CERT-EU

FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

CTI & Information Fusion Benefits and Challenges

CTI EU Workshop

Frédéric Garnier

January 2020

TLP:WHITE

Cyber threat intelligence
enables to
“predict the future“
or
“understand the present” ?

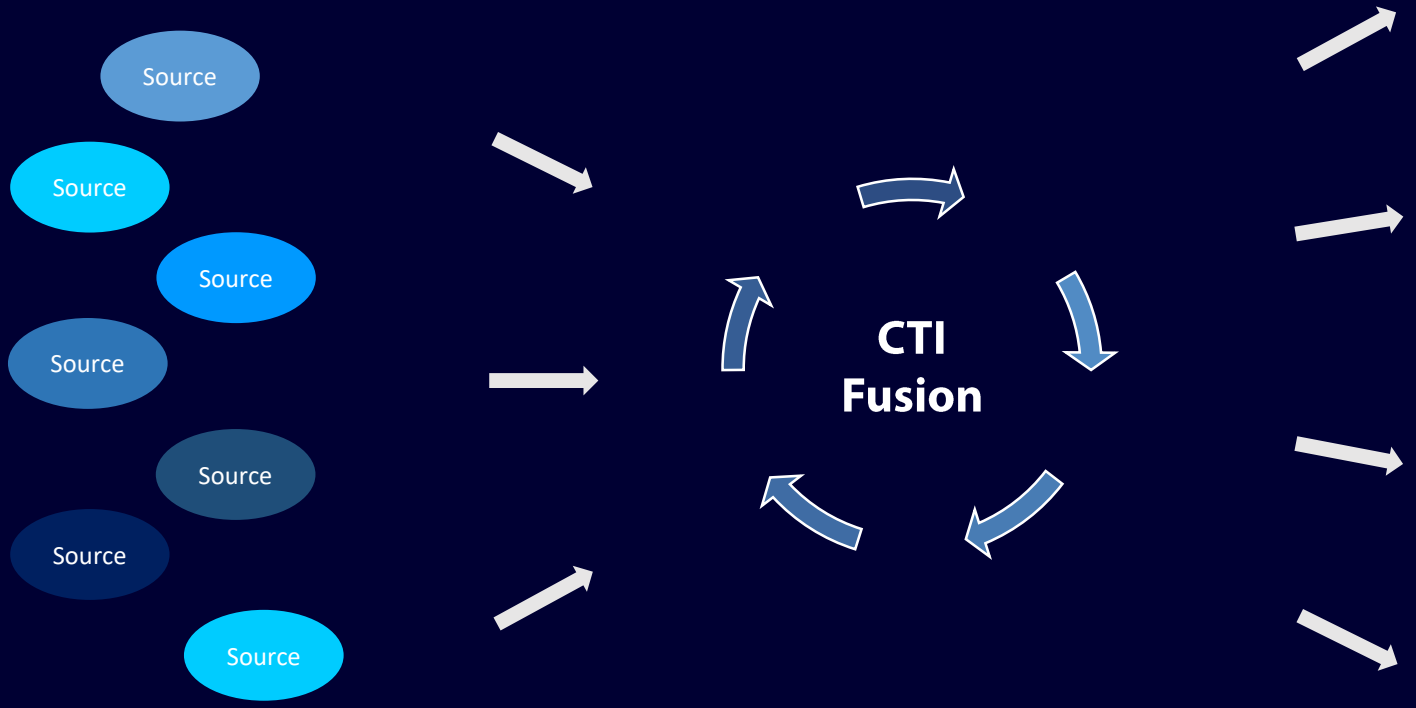
TLP:WHITE

Information fusion

- ❑ Benefits
- ❑ Principles
- ❑ Challenges

Benefits

Information fusion
Supported services



Consolidated
Situational awareness

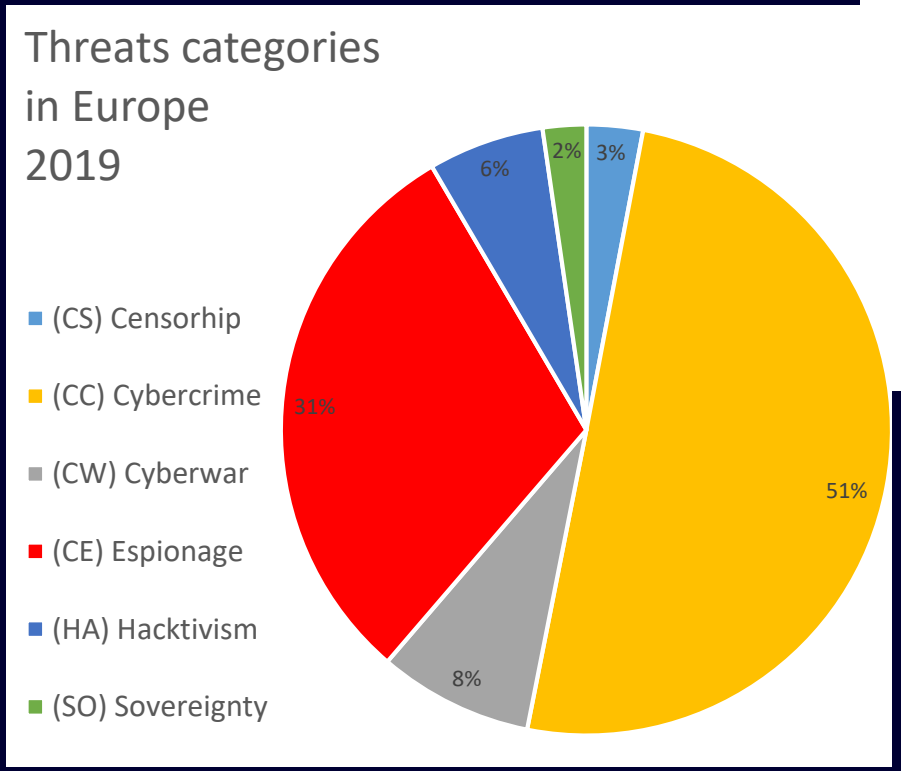
Tailored
Alerts and Memos

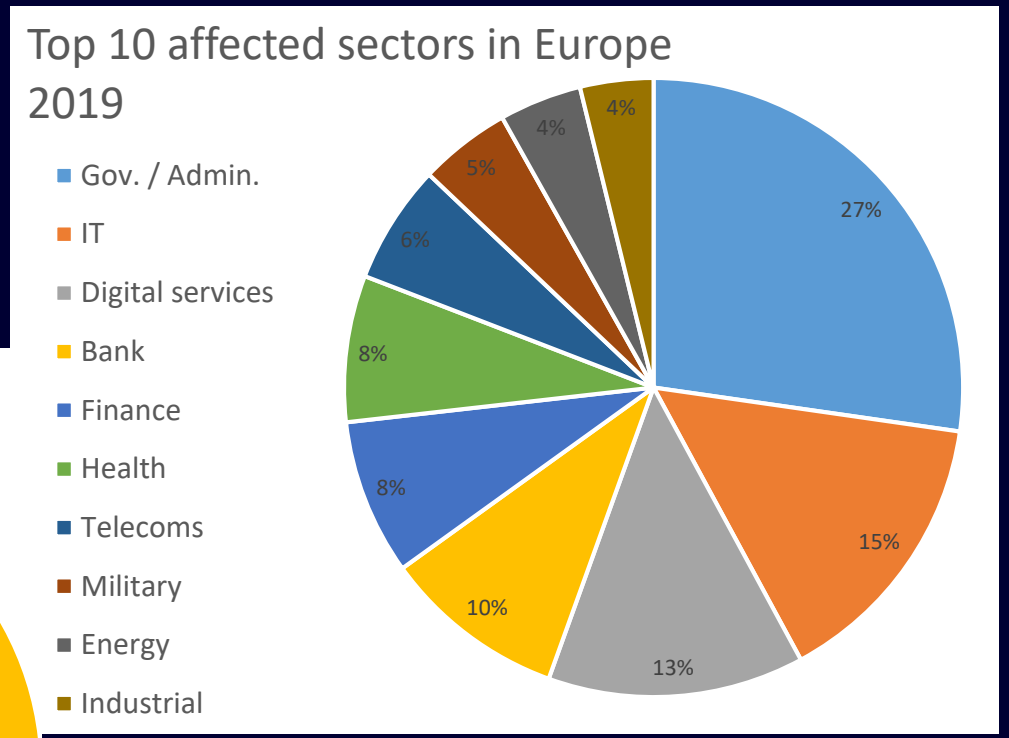
Actionable
Detection and hunting

Consistent
Knowledge bases

TLP:WHITE

Situation awareness - example (1)
Regional threat activity

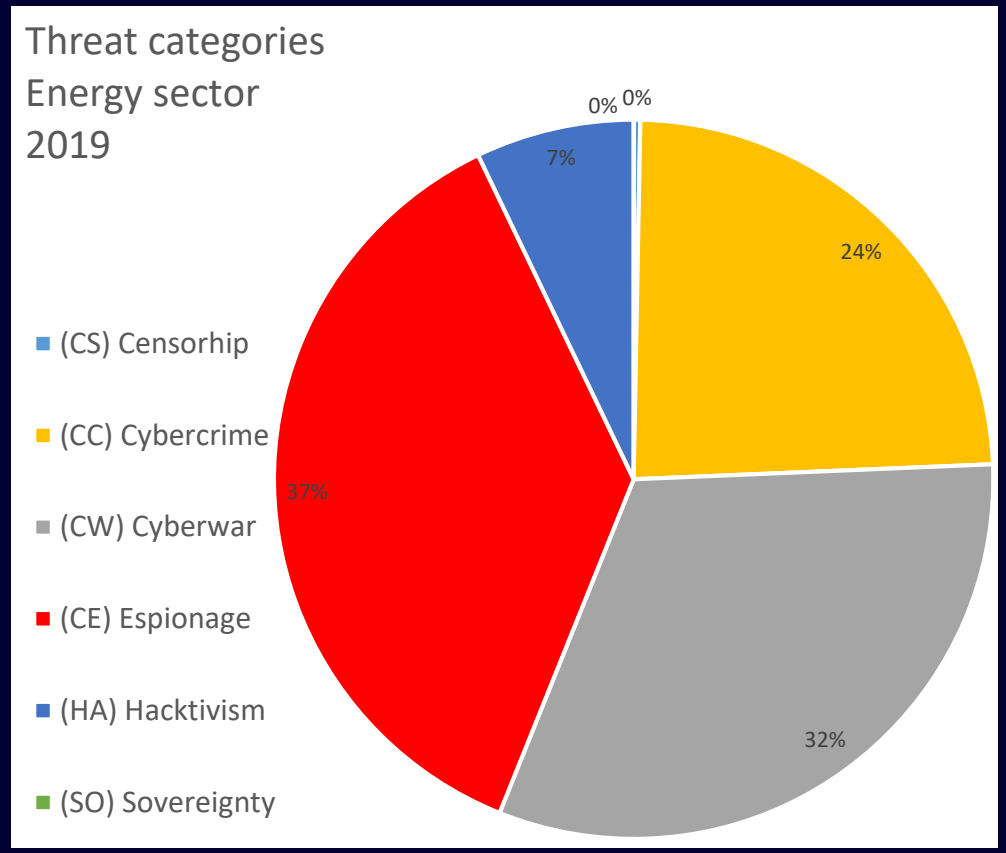




Top 10 malware families (December 2019)	
1	TrickBot
2	Qbot
3	Mofksys
4	NjRAT
5	Emotet
6	Agent Tesla
7	Tinba
8	UrSnif
9	GandCrab
10	Pony

TLP:WHITE

Situation awareness - example (2)
Sectoral threat activity



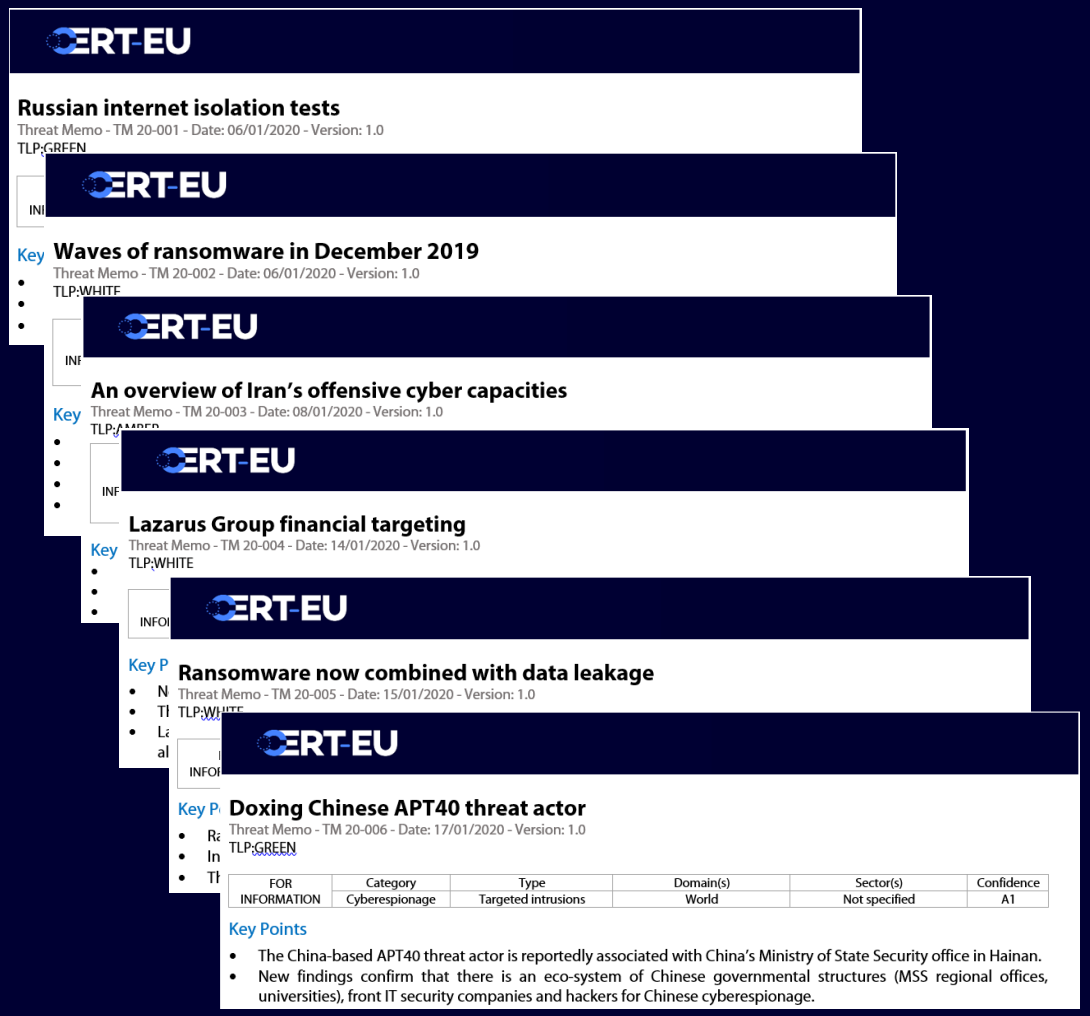
Top threat actors against the energy sector

Rank	Name	Type	Count.	Share
1	APT34	CE	IR	23%
2	Berserk Bear	CE	RU	20%
3	APT33	CE	IR	12%
4	Energetic Bear	CE	RU	10%
5	Lazarus Group	CE	NK	9%
6	MuddyWater	CE	IR	7%
7	Sandworm	CE	RU	5%
8	Hexane	CE		5%
9	APT35	CE	IR	4%
10	APT28	CE	RU	4%

Top-20 affected countries in the energy sector

Rank	Name	Share
1	US	18%
2	Middle East	14%
