IntelOwl Project

making the life of cyber security analysts easier

HackInBo '23

$ say hi to the team :)

Matteo Lodi

@matte_lodi

mlodic

Simone Berni

@0ssig3no

0ssigeno

certego

Threat Intelligence Team

Is it cool to work in Cyber Security?

- Higher pay grades
- Fast career paths
- Never-ending learning jobs
- Challenging
- Ethical

ref: Fortune

ref: Enisa

Is it cool to work in Cyber Security?

- Higher pay
- Fast career
- Never-endi
- Challenging
- Ethical

CAREER GUIDES RANKINGS MORE

R WAGES

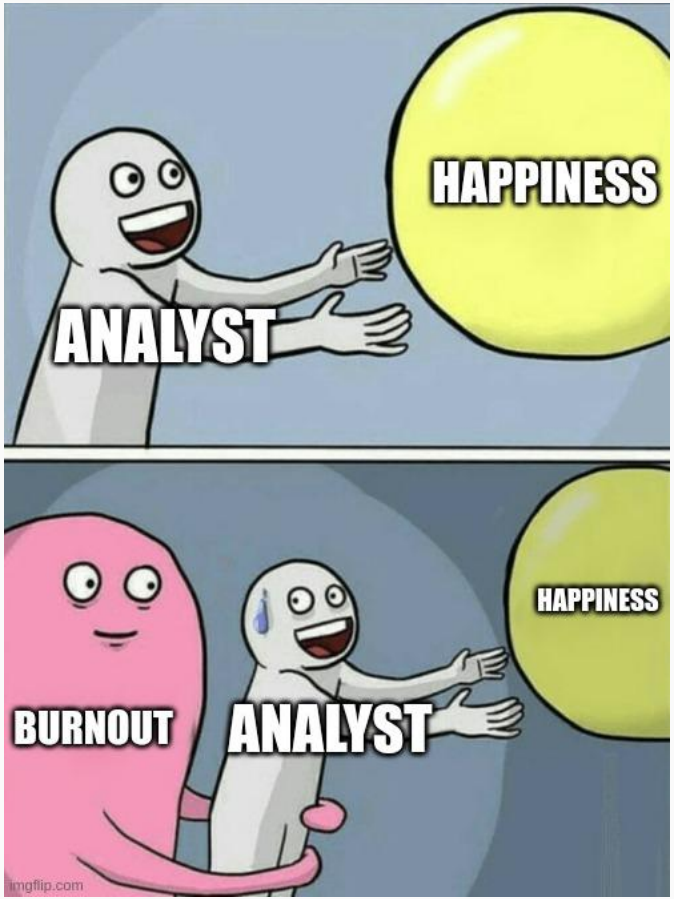
y industry
n workers
ws for cyber

nderstanding the
EU

number in the next 2-3 years as
by European Union Agency for

ref: Enisa

Unveil the reality



Unveil the reality

Cyber security analysts are:

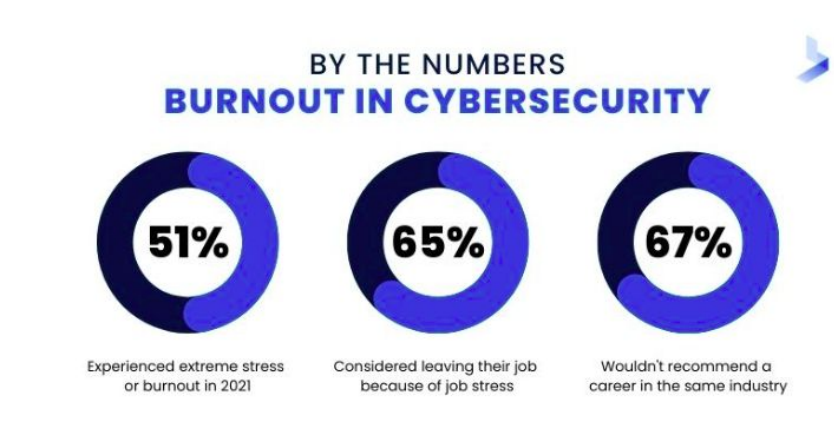
- understaffed
- overworked
- working 24/7
- without work-life balance
- used as scapegoats
- **do a lot of manual work**

  which could be automated

Cybersecurity burnout is real. And it's going to be a problem for all of us

Burnout might be the most critical cybersecurity risk facing organizations in 2022. So, how do we tackle it?

ref: ZDNet



ref: Bitlyft

Automate, automate, automate

2017:

- Working in a little team of cyber security analysts
- Overwhelmed by security alerts
- Burnt-out myself

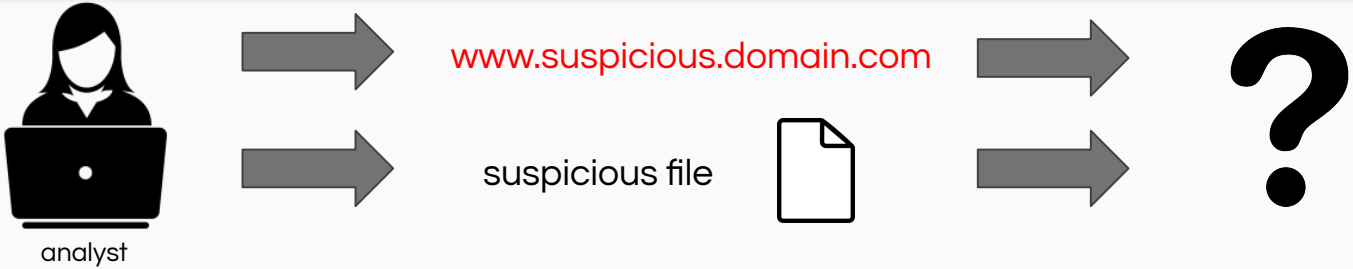
Automate, automate, automate

2017:

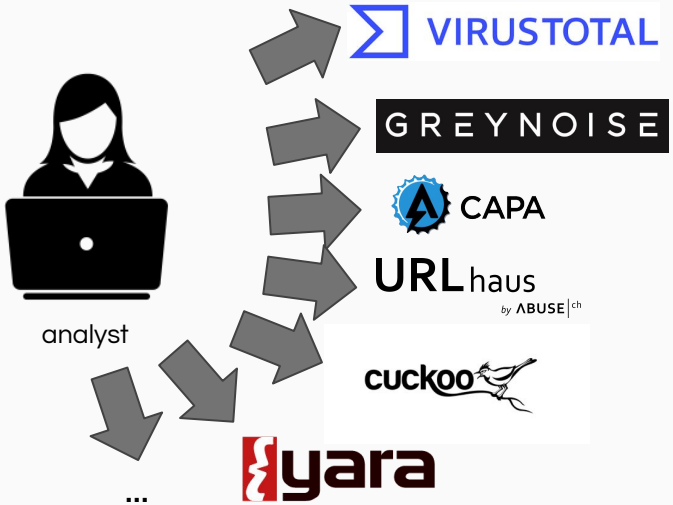
- Working in a little team of cyber security analysts
- Overwhelmed by security alerts
- Burnt-out myself

We needed to start to **automate** our most common workflows.

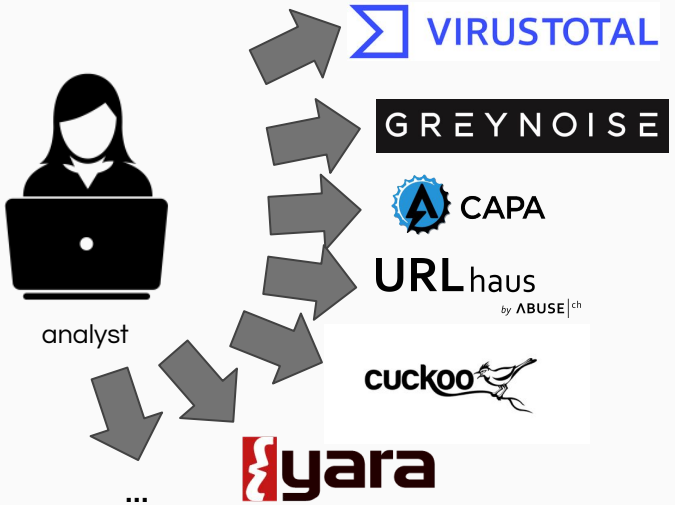
The bottleneck: acquisition of threat intelligence context

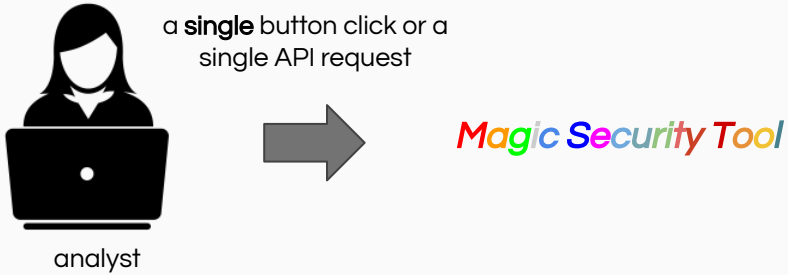


The bottleneck: acquisition of threat intelligence context



The bottleneck: acquisition of threat intelligence context





We were looking for a tool

Our requirements were:

We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface

We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface
- Client library for easy integrations with other security tools
- High possibility of customization to allow different use cases

We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface
- Client library for easy integrations with other security tools
- High possibility of customization to allow different use cases
- High level of scalability and speed
- Open source

We were looking for a tool

Our requirements were:

- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface
- Client library for easy integrations with other security tools
- High possibility of customization to allow different use cases
- High level of scalability and speed
- Open source
- Written with the most recent technologies
- Well maintained and updated

