CAMPUS
CYBER

A CTI doctrine for CTI production

00. ABOUT US.

CAMPUS CYBER

sekoia

Fabien Gainier
Head of Commons studio

David Bizeul
Chief Scientific Officer,

CAMPUS CYBER PROJECT

GOALS

DEVELOPPEMENT OF SOVEREIGN CYBER SOLUTIONS

REINFORCE THE SYNERGIES BETWEEN THE CYBER ACTORS

INCREASE ATTRACTIVITY

IN FEW WORDS

39% public / 61% private

A 26 000m² facility

187 Members - 46 Partners - 134 Residents

CAMPUS CYBER

COMMONS STUDIO

COMMONS STUDIO.

+ EXPLORE

+ PRODUCE

+ SHARE

Explore complex issues[1]

Identify and anticipate future developments in the cyber market.

Explore by reducing investment risks through pooling.

Raise innovation by pooled assets[2]

Deliver proof of concept, prototype, guideline, doctrine.

Lever ecosystem impact with common spread[3]

Spread European ecosystem points of view.

Foster development of European standard.

Increase the interoperability of European solutions.

COMMONS STUDIO IN FIGURES.

+ 24 Commons

Produce or in production

+ 14 Workgroups

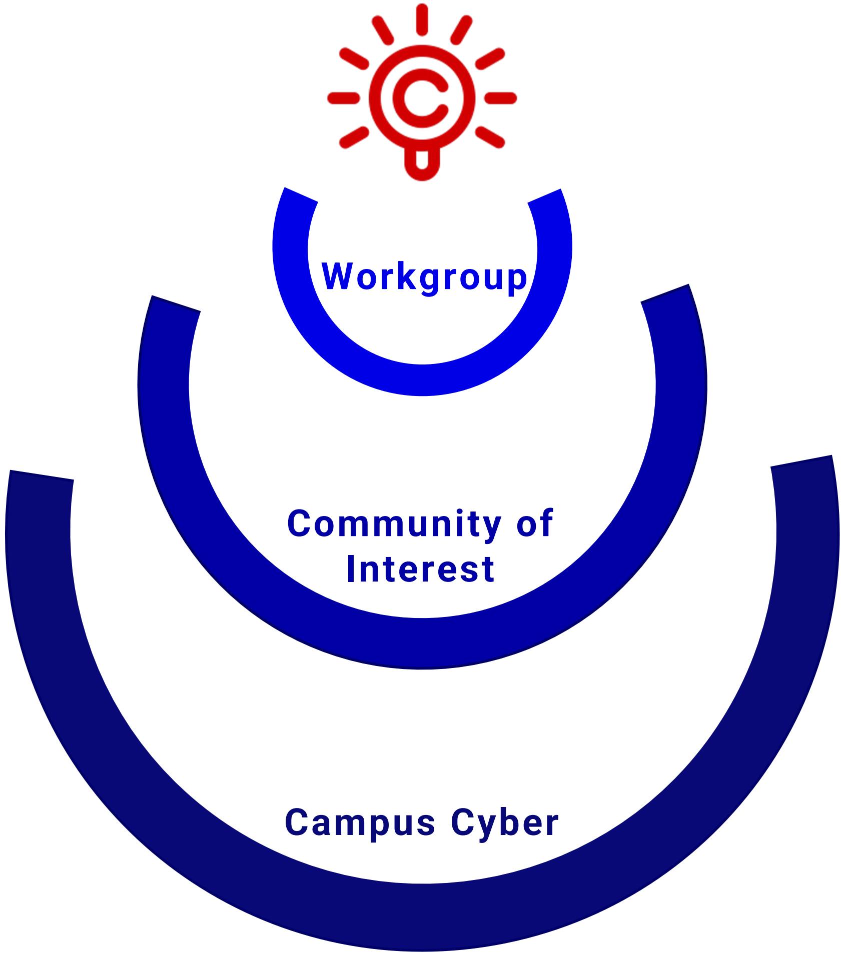
12 still on going from 10 to 20 members

+ 650 People involved

From 20 to 80 specialists by community

+ 200 Organisations

Involved in the studio

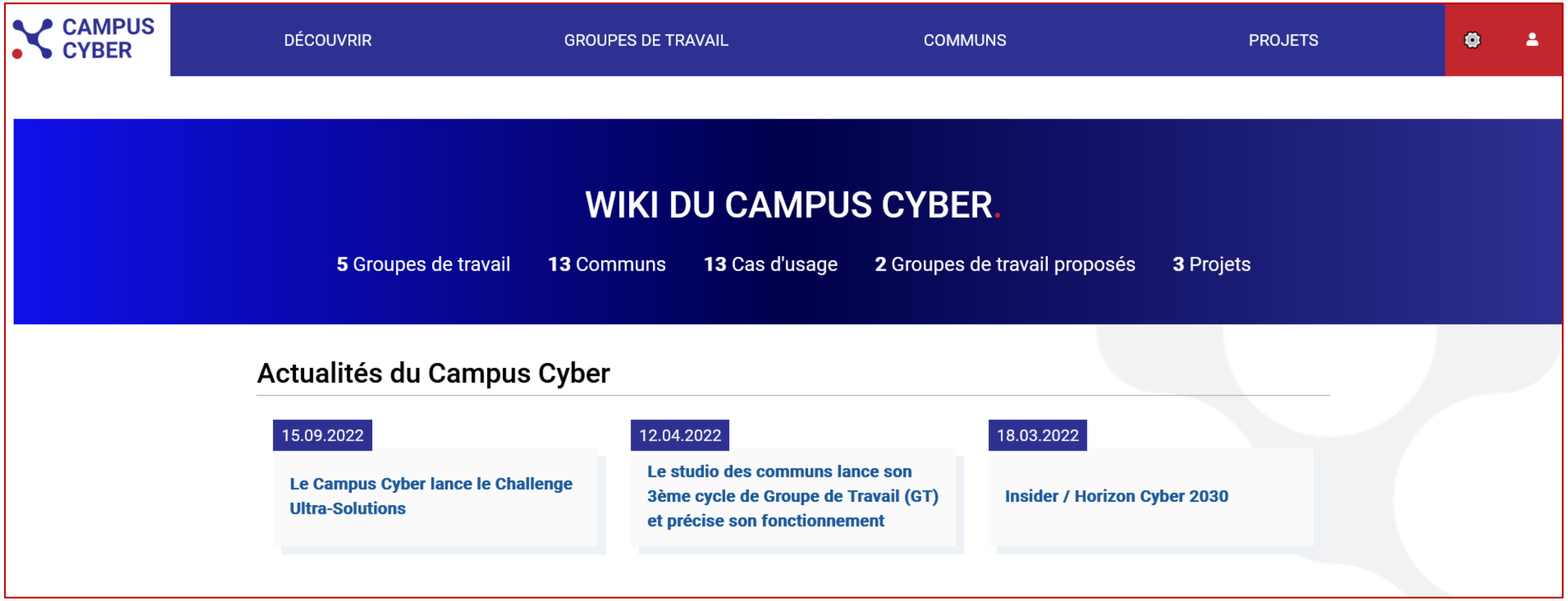


COMMUNITY OF INTEREST.

