SEKOIA.IO

Utilisation de STIX

COMET 2021

SEKOIA.IO

Agenda

- Rappels sur STIX
- Cas concrets
- Difficultés
- Perspectives

STIX c’est quoi

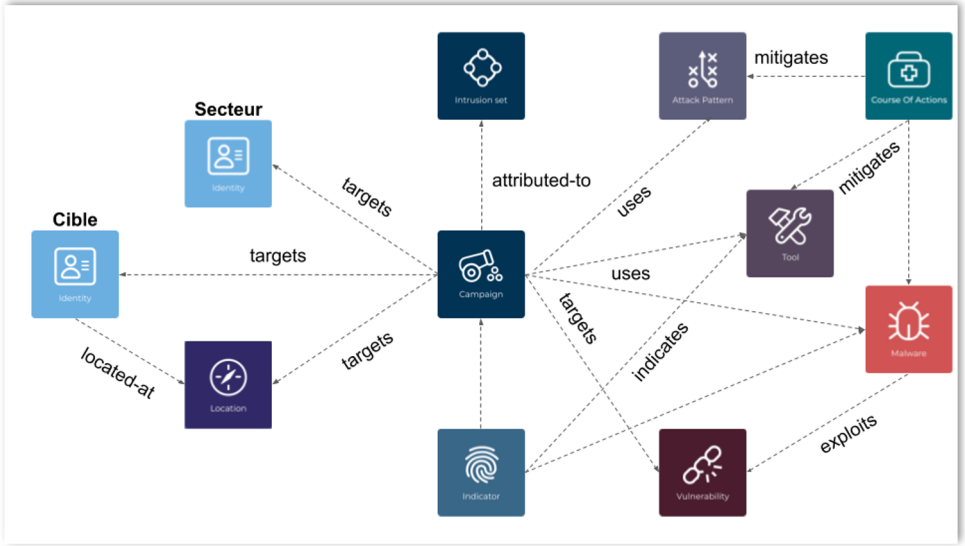
STIX est un format graphe pour modéliser la threat intelligence

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-aa1c-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

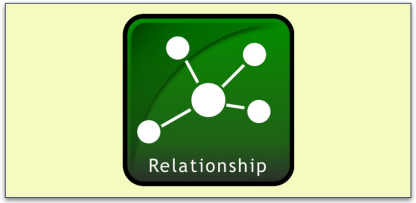
TTP Objects

Supporting Objects

Remediation Objects

Detection Objects

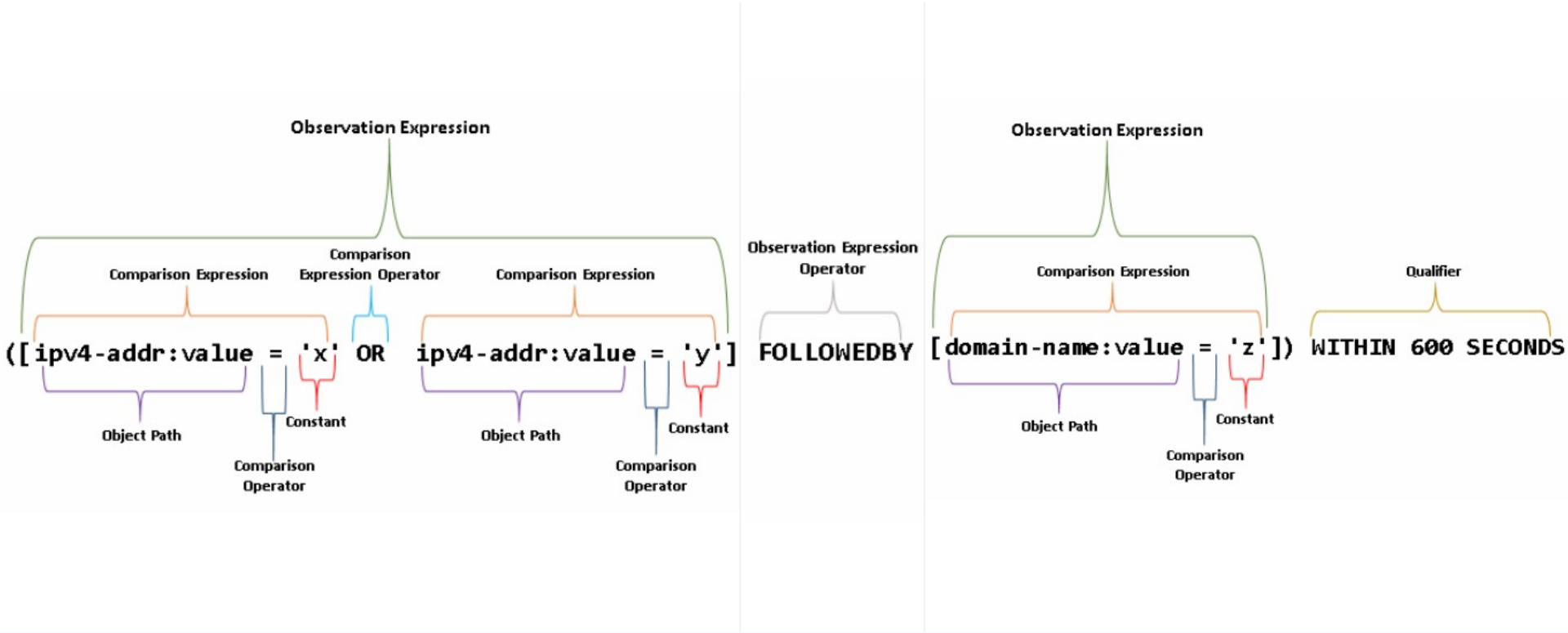
Les relations (SRO)



