RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: HT-F03

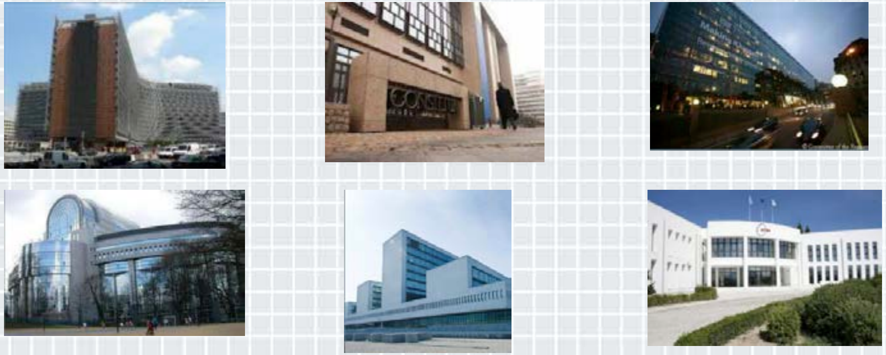
STIX in Practice for Incident Response

Freddy Dezeure

Head of CERT-EU

http://cert.europa.eu/

About Us



- EU Institutions’ own CERT
- Supports 60+ entities
- Operational defense against cyber threats

Other EU Cyber Bodies

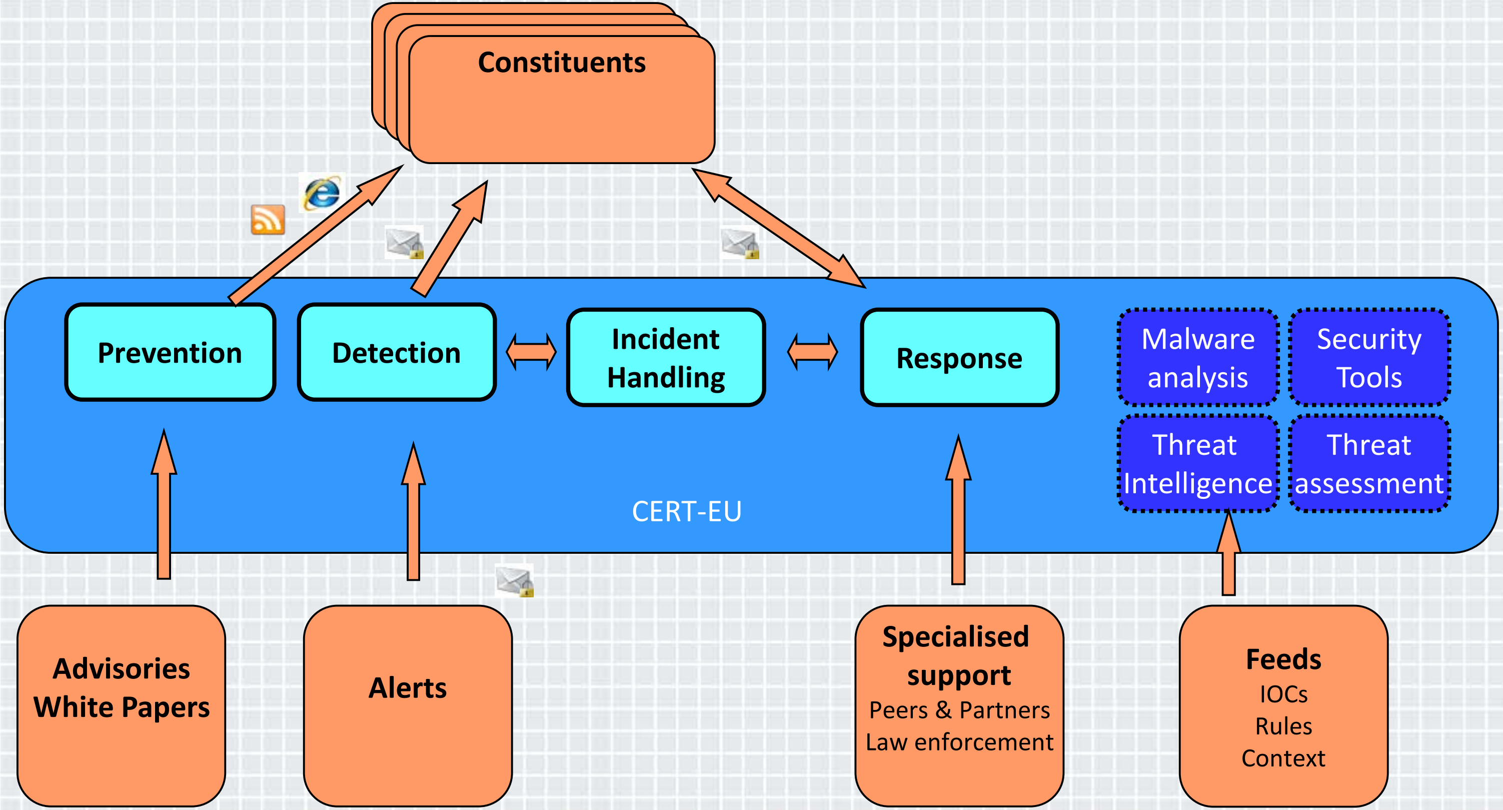
ENISA

- Europe-wide mandate in cyber security
- Supporting best practices, capacity building and awareness raising

EUROPOL EC3

- Europe-wide mandate in fight against cyber-crime
- Operational cooperation between police computer crime units