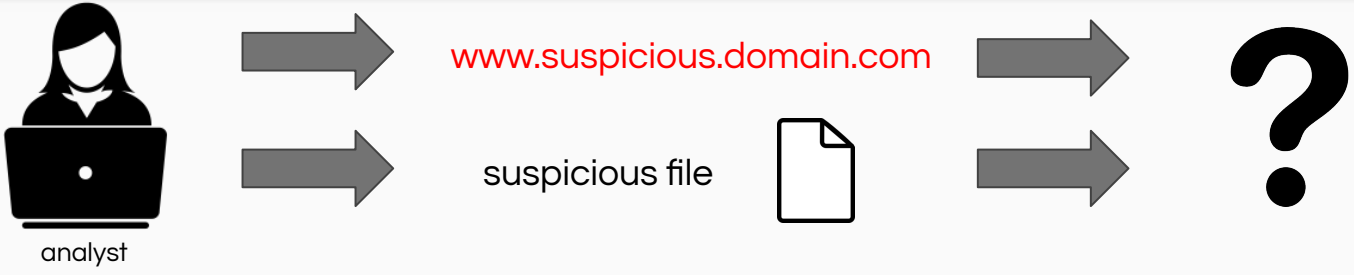
IntelOwl was born

Intel owl

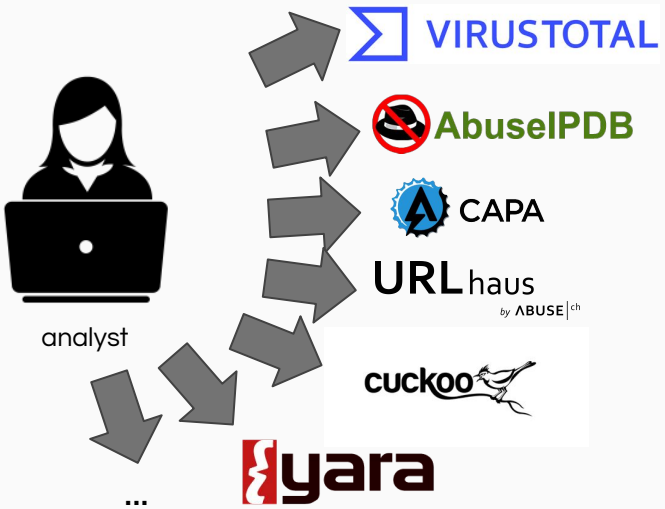
Born in Certego at the start of 2020, it is a great example of a successful Open Source project: right now it is one of the most popular Threat Intel projects on GitHub (>2.8k stars).

IntelOwl provides data **enrichment** of threat intel artifacts (IP, Domain, URL, files, PCAP, hash, etc).

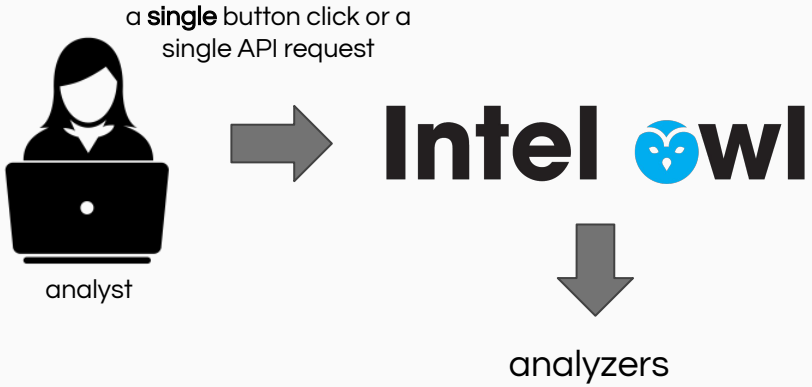
IntelOwl solution



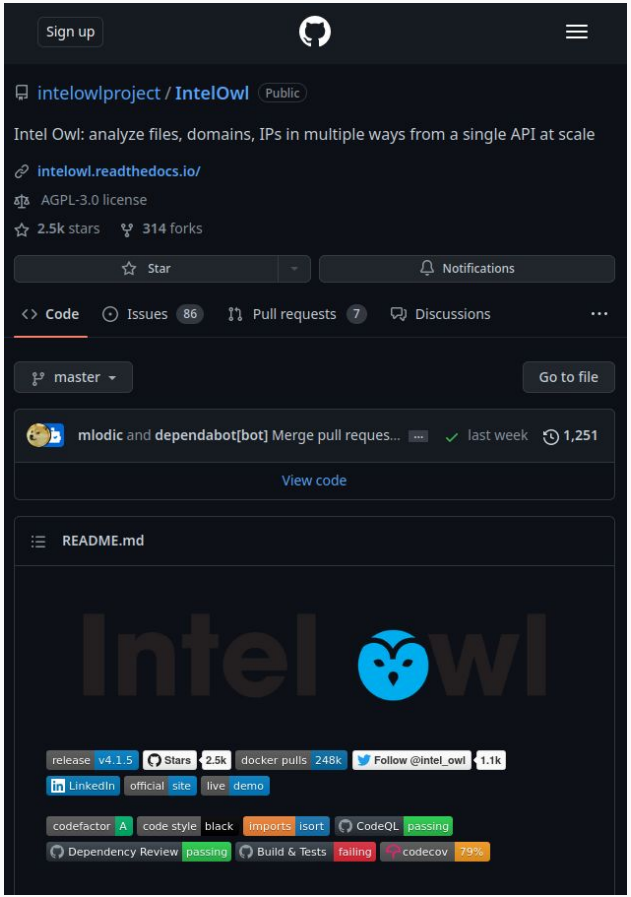
WithOUT Intel Owl



With Intel Owl



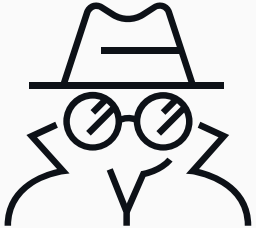
IntelOwl Repository & Tech Stack



The most common (and open source) technologies and framework are used and we keep them constantly updated:

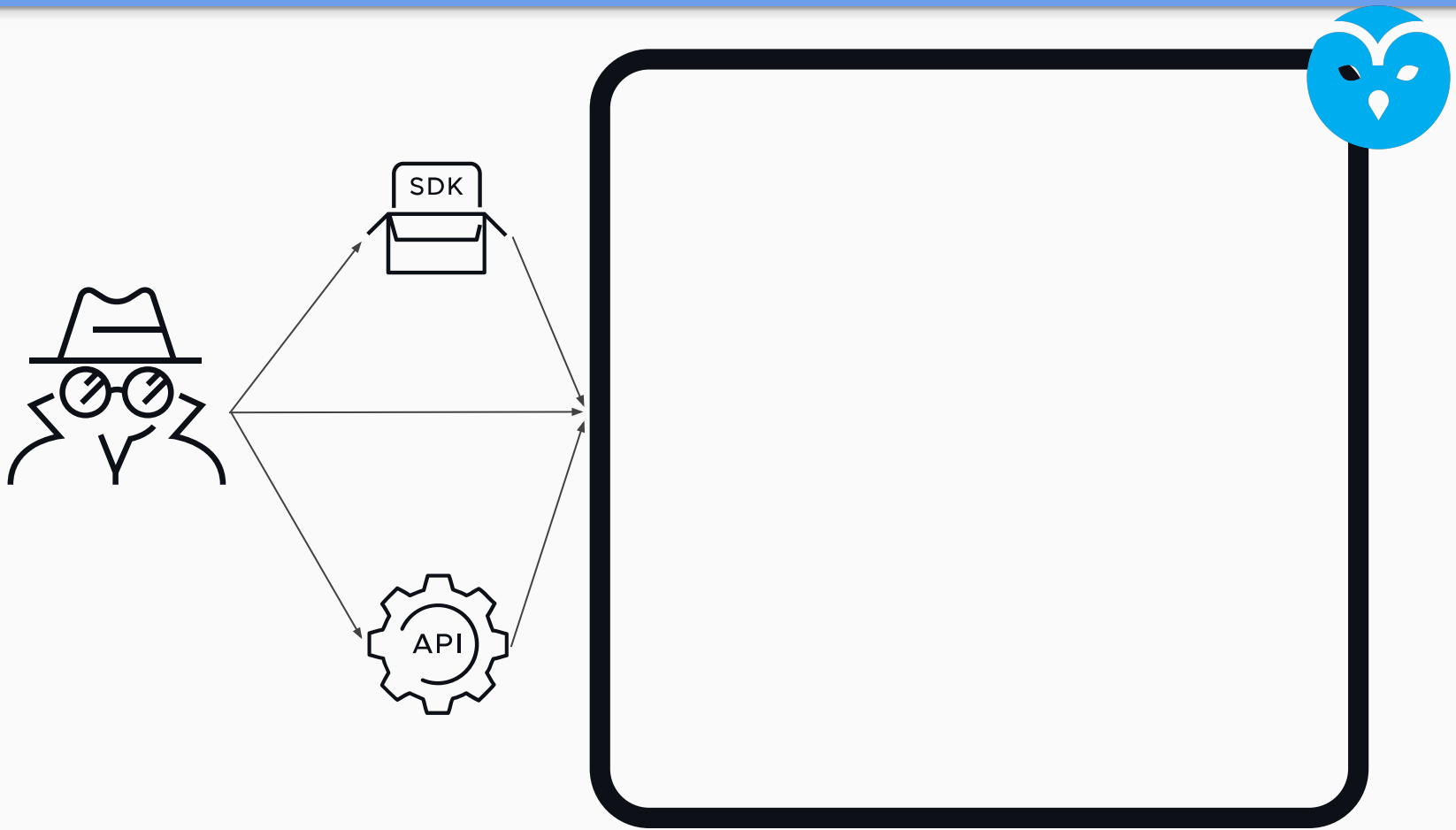
- Docker
- Python
- Django
- Django Rest Framework
- PostgreSQL
- ElasticSearch
- Nginx
- Uwsgi
- Rabbit-MQ/SQS
- ReactJS
- Celery