- + IA AND CYBERSECURITY
- + CRYPTO-ASSETS SECURITY
- + CYBER4TOMORROW
- + TRAINING AND CRISIS CYBER
- + CTI
- + POST QUANTUM CRYPTOGRAPHY
- + SECURITY AND DETECTION IN CLOUD
- + FINANCIAL AND INSURANCE
- + MONITORING AND DETECTION IN MOBILITY
- + DRONES ET ROBOTS SECURITY
- + AGILE SECURITY
- + VULNERABILITY MANAGEMENT
- + TRAINING

09. COMMONS STUDIO WIKI.

Wiki of the cyber commons studio for the dissemination of knowledge (wiki.campuscyber.fr)



WIKI DU CAMPUS CYBER.

5 Groupes de travail **13** Communs **13** Cas d'usage **2** Groupes de travail proposés **3** Projets

Actualités du Campus Cyber

15.09.2022 — Le Campus Cyber lance le Challenge Ultra-Solutions

12.04.2022 — Le studio des communs lance son 3ème cycle de Groupe de Travail (GT) et précise son fonctionnement

18.03.2022 — Insider / Horizon Cyber 2030

CAMPUS CYBER

CTI WG

AGENDA.

01. GOAL.

02. USE CASES.

03. DOCTRINE.

04. PLATFORM.

05. TAKE AWAYS.

OBSERVATIONS 101

- Information overload everywhere
  - Even in cybersecurity
  - Even on cyber threat intelligence
- But lack of structure
  - Source and context is a value driver
  - Plaintext files often come from somewhere else
  - No TTP, IOCs in JPG format….
- People who know do not share (so much…)
  - Intelligence as a weapon
  - Intelligence as a business mode
  - Intelligence as a key advantage

Volume Interest

⚖

Plain Text Structured Objects

⚖

Community Sensitivity

⚖

CTI AS A GROUP 101

- Federate people
  - Willing to share
  - Understanding the benefit of mutualization
- Agree on guidelines
  - Orientation (what to focus on)
  - Structure and format
  - Toolset that is relevant
- Run a proof of concept
  - Explain before starting
  - Provide attractive deliverables to start
  - Extend the network to maintain

Shared goals

Method alignment

Start when ready

01. GOALS (why?).

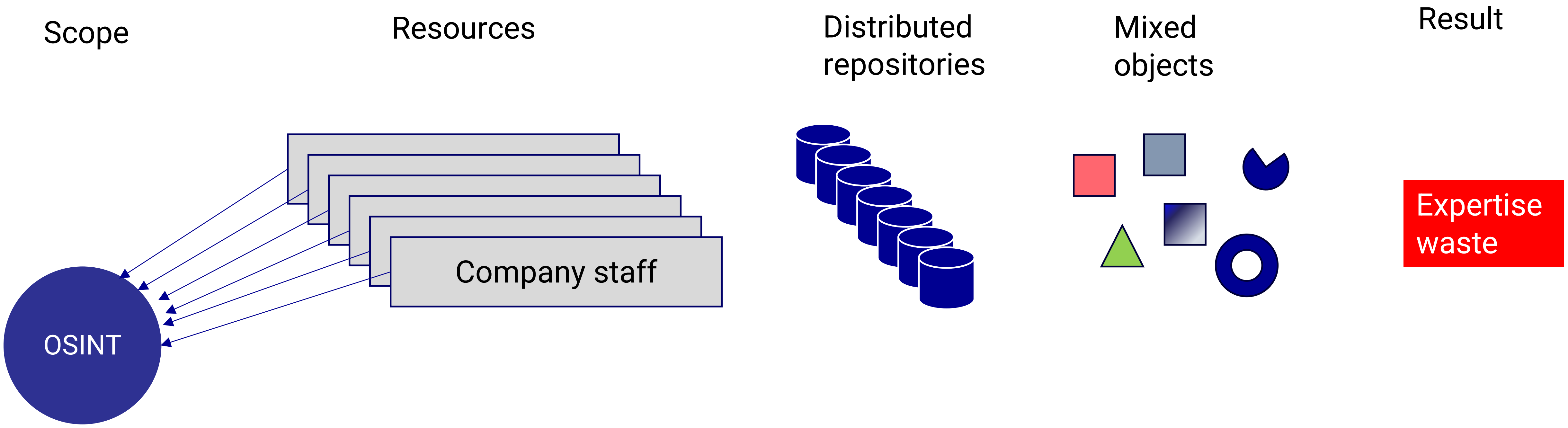
- OPTIMIZE analyst time
- STORE in a central repository
- ENHANCE sharing of expert best practices
- IMPROVE CTI quality for actionability

02. USE CASES (what?).

5 **ACHIEVABLE** use cases :

- Cyber Threat Intelligence in OSINT world 1
  - Blog posts consolidation as structured data
- Hot topics and CTI Focus 2
  - Exploited vulnerability
  - Geopolitical event and collateral damage
- Collaborative report 3
  - Shared analysis and write a joint paper as an industry position
- Incident sharing 3
  - Detailed information from a victim in order to protect its peers
- Sightings and measures 3
  - What is being observed, when and where