Services



Constituents

Prevention

Detection

Incident Handling

Response

Malware analysis

Security Tools

Threat Intelligence

Threat assessment

CERT-EU

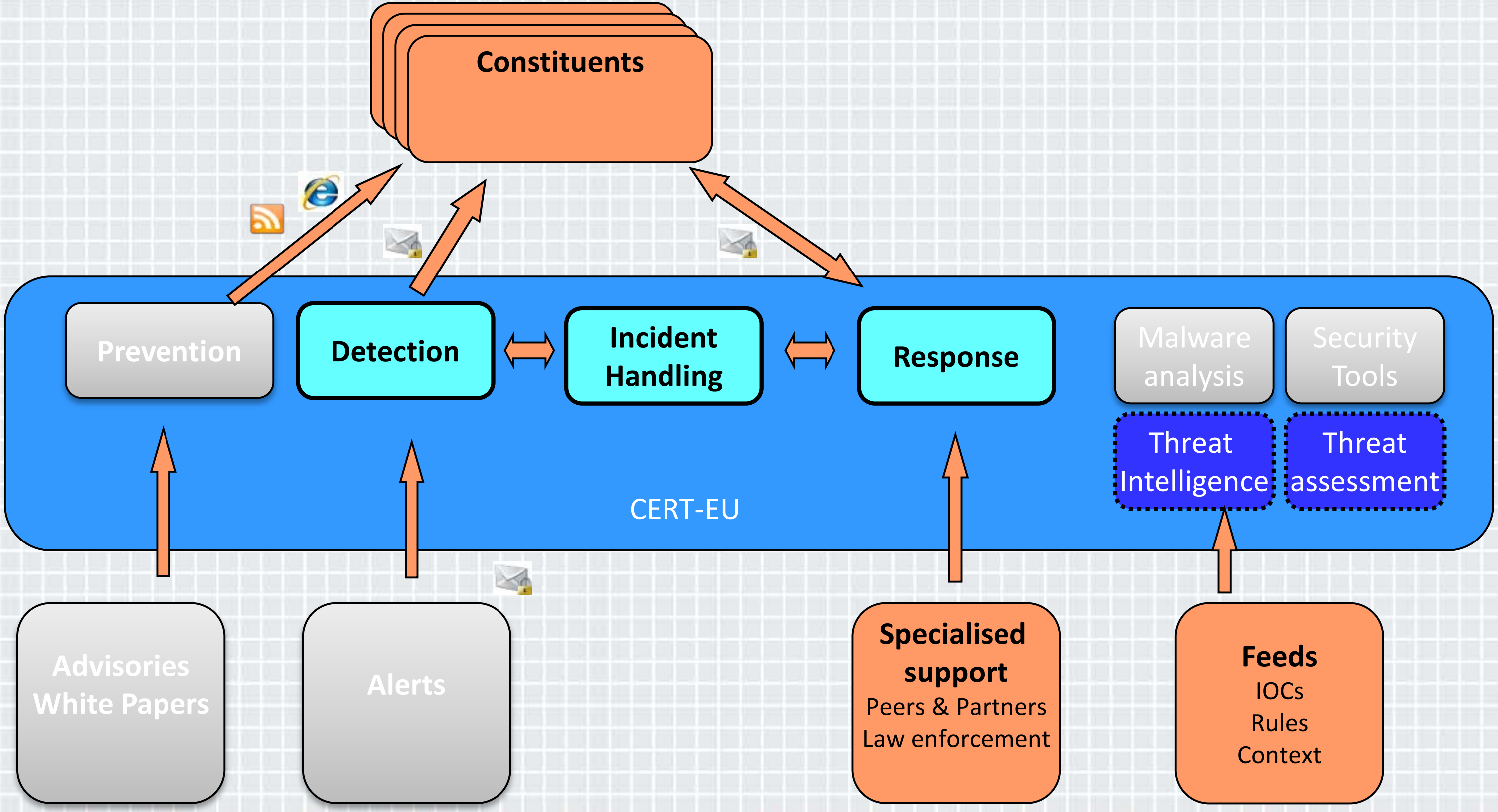
Advisories White Papers

Alerts

Specialised support
Peers & Partners
Law enforcement

Feeds
IOCs
Rules
Context

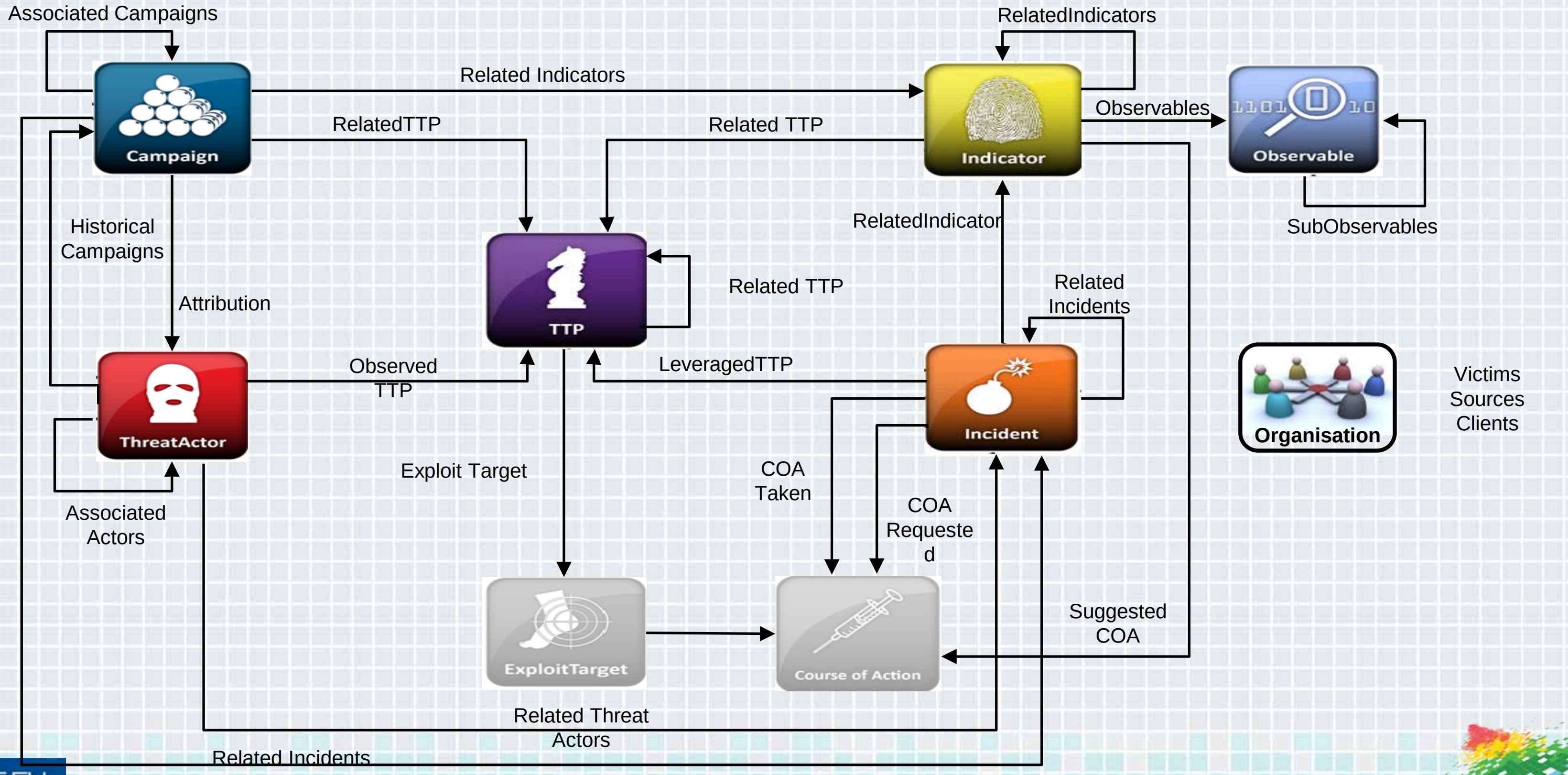
Services


Constituents
Prevention
Detection
Incident Handling
Response
Malware analysis
Security Tools
Threat Intelligence
Threat assessment
CERT-EU
Advisories White Papers
Alerts
Specialised support
Peers & Partners
Law enforcement
Feeds
IOCs
Rules
Context

