last seen	✓
KillChain	✓
Targeting	✗
Geoloc	
Sector	

Resolve	First	Last	Source
crl.microsoft.com	2014-10-21 12:11:00	2015-07-21 10:54:00	kaspersky
ardownload.adobe.com	2014-10-19 23:10:00	2015-07-21 10:46:00	kaspersky
fbexternal-a.akamaihd.net	2014-10-21 15:16:00	2015-07-21 10:22:00	kaspersky

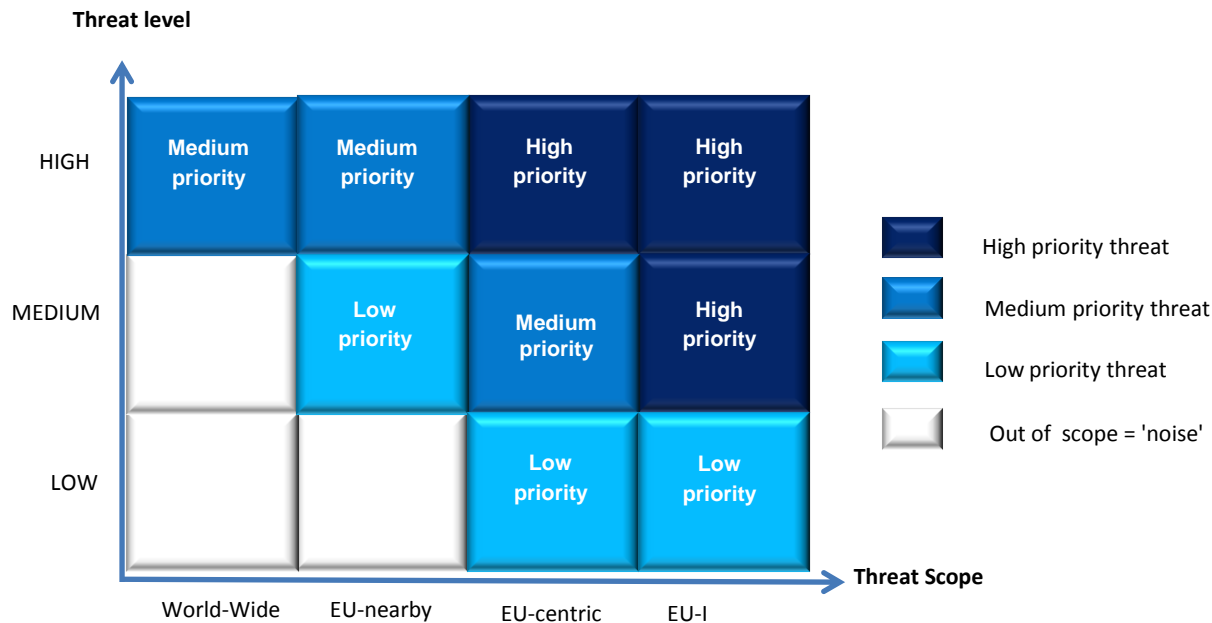
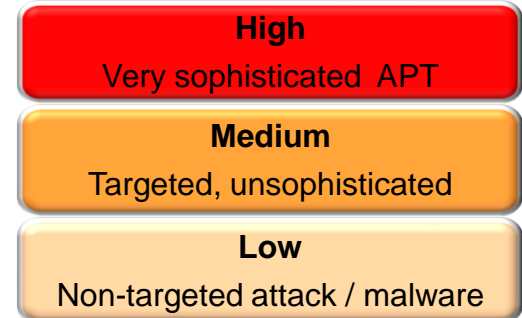


Proximity / Threat Level

Proximity



Threat Level



SECURELIST

THREATS ▼ CATEGORIES ▼ TAGS ▼ ENCYCLOPEDIA

The Naikon APT

Tracking Down Geo-Political Intelligence Across APAC, One Nation at a Time

Our recent report, "The Chronicles of the Helsing APT: the Empire Strikes Back" began with an introduction to the Naikon APT, describing it as "One of the most active APTs in Asia, especially around the South China Sea".

Naikon was mentioned because of its role in what turned out to be a unique and surprising story about payback. It was a Naikon attack on a Helsing-related organization that first introduced us to the Helsing APT. Considering the volume of Naikon activity observed and its relentless, repeated attack attempts, such a confrontation was worth looking into, so we did.



The **#NaikonAPT group** was spear-phished by an actor we now call "Helsing"

Tweet

Tracking Down Geo-Political Intelligence Across APAC Victims of the Naikon cyberespionage group

Government Civil organizations Military organizations



© 2015 Kaspersky Lab

GREAT KASPERSKY

Below is a partial list of organizations affected by Naikon's "operator X's" espionage campaign in country X.