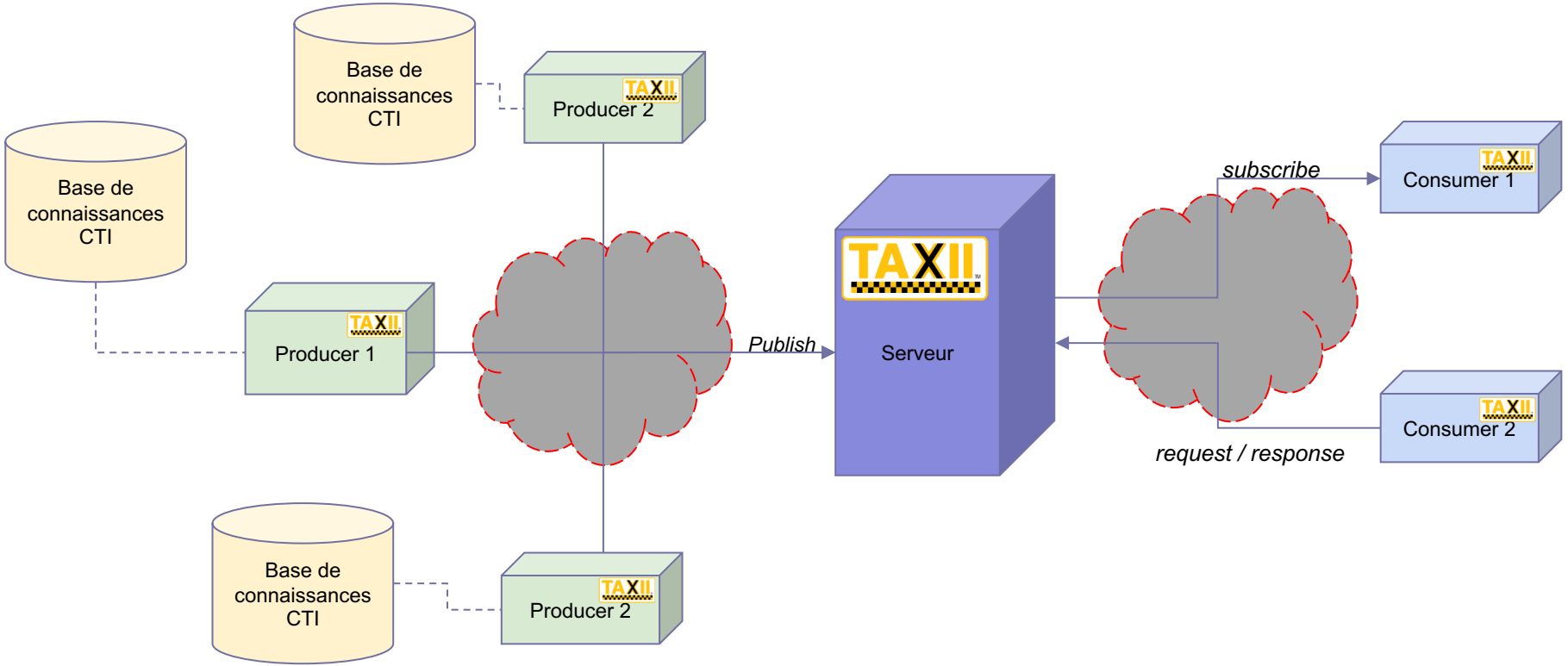
Standard Relationship Objects

Special Relationship Objects

Le langage (STIX patterning)