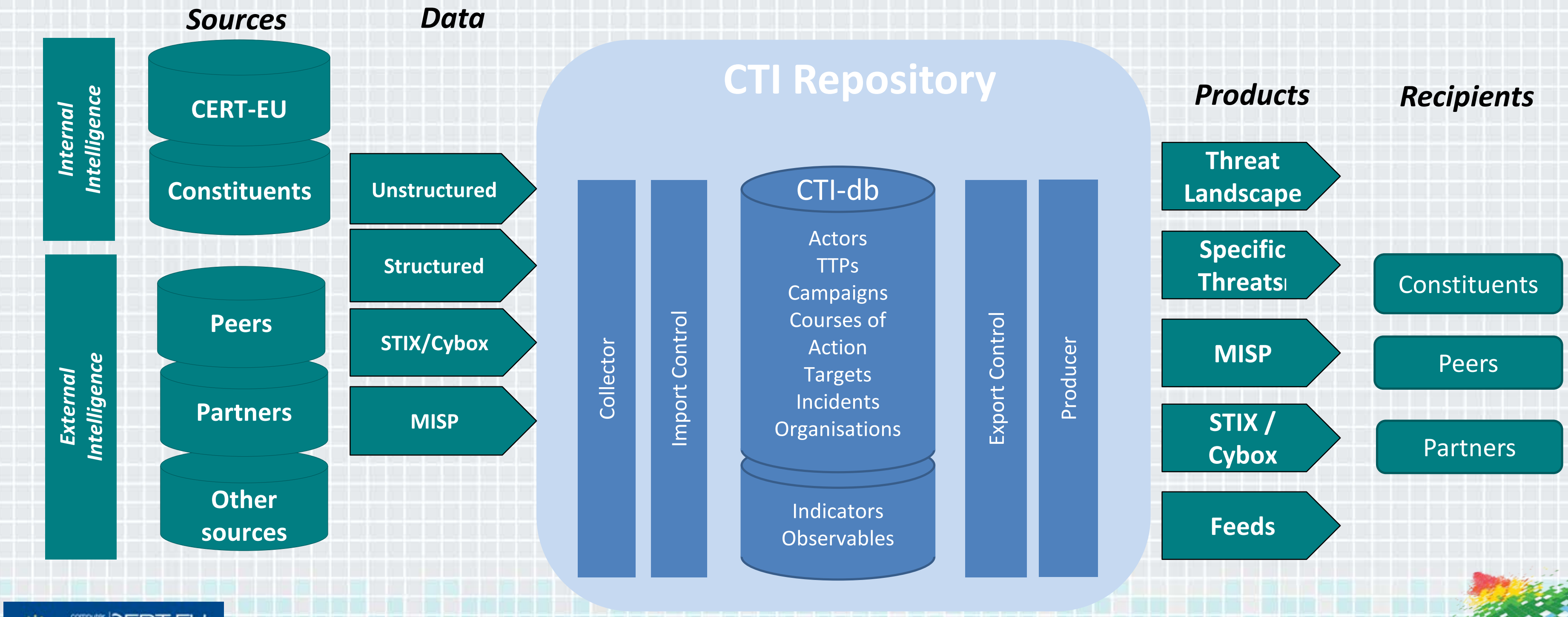
Agenda

- Introduction
- Architecture
- Use case 1: Detection
- Use case 2: Scoping
- Use case 3: Strategic insight
- Apply