3	Iran	9%
4	India	8%
5	Italy	5%
6	Ukraine	5%
7	South Africa	5%
8	Saudi Arabia	5%
9	UK	4%
10	Canada	4%
11	Turkey	4%
12	Israel	3%
13	Germany	3%
14	Vietnam	3%
15	Australia	3%
16	Europe	2%
17	Kuwait	2%
18	Mexico	2%
19	Asia	2%
20	Belarus	2%

Tailored intelligence Memos and Alerts



Russian internet isolation tests
Threat Memo - TM 20-001 - Date: 06/01/2020 - Version: 1.0
TLP:GREEN

Waves of ransomware in December 2019
Threat Memo - TM 20-002 - Date: 06/01/2020 - Version: 1.0
TLP:WHITE

An overview of Iran's offensive cyber capacities
Threat Memo - TM 20-003 - Date: 08/01/2020 - Version: 1.0

Lazarus Group financial targeting
Threat Memo - TM 20-004 - Date: 14/01/2020 - Version: 1.0
TLP:WHITE

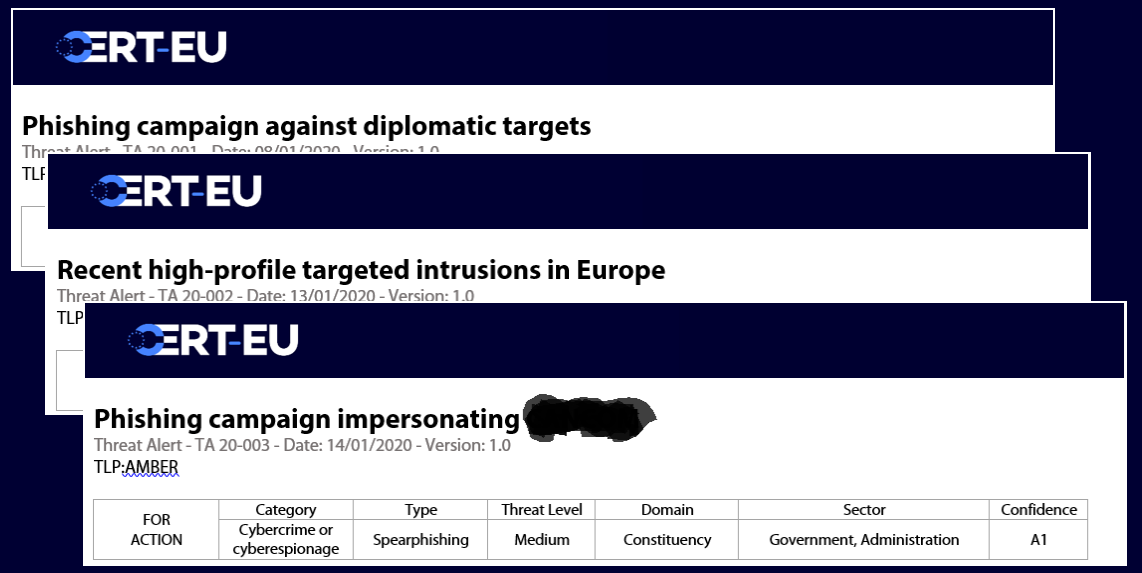
Ransomware now combined with data leakage
Threat Memo - TM 20-005 - Date: 15/01/2020 - Version: 1.0

Doxing Chinese APT40 threat actor
Threat Memo - TM 20-006 - Date: 17/01/2020 - Version: 1.0
TLP:GREEN

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Cyberespionage	Targeted intrusions	World	Not specified	A1

Key Points

- The China-based APT40 threat actor is reportedly associated with China's Ministry of State Security office in Hainan.
- New findings confirm that there is an eco-system of Chinese governmental structures (MSS regional offices, universities), front IT security companies and hackers for Chinese cyberespionage.