Le transport (TAXII)



SEKOIA.IO

Agenda

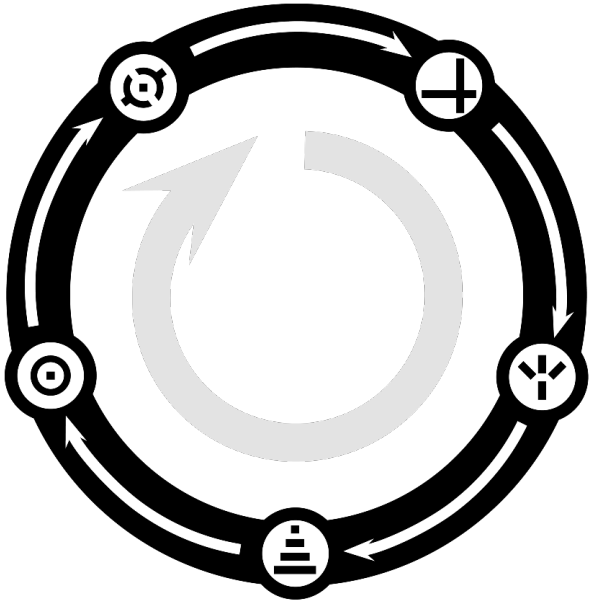
- Rappels sur STIX
- Cas concrets
- Difficultés
- Perspectives

#0

Modélisation

STIX dans le cycle du renseignement

Amélioration du cycle du renseignement / Outils & Analystes



1

Orientation
Choix de la direction et du focus

2

Collecte
Capture de SCO
Relations génériques selon collecteur

3

Traitement
Reconnaissance automatique de SCO
Enrichissement avec bases de SCO
Qualification et vérification

4

Analyse
Vérification
Relations

5

Diffusion
Distribution en flux technique
Distribution en rapport
Navigation au sein d'une base de connaissance