IntelOwl: Infrastructure Architecture

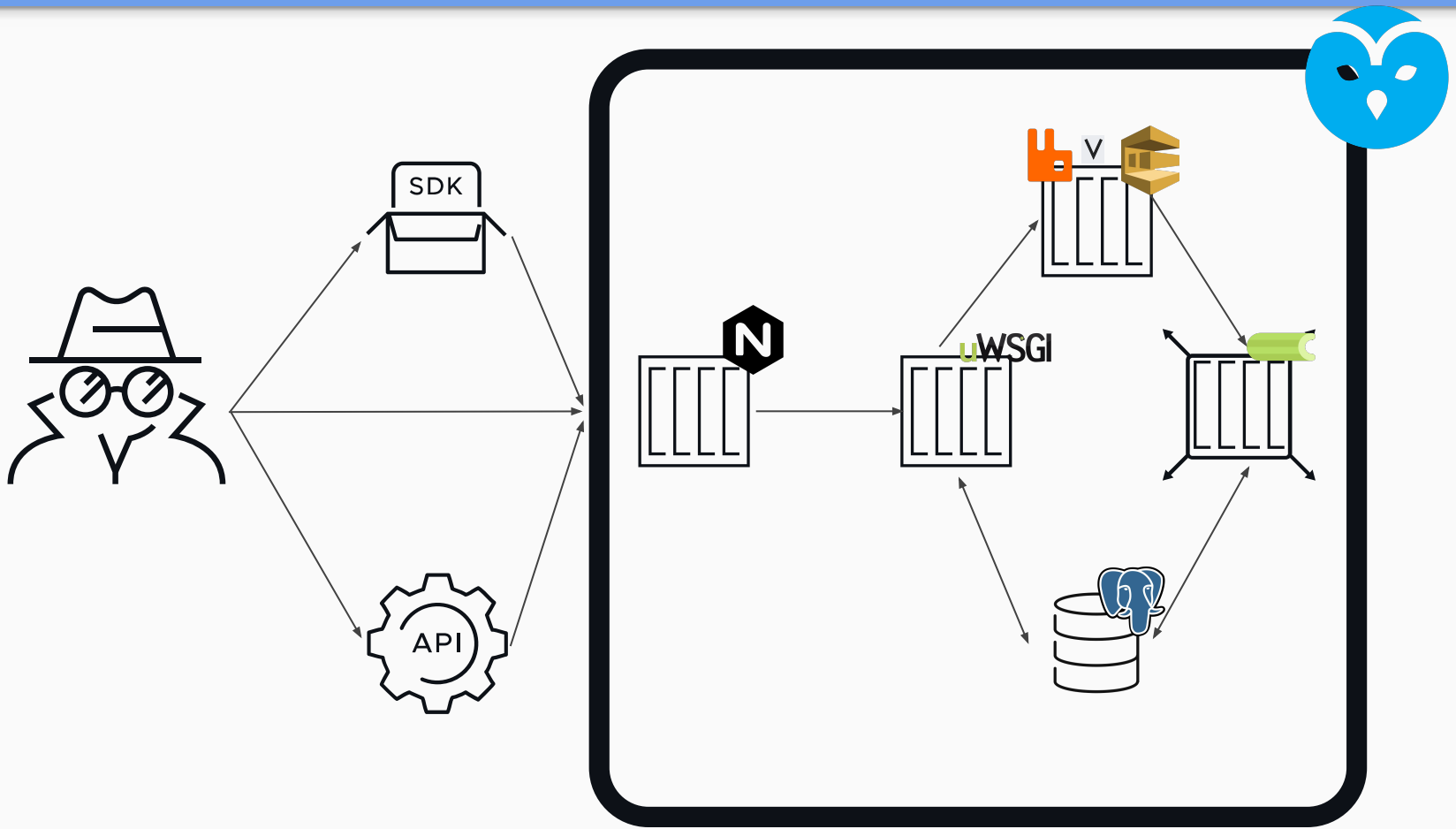


Analyst

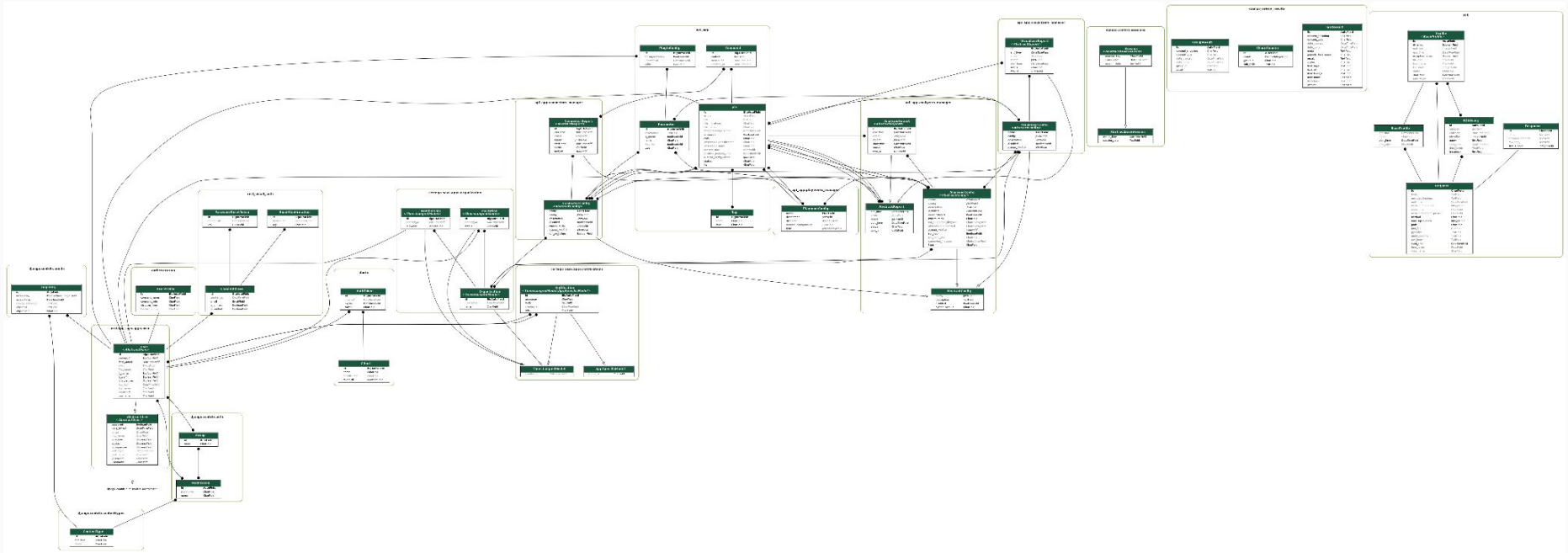
IntelOwl: Infrastructure Architecture



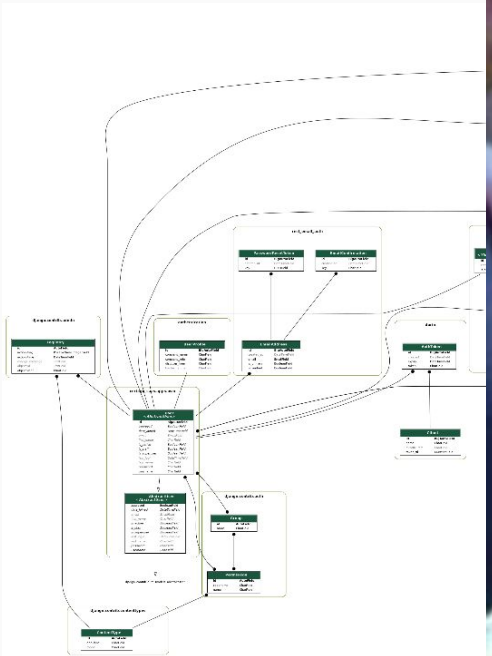
IntelOwl: Infrastructure Architecture

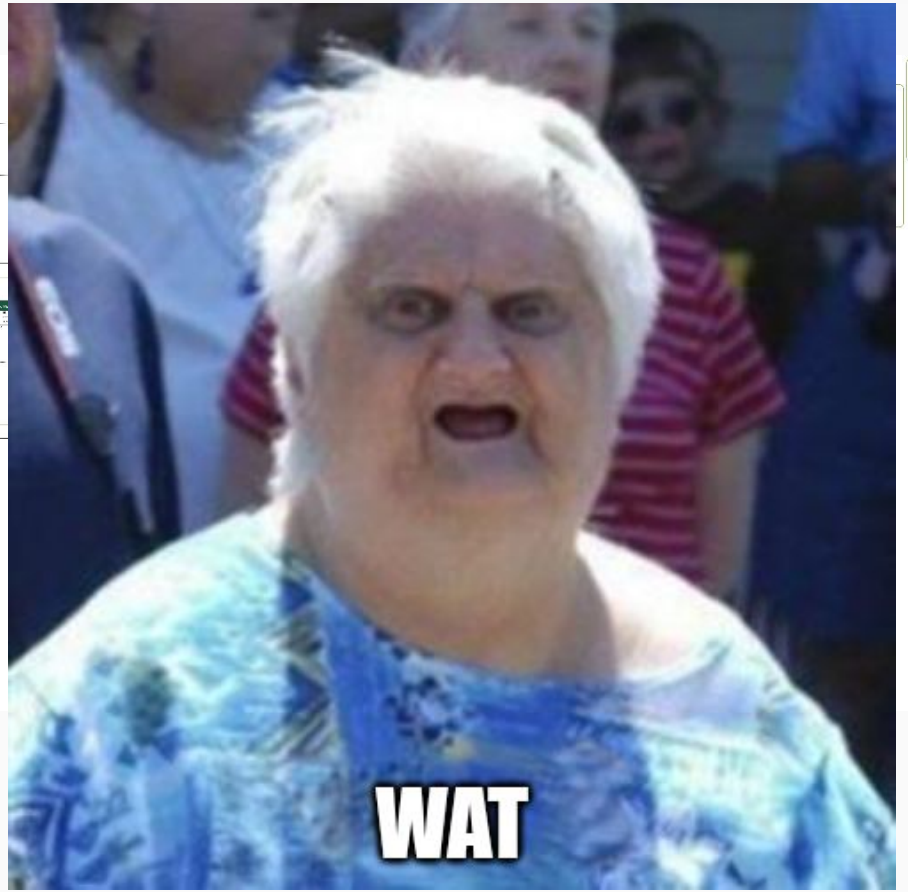


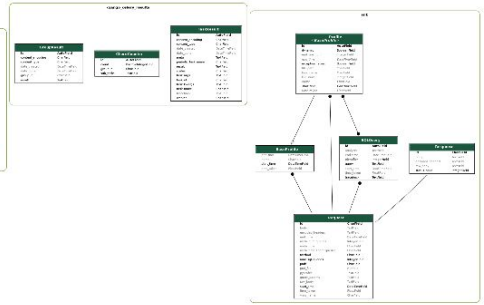
IntelOwl: Software Architecture



IntelOwl: Software Architecture





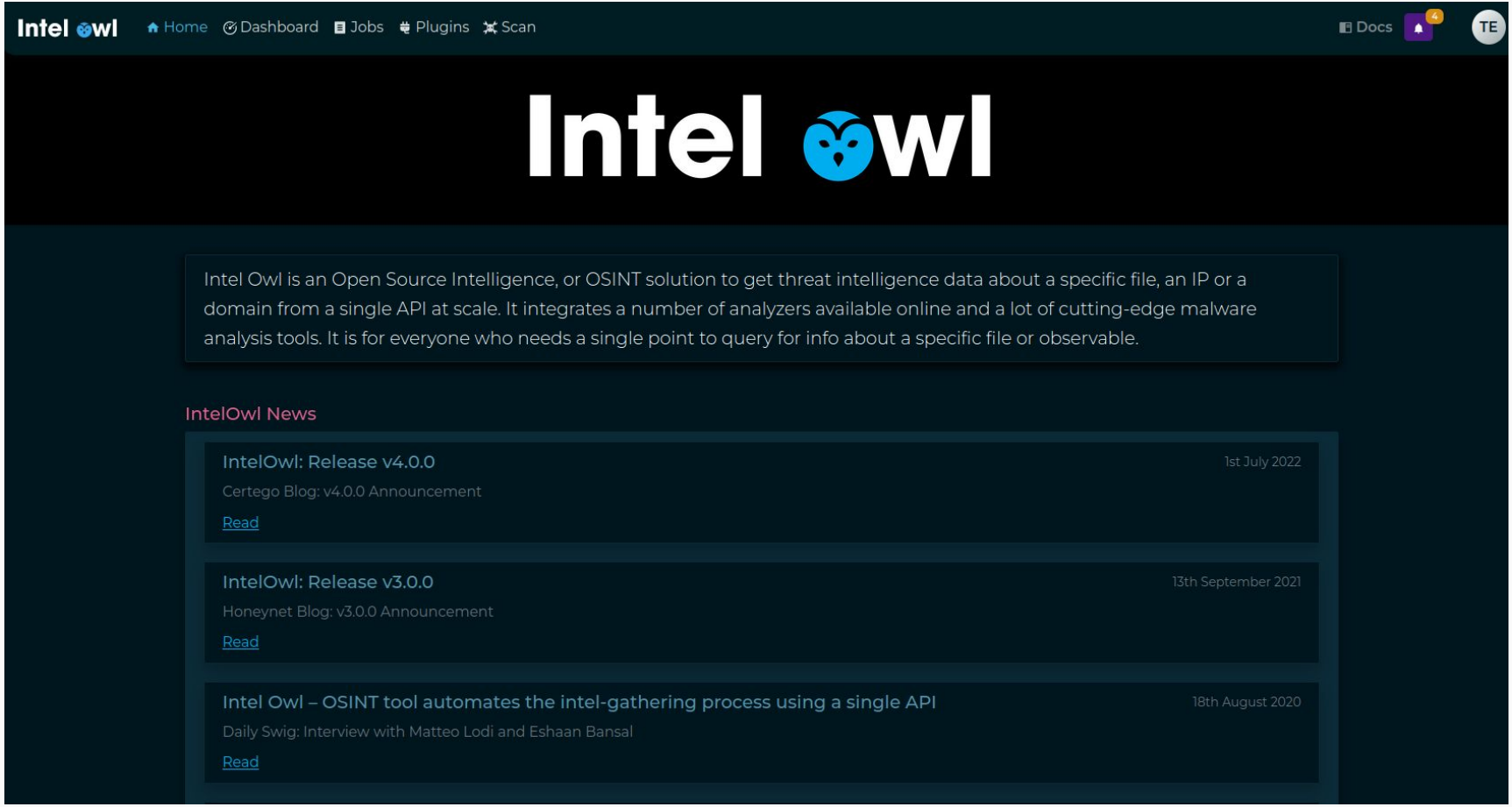


IntelOwl: Installation

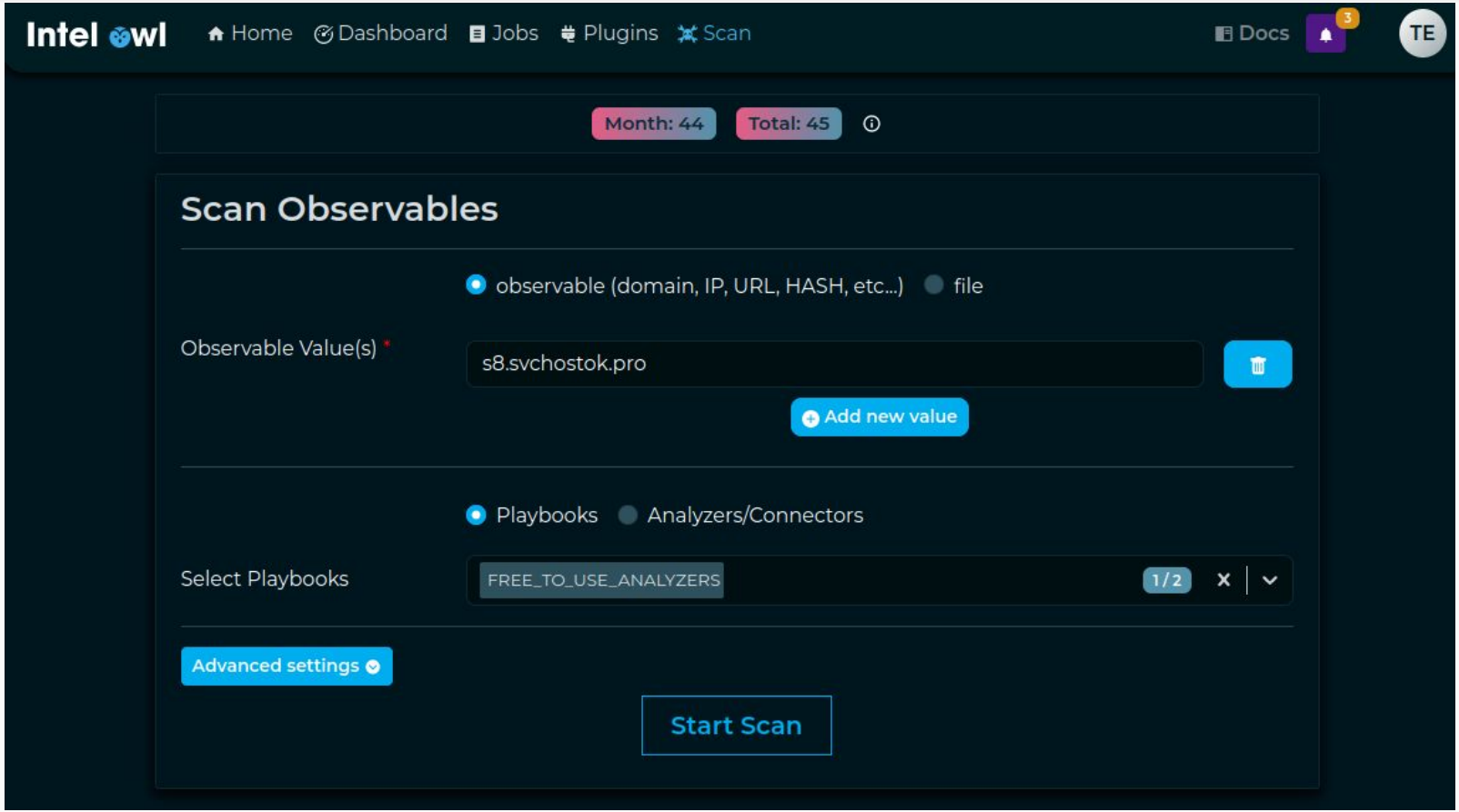
Easy and fast steps. Follow the official documentation (which we strive to keep up to date):

```
git clone https://github.com/intelowlproject/IntelOwl
cd IntelOwl/

# construct environment files from templates
cd docker/
cp env_file_app_template env_file_app
cp env_file_postgres_template env_file_postgres
cp env_file_integrations_template env_file_integrations

# (optional) verify installed dependencies
cd ..
./initialize.sh

# start the app
python3 start.py prod up

# create a super user
docker exec -ti intelowl_uwsgi python3 manage.py createsuperuser


# now you can login with the created user http://localhost:80

# Have fun!
```

