

Home Made Distributed Blocklist

Because you are never as well served as
when you serve yourself...

TLP:White

PTS2021 - Xavier Mertens - July 2021



About?

In a few words

- Xavier Mertens
- Belgium
- Freelance Consultant
- SANS
- BruCON
- Free software > integration & automation ❤️ (OSSEC)

Some Facts?

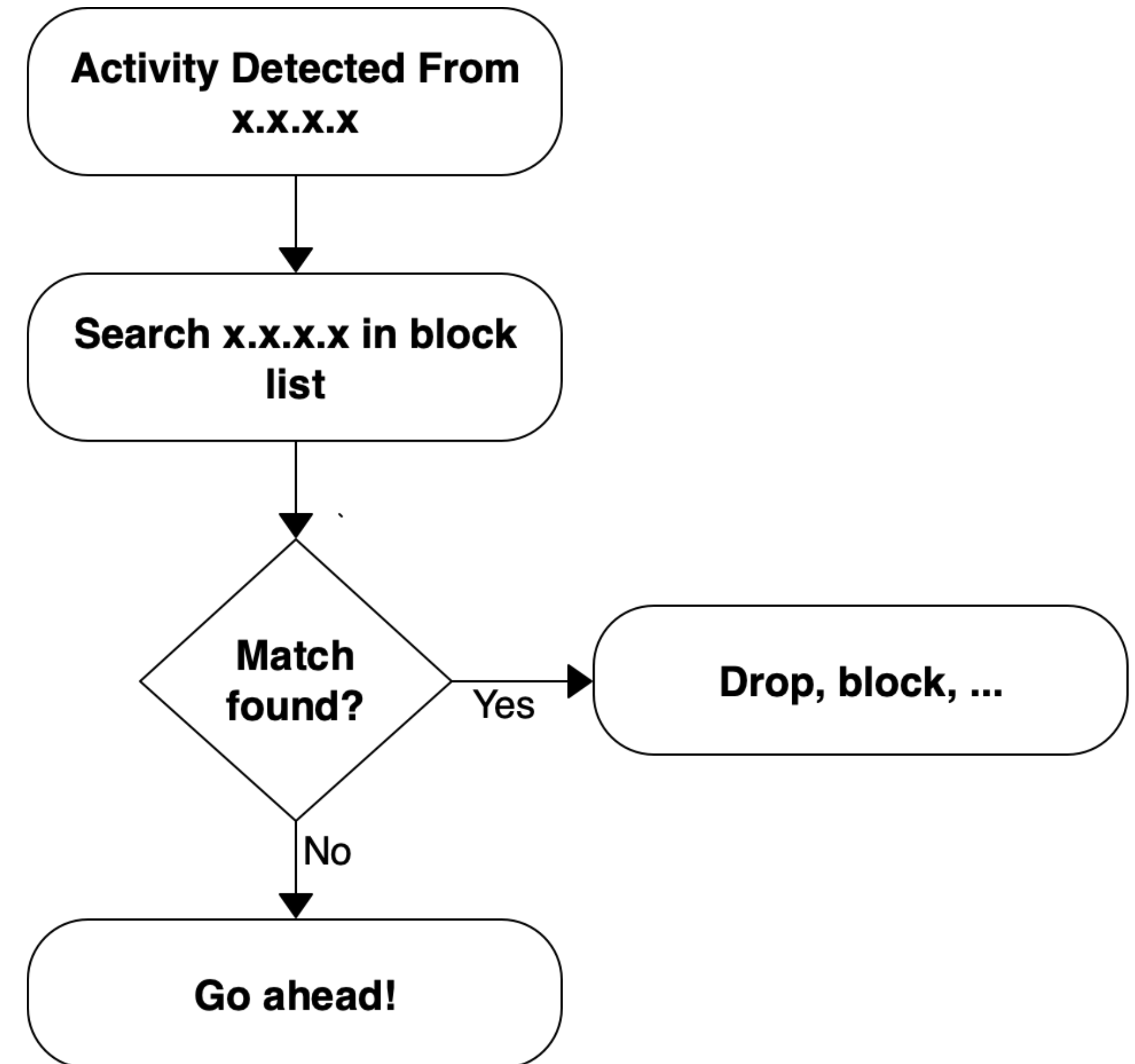
The idea behind this talk

- We expose more and more applications, devices (“0-trust”)
- The perimeter does not exist anymore
- Applications are split across multiple micro-services (read: “dockerized”)
- The attack surface keeps growing therefore attacks too
- We need efficient tools to help us (defenders) to do our job

How to Protect Ourselves?

