



**SEKOIA.IO**

# Utilisation de STIX

COMET 2021



**SEKOIA.IO**

- Rappels sur STIX
- Cas concrets
- Difficultés
- Perspectives

# STIX c'est quoi

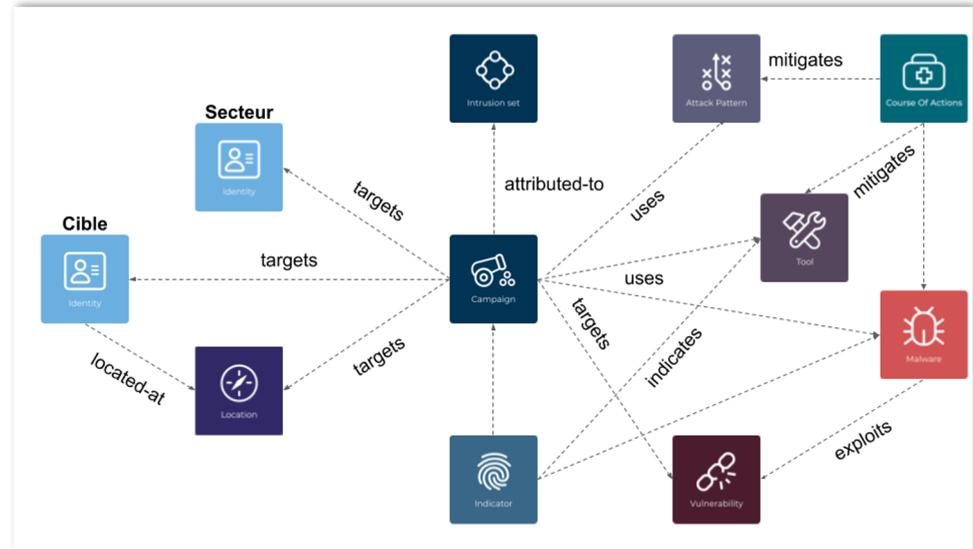
## STIX est un format graphe pour modéliser la threat intelligence

### Modélisation de multiples objets

- Campagne
- Mode opératoire
- Contre mesures
- Indicateurs
- Groupe d'attaquant

### Modélisation des relations

- Liaison
- Observation



Format lisible par les machines, graphes compréhensibles par l'humain

# Historique

- Origine

- Naissance de l'idée sur mailing list US en 2010
- Volonté de standardiser les indicateurs pour mieux partager
- Projet académique avec sponsoring DHS, US-CERT, MITRE en 2012
- Puis reprise industrielle et internationalisation en 2015

- Combats menés

- IOC de Mandiant gagne la première manche
- MISP objects reste un challenger
- STIX prend son envol avec STIX v2 (2017)
- Généralisation progressive dans l'industrie depuis 2019 avec STIX 2.1

# Le format

```
{
  "type": "bundle",
  "id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",
  "spec_version": "2.0",
  "objects": [
    {
      "type": "indicator",
      "id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
      "created_by_ref": "identity--f431f809-377b-45e0-aal1c-6a4751cae5ff",
      "created": "2016-04-29T14:09:00.000Z",
      "modified": "2016-04-29T14:09:00.000Z",
      "object_marking_refs": ["marking-definition--089a6ecb-cc15-43cc-9494-767639779123"],
      "name": "Poison Ivy Malware",
      "description": "This file is part of Poison Ivy",
      "pattern": "[file:hashes.'SHA-256' = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f']"
    },
    {
      "type": "marking-definition",
      "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",
      "created": "2016-08-01T00:00:00.000Z",
      "definition_type": "tlp",
      "definition": {
        "tlp": "green"
      }
    }
  ]
}
```

