SEKOIA.IO

Automatisation de la cyber sécurité

OSSIR
14/12/2021

david.bizeul@sekoia.io

Automatisation

”

Exécution totale ou partielle de tâches techniques par des machines fonctionnant sans intervention humaine.

SEKOIA.IO

2008 — Création

2013 — CERT

2016 — Acquisition et développement

2020 — Lancement

SEKŌIA

Accompagnement opérationnel

CERT (Red, Purple, Blue Teams)

SEKOIA.IO

Renseignement CTI

Plateforme XDR

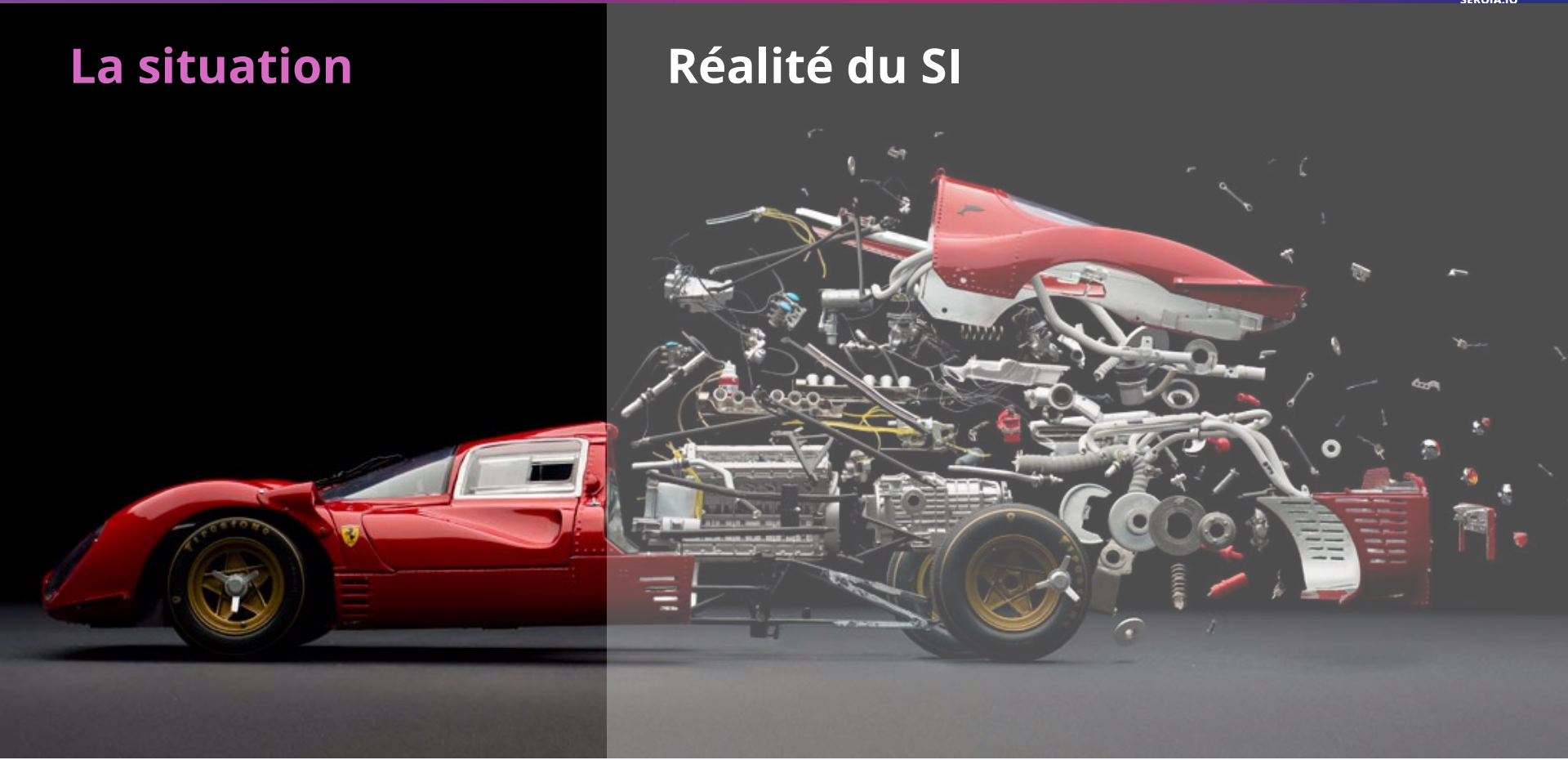
SEKOIA.IO

Agenda

- La réalité d’un SI et des équipes
- Les pistes
- Illustrations
- Conclusion

La situation

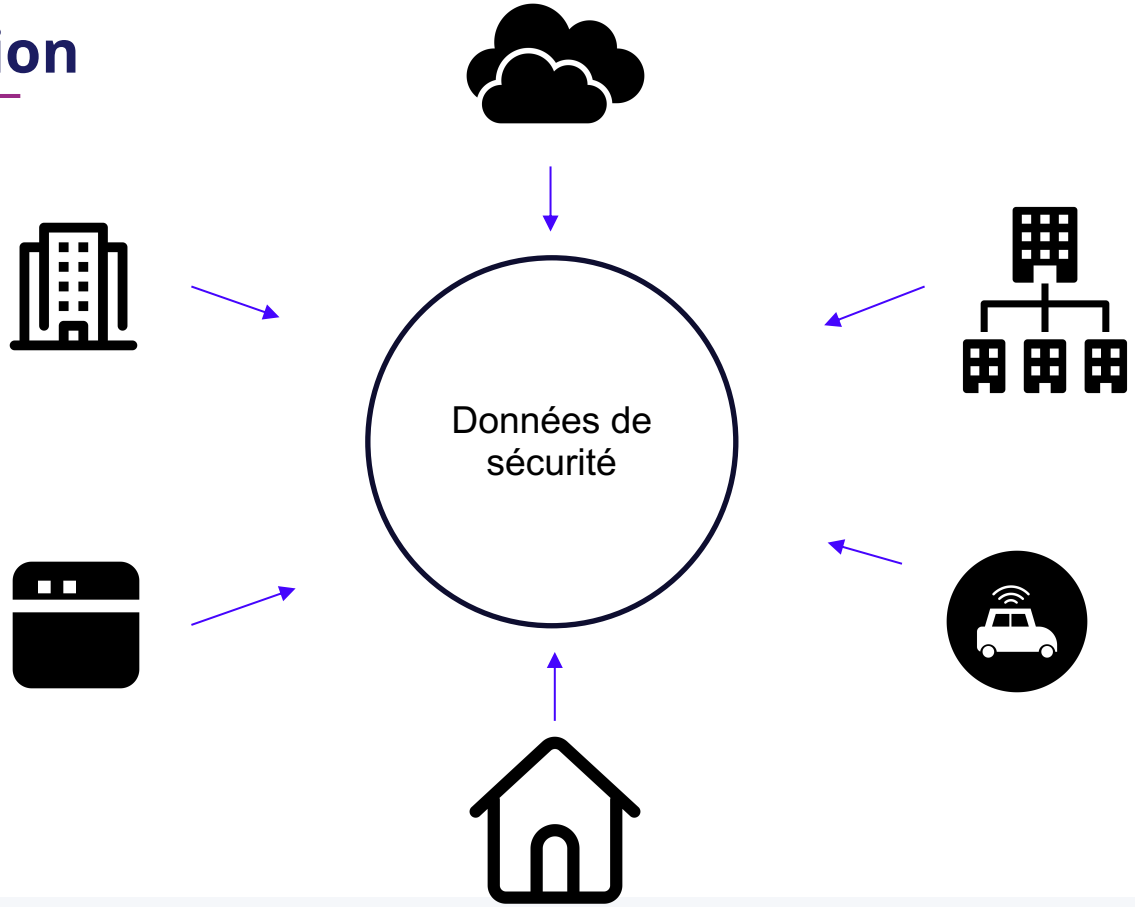
Réalité du SI



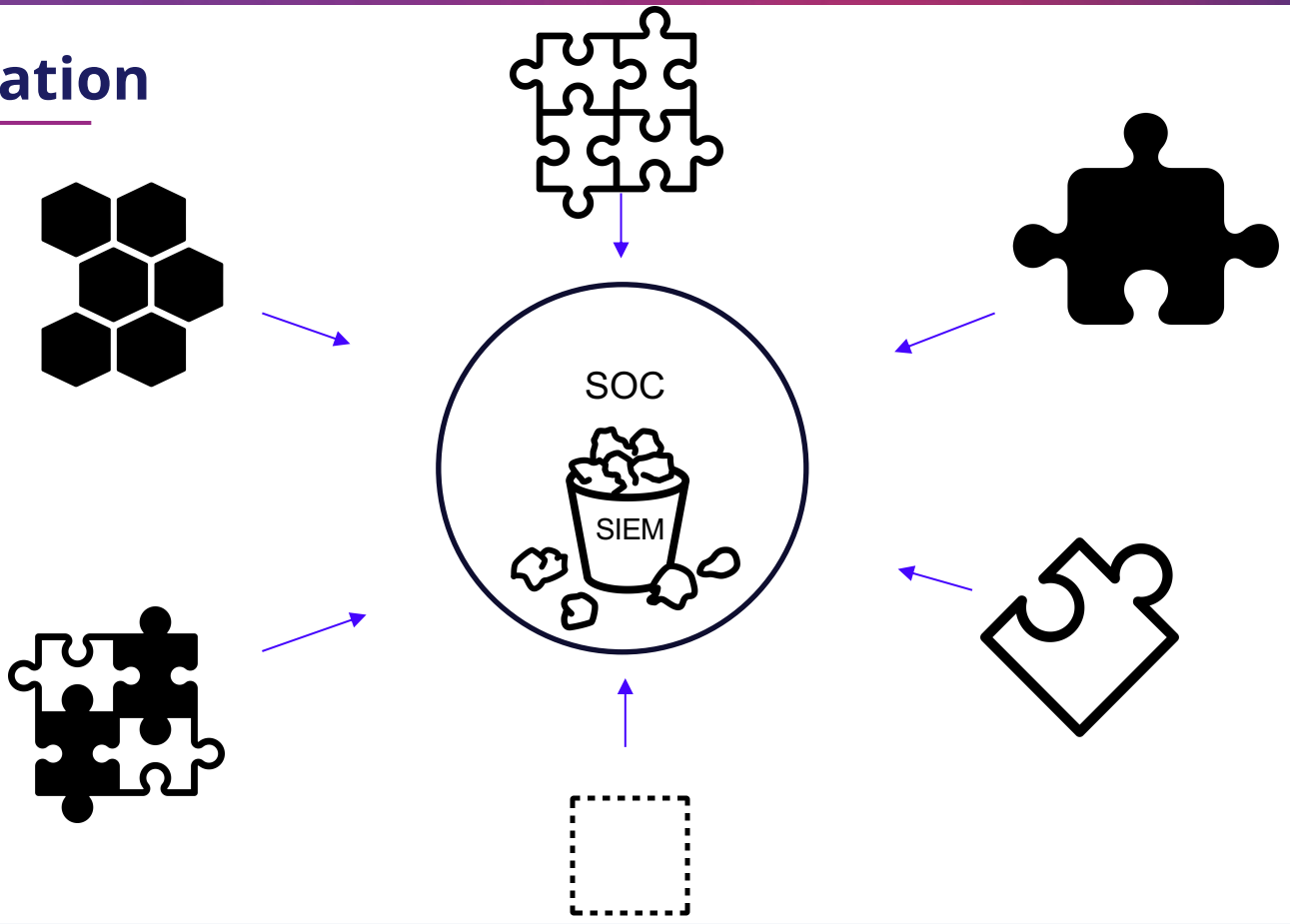
La situation

Couche de sécurité nécessaire

La situation



La situation

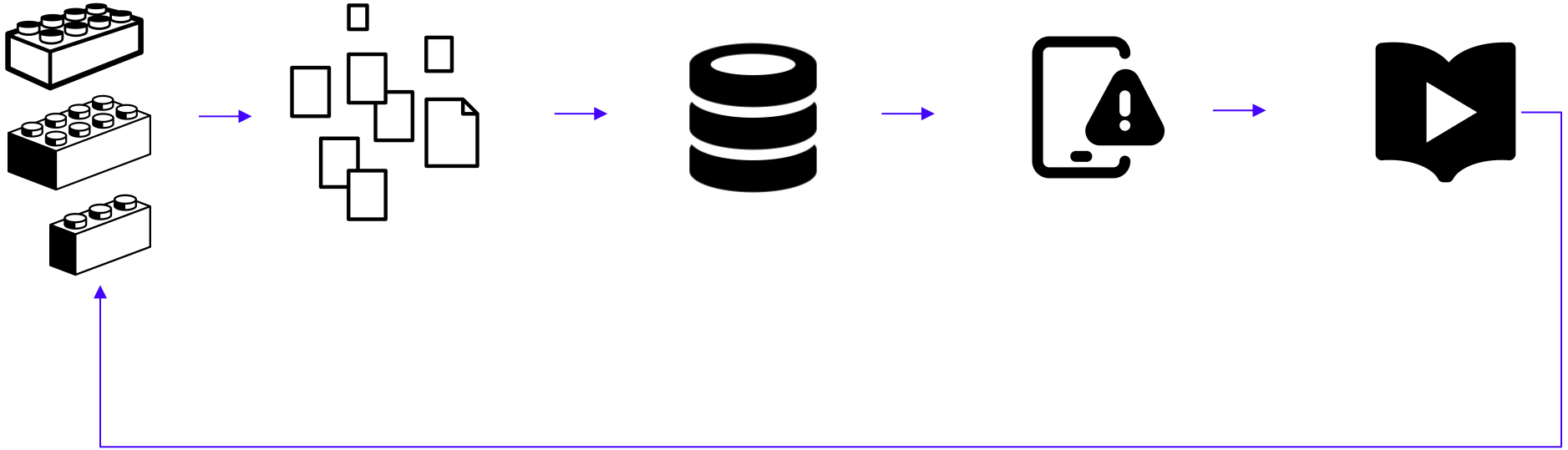


SEKOIA.IO

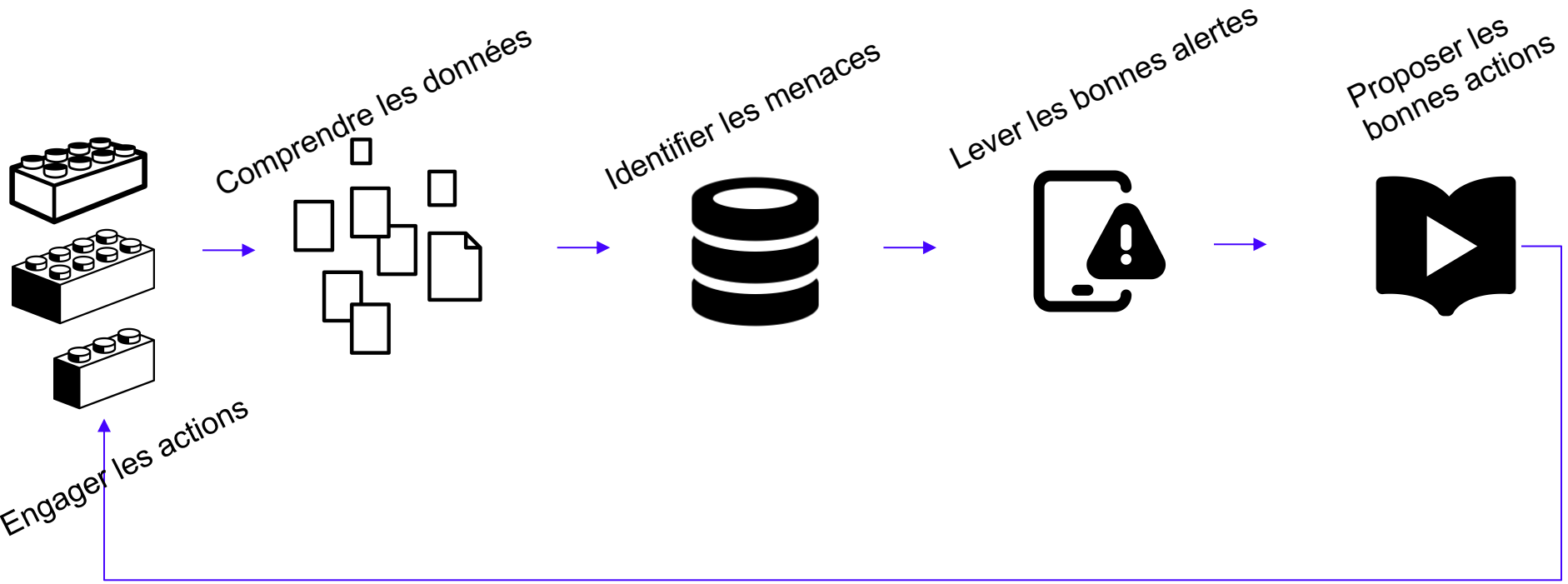