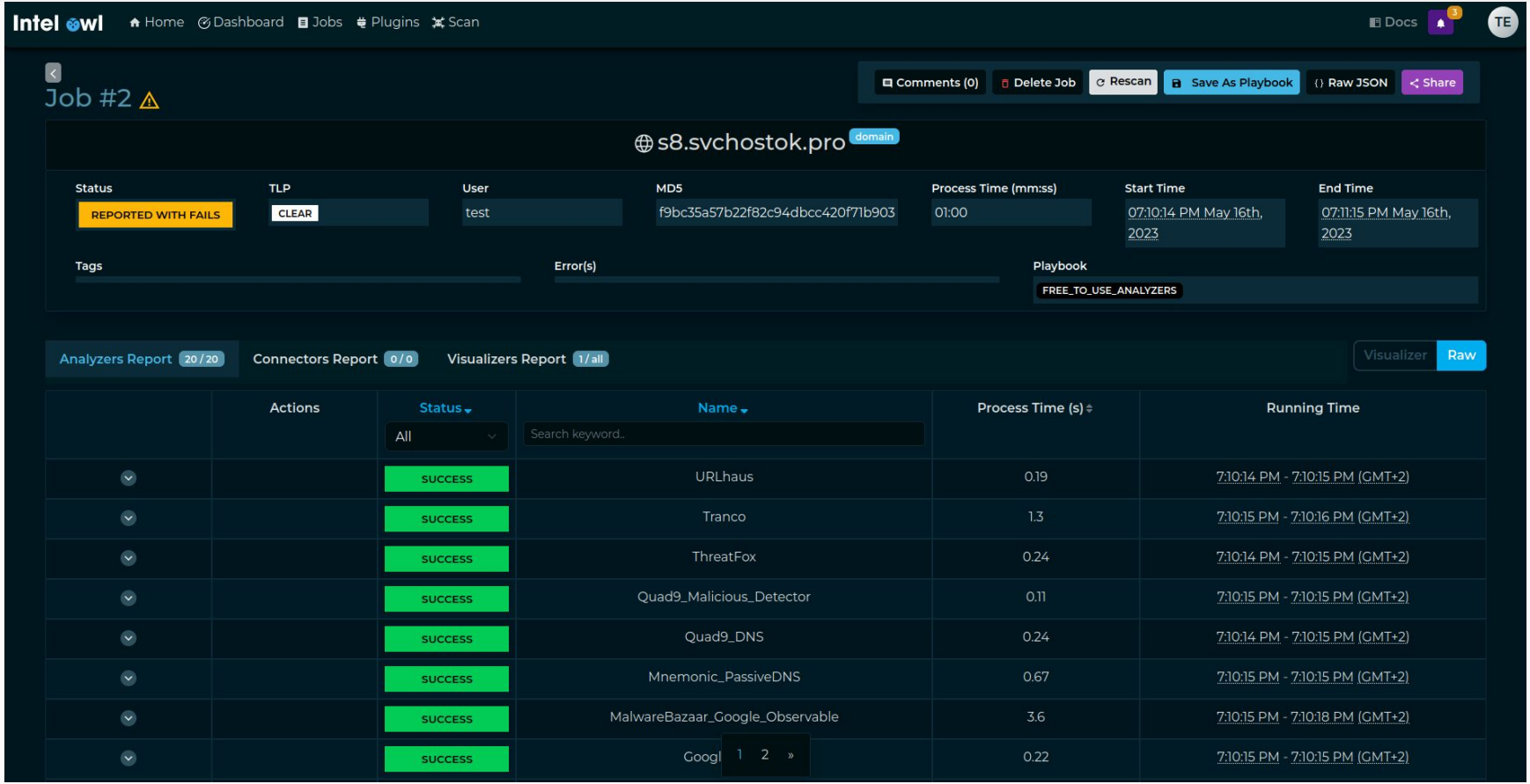
IntelOwl: Homepage



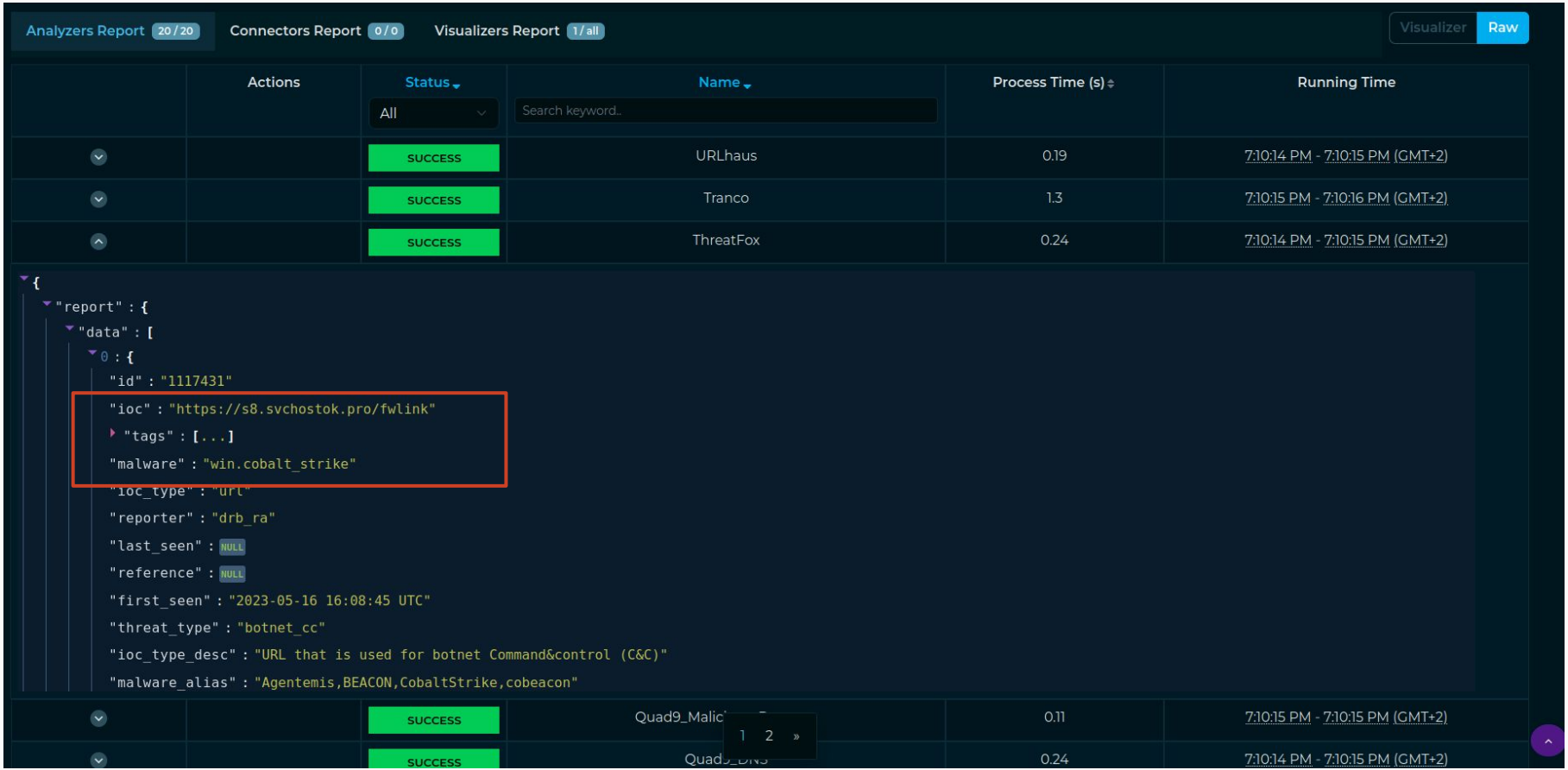
IntelOwl: Scan Page



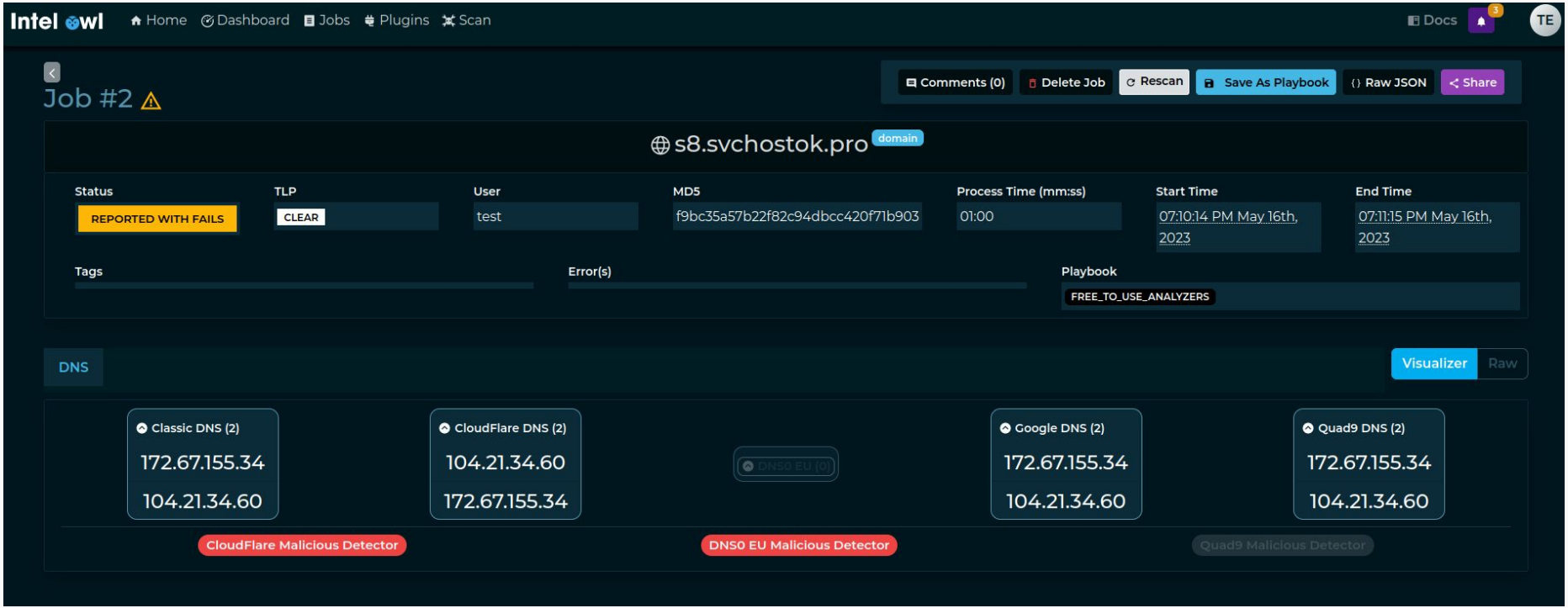
IntelOwl: Job Result (Raw Data) 1/2



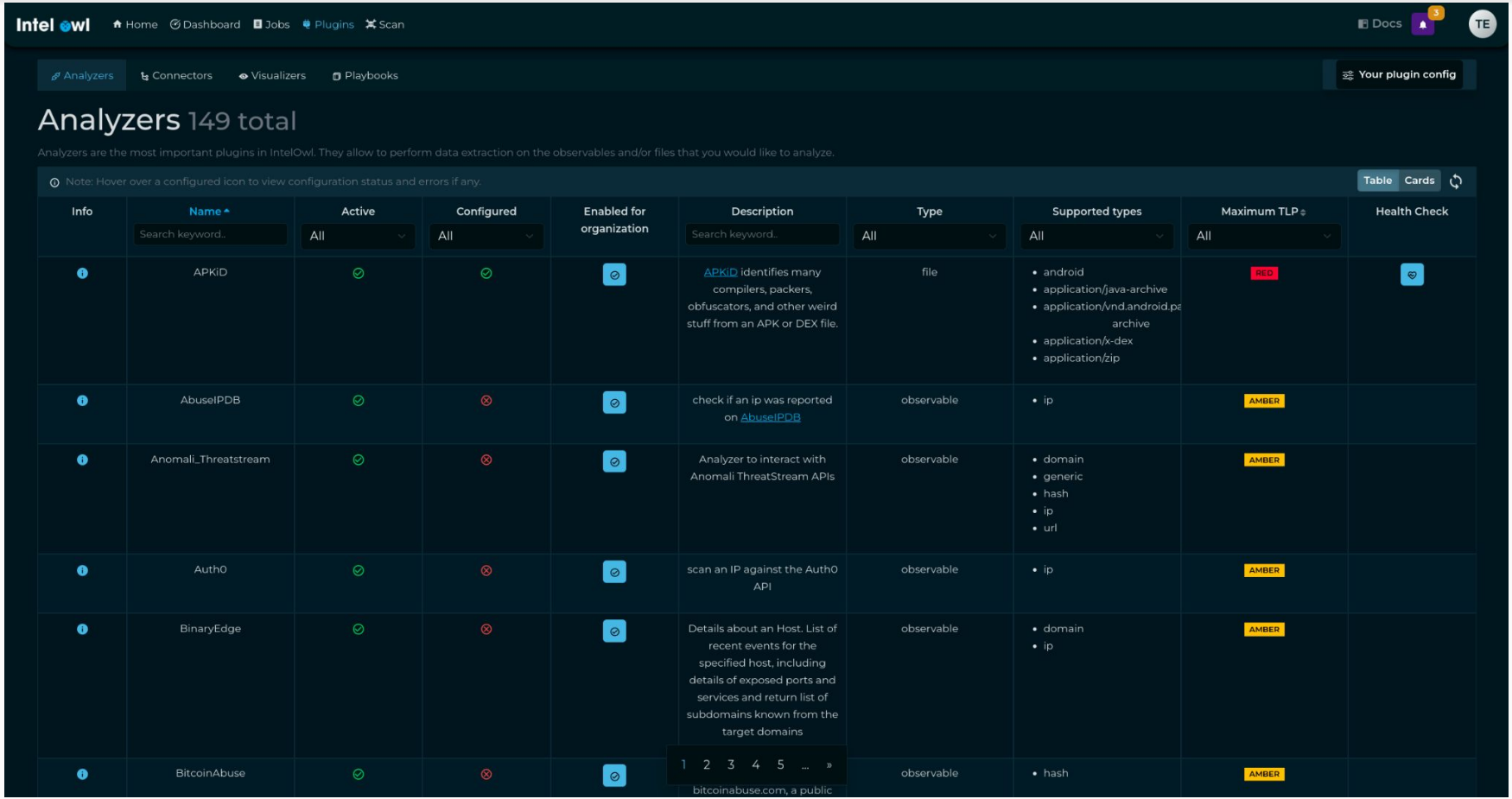
IntelOwl: Job Result (Raw Data) 2/2