# Les Objets (SDOs) importants



**Adversary Objects**



**TTP Objects**



**Supporting Objects**

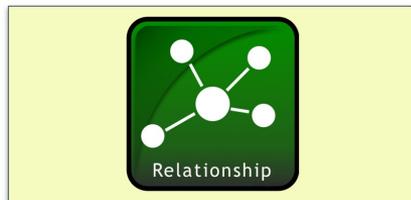


**Remediation Objects**



**Detection Objects**

# Les relations (SRO)

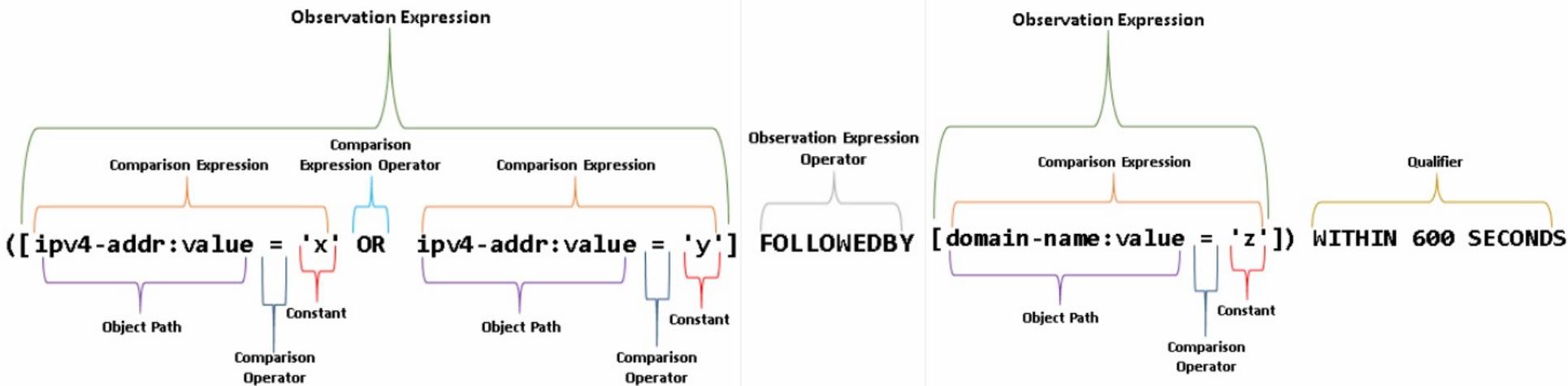