Phishing campaign against diplomatic targets

Recent high-profile targeted intrusions in Europe
Threat Alert - TA 20-002 - Date: 13/01/2020 - Version: 1.0

Phishing campaign impersonating [redacted]
Threat Alert - TA 20-003 - Date: 14/01/2020 - Version: 1.0
TLP:AMBER

FOR ACTION	Category	Type	Threat Level	Domain	Sector	Confidence
	Cybercrime or cyberespionage	Spearphishing	Medium	Constituency	Government, Administration	A1

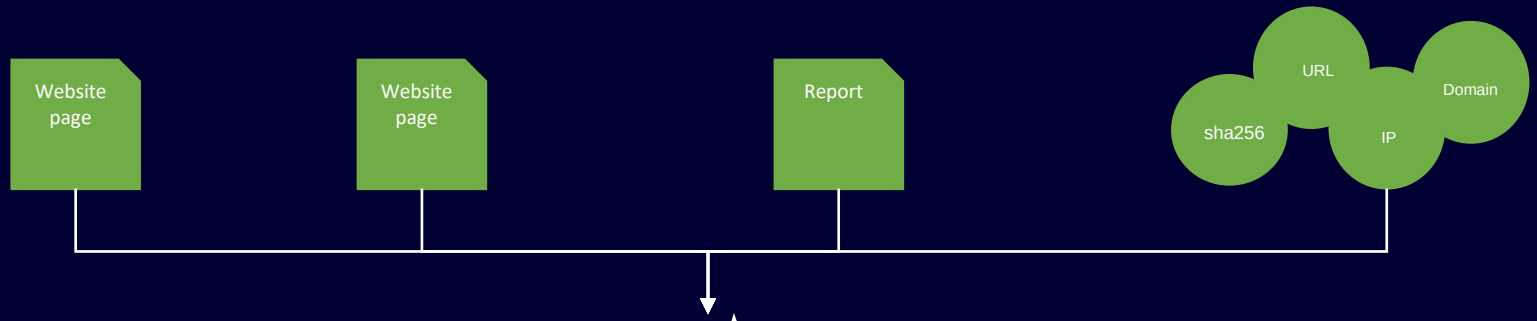
TLP:WHITE

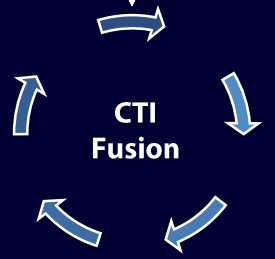
Tailored intelligence Alerts

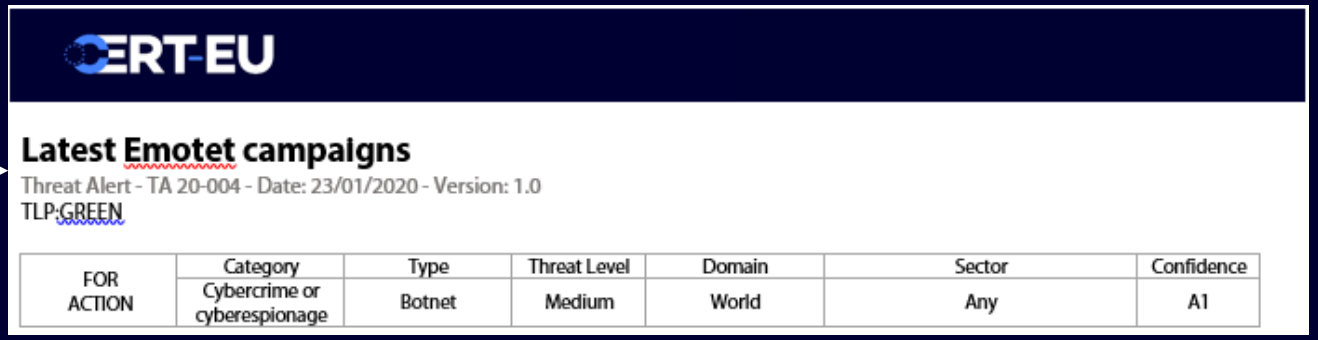
BLEEPINGCOMPUTER

MITRE ATT&CK

EU Institutions







CERT-EU

Latest Emotet campaigns

Threat Alert - TA 20-004 - Date: 23/01/2020 - Version: 1.0

TLP:GREEN

	Category	Type	Threat Level	Domain	Sector	Confidence
FOR ACTION	Cybercrime or cyberespionage	Botnet	Medium	World	Any	A1

TLP:WHITE

Tailored intelligence
Actionable data - Example

Actionable information

Attack timeline

Date	Event
13/01/2020	Phishing email from a compromised [redacted] email address.

Techniques, tactics and procedures (TTPs)

Kill chain	Techniques and Tools	ATT&CK
Initial access	Spearphishing attachment Spearphishing link	T1193 T1192
Credential access	Input capture	T1056

Indicators of compromise, detection and hunting rules

MISP-EU IoC	cbd551bb[redacted]

Recommendations and mitigations

Name	Details	ATT&CK
Restrict Web-Based Content	N/A	M1021
User Training	N/A	M1017
Antivirus/Antimalware	N/A	M1049
Network Intrusion Prevention	N/A	M1031