Agenda

- La réalité d’un SI et des équipes
- Les pistes
- Illustrations
- Conclusion

Monde idéal



Monde idéal


Comprendre les données
Identifier les menaces
Lever les bonnes alertes
Proposer les bonnes actions
Engager les actions

pistes #1

STIX

La threat intel et son contexte

STIX c’est quoi

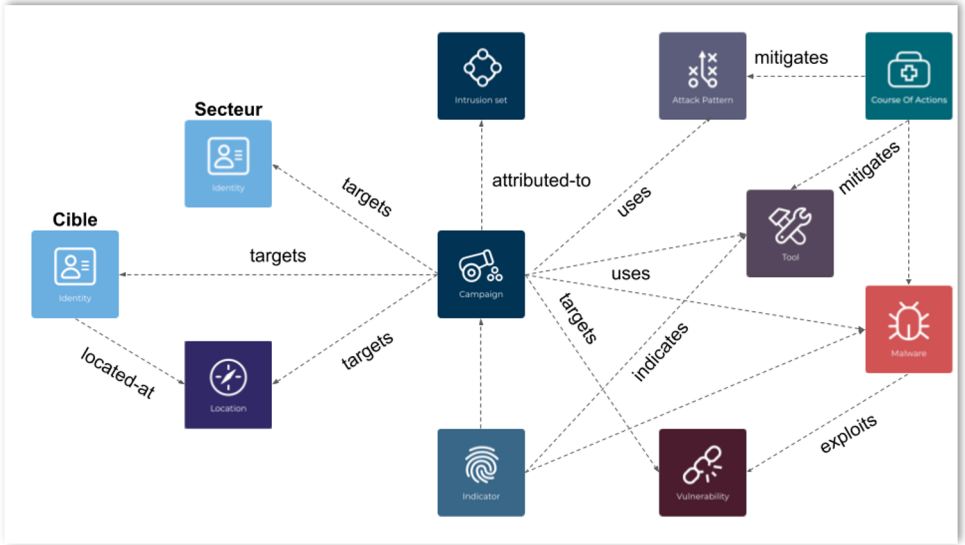
STIX est un format graphe pour modéliser la threat intelligence

Modélisation de multiples objets

- Campagne
- Mode opératoire
- Contre mesures
- Indicateurs
- Groupe d’attaquants

Modélisation des relations

- Liaison
- Observation



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

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

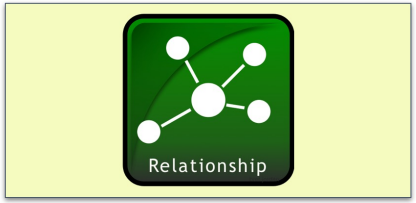
TTP Objects

Supporting Objects

Remediation Objects

Detection Objects

Les relations (SRO)



