



**SEKOIA.IO**

# Automatisation de la cyber sécurité

OSSIR  
14/12/2021

[david.bizeul@sekoia.io](mailto:david.bizeul@sekoia.io)

# Automatisation

”

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

# SEKOIA.IO



SEKŌIA



Accompagnement opérationnel  
CERT (Red, Purple, Blue Teams)

Renseignement CTI  
Plateforme XDR



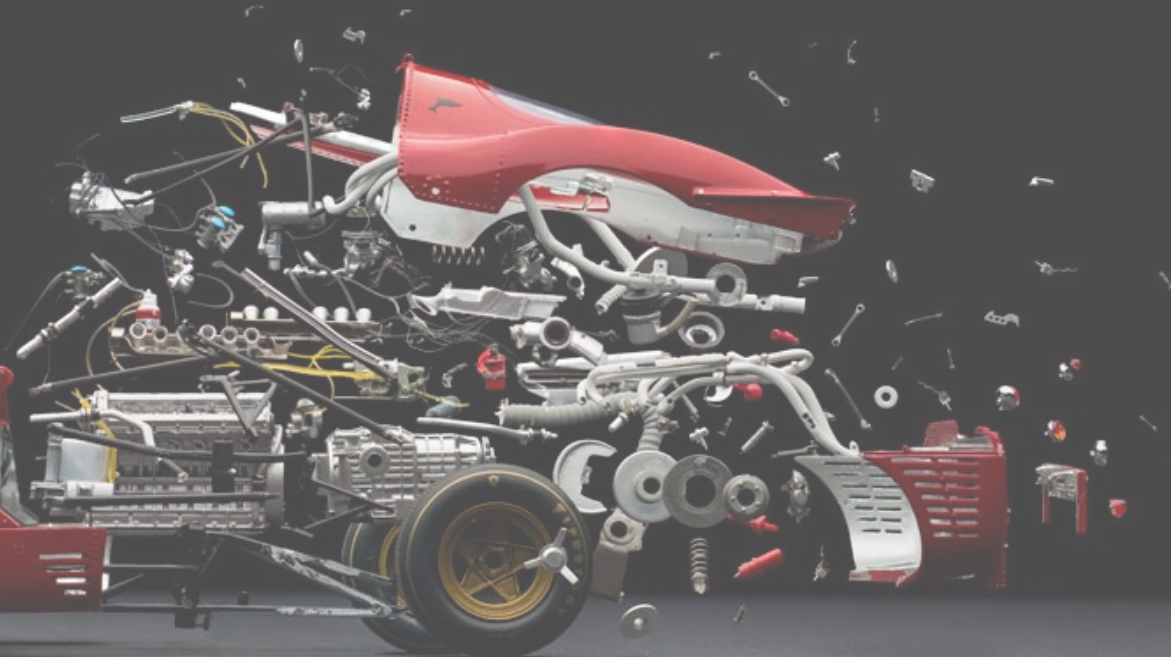
**SEKOIA.IO**

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

## La situation



## Réalité du SI

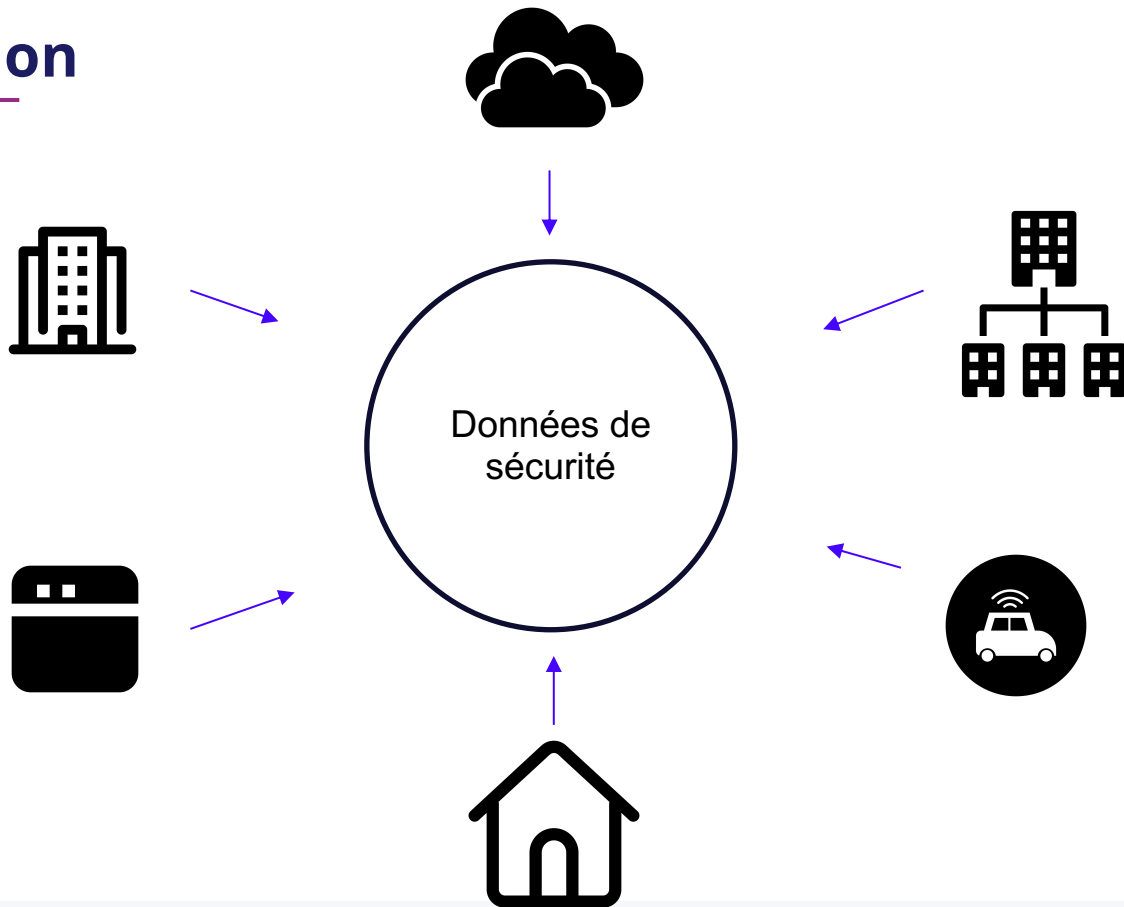


# La situation

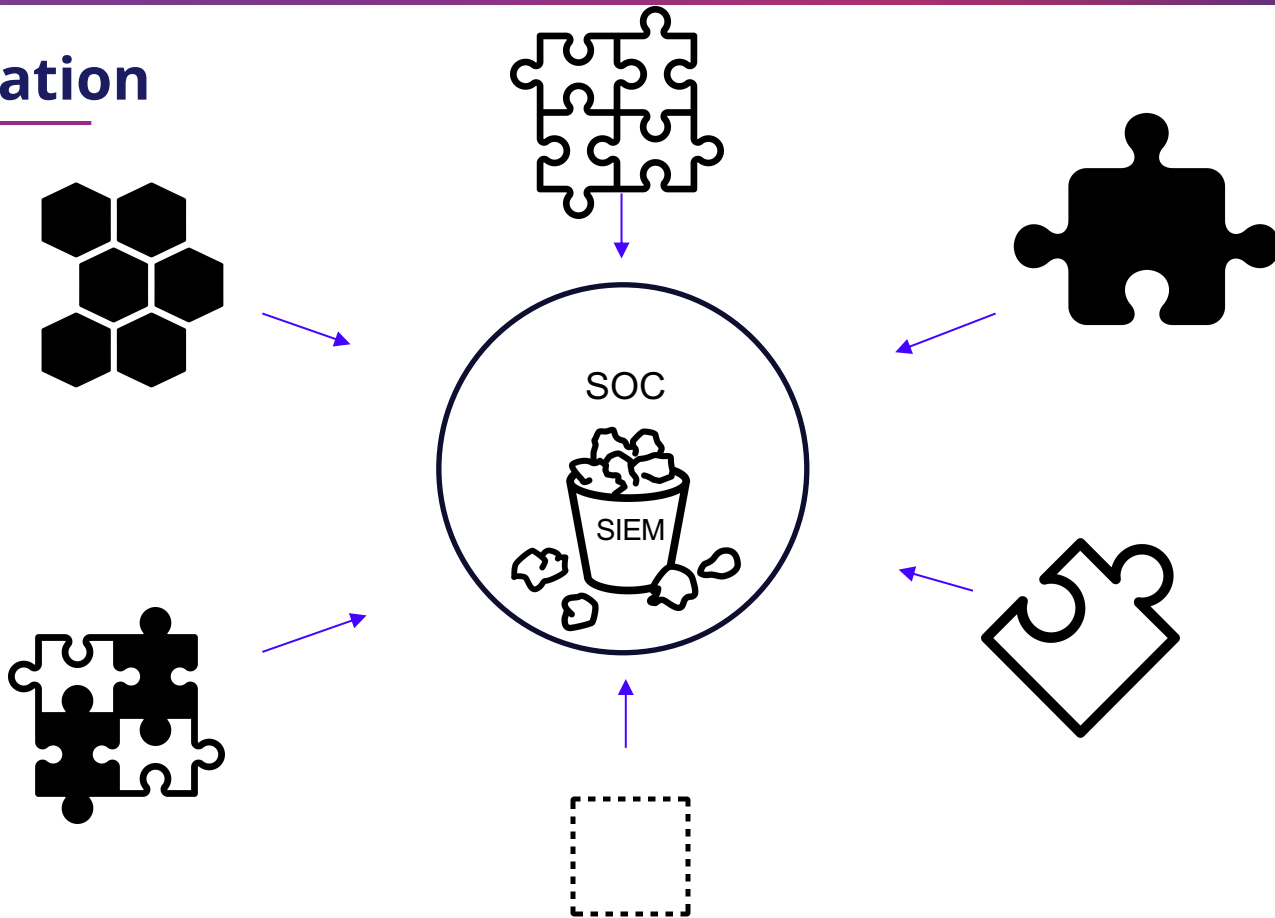
An exploded view of a red Ferrari sports car, showing the engine, chassis, and various components like wheels, suspension, and body panels. The car is shown in a disassembled state, with parts floating around it. The text "Couche de sécurité nécessaire" is overlaid on the image.