#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

2 – Le marquage

3 – Toutes les données associées

#2

Modéliser de la CTI tactique en STIX

Une campagne d'attaque

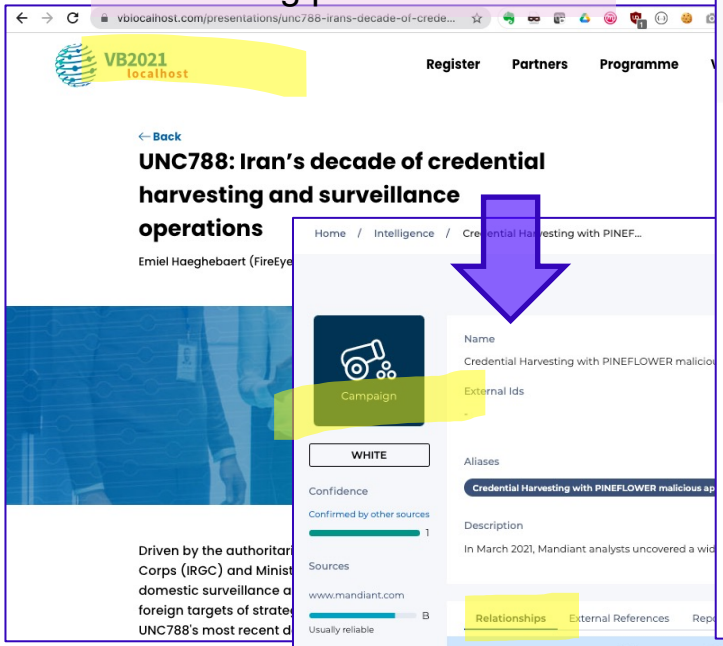
🎬 Une publication

- 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

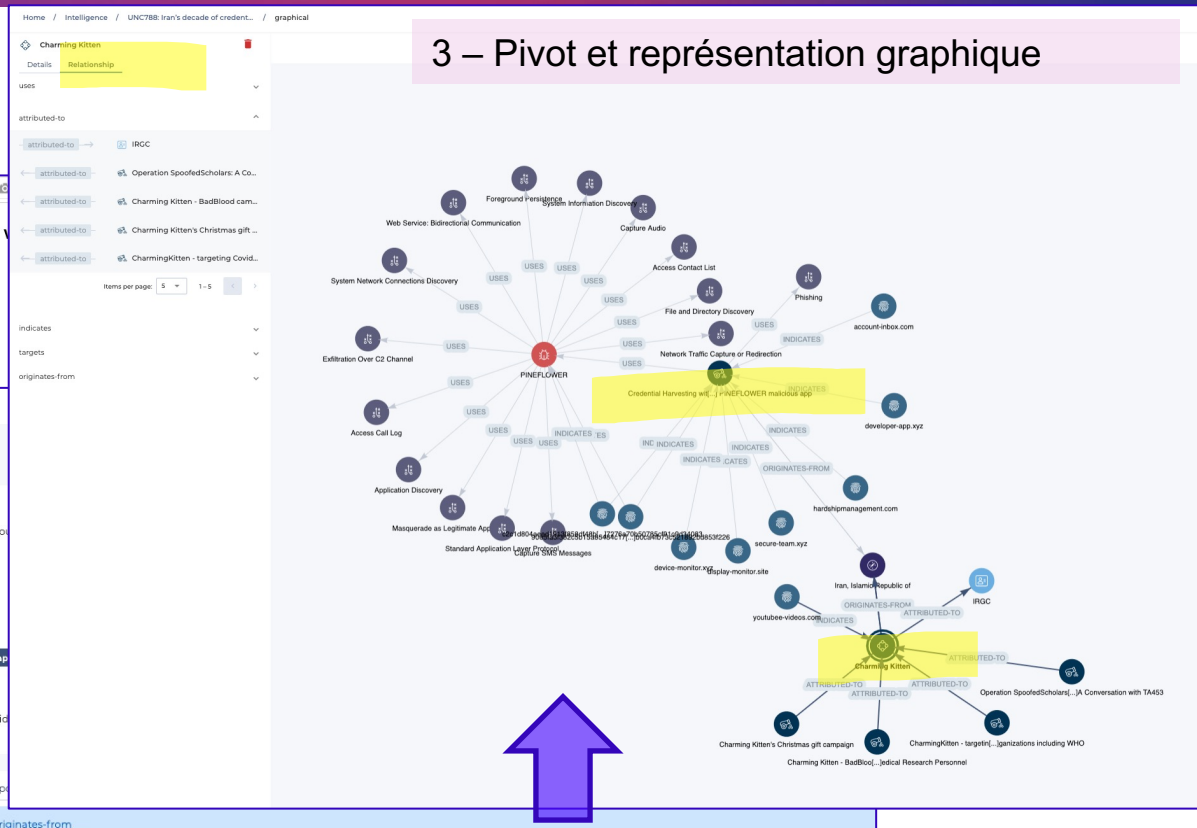
Exemple

1 – Un blog post



2 – Les relations

3 – Pivot et représentation graphique



#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

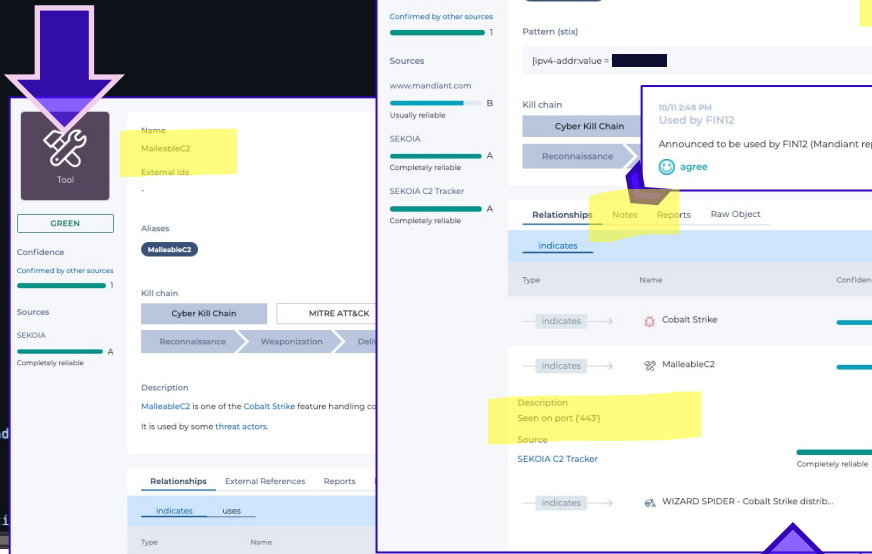
- Permettant de découvrir des nouveaux indicateurs modélisables en STIX
  - Contexte et description
  - Sensibilité de l'information