02. USE CASES (OSINT example).



Scope

Resources

Distributed repositories

Mixed objects

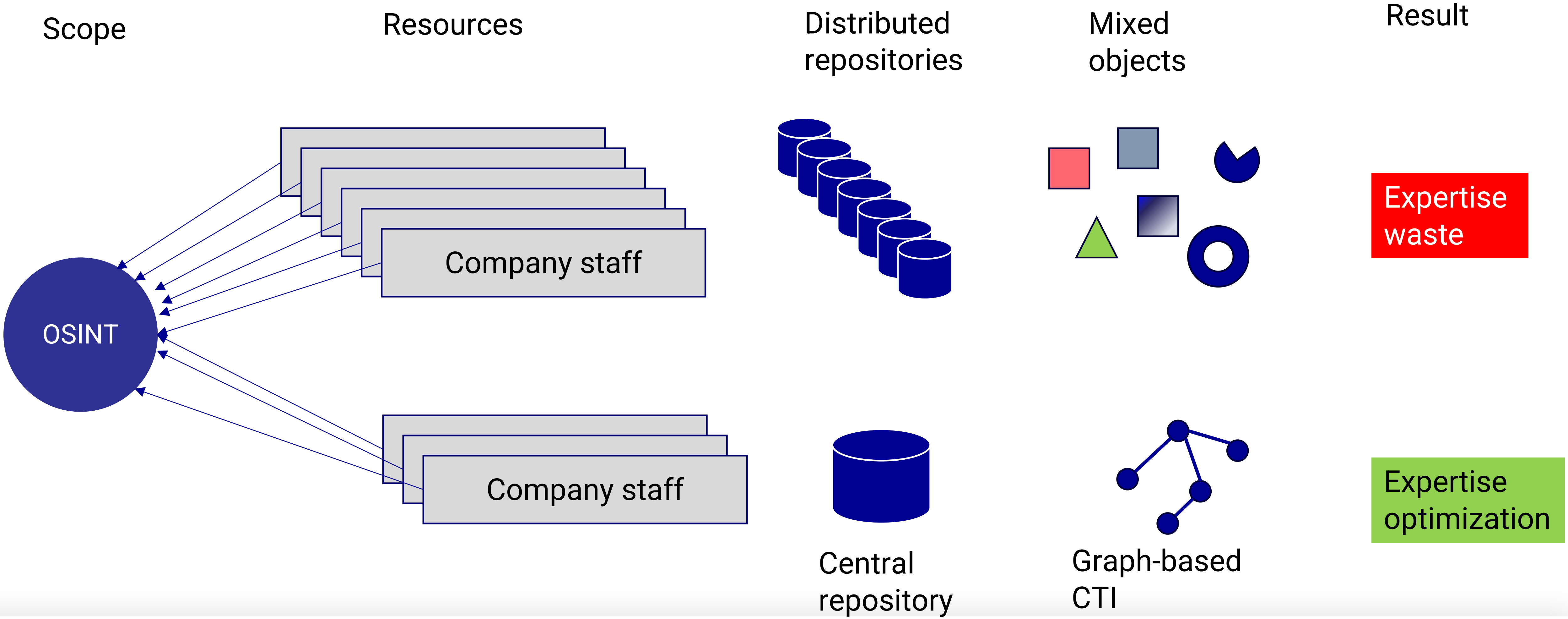
Result

OSINT

Company staff

Expertise waste

02. USE CASES (OSINT example).



Scope

Resources

Distributed repositories

Mixed objects

Result

OSINT

Company staff

Expertise waste

Company staff

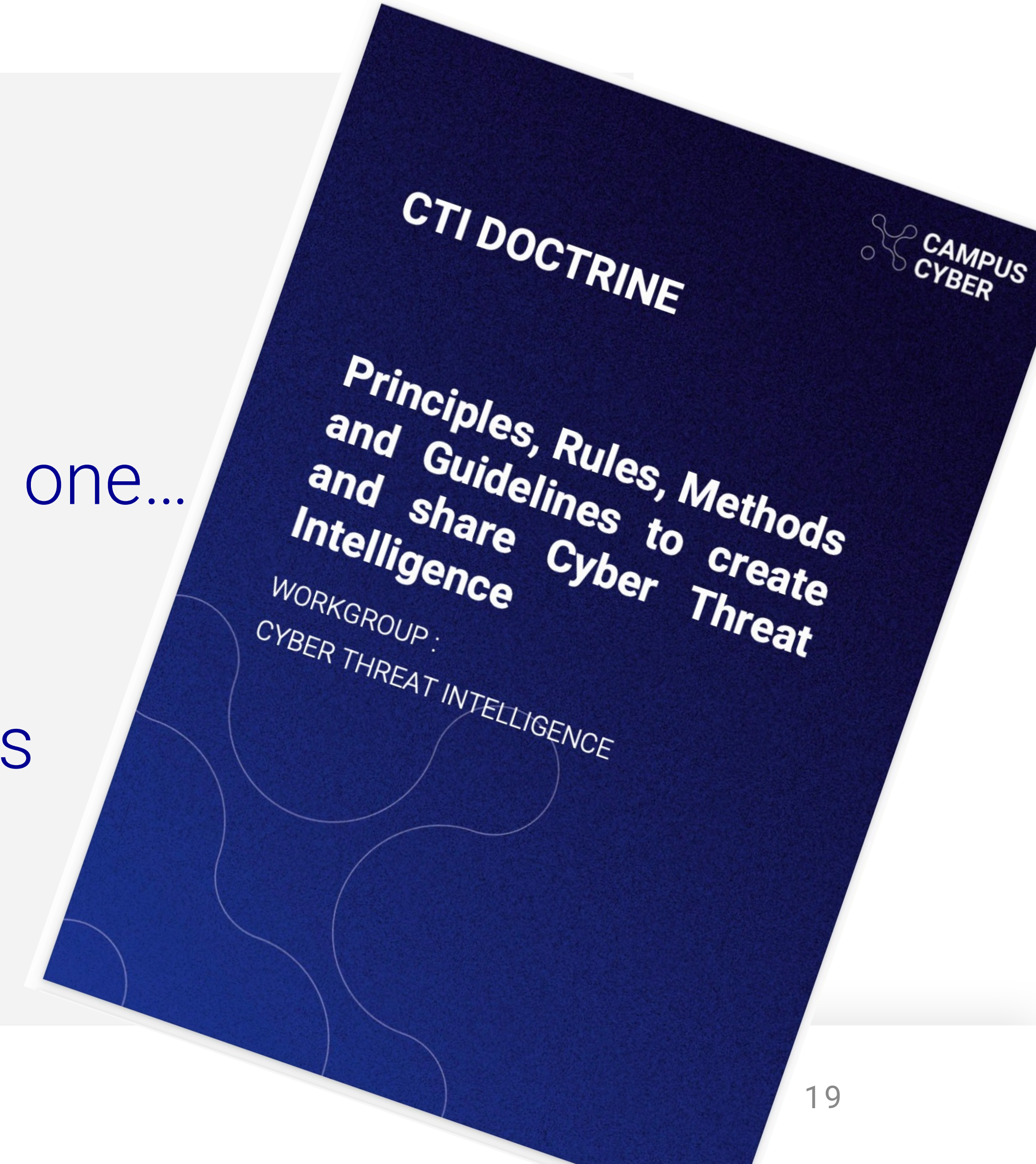
Central repository

Graph-based CTI

Expertise optimization

03. DOCTRINE (how?).

- Pack of 60 rules to do great things
- Available in PDF for everyone
- We did that because we did not find one…
- Organized in scoping rules
  - Global rules
  - Specific rules for use cases focus



CTI DOCTRINE

CAMPUS CYBER

Principles, Rules, Methods and Guidelines to create and share Cyber Threat Intelligence