Couche de sécurité nécessaire

# La situation



## La situation



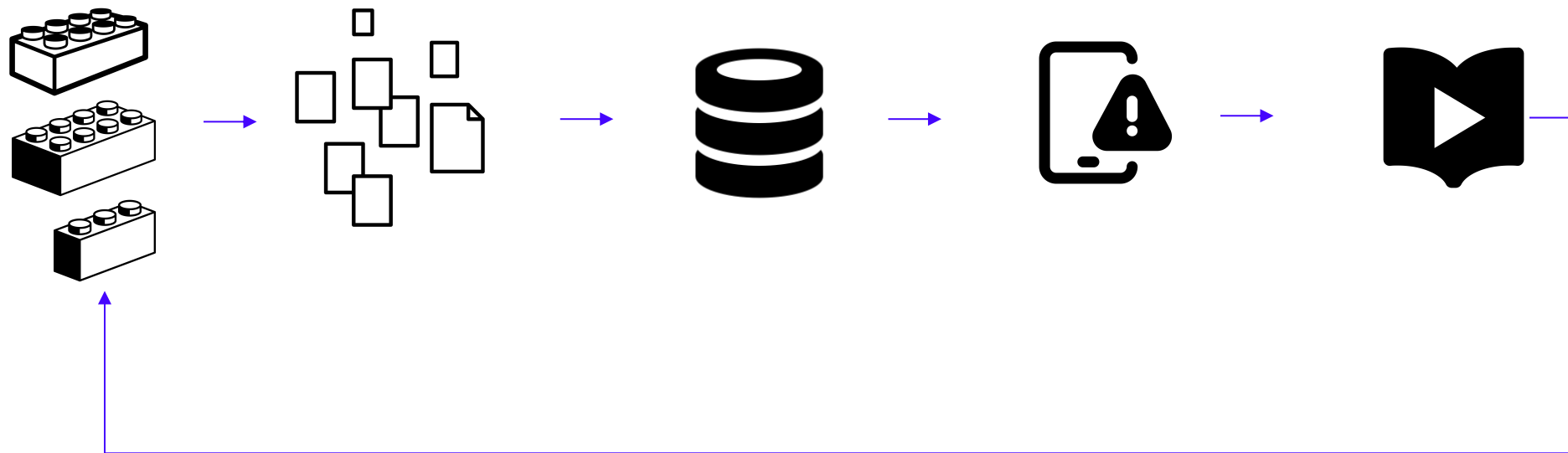




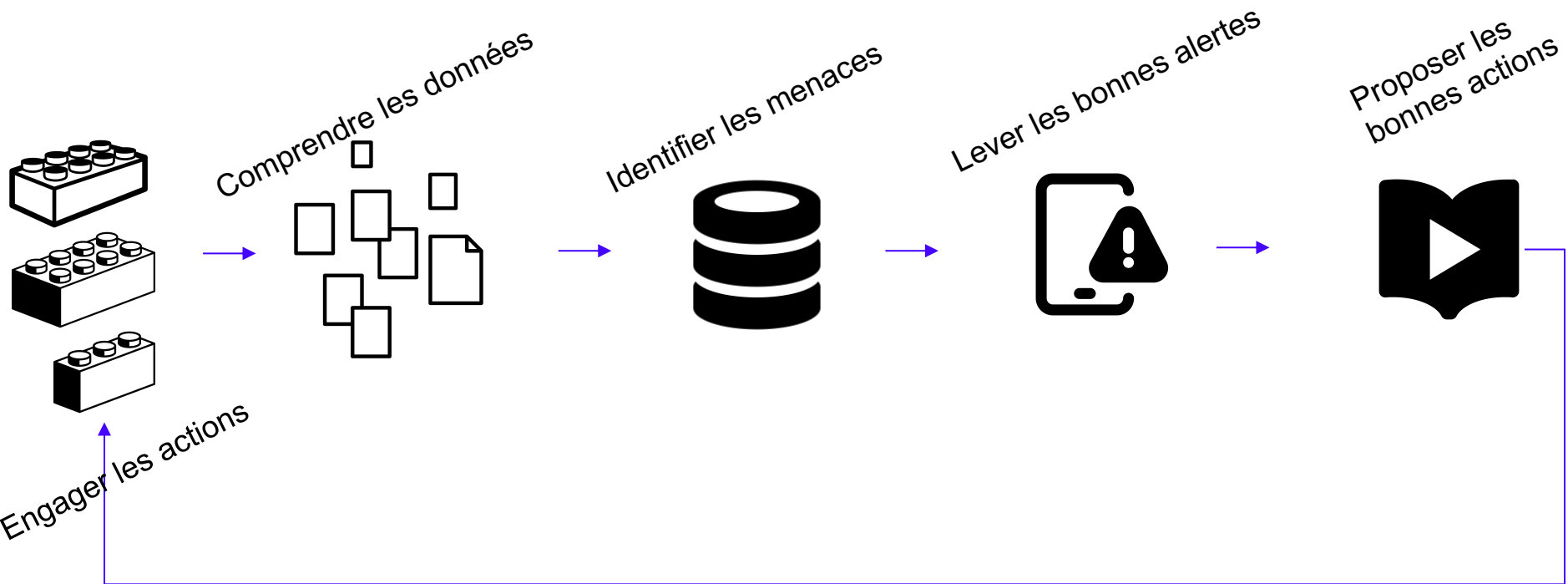
**SEKOIA.IO**

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

# Monde idéal



# Monde idéal



# pistes **#1**

STIX

La threat intel et son contexte

# STIX c'est quoi

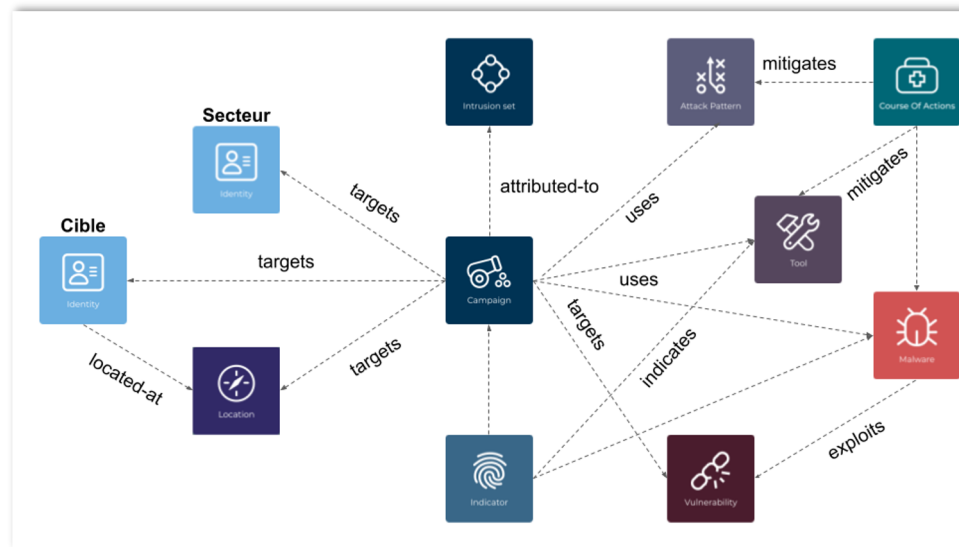
## STIX est un format graphe pour modéliser la threat intelligence

