From 0 to Hero
Actionable Threat Intelligence

Raffaele Di Taranto – Vito Lucatorto

Our Journey in CTI : Problems & Solutions in Critical Infrastructure

ROMHACK

Vito Lucatorto

- Cyber Security Engineer @ FS Holding
- Experience in Banking companies
- Passionate about Threat Intelligence,

APT and Aviation World

- Hunter about new cyber defense

and cyber attack techniques

- Watchwords: Automate all, be curious, cooperate

vitolucatorto@gmail.com

https://www.linkedin.com/in/vlucatorto/

Raffaele Di Taranto

- Cyber Security Engineer @ FS Holding
- MSc Computer Eng @ Turin Politecnico
- Experience in Defence companies
- In love with Cyber Security
- OffSec 4 fun and study: OSCP, ECPPT
- Watchwords: explore cyber at 360°, go deeper in securing architectures, monitor and automate where possible

raf.ditaranto@gmail.com

https://www.linkedin.com/in/rditaranto/

Threat Intelligence: what is it?

Context

Tactics

Resources

Knowledge of the «threat»

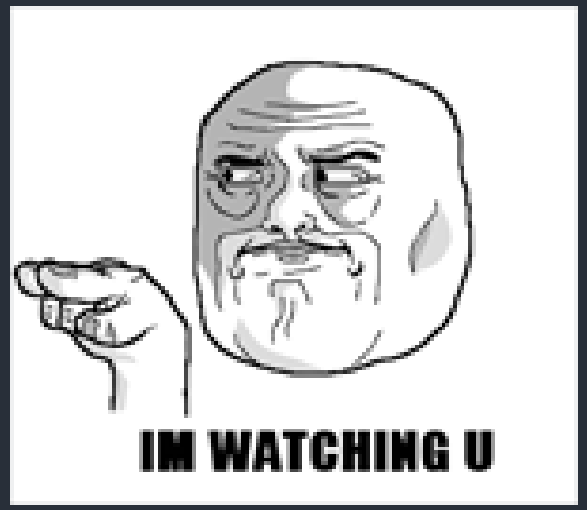
Informed decisions

Attack prevention

Threat Intelligence Idea

How our friends see us

How society see us



How we see ourselves

Just to be clear…this is our myth

Threat Intelligence as a Process

Operational Threat Intelligence

Ongoing cyberattacks, events and campaigns

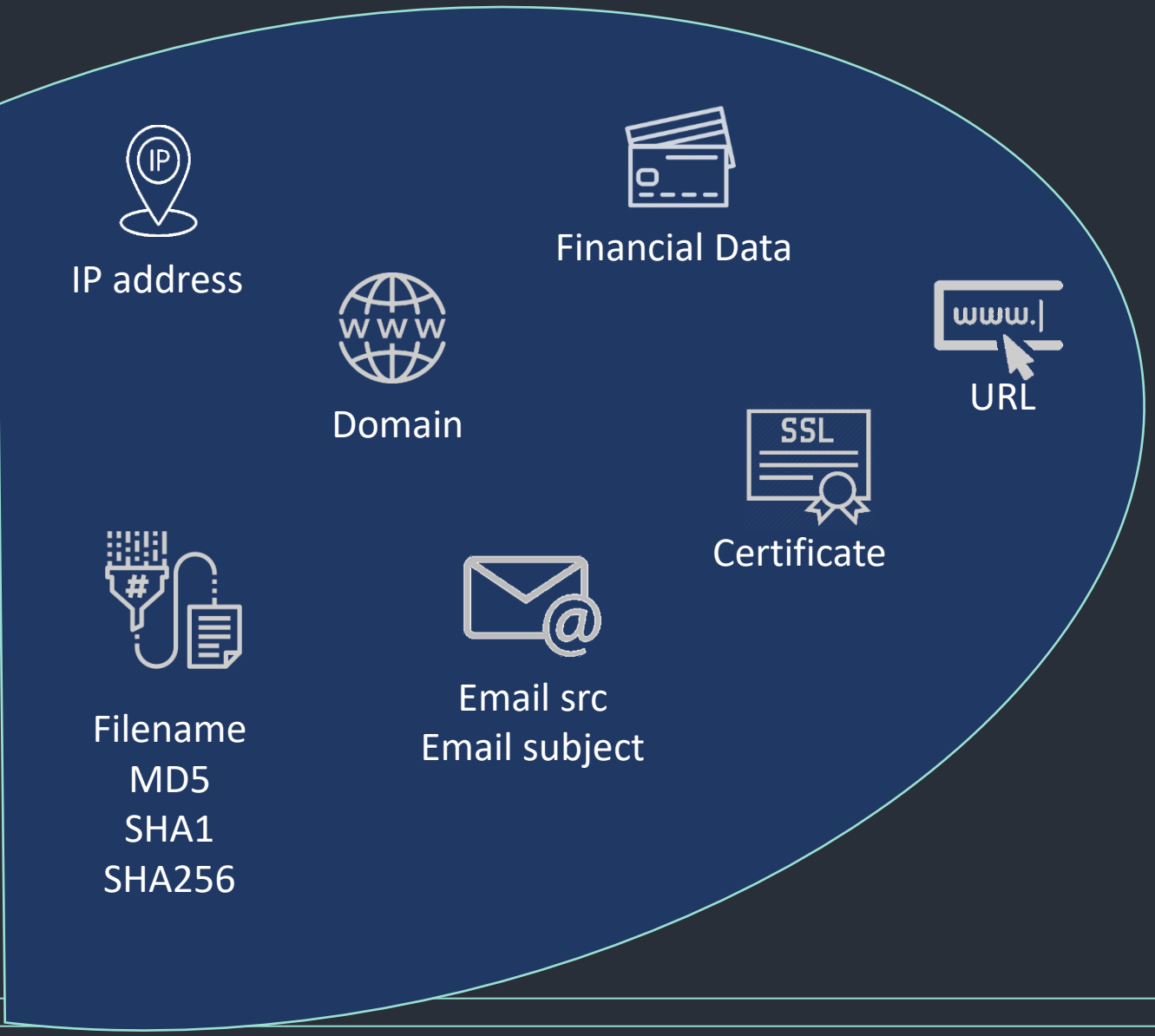
Incident response teams insights on attacks

Speed up processes and make informed decisions

Operational Threat Intelligence Output

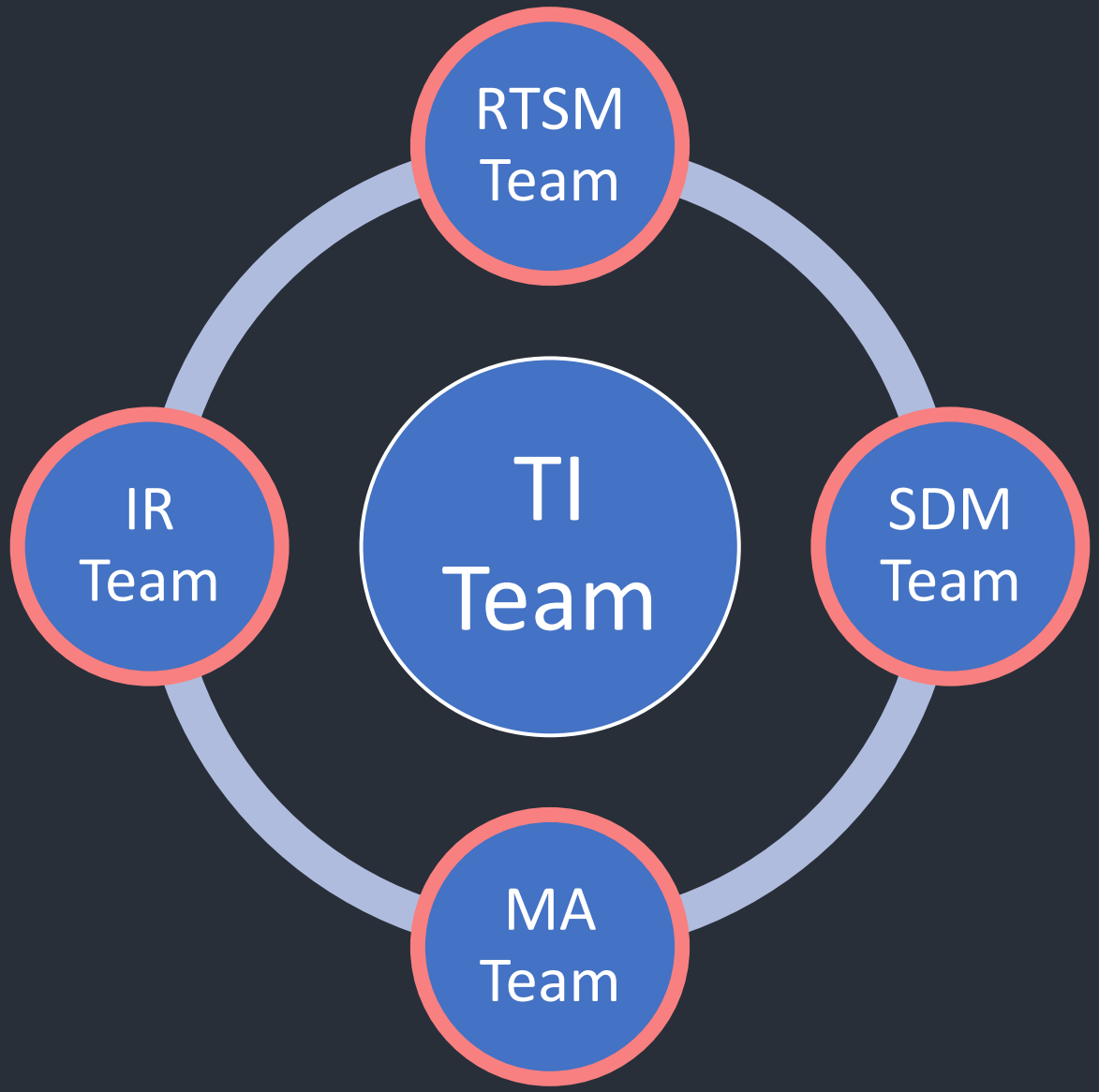
Indicators of Compromise (IoC)

Operational Threat Intelligence Output



- Indicators of Compromise represents technical «**clues**» of the presence of a malicious actor
- More reliable are the clues, less waste of time in security monitoring
- Contextualize the data

Operational Threat Intelligence in SOC



Bla bla bla … Where Is the experience?