**Standard Relationship Objects**

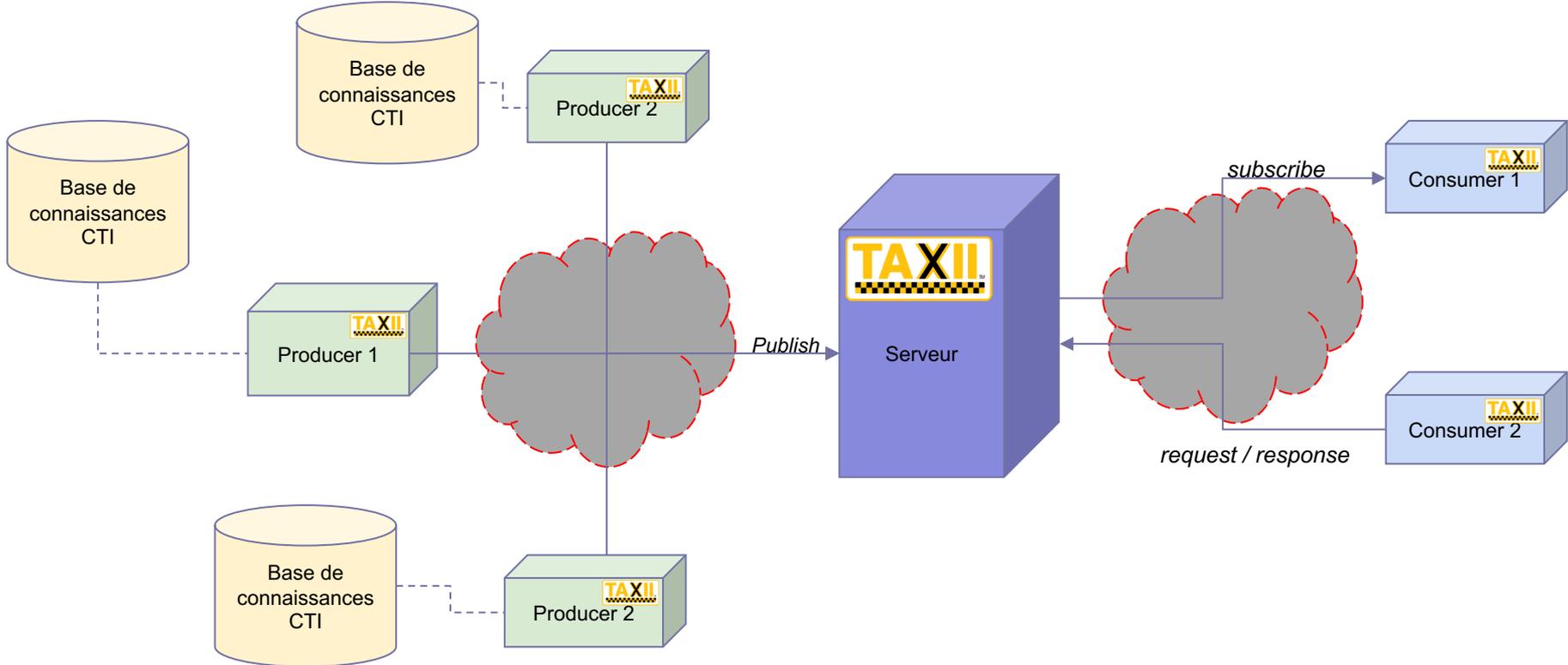


**Special Relationship Objects**

# Le langage (STIX patterning)



# Le transport (TAXII)





**SEKOIA.IO**

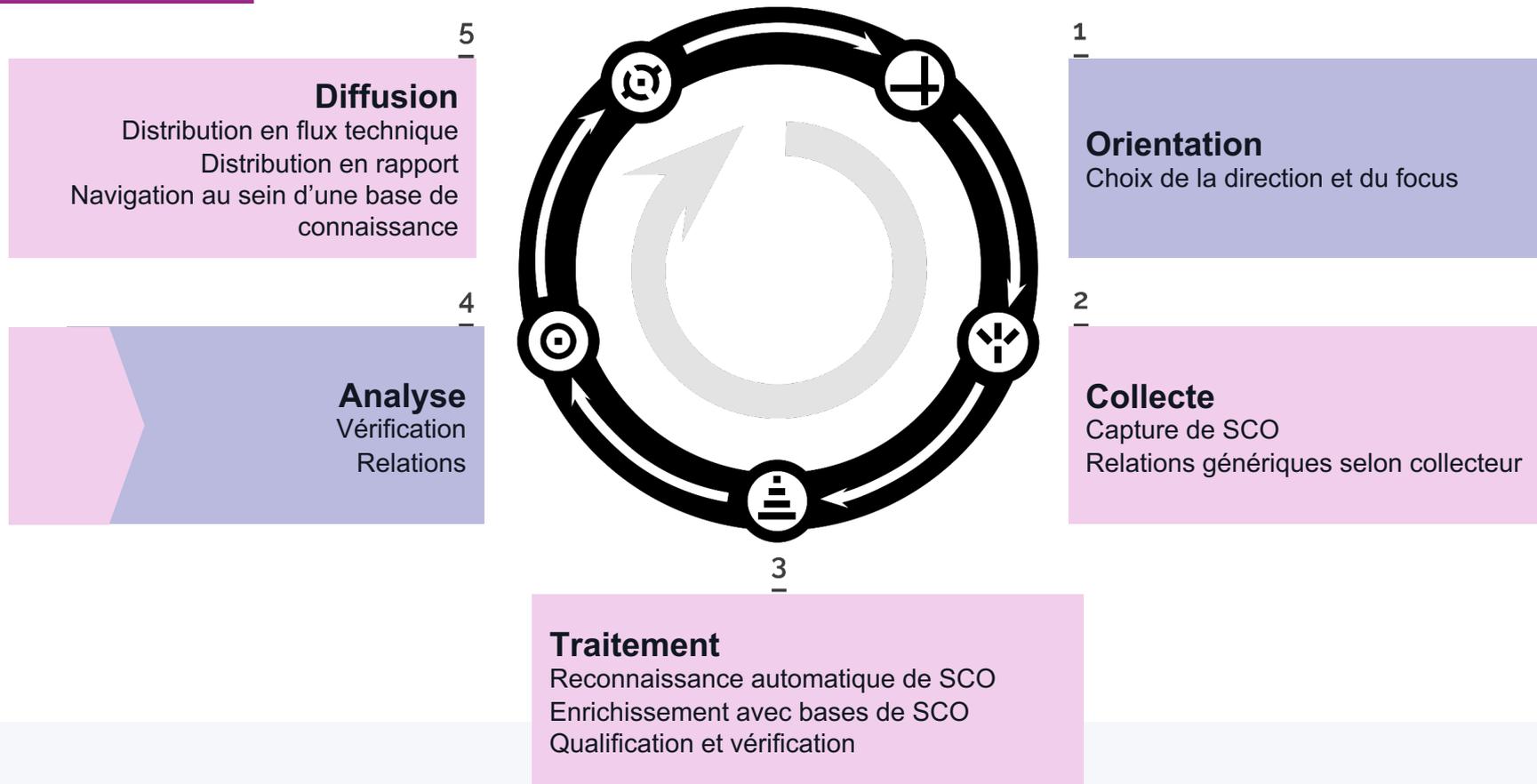
- Rappels sur STIX
- Cas concrets
- Difficultés
- Perspectives

