



computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

Handling an incident in CERT-EU

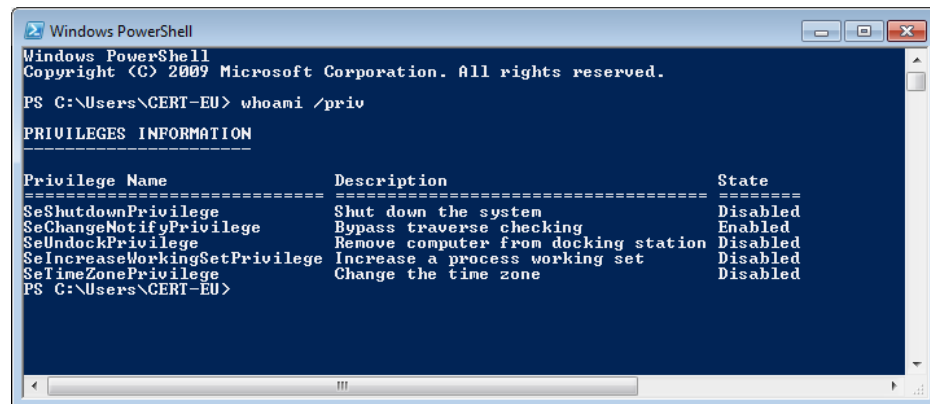
FIRST - 2017

Emilien LE JAMTEL

emilien.le.jamtel@cert.europa.eu



Introduction



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\CERT-EU> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                State
-----
SeShutdownPrivilege Shut down the system      Disabled
SeChangeNotifyPrivilege Bypass traverse checking  Enabled
SeUndockPrivilege    Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege  Change the time zone     Disabled
PS C:\Users\CERT-EU>
```



- CERT for European Institutions, Agencies, and Bodies.
- Created in 2011.
- Operational support to infrastructure teams.
- Defence against targeted cyber threats.
- Hub of information and skills.

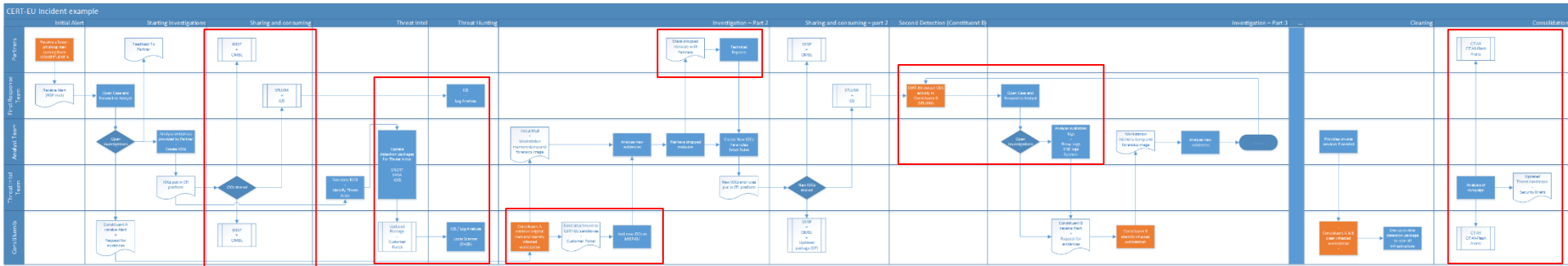


- Around 60 organisations
- From 40 – 40.000 users
- Seperate, heterogenous networks