Our Big Farm

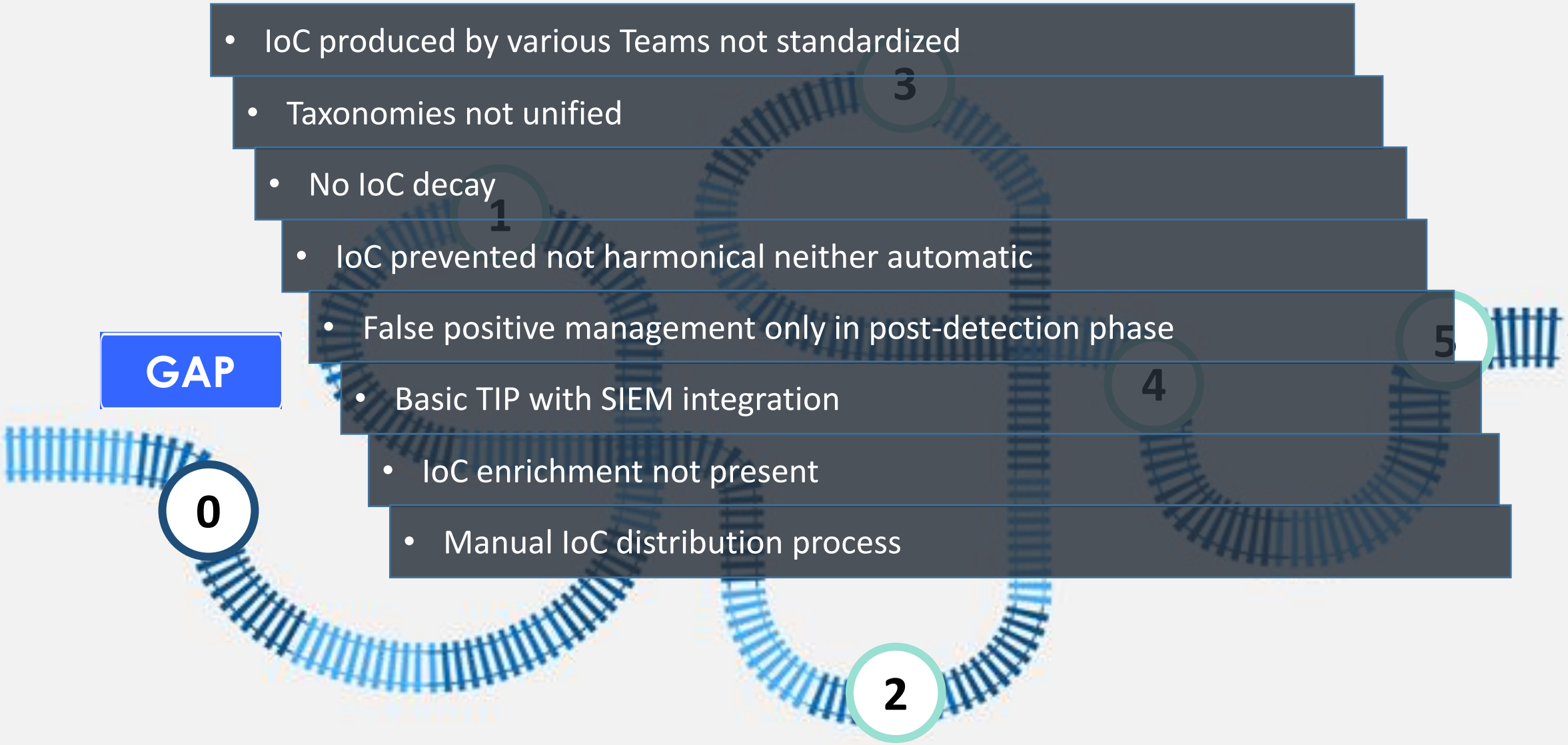
Dati aggiornati al 08/07/2020

Tons of IoC…

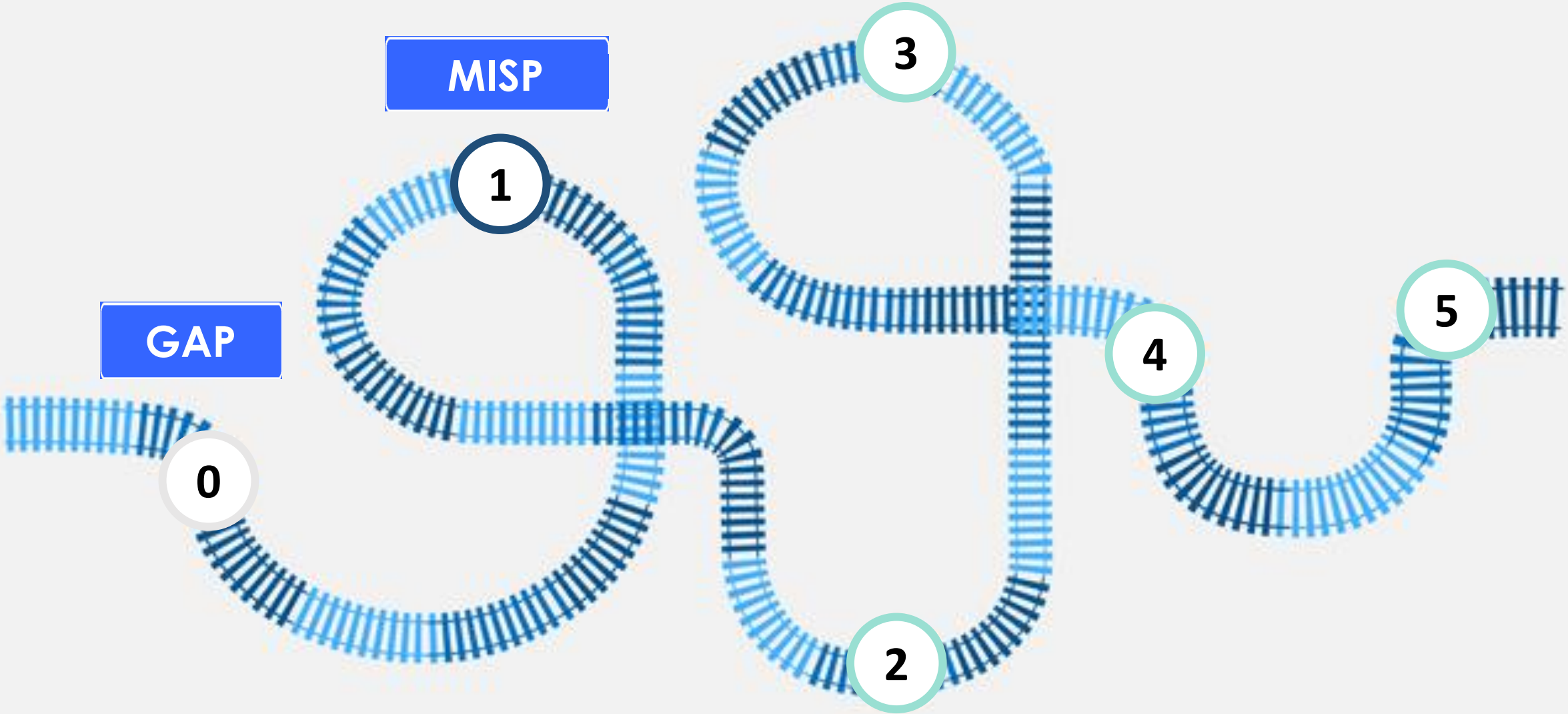
Grow UP!