### Modélisation de multiples objets

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

### Modélisation des relations

- Liaison
- Observation

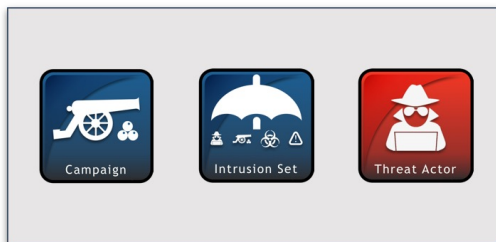


Format lisible par les machines, graphes compréhensibles par l'humain

# 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-aalc-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"
      }
    }
  ]
}
```

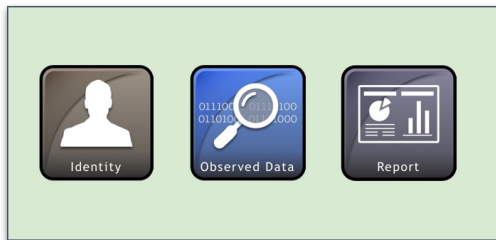
# Les Objets (SDOs) importants



**Adversary Objects**



**TTP Objects**



**Supporting Objects**

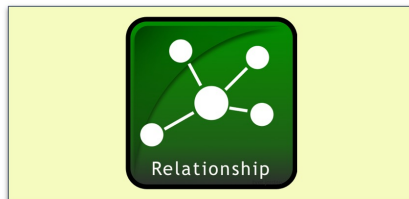


**Remediation Objects**



**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

Report

## 2 – Le marquage

Created by  
SEKOIA

Created at  
Oct 8, 2021

Modified at  
Oct 8, 2021

Name: BRINT - Etat de la Menace Ransomware (Octobre 2021)

External Ids: -

Report types: threat-report

Published at: Oct 8, 2021

Object References
Raw Object

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

# 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

vblocalhost.com/presentations/unc788-irans-decade-of-crede...

**VB2021 localhost** Register Partners Programme

**UNC788: Iran's decade of credential harvesting and surveillance operations**

Emiel Haeghebaert (FireEye)

Home / Intelligence / Credential Harvesting with PINEFLOWER...

**Campaign**

**WHITE**

Confidence: Confirmed by other sources 1

Sources: www.mandiant.com Usually reliable B

**Relationships** External References

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

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

**Charming Kitten**

Relationship

uses

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

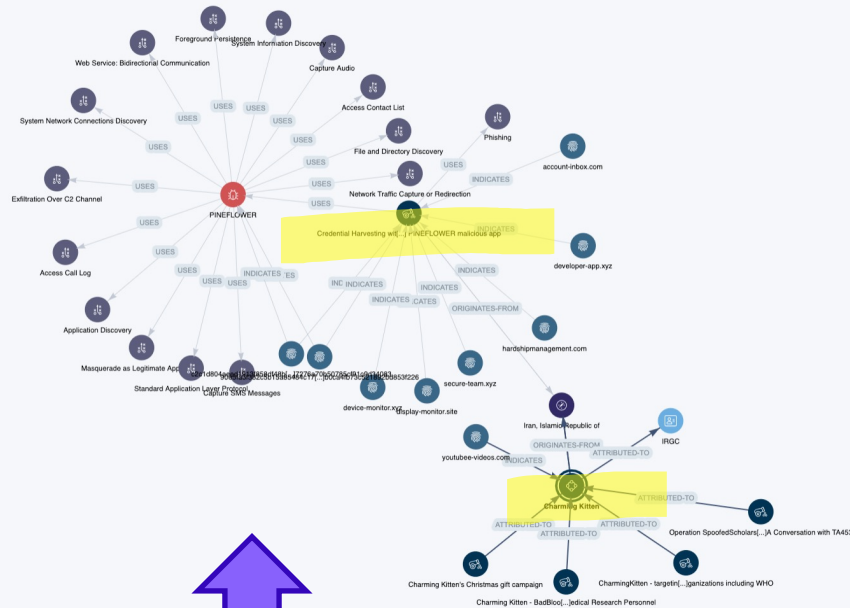
Items per page: 5 1-5

indicates

targets

originates-from

## 3 – 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

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  
 Confirmed by other sources: 1  
**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  
**External References:** 106.15.197.67, 313.41.181, 15.185.226.230, 23.96.10.0, 54.763.220.118

## 3 – Les compléments

**Name:** 23.81.246.17  
**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:** Completely reliable  
**Confirmed by other sources:** 1  
**Pattern (stix):** [ipv4-addrvalue = '23.81.246.17']  
**Sources:** www.mandiant.com (Usually reliable), SEKOIA (Completely reliable), SEKOIA C2 Tracker (Completely reliable)  
**Kill chain:** Cyber Kill Chain (Used by FIN12), Reconnaissance  
**Notes:** 10/11 2:48 PM Used by FIN12. Announced to be used by FIN12 (Mandiant report) but outdated information. agree  
**Relationships:** Indicates, 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
Indicates	WIZARD SPIDER - Cobalt Strike distrib...	SEKOIA	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



## 2 – Les indicateurs associés

- SEKOIA, SEKOIA C2 Tracker about 2 hours ago
- SEKOIA C2 Tracker about 2 hours ago
- SEKOIA C2 Tracker about 2 hours ago
- SEKOIA C2 Tracker about 2 hours ago
- SEKOIA C2 Tracker about 2 hours ago
- SEKOIA C2 Tracker about 2 hours ago

# pistes **#2**

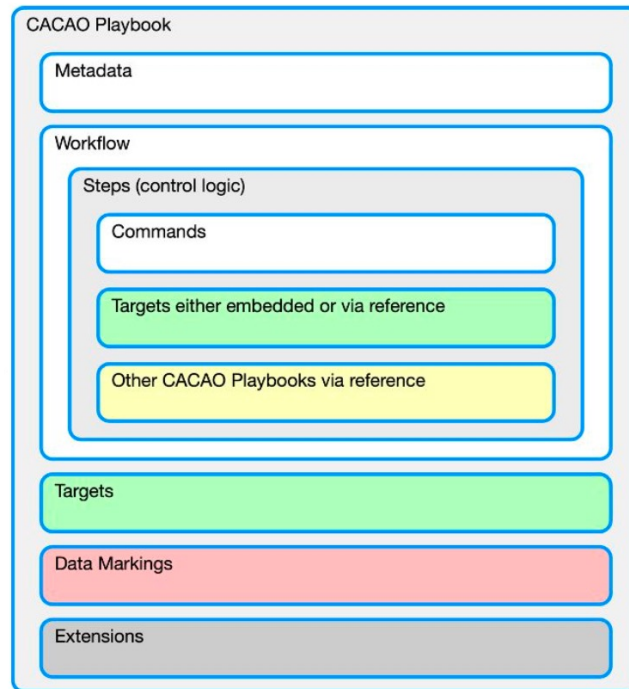
CACAO

Des plans d'actions génériques

# CACAO : c'est quoi ?

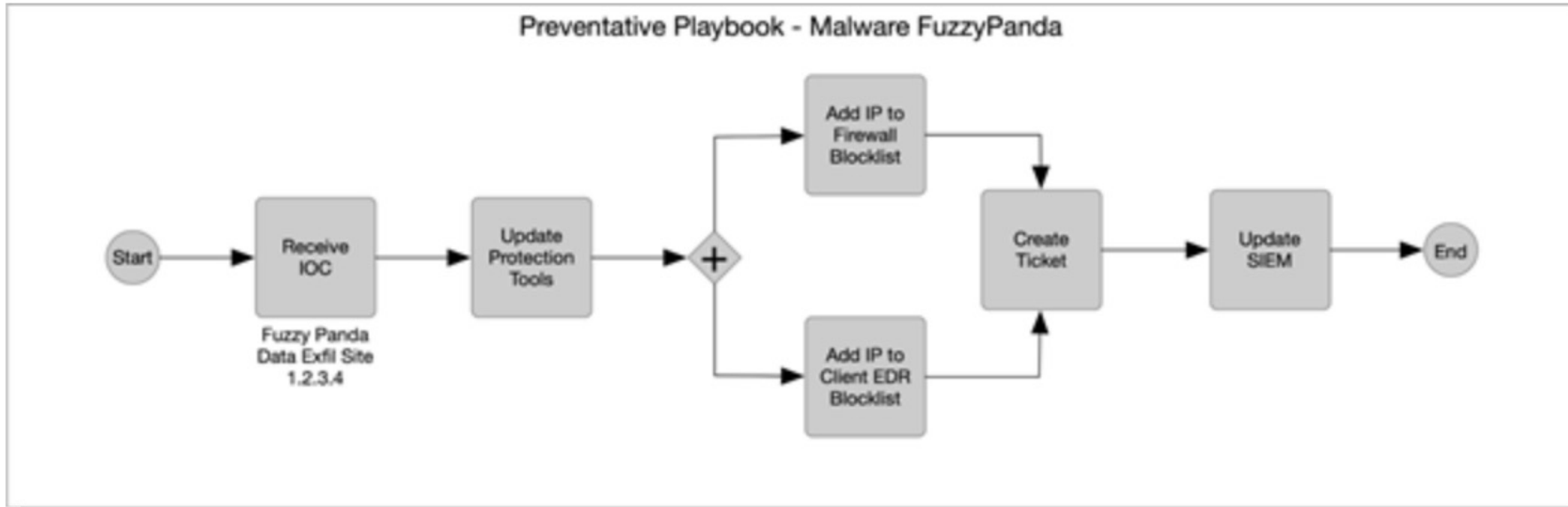
## Langage de Workflow pour orchestrer les actions

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





# CACAO : illustration



# pistes **#3**

OpenC2

Des actions automatisables

# OpenC2 : c'est quoi ?

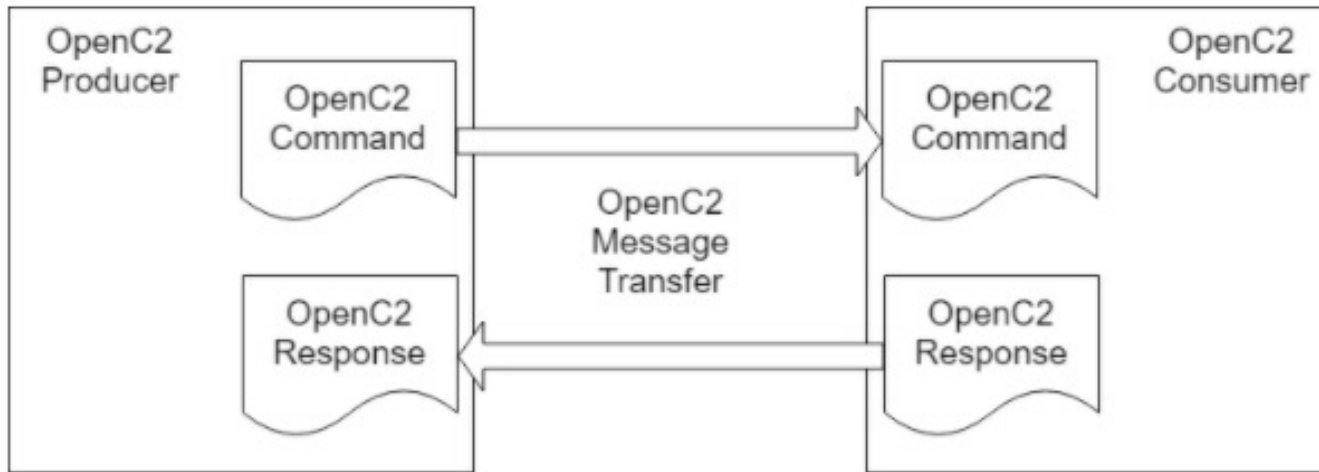
**Langage pour automatiser les actions sur les composants du SI**

- Un ordre
- Une cible
- Eventuellement un exécutant

## OpenC2 : illustration

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

# OpenC2 : Commandes et réponses





**SEKOIA.IO**

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

# illustrations #1

Proposer les meilleures stratégies  
grâce au renseignement

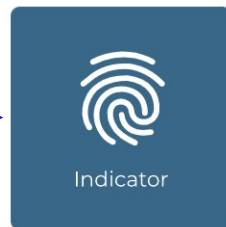
Pivot automatisés via STIX

# Les pivots intéressants dans une alerte

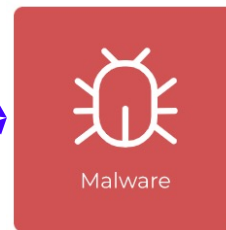
Sur un réseau



?

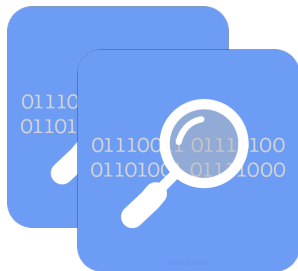


indicates

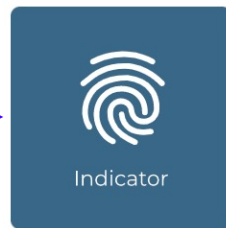


indicates

Sur une machine



?



indicates



# Exemple

## 1 – Des événements

The screenshot displays the SEKOIA.IO interface for a specific alert. The main alert is titled "SEKOIA Intelligence Feed" with ID "AL3BJYWhj5Vh" and is categorized as "malware". It shows a severity of "Low" (40) and is related to "Intrusion using Cobalt Strike". The interface includes a "Kill chain phases" diagram with "Command and Control" highlighted, and a "Threat Intelligence Context" section for IP address "20.199.116.167".