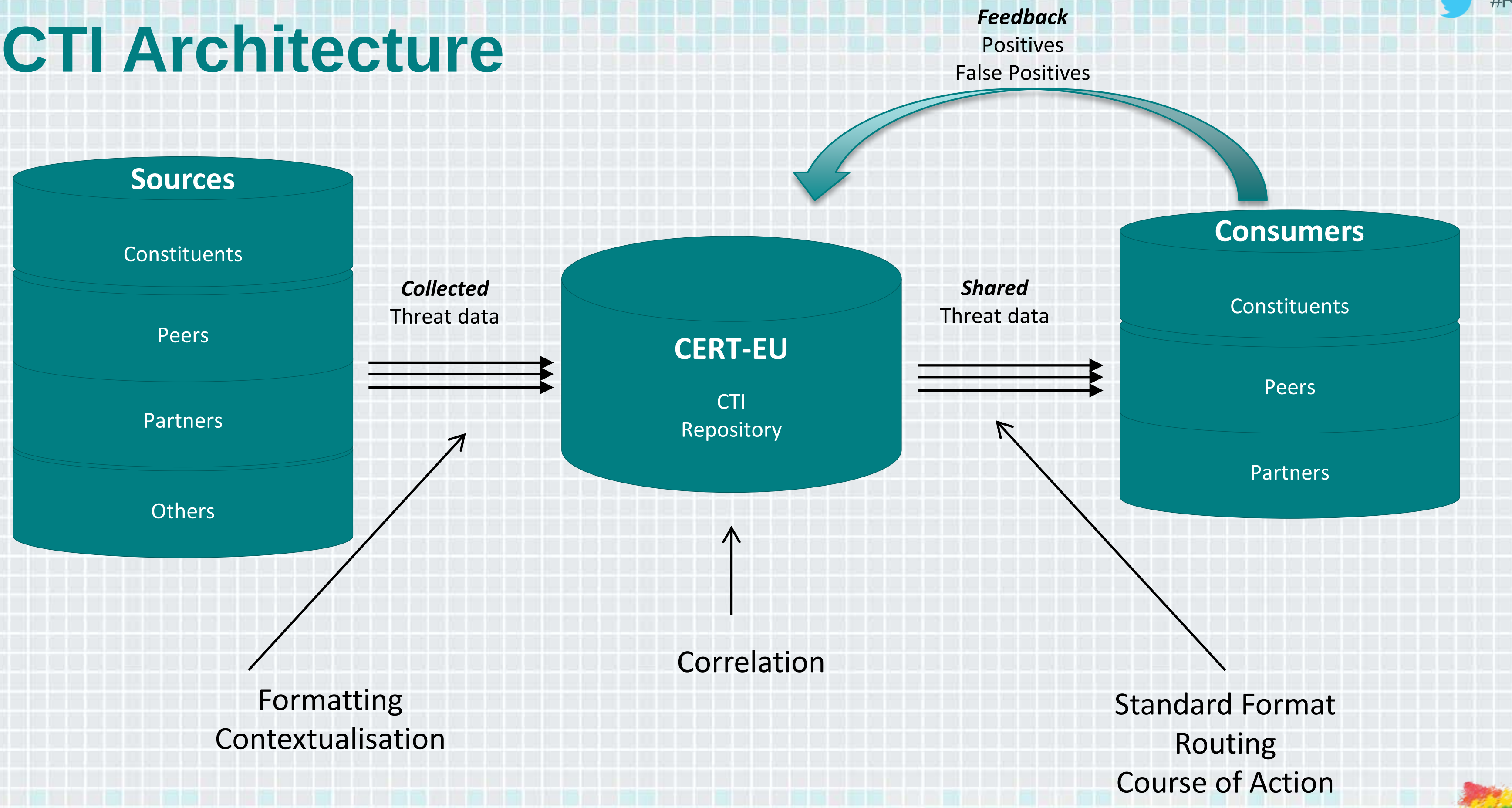
STIX Model$^+$


Associated Campaigns
RelatedIndicators
Related Indicators
Campaign
RelatedTTP
Related TTP
Indicator
Observables
Observable
1101
10
SubObservables
Historical
Campaigns
RelatedIndicator
TTP
Related TTP
Related
Incidents
Attribution
Observed
TTP
LeveragedTTP
ThreatActor
Incident
Organisation
Victims
Sources
Clients
Exploit Target
COA
Taken
COA
Requeste
d
Associated
Actors
Suggested
COA
ExploitTarget
Course of Action
Related Threat
Actors
Related Incidents

CTI Architecture



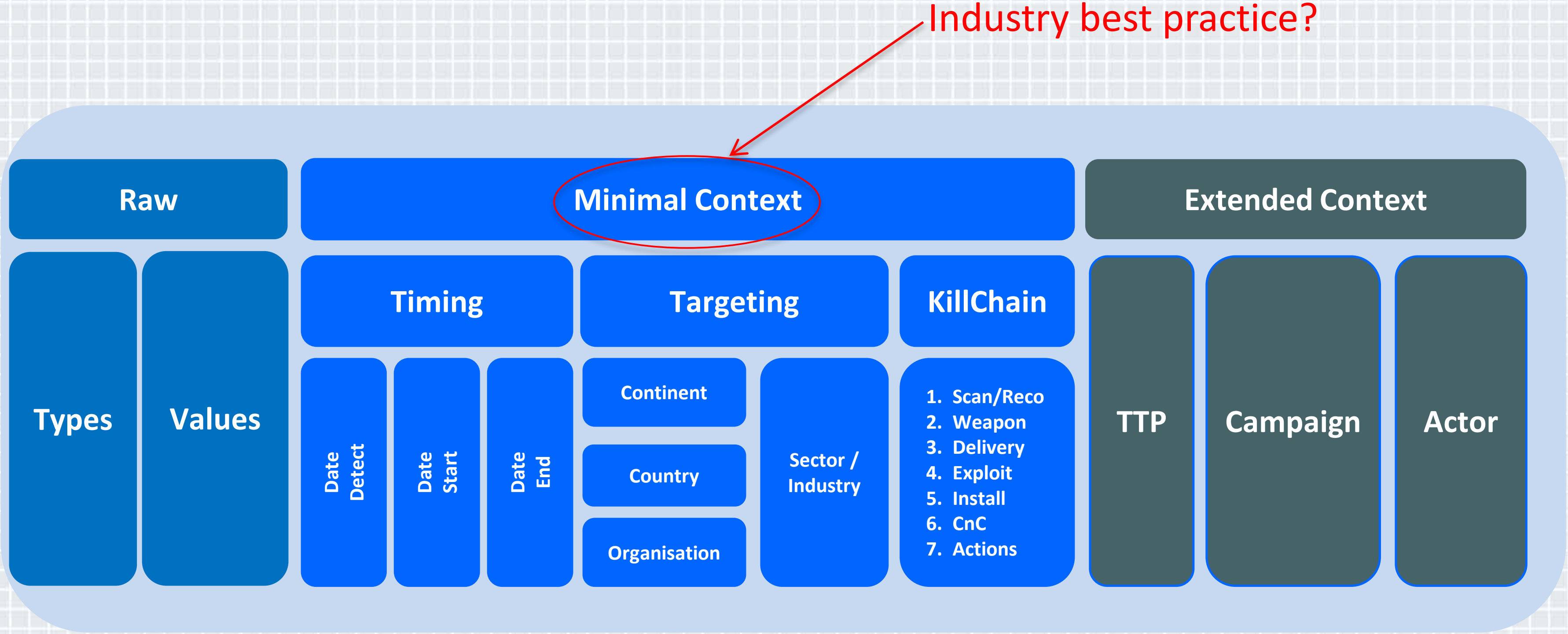
CTI Architecture



Threat Data Collection

- Large diversity of information sources
- Too much irrelevant information
- Accuracy not guaranteed
- Unclear timing
- Unclear sighting or targeting
- Difficult prioritisation

Contextualisation



Industry best practice?