Let's block attackers!

- Block traffic from suspicious locations?
- Block traffic based on suspicious activity?
- ~~Black~~ Block lists to the rescue?



Blocklists

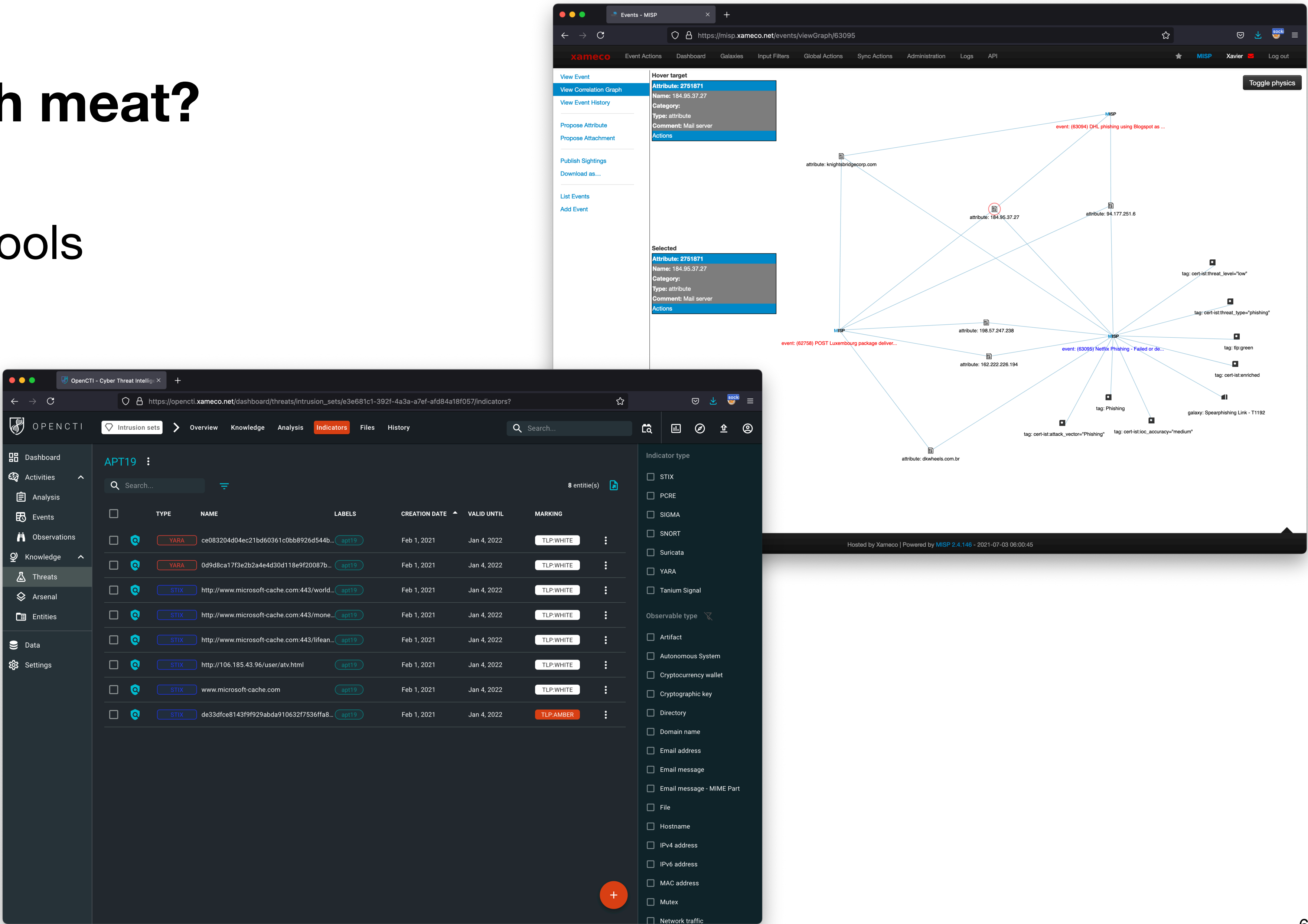
Love & hate relationship...

- Easy to implement!
- But blocklists are a pain...
 - Not very effective
 - Reliability?
 - Hard to manage (sync, update, ...)