The "Timeline" section on the right shows a series of events, with the first event highlighted by a red box and a large red "1". The events are:

- 18:51:20: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (s...
- 18:45:20: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (s...
- 18:42:19: Event
- 18:39:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (s...
- 18:37:19: Event
- 18:30:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (s...
- 18:28:19: Event
- 18:25:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (s...
- 18:22:19: Event
- 18:21:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (s...
- 18:19:19: Event
- 18:16:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (s...

# Exemple

1 - Des événements

2 - Repérage d'un indicateur dans le contenu

SEKOIA.IO DEMO-PROD-COMMUNITY

Home / Alerts / AL3BJYWhj5Vh

SEKOIA Intelligence Feed  
ID: AL3BJYWhj5Vh - Matched 9 days ago

Details Tasks Events 13813 Graph Investigation

Alert Type: malware  
Impacted Entity: Demo CS  
Urgency: Low (40) / previous (60) / Low

Related cases: Intrusion using Cobalt Strike

Threats: EICAR SEKOIA test campaign, Cobalt Strike

Kill chain phases: Cyber kill chain  
Reconnaissance → Weaponization → Delivery → Exploitation → Installation → **Command and Control** → Actions on Objectives

Triggered rule: SEKOIA Intelligence Feed  
Detect threats based on indicators of compromise (IOCs) collected by SEKOIA's Threat and Detection Research team.

Threat Intelligence Context

20.199.116.167 (malicious-activity) [WHITE]

Pattern (stix): [ip4-addr:value = '20.199.116.167']

Confidence: Confirmed by other sources 1 Sources SEKOIA

EICAR SEKOIA test campaign (GREEN)

Context: This campaign has been initiated by SEKOIA to create a complete environment that can be used to simulate a real threat actor

Timeline (12 Oct, 2021):

- Event 18:51:20: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)
- Event 18:45:20: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)
- Event 18:42:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)
- Event 18:39:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)
- Event 18:37:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)
- Event 18:30:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)
- Event 18:28:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)
- Event 18:25:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)
- Event 18:22:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)
- Event 18:21:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)
- Event 18:19:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)
- Event 18:16:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)

# Exemple

1 – Des événements

2 – Repérage d'un indicateur dans le contenu

3 – Génération d'une alerte

The screenshot displays the SEKOIA.IO security dashboard. The main content area features a 'SEKOIA Intelligence Feed' card for alert ID AL3BJYWhj5Vh, which is 9 days old. The card shows an alert type of 'malware', impacted assets of 'Demo CS', and a severity of 'Low'. It lists related cases such as 'Intrusion using Cobalt Strike' and threats including 'EICAR SEKOIA test campaign' and 'Cobalt Strike'. A 'Cyber kill chain' diagram is visible, with 'Command and Control' highlighted in orange. The 'Timeline' on the right shows a series of 'User made GET request' events from 18:51:20 to 18:16:19 on 12 Oct, 2021. The 'Threat Intelligence Context' section shows a threat indicator for IP address 20.199.116.167, identified as 'malicious-activity' with a 'WHITE' confidence level, and a source 'SEKOIA'. Another threat indicator, 'EICAR SEKOIA test campaign', is shown with a 'GREEN' confidence level.

# 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

SEKOIA.IO DEMO-PROD-COMMUNITY

Home / Alerts / AL3BJYWhj5Vh

SEKOIA Intelligence Feed  
ID: AL3BJYWhj5Vh - Matched 9 days ago

Details Tasks Events 13813 Graph Investigation

Alert Type: malware  
Impacted Entity: Demo CS  
Urgency: Low (40) (previous: 60)

Related cases: Intrusion using Cobalt Strike

Threats: EICAR SEKOIA test campaign, Cobalt Strike

Kill chain phases: Cyber kill chain  
Reconnaissance → Weaponization → Delivery → Exploitation → Installation → Command and Control → Actions on Objectives

Triggered rule: SEKOIA Intelligence Feed  
Detect threats based on indicators of compromise (IOCs) collected by SEKOIA's Threat and Detection Research team.

Threat Intelligence Context  
20.199.116.167 (malicious-activity) [WHITE]  
Pattern (stix): [ip4-addr:value = '20.199.116.167']  
Confidence: Confirmed by other sources 1 Sources SEKOIA

EICAR SEKOIA test campaign  