- Cross-sectoral
 - Government, foreign policy, embassies
 - Banking, energy, pharmaceutical, chemical, food, telecom
 - Maritime, rail and aviation safety
 - Law enforcement (EUROPOL, FRONTEX, EUPOL) and justice
 -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





- Step-by-step incident case
- Focus on tools and exchange of information
 - With external entities
 - Between CERT-EU teams



- Involved parties



Partners



First Response Team



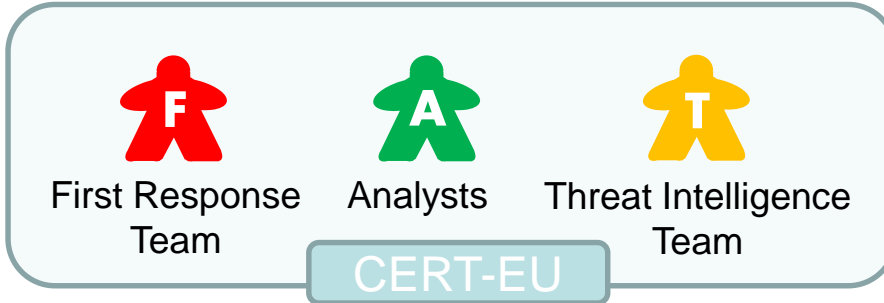
Analysts



Threat Intelligence Team



Constituents



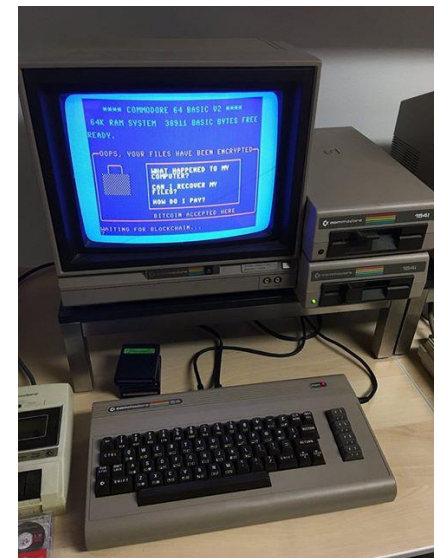


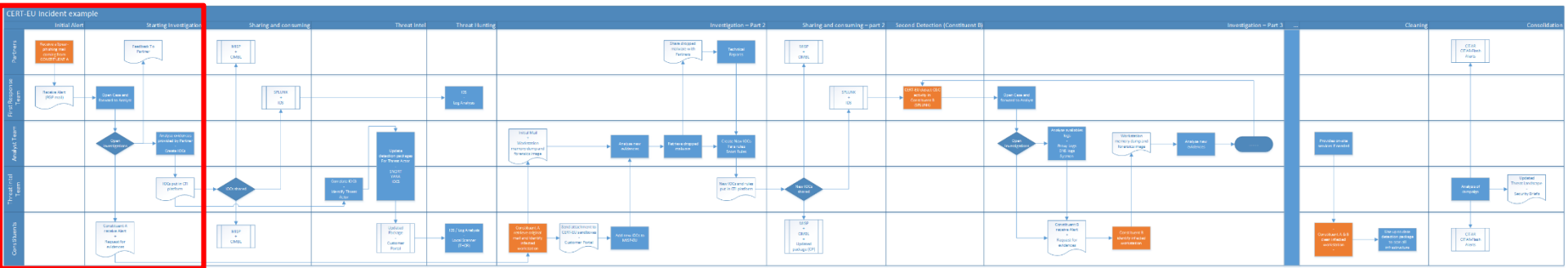
computer
emergency
response
team

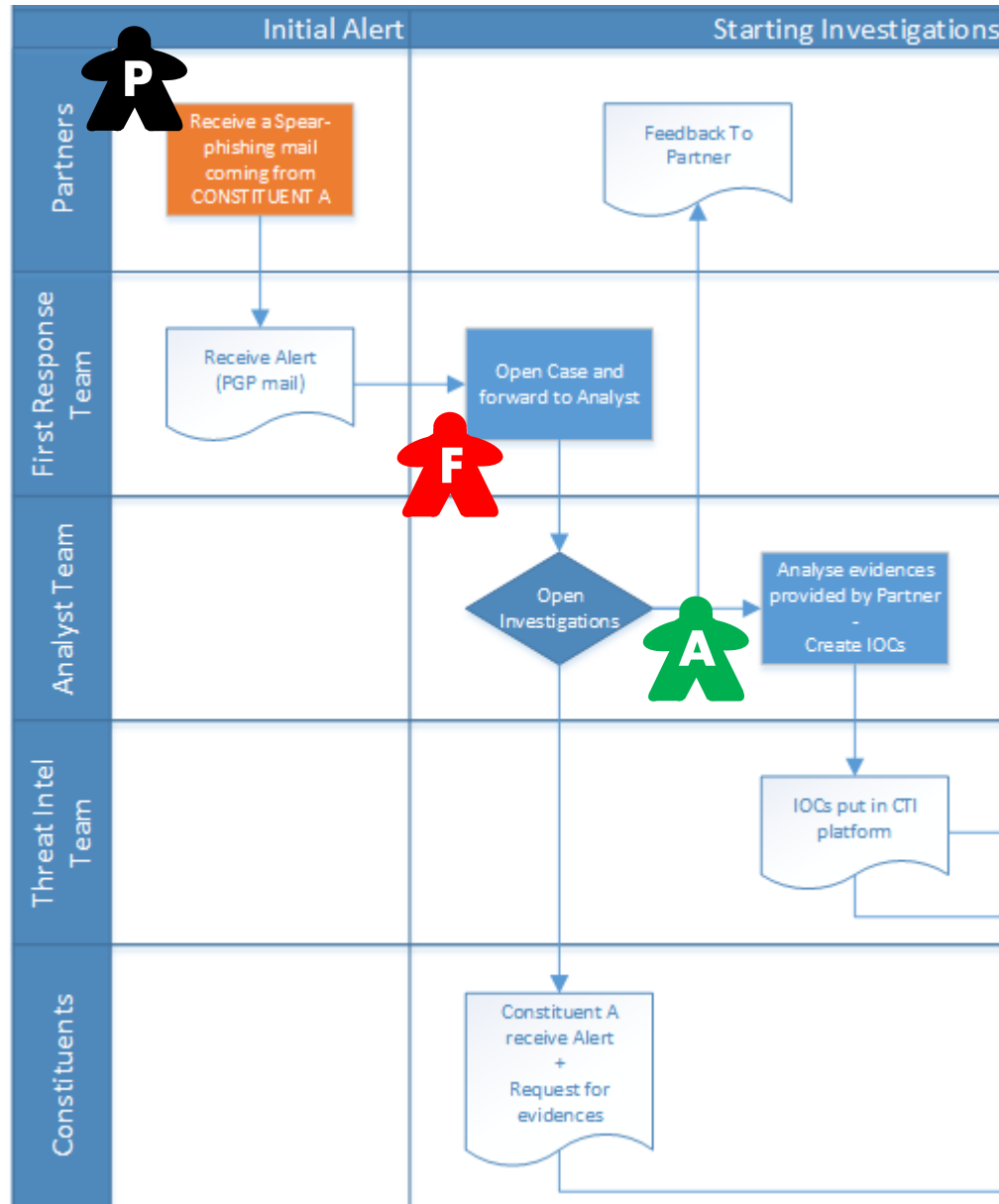
CERT-EU
for the EU institutions, bodies
and agencies

Chapter 1

Initial alert









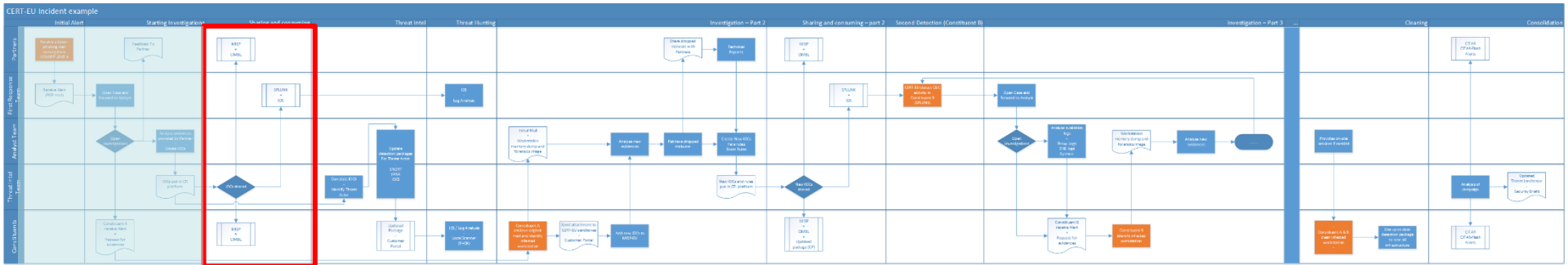
computer
emergency
response
team

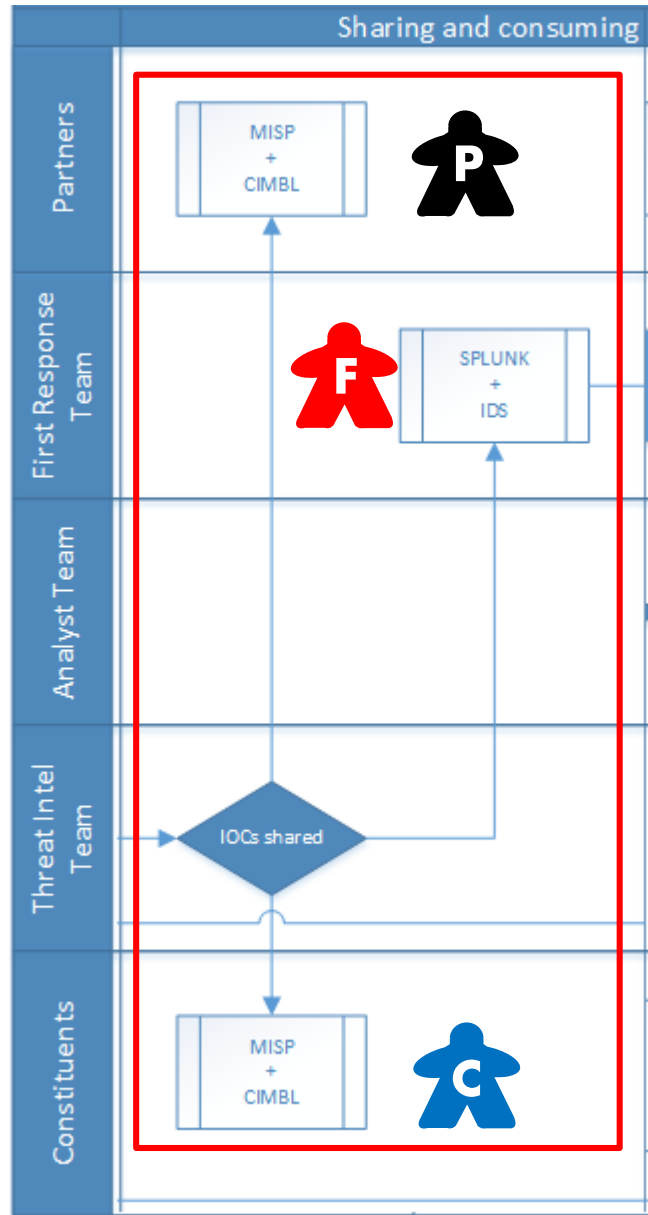