WORKGROUP :
CYBER THREAT INTELLIGENCE

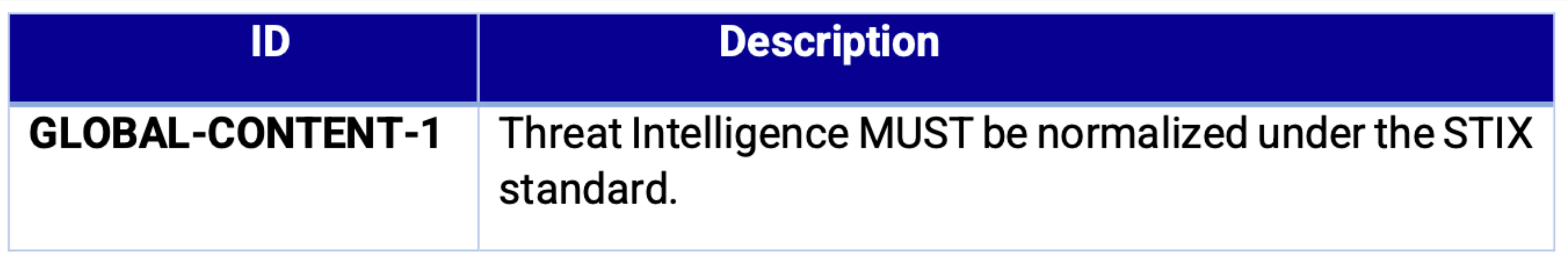
03. DOCTRINE.

- Example #0 – Naming convention

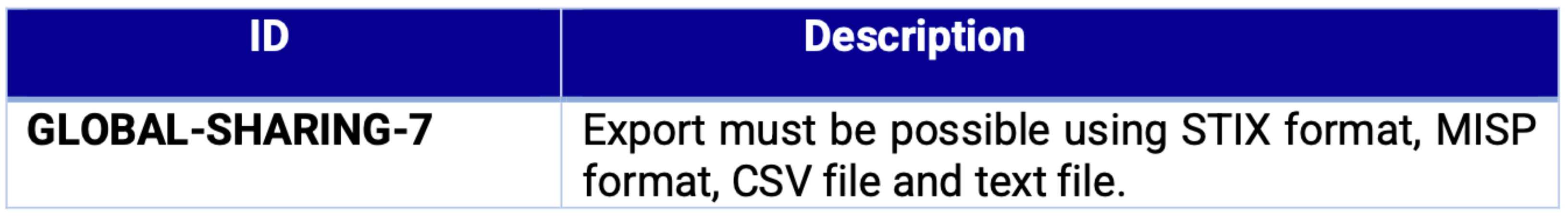
ID	Description
SCOPE – FIELD - ID	Summary of the rule with a MUST/SHOULD criteria

03. DOCTRINE.

- Example #1 – Creation and Sharing



ID	Description
GLOBAL-CONTENT-1	Threat Intelligence MUST be normalized under the STIX standard.

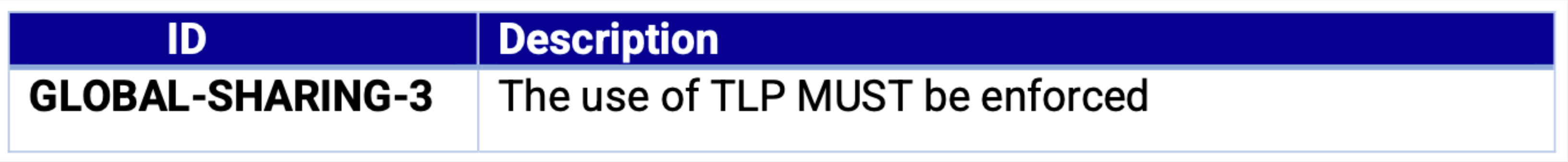


ID	Description
GLOBAL-SHARING-7	Export must be possible using STIX format, MISP format, CSV file and text file.

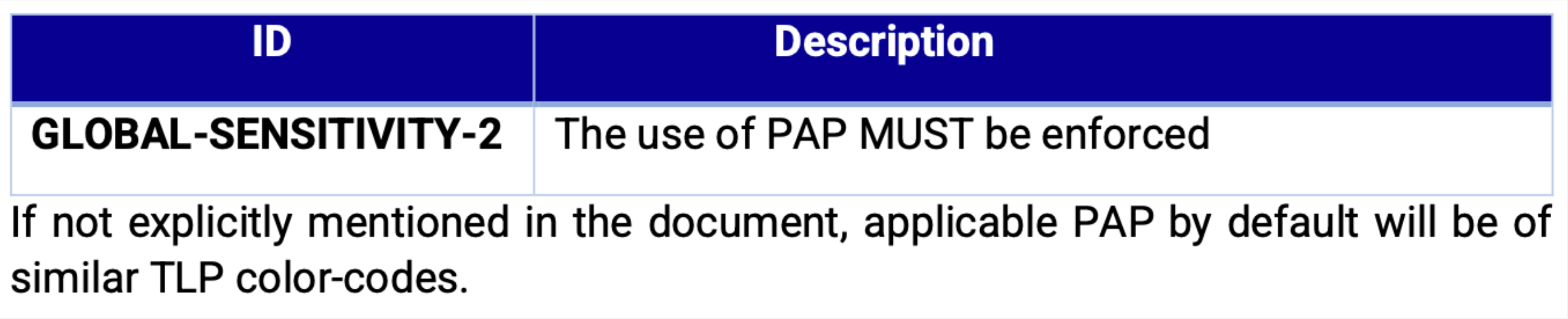
03.

DOCTRINE.