- Defend the companies
- Give value at single IoC
- Avoid false positives
- Improve Incident Response
- Automate and define all processes

Mind the Gap


• IoC produced by various Teams not standardized
• Taxonomies not unified
• No IoC decay
• IoC prevented not harmonical neither automatic
• False positive management only in post-detection phase
• Basic TIP with SIEM integration
• IoC enrichment not present
• Manual IoC distribution process
GAP
0
1
2
3
4
5

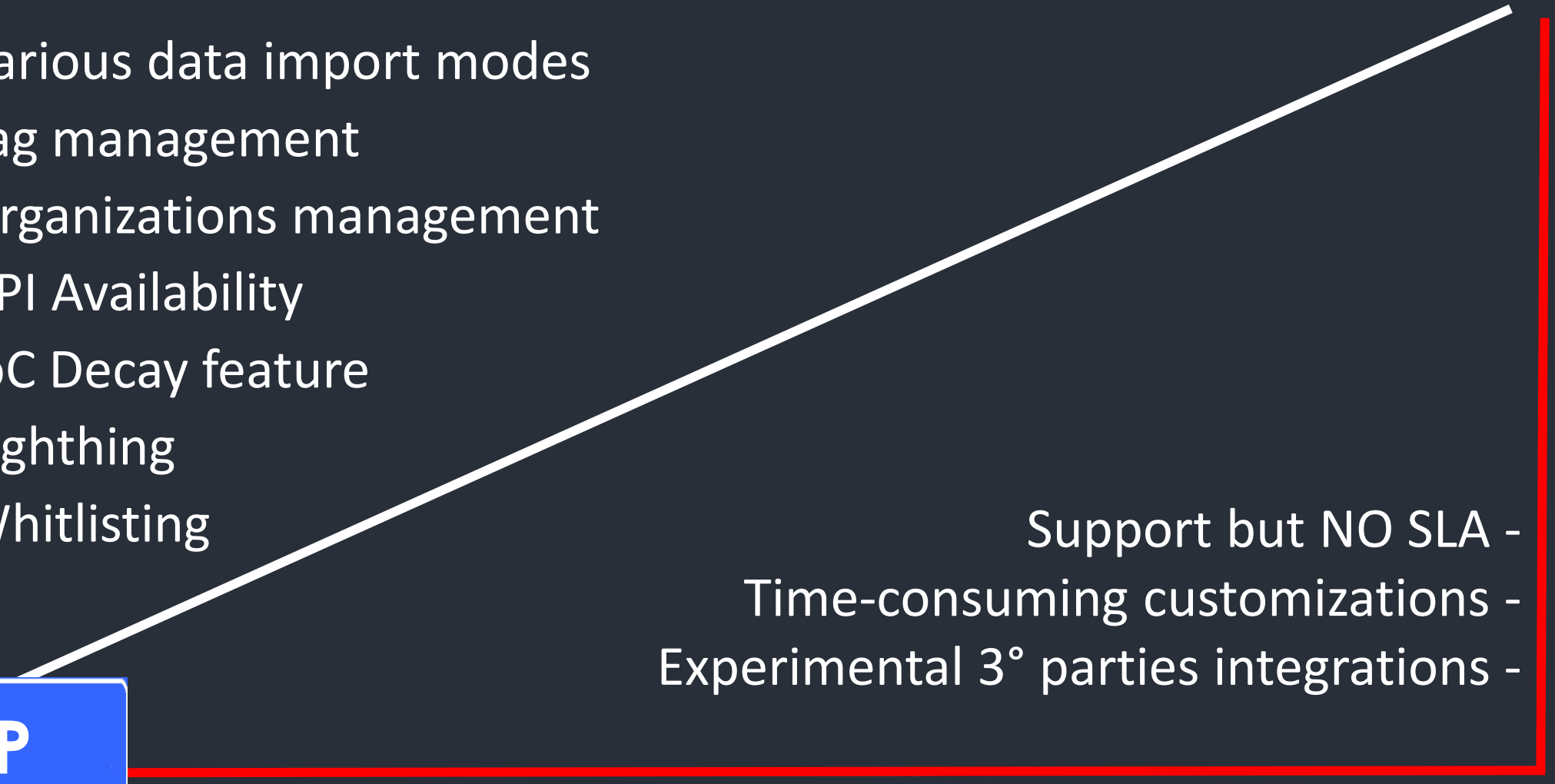
Choose a Threat Intelligence Platform



Choose a Threat Intelligence Platform

PRO

+ Various data import modes
+ Tag management
+ Organizations management
+ API Availability
+ IoC Decay feature
+ Sighthing
+ Whitlisting

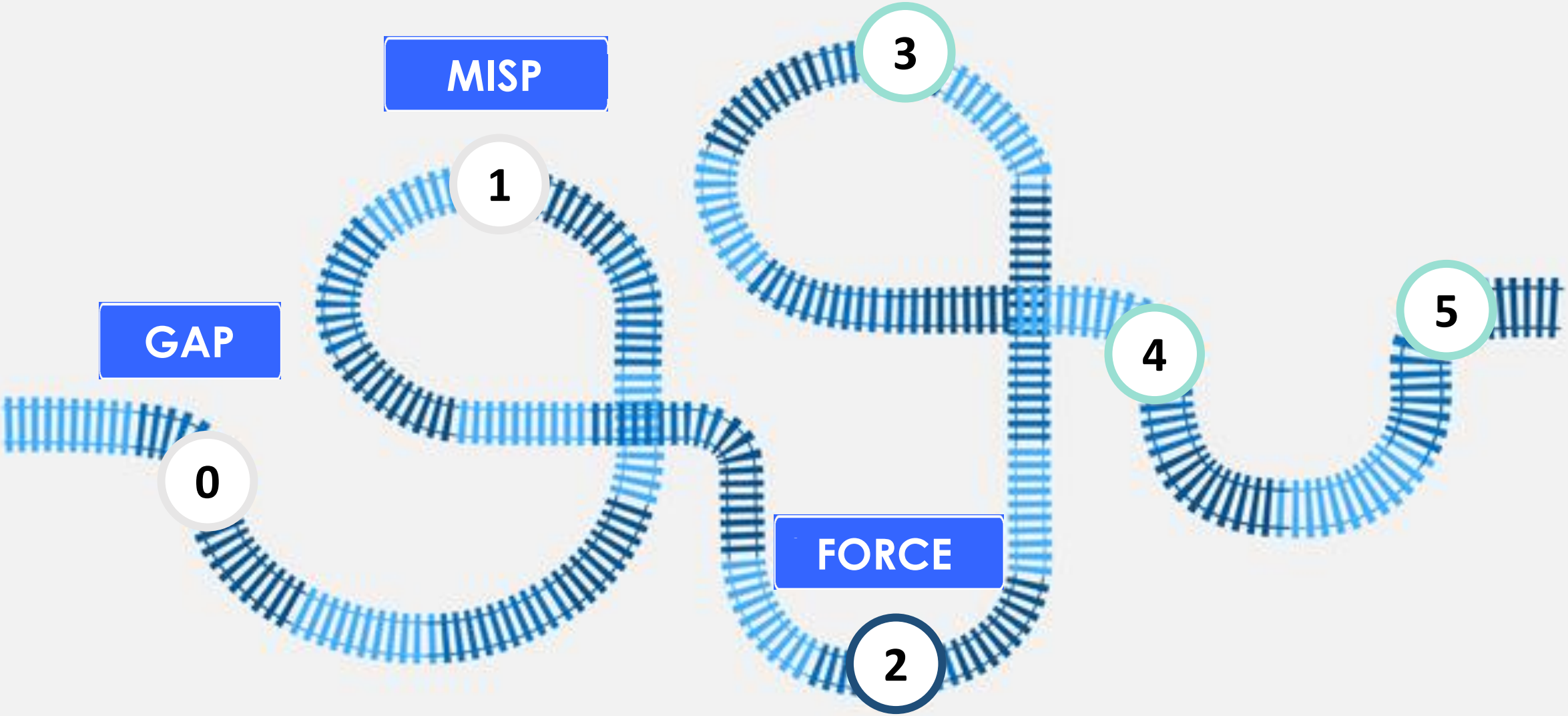


Support but NO SLA -
Time-consuming customizations -
Experimental 3° parties integrations -