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



2 – Les indicateurs associés

3 – Les compléments

#4

La détection

Usage basique de STIX patterning

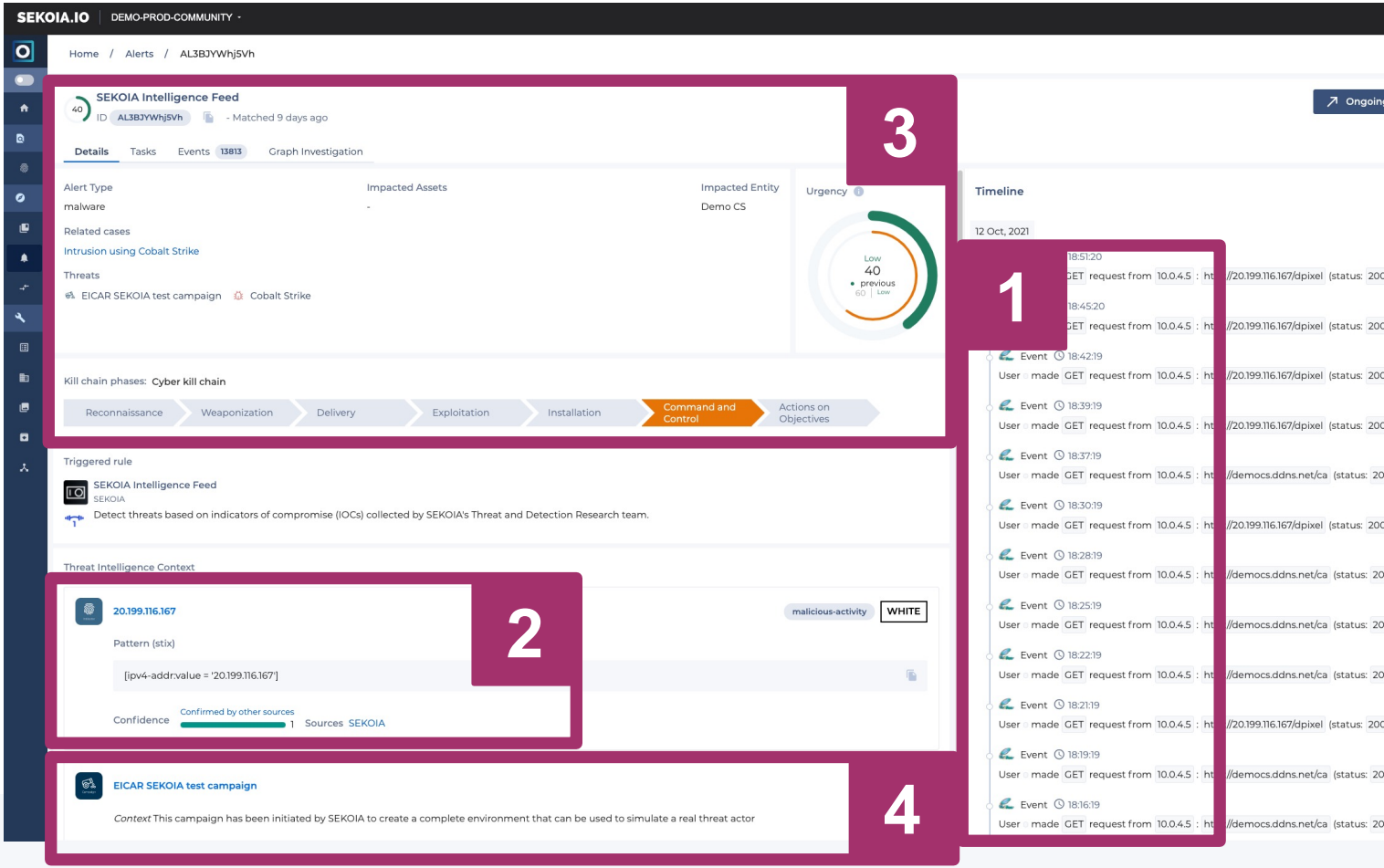
Exemple

1 – Des evénements

2 – Repérage d'un indicateur dans le contenu

3 – Génération d'une alerte

4 – Utilisation des pivots pour créer du contexte



#5

La réaction

Utiliser les Course of Actions