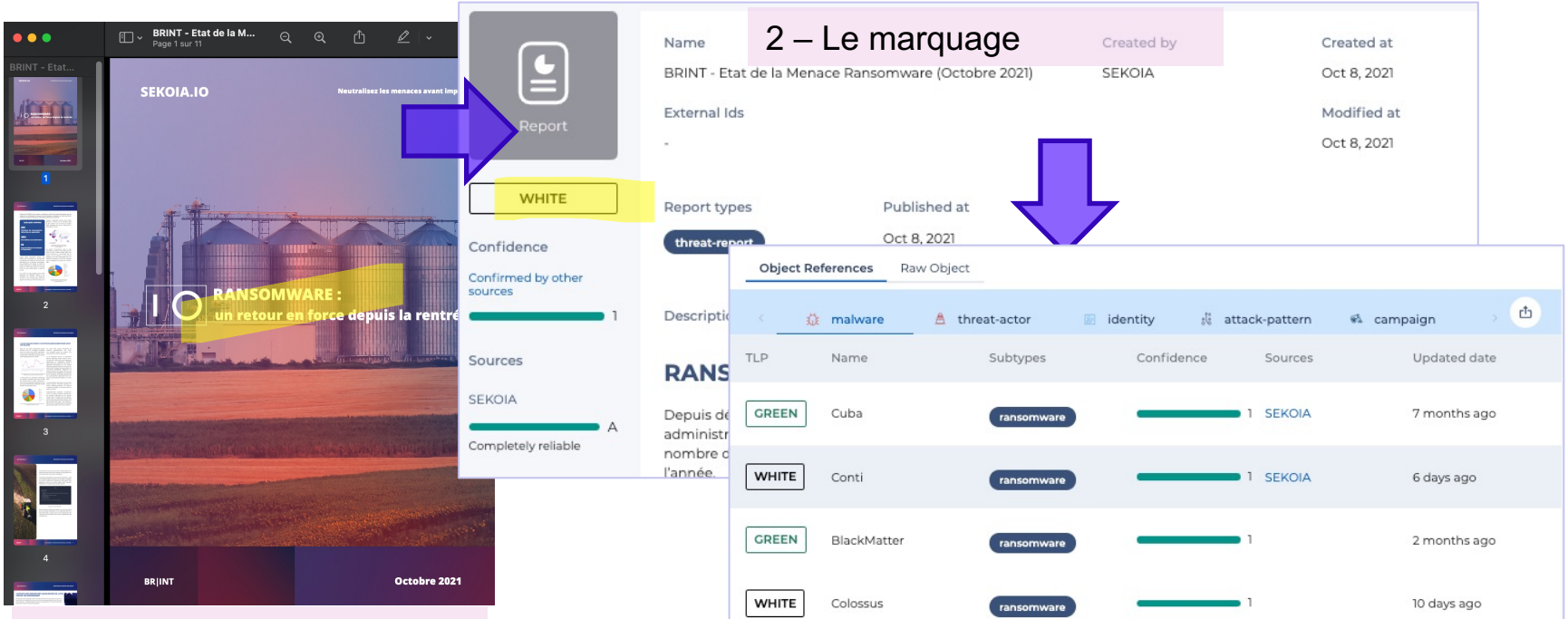
Standard Relationship Objects

Special Relationship Objects

Capitalisation de la connaissance

- 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



1 - Le rapport source

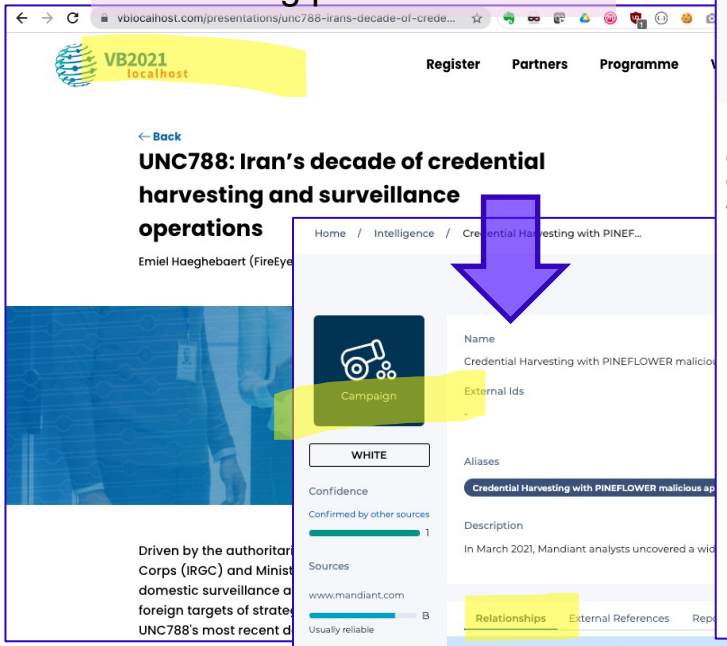
Modélisation d'informations tierce

- 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

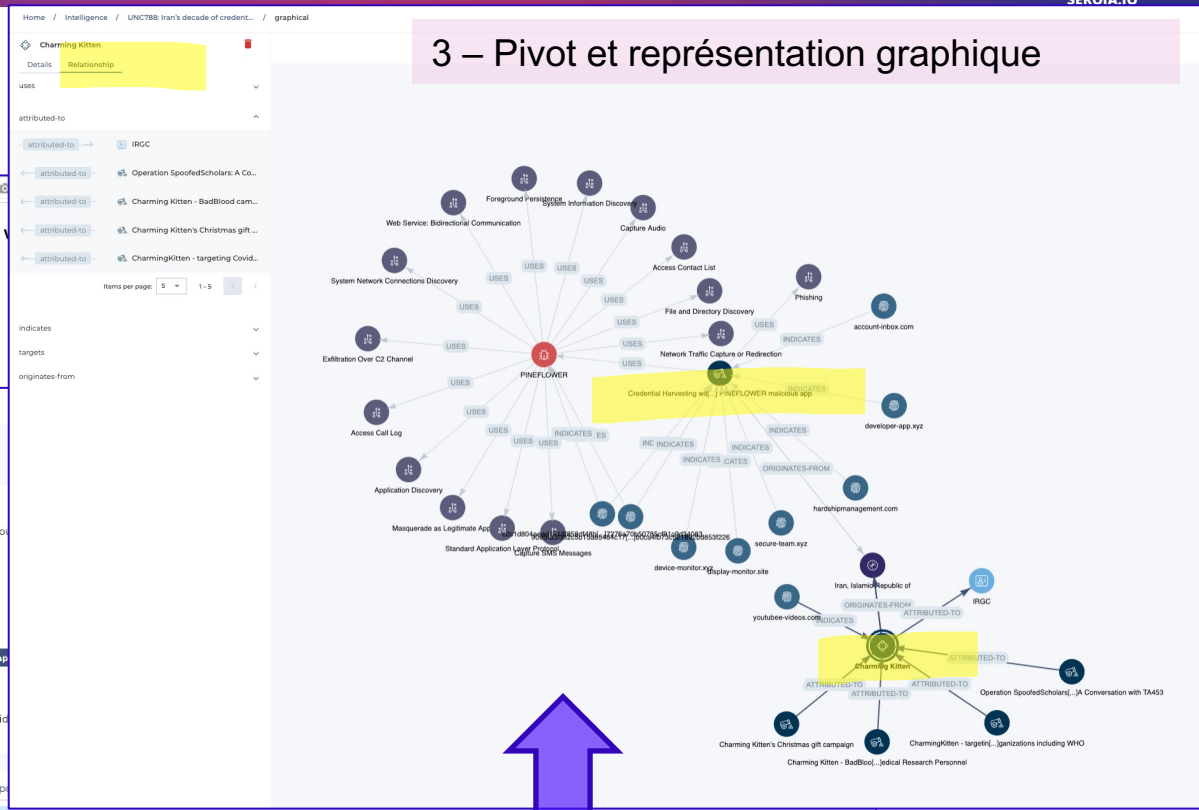
Exemple 2

1 – Un blog post



2 – Les relations

3 – Pivot et représentation graphique

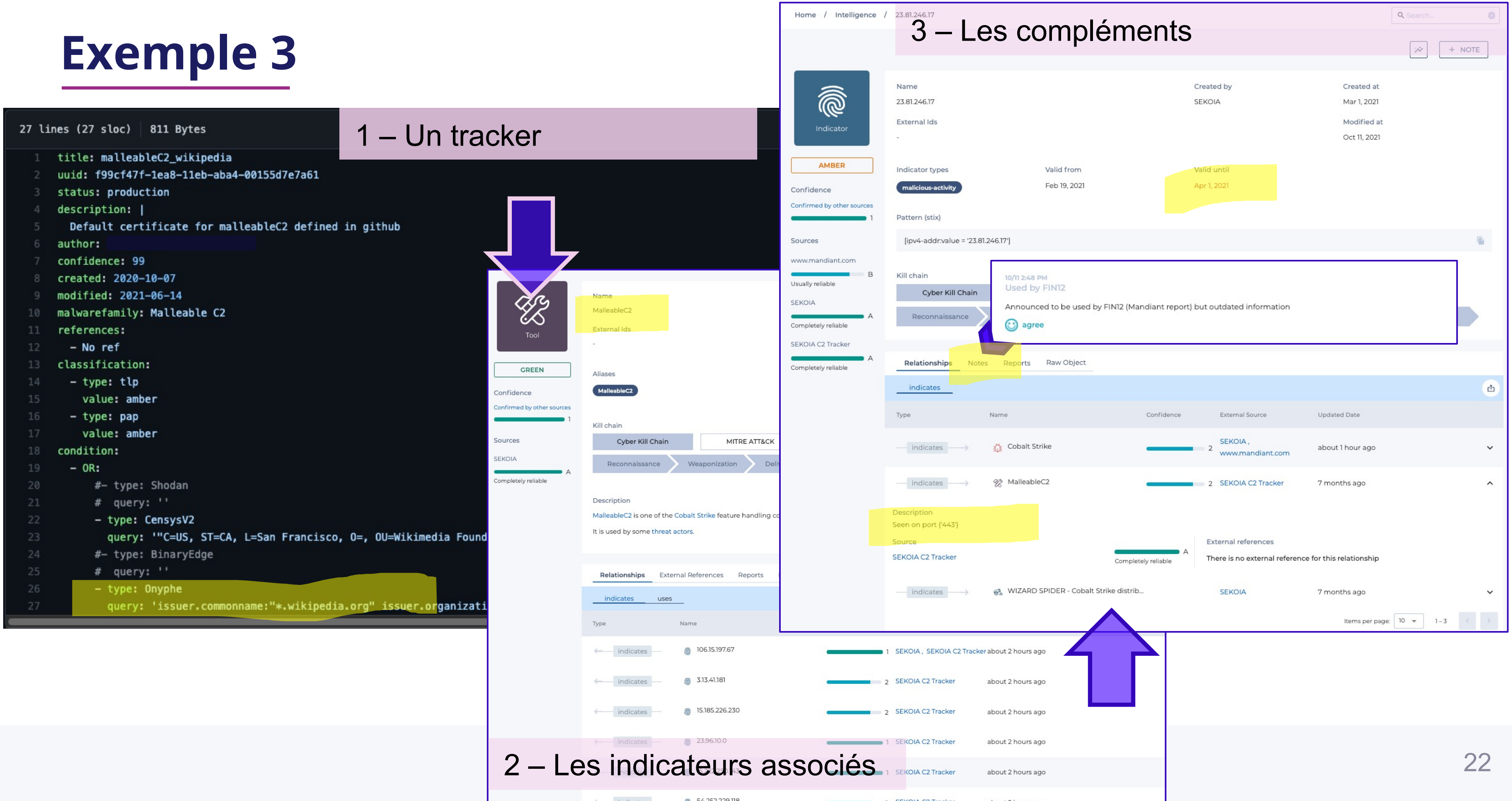


Contextualisation maximisée autour des indicateurs

- 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 3



1 – Un tracker
27 lines (27 sloc) 811 Bytes
title: malleableC2_wikipedia
uuid: f99cf47f-1ea8-11eb-aba4-00155d7e7a61
status: production
description: |
Default certificate for malleableC2 defined in github
author: [redacted]
confidence: 99
created: 2020-10-07
modified: 2021-06-14
malwarefamily: Malleable C2
references:
- No ref
classification:
- type: tlp
value: amber
- type: pap
value: amber
condition:
- OR:
#- type: Shodan
query: ''
- type: CensysV2
query: '"C=US, ST=CA, L=San Francisco, O=, OU=Wikimedia Found
#- type: BinaryEdge
query: ''
- type: Onyphe
query: 'issuer.commonname:"*.wikipedia.org" issuer.organizati
2 – Les indicateurs associés
Tool
GREEN
Confidence
Confirmed by other sources
Sources
SEKOIA
Completely reliable
Name
MalleableC2
External Ids
Aliases
MalleableC2
Kill chain
Cyber Kill Chain
MITRE ATT&CK
Reconnaissance
Weaponization
Description
MalleableC2 is one of the Cobalt Strike feature handling co
It is used by some threat actors.
Relationships
External References
Reports
indicates
uses
Type
Name
indicates 106.15.197.67 SEKOIA, SEKOIA C2 Tracker about 2 hours ago
indicates 3.13.41.181 SEKOIA C2 Tracker about 2 hours ago
indicates 15.185.226.230 SEKOIA C2 Tracker about 2 hours ago
indicates 23.96.10.0 SEKOIA C2 Tracker about 2 hours ago
SEKOIA C2 Tracker about 2 hours ago
3 – Les compléments
Home / Intelligence / 23.81.246.17
NOTE
Indicator
AMBER
Confidence
Confirmed by other sources
Sources
www.mandiant.com
Usually reliable
SEKOIA
Completely reliable
SEKOIA C2 Tracker
Completely reliable
Name
23.81.246.17
External Ids
Created by
SEKOIA
Created at
Mar 1, 2021
Modified at
Oct 11, 2021
Indicator types
malicious-activity
Valid from
Feb 19, 2021
Valid until
Apr 1, 2021
Pattern (stix)
[ipv4-addr:value = '23.81.246.17']
Kill chain
Cyber Kill Chain
Reconnaissance
10/11 2:48 PM
Used by FIN12
Announced to be used by FIN12 (Mandiant report) but outdated information
agree
Relationships
Notes
Reports
Raw Object
indicates
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
Description
Seen on port ('443')
Source
SEKOIA C2 Tracker
Completely reliable
External references
There is no external reference for this relationship
indicates WIZARD SPIDER - Cobalt Strike distrib... SEKOIA 7 months ago
Items per page: 10
1 – 3