CONS

MISP

Improve the FORCE

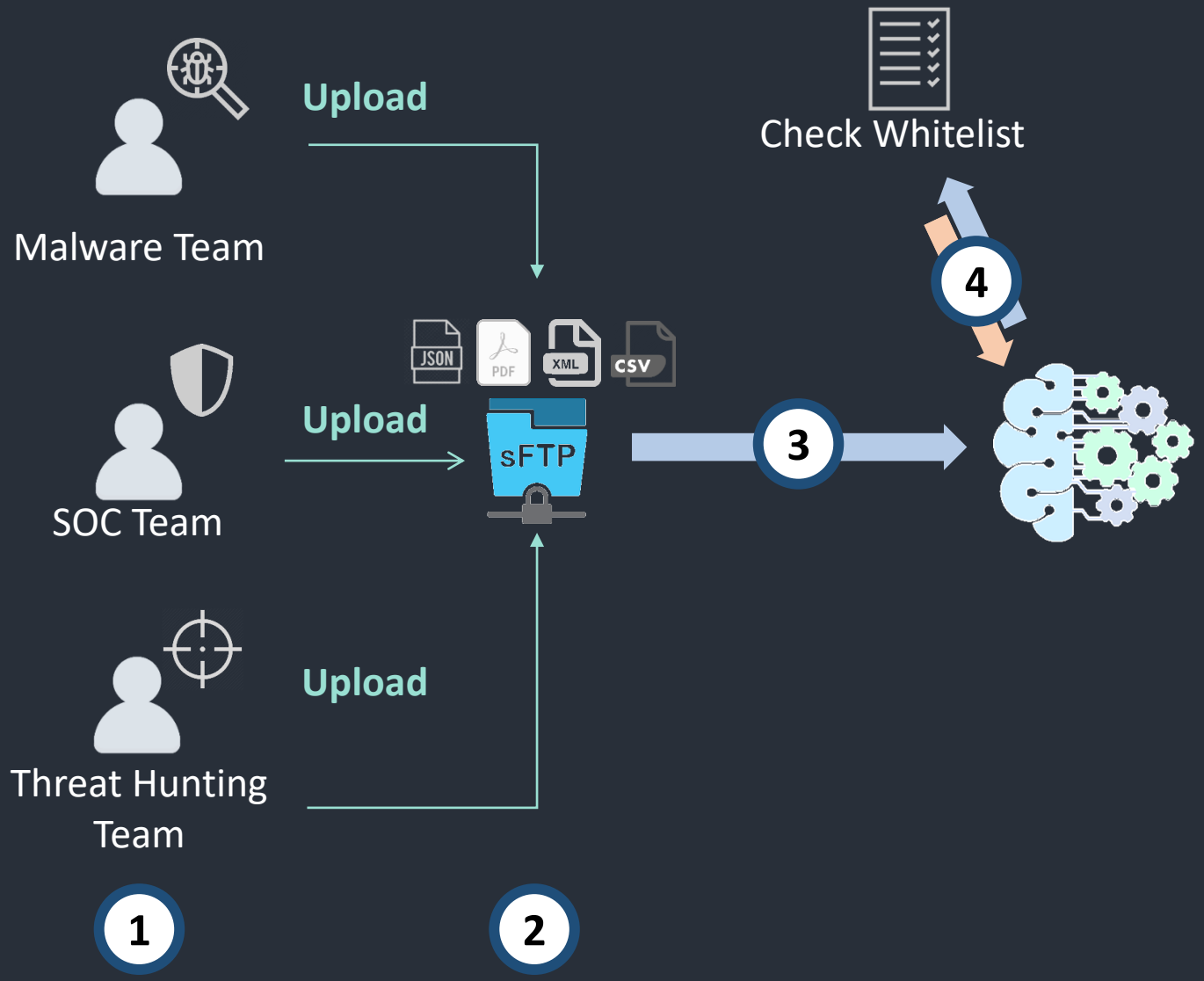


Improve the FORCE

- Automatic Massive import development differentiated by organization and operating group
- Historical Search into Siem
- Whitelist-based detection for false positives avoidance
- Automatic tag system based on fixed variables or natural language
- IoC Enrichment

FORCE

Improve the FORCE - Big Brain at Work



IR Team

MA Team

Improve the FORCE - Example of Whitelisting

IR Team

MA Team

Check Whitelist

4

google.ae

REST API

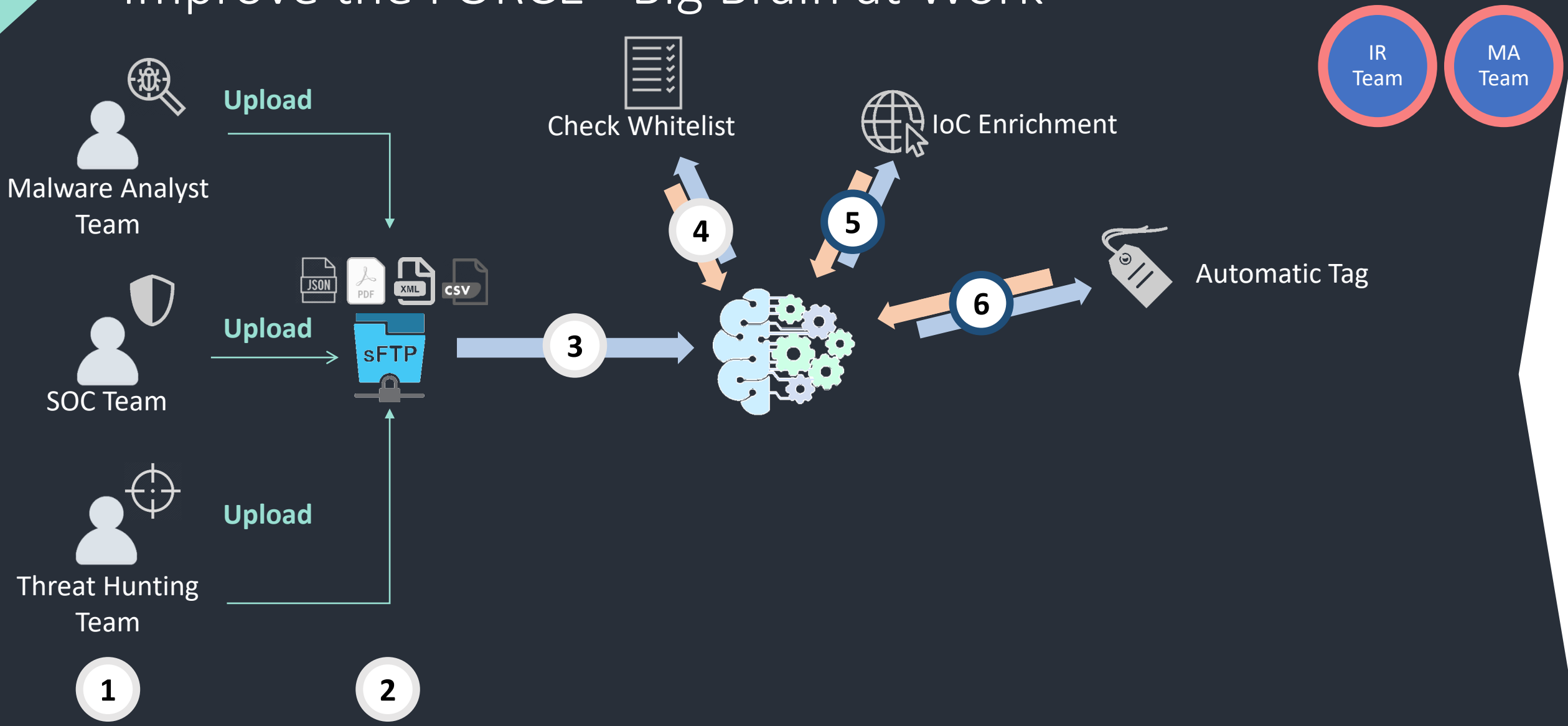
```
"amazon.ca",
"amazon.cn",
"amazon.co.jp",
"amazon.co.uk",
"amazon.com",
"amazon.com.mx",
"amazon.de",
"amazon.es",
"amazon.fr",
"amazon.in",
"amazon.it",
"google.ae",
"google.at",
"google.az",
"google.be",
"google.ca",
"google.ch",
"google.cl",
"google.cn",
"google.co.ao",
"google.co.id",
```

Categoria	Tipo	Valore	Commento	Correlazione	IDS
Network activity	domain	google.ae		☑	☐
Network activity	email-src	@cfr.ro	email sender	☑	☑
Network activity	email-subject		subject	☑	☑
Network activity	url	https://[redacted]/mysite	url phishing	☑	☑