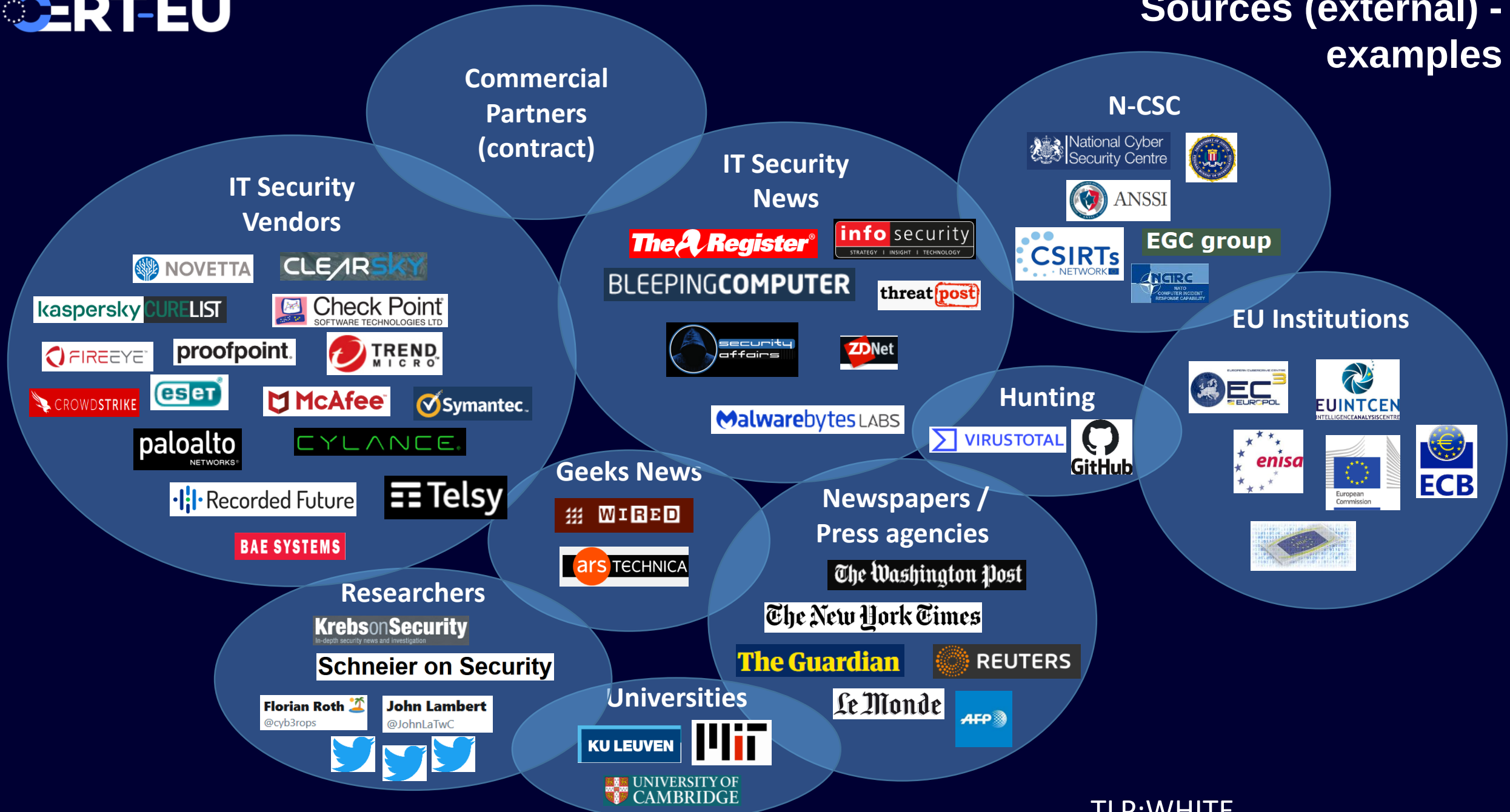
TLP:WHITE

Principles

Conditions

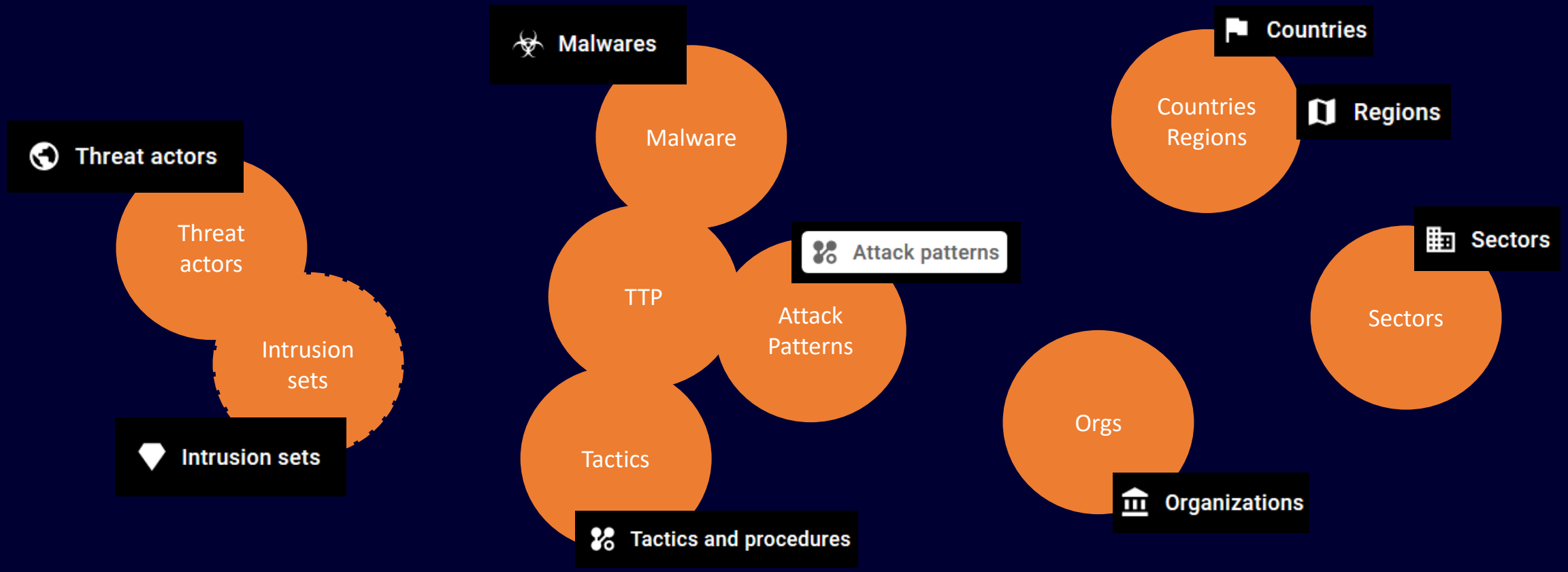
- Reliable sources
- Sufficient context from sources
- Consistent data model
- Well defined process
- Automation

Sources (external) - examples



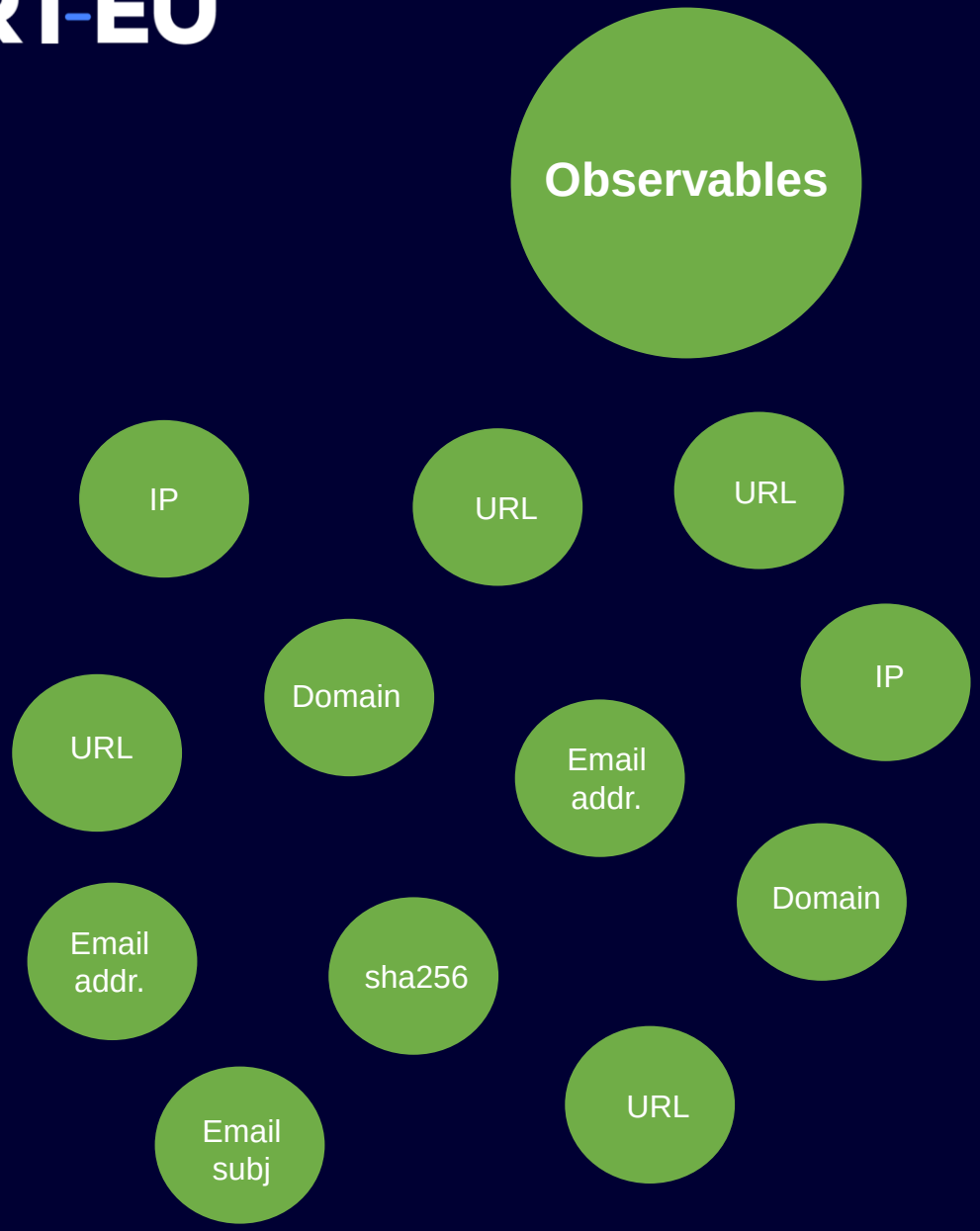
TLP:WHITE

Cosmology



TLP:WHITE

Incoming threat information



TLP:WHITE

Report stream (fictitious examples)

Date	Source	TLP	Reports	Category	Countries	Sectors	TTP	Threat Actor	Assets
11/9/2019	Secureworks	TLP:WHITE		Cybercrime	World	Finance	Lokibot	XYZ Spider	Banking data
11/9/2019	ESET	TLP:WHITE		Espionage	Unspecified	Government, Foreign affairs	Malware XYZ, ATT&CK T1189, T1059, …	APT15. China	Classified data
11/9/2019	Reuters	TLP:WHITE		Hacktivism	Brazil	Government	Defacement, Leakage	Anonymous Brazil	Personal data
11/9/2019	Commercial source A	TLP:AMBER		Cyberwar	Asia	Media	Wiper XYZ	Xyz Tiger	
11/9/2019	Commercial source B	TLP:AMBER		Censorship	China	Citizens	Great Firewall, Blocking	MSS, China	
12/9/2019	Commercial source C	TLP:AMBER		Sovereignty	Russia	Digital services	Ban	Russia	
12/9/2019	US CERT	TLP:GREEN		Espionage	US	Universities	Malware XYZ	North Korea	
12/9/2019	CitizenLabs	TLP:WHITE		Cybercrime	UAE	Citizens	Tool XYZ		
12/9/2019	Bleeping Computer	TLP:WHITE		Cybercrime	Europe	Digital infra	Ransomware Ryuk, Extortion	XYZ Spider	Cryptocurrency
12/9/2019	European CSIRT	TLP:RED		Espionage	Country A, Country B	Government	Malware XYZ, ATT&CK T1223, T1118, …	APT28, Russia	Military data

Meta data

21.3 reports per day in 2019

Threat analysis

TLP:WHITE

Observables stream (fictitious examples)