- Office of the President
- Military Forces
- Office of the Cabinet Secretary
- National Security Council
- Office of the Solicitor General
- Intelligence Services
- Civil Aviation Authority
- Department of Justice
- Federal Police
- Executive/Presidential Administration and Management Staff

WHO - Threat name

→ Threat Actor



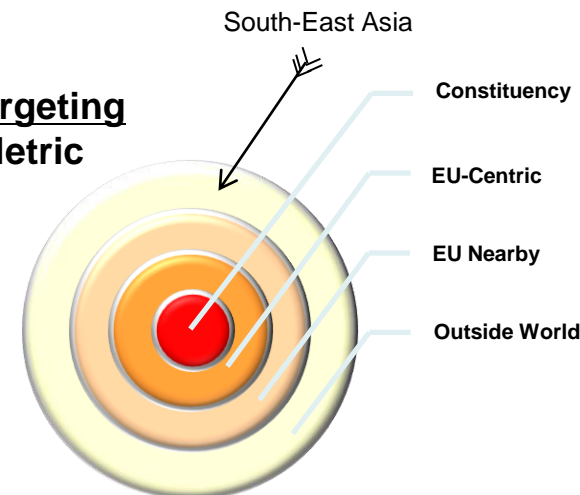
WHAT - Campaign

→ Cyber Espionage



WHERE - Geographical targeting

→ 1st Threat Proximity Metric



WHERE - Sectoral targeting

→ 2nd Threat Proximity Metric



Extended Context — Example 1

Payload

The main module is a remote administration utility. Using SSL, the module establishes a reverse connection to the C&C server as follows: it sets up an outgoing connection to the C&C server and checks if there is a command that it should execute. If there is, it executes the command and returns the result to the C&C. There are 48 commands in the module's repertoire, which a remote operator can use to effectively control the victim computer. This includes taking a complete inventory, downloading and uploading data, installing add-on modules, or working with the command line.

d085ba82824c1e61e93e113a705b8e9a	118272	Aug 23 18:46:57 2012
b4a8dc9eb26e727eafb6c8477963829c	140800	May 20 11:56:38 2013
172fd9cce78de38d8cbcad605e3d6675	118784	Jun 13 12:14:40 2013
d74a7e7a4de0da503472f1f051b68745	190464	Aug 19 05:30:12 2013
93e84075bef7a11832d9c5aa70135dc6	154624	Jan 07 04:39:43 2014

Command & Control

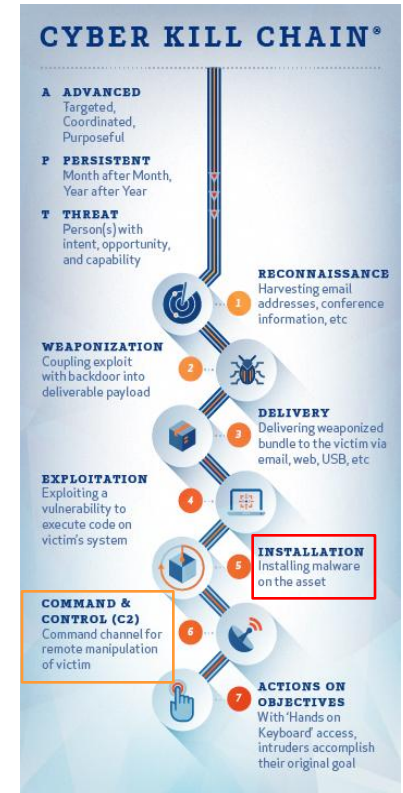
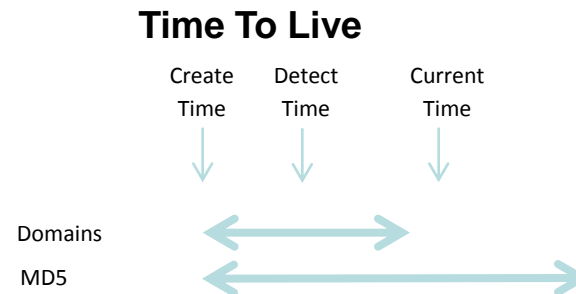
Here is a partial list of C&C servers and victim locations, demonstrating the geo-specific correlation:

ID	Jakarta	linda.googlenow.in
ID	Jakarta	admin0805.gnway.net
ID	Jakarta	free.googlenow.in
ID		frankhere.oicp.net
ID	Bandung	frankhere.oicp.net
ID	Bandung	telcom.dhtu.info
ID	Jakarta	laotel08.vicp.net
JP	Tokyo	greensky27.vicp.net
KH		googlemm.vicp.net
KH	Phnom Penh	googlemm.vicp.net
MM		peacesyou.imwork.net
MM		sayakyaw.xicp.net
MM		ubaoyouxiang.gicp.net
MM	Yangon	htkg009.gicp.net

HOW – TTP & Kill Chain



WHEN – Timing



Contextualisation

Timing	✓
Detect_date	✓
Start_date	✓
End_date	N/A
KillChain	✓
Targeting	✓
Geoloc	✓
Sector	✓



FireEye Intelligence Exchange Alert

The Teenage Mutant Malvertiser Network

By J.Gomez | FireEye Labs

Since early 2015 FireEye Labs has observed a highly **active malvertising** operation involving Bedep ad fraud activity and malicious redirection to Exploit Kits via a multitude of advertising and search affiliated domains. Among the exploit kits being redirected to are well known names like Angler, Magnitude, Nuclear and Rig, each redirection to an EK sharing a common link. We believe this particular operation has been active since at least **mid 2014**, if not prior, and is still very active at time of this writing.

...

by the "click2." prefixed sub domains alone.

Some of the most active destination (or cushion servers as they are commonly referred to) domains leading to EK's include but are not limited to the following, as you will notice some domains redirect to more than one EK.

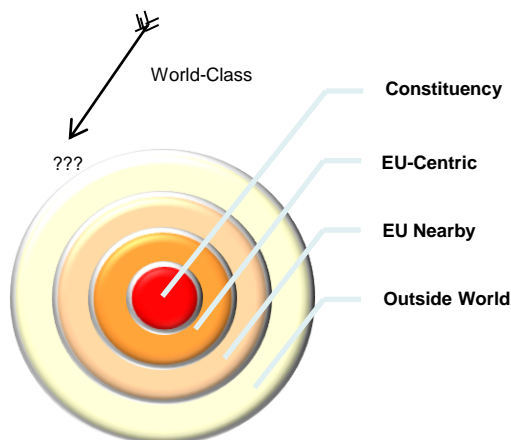
Angler	Magnitude	Nuclear	Rig / Other
ads.fsinc.biz	click2.systemaffiliate.com	click2.systemaffiliate.com	click2.systemaffiliate.com
hit.buy-targeted-traffic.com	click2.danarimedia.com	news4news015.com	buyadvertort.com
bbwlebsians.xblog.in	ado-global.com	news4news14.com	buyadvertview.com
find-everything.info	ads.fsinc.biz	news4news15.com	buyadvlst.com
little-finder.me	click.upperseeker.com	news4news2014.com	dealsadvdeals.com
megafinder24.info	death-tostock.com	news4news2015.com	dealsadvdeals.com
searchl.org	find-all.biz		dealsadvdeals.com
searchwebfind.org	find-everything.info		dealsadvdeals.com
truesearchresults.com	global-search24.biz		dealsadvdeals.com
webwebfind.com	integrosearch.com		dealsadvdeals.com
news4news015.com	little-finder.me		buyadvertview.com
news4news14.com	megafinder24.info		
news4news15.com	millsearch.net		
news4news2014.com	searchl.org		
news4news2015.com	searchwebfind.org		
	superior-movies.com		
	truesearchresults.com		
	webwebfind.com		

HOW – TTP & Kill Chain



WHEN

WHERE ?