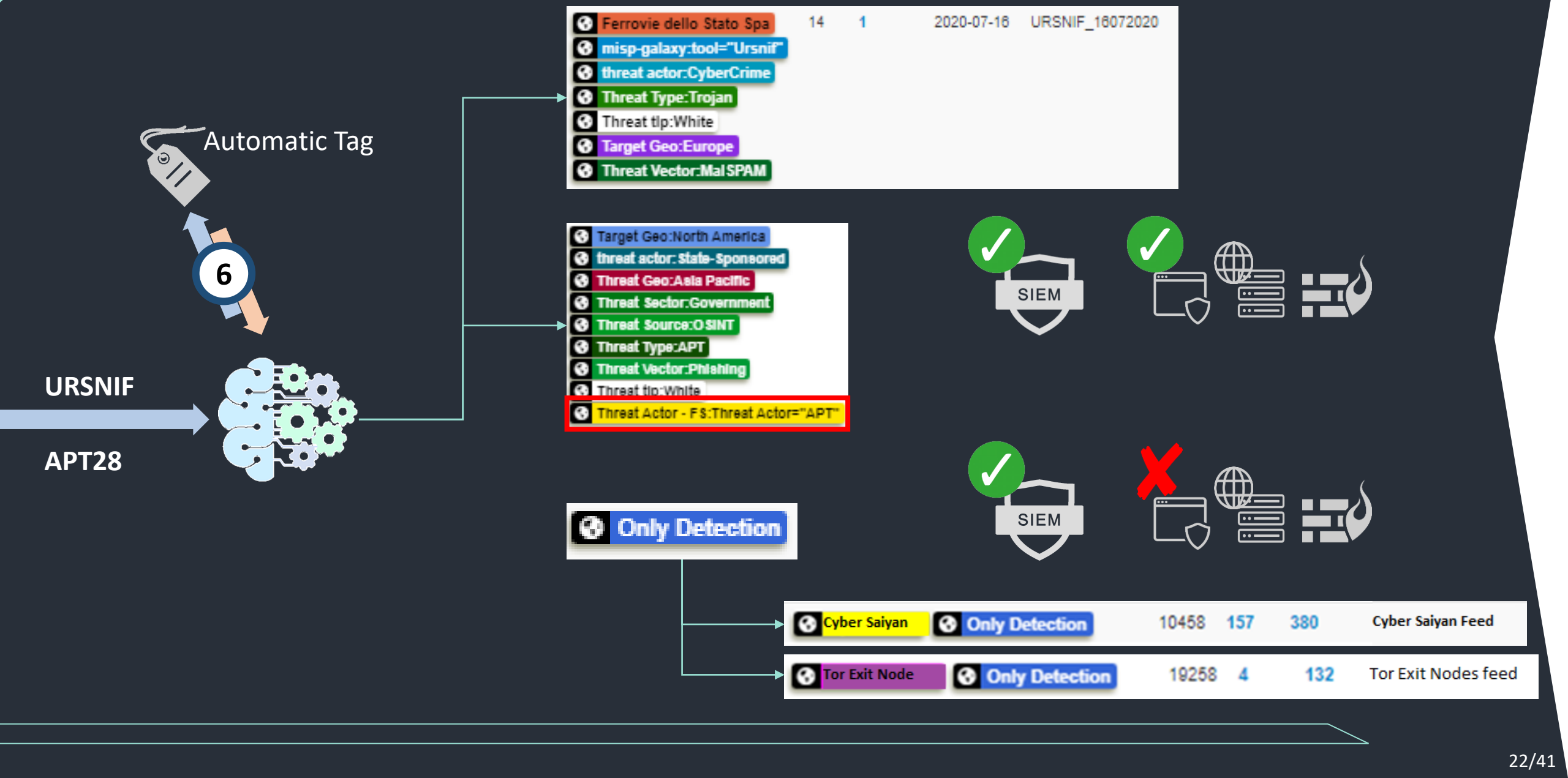
TO_IDS = FALSE

TO_IDS = TRUE

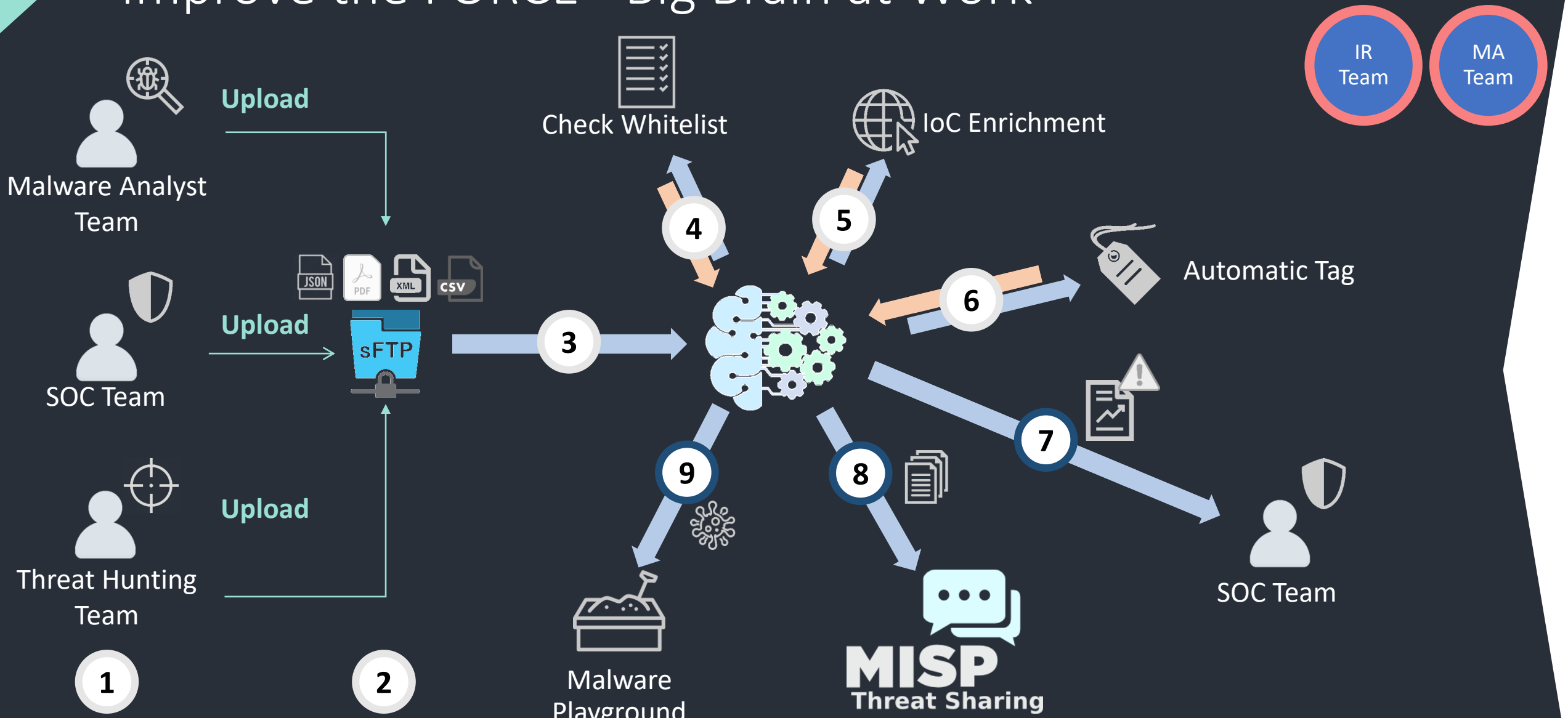
Improve the FORCE - Big Brain at Work



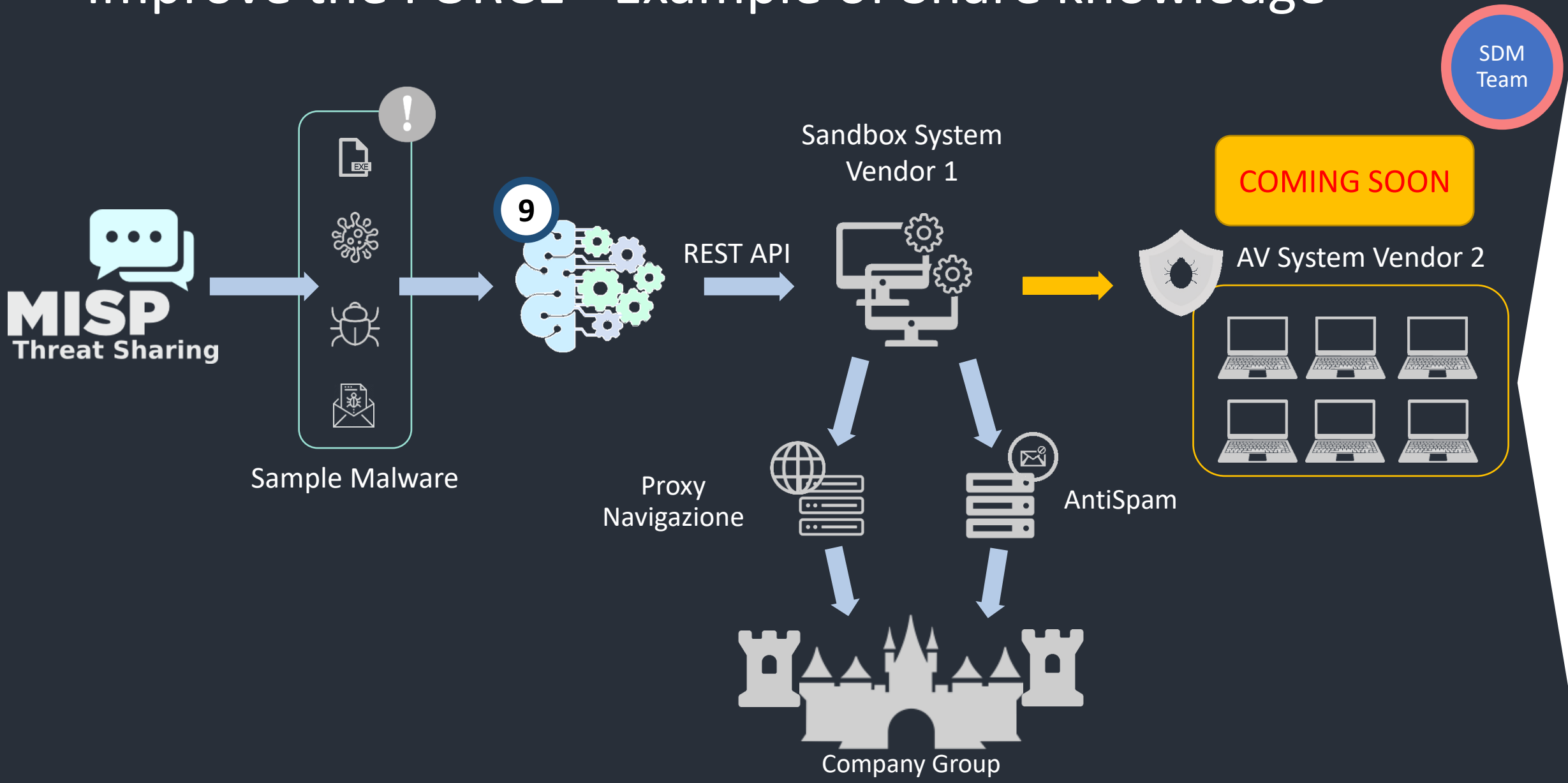
Improve the FORCE - Example of Automatic Tag