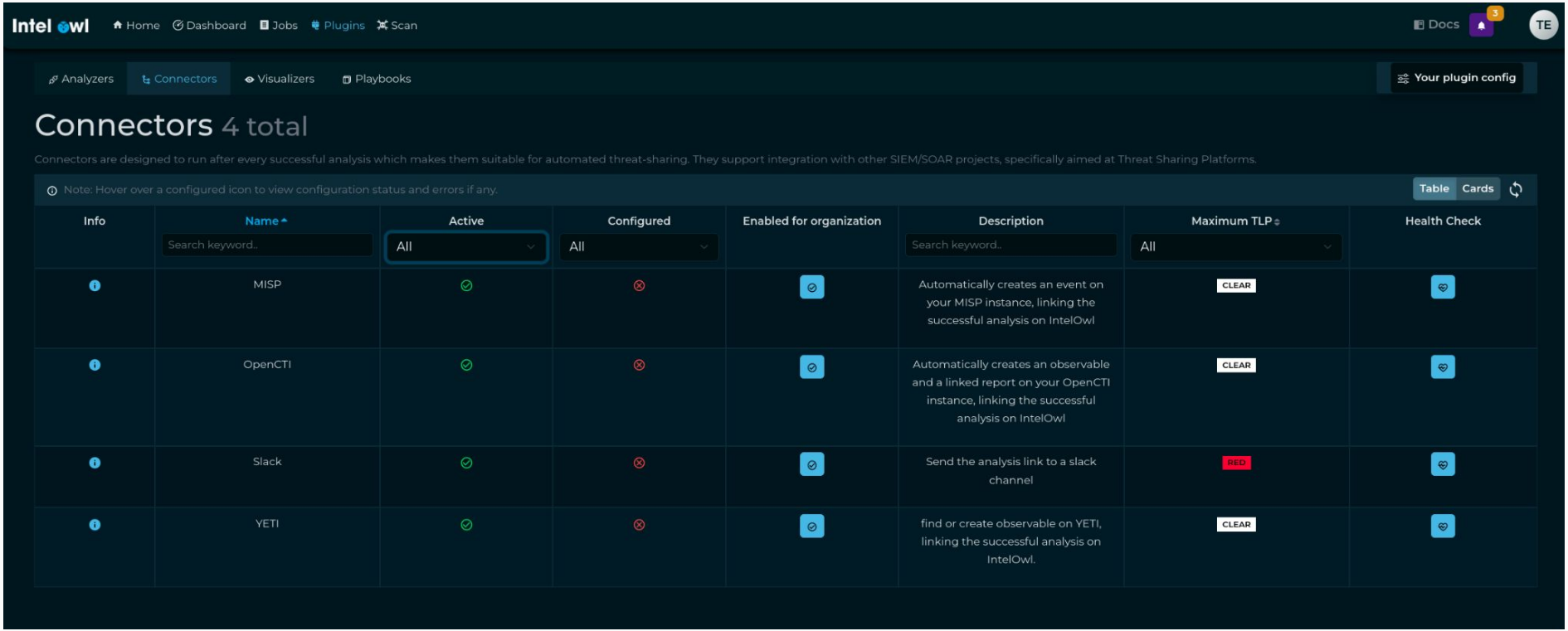
IntelOwl: Job Result (Visualizers)



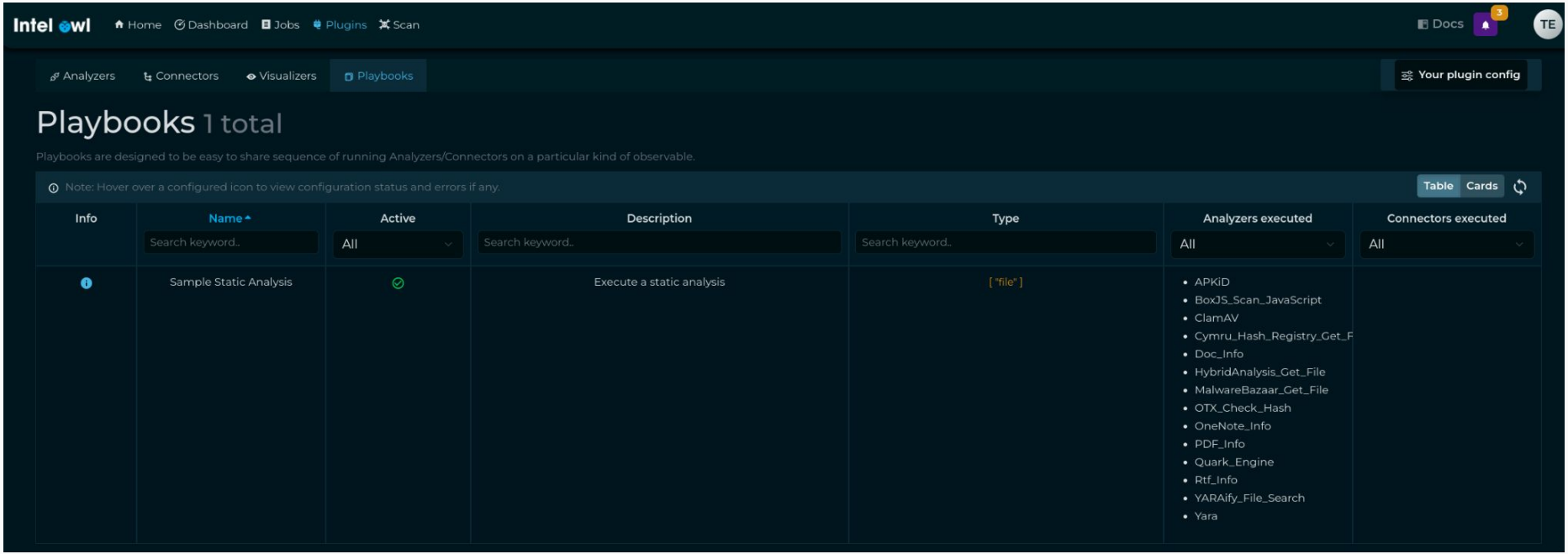
IntelOwl: Plugins (Analyzers)



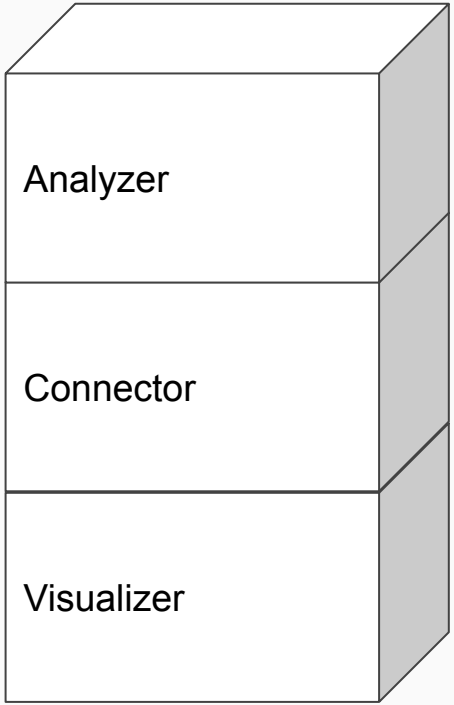
IntelOwl: Plugins (Connectors)



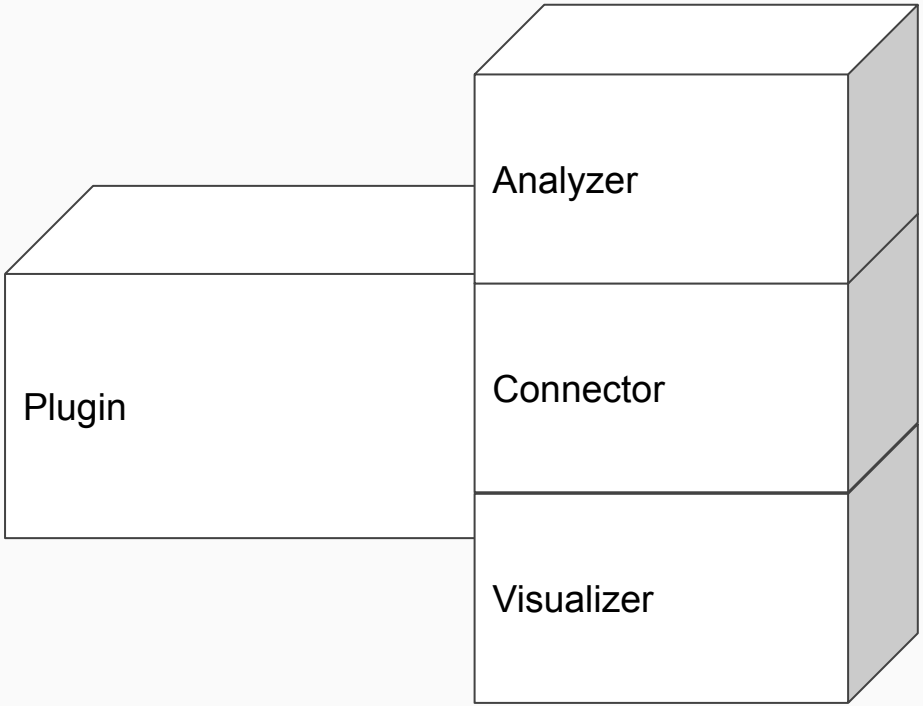
IntelOwl: Plugins (Playbooks)