Contextualisation

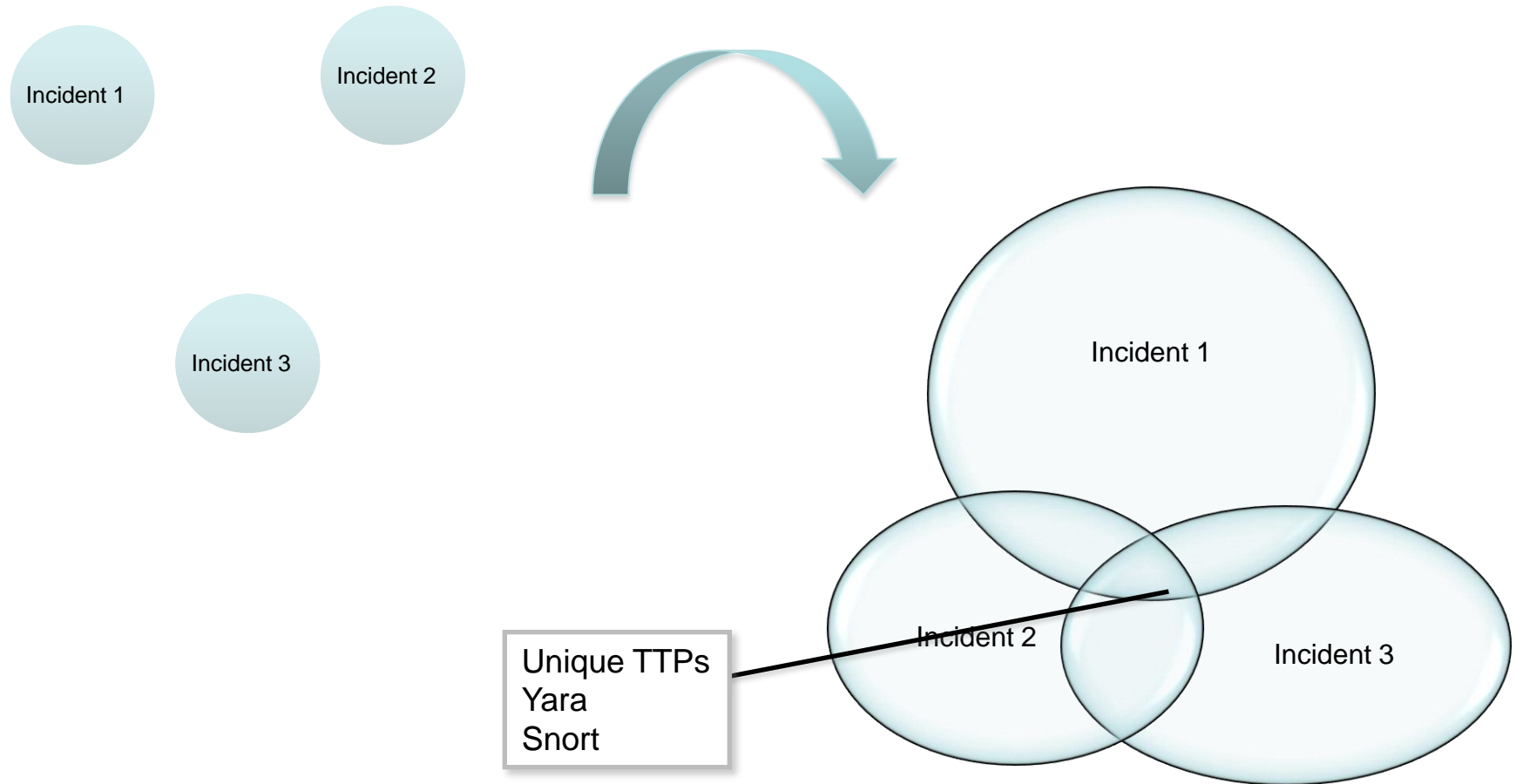
Timing	
Detect_date	✗
Start_date	
End_date	N/A
KillChain	
Targeting	✓
Geoloc	✗
Sector	



- Taxonomy
- Correlation
 - Previous incidents in the constituency
 - Previous reports
 - Intensity
 - TTPs / Actors / Campaigns
- Unique TTPs
 - Behaviour
 - Unique patterns
 - Effective detection rules



Pivoting via TTP





- Adapting the product to the audience
 - Drawing from the intell and context
 - Adapting content and format
 - Timing
- Routing / Course of Action
 - What to do (prevent, detect, block, hunt)
 - How
- Respect the sharing limitations (TLP)
- Anonymisation (sources / victims)
- Automation when possible
- Escalation when needed