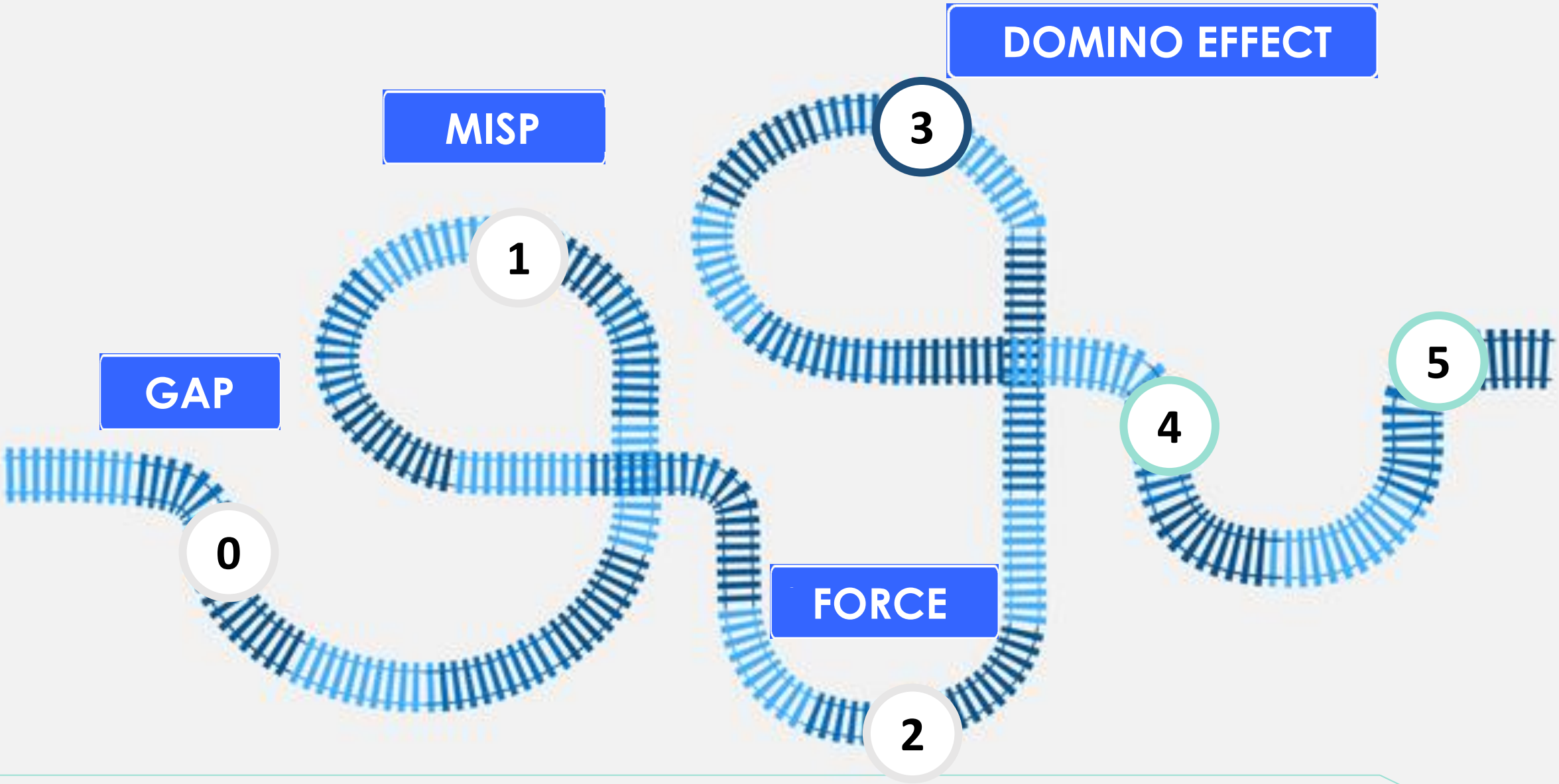
Improve the FORCE - Big Brain at Work



Improve the FORCE - Example of Share knowledge



Explore the Farm



Explore the Farm - Prevention

SDM Team

TO_IDS = TRUE

```
curl -k -X POST -H "Content-Type: application/json" -H
"Authorization: apitoken" -d '{"returnFormat": "json",
"type": {"OR": ["url"]}, "published":true,
"to_ids":true, "enforceWarninglist": 1, "includeEventTags":1,
"tags": {"NOT": ["Only Detection"]}, "includeDecayScore": 1,
"excludeDecayed":1,"modelOverrides": {"threshold":
1},"decayingModel": [21]}' https://misp/attributes/restSearch
> /tmp/json/mispUrlBase
```

MISP Threat Sharing

1

2

Data processing and normalization

Sec System Vendor1 List

```
http://realmalicious.com/bad.php
...
```

```
*//realmalicious.com/bad.php
...
```

Sec System Vendor2 List

Explore the Farm - Prevention

SDM Team

MISP Threat Sharing

1

2

3

Data processing and normalization

REST API

Web exposed IoC lists

FIREWALL, WAF & PROXY

OTHER COMPANIES SEC/ICT TEAMS

Explore the Farm - Detection

RTSM Team

IR Team

Automated scheduled data preparation for SIEM ingestion

ACTION

Metadata normalization

\+ IoC → Data Enrichment

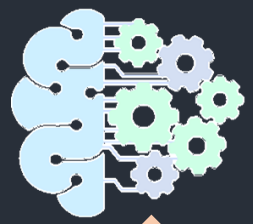
Explore the Farm - Detection

RTSM Team

IR Team

TO_IDS = TRUE

1



2

3

TI Automated Import

Data processing and normalization

Explore the Farm – Focus on SIEM

RTSM Team

IR Team

IoC enrichment

IoC list match

IoC type: url
IoC campaign: lokibot
IoC source: MA team
IoC Threat type: malware
IoC date: 26/09/2020

IoC value: http://realmalicious.com/bad.php
url: http://realmalicious.com/bad.php
domain: realmalicious.com
ip src: 10.10.10.5

```
Sep 27 12:22:22 proxy1 CEF:0|webnavig|
url=http://realmalicious.com/bad.php src_ip=10.10.10.5
src_port=6734
```

```
Sep 27 12:22:22 fw1 CEF:0|fwinternet|
domain=realmalicious.com uri=bad.php srv=80 sip=10.10.10.5
sport=6734
```

Explore the Farm - Detection

RTSM Team

IR Team

Automated scheduled data preparation for SIEM ingestion

Metadata normalization

IoC → Data Enrichment

ACTION

RETROACTION

SIEM

Register IoC sightings

Real Time correlation rules for IoC detection and report sighting via API to MISP