CERT-EU

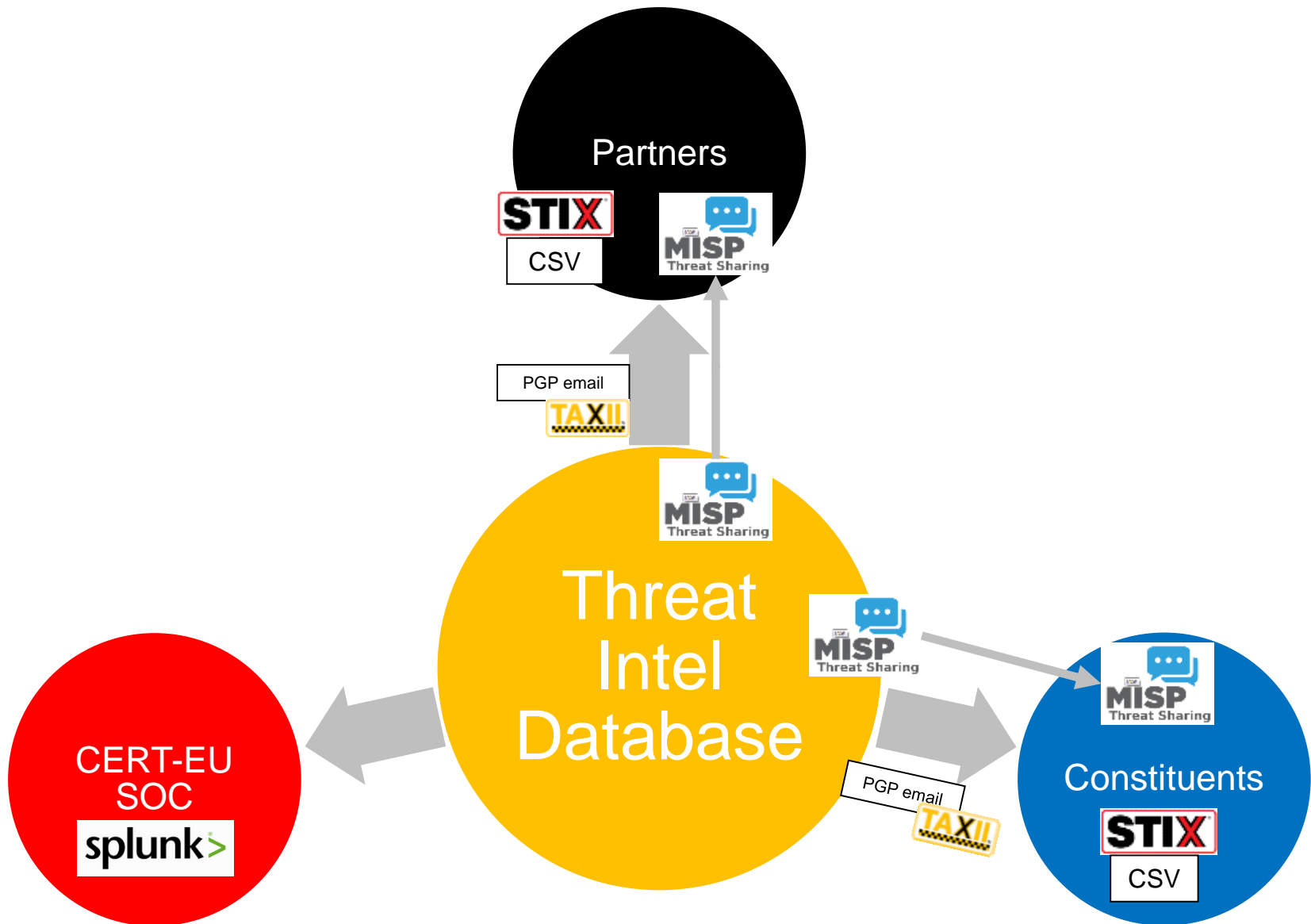
for the EU institutions, bodies
and agencies

Chapter 2 **Sharing**











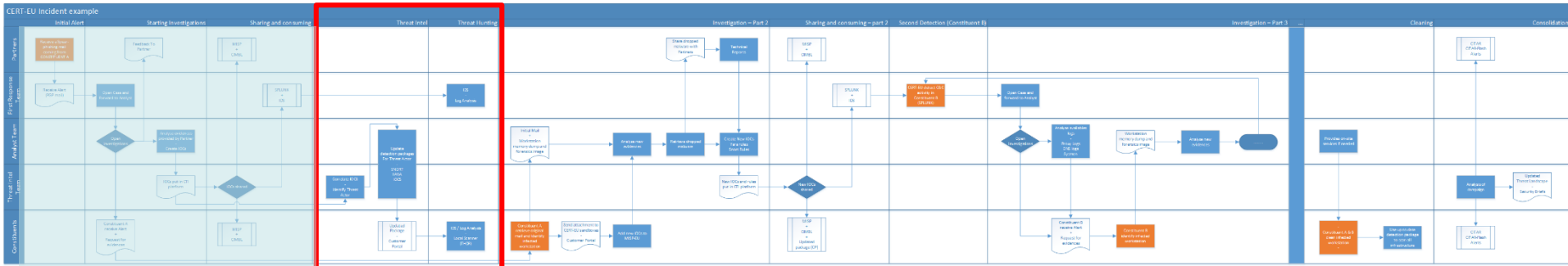
computer
emergency
response
team

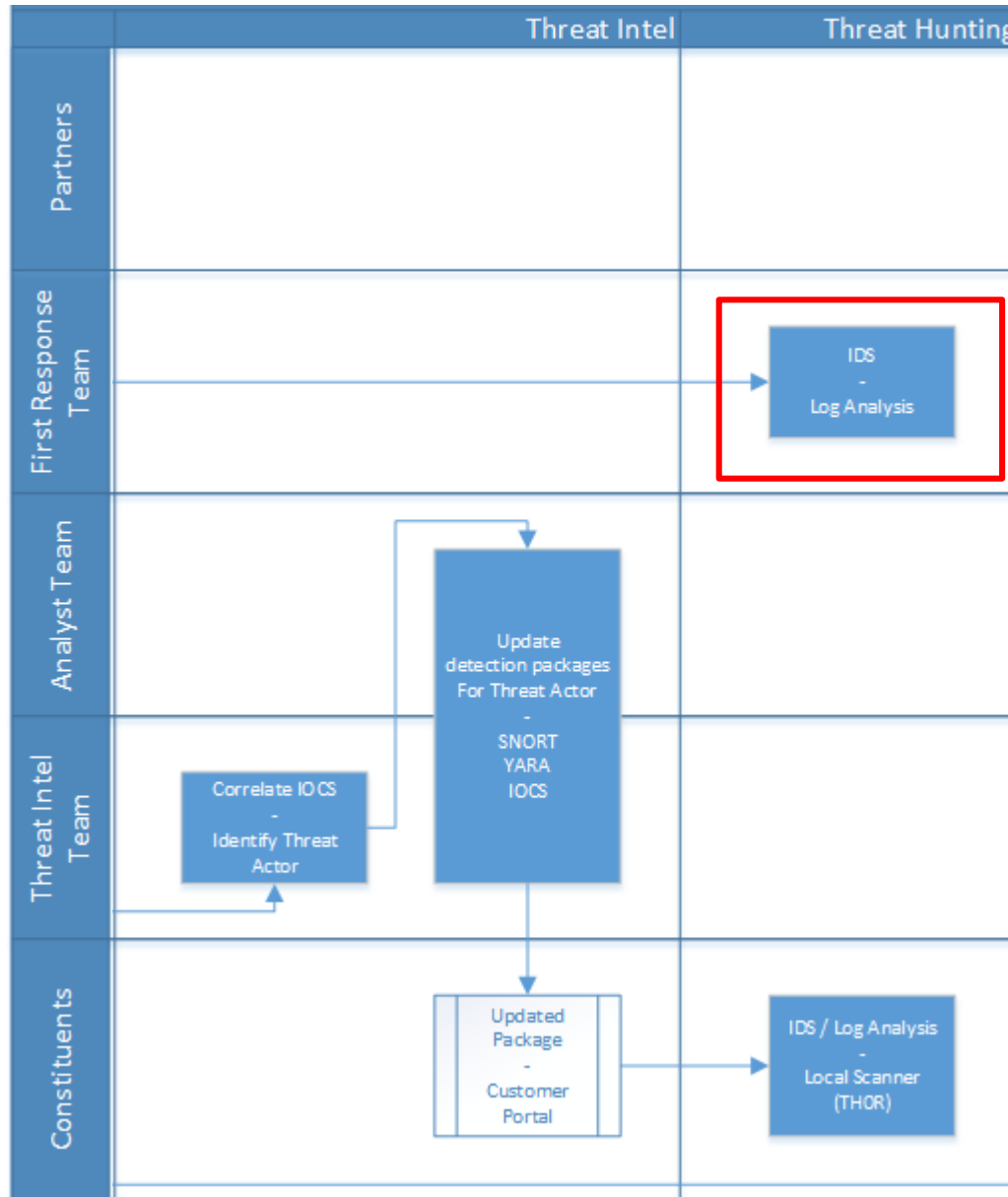
CERT-EU
for the EU institutions, bodies
and agencies

Chapter 3

Hunting



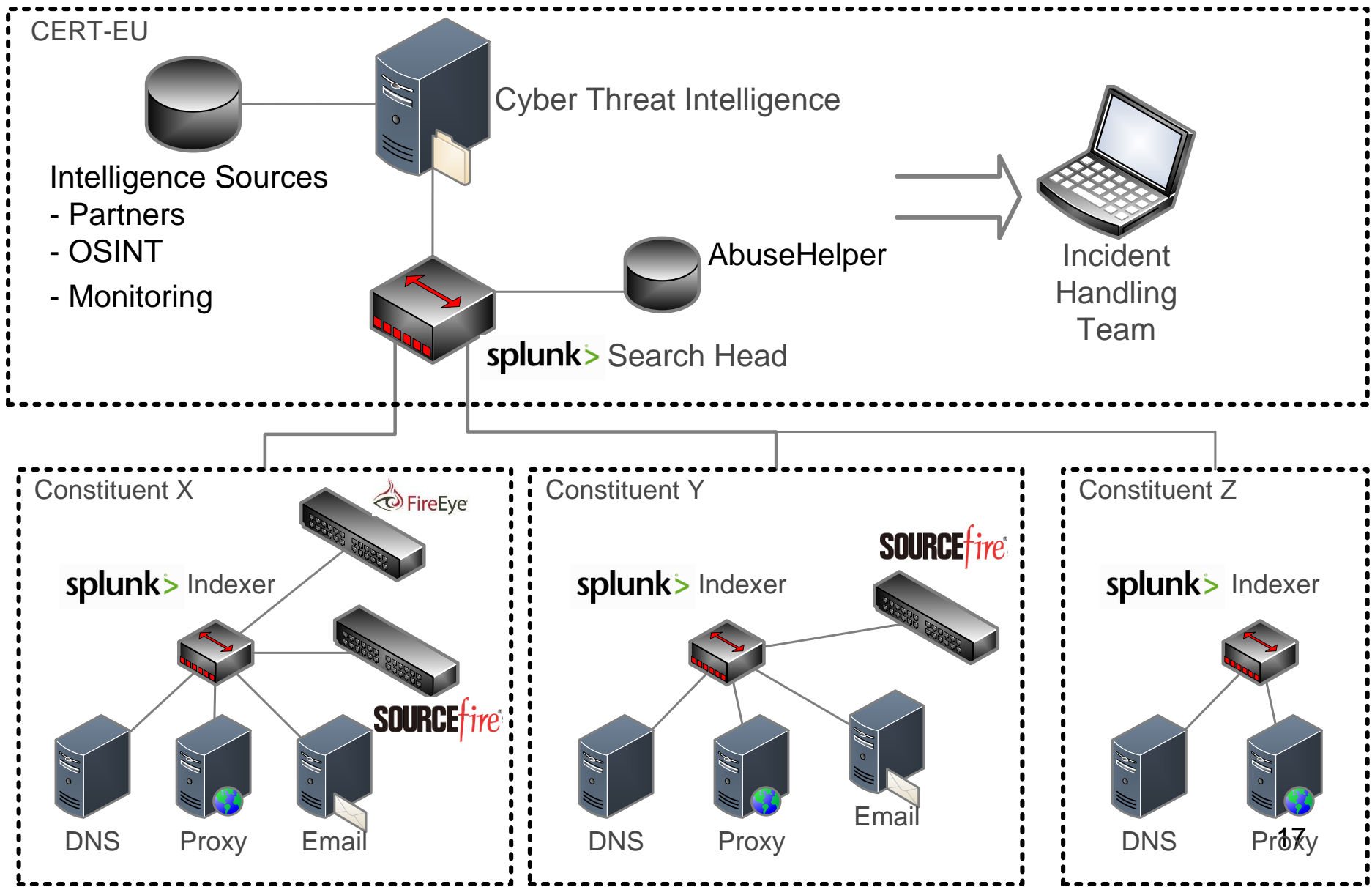






- Log management tool: **splunk**>
- IDS: **SOURCEfire**[®]
- Cyber Threat Intelligence database: **CERT-EU**
- Monitoring:





Web traffic:

- » DNS
- » Proxy

Emails:

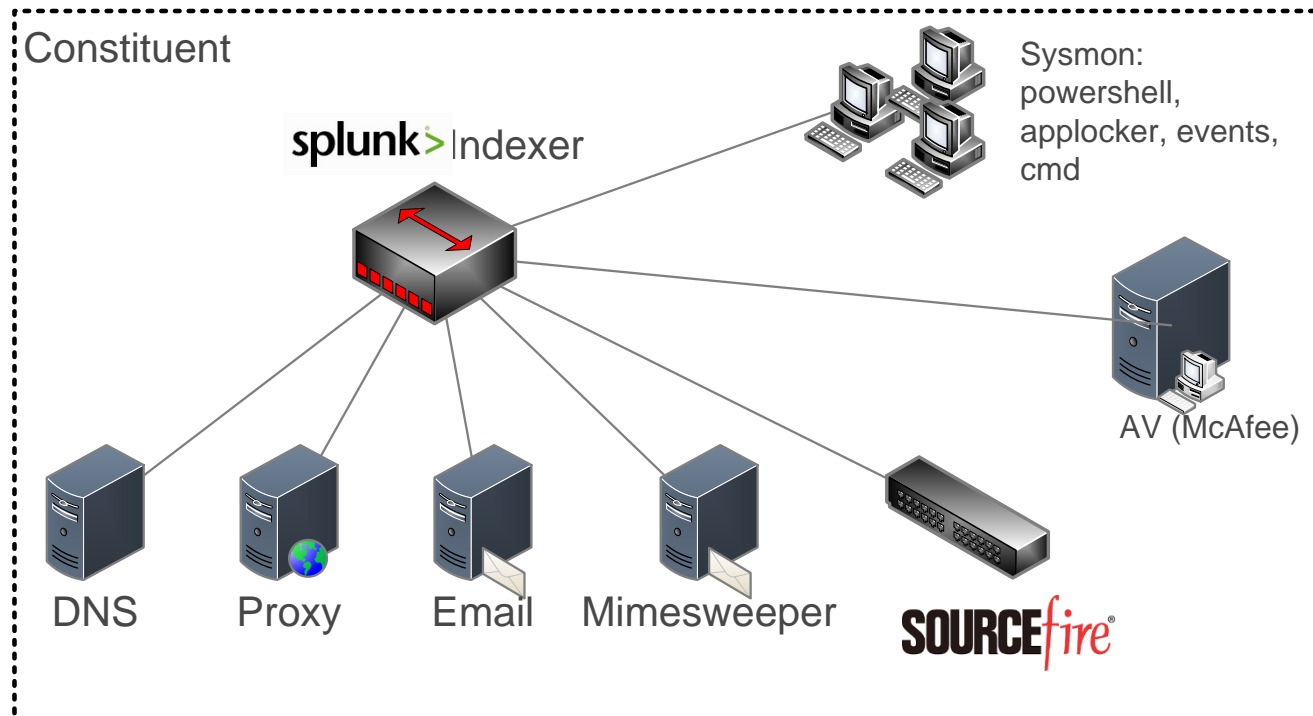
- » Exchange
- » Mimesweeper

Hosts:

- » Sysmon
- » Applocker
- » McAfee

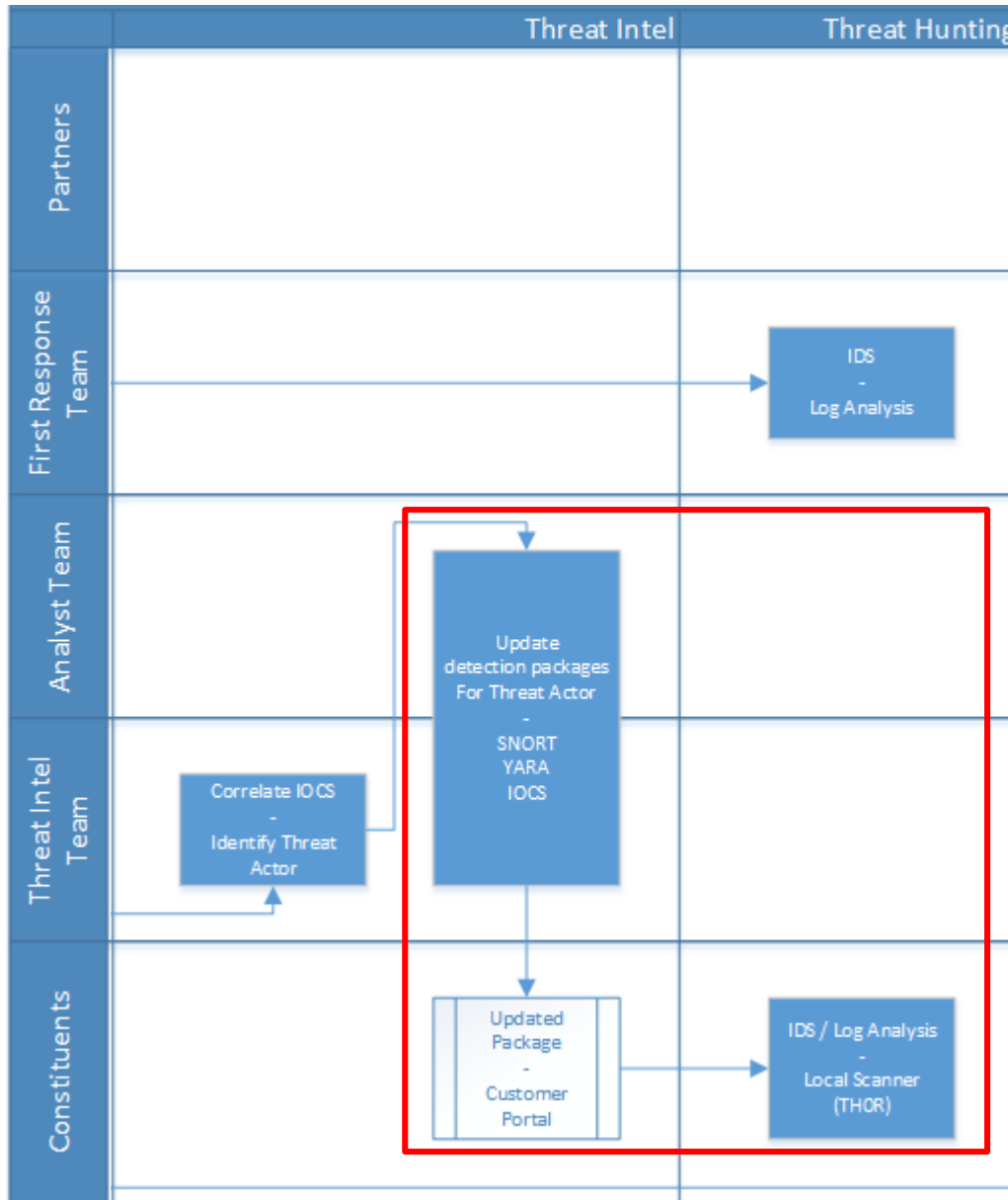
Appliances:

- » Sourcefire
- » Ironport
- » FireEye




Future :

- ▶ Firewalls
- ▶ Active Directory
- ▶ Servers
- ▶ Reverse Proxy





Th0r Packages

- Preparation 
 - YARA rules
 - Evil hashes
 - Custom filenames characteristics