pistes

#2

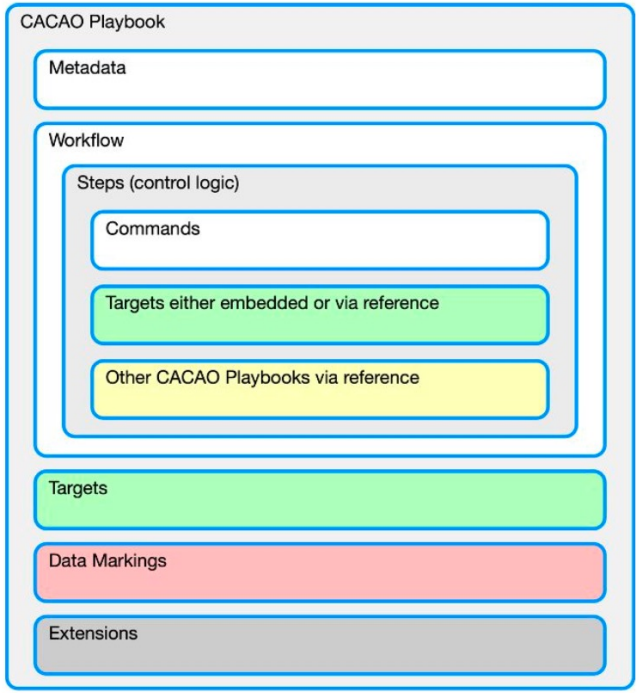
CACAO

Des plans d’actions génériques

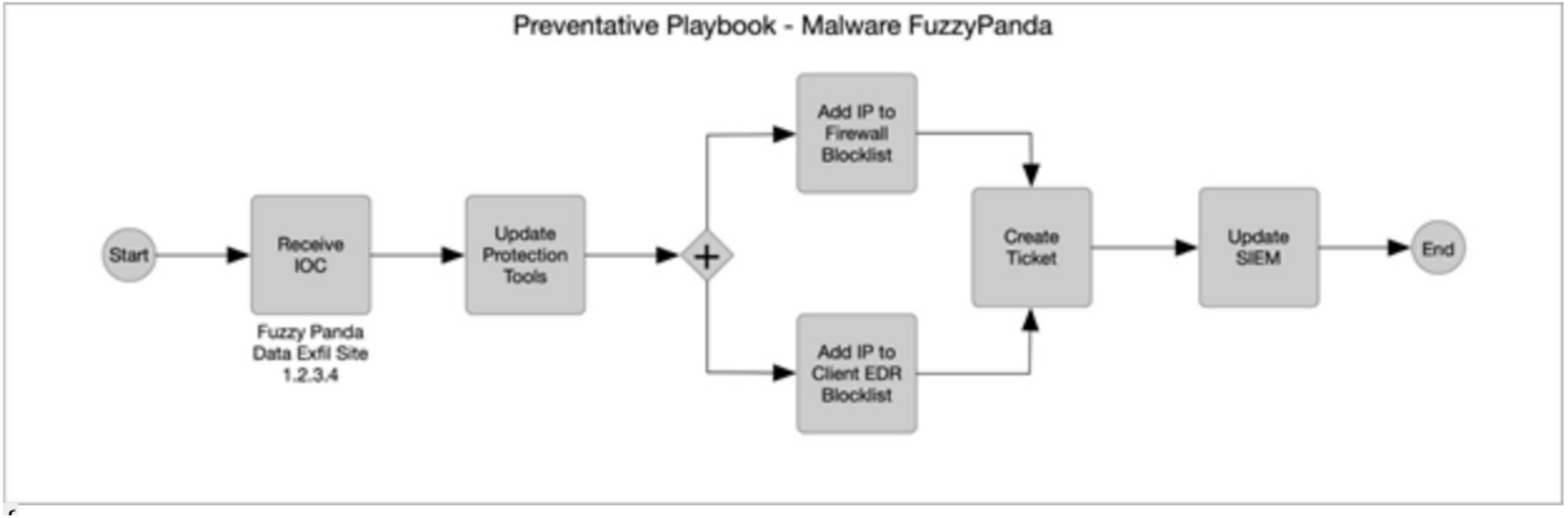
CACAO : c’est quoi ?

Langage de Workflow pour orchestrer les actions

- Un séquencement
- Des actions à suivre
- Des actionneurs pouvant recevoir les ordres



CACAO : illustration



pistes #3

OpenC2

Des actions automatisables

OpenC2 : c’est quoi ?

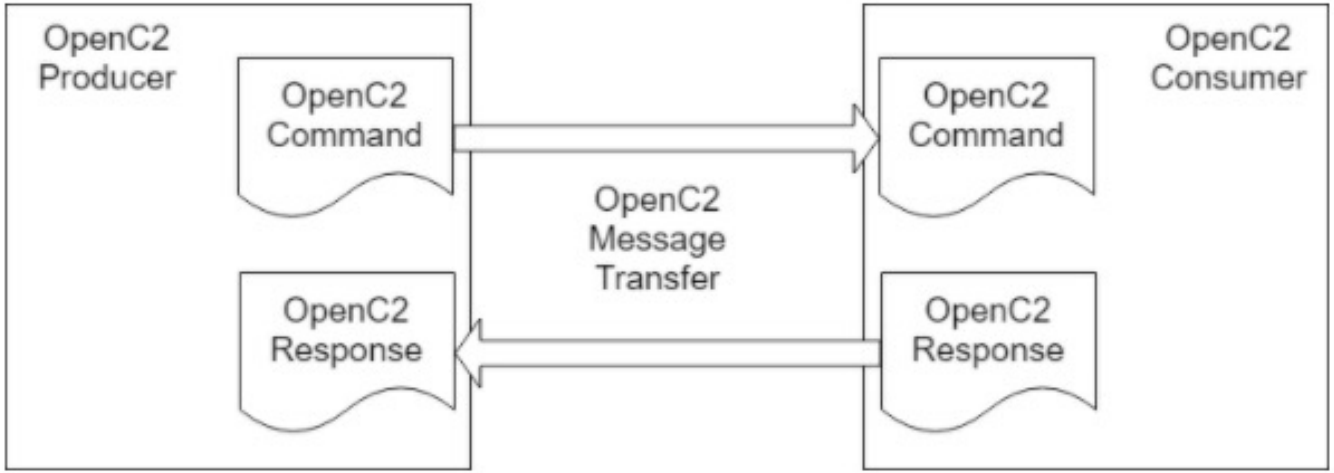
Langage pour automatiser les actions sur les composants du SI

- Un ordre
- Une cible
- Eventuellement un exécutant

OpenC2 : illustration

```
{
    "action": "deny",
    "target": {
        "file": {
            "hashes": {
                "md5": "d41d8cd98f00b204e9800998ecf8427e"
            }
        }
    }
}
```

OpenC2 : Commandes et réponses



SEKOIA.IO

Agenda

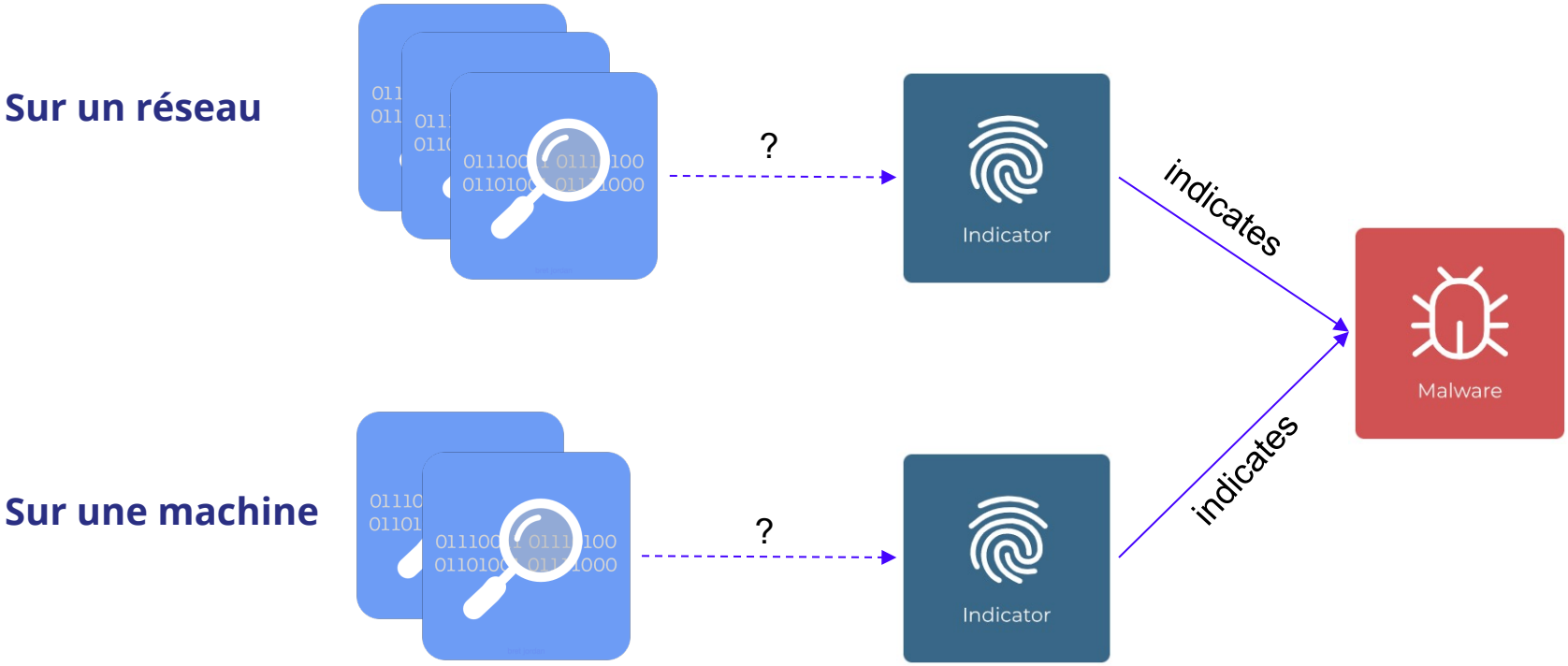
- La réalité d’un SI et des équipes
- Les pistes
- Illustrations
- Conclusion