DOMINO EFFECT

Explore the Farm - Detection

RTSM Team

IR Team

TO_IDS = TRUE

TO_IDS = TRUE

MISP Threat Sharing

1

2

3

TI Automated Import

SIEM

ALERT: IoC Detected

4

SOC Team

5

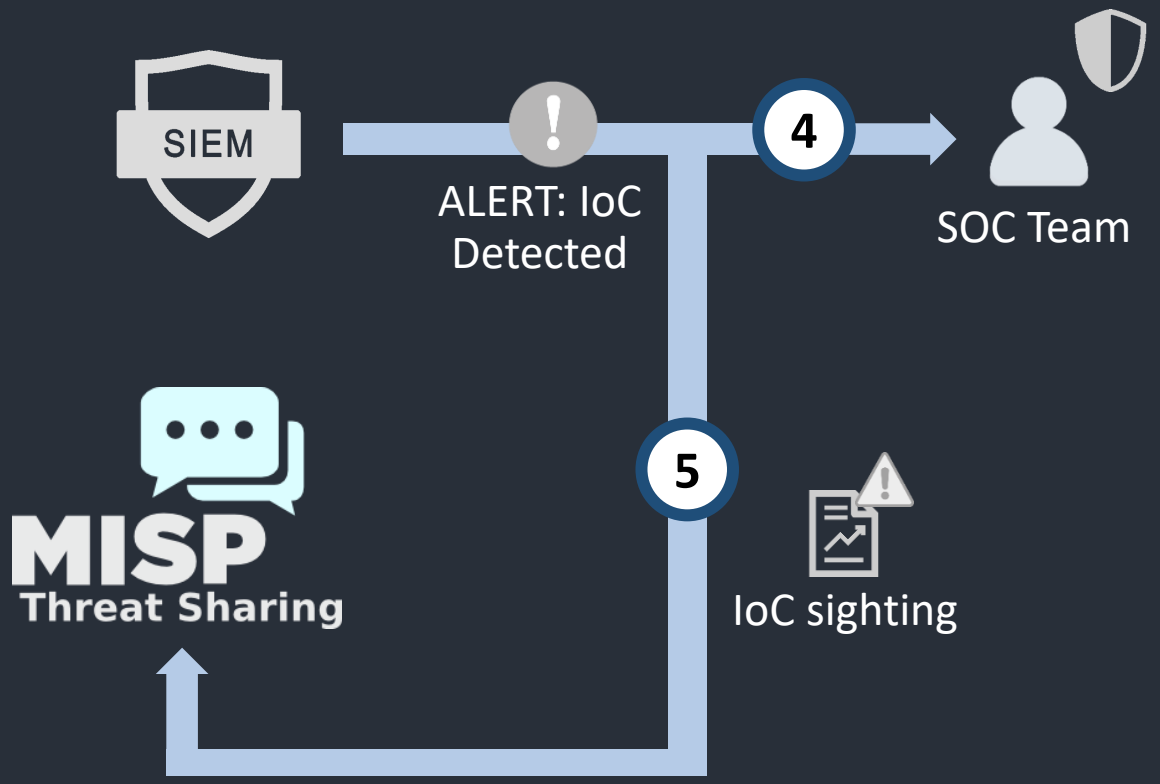
IoC sighting

Data processing and normalization

Explore the Farm - Detection

RTSM Team

IR Team

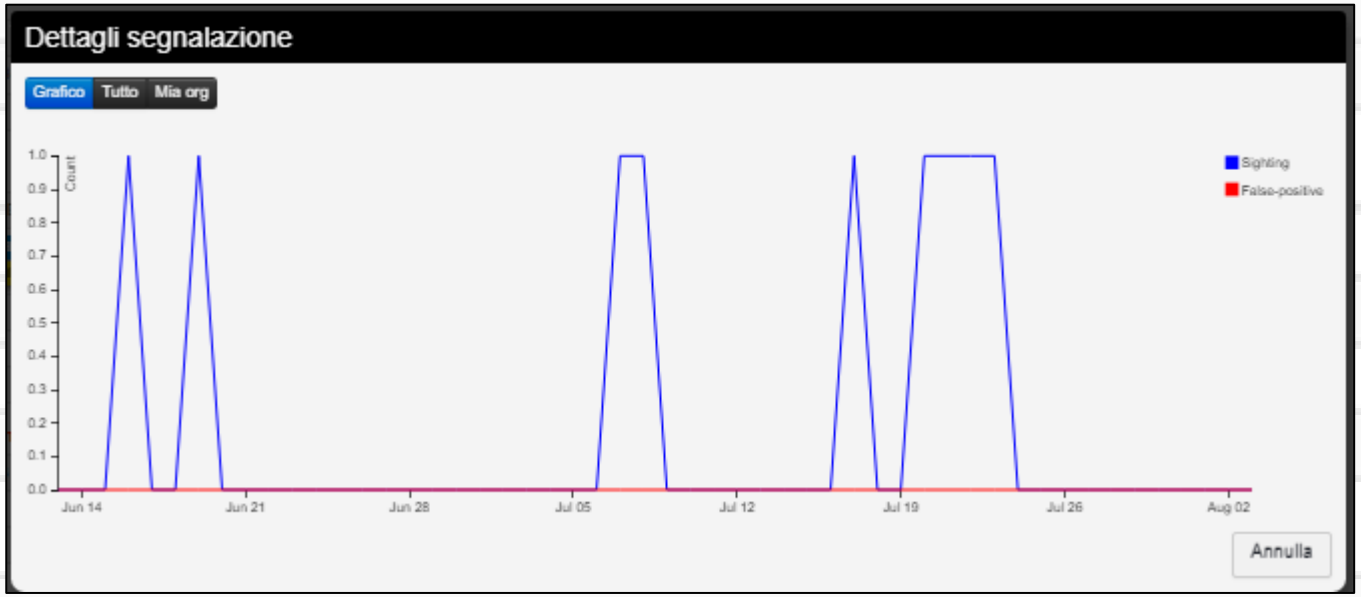


INC-402189	7/27/2020 8:22 AM	Indicator of Compromise Network	Escalated

```
curl -d "{\"source\":\"SIEM\", \"values\":"http://realmalicious.com/bad.php"}" -H
"Authorization: apitoken" -H "Accept: application/json" -H "Content-type:
application/json" -k -X POST "https://misp/sightings/add
```

Winnie the Pooh is a threat actor

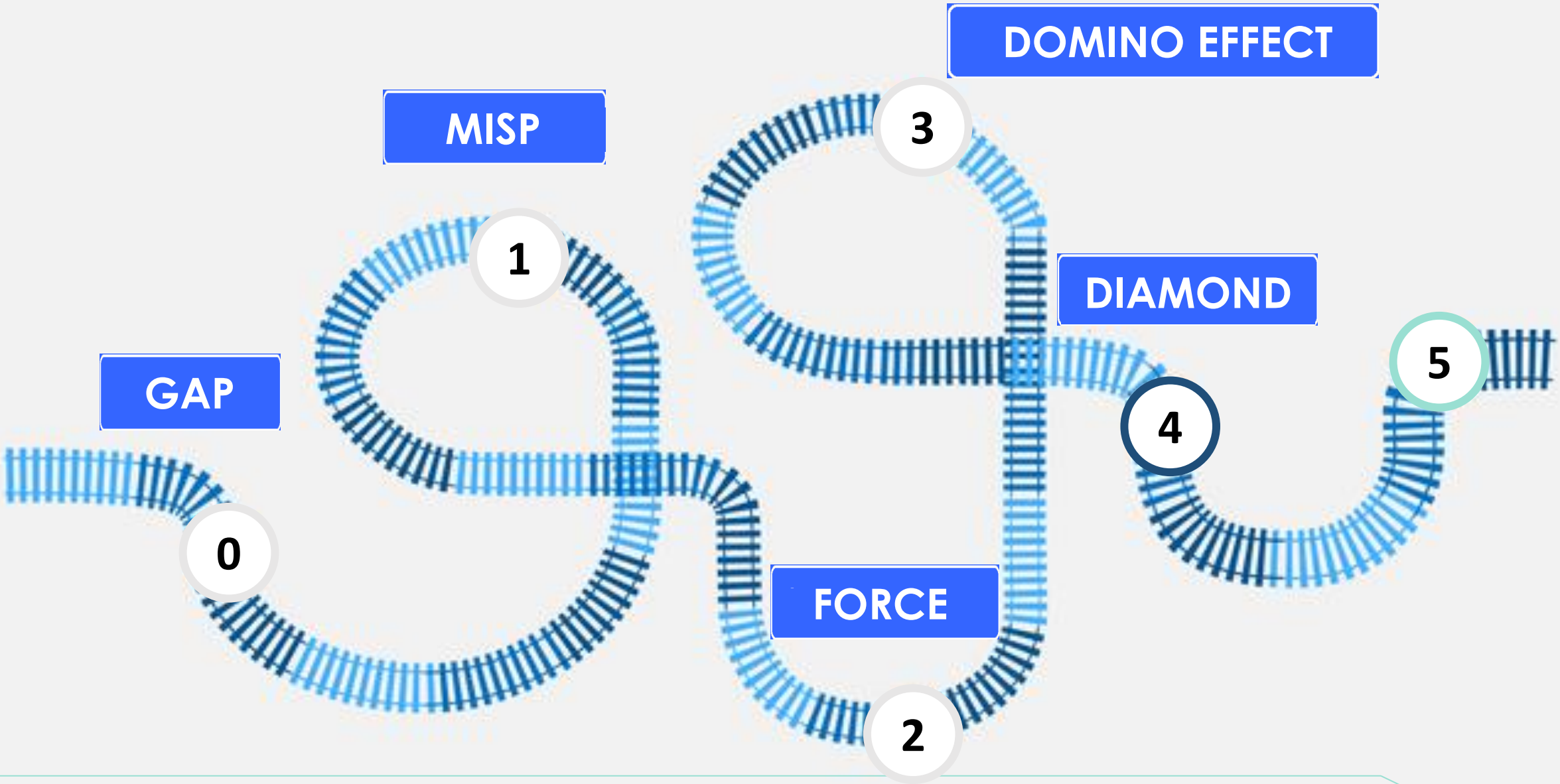
ID Evento	7101
UUID	5edfa031-15ec-4bc9-8678-0fe30a0a2864
Organizzazione proprietaria	Ferrovie dello Stato Spa
Tag	Threat actor:CyberCrime x · Threat Sector:Finance x · Threat Type:Malware x · Threat tlp:White x · Threat Actor - FS:Threat Actor="APT" x
Data	2020-06-09
Analisi	Completed
Distribuzione	Solo la tua organizzazione
Pubblicato	Sì (2020-07-06 13:12:12)
#Attributi	166 (0 Object)
Prima modifica registrata	2020-06-09 14:44:12
Ultima modifica	2020-06-23 15:24:39
Modification map	
Sighting	9 (9) - limitato ai proprietari di organizzazione.
Attività	



☐	2020-03-31	Network activity	url	http://realmalicious.com/bad.php

(5/0/0)

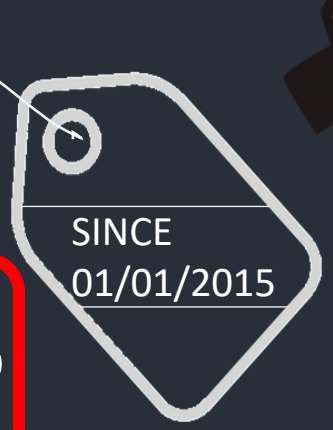
Destroy the diamond…



Destroy the diamond…

IoCs are NOT forevah !