```

054 rule Uroburos_Rootkit_Driver {
055   meta:
056     description = "Uroburos Rootkit - Gdata Finding"
057     author = "Florian Roth"
058     hash = "e869c8e7f61d4449d357d02179d45749661a66"
059     score = 100
060   strings:
061     $s0 = "Adeptec StorPort Ultra3 SCSI"
062     $s1 = "72.000.000 (NT.070231-1245)"
063     $s9 = "PH 3.0 MS_V98_V564_bw02 - R"
064     $s2 = "Ultra3.sys" fullword wide
065     $s3 = "TDI.sys" fullword
066     $s4 = "MDIS.sys" fullword
067     $s5 = "ZwControlFile" fullword
068   condition:
069     all of them
070 }

```

```

THOR CUSTOM EVIL HASHES
This file contains MD5, SHA1 and SHA256 hashes and a short info 1
or hash origin

APPLICATION -----
Every line is treated as STRING.
Every detection with one of these hashes increments the score by

FORMAT -----
MD5;COMMENT
SHA1;COMMENT
SHA256;COMMENT

EXAMPLES -----
0c2674c3a97c53802187d930efb645c2;DEEP_PANDA
00c907d39924de62b5891f80e83116;The_Darkhot

```

```

THOR File Name Characteristics
This file contains regex definitions and a score

APPLICATION -----
Every line is treated as REGEX case sensitive
Every line includes a score that adds up to a total score for this module.