Context: This campaign has been initiated by SEKOIA to create a complete environment that can be used to simulate a real threat actor

Timeline (12 Oct, 2021):  
Event 18:51:20: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)  
Event 18:45:20: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)  
Event 18:42:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)  
Event 18:39:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)  
Event 18:37:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)  
Event 18:30:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)  
Event 18:28:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)  
Event 18:25:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)  
Event 18:22:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)  
Event 18:21:19: User made GET request from 10.0.4.5 : http://20.199.116.167/dpixel (status: 200)  
Event 18:19:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)  
Event 18:16:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 200)

4

# 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
- 5 - Disposer de stratégies de réaction

The screenshot displays the SEKOIA.io interface for a Network Intrusion Prevention (NIP) alert. The alert is titled "EICAR SEKOIA test campaign" and is currently in a "GREEN" state. The TLP (Traffic Light Protocol) is set to "WHITE". The description reads: "Use intrusion detection signatures to block traffic at network boundaries." The interface shows a sidebar with navigation options and a main content area with details and a relationship graph.

**Network Intrusion Prevention Details:**

- Alert Type: malware
- Related cases: Intrusion using Co...
- Threats: EICAR SEKOIA...
- Kill chain phases: Reconnaissance
- Triggered rule: SEKOIA Intel SEKOIA Detect threa
- Threat Intelligence: 20.199.11...

**Relationship Graph:**

The graph illustrates the relationships between various entities and actions:

- Entities:** France, Technology, Dropper TEST EICAR SEKOIA.IO, Commonly Used Port, Data Encrypted for Impact, Command and Scripting interpreter: PowerShell, Network Segmentation, Network Intrusion Prevention, Code Signing, eicar.sekoia.io, SEKOIA-EICAR.png, 79.137.123.241, b4f23a2f0467a66c3fafaa8bafb5b0c0, SEKOIA\_payload\_DROPPER.ps1, SEKOIA\_payload\_EICAR.txt, eicar@sekoia.io, cf1e31b419b4ed689d8b3f11e0605a73, EICAR Unit of SEKOIA.
- Actions:** INDICATES, TARGETS, USES, MITIGATES, ATTRIBUTED-TO.
- Key Relationships:**
  - France and Technology are TARGETS of the EICAR SEKOIA test campaign.
  - The EICAR SEKOIA test campaign USES the Dropper TEST EICAR SEKOIA.IO.
  - The Dropper TEST EICAR SEKOIA.IO USES Commonly Used Port, Data Encrypted for Impact, and Command and Scripting interpreter: PowerShell.
  - Commonly Used Port and Data Encrypted for Impact MITIGATE Network Segmentation.
  - Command and Scripting interpreter: PowerShell MITIGATES Code Signing.
  - SEKOIA-EICAR.png, 79.137.123.241, b4f23a2f0467a66c3fafaa8bafb5b0c0, SEKOIA\_payload\_DROPPER.ps1, SEKOIA\_payload\_EICAR.txt, and eicar.sekoia.io all INDICATE the EICAR SEKOIA test campaign.
  - The EICAR SEKOIA test campaign ATTRIBUTES TO the EICAR Unit of SEKOIA.

**Alert Log:**

- Event 18:19:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 20)
- Event 18:16:19: User made GET request from 10.0.4.5 : http://democs.ddns.net/ca (status: 20)

# 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

1

Enrich alert with VirusTotal

✎

Disable

---

Community  
Demo-prod-Community

Created by  
Erwan Chevalier

Created at  
01/09/2021

Last update by  
Erwan Chevalier

Last update at  
20/10/2021

Description  
Enrich alert with information from Virus Total

---

Runs in the last week

Total  
0

In Progress  
0

Succeeded  
0

Failed  
0

---

GRAPH
CODE
RUNS 0

SAVE or DISCARD

---

^ virustotal

Σ livehunt\_notification\_files

Σ Scan IP

Σ Scan Hash

Σ Scan File

Σ Post Comment

Σ Get Comments

Σ Scan URL

Σ Scan Domain

^ triage

⚙️ Action

Name

Module Configuration

+ Create new configuration  
✓ Edit selected

Configuration Variables

url

The url to scan

The number of positives from VirusTotal that will be used as a threshold of detection

# ~CACAO en action

1 – Un enrichisseur  
VT

2 – Prise en compte  
du contexte de  
l'alerte

**Enrich alert with VirusTotal** Disable

Community: Demo-prod-Community | Created by: Erwan Chevalier | Created at: 01/09/2021 | Last update by: Erwan Chevalier | Last update at: 20/10/2021

Description: Enrich alert with information from Virus Total

Runs in the last week: Total 0 | In Progress 0 | Succeeded 0 | Failed 0

GRAPH CODE RUNS 0 SAVE or DISCARD

**virustotal**

- livehunt\_notification\_files