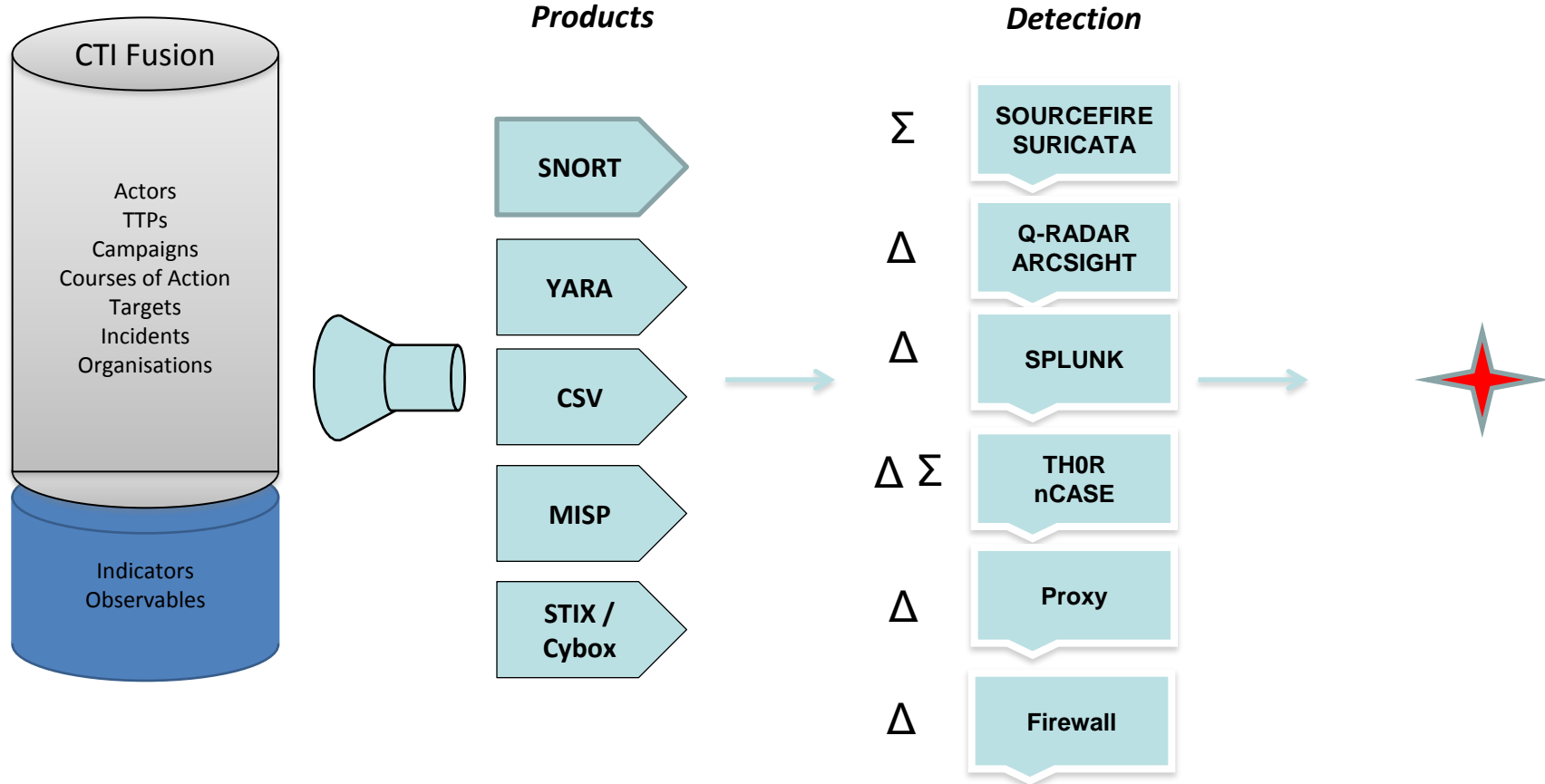


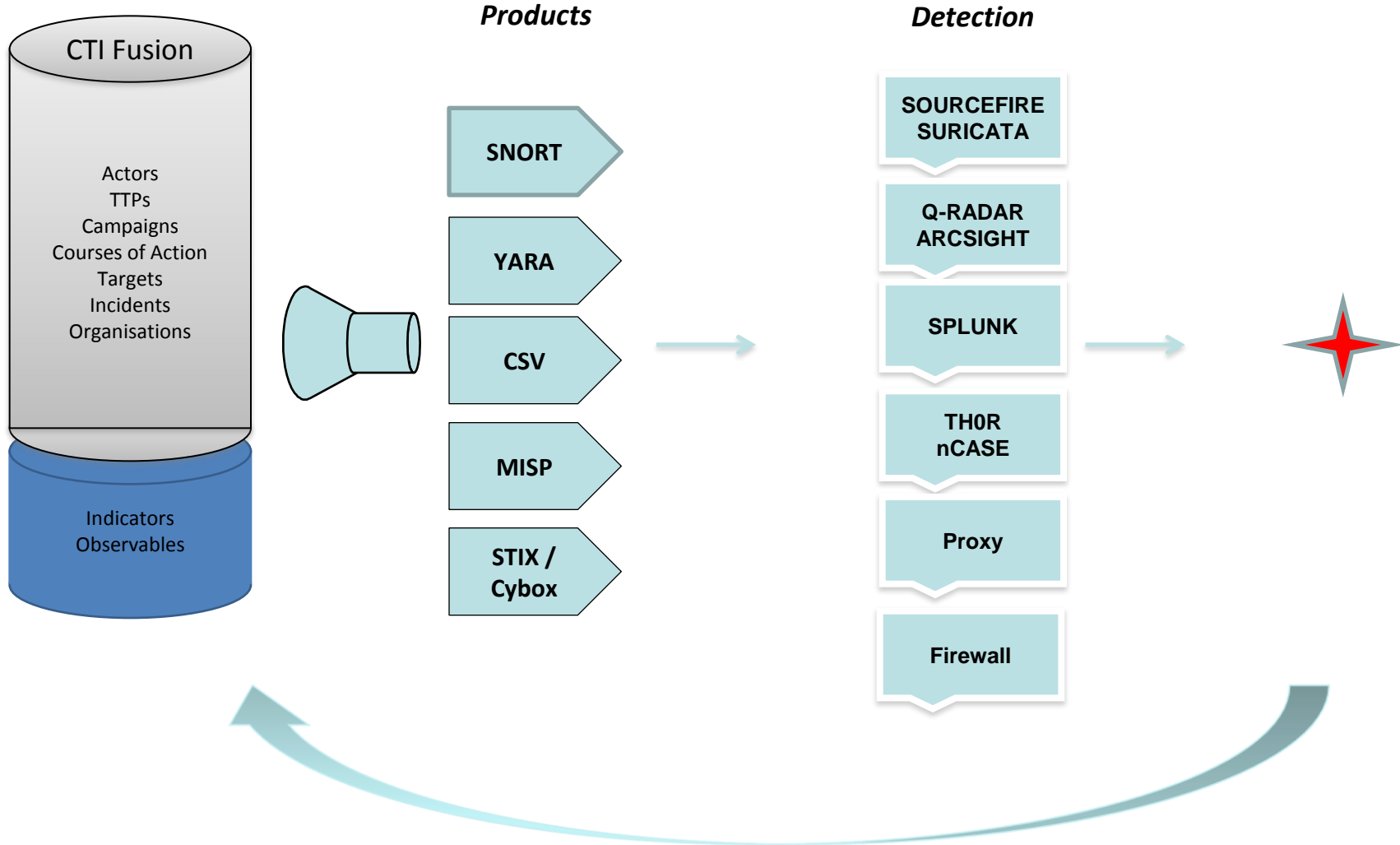
Adapting the Product to the Audience

Strategic	<ul style="list-style-type: none">• Understanding the broader context.• Strategic context: profile, motives, new techniques/tactics, sector and location of victims, business risk.• Planning high level actions for non-technical treatment of the threat.	<ul style="list-style-type: none">• CEO• Business VP• CIO	Periodic Bulletin	Threat Landscape Security Brief
Tactical	<ul style="list-style-type: none">• Understanding cyber-attacks tactical context: threat type and level, timing of events, techniques/malware.• Planning structured course of actions for permanent protection	<ul style="list-style-type: none">• CIO• Cyber-defense teams	For every significant campaign	Threat Alert Report (CITAR)
Technical	<ul style="list-style-type: none">• Immediate reaction to threats: Detection, Prevention, Reaction (eradication, recovery), Report• Dynamic feeding cyber-defense tools: IDS, IPS, SIEM, Security Scanners, Mailguard, Firewalls, etc	<ul style="list-style-type: none">• Cyber-defense teams• IT administrators (or direct tool feeding)	(Near real-time -> Towards full automation)	Indicators Signatures Rules Detection Mechanisms (CIMBL)