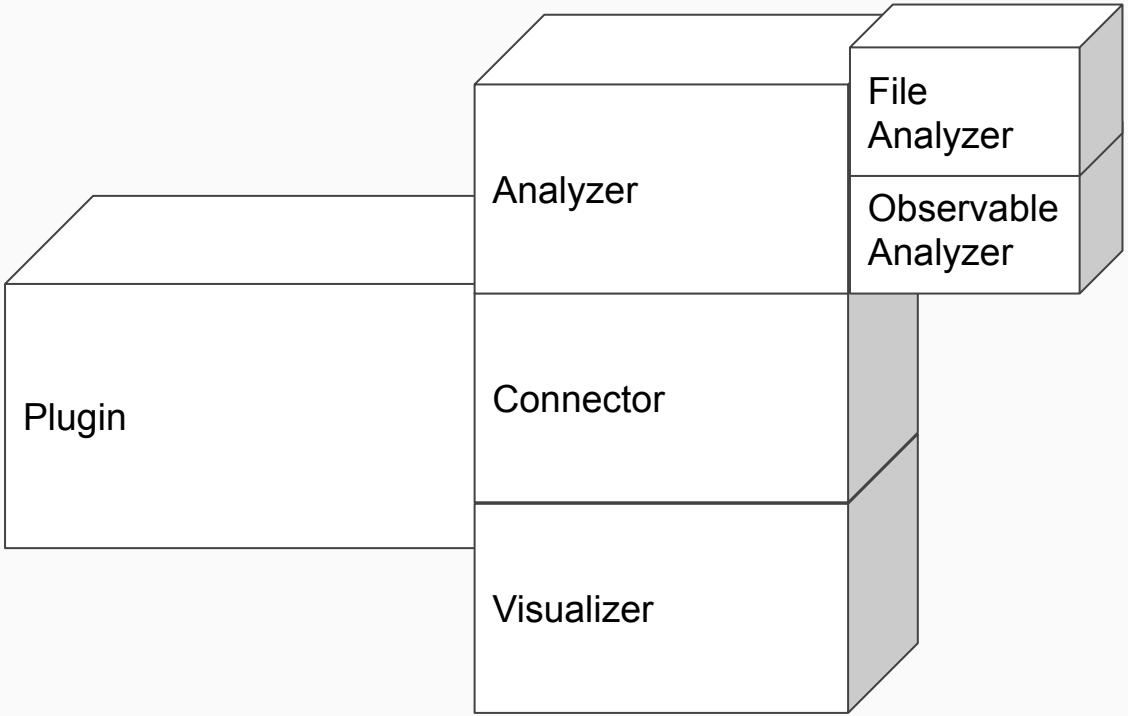
IntelOwl: Plugins



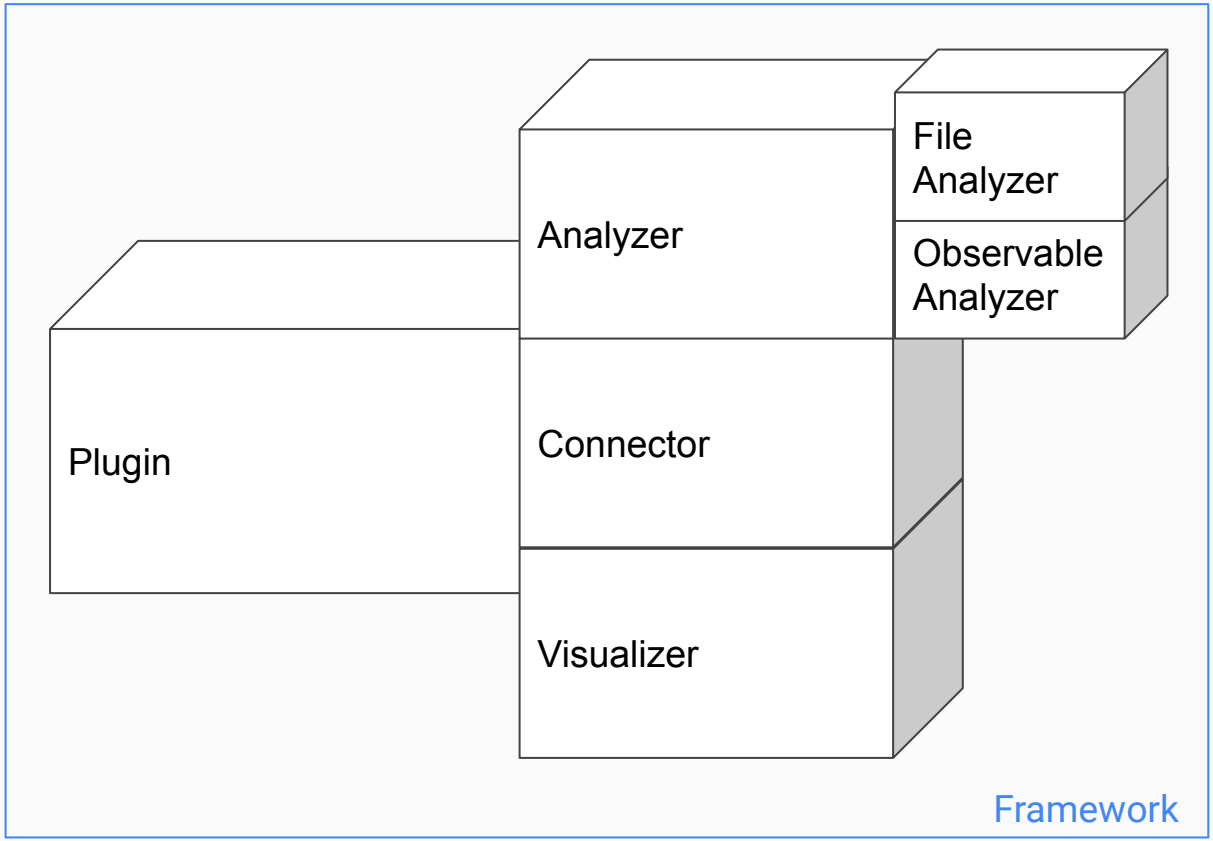
IntelOwl: Plugins



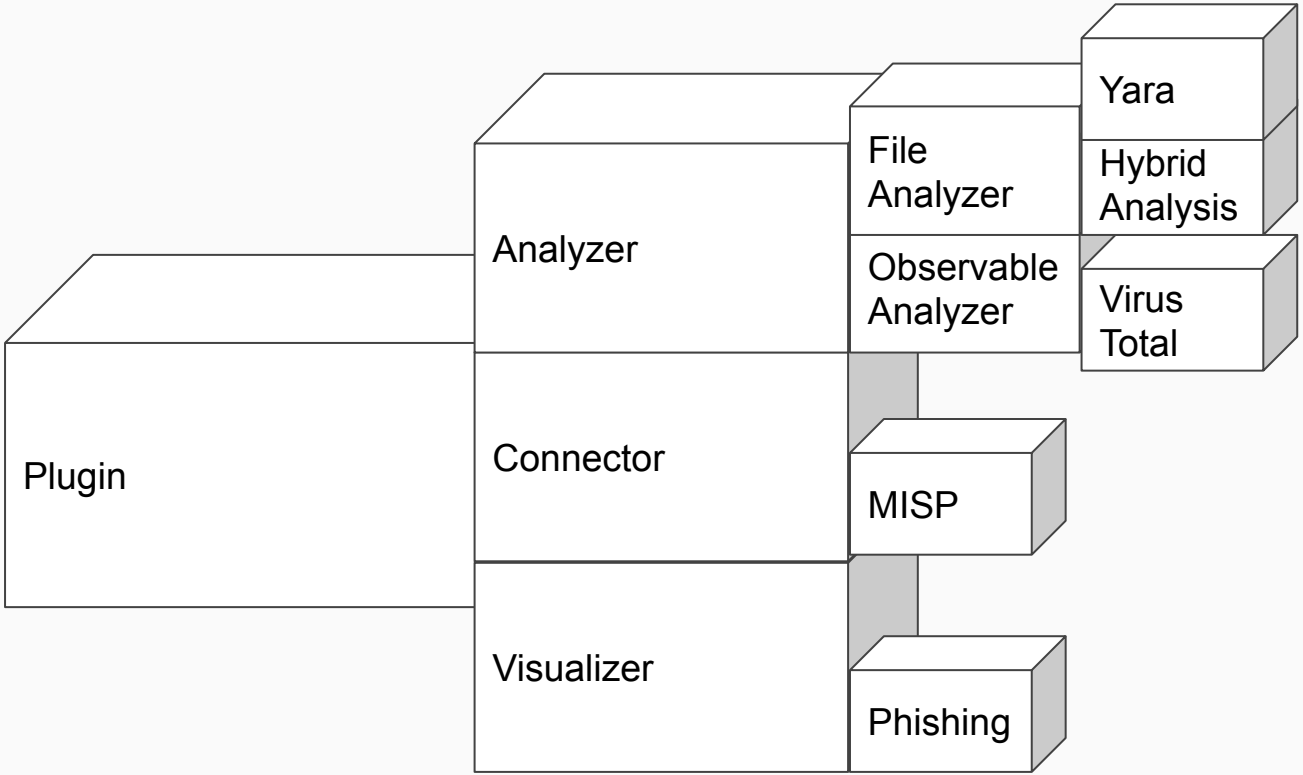
IntelOwl: Plugins



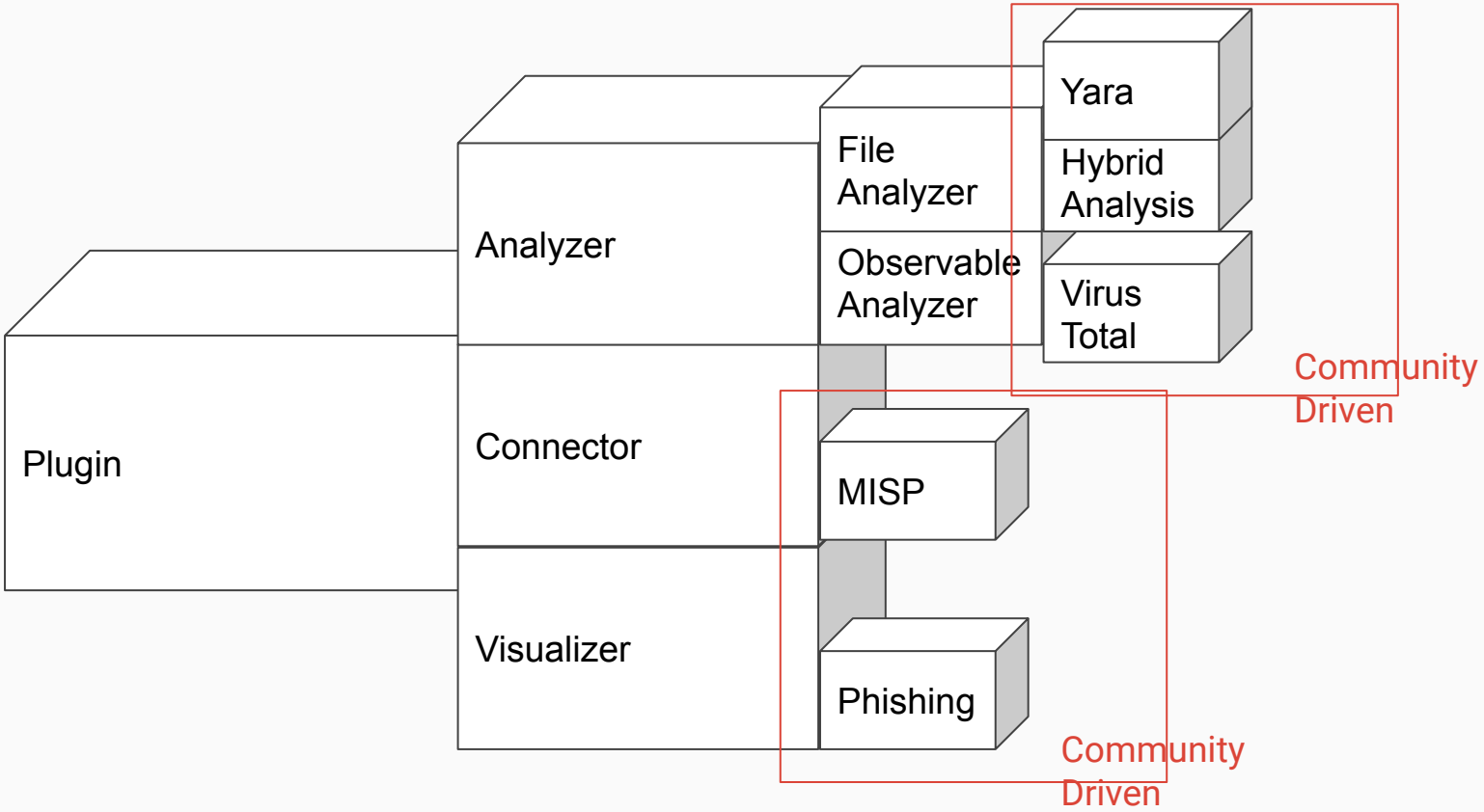
IntelOwl: Plugins



IntelOwl: Plugins



IntelOwl: Plugins