Raw

Types

Values

Minimal Context

Timing

Date Detect

Date Start

Date End

Targeting

Continent

Country

Organisation

Sector / Industry

KillChain

1. Scan/Reco
2. Weapon
3. Delivery
4. Exploit
5. Install
6. CnC
7. Actions

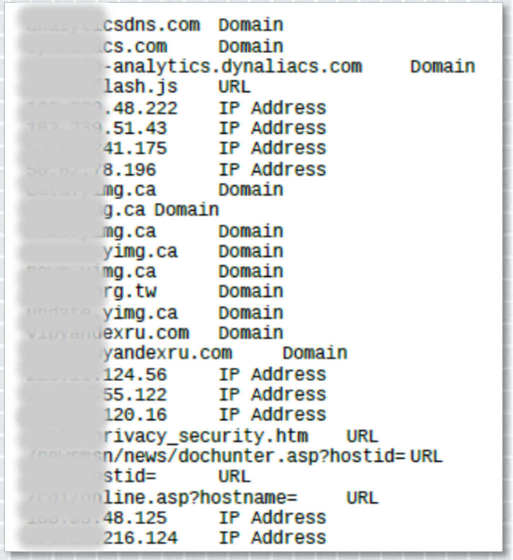
Extended Context

TTP

Campaign

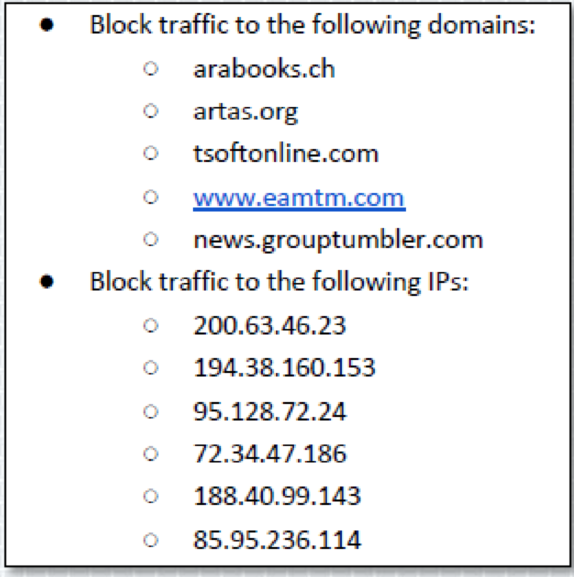
Actor

Poor Context



```
[redacted]csdns.com  Domain
[redacted]cs.com     Domain
[redacted]-analytics.dynaliacs.com     Domain
[redacted]lash.js    URL
[redacted].48.222    IP Address
[redacted].51.43     IP Address
[redacted]41.175     IP Address
[redacted]8.196      IP Address
[redacted]mg.ca      Domain
[redacted]g.ca Domain
[redacted]mg.ca      Domain
[redacted]yimg.ca    Domain
[redacted]mg.ca      Domain
[redacted]rg.tw      Domain
[redacted]yimg.ca    Domain
[redacted]exru.com   Domain
[redacted]yandexru.com     Domain
[redacted]124.56     IP Address
[redacted]55.122     IP Address
[redacted]120.16     IP Address
[redacted]rivacy_security.htm    URL
[redacted]n/news/dochunter.asp?hostid= URL
[redacted]stid=      URL
[redacted]line.asp?hostname=     URL
[redacted]48.125     IP Address
[redacted]216.124    IP Address
```

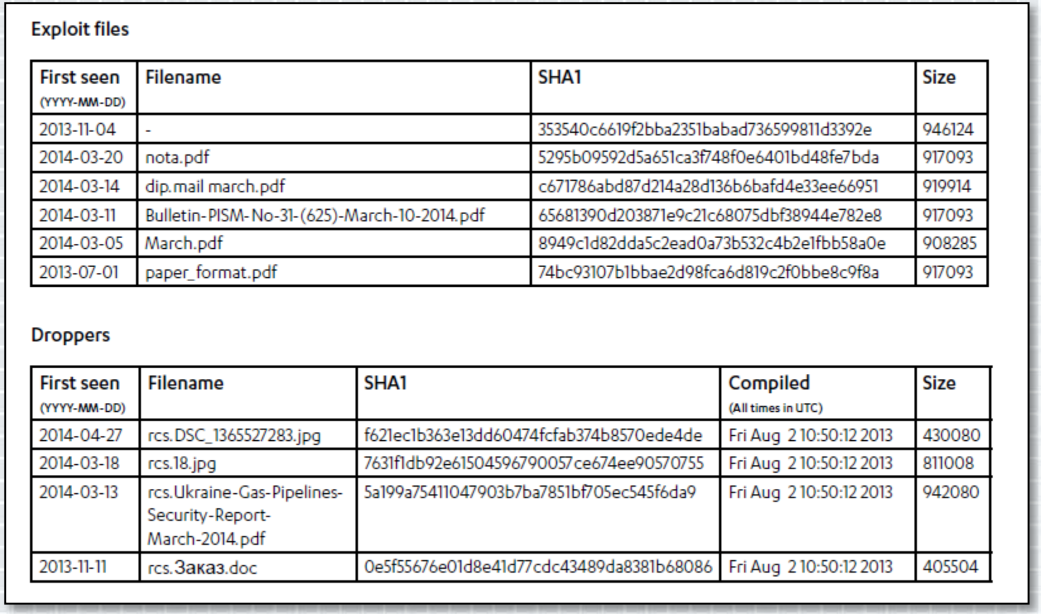
Timing	✗
Detect_date	
Start_date	
End_date	
KillChain	✗
Targeting	✗
Geoloc	
Sector	



- 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

Timing	✗
Detect_date	
Start_date	
End_date	
KillChain	✗
Targeting	✗
Geoloc	
Sector	

Better Context



Exploit files

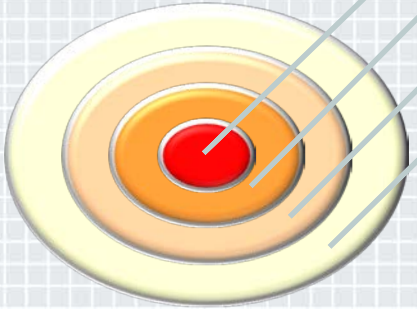
First seen (YYYY-MM-DD)	Filename	SHA1	Size
2013-11-04	-	353540c6619f2bba2351babad736599811d3392e	946124
2014-03-20	nota.pdf	5295b09592d5a651ca3f748f0e6401bd48fe7bda	917093
2014-03-14	dip.mail march.pdf	c671786abd87d214a28d136b6bafd4e33ee66951	919914
2014-03-11	Bulletin-PISM-No-31-(625)-March-10-2014.pdf	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	7631f1db92e6150459679005 7ce674ee90570755	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.Заказ.doc	0e5f55676e01d8e41d77cdc43489da8381b68086	Fri Aug 2 10:50:12 2013	405504

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

Threat Scope



EU-I - Targeting one or more constituents

EU-Centric – Targeting EU Member States

EU Nearby - Targeting close partners (e.g. NATO, USA)