# #0

Modélisation

STIX dans le cycle du renseignement

# Amélioration du cycle du renseignement / Outils & Analystes



# #1

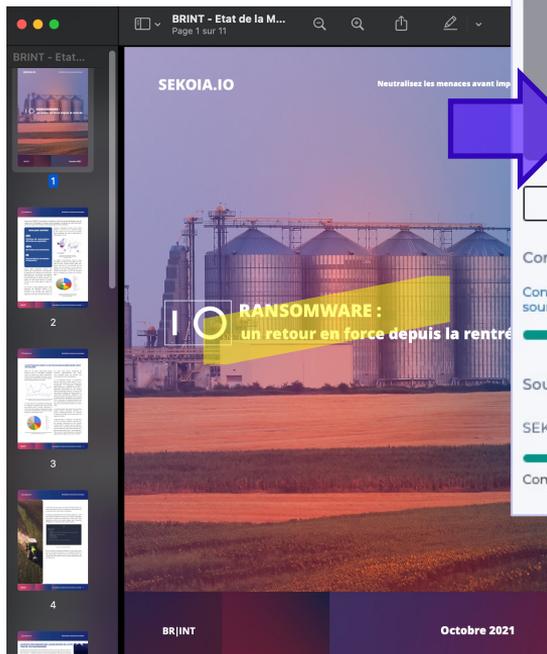
Modéliser de la CTI stratégique en STIX

Un rapport sectoriel interne

# Un rapport interne

- Un PDF
  - Avec texte
  - Et images
  - Encapsulable en base64
- Transformable en structure STIX
  - Un objet REPORT représentant le rapport
    - Des informations de marquage sur
      - La confiance
      - La source
      - Les critères de diffusion
    - Des objets différents qui lui sont reliés