- Example #2 - Metadata



ID	Description
GLOBAL-SHARING-3	The use of TLP MUST be enforced

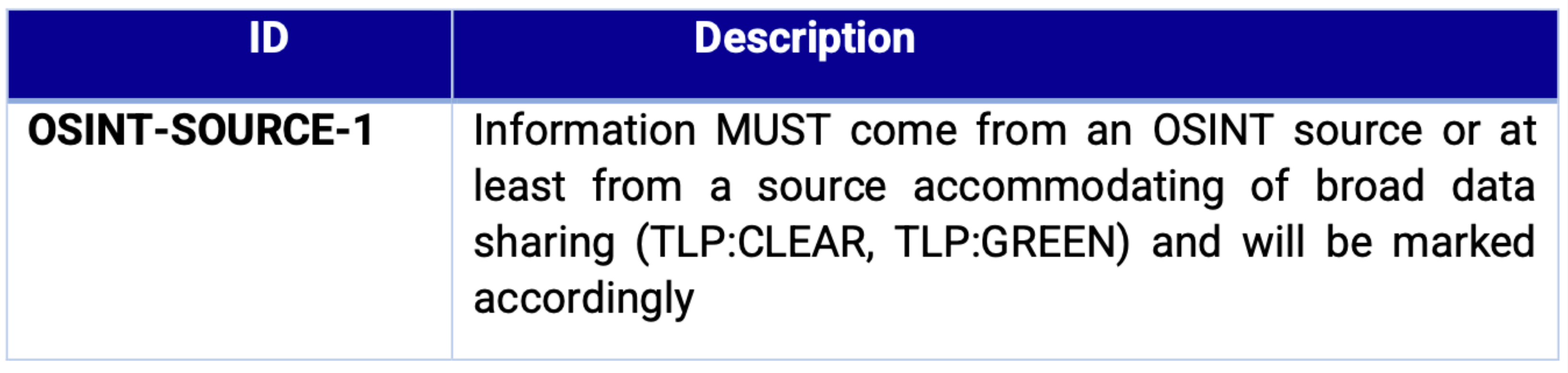


ID	Description
GLOBAL-SENSITIVITY-2	The use of PAP MUST be enforced

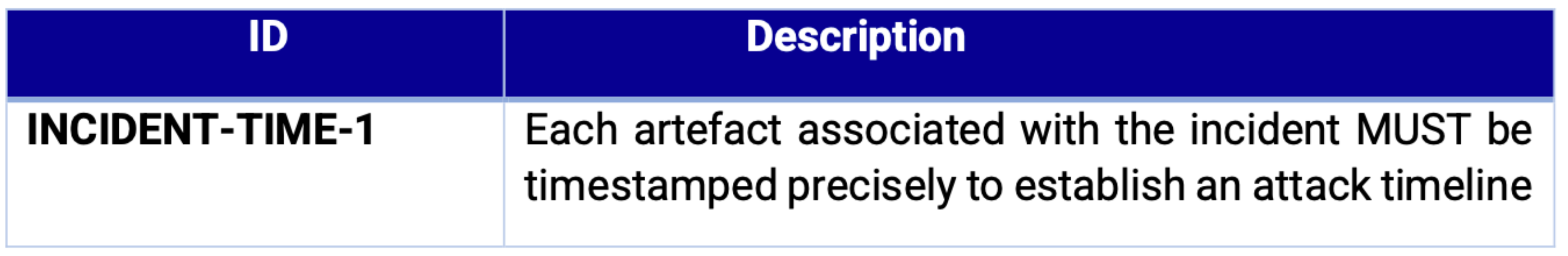
If not explicitly mentioned in the document, applicable PAP by default will be of similar TLP color-codes.

03. DOCTRINE.

- Example #3 – Use cases focused rules



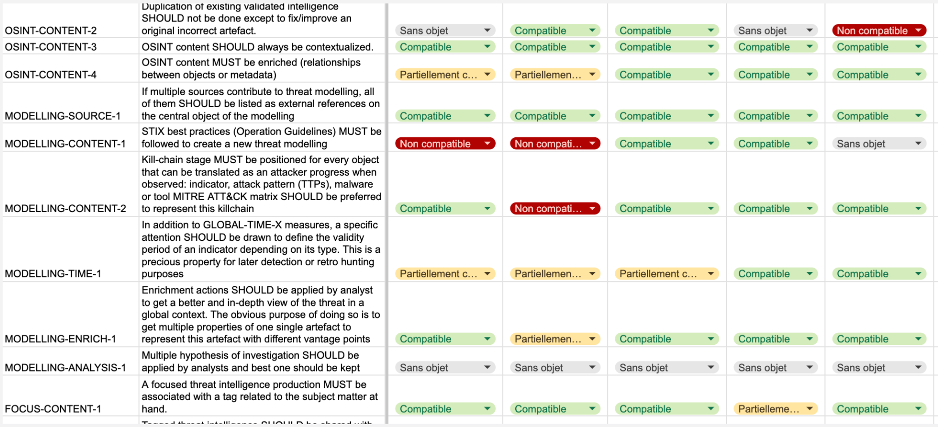
ID	Description
OSINT-SOURCE-1	Information MUST come from an OSINT source or at least from a source accommodating of broad data sharing (TLP:CLEAR, TLP:GREEN) and will be marked accordingly



ID	Description
INCIDENT-TIME-1	Each artefact associated with the incident MUST be timestamped precisely to establish an attack timeline

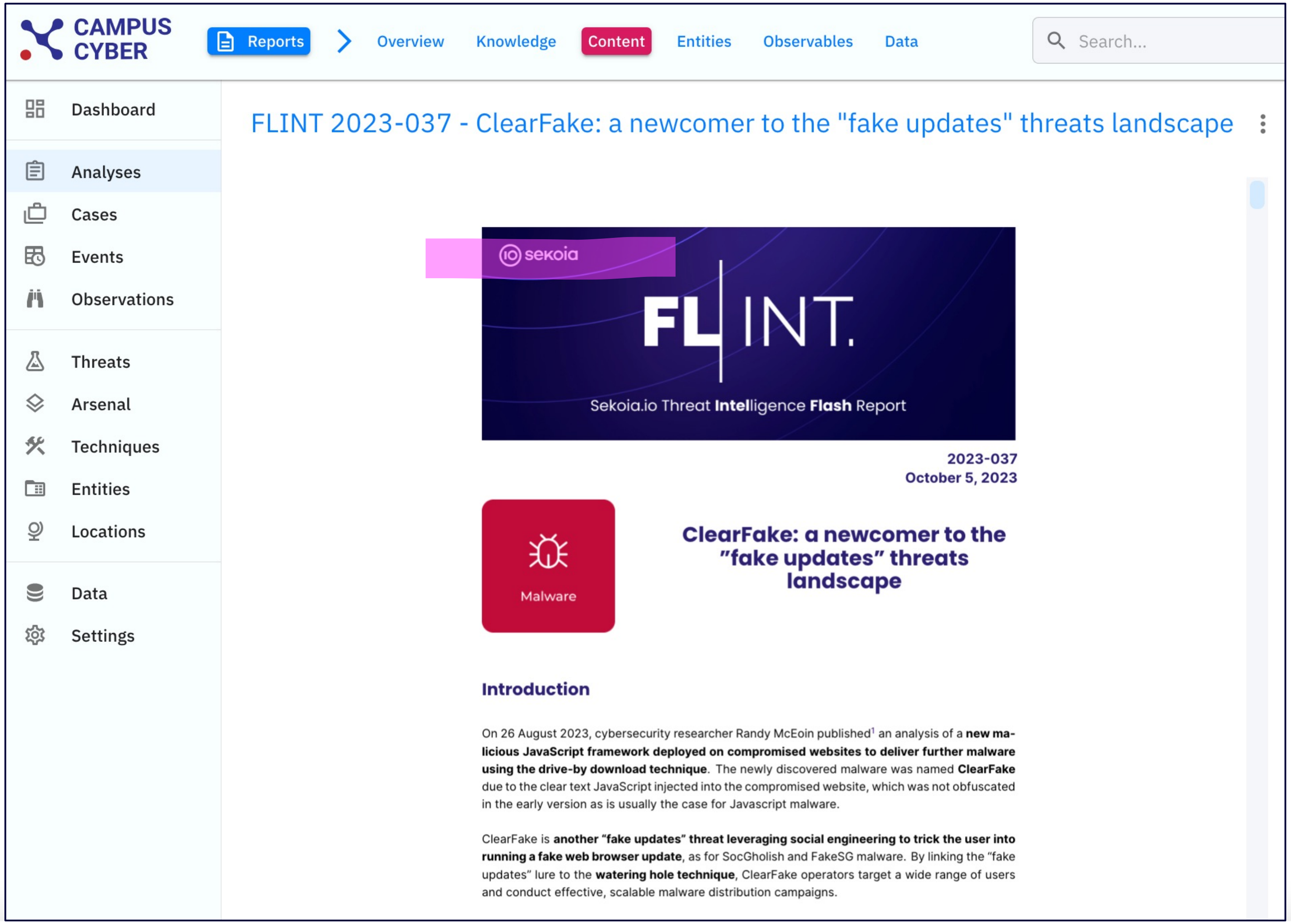
04. PLATFORM (where?).