- Scan IP
- Scan Hash
- Scan File
- Post Comment
- Get Comments
- Scan URL
- Scan Domain

**Action**

Name: Get an alert

**Module Configuration**

sekoia.io

+ Create new configuration  
✓ Edit selected

**Configuration** Variables

- stix
- uuid
- `{{ (store.uuid | reject('equal', Nor`



# ~CACAO en action

1 – Un enrichisseur  
VT

2 – Prise en compte  
du contexte de  
l'alerte

3 – Différents calls  
VT selon le contenu

The screenshot displays the CACAO configuration interface for an alert enrichment rule titled "Enrich alert with VirusTotal".

- Header:** "Enrich alert with VirusTotal" with a "Disable" button.
- Metadata:** Community: Demo-prod-Community; Created by: Erwan Chevalier; Created at: 01/09/2021; Last update by: Erwan Chevalier; Last update at: 20/10/2021.
- Description:** "Enrich alert with information from VirusTotal".
- Runs in the last week:** Total: 0; In Progress: 0; Succeeded: 0; Failed: 0.
- Navigation:** GRAPH (selected), CODE, RUNS (0).
- Workflow:** A flowchart under the "virustotal" section. A red box highlights a specific node labeled "3" which is "Scan URL API with IP". Other nodes include "Manual", "Here", "Get an alert", "Read IP/URL file for domain", "Scan Domain", "Check list", "Add IP/URL file for URL", "Scan URL", "Scan Domain", "Post general alert comment", "Fetch", "Store", "List of domain categories (Context)", "Add information to description", "Report the alert", "Validate", "Auto inhibition", "Condition", "Fetch", "URL VT score", "Read list of security vendors", and "Comment: List of security vendors".
- Action Panel:** "Action" section with "Scan URL API with IP" selected. "Module Configuration" shows "Query\_VT" selected. "Configuration" shows "url" set to "{{ node2[output][0] }}". A note states: "The number of positives from VirusTotal that will be used as a threshold of detection".

# ~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

The screenshot displays the SEKOIA.IO interface for an alert with ID ALYKZxjEVp7Q. The interface includes a navigation sidebar, a main content area with tabs for Details, Tasks, Events, and Graph Investigation, and a right-hand timeline panel. The alert is categorized as 'malware' and 'Mozi malware', with an urgency of 'Medium'. The kill chain phases are 'Reconnaissance', 'Weaponization', 'Delivery', 'Exploitation', and 'Installation'. The timeline shows enrichment by VirusTotal and a URL VT score.

SEKOIA.IO | DEMO-PROD-COMMUNITY

Home / Alerts / ALYKZxjEVp7Q

SEKOIA Intelligence Feed  
ID ALYKZxjEVp7Q - Matched about 2 months ago

Ongoing ADD TO CASE

Details Tasks Events 1 Graph Investigation

Alert Type: malware  
Impacted Assets: -  
Impacted Entity: Demo CS  
Urgency: Medium

Related cases: Mozi malware  
Threats: Mozi

Kill chain phases: Cyber kill chain

Reconnaissance → Weaponization → Delivery → Exploitation → Installation  
Command and Control → Actions on Objectives

Timeline

21 Oct, 2021

- IP enrich by VirusTotal 11:56:55  
4/79 security vendors flagged the target IP (108.62.12.121) as malicious. [Direct link to VirusTotal](#)
- TDR Team 11:56:55  
List of security vendors which detected this IP as malicious: ESET,Sophos,CyRadar,Fortinet
- URL VT score 11:56:45  
13/91 security vendors flagged the target url (http://112.226.40.56:55153/Mozi.a) as malicious. [Direct link to VirusTotal](#)

20 Oct, 2021

4

# illustrations

# #3

Automatiser

Quand c'est possible

# OpenC2 en action

0 – Récupérer le contexte de l'alerte

The screenshot displays the SEKOIA Operation Center interface. On the left is a dark navigation sidebar with options: Dashboard, Detect, Rules Catalog, Investigate, Cases, Alerts, Events, Configure, Intakes, Entities, Assets, and Playbooks. The main content area shows an alert for 'SEKOIA Intelligence Feed' with ID 'ALJALzEUCPMF' and a severity of 80. A red box highlights the 'Details' tab, which shows 'Alert Type: malware', 'Impacted Assets: High-Priority Inter', and 'Threats: TrickBot'. To the right, a circular gauge shows an urgency score of 80, with 'High' and '80' highlighted in red. Below the alert, a 'Kill chain phases: Cyber kill chain' diagram shows 'Command and Control' as the active phase. The 'Triggered rule' section shows a rule from SEKOIA Intelligence Feed: 'Detect threats based on indicators of compromise (IOCs) collected by SEKOIA's Threat and Detection Research team.' The 'Threat Intelligence Context' section includes a rule for 'Network traffic to 97.83.40.67 on port 443' with a confidence of 'Probably True' and sources 'tria,ge MWDB feodotracker.abuse.ch'. At the bottom, the 'TrickBot' threat is identified with tags: 'backdoor', 'keylogger', 'remote-access-trojan', 'spyware', and 'WHITE'. A 'Summary' section begins with the text: 'TrickBot is a modular banking Trojan active since 2016 targeting Windows machines. The trojan is believed to be a derivative of Dyre - a now defunct banking trojan. Initially designed to steal banking credentials from its victims, the malware has since received various updates and new features from its authors. TrickBot campaigns target financial services from all around the world. Since June 2019, the trojan has been identified during various Ryuk ransomware attacks.'