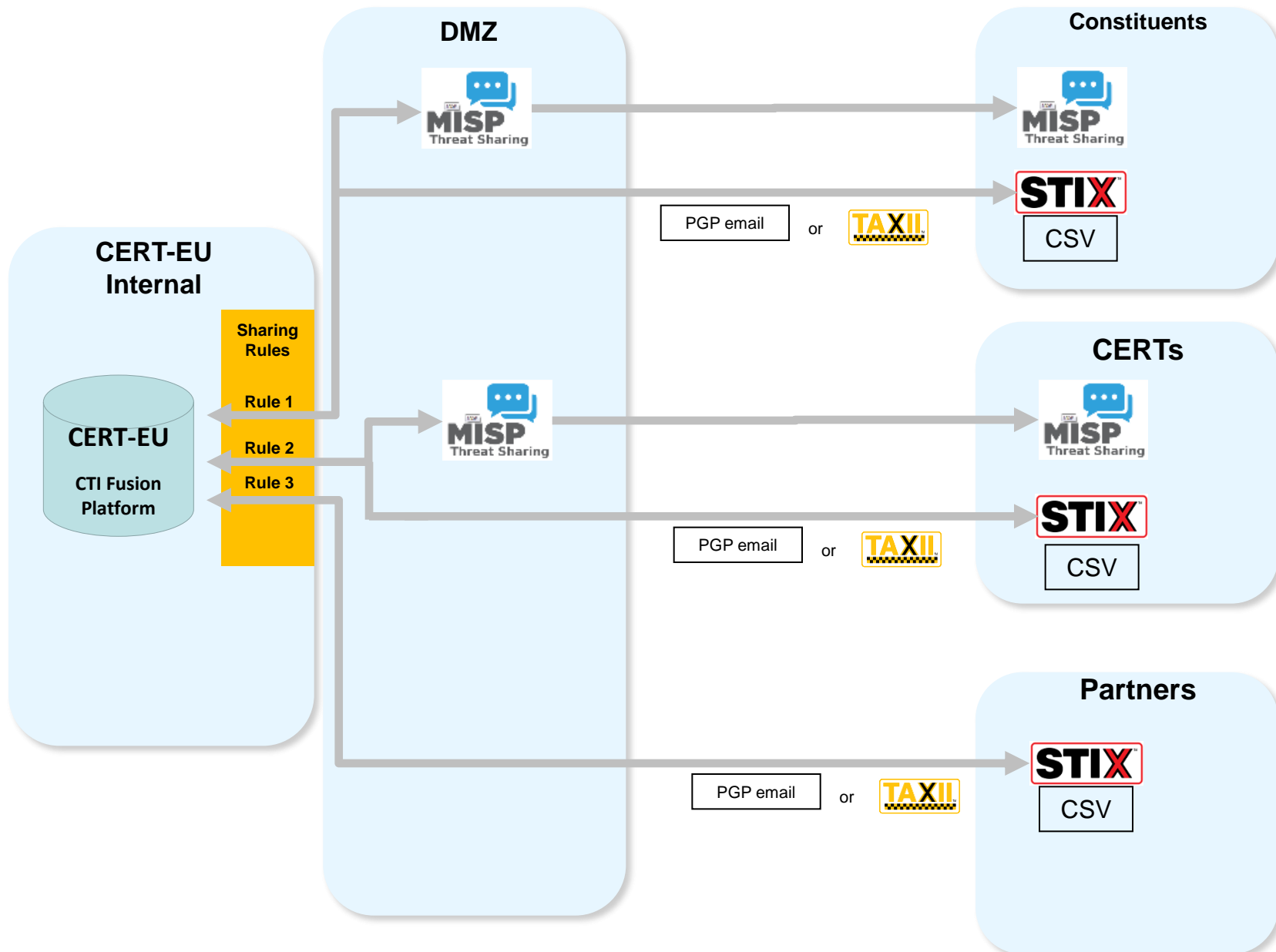
Routing / Course of Action







Sharing Groups





Sharing Rules

Sharing Groups

1. **Constituents**
2. **CERTs**
3. **Partners** (NDA)

Sharing Criteria

- *TLP*
- *Proximity*
- *Producer*

Sharing Security

- *Sharing = workflow-based*
- *Export control to avoid errors*
- *TLP enforcement*
- *Encryption*
- *Anonymisation*
- *Source security*
- *Data Protection enforcement*

Sharing Rules

Rule1 : (TLP <> RED) AND (TargetedDomain <> Outside World)

Rule 2 : (Producer = 'Constituent ' OR 'CERT-EU') AND (TLP <> 'RED')

Rule 3 : (Producer = 'Constituent ' OR 'CERT-EU') AND (TLP <> 'RED' OR 'AMBER')



- Change in proximity of a high threat actor
- Detection in the constituency of a high threat actor
- Alert + Context
- Active hunting
- « Don't wait until Monday »



