RawSec

MISP + WHIDS = <3

Github / Twitter: 0xrawsec

Project: https://github.com/0xrawsec/whids

Me

First Name: Quentin **Last Name**: JEROME **Age**: 32

Freelance Security Consultant working in Luxembourg, running for my own company

- Originally doing Incident Response, digital forensics, malware oriented digital forensics, endpoint's based Threat Hunting …
- Open-Source developer (in my free time) mainly Go, C, Python. At the origin of several projects: Gene, WHIDS, golang-evtx, golang-misp, golang-etw …

Why do I do that ?: for pure fun, to bring Open Source alternative, to help people, ~~to make money~~

RawSec

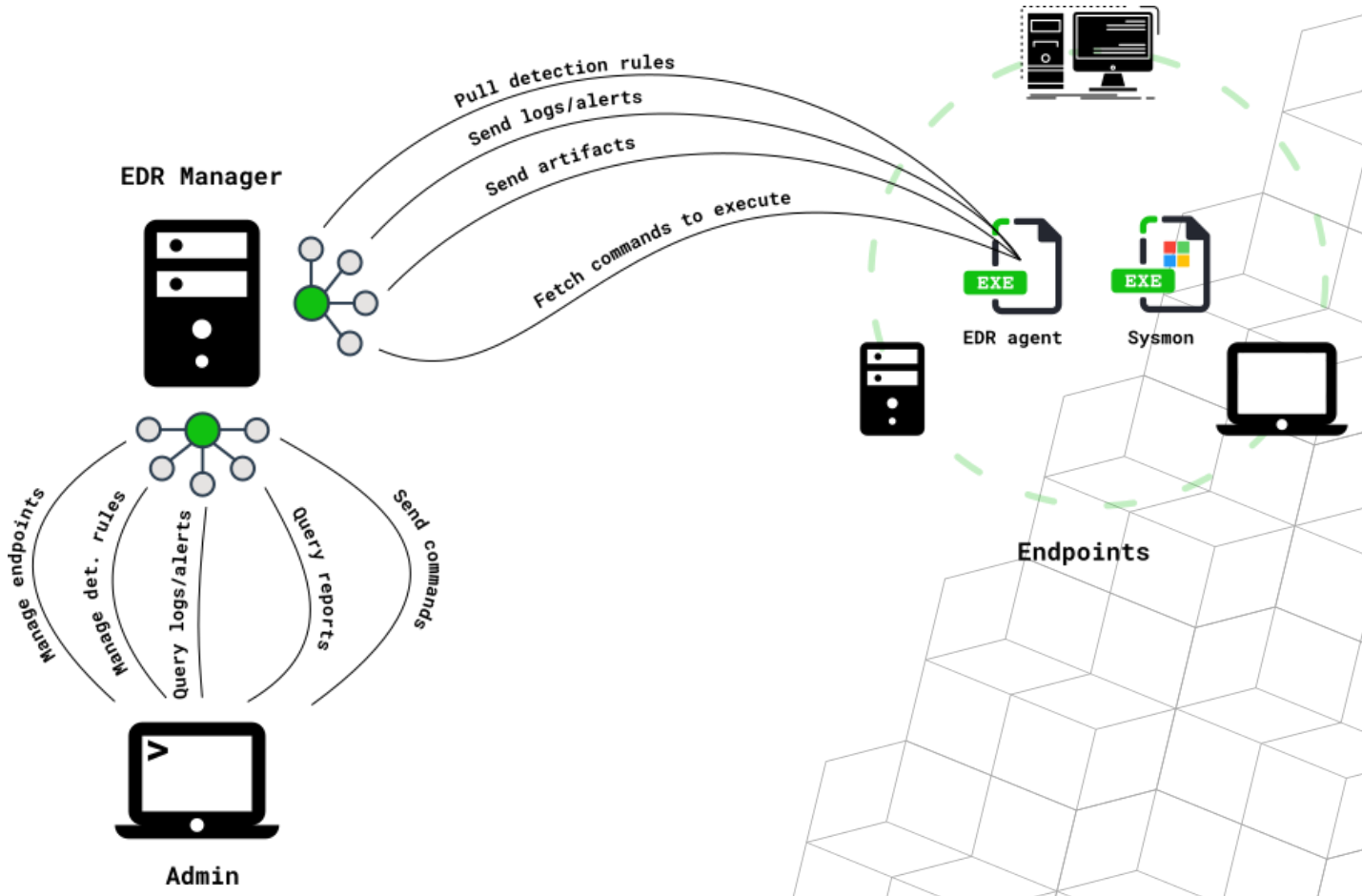
Brief Recap

Agent

- **Correlate** events on host
- **Detect** in real time suspicious events (raw/correlated) based on user defined rules
- **React** to detection in RT: dump artifacts (files, process, registries), blacklist process, kill process