Blocklists

Where to find fresh meat?

- Threat Intelligence tools
- Free feeds
- \$\$\$ feeds
- Local intelligence



The IOC Problem

It's a question of context

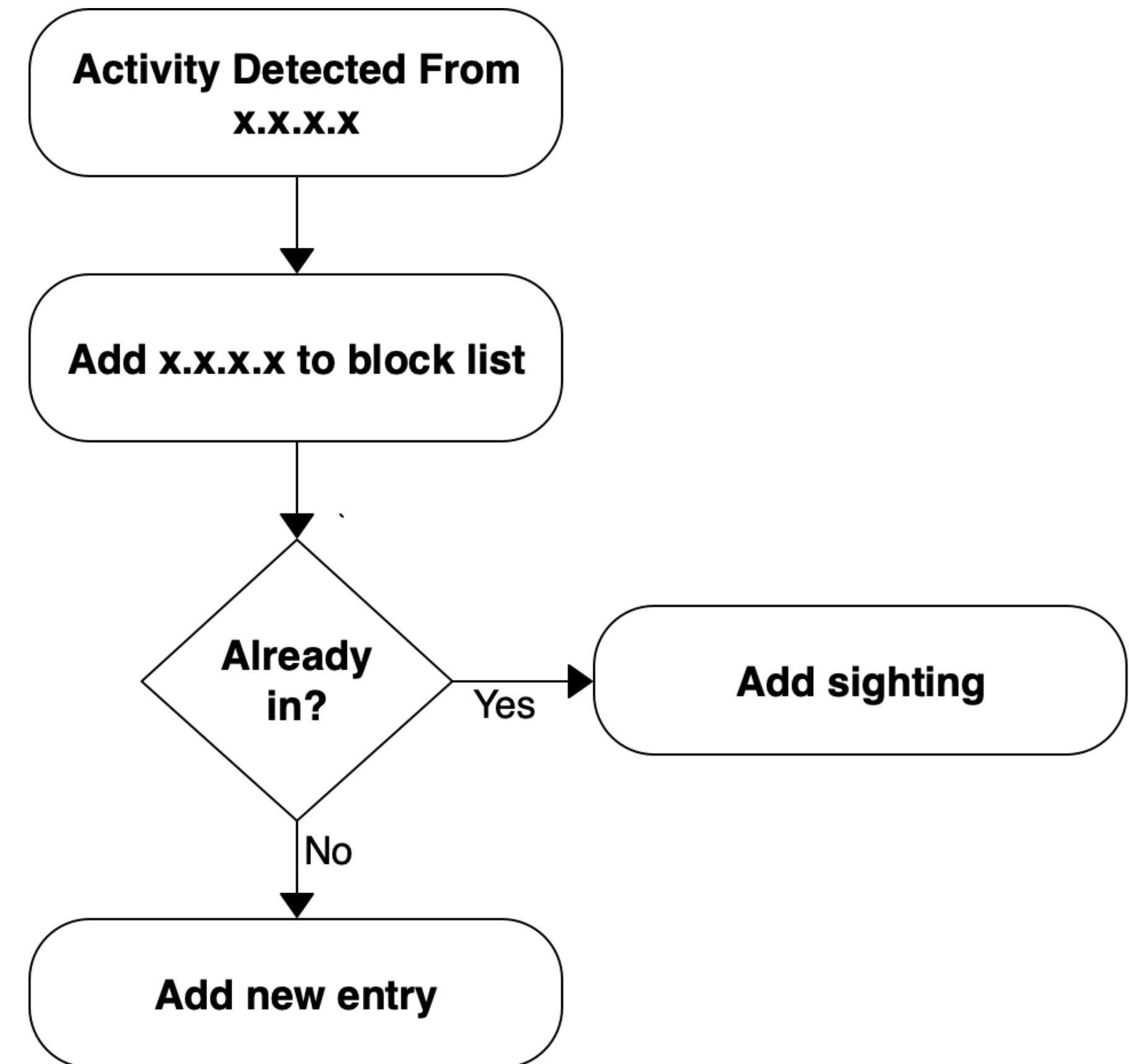
- An IOC out of its context has less/no value
- I like the approach used in TheHive^(*)
 - We have « observables »
 - We convert them to «IOCs » if relevant to us (in our context)

^(*) <https://thehive-project.org>

Why?