# OpenC2 en action

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

The screenshot displays the OpenC2 Operation Center interface. The main view shows an alert for 'malware' with a severity of 80. The alert details include 'Threats: TrickBot' and 'Impacted Assets: High-Priority Inter'. A 'Kill chain phases' diagram shows the progression from Reconnaissance to Command and Control. The 'Triggered rule' section identifies the rule as 'SEKOIA Intelligence Feed' which detects threats based on indicators of compromise (IOCs). The 'Threat Intelligence Context' section provides details for 'Network traffic to 97.83.40.67 on port 443', including its pattern, confidence, and sources.

A table in the bottom left corner, titled 'Relationships', shows the following data:

Relationships	External References	Reports	Raw Object	
delivers	uses	authored-by	downloads	
mitigates	drops	targets	indicates	
Type	Name	Confidence	External Source	Updated Date
mitigates	Education		SEKOIA	over 1 year ago
mitigates	Indicator Blocking Mitigation		SEKOIA	over 1 year ago

# OpenC2 en action

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

2 – batterie d'actions possibles

The screenshot displays the OpenC2 interface. On the left is a dark sidebar with navigation options: Dashboard, Detect, Rules Catalog, Investigate, Cases, Alerts, Events, Configure, Intakes, Entities, Assets, and Playbooks. The main content area shows a breadcrumb path: Home / Alerts / ALogJ2mpcu5. Below this is a 'SEKOIA Intelligence Feed' section for ID ALogJ2mpcu5, which was matched about 19 hours ago. A progress bar indicates 1/6 actions. A list of actions is shown, with a red box and the number '2' highlighting the 'Block the local device' and 'Collect more information on the concerned case' sections. The actions listed are:

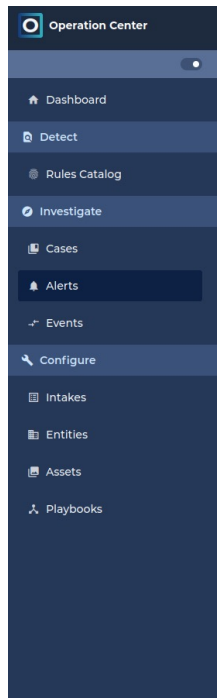
- Indicator Blocking Mitigation: Ensure event tracers/forwarders (Citation: Microsoft ETW May 2018), firewall policies, and other associated services are secured with appropriate permissions and access controls. Consider automatically relaunching services.
- Education: Educate employees to report suspicious emails and avoid clicking on attached files in case of any doubt.
- Block the local device: Block the local device.
  - Show 1 subtask
    - 1 Block the physical address of the computer
- Collect more information on the concerned case: Collect more information on the concerned case.
  - Show 1 subtask
    - 4 Launch a forensic tool to collect information on suspicious systems

# OpenC2 en action

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

2 – batterie d'actions possibles

3 – Une action atomique OpenC2



The image shows the main content area of the Operation Center interface. At the top, there is a breadcrumb trail: Home / Alerts / ALocjU2mpcu5. Below this is a header for the 'SEKOIA Intelligence Feed' with an ID of 'ALocjU2mpcu5' and a timestamp of '- Matched about 19 hours ago'. There are tabs for 'Details', 'Tasks', 'Events' (with a count of 218), and 'Graph Investigation'. A progress bar indicates '1/6' tasks completed. The first task is 'Indicator Blocking Mitigation', which includes a description: 'Ensure event tracers/forwarders (Citation: Microsoft ETW May 2018), firewall policies, and other associated mechanisms are secured with appropriate permissions and access controls. Consider automatically relaunching applying appropriate change management to firewall rules and other related system configurations.' The second task is 'Education', with a description: 'Educate employees to report suspicious emails and avoid clicking on attached files in case of any doubt.' The third task, 'Block the local device', is highlighted with a red box and a large number '3'. It includes a subtask 'Show 1 subtask' which is expanded to show '1 Block the physical address of the computer'. The fourth task is 'Collect more information on the concerned case', with a subtask 'Show 1 subtask' expanded to show '4 Launch a forensic tool to collect information on suspicious systems'.

# 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