FORMAT -----
COMMENT
REGEX.SCORE to add

EXAMPLES -----

```

- Distribution 
 - GPO
 - Endpoint Management

Time	Event
Aug 24 15:18:37 10.1.1.10 Aug 24 15:18:37.000	gerous file found MODULE: Filescan FILE: 73eed7ad7a083e4e SHA1: 8091b492c808687475670202d6163e365707465756c61 / proc 14-03-13 2015 ACCESSED: Sun Feb 22 14:1c Rule Value: Str1: -ma lsass.exe ACCESSED = Sun Feb 22 14:03 COMPANY = N/A C FIRSTBYTES = 70726f6364756d70202d616363657 MESSAGE = Possibly Dangerous file found - MOI REASON: 1 = Procdump_BAT / Procdump - Batch file SHA1 = 8b91b492c808687475670202d6163e365707465756c61 / mod: date_month = august date_second = 37 date event = Warning: MODULE: Filescan MESSAGE: Po file = C:\Users\1\Desktop\onpower\to\move\N mainreason = Procdump_BAT / Procdump - Batch message = Possibly Dangerous file found - mod: entlink -servar = entlinksh part elunas ex - servar

- Reporting and analysis 
 - Text/HTML report
 - Splunk app

THOR Report on ZEUS

Scan Information	Sections	Statistics
Thor Version: 2.6.3b	Local user accounts	Alarms: 27
Run on System: ZEUS	Profile directories	Warnings: 126
Argument list: D:\Dropbox\Code\gong\thor.exe -4 10	Installed hotfixes	Errors: 1
Signature Database: unknown	DNS Cache	Notices: 191
Start Time: 2013-03-10 14:55:49	Eventlog System	Infos: 961
End Time: 2013-03-10 17:00:33	Eventlog Application	Debugs: 33
Run as user: neo	Eventlog Security	
Run with admin rights: yes	Currently logged in users	
	Running Processes	
	Network Connections	
	Network Shares	
	Network Sessions	



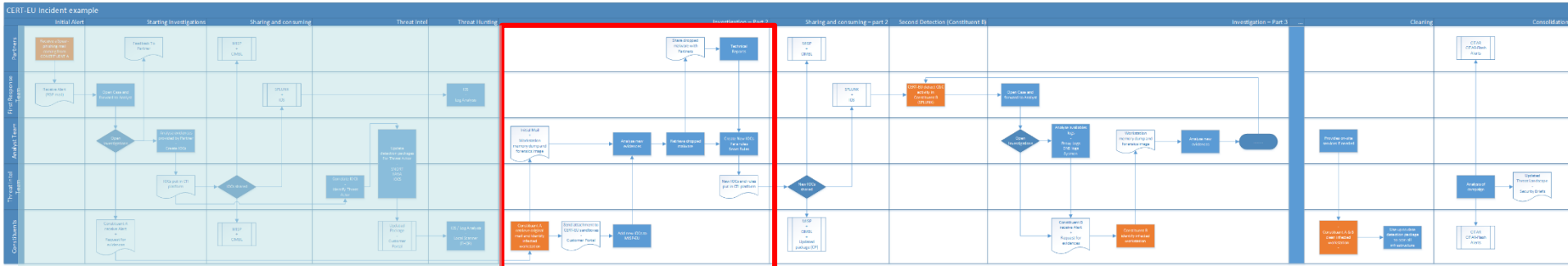
computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

Chapter 4

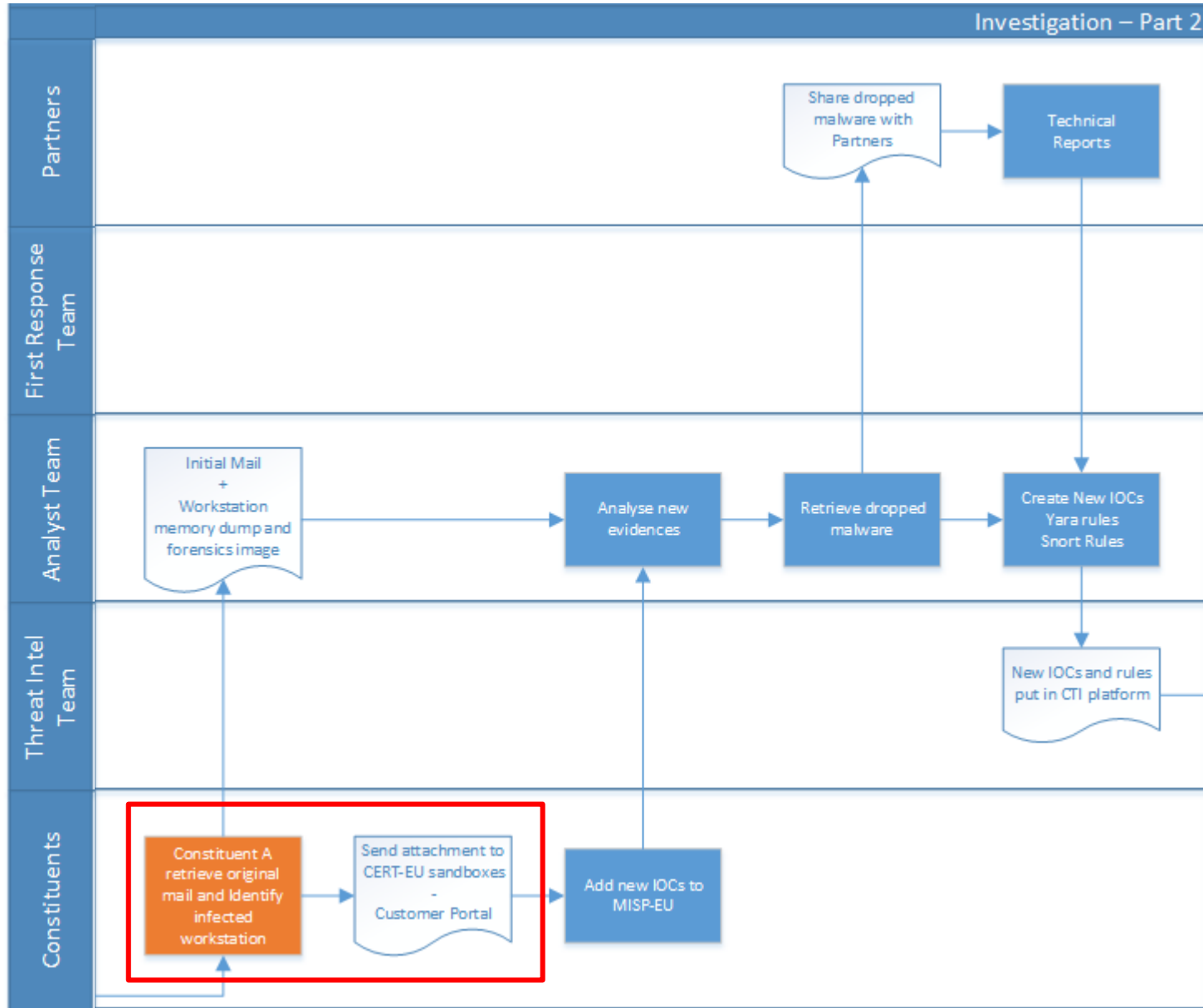
New evidence







Investigation – Part 2





- Constituents details
- CERT-EU deliverables