World-Class - EU-I might be 'opportunity' or 'collateral' victims of major world-wide threats

Threat Level

High
Very sophisticated APT

Medium
APT

Low
Non-targeted mass attacks / malware

Threat level	World-Wide	EU-nearby	EU-centric	EU-I
HIGH	Medium priority	Medium priority	High priority	High priority
MEDIUM		Low priority	Medium priority	High priority
LOW			Low priority	Low priority

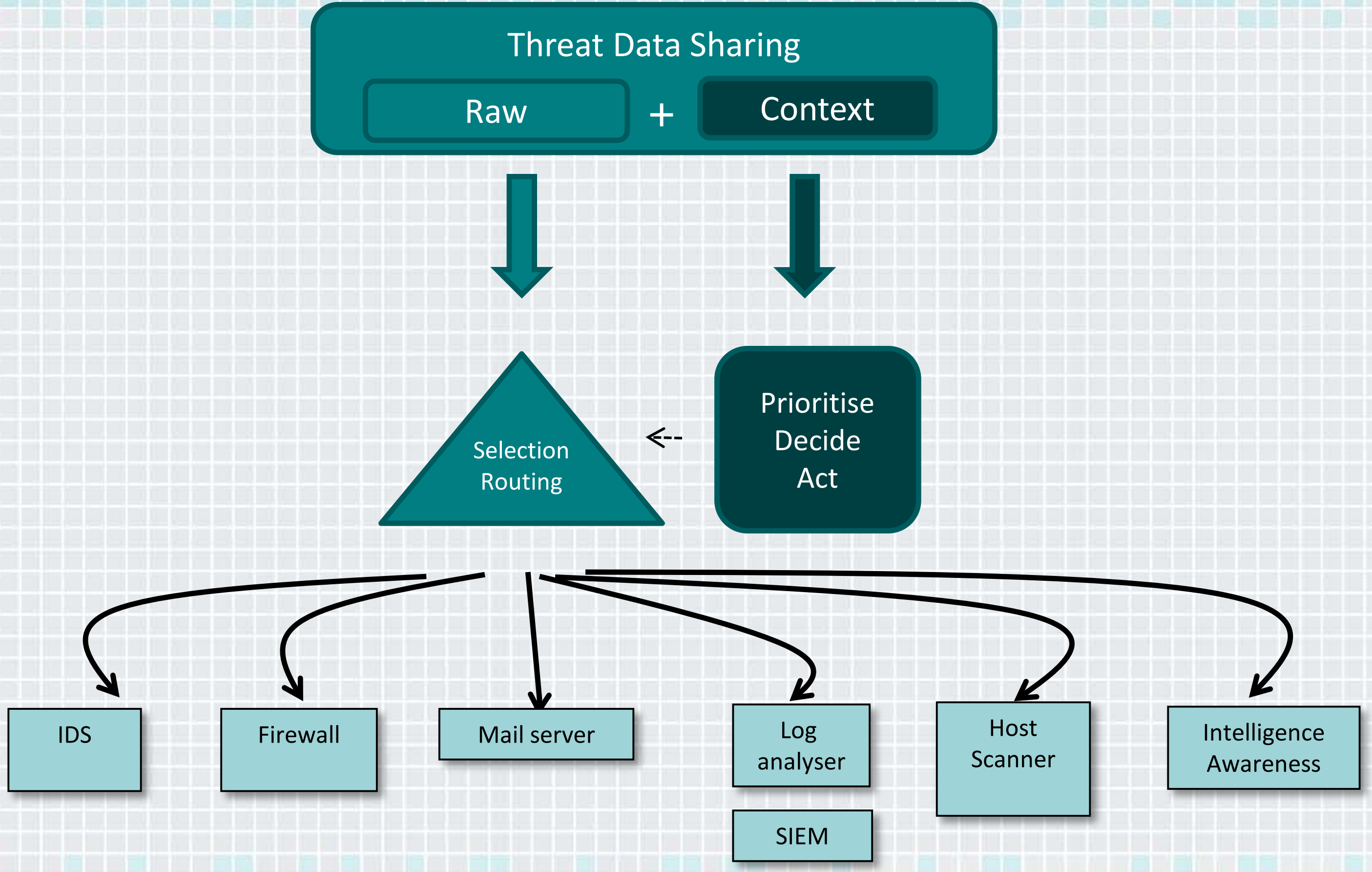
Threat Scope

■	High priority threat
▨	Medium priority threat
▤	Low priority threat
□	Out of scope = 'noise'