`http://realmalicious.com/bad.php`



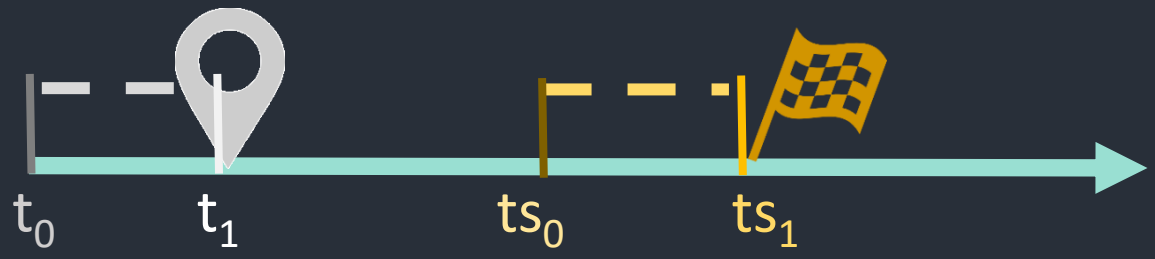
- When URL is no more malicious?
- Waste of resources preventing it nowaday ?
- And if you have 100 billions sculptured on sec techs?

In Practice

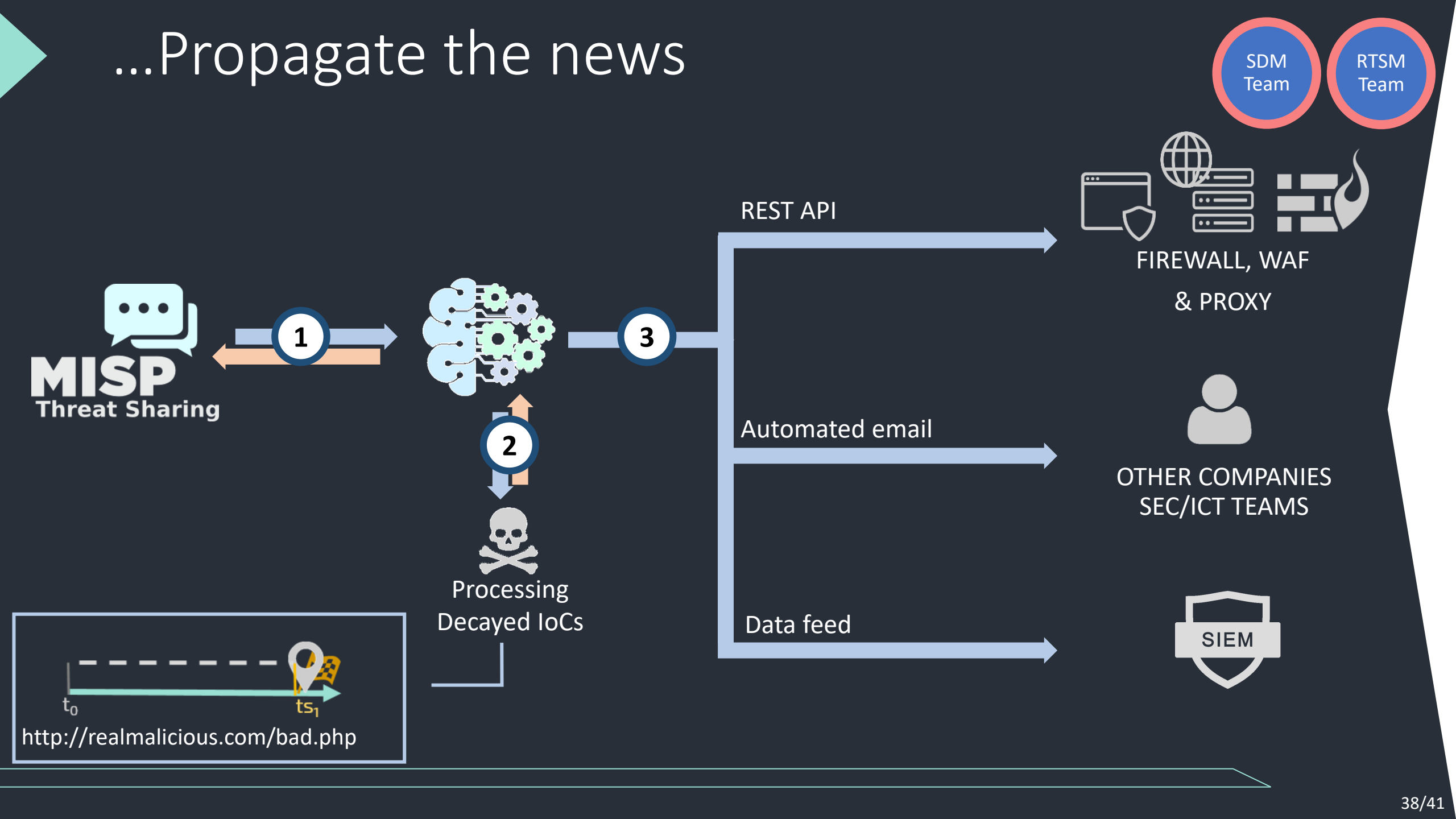
http://realmalicious.com/bad.php

Sighting to MISP

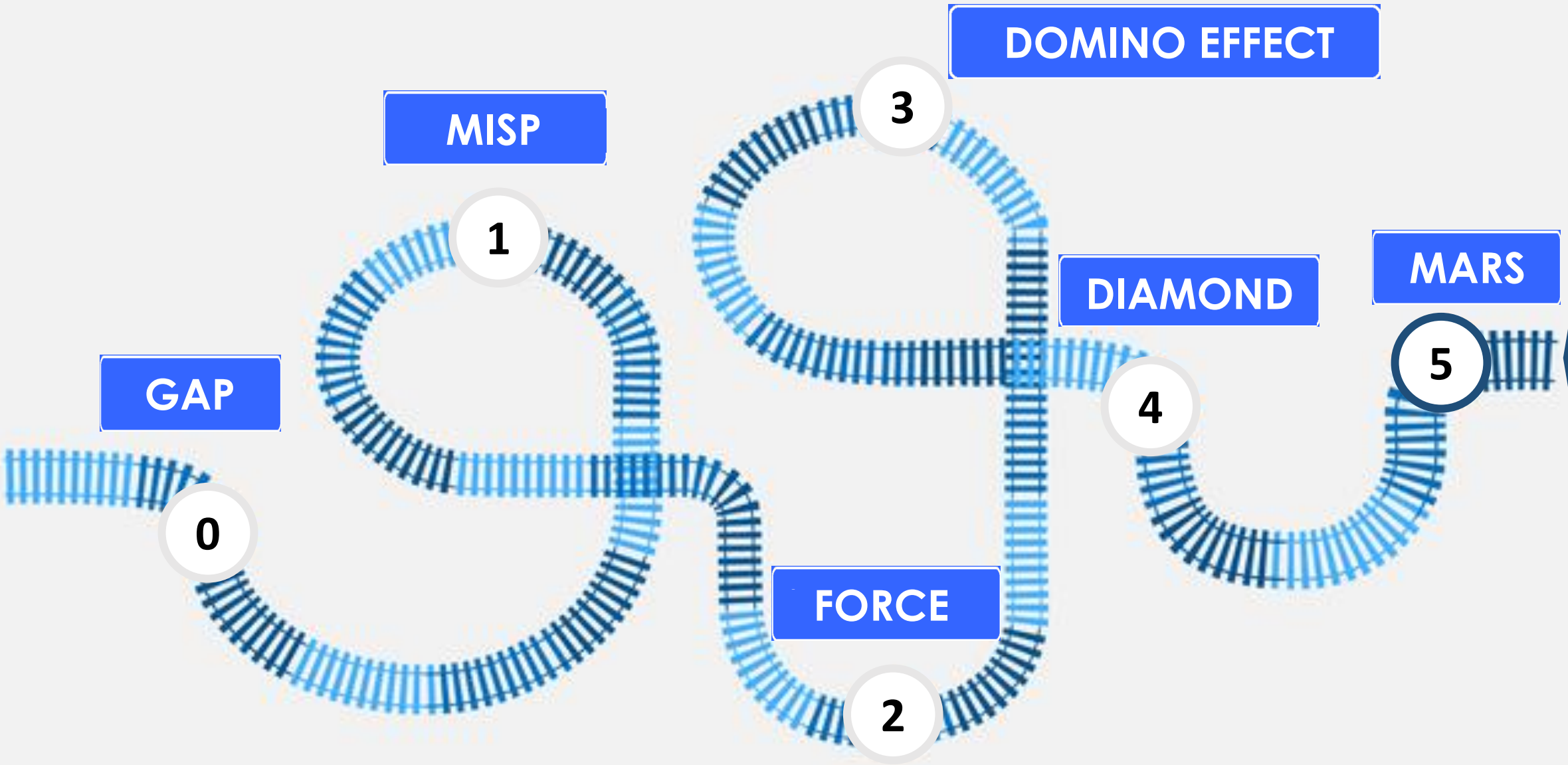
IoC time is over



…Propagate the news



From Train to Rocket



From Train to Rocket

- Integrated Dashboard & report system
- TLP-based IoC visibility for different roles
- Incident full prioritization
- Threat data feeds supply input for threat intelligence, but by themselves are not threat intelligence
- COLLABORATION !

MARS

THANK YOU

…QUESTIONS?