# Exemple



1 - Le rapport source

Report

## 2 – Le marquage

Created by  
SEKOIA

Created at  
Oct 8, 2021

Modified at  
Oct 8, 2021

**WHITE**

Confidence

Confirmed by other sources

Sources

SEKOIA

Completely reliable

Report types

Published at

Oct 8, 2021

Object References

## 3 – Toutes les données associées

malware threat-actor identity attack-pattern campaign

TLP	Name	Subtypes	Confidence	Sources	Updated date
GREEN	Cuba	ransomware	1	SEKOIA	7 months ago
WHITE	Conti	ransomware	1	SEKOIA	6 days ago
GREEN	BlackMatter	ransomware	1		2 months ago
WHITE	Colossus	ransomware	1		10 days ago
WHITE	KARMA ransomware	ransomware	2		about 2 months ago
WHITE	LockBit	ransomware	1		about 1 month ago
GREEN	Ragnar Locker	ransomware	1	SEKOIA The MITRE Corporation	about 1 month ago

# #2

Modéliser de la CTI tactique en STIX

Une campagne d'attaque

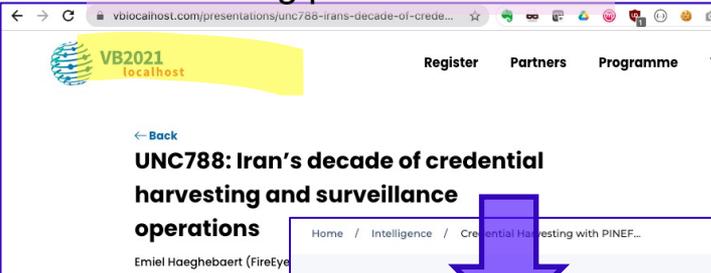


# Une publication

- Un **blog post** sur Internet
  - Du contenu avec des éléments connus et inconnus
  - Différentes formulations
    - Certains contenus sous forme de phrases
    - Certains sous forme de listes d'indicateurs
- Transformable en structure STIX
  - Une campagne clairement identifiée
  - Des objets associés
  - Possibilité de pivoter autour de chaque objet pour relier d'autres campagnes

# Exemple

## 1 – Un blog post



Home / Intelligence / Credential Harvesting with PINEF...

**Name**  
Credential Harvesting with PINEFLOWER malicious app

**External Ids**

**Aliases**  
Credential Harvesting with PINEFLOWER malicious ap

**Description**  
In March 2021, Mandiant analysts uncovered a wide

**Relationships** External References Rep...

targets	uses	indicates	originates-from	
Type	Name	Confidence	External Source	Updated Date
originates-from	Iran, Islamic Republic of	2	www.mandiant.com	39 minutes ago

## 2 – Les relations

## 3 – Pivot et représentation graphique

Home / Intelligence / UNC788: Iran's decade of creden... / graphical

Charming Kitten

Relationship

uses

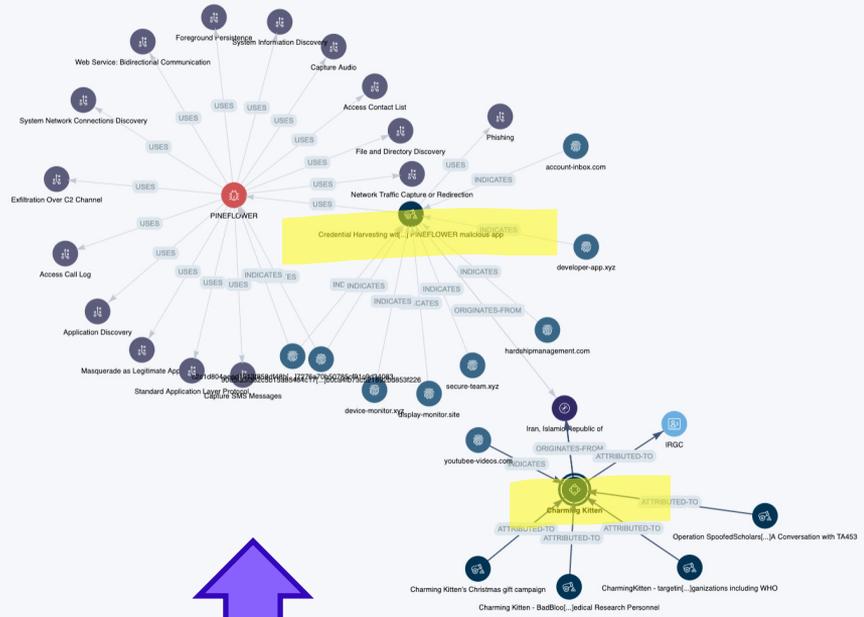
- IRCC
- Operation SpoofedScholars: A Co...
- Charming Kitten - BadBlood cam...
- Charming Kitten's Christmas gift...
- CharmingKitten - targeting Covid...