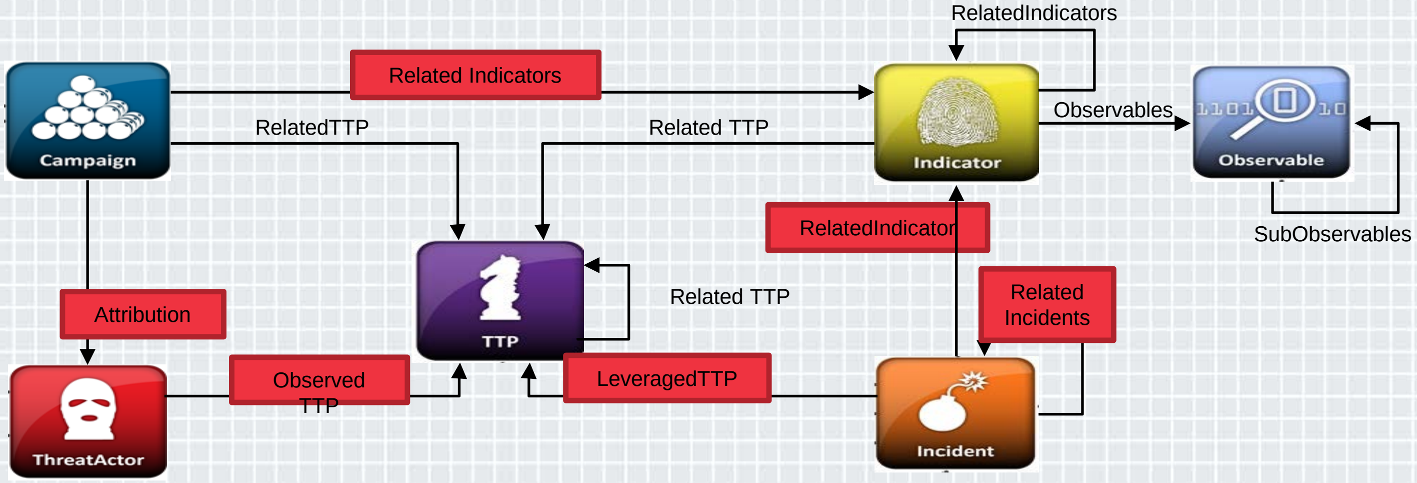
Constituent Perspective

- Limited resources
- Specific IT security tools
- Specific policies

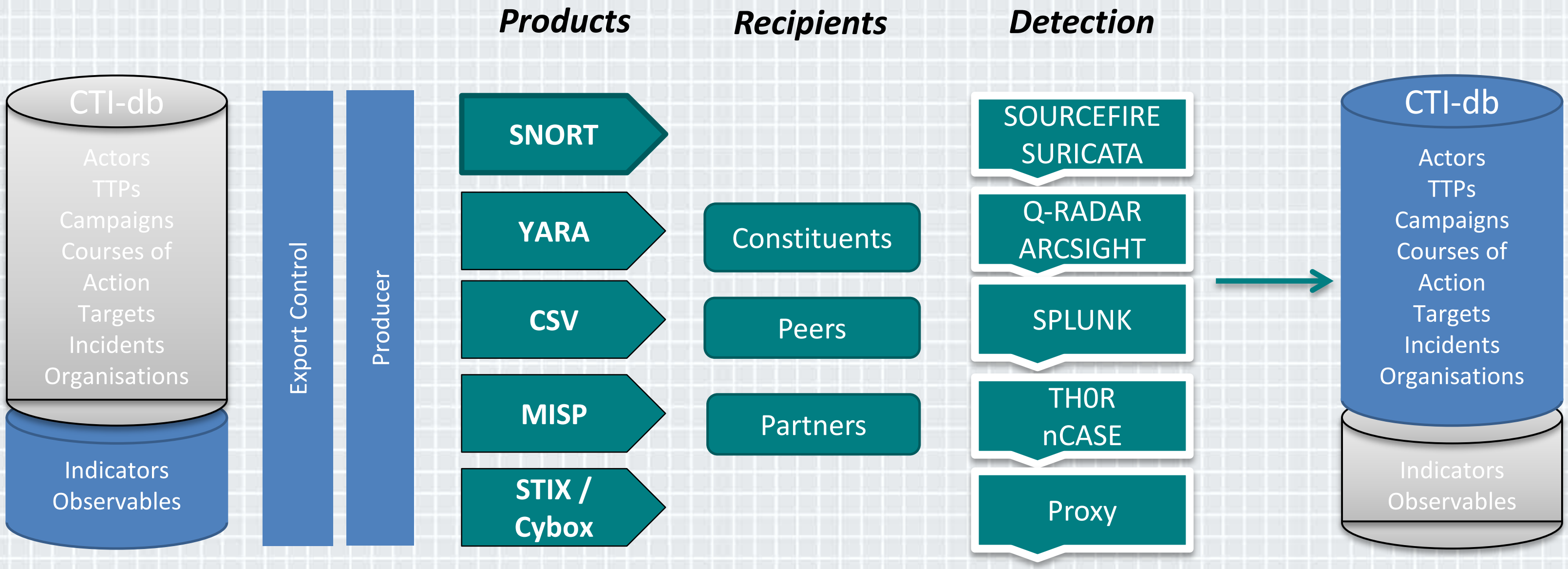
- Prioritisation
- Automation / Routing
- Minimise false-positives
- Actionable context when needed


Threat Data Sharing
Raw
+
Context
Selection
Routing
Prioritise
Decide
Act
IDS
Firewall
Mail server
Log analyser
SIEM
Host Scanner
Intelligence Awareness

STIX Model


RelatedIndicators
Related Indicators
Campaign
RelatedTTP
Related TTP
Indicator
Observables
Observable
SubObservables
RelatedIndicator
TTP
Related TTP
Related Incidents
Attribution
ThreatActor
Observed TTP
LeveragedTTP
Incident