illustrations
#1

Proposer les meilleures stratégies grâce au renseignement

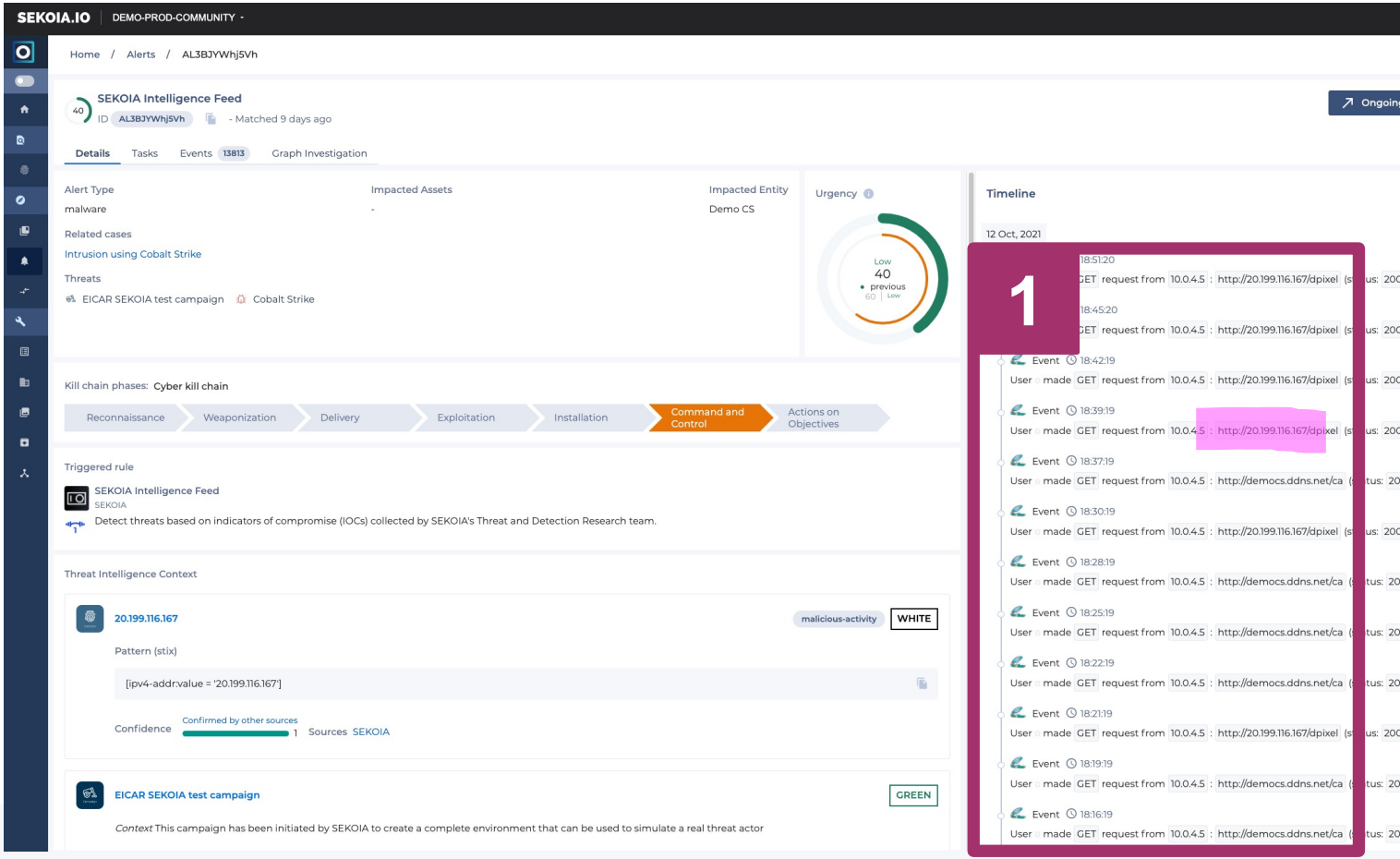
Pivot automatisés via STIX

Les pivots intéressants dans une alerte



Exemple

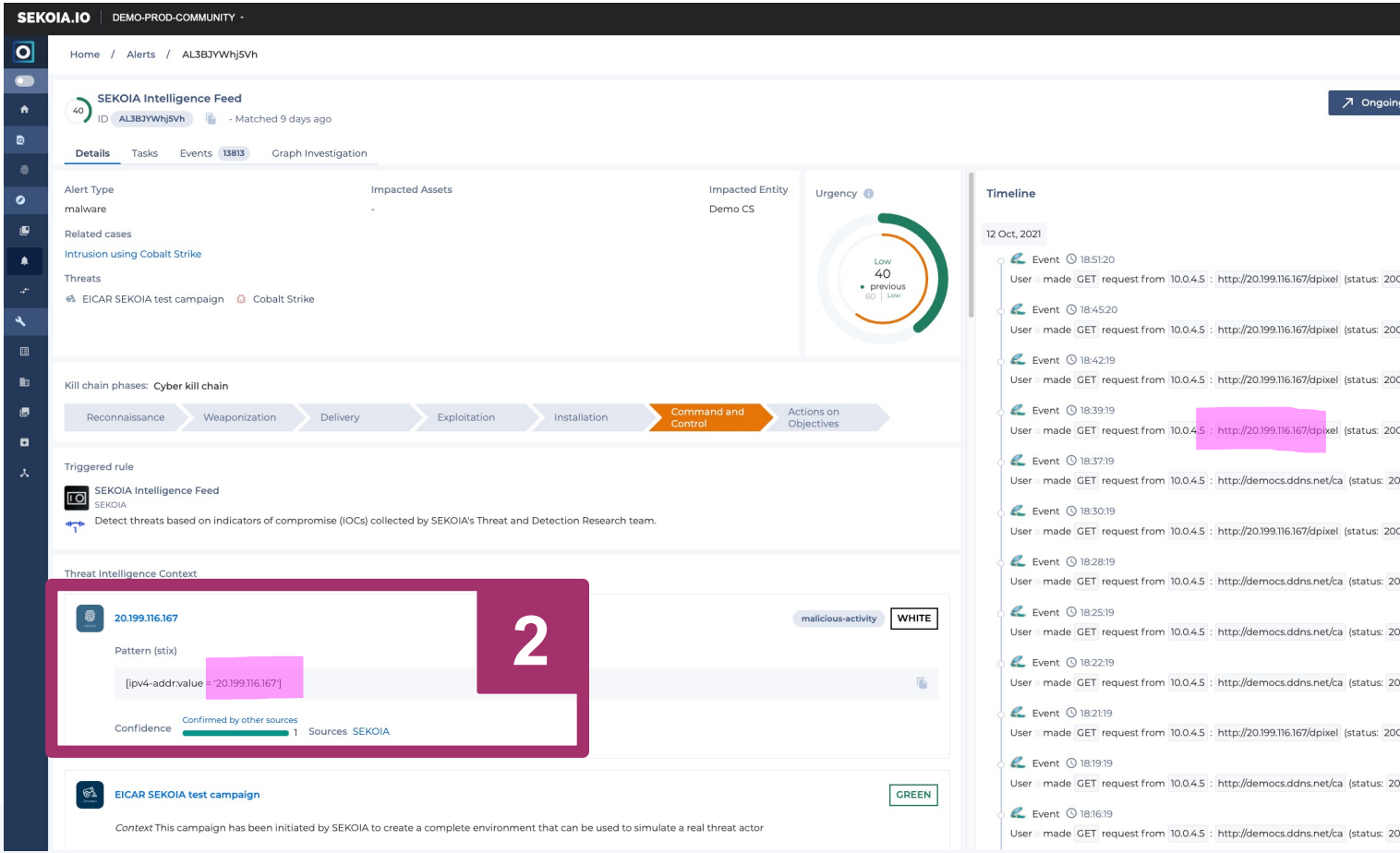
1 – Des evénements



Exemple

1 – Des evénements

2 – Repérage d'un indicateur dans le contenu

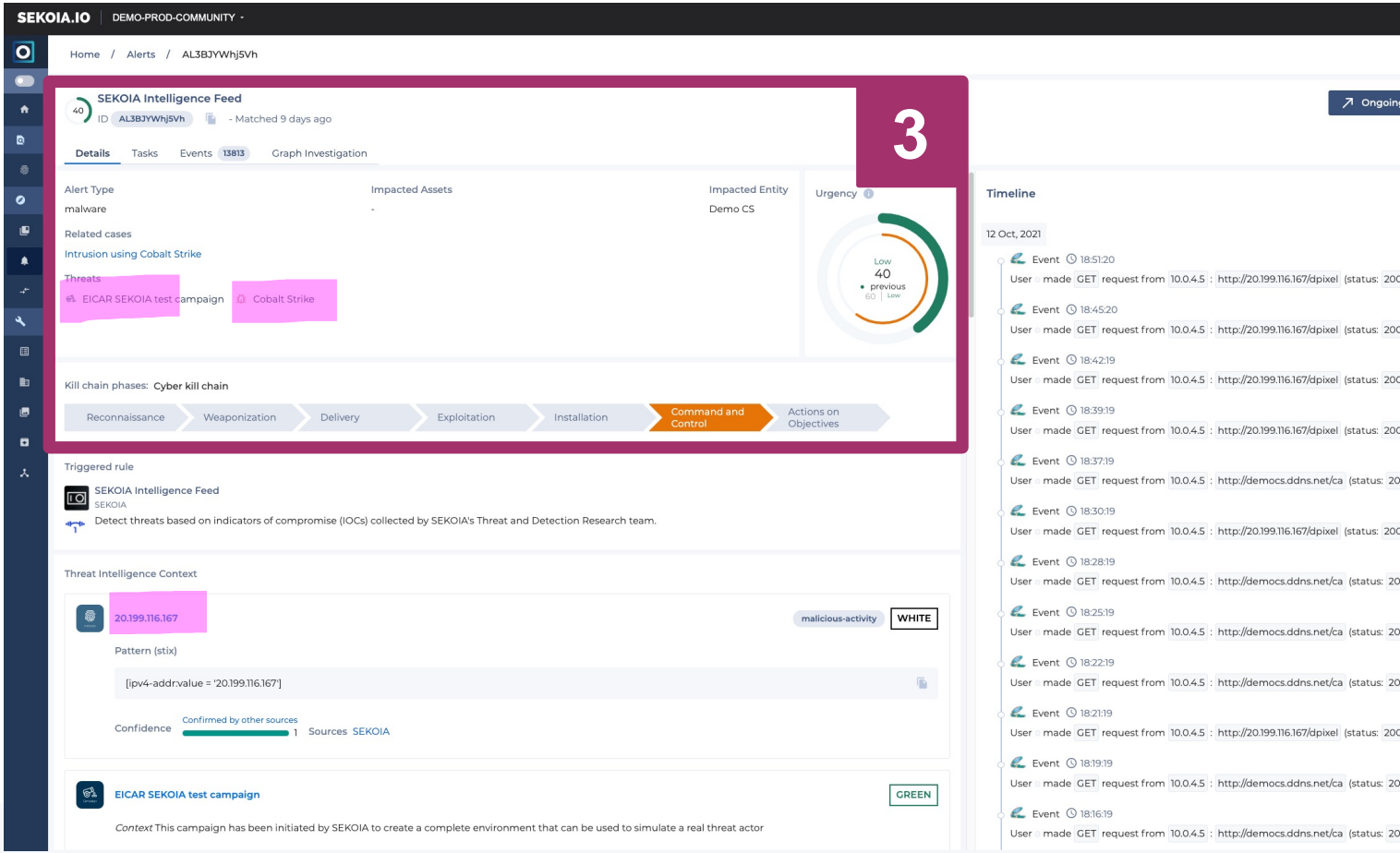


Exemple

1 – Des evénements

2 – Repérage d'un indicateur dans le contenu

3 – Génération d'une alerte



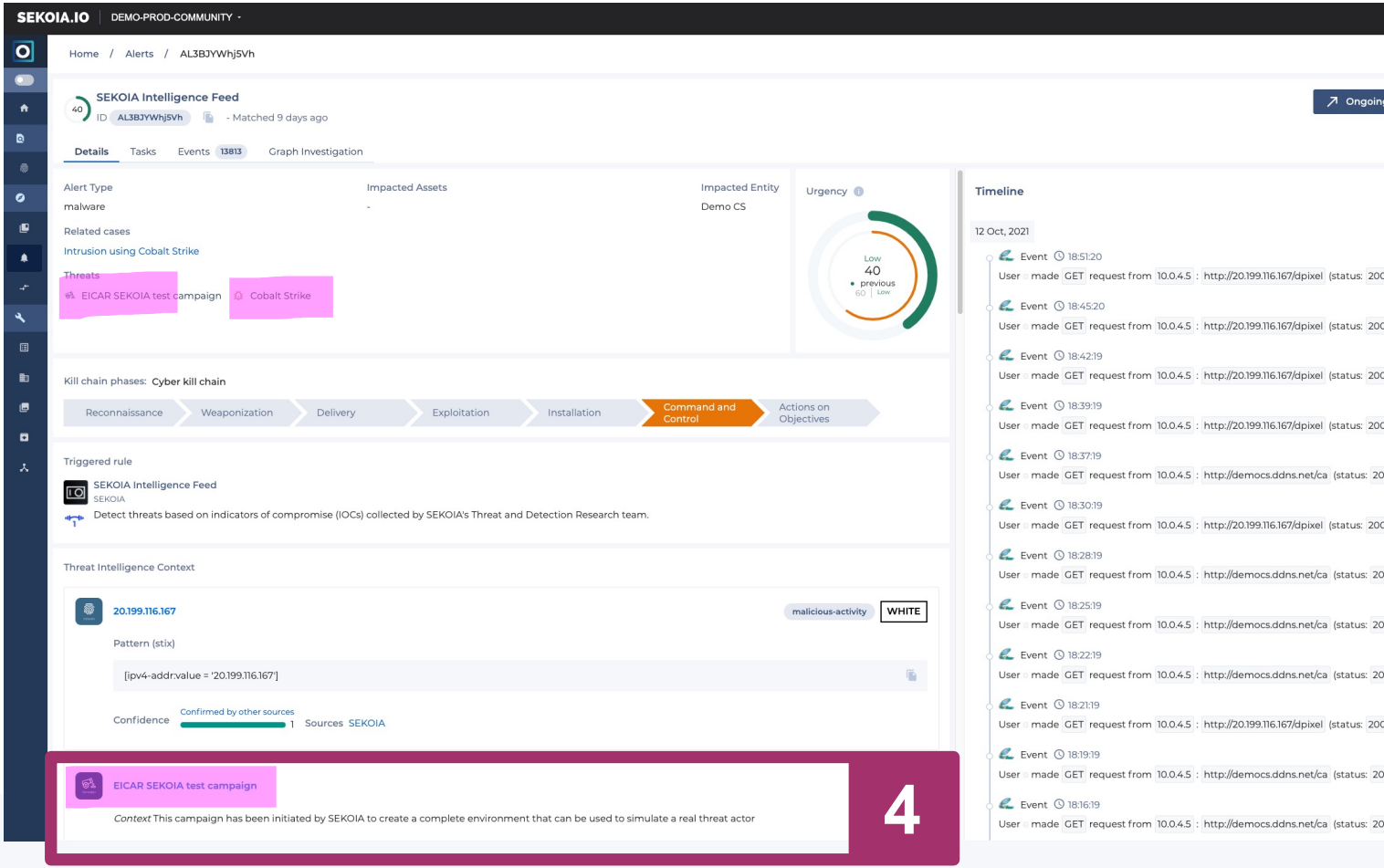
Exemple

1 – Des evénements

2 – Repérage d'un indicateur dans le contenu

3 – Génération d'une alerte

4 – Utilisation des pivots pour créer du contexte



Exemple

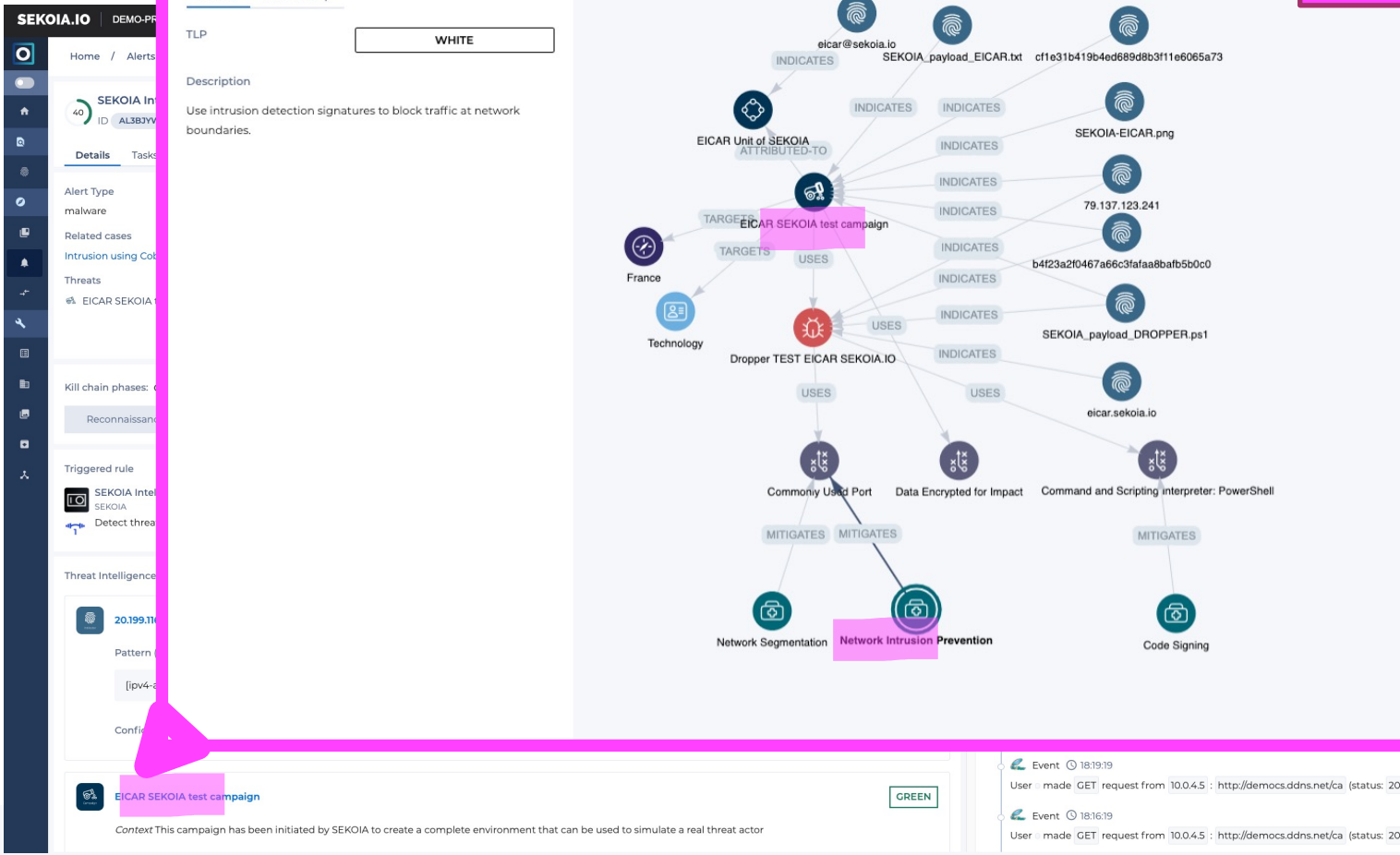
1 – Des evénements

2 – Repérage d’un indicateur dans le contenu

3 – Génération d’une alerte

4 – Utilisation des pivots pour créer du contexte

5 – Disposer de stratégies de réaction