Items per page: 5 1-5

indicates

targets

originates-from



# #3

Modéliser de la CTI technique en STIX

L'évolution d'une infrastructure

# Un mode opératoire

- Une **propriété technique** d'un groupe d'attaquants
  - Qui les caractérise
  - Qui peut s'observer sur un actif informatique
- Permettant de découvrir des nouveaux indicateurs modélisables en STIX
  - Contexte et description
  - Sensibilité de l'information

# Exemple

27 lines (27 sloc) | 811 Bytes

```

1 title: malleableC2_wikipedia
2 uuid: f99cf47f-1ea8-11eb-aba4-00155d7e7a61
3 status: production
4 description: |
5   Default certificate for malleableC2 defined in github
6 author:
7 confidence: 99
8 created: 2020-10-07
9 modified: 2021-06-14
10 malwarefamily: Malleable C2
11 references:
12   - No ref
13 classification:
14   - type: tlp
15     value: amber
16   - type: pap
17     value: amber
18 condition:
19   - OR:
20     #- type: Shodan
21     # query: ''
22     - type: CensysV2
23     query: '"C=US, ST=CA, L=San Francisco, O=, OU=Wikimedia Found
24     #- type: BinaryEdge
25     # query: ''
26     - type: Onyphe
27     query: 'issuer.commonname: "*.wikipedia.org" issuer.organizati
  
```

## 1 – Un tracker



**Name:** MalleableC2

**External ids:** -

**Aliases:** MalleableC2

**Confidence:** GREEN

**Sources:** SEKOIA (Completely reliable)

**Kill chain:** Cyber Kill Chain, MITRE ATT&CK, Reconnaissance, Weaponization, Delivery

**Description:** MalleableC2 is one of the Cobalt Strike feature handling components. It is used by some threat actors.

**Relationships:** Indicates uses

Type	Name	Confidence	Updated Date
Indicates	106.15.197.67	1	about 2 hours ago
Indicates	313.41.181	2	about 2 hours ago
Indicates	15.185.226.230	2	about 2 hours ago
Indicates	23.96.10.0	1	about 2 hours ago
Indicates	54.263.220.118	1	about 2 hours ago

## 2 – Les indicateurs associés

## 3 – Les compléments

**Name:** [REDACTED]

**Created by:** SEKOIA

**Created at:** Mar 1, 2021

**External ids:** -

**Modified at:** Oct 11, 2021

**Indicator types:** malicious-activity

**Valid from:** Feb 19, 2021

**Valid until:** Apr 1, 2021

**Confidence:** malicieux-activité

**Confirmed by other sources:** 1

**Pattern (stix):** [ip4-addr:value = [REDACTED]]

**Sources:** www.mandiant.com (Usually reliable), SEKOIA (Completely reliable), SEKOIA C2 Tracker (Completely reliable)

**Kill chain:** Cyber Kill Chain (Used by FIN12), Reconnaissance

**Relationships:** Notes, Reports, Raw Object

Type	Name	Confidence	External Source	Updated Date
Indicates	Cobalt Strike	2	SEKOIA, www.mandiant.com	about 1 hour ago
Indicates	MalleableC2	2	SEKOIA C2 Tracker	7 months ago
Indicates	WIZARD SPIDER - Cobalt Strike distrib...	1	SEKOIA	7 months ago