Use Case 1: Detection



Products *Recipients* *Detection*

CTI-db
Actors
TTPs
Campaigns
Courses of Action
Targets
Incidents
Organisations

Indicators
Observables

Export Control

Producer

SNORT

YARA

CSV

MISP

STIX / Cybox

Constituents

Peers

Partners

SOURCEFIRE
SURICATA

Q-RADAR
ARCSIGHT

SPLUNK

THOR
nCASE

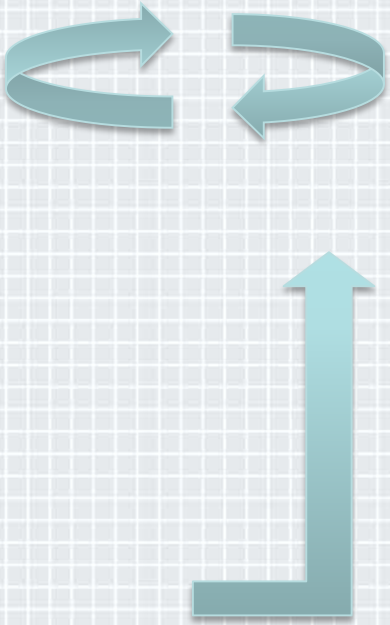
Proxy

CTI-db
Actors
TTPs
Campaigns
Courses of Action
Targets
Incidents
Organisations

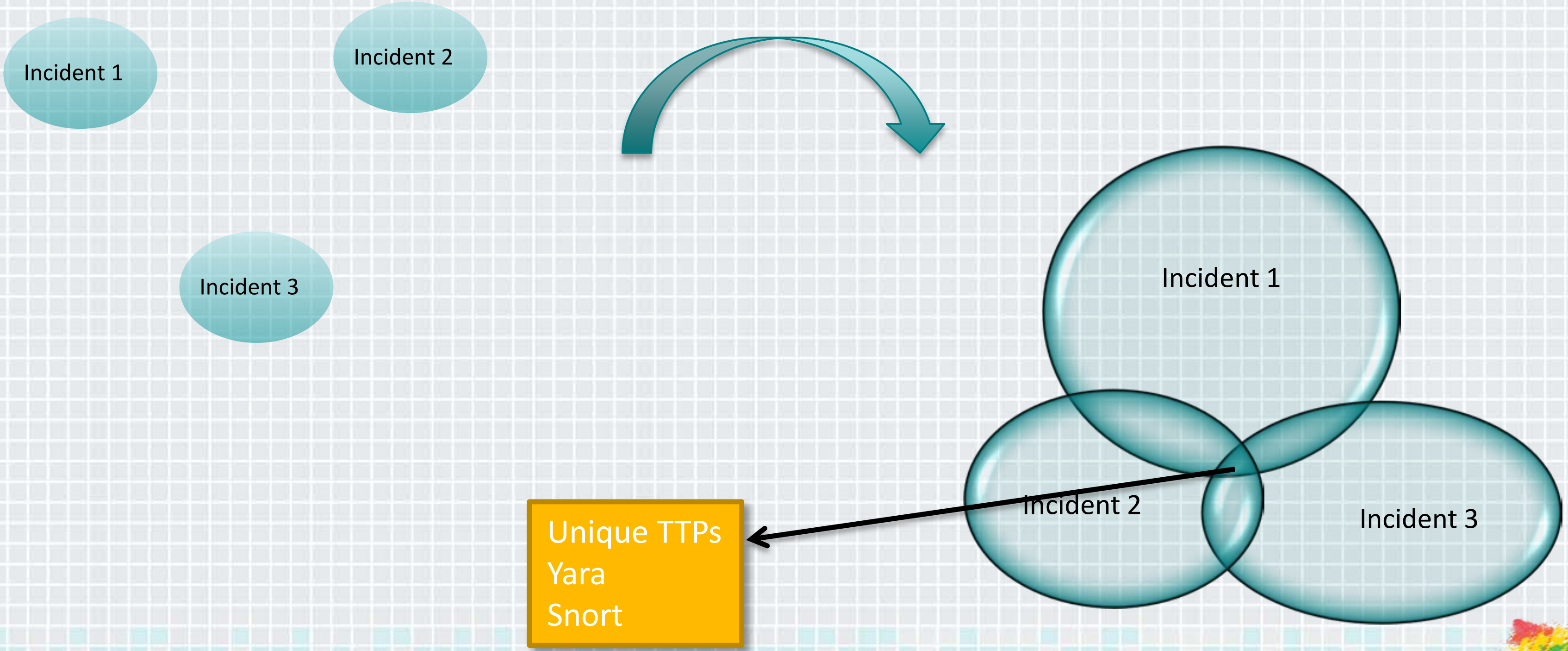
Indicators
Observables

Use Case 2: Scoping

- Malware reversing
- Internal process
    - Scanning for IOCs in logs and hosts
    - Scanning for anomalous traffic
    - Hits on the proxy/IDS
- External process
    - Has anybody else seen this?
        - No? -> You're on your own
        - Yes? -> Multiply knowledge on IOCs
        - What's the timeline
    - *Sinkholing*



Pivoting via Actor / Campaign



Unique TTPs
Yara
Snort

Use Case 3: Strategic Insight

Strategic	• 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.	• CEO • Business VP • CIO	Periodic Bulletin	Threat Landscape Security Brief
Tactical	• Understanding cyber-attacks tactical context: threat type and level, timing of events, techniques/malware used. • Planning structured course of actions for permanent protection	• CIO • Cyber-defense teams	For every new significant campaign	CITAR
Technical	• Immediate reaction to threats: Detection, Prevention, Reaction (eradication, recovery), Report • Dynamic feeding cyber-defense tools: IDS, IPS, SIEM, Security Scanners, Mailguard, Firewalls, etc	• Cyber-defense teams • IT administrators (or direct tool feeding)	IOCs Rules (Near real-time -> Towards full automation)	CIMBL Feeds

Current Content

Threat Actors

ThreatActor

- 200+
- Espionage/Strategic
- Hacktivists
- Cyber-criminals

Campaigns

Campaign

- 300+
- Espionage (political, industrial, etc)
- Hacktivism
- CyberCrime

Incidents & Indicators

Incident

Indicator

- 3000+ per year
- Scope: Constituency / EU-centric / EU-nearby/ World-class

Victims

Victims

- 500+
- Continet/country
- Sector (Diplomacy, Defense, Energy, Transport, etc)
- Type (Private, Public)

Observables

Observable

- 800.000 targeted IOCs
- Malicious Domains = 65 %
- Malicious Files = 10%
- Malicious email addresses = 8%
- Malicious IP = 5 %
- Malicious URL = 4 %
- Other (Regkey, snort, etc) = 8%

Techniques, Tactics, Procedures

TTP

- 500+
- "Idendity card" of malware, botnets, C&C infrastructures, tools, exploit-kits
- Killchain analysis
- Focus on sophisticated & targeted TTP

Some Open Issues

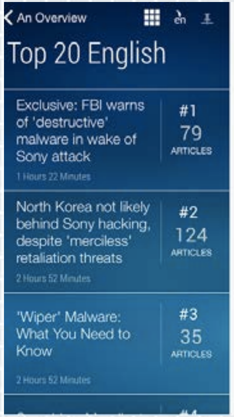
- How to manage lifetime of the data
- How to remove data downstream
- How to control sharing groups downstream
- Implement Course of Action
- How to maintain the treasure trove of TTPs

Apply Slide

- Insist with your suppliers to deliver context with their feeds
- Identify “your” definitions to filter inputs/outputs
  - Threat scope and level
  - Sharing groups
  - Course of Action
  - …
- Start implementing your own internal STIX repository
- Embed it in your processes

RSAConference2015

San Francisco | April 20-24 | Moscone Center



An Overview

Top 20 English

Exclusive: FBI warns of 'destructive' malware in wake of Sony attack — #1 79 ARTICLES

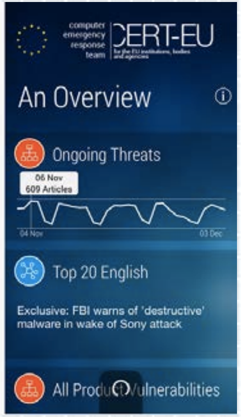
1 Hours 22 Minutes

North Korea not likely behind Sony hacking, despite 'merciless' retaliation threats — #2 124 ARTICLES

2 Hours 52 Minutes

'Wiper' Malware: What You Need to Know — #3 35 ARTICLES

2 Hours 52 Minutes



computer emergency response team CERT-EU for the EU institutions, bodies and agencies

An Overview

Ongoing Threats

06 Nov 609 Articles

Top 20 English

Exclusive: FBI warns of 'destructive' malware in wake of Sony attack

All Product Vulnerabilities

Thank You!

http://cert.europa.eu/

#RSAC