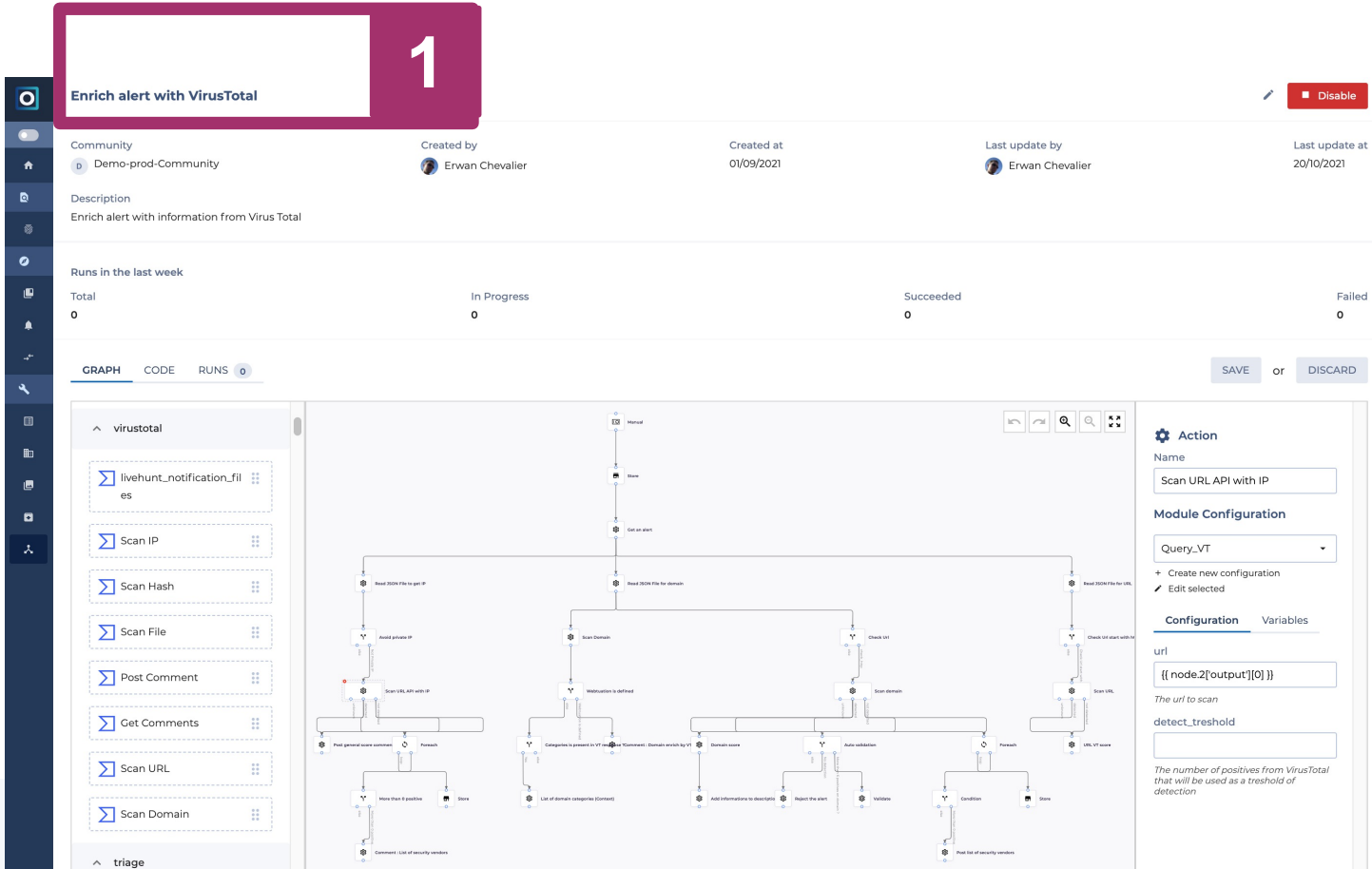
illustrations
#2

Orchestrer ce qu'il est bien de faire

Selon ce que l'on sait/peut faire

~CACAO en action

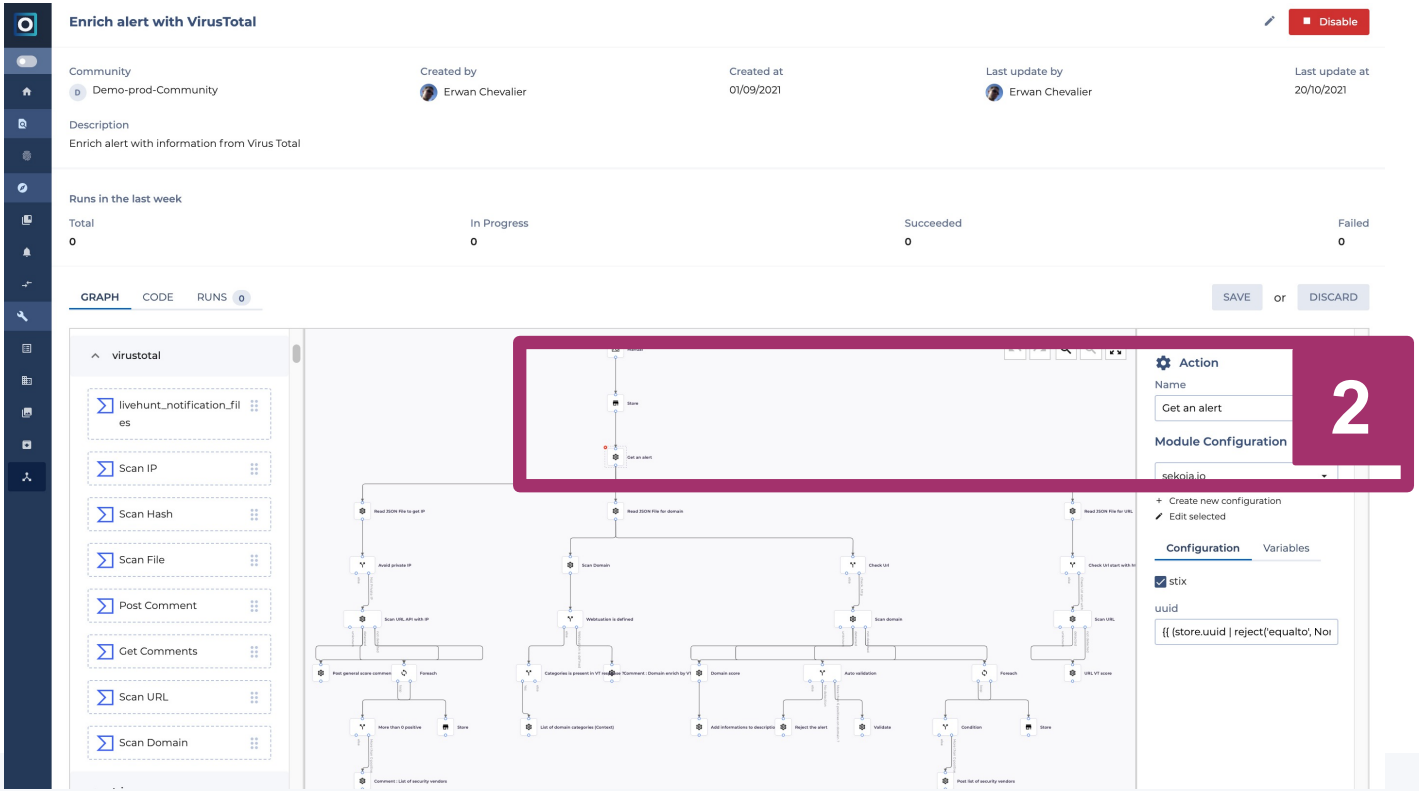
1 – Un enrichisseur VT



~CACAO en action

1 – Un enrichisseur VT

2 – Prise en compte du contexte de l'alerte

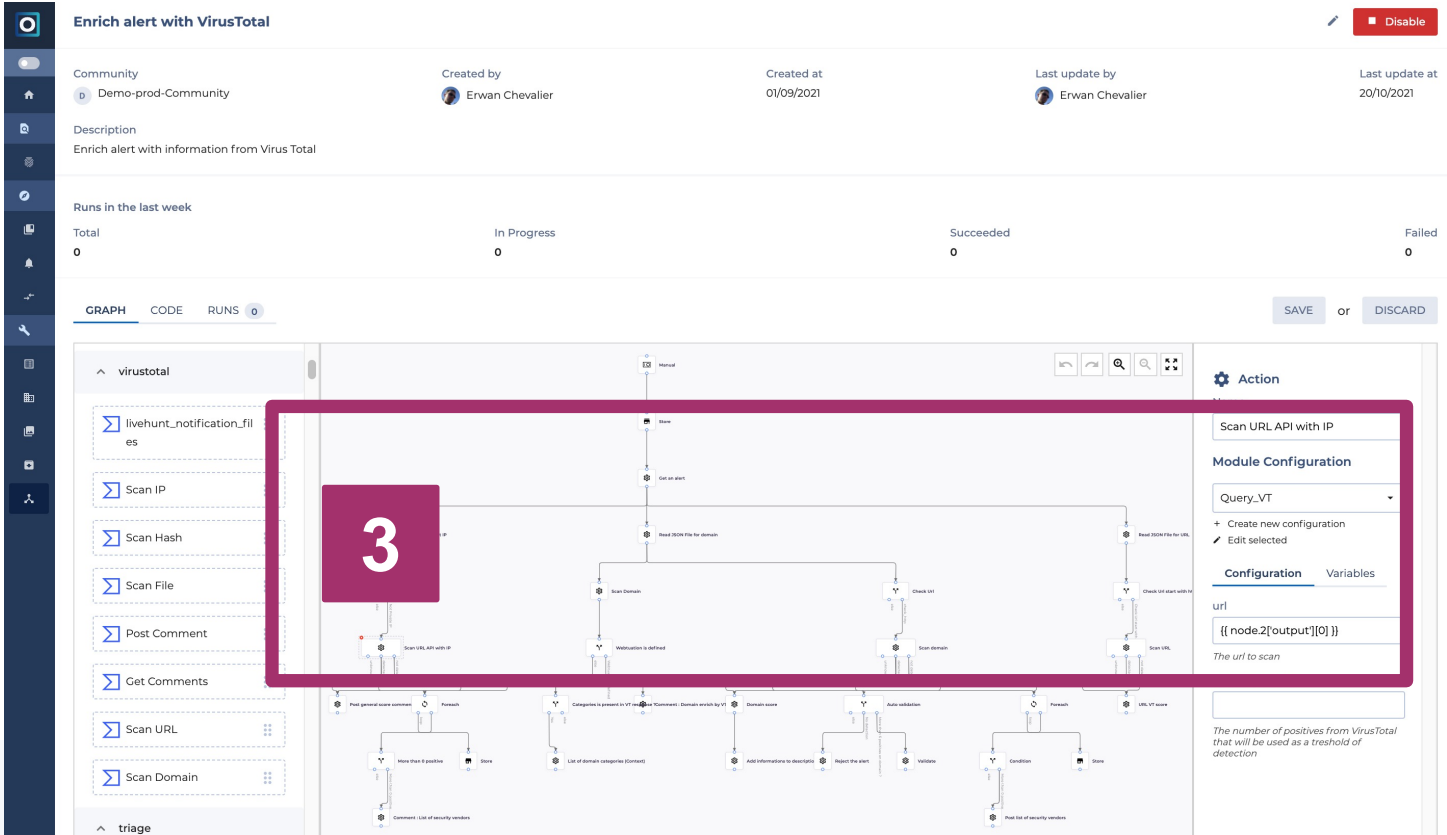


~CACAO en action

1 – Un enrichisseur VT

2 – Prise en compte du contexte de l'alerte

3 – Différents calls VT selon le contenu



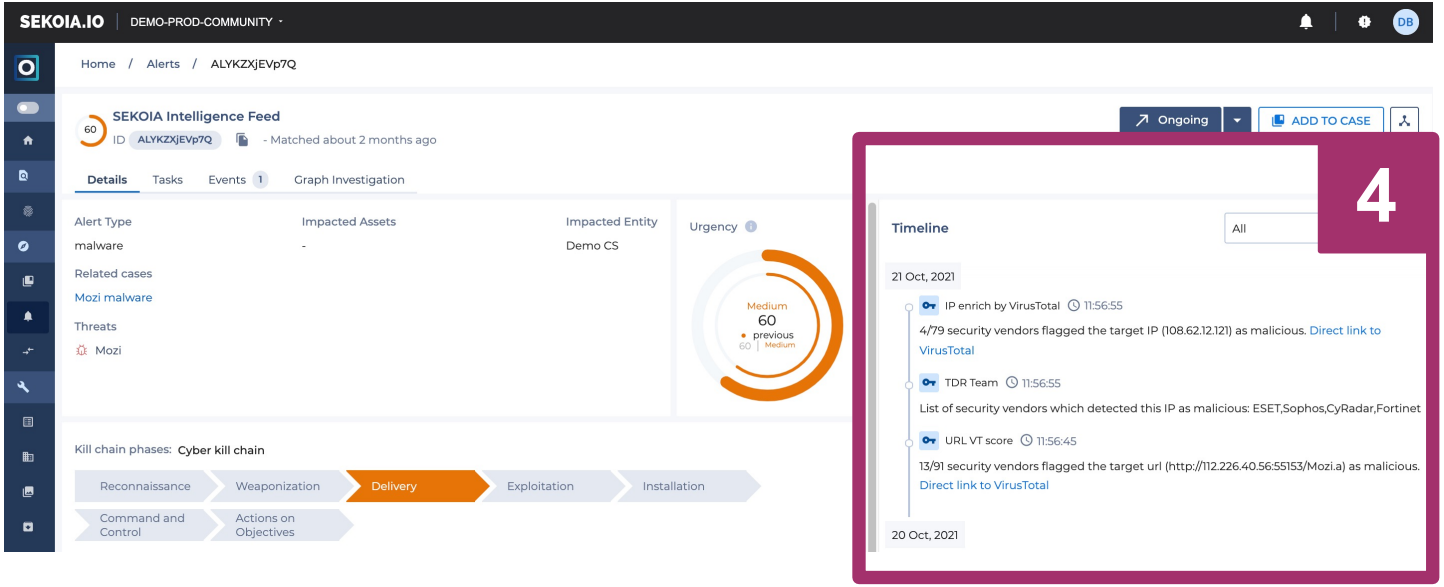
~CACAO en action

1 – Un enrichisseur VT

2 – Prise en compte du contexte de l'alerte

3 – Différents calls VT selon le contenu

4 – Consolidation des résultats dans le commentaire via hook de l'alerte



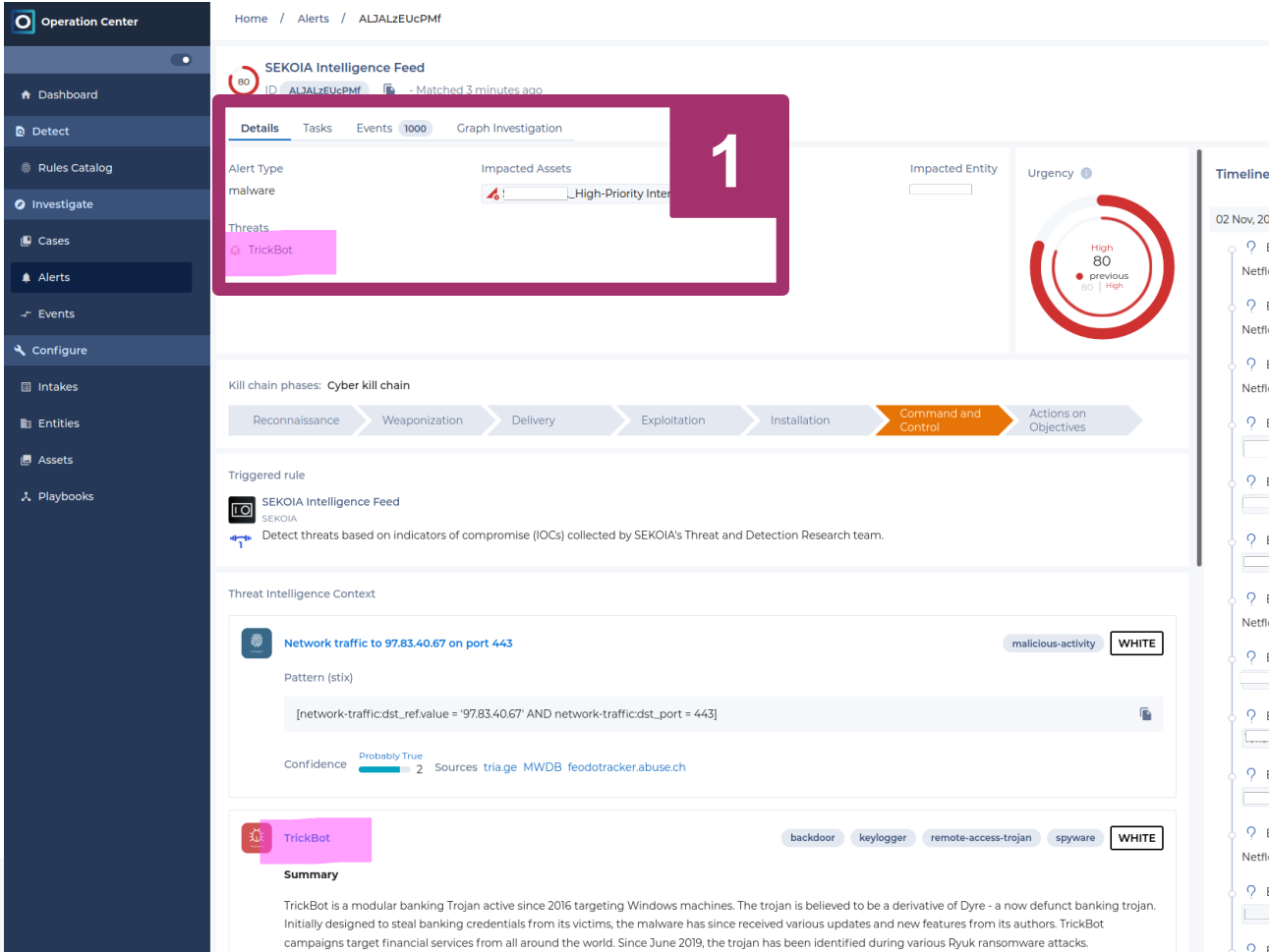
illustrations
#3

Automatiser

Quand c’est possible

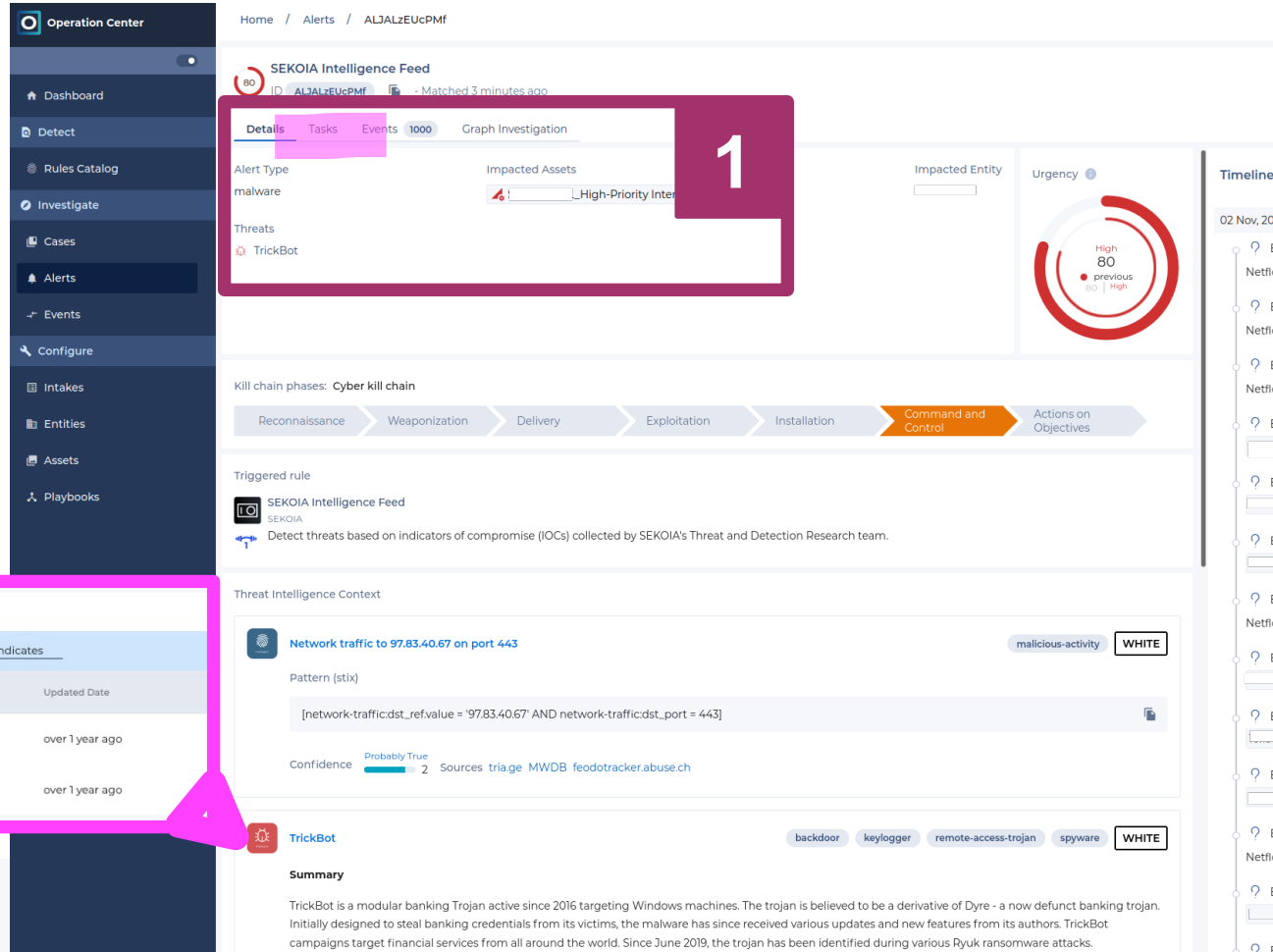
OpenC2 en action

0 – Récupérer le contexte de l'alerte