```
1  [
2    {
3      "name": "Block the local device",
4      "description": "Block the local device",
5      "countermeasures": [
6        {
7          "type": "openc2",
8          "description": "Block the physical address of the computer",
9          "object": {
10             "action": "deny",
11             "target": {
12               "mac_addr": "@mac_addr"
13             }
14           },
15           "name": "1"
16         }
17       ],
18       "relevance": 60
19     }
20  ]
```

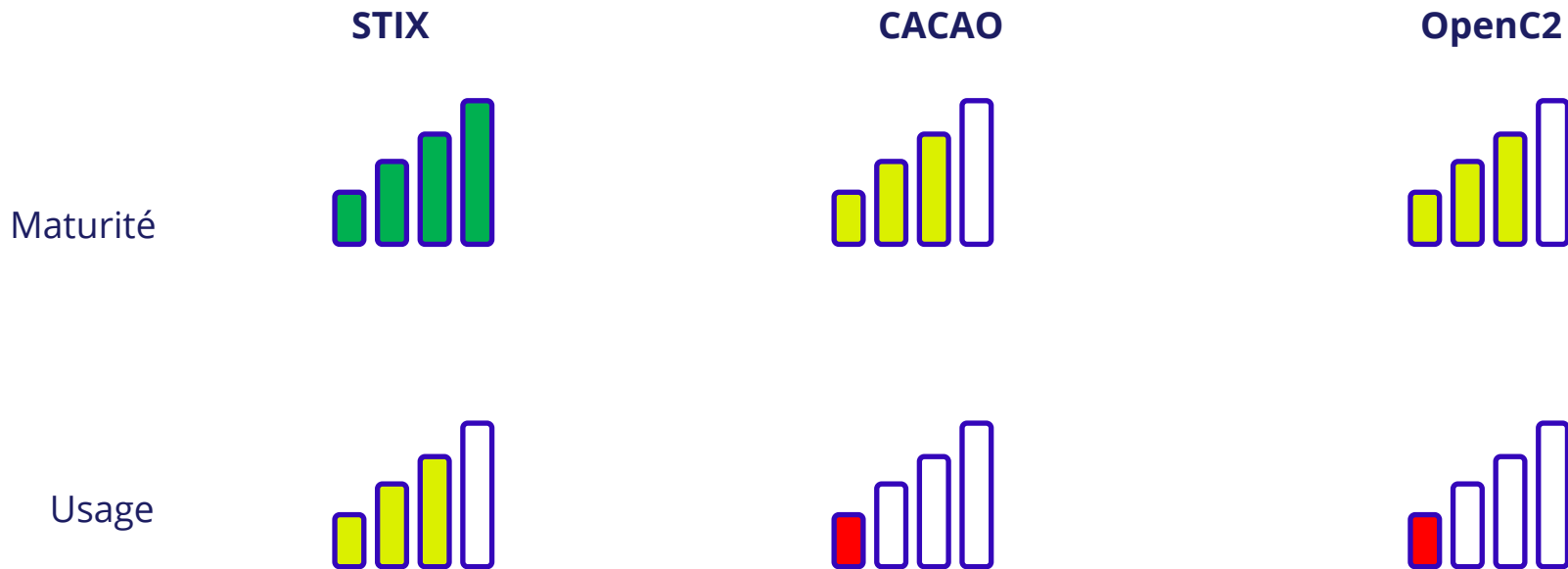




**SEKOIA.IO**

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

# Niveaux de maturité



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