How to populate?

- Multiple sources of informations
- Manual input?
- Automation!



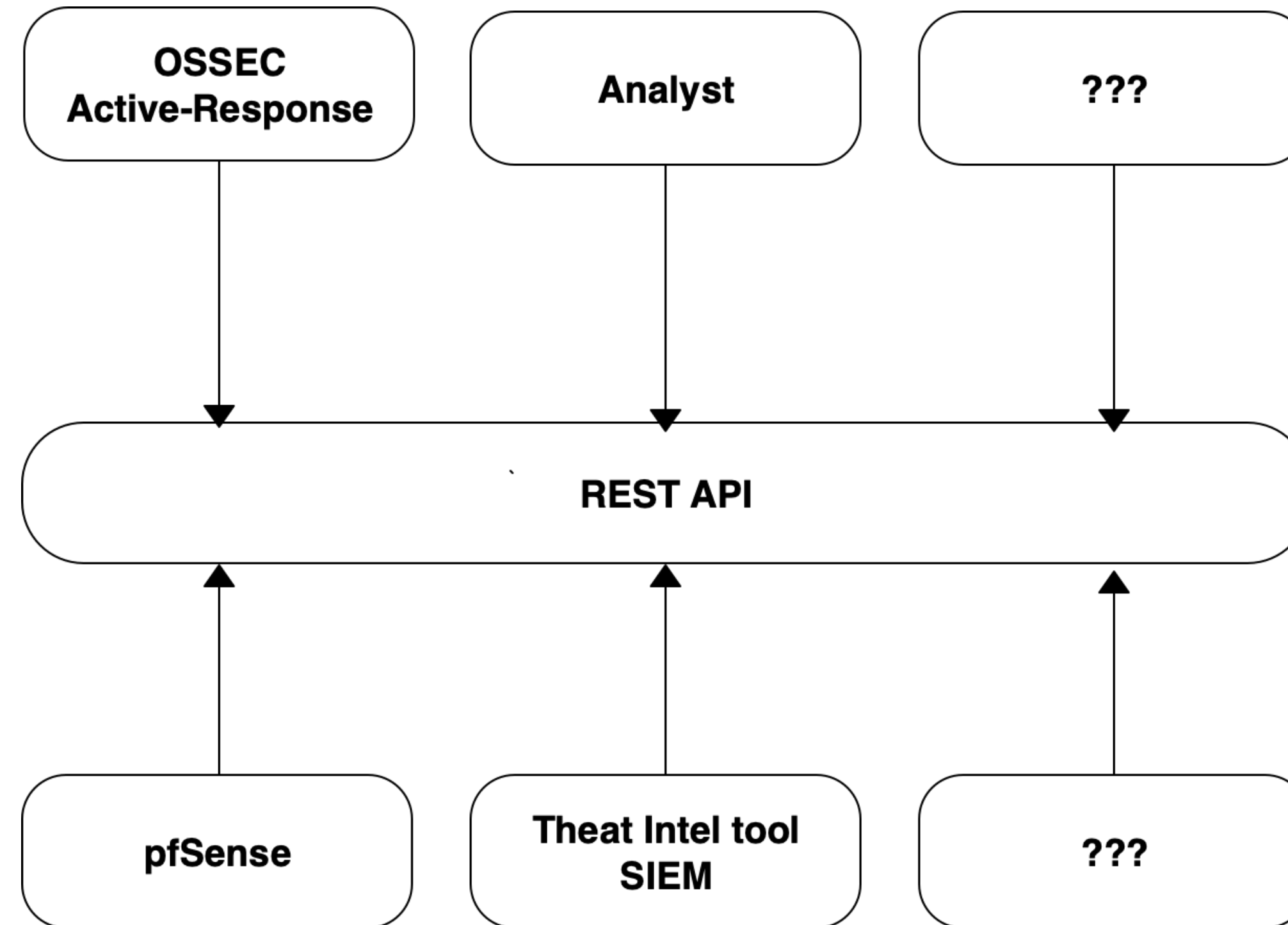
How?

Requirements

- Light
- REST API
 - To populate/query from many sources
 - To register users/devices
- Multiple output formats (JSON, XML, CSV)
- Easy to deploy (Docker)
- To have fun, learn...