- Criterias
  - Mapping of technical features vs doctrine
  - Members experience and apetite
  - Hosting environment
- Choice
  - OpenCTI w/ Filigran support



OSINT-CONTENT-2	Duplication of existing validated intelligence SHOULD not be done except to fix/improve an original incorrect artefact.	Sans objet	Compatible	Compatible	Sans objet	Non compatible
OSINT-CONTENT-3	OSINT content SHOULD always be contextualized.	Compatible	Compatible	Compatible	Compatible	Compatible
OSINT-CONTENT-4	OSINT content MUST be enriched (relationships between objects or metadata)	Partiellement c…	Partiellemen…	Compatible	Compatible	Compatible
MODELLING-SOURCE-1	If multiple sources contribute to threat modelling, all of them SHOULD be listed as external references on the central object of the modelling	Compatible	Compatible	Compatible	Compatible	Compatible
MODELLING-CONTENT-1	STIX best practices (Operation Guidelines) MUST be followed to create a new threat modelling	Non compatible	Non compati…	Compatible	Compatible	Sans objet
MODELLING-CONTENT-2	Kill-chain stage MUST be positioned for every object that can be translated as an attacker progress when observed: indicator, attack pattern (TTPs), malware or tool MITRE ATT&CK matrix SHOULD be preferred to represent this killchain	Compatible	Non compati…	Compatible	Compatible	Compatible
MODELLING-TIME-1	In addition to GLOBAL-TIME-X measures, a specific attention SHOULD be drawn to define the validity period of an indicator depending on its type. This is a precious property for later detection or retro hunting purposes	Partiellement c…	Partiellemen…	Partiellement c…	Compatible	Compatible
MODELLING-ENRICH-1	Enrichment actions SHOULD be applied by analyst to get a better and in-depth view of the threat in a global context. The obvious purpose of doing so is to get multiple properties of one single artefact to represent this artefact with different vantage points	Compatible	Partiellemen…	Compatible	Compatible	Compatible
MODELLING-ANALYSIS-1	Multiple hypothesis of investigation SHOULD be applied by analysts and best one should be kept	Sans objet	Sans objet	Sans objet	Sans objet	Sans objet
FOCUS-CONTENT-1	A focused threat intelligence production MUST be associated with a tag related to the subject matter at hand.	Compatible	Compatible	Compatible	Partielleme…	Compatible
	Tagged threat intelligence SHOULD be shared with					

04. PLATFORM (Use case #1/OSINT).



FLINT 2023-037 - ClearFake: a newcomer to the "fake updates" threats landscape

2023-037
October 5, 2023

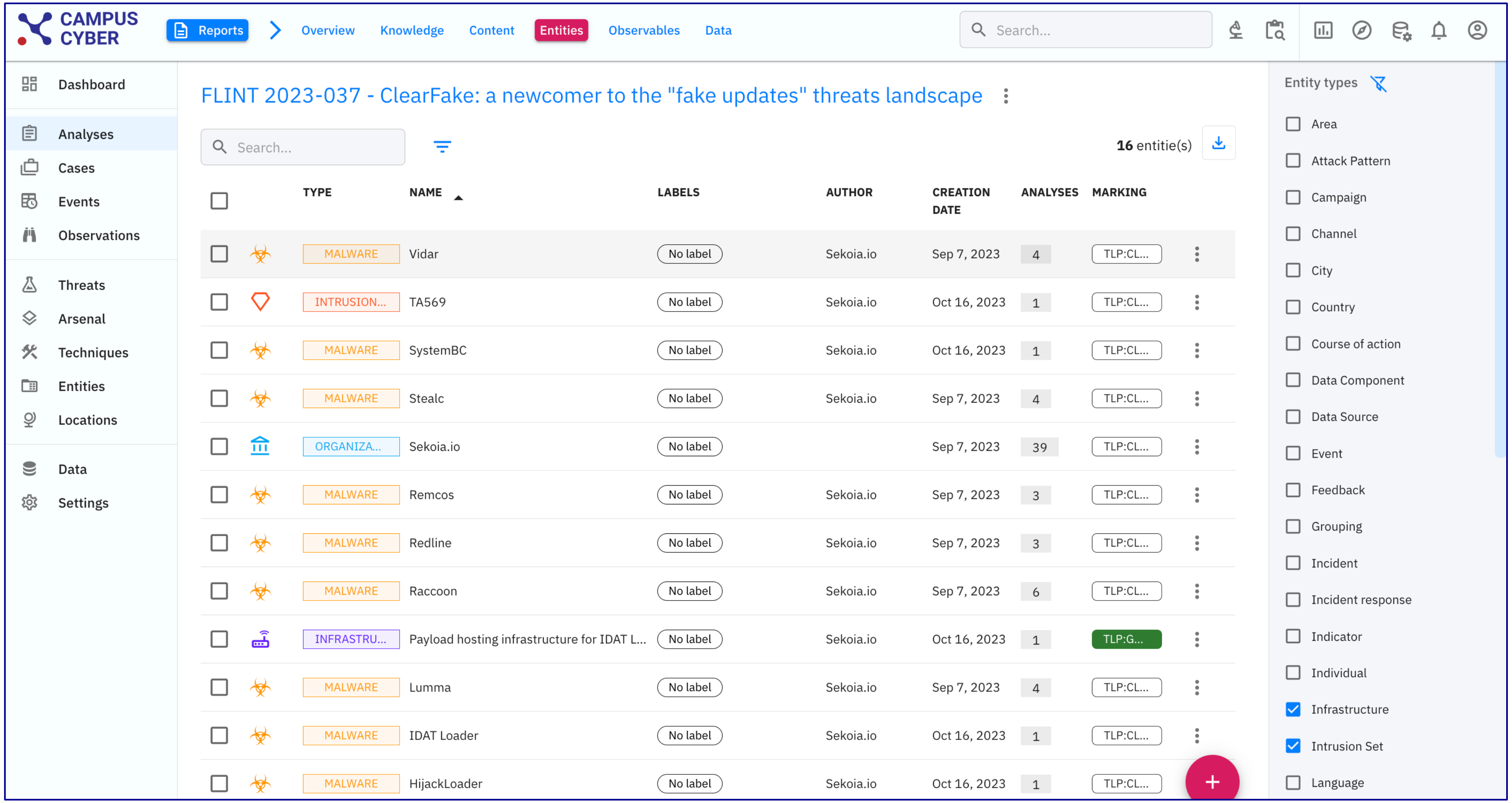
ClearFake: a newcomer to the "fake updates" threats landscape