- Indicator search
- File Analysis
- Vulnerability scanning

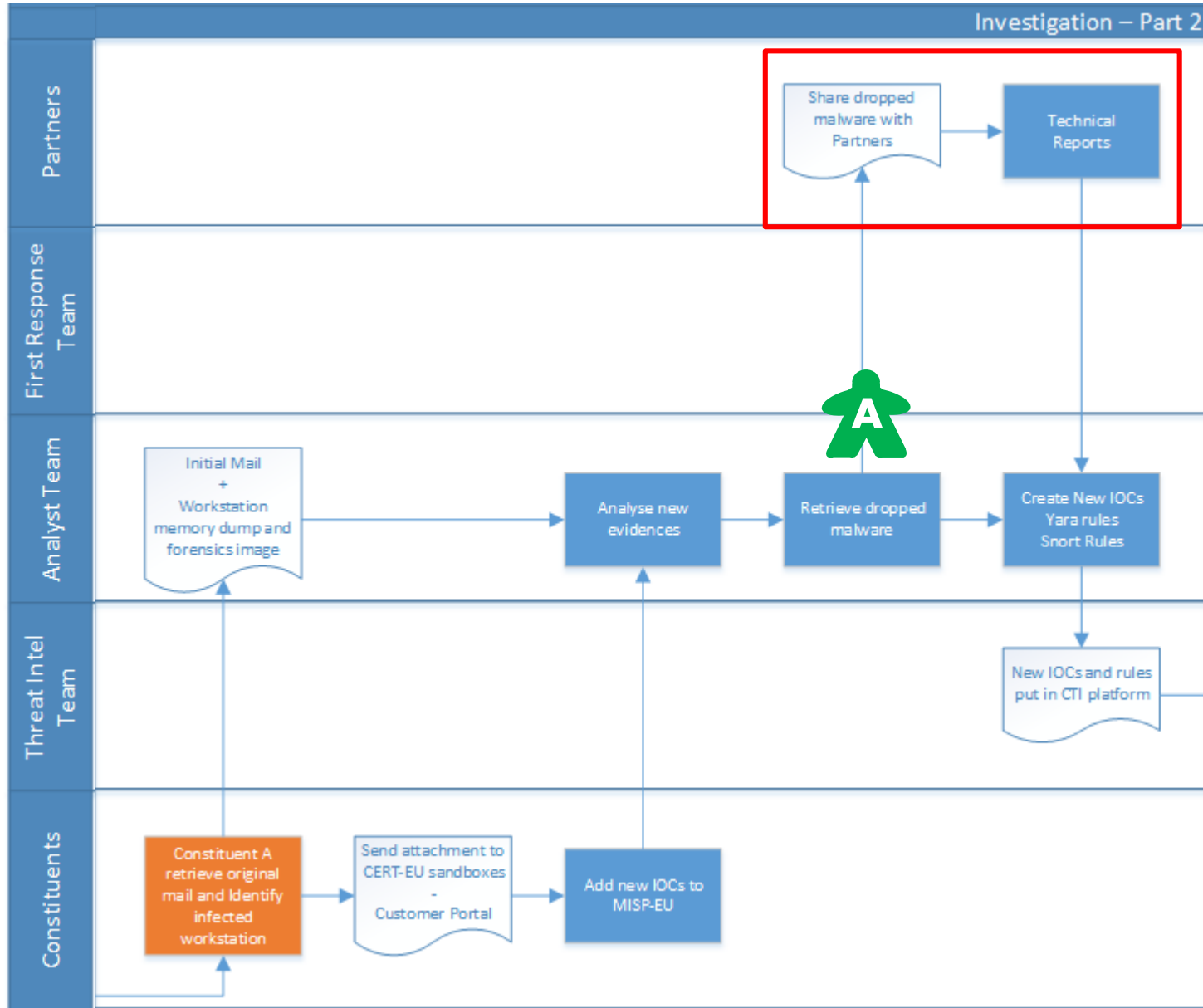
Edit organization details

Abbreviation	<input type="text" value="CERT-EU"/>
Name	<input type="text" value="Computer Emergency Response Team for EU Institutions Agencies and Bodies"/>
Mailing interval	<input type="text" value="3600"/>
IP ranges	<input type="text" value="212.8.189.16/28"/> <input type="button" value="+"/> <input type="button" value="-"/>
ASNs	<input type="text" value="5400"/> <input type="button" value="+"/> <input type="button" value="-"/>
Abuse E-mails	<input type="text" value="stavros.lingris@ec.europa.eu"/> <input type="button" value="+"/> <input type="button" value="-"/>
Contact E-mails	<input type="text" value="alexandru.ciobanu@ec.europa.eu"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="CP"/> <input type="button" value="CP"/>
	<input type="text" value="collector@cert.europa.eu"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="CP"/>
	<input type="text" value="sotirios.meintanis@cert.europa.eu"/> <input type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="CP"/>
FQDNs	<input type="text" value="cert.europa.eu"/> <input type="button" value="+"/> <input type="button" value="-"/>

Name	Type	Actions
CERT-EU_THOR_Bundle_20160826.zip	THOR	<input type="button" value="⬇"/>
5577-crowdstrike_yara_master_20160826.zip	YARA rules	<input type="button" value="⬇"/>
CITAR-Flash-2016-007.zip	Flash-CITAR	<input type="button" value="⬇"/>
CITAR-014-Duke-and-Baron.zip	CITAR	<input type="button" value="⬇"/>
CIMBL-267.zip	CIMBL	<input type="button" value="⬇"/>
CIMBL-268.zip	CIMBL	<input type="button" value="⬇"/>
CIMBL-269.zip	CIMBL	<input type="button" value="⬇"/>



Investigation – Part 2





computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

Peers - Partners



National Cyber Security Centre
Ministry of Security and Justice



GovCERT AUSTRIA



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY



Check Point
SOFTWARE TECHNOLOGIES LTD.



CERT.BG



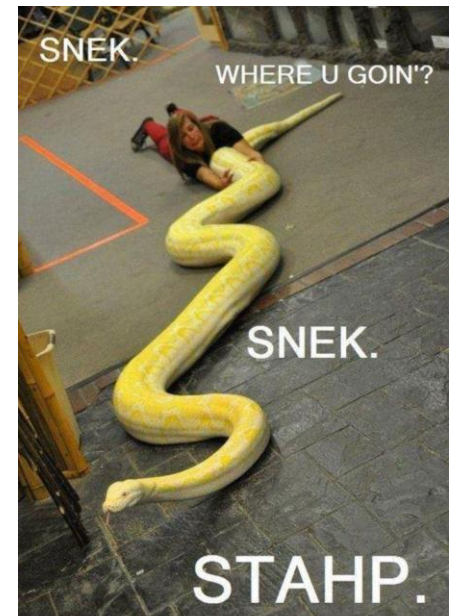


computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

Chapter 5

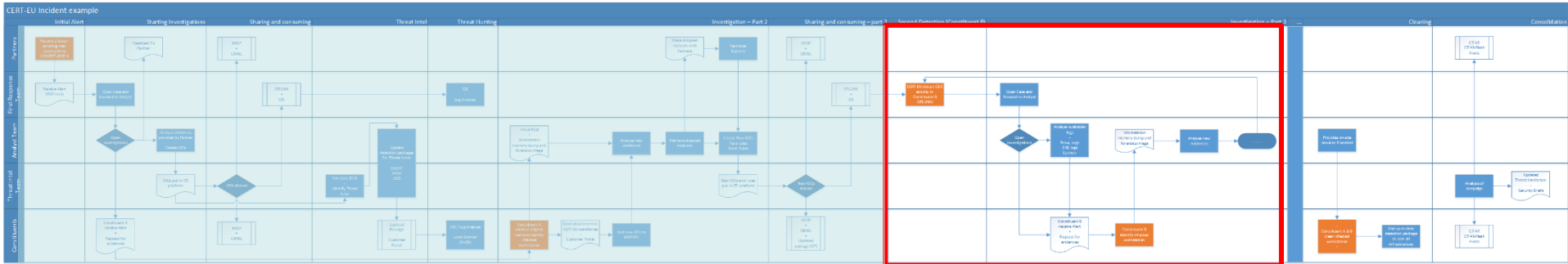
Another infection?

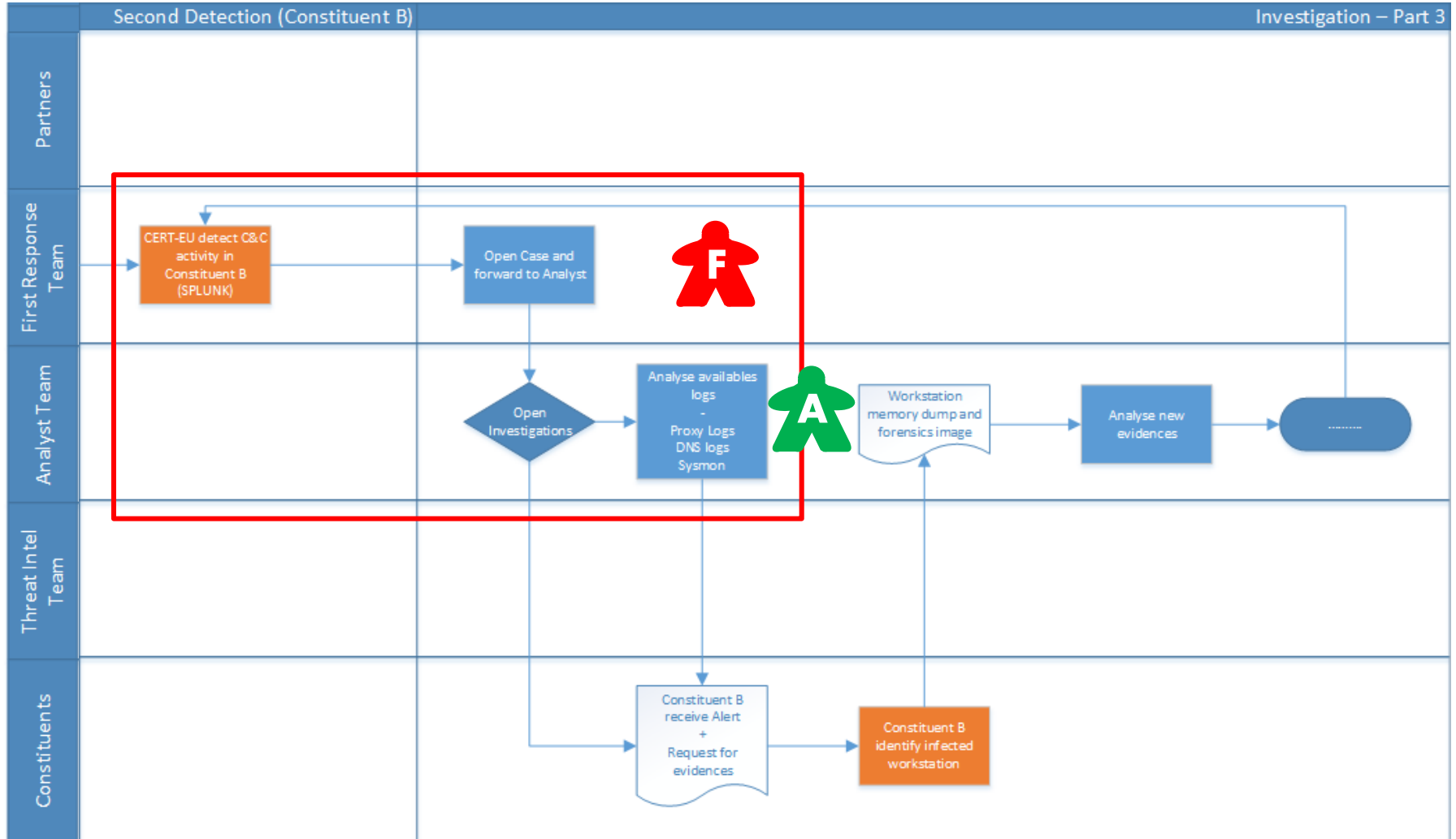




computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies







Daily findings summary report

Daily findings summary report based on all the available logs from our Constituents.

Edit ⌵ ⌵ ⌵

Please select the search artifact of interest

Filter by Constituent

2016-09-01, 105 hits (max duration 01:13:35) ⌵ ⌵

All ⌵ ⌵



DNS logs findings ⚠

i	from_splunk	query	id	feed_type	hits	first_seen	last_seen	actions
>	pa.eu	dpsu.gov.ua	CSIT-15112	cs_w_report (malicious_domain)	3	01/09/2016 08:42:56	01/09/2016 08:42:56	Report to CTI Toggle as done
>	pa.eu	old.dpsu.gov.ua	CSIT-15112	cs_w_report (malicious_domain)	3	01/09/2016 08:42:56	01/09/2016 08:42:56	Report to CTI Toggle as done
>	opa.eu	dcleaks.com	224fe9f4-63c6-11e6-a9a9-0050568e34e1	cti (malicious_domain)	2	01/09/2016 01:12:59	01/09/2016 01:12:59	Report to CTI Toggle as done
>	opa.eu	dpsu.gov.ua	CSIT-15112	cs_w_report (malicious_domain)	77	01/09/2016 00:06:15	01/09/2016 23:46:22	Report to CTI Toggle as done
>	pa.eu	www.dcleaks.com	224fe9f4-63c6-11e6-a9a9-0050568e34e1	cti (malicious_domain)	2	01/09/2016 01:12:58	01/09/2016 01:12:58	Report to CTI Toggle as done

Proxy logs findings ⚠

i	from_splunk	dest	id	feed_type	hits	d_clients	first_seen	last_seen	actions