CERT-EU

Exp date	Rating	Obs	Indicator	Sighting	TTP	Threat actor	Report
31-11-19	100	IP	Malicious domains	Diplomacy Europe		APT28	Commercial report
31-11-19	100	IP					
31-11-19	100	Domain					
31-11-19	100	Domain					
31-11-19	100	comment					
28-10-21	100	Email-addr	Phishing email	EU-I	Emotet		Constituent report
28-10-21	100	Email-subject					
28-10-21	100	url					
28-10-21	0	Email-addr	Phishing email	Partner			Partner report
28-10-21	100	filename					
05-01-20	100	sha256					
05-01-20	100	sha256	RAT	Unknown		Turla	vendor report
05-01-20	100	sha256					
05-01-20	100	sha256					
05-01-20	100	url	Phiishing campaign	Europe	Lokibot		vendor report
05-01-20	100	url					
07-06-20	100	url					
07-06-20	100	url					
07-06-20	100	text					
07-06-20	100	sha256	Malicious samples	United States	GandCrab		OSINT report
07-06-20	100	sha1					
07-06-20	100	md5					
07-06-20	100	sha256					
07-06-20	100	sha1					
07-06-20	100	md5					
15-12-19	100	sha256					
15-12-19	100	sha1					
15-12-19	100	md5					
15-12-19	100	filename	Targeted intrusion	EU-I		APT1	Constituent report
15-12-19	100	filename					
15-12-19	100	filename					
15-12-19	100	yara					
15-12-19	100	yara					
07-12-23	100	snort					
07-12-23	100	IP					
07-12-23	100	IP					
07-12-23	100	regkey					
07-12-23	100	regkey					
07-12-23	100	regkey					
07-12-23	100	IP	Botnet	World	Mirai		OSINT report
07-12-23	100	IP					
07-12-23	100	IP					
28-07-22	100	IP					
28-07-22	100	IP					
28-07-22	100	link					
28-07-22	100	yara	Yara master	Unknown			
28-07-22	100	yara					
28-07-22	100	yara					
28-07-22	100	yara					
28-07-22	100	yara					
13-10-19	100	snort	snort master	Unknown			
13-10-19	0	snort					
13-10-19	100	snort					
13-10-19	100	snort					
13-10-19	100	snort					
13-10-19	100	pattern-in-file	Malware analysis	Unknown	Dridex		
13-10-19	100	pattern-in-file					
13-10-19	100	pattern-in-file					
13-10-19	100	patter-in-traffic					
13-10-19	100	patte					
13-10-19	100	patte					