Manager

- **Central** manager to administrate endpoints
- **Collect** logs, and artifacts
- **HTTP API** for administrators and plugins



User's have full control over detection/forwarding rules

Existing Integration with MISP

Since WHIDS **v1.6.2**:

- MISP IoCs are pulled **periodically** from the manager and updated on the endpoints
- **Not all** MISP IoCs can be used, only the ones with **IDS flag** and belonging to those categories:
  - md5 / sha1 /sha256
  - hostname / domain

Future Plan (very soon):

- Decouple **MISP** from WHIDS and provide a **HTTP API** to push IoCs
- More flexible approach, can be used to feed EDR with any feed of IoCs

New Integration: sightings.py

Goal: push sightings from EDR in real-time to MISP

Issue: How to design a nice HTTP API to stream logs in RT ?

Answer: websockets ☺ (thx to @gallypette)

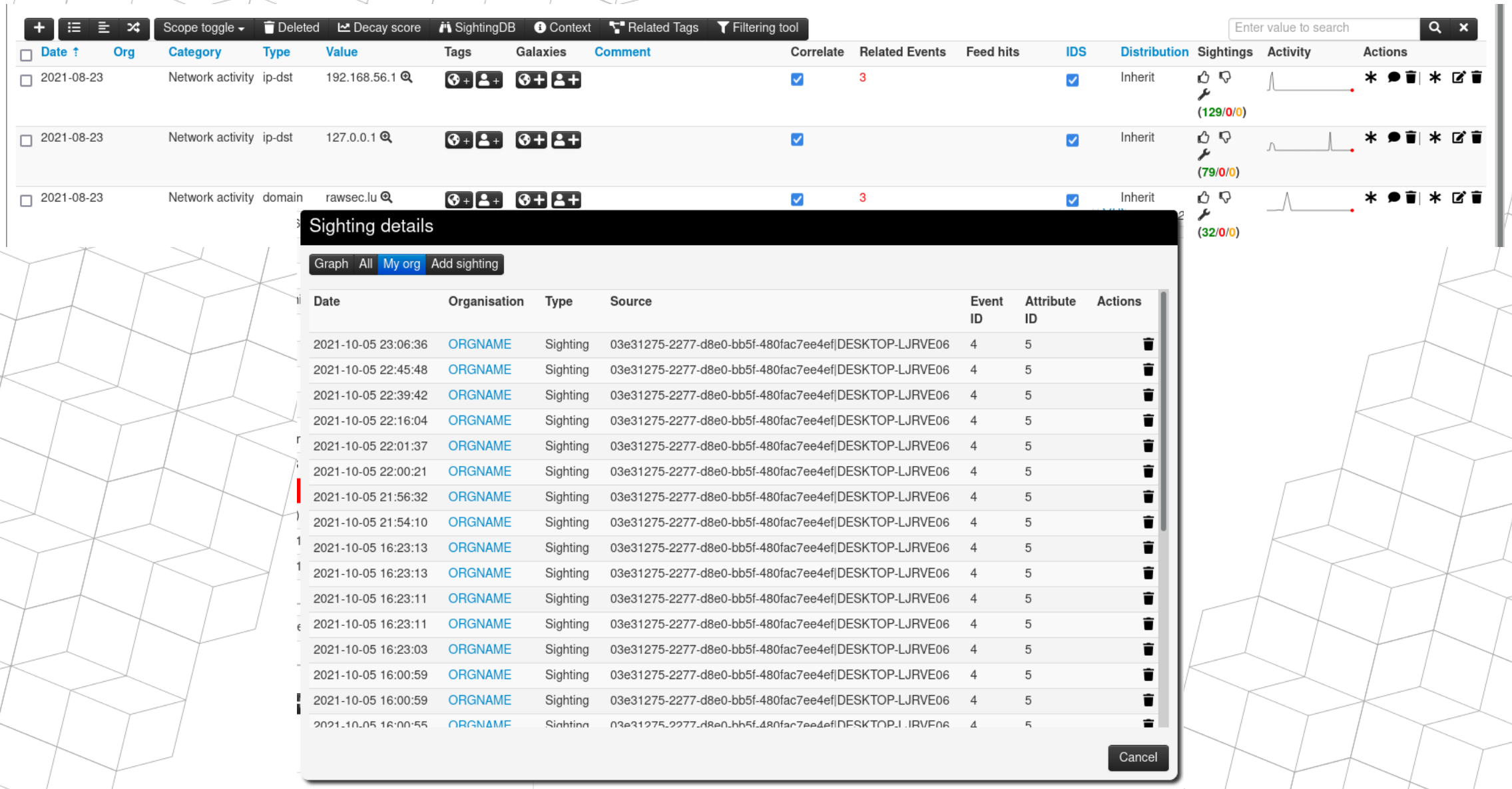
What kind of sightings ?