>		www.europeanlawmootcourt.eu	CSIT-15112	cs_w_report (malicious_domain)	18	2	01/09/2016 11:56:39	01/09/2016 17:05:36	Report to CTI Toggle as done





DNS logs findings

i	from_splunk	query	id	feed
▼	europa.eu	sikol.heidiandrobwedding.com	5718da8a-15f0-4883-b4b6-15ffac110003	cti (malicious_domain)

i	Event
▼	4/18/2016 5:08:33 PM ODF8 PACKET 0000008658B65AB0 UDP R sikol.heidiandrobwedding.com

Event Actions ▼


Type	Field	Value
Event	eventtype ▼	dns_logs (dns network resolution)
	feed_type ▼	cti (malicious_domain)
	from_splunk ▼	.europa.eu
	id ▼	5718da8a-15f0-4883-b4b6-15ffac110003
	ioc ▼	sikol.heidiandrobwedding.com
	query ▼	sikol.heidiandrobwedding.com
	splunk_server ▼	:europa.eu
	src ▼	10.1.8.136
Time	_time ▼	2016-04-18T17:08:33.000+02:00



CTI Cyber Threat Intelligence by CERT-EU Version 3

Home Threat Object Detections Imports Export Statistics
Files Search Cyber Events

Observable



Observable

Type	hostname
Kill Chain	Command and Control
value1	sikol.heidiandrobwedding.com

31



computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

Chapter 6

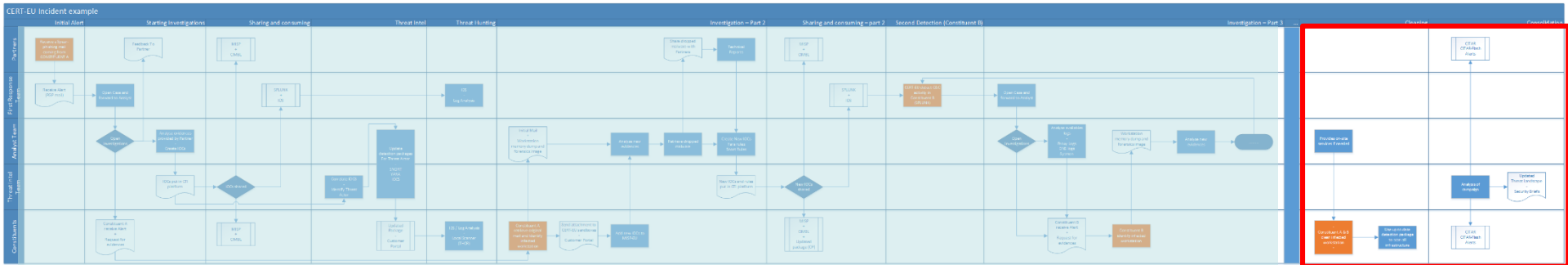
And now what?

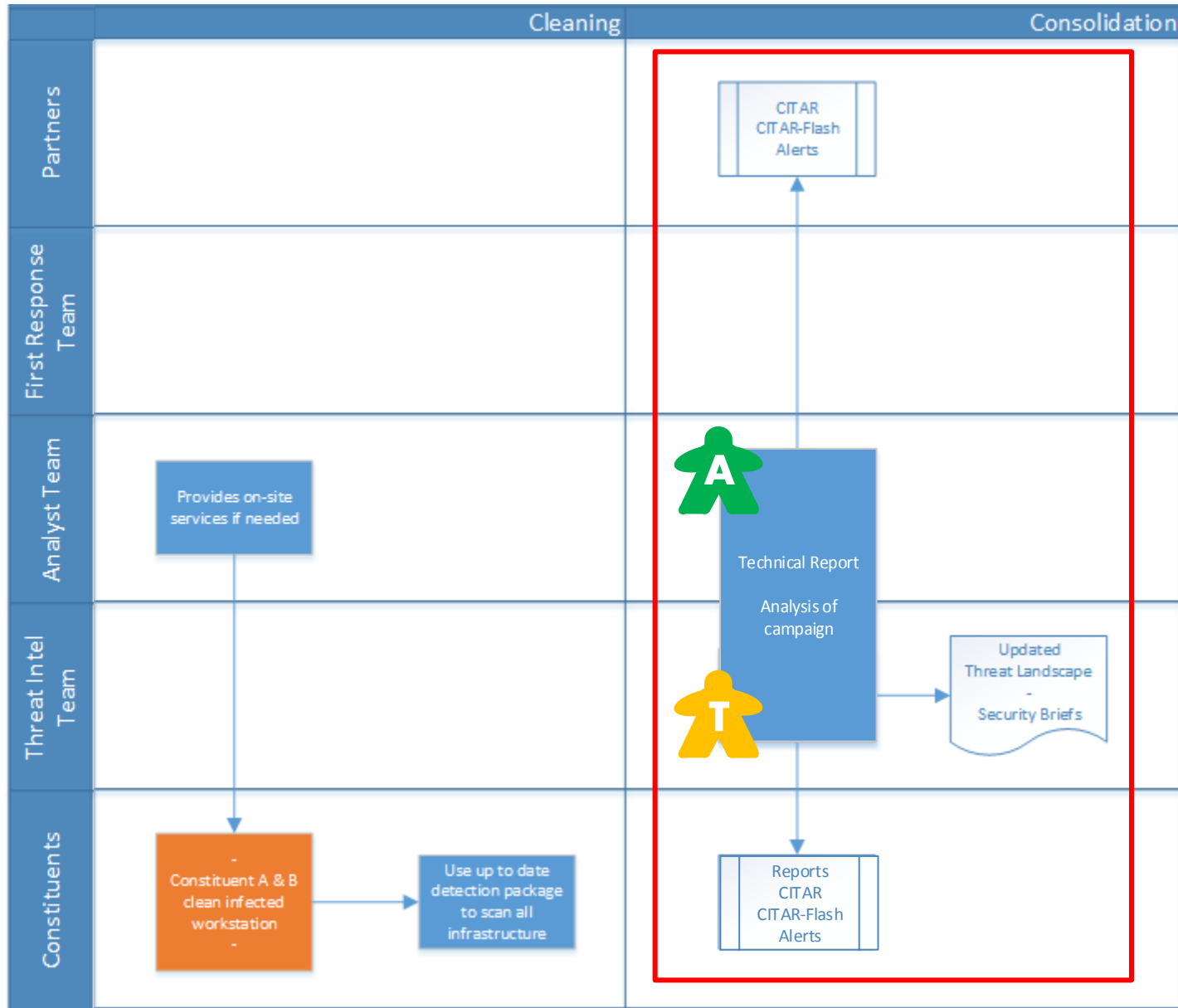


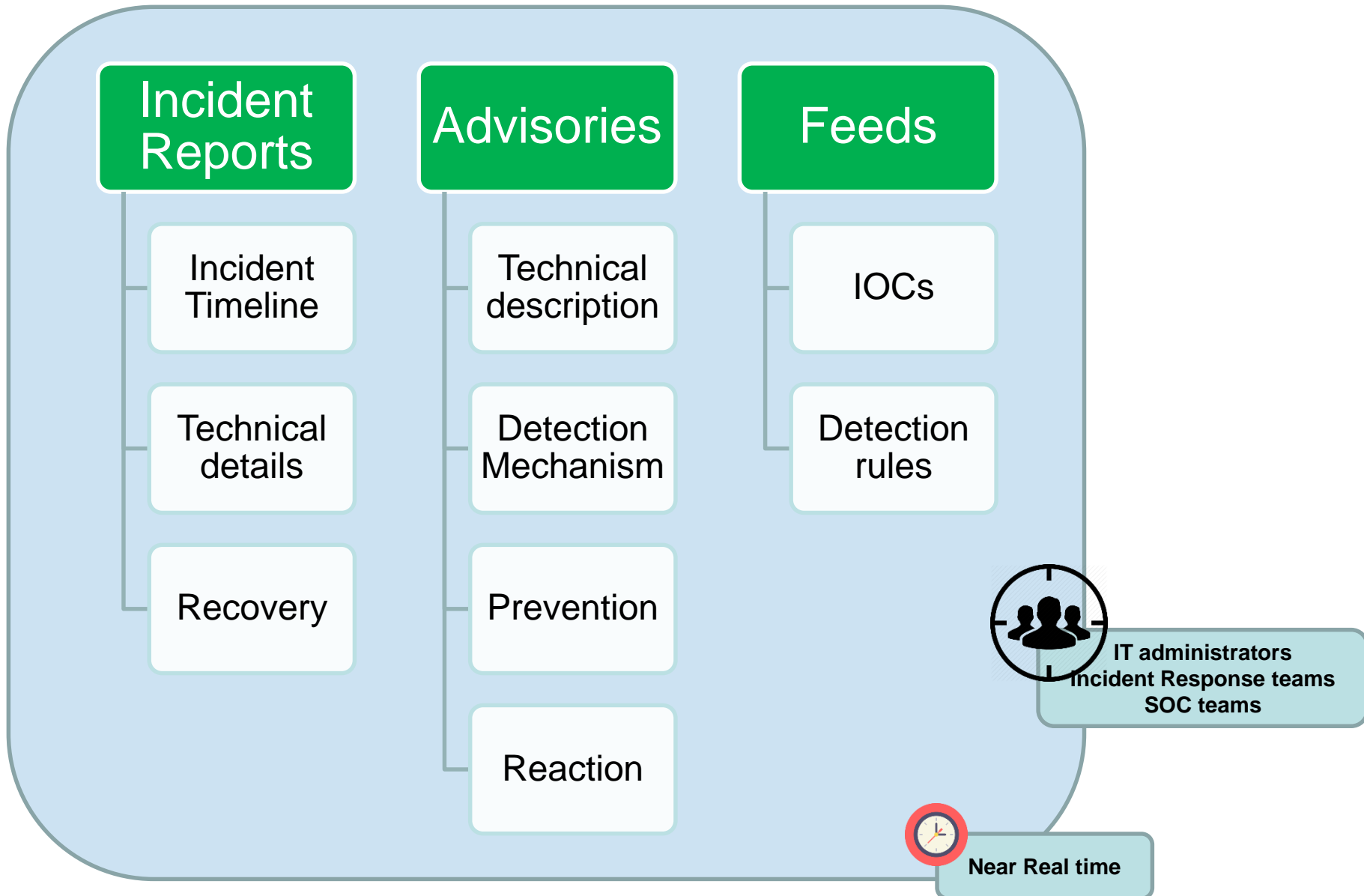


computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

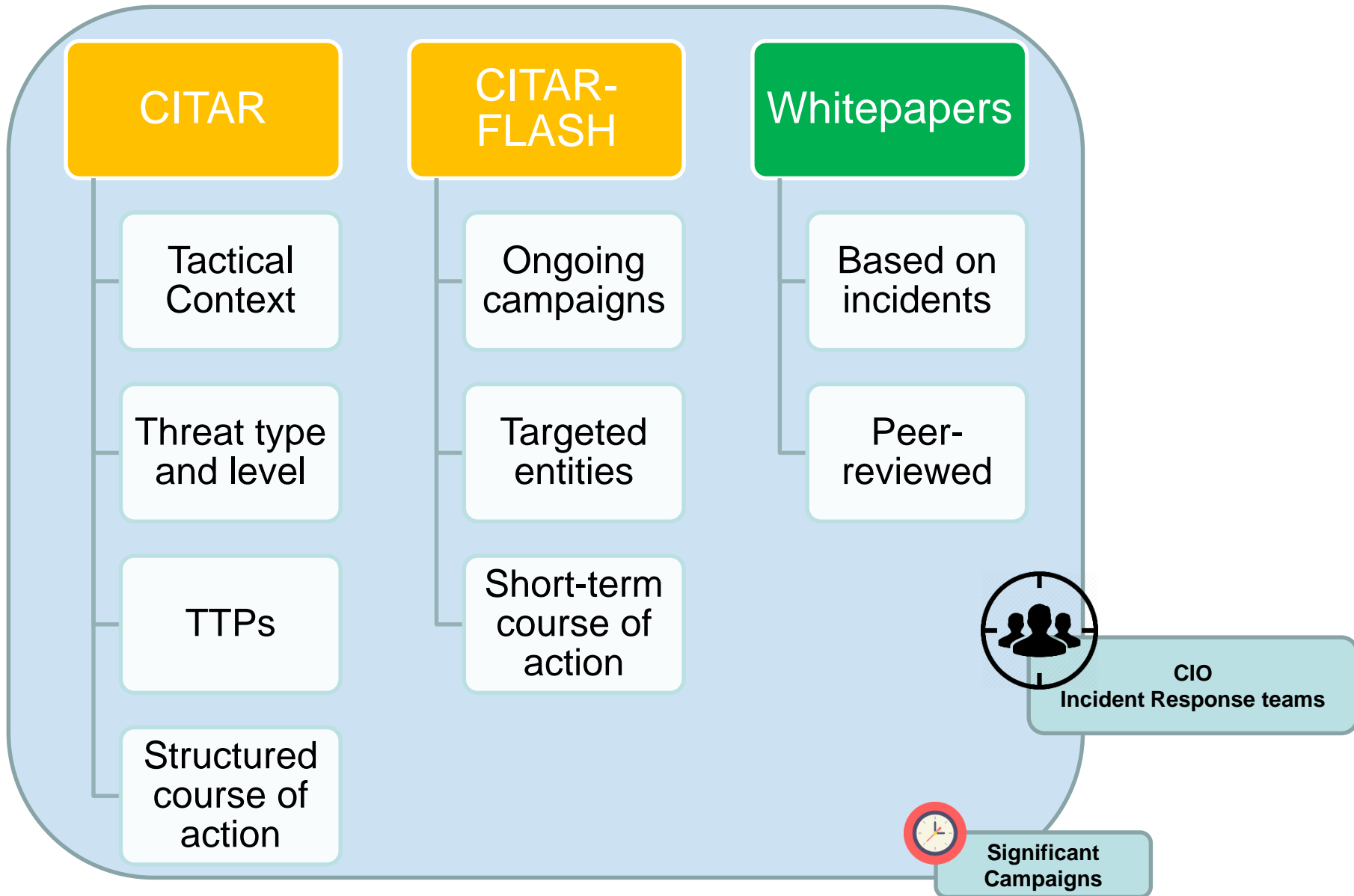


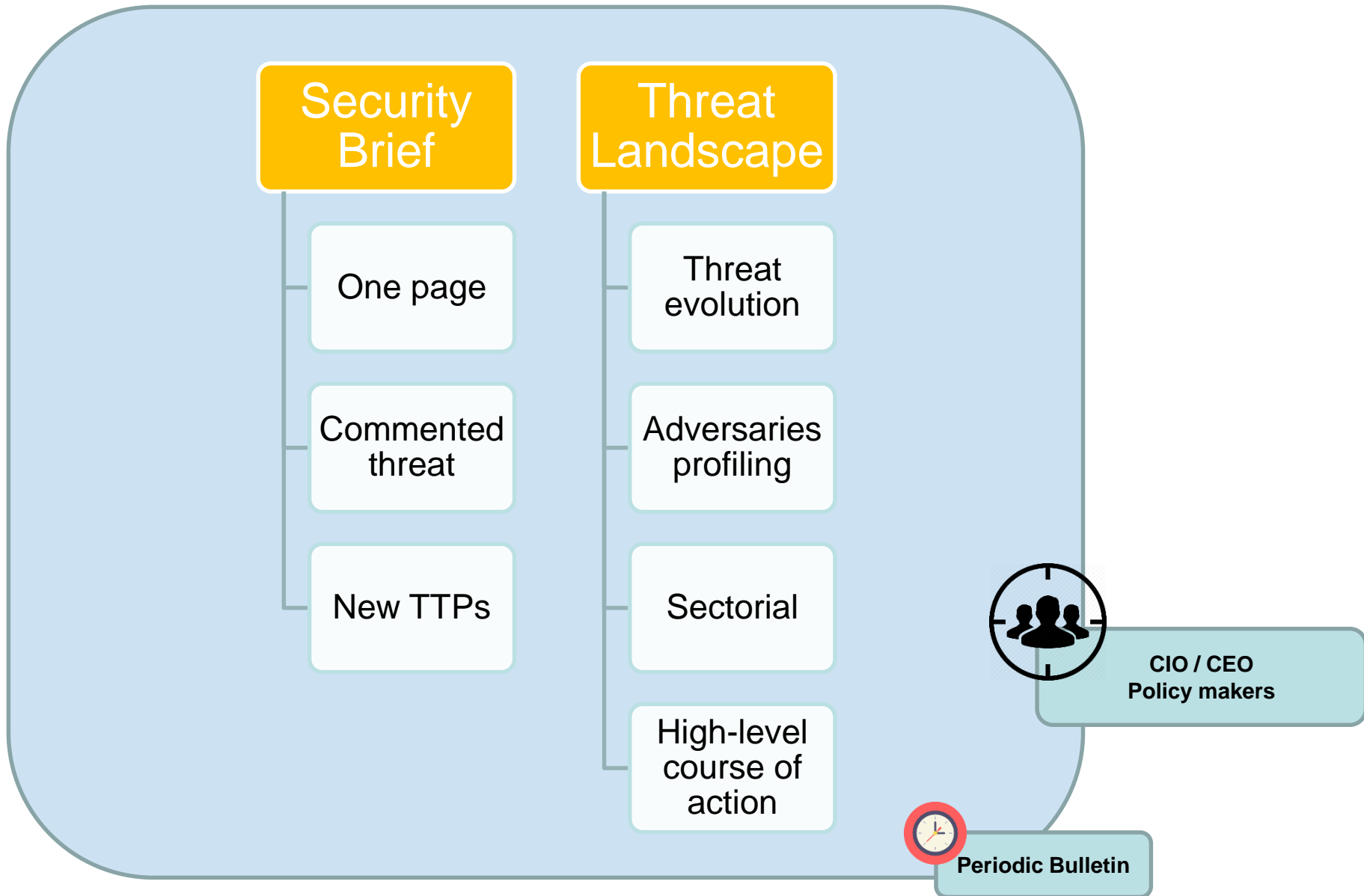






Tactical Products



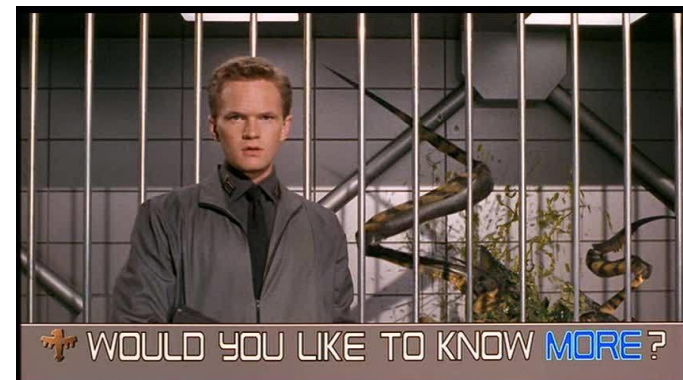




computer
emergency
response
team

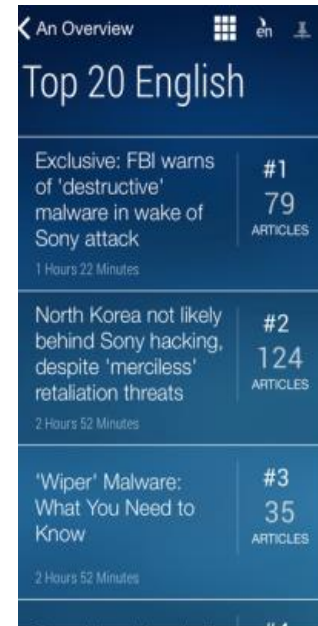
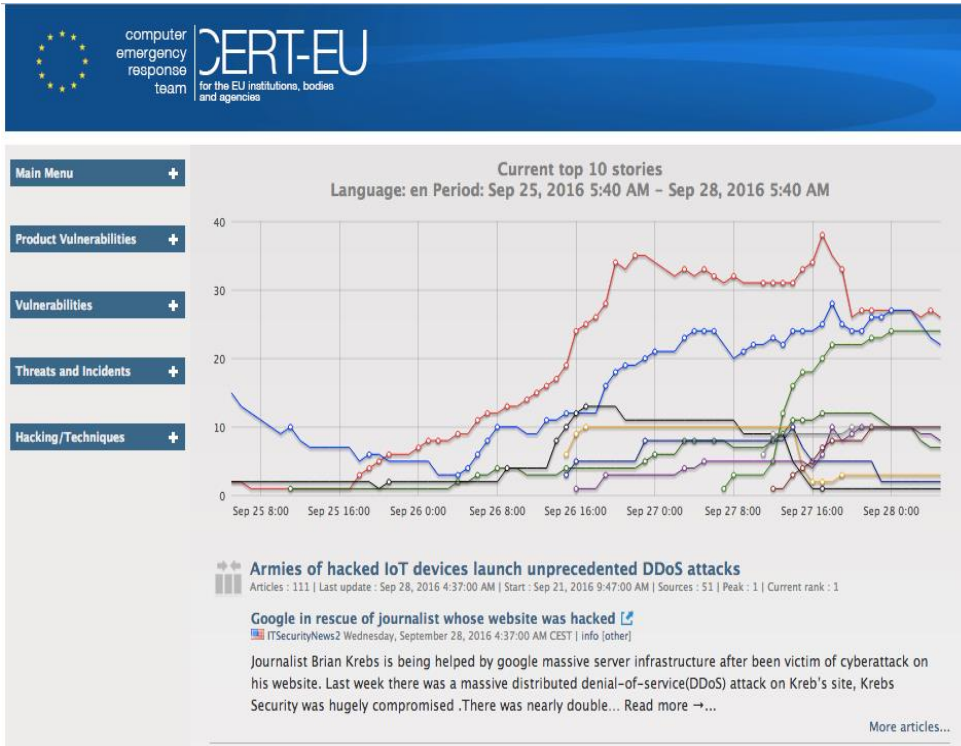
CERT-EU
for the EU institutions, bodies
and agencies

Epilogue





- Red Team
- Vulnerability Assessment services
- Bugbounty program
- Research and whitepapers
- Automation framework (AH)
- Workshops / trainings
- ...



<https://cert.europa.eu/>
<https://github.com/certeu/>