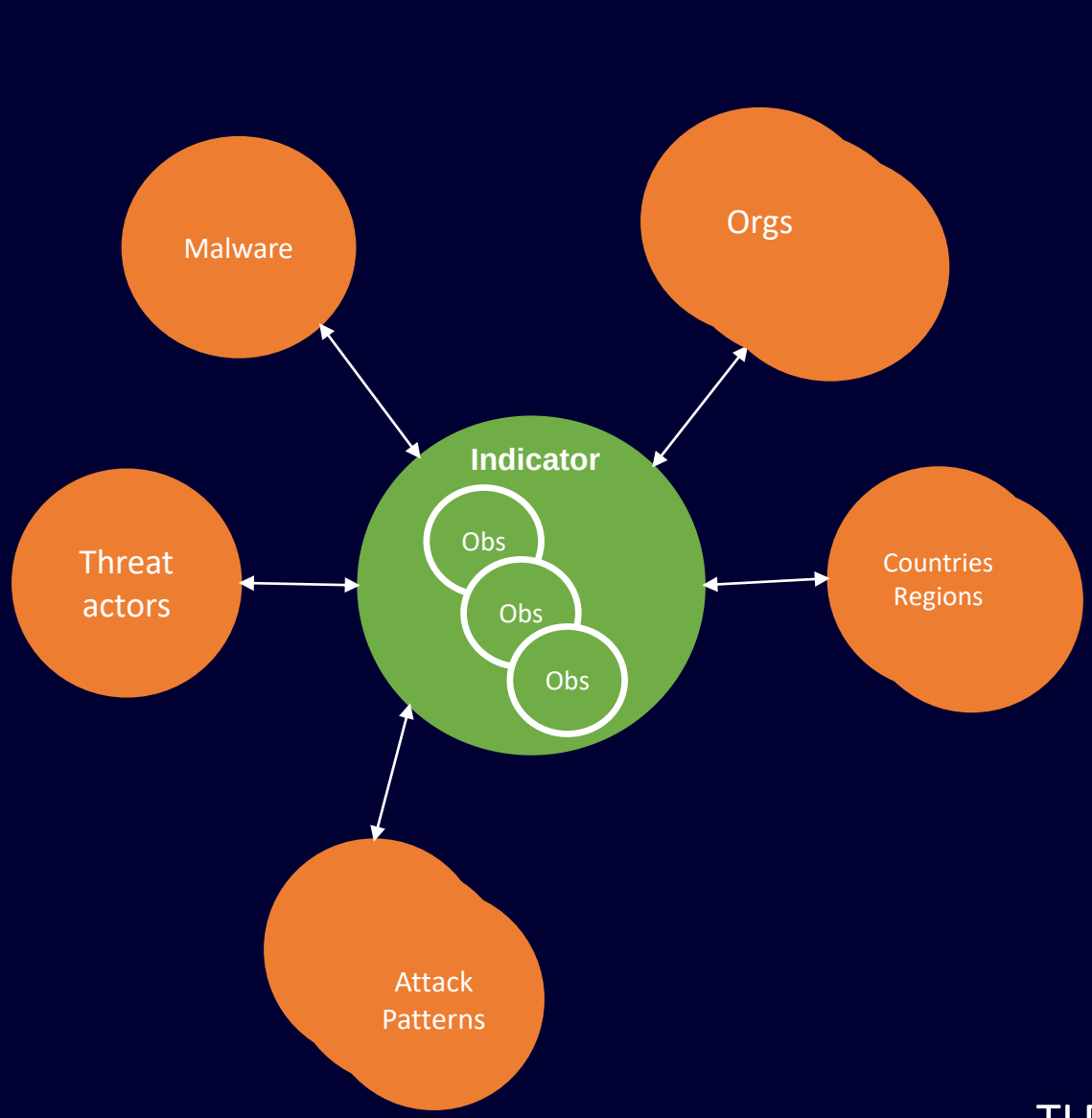
Context

Raw data

Actionable parameters

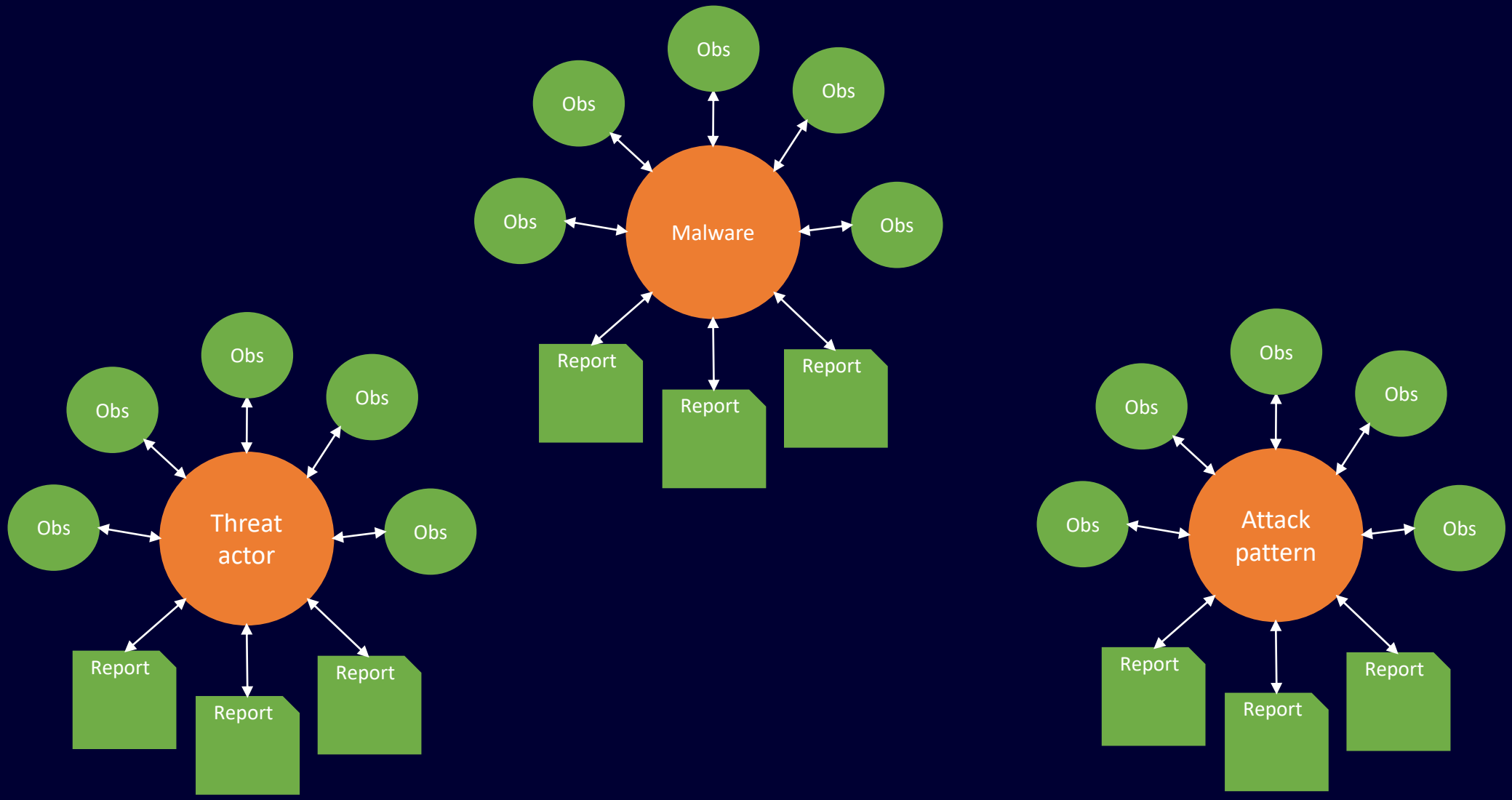
28.5K
Per day
in 2019

Association



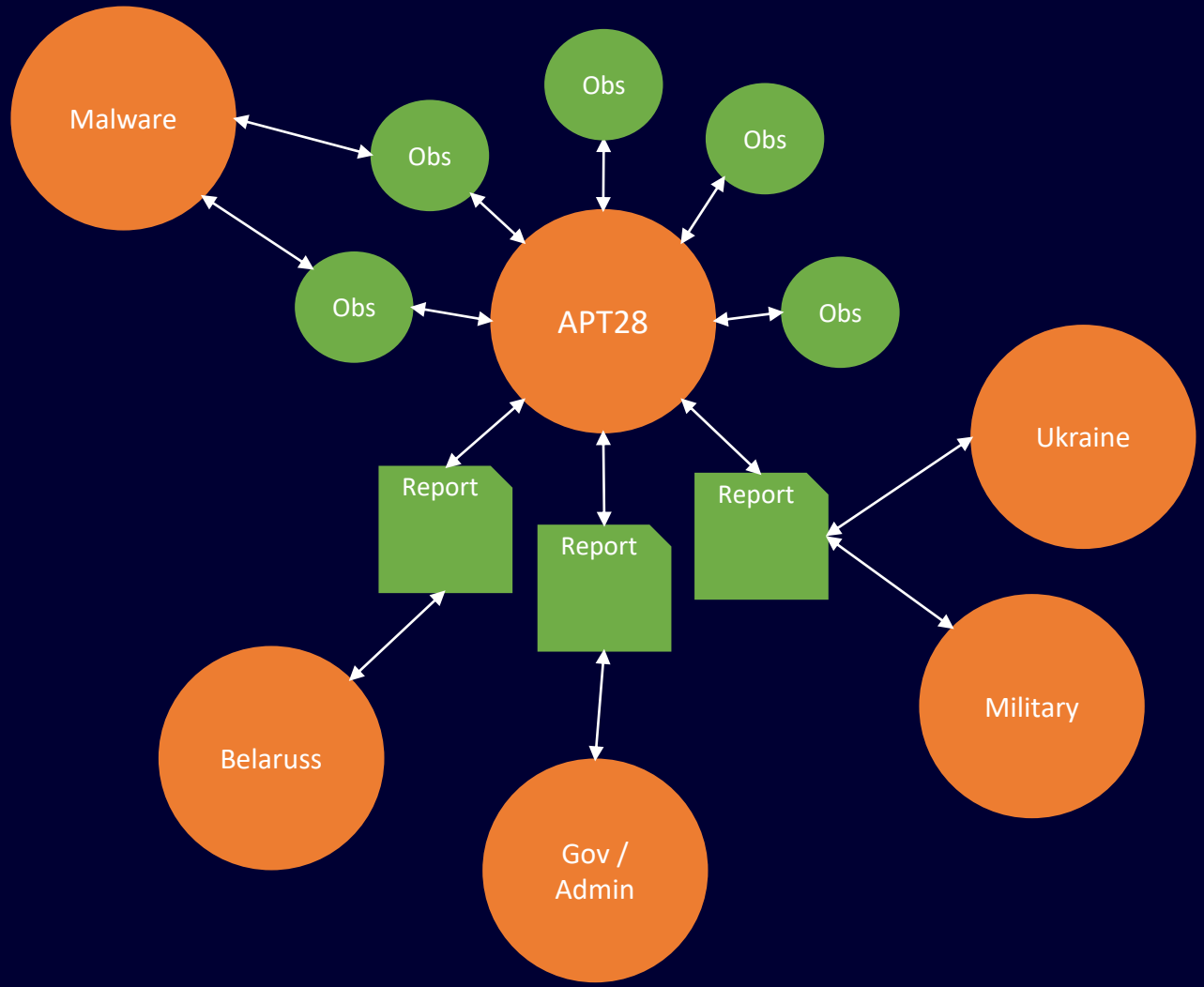