Introduction

On 26 August 2023, cybersecurity researcher Randy McEoin published[1] an analysis of a **new malicious JavaScript framework deployed on compromised websites to deliver further malware using the drive-by download technique**. The newly discovered malware was named **ClearFake** due to the clear text JavaScript injected into the compromised website, which was not obfuscated in the early version as is usually the case for Javascript malware.

ClearFake is **another "fake updates" threat leveraging social engineering to trick the user into running a fake web browser update**, as for SocGholish and FakeSG malware. By linking the "fake updates" lure to the **watering hole technique**, ClearFake operators target a wide range of users and conduct effective, scalable malware distribution campaigns.

04. PLATFORM (Use case #1/OSINT).



FLINT 2023-037 - ClearFake: a newcomer to the "fake updates" threats landscape

Search...

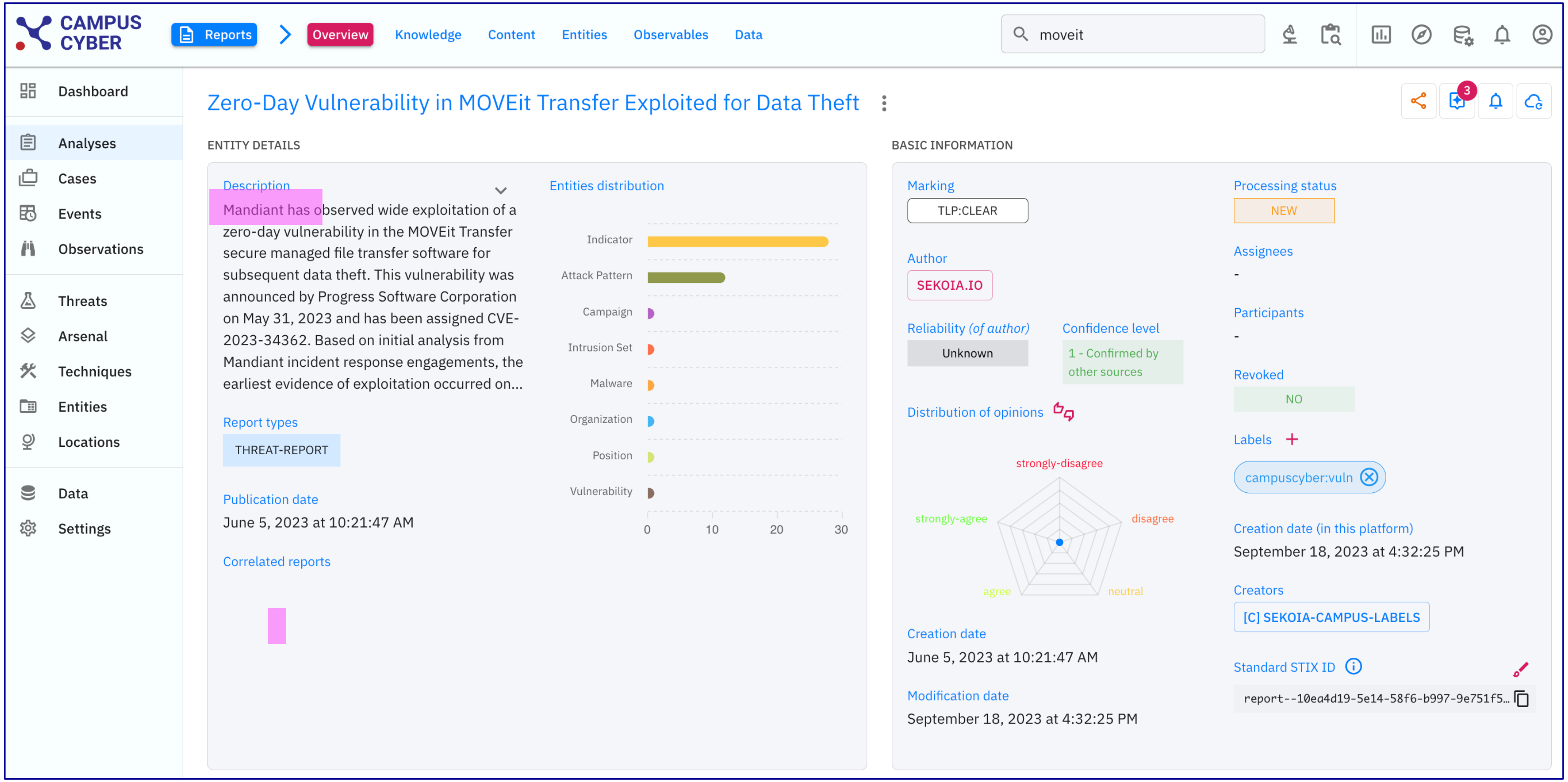
16 entitie(s)

□	TYPE	NAME ▲	LABELS	AUTHOR	CREATION DATE	ANALYSES	MARKING
□	MALWARE	Vidar	No label	Sekoia.io	Sep 7, 2023	4	TLP:CL...
□	INTRUSION...	TA569	No label	Sekoia.io	Oct 16, 2023	1	TLP:CL...
□	MALWARE	SystemBC	No label	Sekoia.io	Oct 16, 2023	1	TLP:CL...
□	MALWARE	Stealc	No label	Sekoia.io	Sep 7, 2023	4	TLP:CL...
□	ORGANIZA...	Sekoia.io	No label		Sep 7, 2023	39	TLP:CL...
□	MALWARE	Remcos	No label	Sekoia.io	Sep 7, 2023	3	TLP:CL...
□	MALWARE	Redline	No label	Sekoia.io	Sep 7, 2023	3	TLP:CL...
□	MALWARE	Raccoon	No label	Sekoia.io	Sep 7, 2023	6	TLP:CL...
□	INFRASTRU...	Payload hosting infrastructure for IDAT L...	No label	Sekoia.io	Oct 16, 2023	1	TLP:G...
□	MALWARE	Lumma	No label	Sekoia.io	Sep 7, 2023	4	TLP:CL...
□	MALWARE	IDAT Loader	No label	Sekoia.io	Oct 16, 2023	1	TLP:CL...
□	MALWARE	HijackLoader	No label	Sekoia.io	Oct 16, 2023	1	TLP:CL...