OpenC2 en action

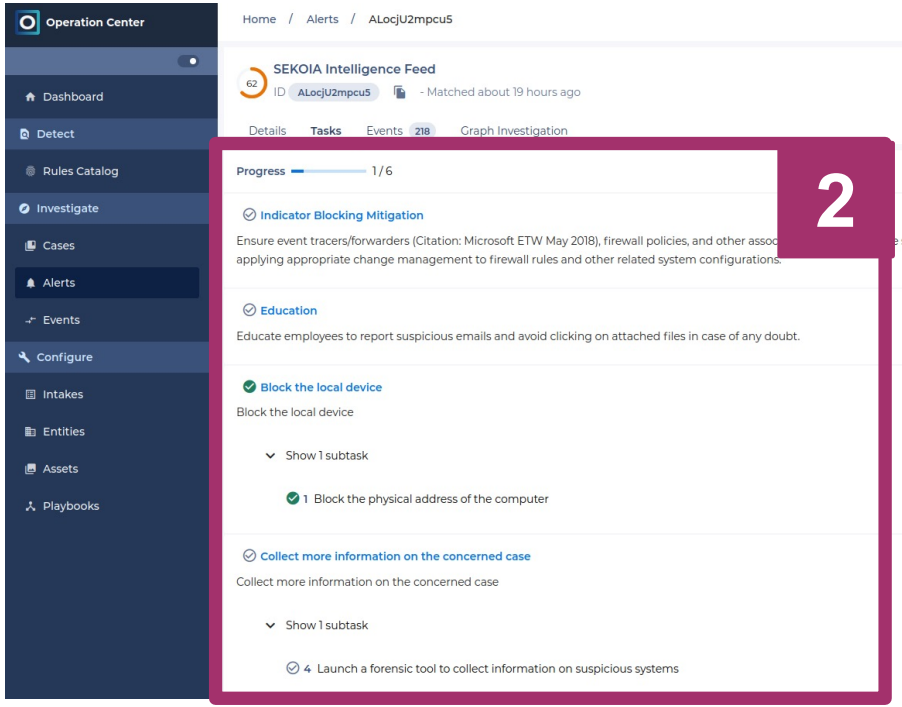
1 – Selon le contexte de l'alerte, identification de contre-mesure



OpenC2 en action

1 – Selon le contexte de l'alerte, identification de contre-mesure

2 – batterie d'actions possibles

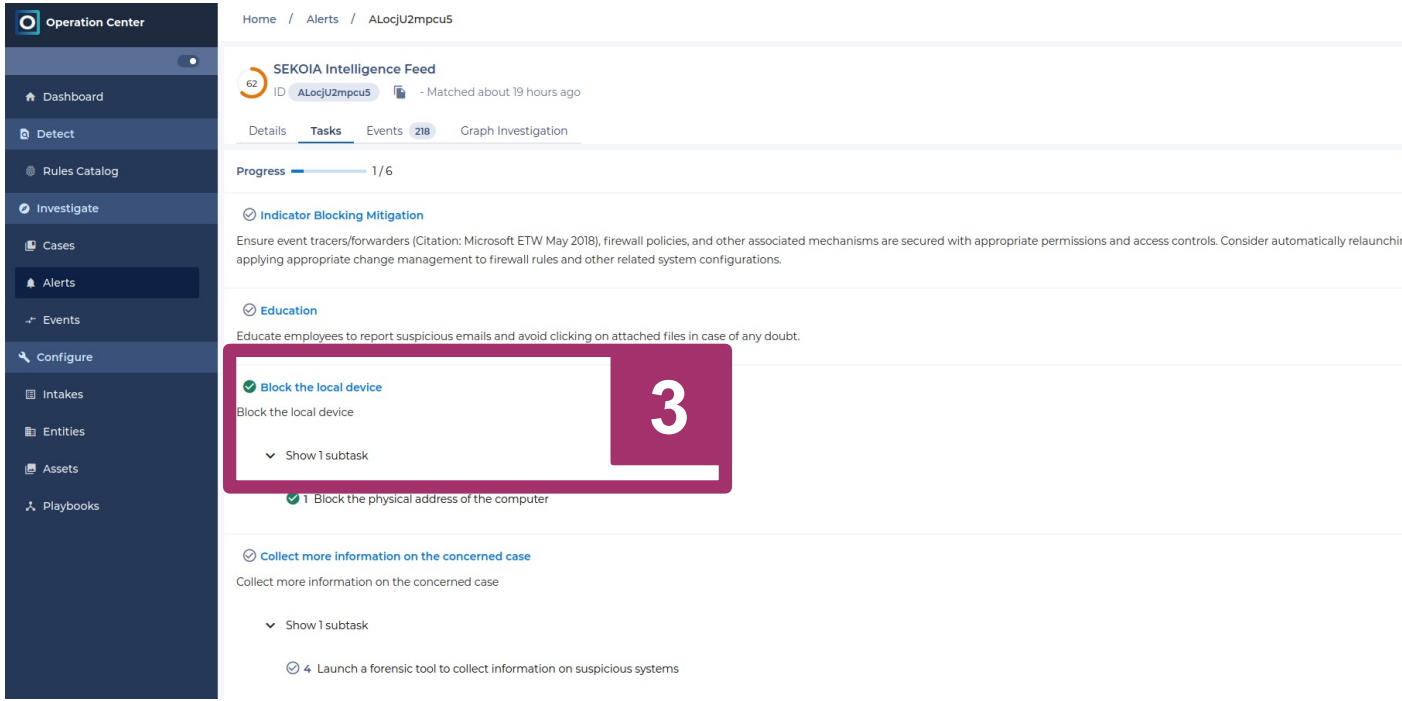


OpenC2 en action

1 – Selon le contexte de l'alerte, proposition de contre-mesure

2 – batterie d'actions possibles

3 – Une action atomique OpenC2



OpenC2 en action

1 – Selon le contexte de l'alerte, proposition de contre-mesure

2 – batterie d'actions possibles

3 – Une action atomique OpenC2

4 – Consommation par un partenaire

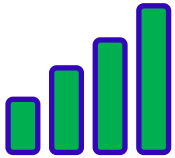
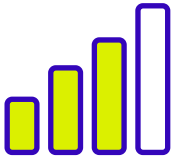
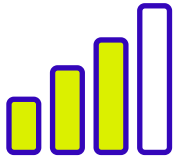
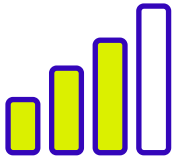
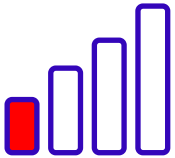
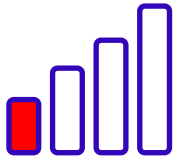
```
[
  {
    "name": "Block the local device",
    "description": "Block the local device",
    "countermeasures": [
      {
        "type": "openc2",
        "description": "Block the physical address of the computer",
        "object": {
          "action": "deny",
          "target": {
            "mac_addr": "@mac_addr"
          }
        },
        "name": "1"
      }
    ],
    "relevance": 60
  }
]
```

SEKOIA.IO

Agenda

- La réalité d’un SI et des équipes
- Les pistes
- Illustrations
- Conclusion

Niveaux de maturité

	STIX	CACAO	OpenC2
Maturité			
Usage			

La suite

Conclusion

- Preuves de concepts efficaces
- Route encore longue

Call to arms

- Les mastodontes ont leur écosystème « fermés »
- L'objectif reste d'enfermer les clients dans une logique propriétaire
  - `Vendeurs : rendez vous compatibles avec OpenC2`
  - `Acheteurs : exigez cette fonctionnalité dans vos produits`

SEKOIA.IO

Neutralisez les menaces avant impact

www.sekoia.io