TLP:WHITE

Pivoting



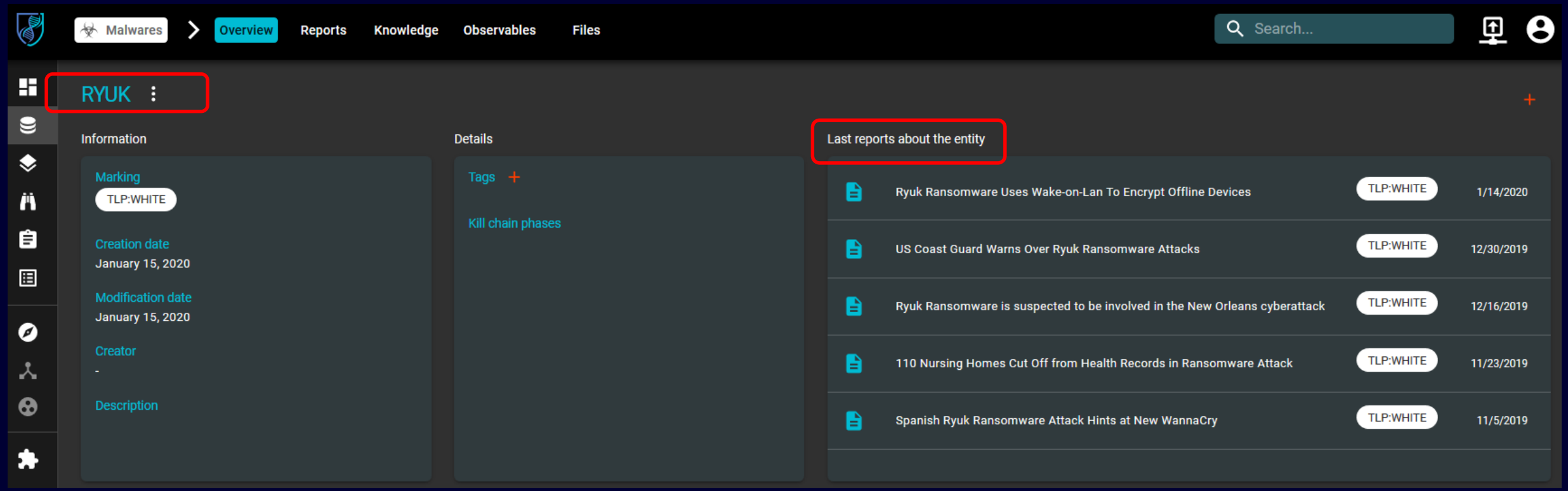
TLP:WHITE

Inference



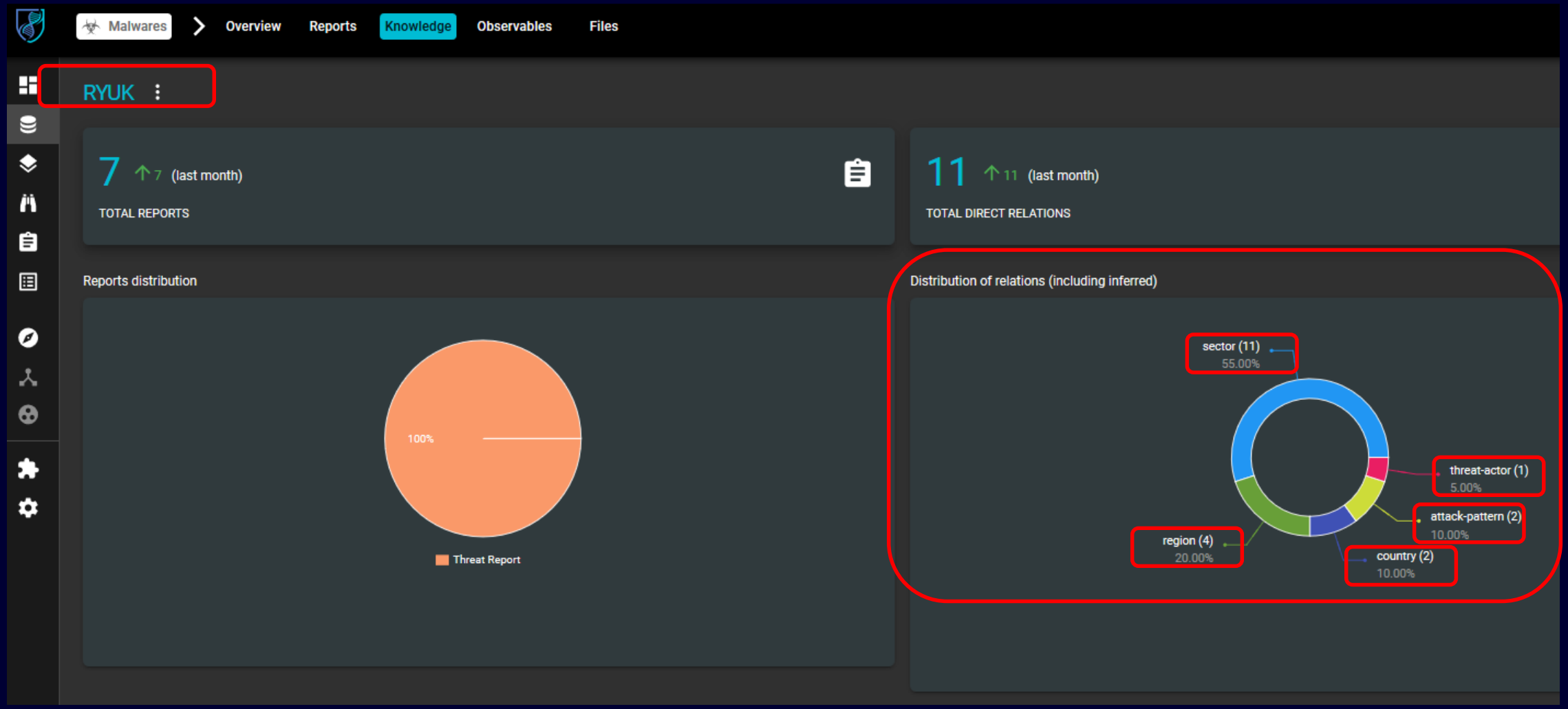
TLP:WHITE

Inference (OpenCTI visualization)