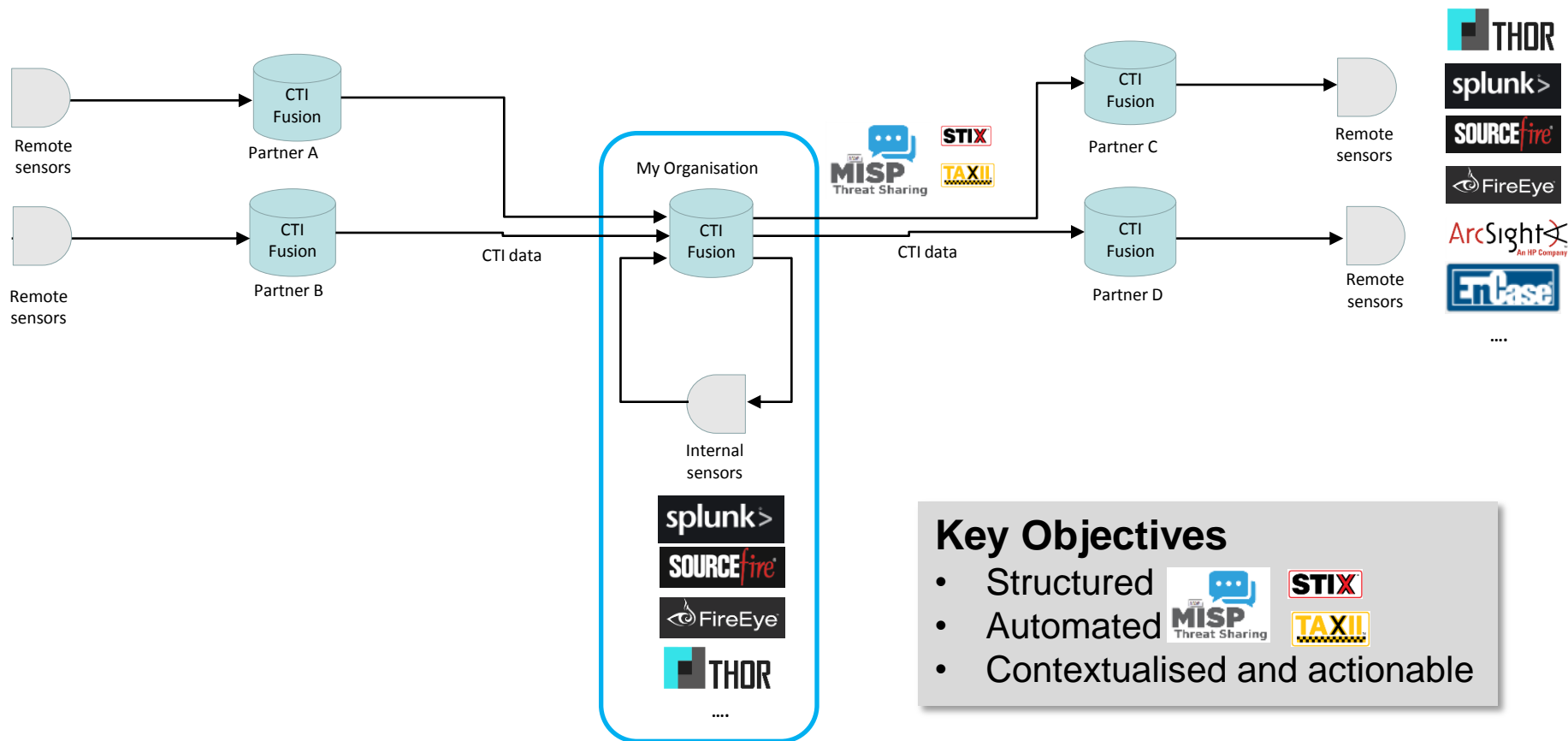
- How to manage lifetime of the data
- How to remove data downstream
 - Ageing window – Time-To-Live (TTL)
 - Feedback positives/false positives
 - Full set ('master_ioc')
- How to control sharing groups downstream
- Implement Routing / Course of Action
- How to maintain the treasure trove of TTPs
 - Dependent on human contacts



- Network of interacting CTI fusion centers
- World-wide sensor network
- Signature-less detection



Outlook - Automated End-to-end Workflow

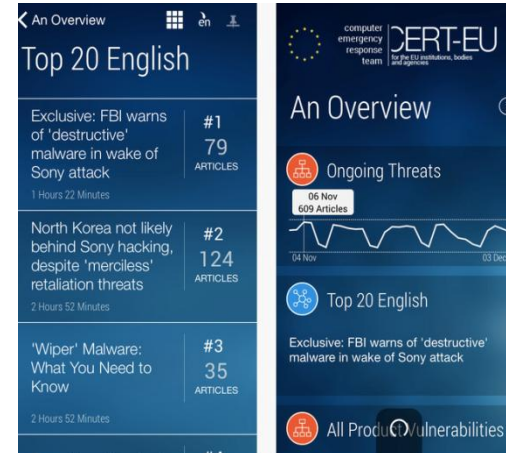


Key Objectives

- Structured
- Automated
- Contextualised and actionable



<http://cert.europa.eu/>



More On Cyber Threat Contextualisation

https://www.sstic.org/media/SSTIC2015/SSTIC-actes/contextualised_and_actionable_information_sharing_/SSTIC2015-Article-contextualised_and_actionable_information_sharing_within_the_cyber-security_community-garnier.pdf