- md5/sha1/sha256/imphash
- domain/hostname/ip
- filepath/registries/pipes

NB: only attributes with IDS flags are updated

Source code: https://github.com/0xrawsec/pywhids/blob/master/edr-plugins/misp/sightings.py

RawSec


Scope toggle
Deleted
Decay score
SightingDB
Context
Related Tags
Filtering tool
Enter value to search
Date
Org
Category
Type
Value
Tags
Galaxies
Comment
Correlate
Related Events
Feed hits
IDS
Distribution
Sightings
Activity
Actions
2021-08-23 Network activity ip-dst 192.168.56.1 3 Inherit (129/0/0)
2021-08-23 Network activity ip-dst 127.0.0.1 Inherit (79/0/0)
2021-08-23 Network activity domain rawsec.lu 3 Inherit (32/0/0)
Sighting details
Graph
All
My org
Add sighting
Date
Organisation
Type
Source
Event ID
Attribute ID
Actions
2021-10-05 23:06:36 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 22:45:48 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 22:39:42 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 22:16:04 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 22:01:37 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 22:00:21 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 21:56:32 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 21:54:10 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 16:23:13 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 16:23:13 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 16:23:11 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 16:23:11 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 16:23:03 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 16:00:59 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
2021-10-05 16:00:59 ORGNAME Sighting 03e31275-2277-d8e0-bb5f-480fac7ee4ef|DESKTOP-LJRVE06 4 5
Cancel

News on WHIDS: IR reports

Goals

- Solve **90% of incidents** without further data acquisition. Incident Handlers can focus on the data **rather than focusing on how to get the data**
- Towards **automation driven IR**. Reports are in a standard format and contains loads of information (baseline reports -> find uncommon patterns).

Two ways to generate reports

1. Automatic: detections can trigger **reporting** actions (on to of already existing **artifacts dumping** actions)
2. On-demand: Commands can be executed on endpoints **from the manager** (hash files, un/contain host, osquery …)

What a **report** contains ?

- **processes** running, **drivers/modules** loaded, **network connections & DNS resolutions** by processes, **last files** opened … -> **instant** to generate (all in memory)
- can include the output of **any tool** (osquery, autoruns …) you like

Report example


```
{
  "Name": "UntrustedDriverLoaded",
  "Tags": [
    "DriverLoaded",
    "Sysmon"
  ],
  "Meta": {
    "Events": {
      "Microsoft-Windows-Sysmon/Operational": [
        6
      ]
    },
    "Computers": [],
    "ATTACK": [
      {
        "ID": "T1014",
        "Tactic": "Defense Evasion",
        "Reference": "https://attack.mitre.org/techniques/T1014/"
      }
    ],
    "Criticality": 10,
    "Disable": false,
    "Filter": false,
    "Schema": "2.0.0"
  },
  "Matches": [
    "$trusted: Signature ~= '^(Microsoft Windows|Microsoft Corporation)$'"
  ],
  "Condition": "!$trusted",
  "Actions": [
    "filedump",
    "report"
  ]
}
```

```
  "{515cd0d1-19df-6161-e291-000000008b00}": {
    "image": "C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe",
    "parent-image": "C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe",
    "pid": 8852,
    "command-line": "\"C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe\" /cr",
    "parent-command-line": "\"C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe\" /c",
    "cwd": "C:\\Program Files (x86)\\Google\\Update\\1.3.36.112\\",
    "parent-cwd": "C:\\Windows\\system32\\",
    "process-guid": "{515cd0d1-19df-6161-e291-000000008b00}",
    "user": "NT AUTHORITY\\SYSTEM",
    "parent-user": "NT AUTHORITY\\SYSTEM",
    "integrity-lvl": "System",
    "parent-integrity-lvl": "System",
    "parent-process-guid": "{515cd0d1-19df-6161-e191-000000008b00}",
    "services": "N/A",
    "parent-services": "N/A",
    "hashes": {
      "imphash": "7df1816239c5bc855600d41210406c5b",
      "md5": "9a66a3de2589f7108426af37ab7f6b41",
      "sha1": "12950d906ff703f3a1e0bd973fca2b433e5ab207",
      "sha256": "a913415626433d5d0f07d3ec4084a67ff6f5138c3c3f64e36dd0c1ae4c423c65"
    },
    "signature": "Google LLC",
    "signature-status": "Valid",
    "signed": true,
    "ancestors": [
      "C:\\Windows\\System32\\svchost.exe",
      "C:\\Program Files (x86)\\Google\\Update\\GoogleUpdate.exe"
    ],
    "modules": [
      {
        "image": "C:\\Windows\\System32\\ntdll.dll",
        "file-version": "10.0.18362.1 (WinBuild.160101.0800)",
        "description": "NT Layer DLL",
        "product": "Microsoft® Windows® Operating System",
        "company": "Microsoft Corporation",
        "orginal-filename": "ntdll.dll",
        "hashes": {
          "imphash": "00000000000000000000000000000000",
          "md5": "3239d9cdc68757ab4620b3ac127e18c5",
          "sha1": "c5085044059f466df8c513b615aaf2f43dcd2ada",
          "sha256": "d6da3bb97f6839436a9399d087138ca44b50e5674c4c8093ce41a4c1658c7259"
        },
        "signature": "Microsoft Windows",
        "signature-status": "Valid",
        "signed": true,
        "load-count": 951,
        "first-load": "2021-10-04T20:42:45.2523525Z",
        "last-load": "2021-10-05T15:23:02.8280276Z"
      },
```