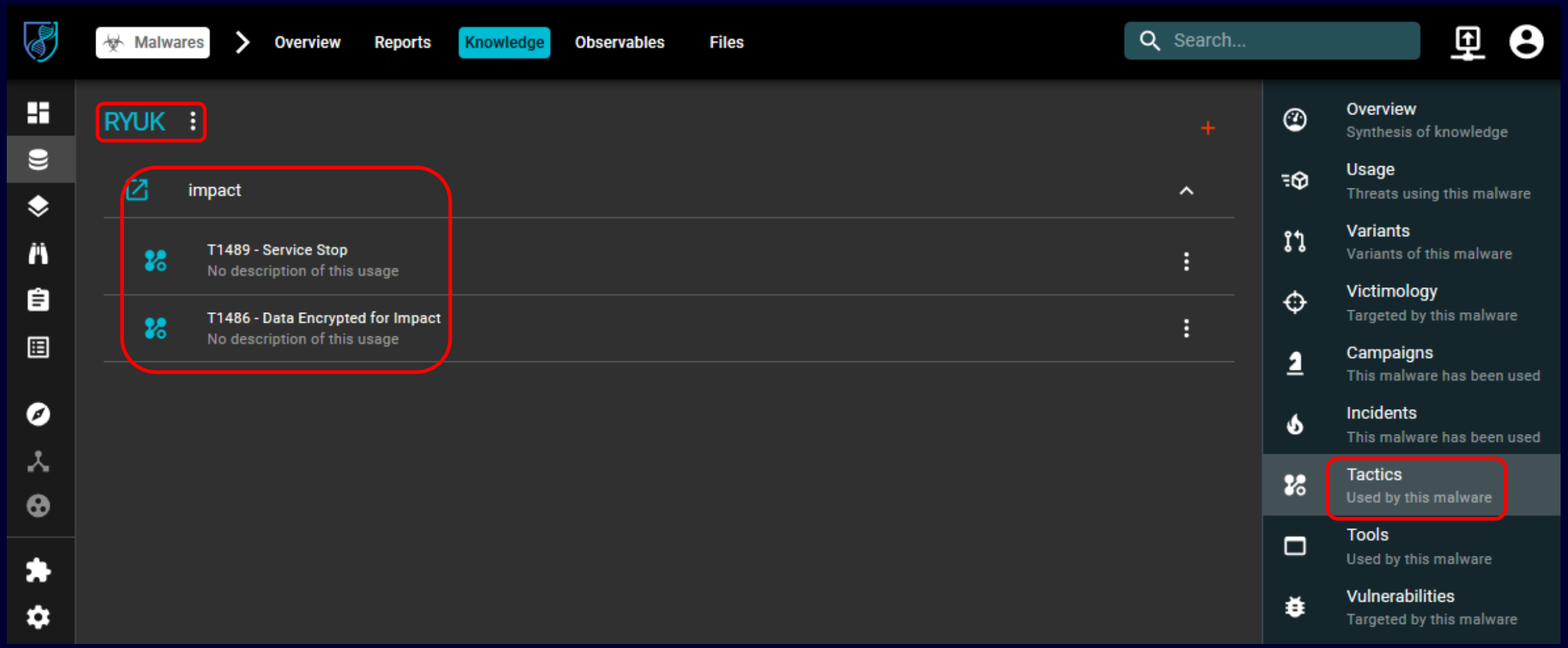
TLP:WHITE

Inference



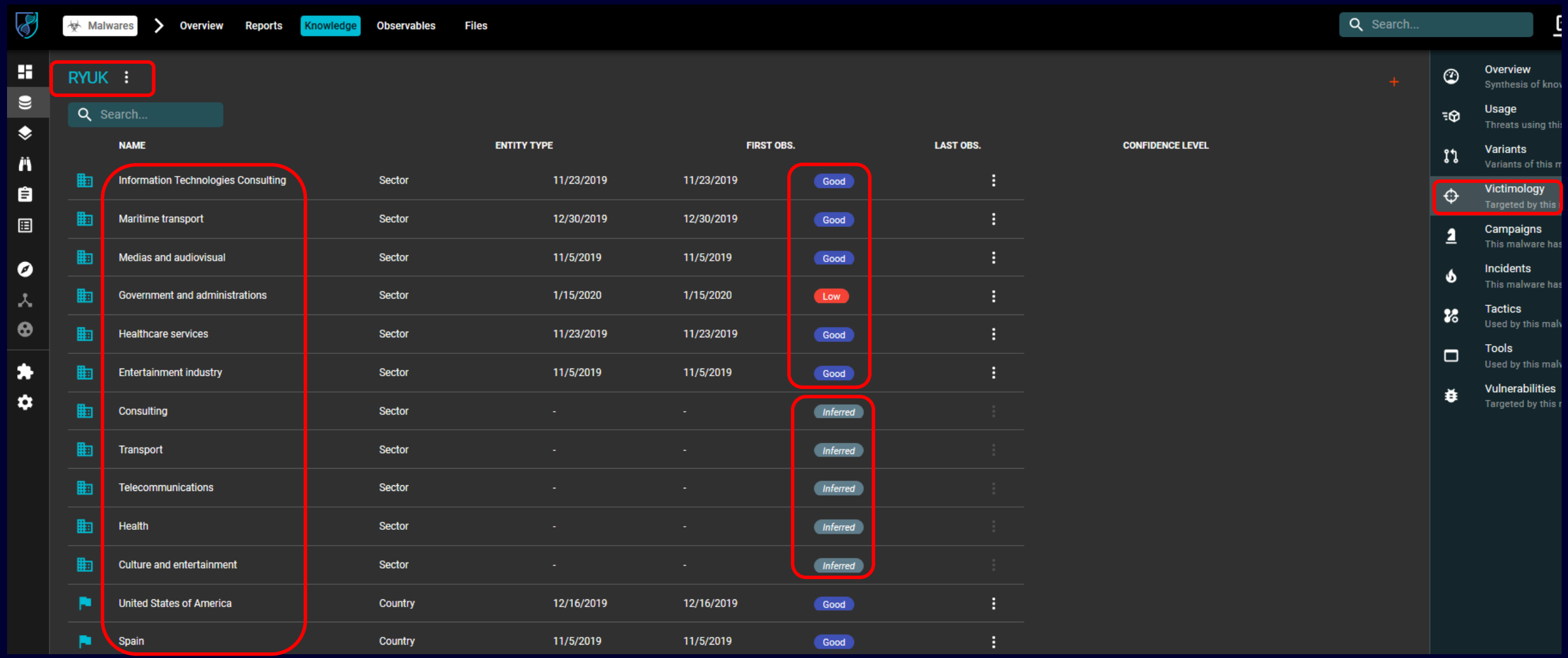
TLP:WHITE

Malware <-> Attack patterns



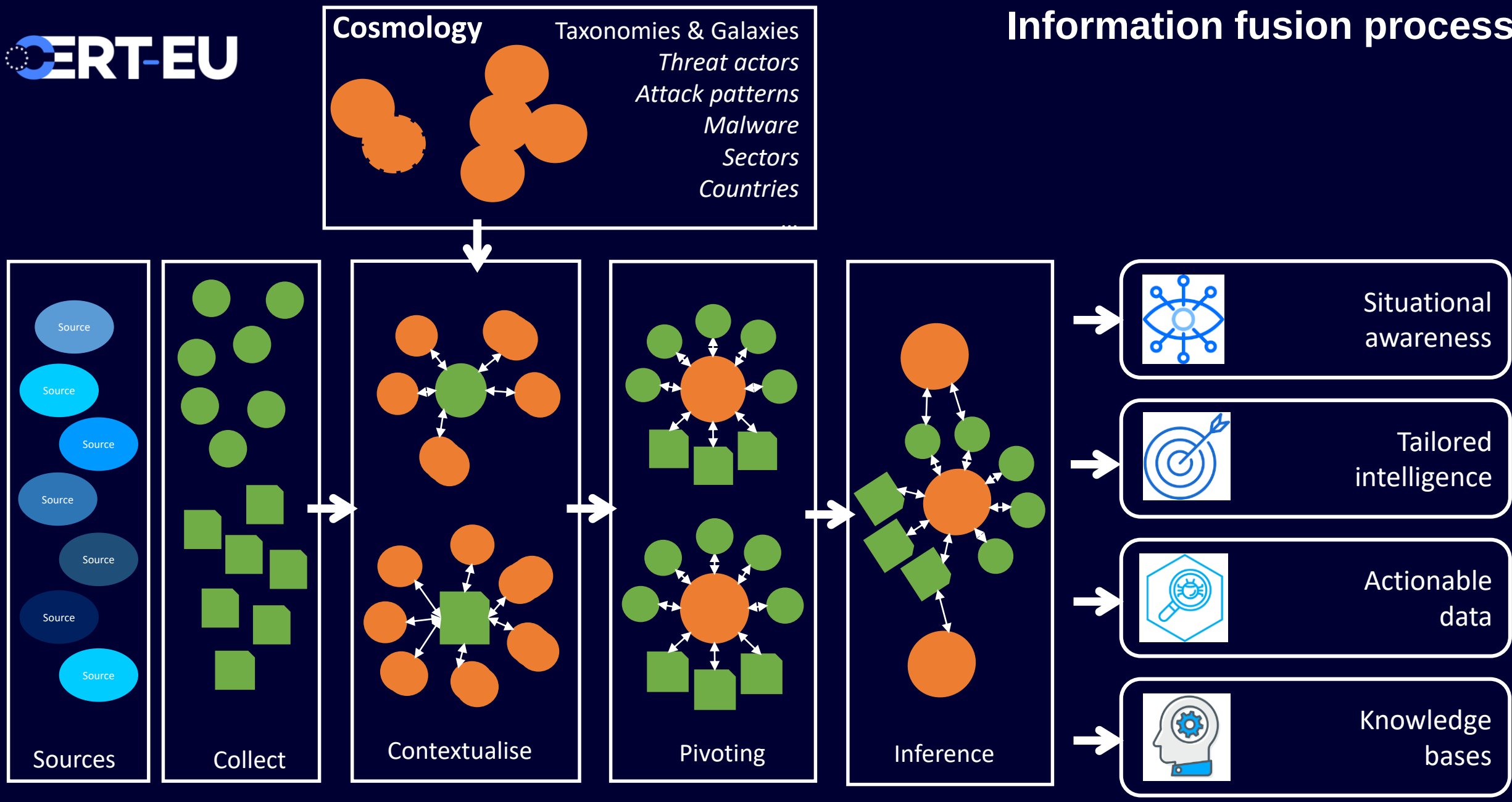
TLP:WHITE

Malware <-> Victimology



TLP:WHITE

Information fusion process



TLP:WHITE

Benefits of information fusion

Qualitative CTI

*merge **a few qualitative** sources for a **limited set of subjects***

- In-depth investigation of *specific* (selected) campaigns or incidents
- Tracking of *specific* (selected) intrusion sets / threat actors or malware families
- Knowledge bases enrichment

“investigative” approach

Quantitative CTI

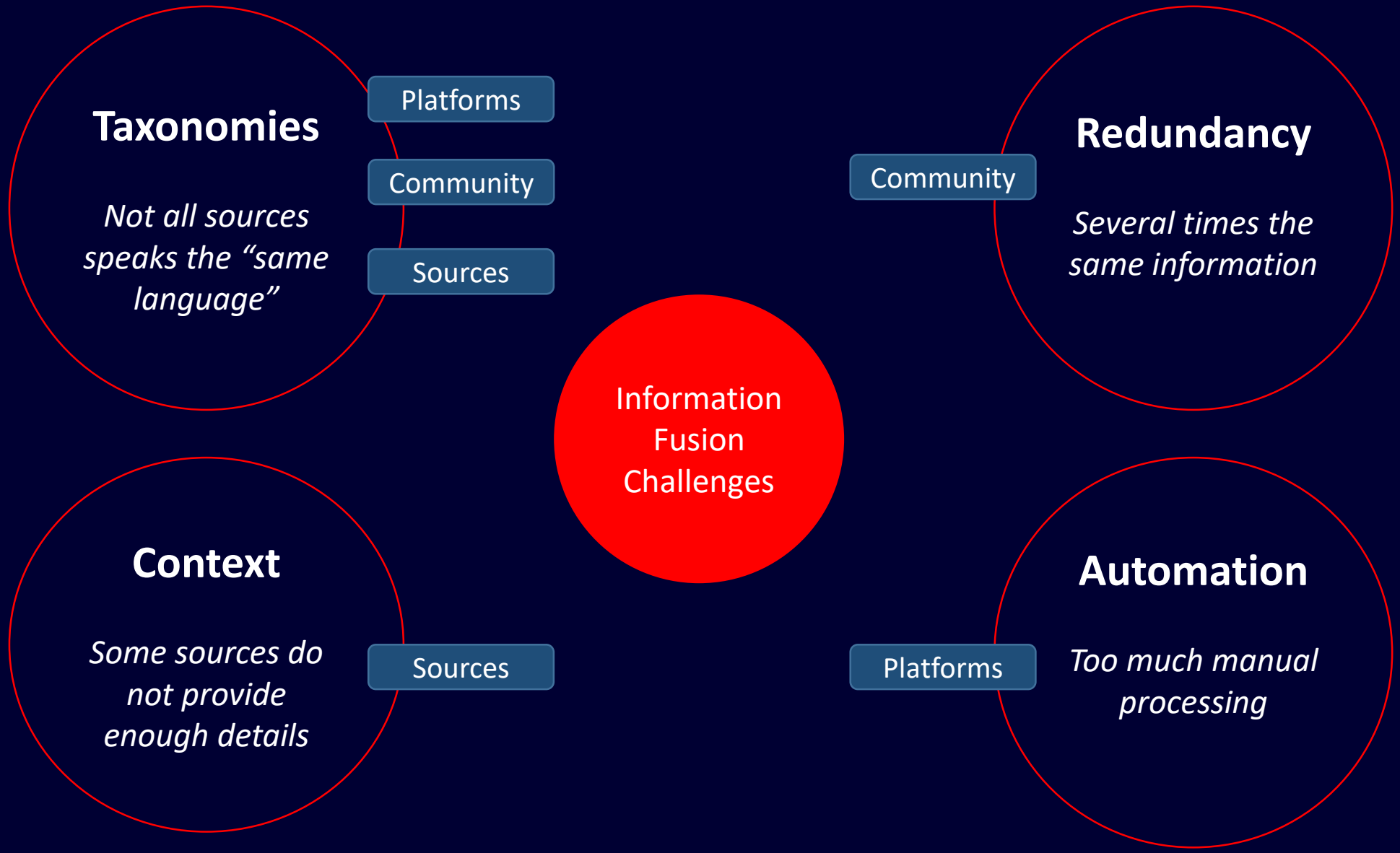
industrial scale** merging of several quantitative – yet reliable - sources for a **large set of subjects

- Monitoring activities of malware, techniques, threat actors / intrusions sets (e.g. determine and rank the most active)
- Monitoring threats per sector, per country, per region
- Monitoring threats from countries

“Landscaping” approach

Challenges

Challenges



TLP:GREEN

Challenge : Redundancy

Issue

- Several sources sharing the same information

OR

- Several organisations relaying the same information (in a community)

- Applies to
  - Reports
  - Observables

Solution / mitigation

- Privilege original sources
- Carefully select and subscribe to aggregators
- Limit OSINT sharing in communities (e.g. MISP)
- Share what YOU see, NOT what OTHERS see

- For observables : unique record based on value
- Develop use of sightings

Challenge : Taxonomies

CERT-EU

Issue

- Sources with different taxonomies
  OR
- Sources with no taxonomies

- Applies to:
  - Observables (type), Sectors, Threat actors, Malware, Countries, Organisations

Solution / mitigation

- For countries, use ISO code (2 letters or 3 letters)
- Develop new taxonomies ?
- Translation between taxonomies ?
- Develop “galaxies” ? → community approach

Challenge : No (structured) context

Issue

- Sources do not provide any context with reports or feeds

  OR

- They provide context in a an unstructured way (no tags)

- For information fusion, manual review is currently needed

Solution / mitigation

- Tools finding and extracting relevant context automatically ?

such as:

- Sectors names
- Countries names
- Malware names
- Threat actors names
- Attack patterns names
- …

Challenge : Automation

CERT-EU

Issue

- Manual operations in the information fusion flow
  - Collection
    - observables : very good level of automation
    - reports : poor level of automation
  - Contextualisation
  - Inferences
  - Analysis
  - Situational awareness

Solution / mitigation

- Taxonomies and structured context
- Step up artificial intelligence in CTI platforms – especially
  - *recognize* victims, TTPs, threat actors, etc
  - *create* smart inferences
  - *assist* situational awareness

Thank you
for
your attention

Contact
frederic.garnier@cert.europa.eu

TLP:WHITE