Entity types

- □ Area
- □ Attack Pattern
- □ Campaign
- □ Channel
- □ City
- □ Country
- □ Course of action
- □ Data Component
- □ Data Source
- □ Event
- □ Feedback
- □ Grouping
- □ Incident
- □ Incident response
- □ Indicator
- □ Individual
- ☑ Infrastructure
- ☑ Intrusion Set
- □ Language

04. PLATFORM (Use case #2/CTI Focus).



Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft

ENTITY DETAILS

Description

Mandiant has observed wide exploitation of a zero-day vulnerability in the MOVEit Transfer secure managed file transfer software for subsequent data theft. This vulnerability was announced by Progress Software Corporation on May 31, 2023 and has been assigned CVE-2023-34362. Based on initial analysis from Mandiant incident response engagements, the earliest evidence of exploitation occurred on...

Report types

THREAT-REPORT

Publication date

June 5, 2023 at 10:21:47 AM

Correlated reports

Entities distribution

BASIC INFORMATION

Marking

TLP:CLEAR

Author

SEKOIA.IO

Reliability *(of author)*

Unknown

Confidence level

1 - Confirmed by other sources

Distribution of opinions

Creation date

June 5, 2023 at 10:21:47 AM

Modification date

September 18, 2023 at 4:32:25 PM

Processing status

NEW

Assignees

-

Participants

-

Revoked

NO

Labels +

campuscyber:vuln

Creation date (in this platform)

September 18, 2023 at 4:32:25 PM

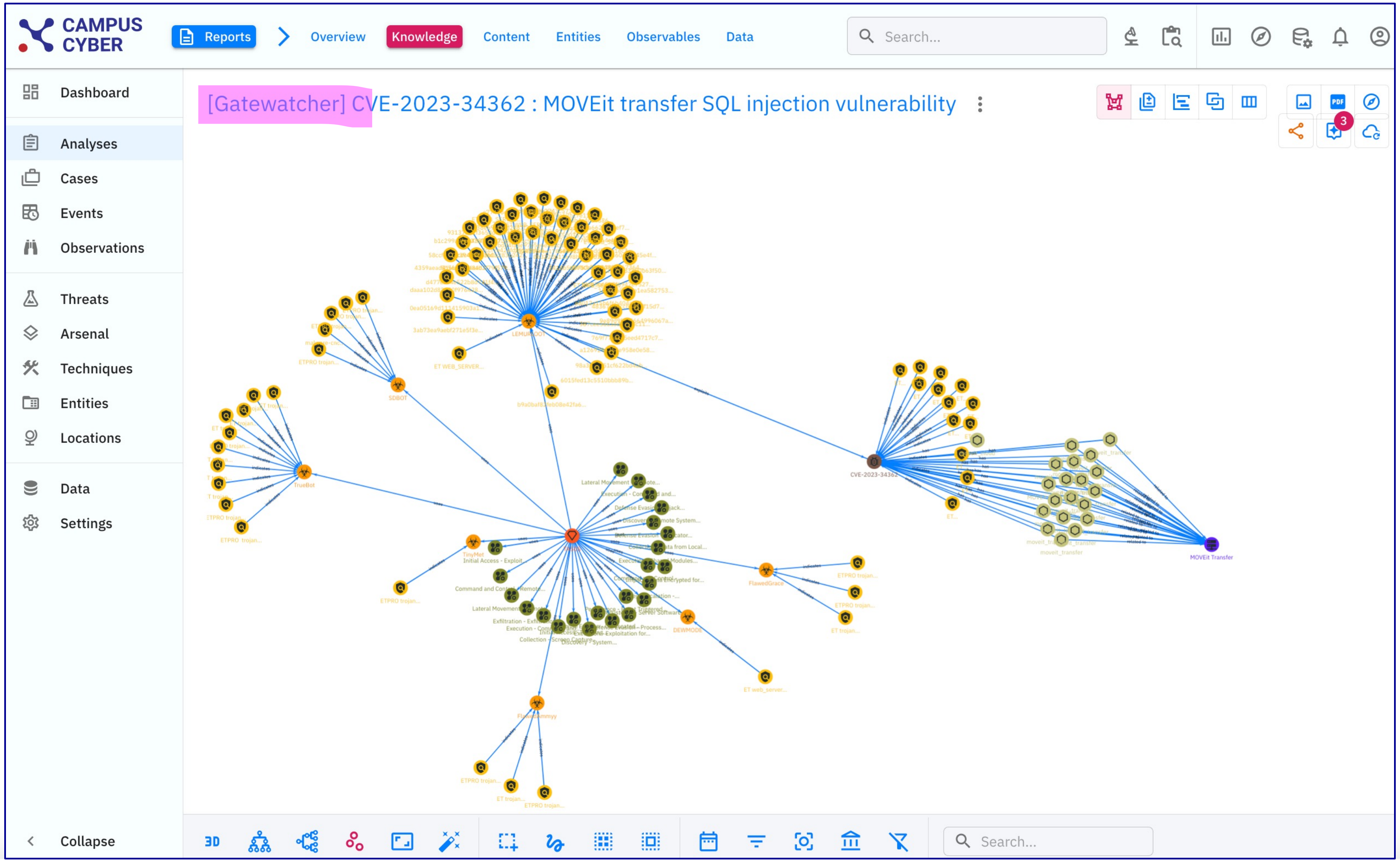
Creators

[C] SEKOIA-CAMPUS-LABELS

Standard STIX ID

report--10ea4d19-5e14-58f6-b997-9e751f5...

04. PLATFORM (Use case #2/CTI Focus).



[Gatewatcher] CVE-2023-34362 : MOVEit transfer SQL injection vulnerability

05. TAKE AWAYS

1 Obvious steps but long-term project

- 2 years
- Tons of discussions to promote sharing (who accept to share what and how?)

2 Doctrine can probably be better

- Adapt it to your environment
- Bring new ideas

3 Governance aspects not 100% ready

- Licence content
- Validation mechanisms

THANK YOU!

fabien@campuscyber.fr

david.bizeul@sekoia.io

Doctrine file

https://wiki.campuscyber.fr/images/1/10/221206_GT_CTI_doctrine.pdf