Setup

In & Out Paths



Deploy

Easy as 1, 2, 3

- Spawn a docker!

```
FROM ubuntu:18.04
MAINTAINER Xavier Mertens
VOLUME [ "/data" ]
RUN apt-get update && apt-get -y upgrade
RUN apt-get -y install python3-pip vim sqlite3

COPY ./requirements.txt /tmp
RUN pip3 install -r /tmp/requirements.txt && rm /tmp/requirements.txt

COPY ./create_db.sh /
COPY ./index.html /
COPY ./api.py /
COPY ./entrypoint.sh /
RUN chmod a+x /entrypoint.sh
RUN touch /.firstboot

ENTRYPOINT [ "/entrypoint.sh" ]
```

```
version: '3'
services:
  api:
    image: xameco/api:20201114
    build: .
    hostname: api.xameco.lab
    container_name: api.xameco.lab
    restart: unless-stopped
    expose:
      - 5000
    volumes:
      - /etc/localtime:/etc/localtime:ro
      - /data/api/data:/data
      - /data/api/log:/log
    environment:
      - TZ='Europe/Brussels'
      - REGISTRATION_TOKEN=SuperSecretToken
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.api.entrypoints=web"
      - "traefik.http.routers.api.middlewares=https_redirect"
      - "traefik.http.routers.api.rule=Host(`api.xameco.lab`)"
      - "traefik.http.routers.api-secure.entrypoints=websecure"
      - "traefik.http.routers.api-secure.rule=Host(`api.xameco.lab`)"
      - "traefik.http.routers.api-secure.tls=true"
      - "traefik.http.routers.api-secure.tls.certresolver=le"
      - "traefik.http.routers.api-secure.service=api"
      - "traefik.http.middlewares.https_redirect.redirectscheme.scheme=https"
      - "traefik.http.middlewares.https_redirect.redirectscheme.permanent=true"
      - "traefik.http.services.api.loadbalancer.server.port=5000"
      - "traefik.http.services.api.loadbalancer.server.scheme=http"
      - "traefik.docker.network=traefik_default"
      - "traefik.tags=lab"
    networks:
      - default
      - traefik_default

networks:
  traefik_default:
    external: true
```

Usage

Register a first user

- Defines your users (system accounts or analysts)

```
root@barney:/data/compose/api# curl \
-H 'x-authentication: SuperSecretToken' \
-H 'Content-Type: application/json' \
--request POST \
--data '{"username":"pts2021","password":"SecretPW"}' \
https://api.xameco.lab/user/register
{"username":"pts2021"}
```

Usage

Add your first IP address

- Just give the IP and a comment (case number, OSSEC rule, ...)

```
root@barney:/data/compose/api# curl \
--user pts21:SecretPW \
-H 'Content-Type: application/json' \
--request POST \
--data '{"ip":"45.146.164.110","comment":"Bad guy"}' \
https://api.xameco.lab/ip/add
{"message":"IP address successfully saved"}
```

Usage

Query an IP address

- Let's search now

```
root@barney:/data/compose/api# curl \
--user pts21:SecretPW \
-H 'Content-Type: application/json' \
https://api.xameco.lab/ip/45.146.164.110 | jq
```

```
[
  {
    "comment": "Bad guy",
    "sighting": 0,
    "source": "172.31.2.1",
    "time_added": "2021-07-03 06:11:13",
    "time_updated": "2021-07-03 06:11:13",
    "type": "ip",
    "value": "45.146.164.110"
  }
]
```

Usage

More queries

- If you add an IP more time, more sightings

```
root@barney:/data/compose/api# curl \
--user pts21:SecretPW \
-H 'Content-Type: application/json' \
https://api.xameco.lab/ip/185.143.223.11 | jq
```

```
[
  {
    "comment": "OSSEC Alert ID 100402",
    "sighting": 10,
    "source": "<redacted>",
    "time_added": "2021-06-15 08:26:06",
    "time_updated": "2021-06-16 13:29:09",
    "type": "ip",
    "value": "185.143.223.11"
  }
]
```

Usage

Format the output

- More formats, easier integration

```
root@barney:/data/compose/api# curl \
--user pts21:SecretPW \
-H 'Content-Type: application/json' \
https://api.xameco.lab/ip/185.143.223.11?format=csv
time_added,time_updated,type,value,sighting,comment,source
2021-06-15 08:26:06,2021-06-16 13:29:09,ip,185.143.223.11,10,OSSEC Alert ID 100402,<redacted>
```