New Integration: reporting.py

Goal: periodically push IR reports received by EDR manager to MISP

Motivation: enable detection reports sharing

How it works

- Upload only detections which triggered a report generation
- Upload any associated artifact collected (files, registry) except process memory dump (too big)
- **One** MISP object (edr-report) per report -> several edr-report objects per MISP event (**one** event created per day)

Source code:https://github.com/0xrawsec/pywhids/blob/master/edr-plugins/misp/reporting.py

RawSec

2021-09-28	**Object name:** edr-report **References:** 0						
2021-09-28	Other	**id:** text	1742c52bb81e525c9b7dbb87ed661ecd8c416352			Unique event identifier	☑	
2021-09-28	Other	**endpoint-id:** text	03e31275-2277-d8e0-bb5f-480fac7ee4ef			Unique endpoint identifier	☑	42
2021-09-28	Network activity	**ip:** ip-src	192.168.56.110			Endpoint IP address	☐	
2021-09-28	Other	**hostname:** text	DESKTOP[redacted]			Endpoint hostname	☑	42
2021-09-28	Other	**comment:** text	Event triggering Builtin:CanaryAccessed caught on endpoint				☐	
2021-09-28	Other	**product:** text	WHIDS			EDR product name	☐	
2021-09-28	External analysis	**event:** attachment	event.json			Report generation trigger	☐	
2021-09-28	External analysis	**processes:** attachment	processes.json			Running process snapshot at detection time	☐	
2021-09-28	External analysis	**modules:** attachment	modules.json			Ever loaded modules since boot until detection time	☐	
2021-09-28	External analysis	**drivers:** attachment	drivers.json			Ever loaded drivers since boot until detection time	☐	
2021-09-28	External analysis	**command:** attachment	command.json			OSQuery processes table	☐	

Latest News

- **PyWHIDS**: python library to interface with WHIDS (work in progress) -> used by **sightings.py** and **reporting.py**
- Uses **ETW logs** as event source -> more logs, less resources and higher throughput
- Improved admin API on manager's side
- Event streaming through Websocket
  - Pretty cool feature to implement any plugin needing to receive logs in realtime
- New commands supported by agent (hash, find, report …)
- Completely new way to index logs on manager making event retrieval very fast
- Use of an ORM like framework (homemade ☺) for manager's data persistence

RawSec

Thank you all !

Special thanks to @adulau, @gallypette and another anonymous supporter for believing in this project since the beginning and for boosting up my motivation

Contact via Twitter/Github **@0xrawsec**

Feel free to open issues, ask questions, give feedbacks/suggestions …

References:

- WHIDS: https://github.com/0xrawsec/whids
- PyWHIDS: https://github.com/0xrawsec/pywhids
- Golang-etw: https://github.com/0xrawsec/golang-etw
- Gene: https://github.com/0xrawsec/gene
- Gene rules: https://github.com/0xrawsec/gene-rules
- Gene Documentation: https://rawsec.lu/doc/gene/2.0