**Description:** Seen on port [443]

**Source:** SEKOIA C2 Tracker (Completely reliable)

**External references:** There is no external reference for this relationship



# #4

La détection

Usage basique de STIX patterning

# Exemple

1 – Des événements

2 – Repérage d'un indicateur dans le contenu

3 – Génération d'une alerte

4 – Utilisation des pivots pour créer du contexte

The screenshot displays the SEKOIA.IO interface for a specific alert. The main panel shows details for an alert with ID AL3BJYWhj5Vh, categorized as 'malware' and 'Intrusion using Cobalt Strike'. A 'Cyber kill chain' diagram is visible, with 'Command and Control' highlighted. A 'Threat Intelligence Context' section shows a pivot for IP address 20.199.116.167, identified as 'malicious-activity' with a 'WHITE' confidence level. A 'Timeline' on the right lists several 'User made GET request' events from the same IP address to various domains.

**3** (Alert details and Kill chain phases)

**1** (Timeline of events)

**2** (Threat Intelligence Context - IP pivot)

**4** (Context for EICAR SEKOIA test campaign)

# #5

La réaction

Utiliser les Course of Actions

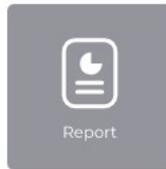




**SEKOIA.IO**

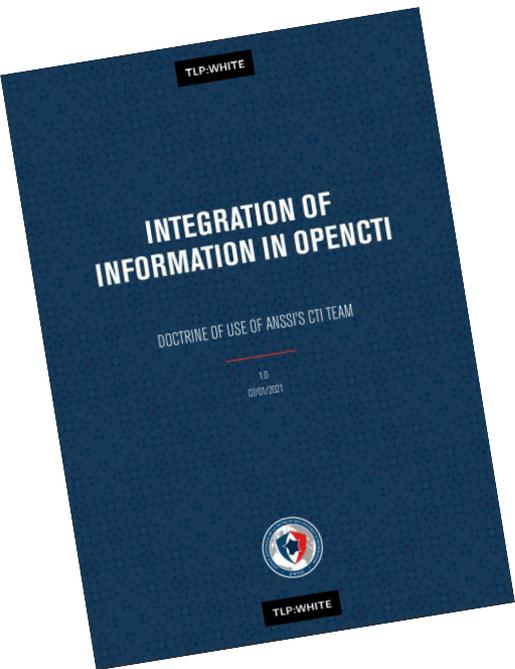
- Rappels sur STIX
- Cas concrets
- Difficultés
- Perspectives

# Les subtilités



- APT31, c'est quoi ?
- Mimikatz c'est quoi ?
- Solarwinds c'est quoi ?

# Le travail collaboratif



- Compréhension de STIX
  - Training minimaliste
- Doctrine d'équipe
  - Interprétation des objets
  - Sens des relations
  - Manière de modéliser ce qui n'existe pas
  - Nomenclature



**SEKOIA.IO**

- Rappels sur STIX
- Cas concrets
- Difficultés
- Perspectives

# La capacité à travailler ensemble en France

- Nombreux groupes au cours du temps pour partager
- Seule initiative qui ait fait ses preuves : Communauté MISP
- Nouvelle initiative **Campus Cyber** avec vraie envergure
  - Objectif : créer ensemble
  - Moyen : méthode commune
  - Format : STIX plebiscité
  - Scope : Modélisation OSINT pour commencer



# Idées fortes

## ATOUS

- STIX est devenu stable et éprouvé
- Format adapté à une capitalisation
  - Massive
  - Contextualisée
  - Où tout est relié
- Format adapté à la diffusion (TAXII)
  - Massive
  - Thématisée
  - Structuration ISAC

## VIGILANCE

- Besoin d'une méthode commune
  - Doctrine CTI
- Besoin d'un outillage compatible
  - Pour produire
  - Pour consommer



**SEKOIA.IO**

Neutralisez les menaces avant impact



[www.sekoia.io](http://www.sekoia.io)