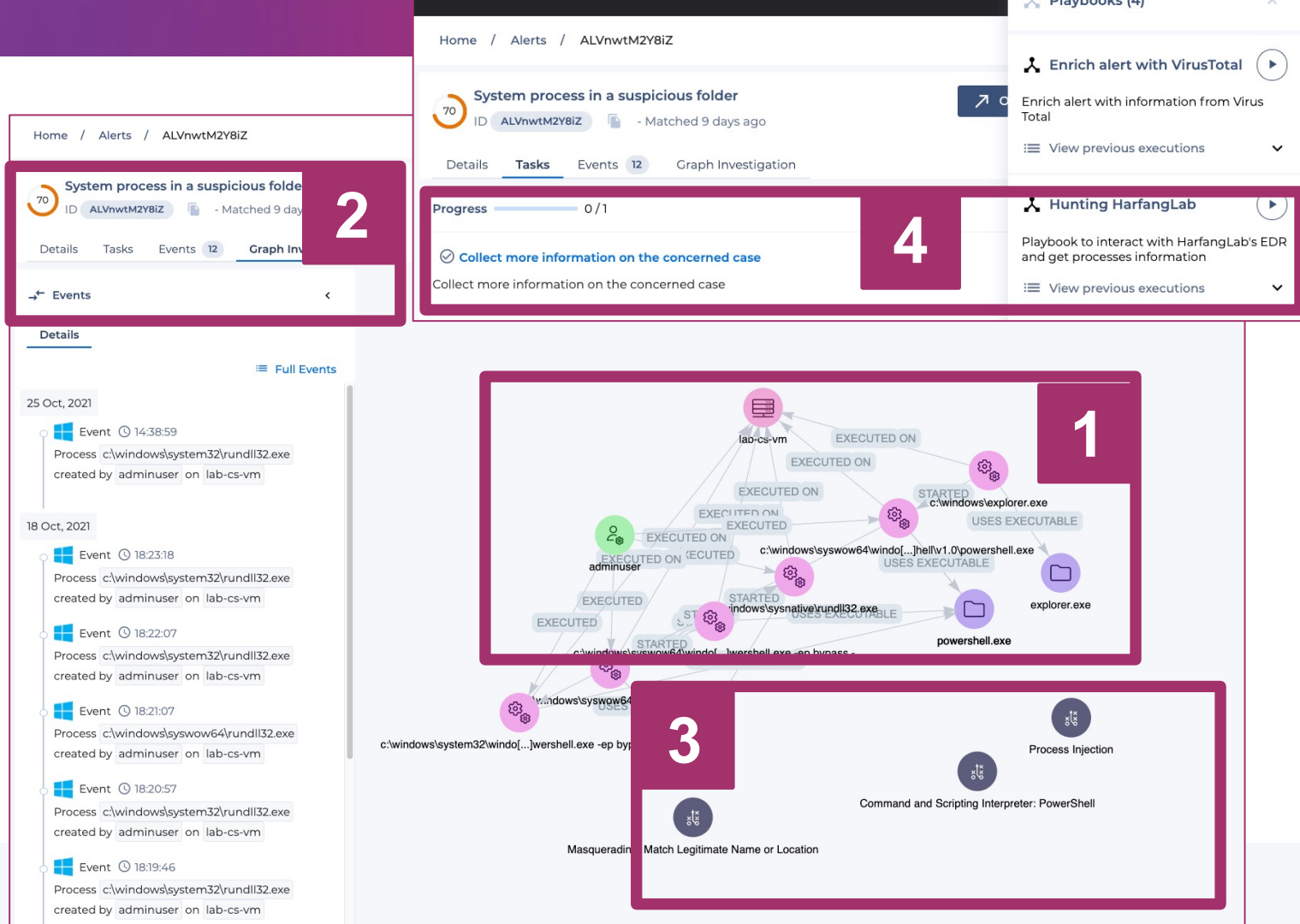
Exemple

1 – Des evénements

2 – Caractérisation d'un comportement malveillant

3 – TTP associés

4 – Contremesures crédibles associées via pivot



SEKOIA.IO

Agenda

- 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

Agenda

- 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

CAMPUS CYBER

Idées fortes

ATOUTS

- 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