Usage

Format the output

- Restrict fields (output)

```
root@barney:/data/compose/api# curl \
--user pts21:SecretPW \
-H 'Content-Type: application/json' \
https://api.xameco.lab/ip/185.143.223.11?fields=sighting | jq
[
  {
    "sighting":10
  }
]
```

Usage

Format the output

- Generate list of suspicious IP addresses

```
root@barney:/data/compose/api# curl \
--user pts21:SecretPW \
-H 'Content-Type: application/json' \
https://api.xameco.lab/ip/all?fields=value&format=csv | tail -10
105.22.34.122
93.76.246.7
14.186.161.104
115.73.219.108
177.104.249.181
14.186.18.13
194.53.176.19
103.196.208.12
65.155.32.252
45.146.164.110
```

Integration

Input: OSSEC

- Active-Response to the rescue!

```
<command>
  <name>api-block</name>
  1 <executable>api_block.py</executable>
    <expect>srcip</expect>
    <timeout_allowed>no</timeout_allowed>
</command>
```

```
<active-response>
  <disabled>no</disabled>
  2 <command>api-block</command>
    <location>server</location>
    <rules_group>block_ip</rules_group>
</active-response>
```

```
<rule id="100402" frequency="10" timeframe="180" level="10">
  <if_matched_sid>5503</if_matched_sid>
  <hostname>marge</hostname>
  3 <regex>john|mike|admin|root</regex>
    <description>Multiple targeted logins in a small period of time</description>
    <group>block_ip,</group>
</rule>
```

Integration

Input: Human

- Use your preferred scripting language

Alert Preview New

OSSEC Multiple web server 400 error codes from same source ip.

ID: ~724689024

Date: 04/07/2021 12:05

Type: alert

Reference: ossec_6429042561

Source: OSSEC

src:OSSEC

Description

45.146.164.110 [04/Jul/2021:11:53:20:102001]"GET /wp-content/plugins/wp-file-manager/readme.txt HTTP/1.1" 404 5598 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"

Addition

No addition

Ob

List of c

Flags

ip

45[.]146[.]1164[.]11

ossec_agent

ma ge

ossec_decoder

web accesslog

ossec_rule

31151

severity

10

Cancel

Mark as read

Ignore new upda

9e4

alert

New

Unread

VT

asTotal

7d61

alert

New

Unread

VT

Look Up "45.146.164.110"

Search with Google

Copy

Share

Speech

Show 1Password mini

Hide 1Password on this page

Inspect Element

Services

Add to Music as a Spoken Track

AIL Lookup

Base64Decode

Blacklist IP

CyberChef-Base64-Decode

CyberChef: Base64 Decode

Open

Open man Page in Terminal

OpenPGP: Decrypt Selection to New Window

OpenPGP: Encrypt Selection to New Window

OpenPGP: Import Key from Selection

OpenPGP: Sign Selection to New Window

OpenPGP: Verify Signature of Selection

Search man Page Index in Terminal

Search With Google

Show in Finder

Show Info in Finder

VTI SHA256 Lookup

Comment?

OSSEC Multiple web server 400 error codes from same source ip

Cancel

OK

Integration

Output: pfSense

- Use the dynamic aliases feature

1

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Aliases / URLs

IP Ports URLs All

Firewall Aliases URLs

Name	Values	Description	Actions
misp_ip	http://192.168.254.8/misp-ip.txt	MISP Blocklist	
xameco_blocklist	http://192.168.254.8/xameco-blocklist.txt	IP block list generated by	

+ Add

2

☐		0 / 470.51 MiB	IPv4 *	black_list	*	*	*	*	none	Blacklisted Hosts	
☐		0 / 46.04 MiB	IPv4 *	xameco_blocklist	*	*	*	*	none	Blacklisted Xameco	
☐		0 / 1.67 MiB	IPv4 *	misp_ip	*	*	*	*	none	Blacklisted MISP	

Overview

API Reference

- Still ongoing...

POST /user/register

GET /user/<id>

GET /ip/<address>

GET /ip/all

POST /ip/add

POST /ip/delete

- To add: domains, users, ... (just copy/paste the existing functions)

Conclusion

That's all folks!

- The goal was not to build a new “MISP”
- The core idea was to easily share stuff inside a network
- Code will be released on GitHub soon (need some cleanup ;-)
- Ideas are welcome as usual...

Thank You

xavier@rootshell.be | @xme | <https://blog.rootshell.be/>