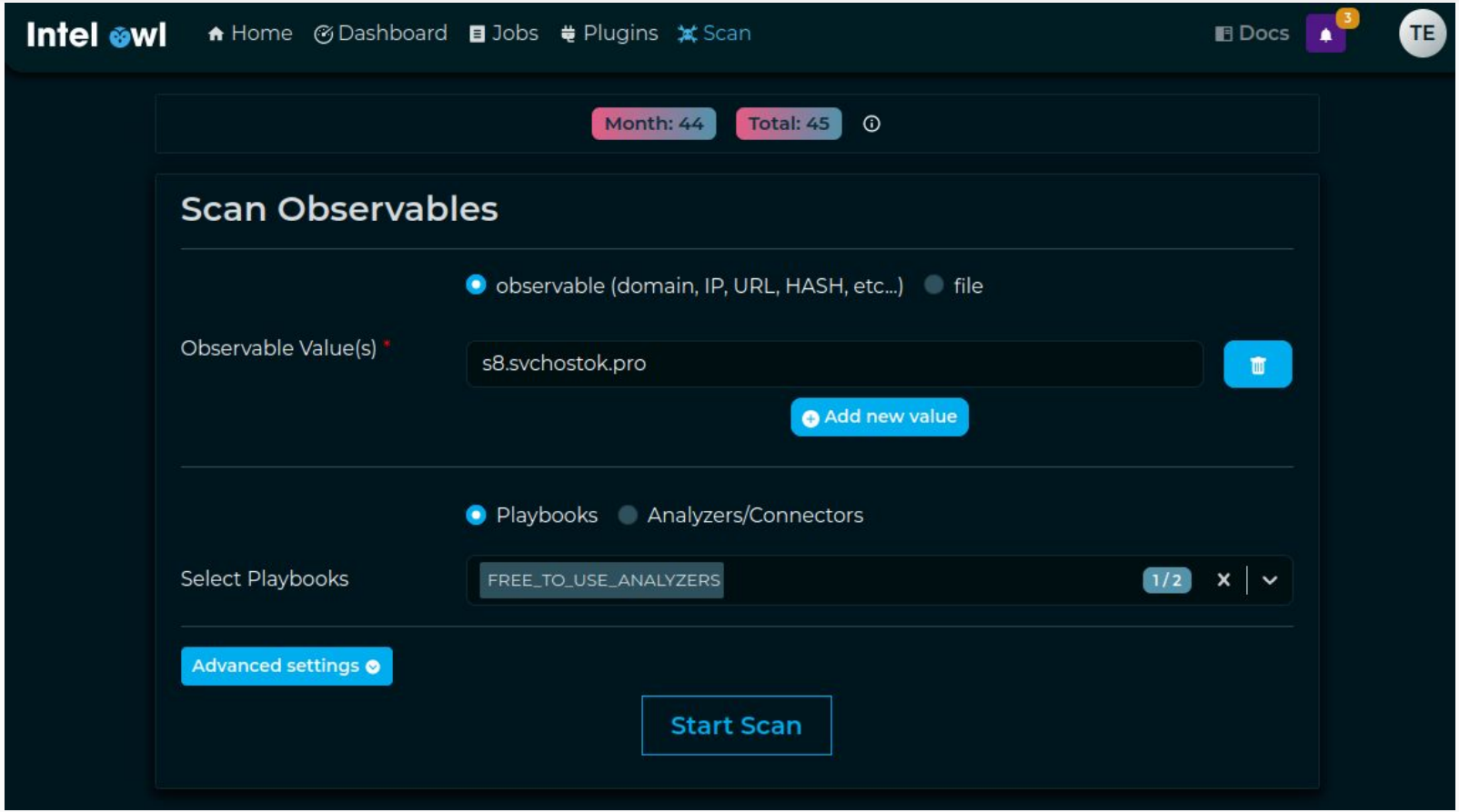
IntelOwl: Plugins

Plugin

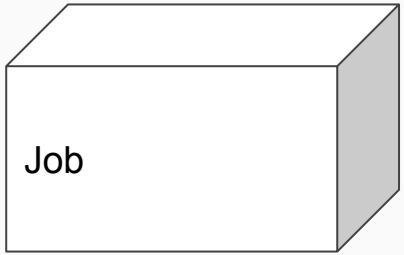
Community Driven

Driven

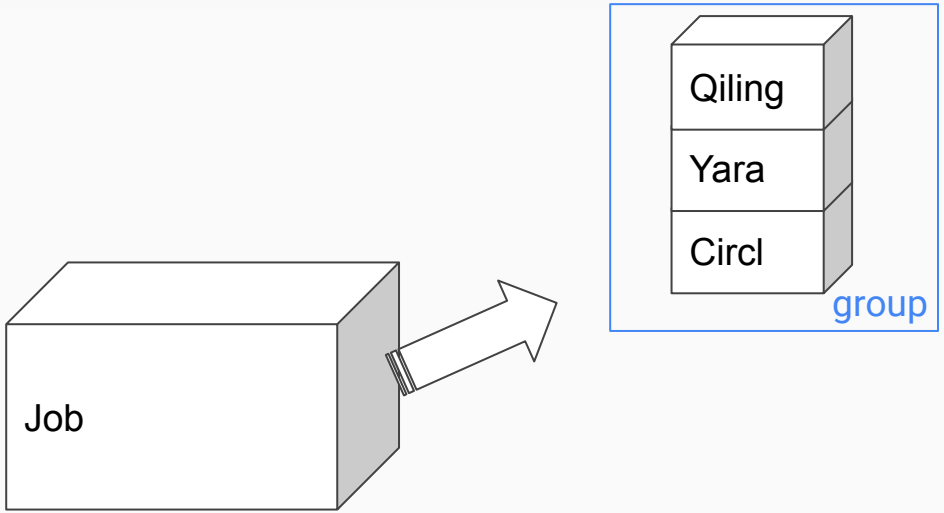
IntelOwl: Scan Page



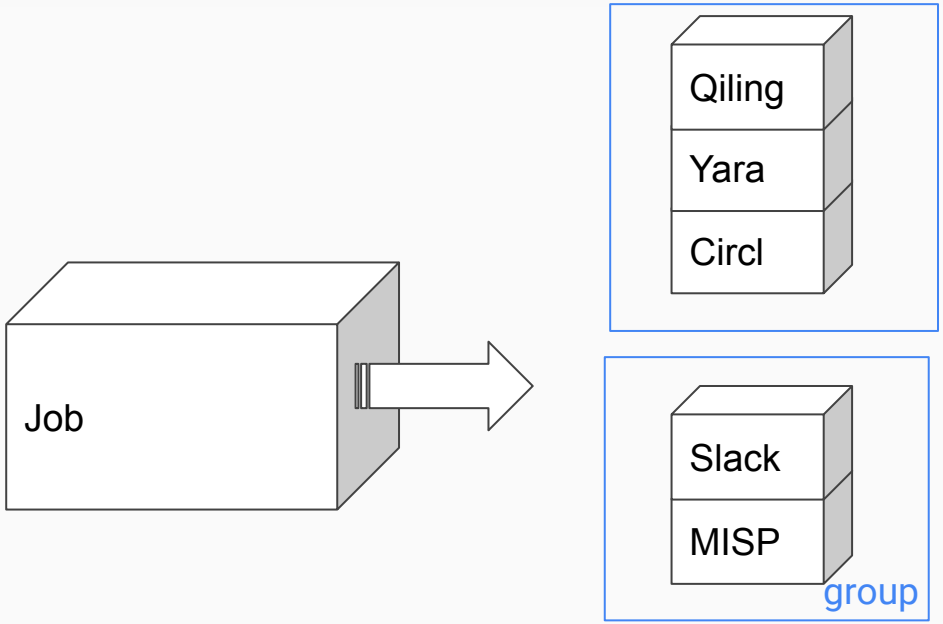
IntelOwl: Software Architecture



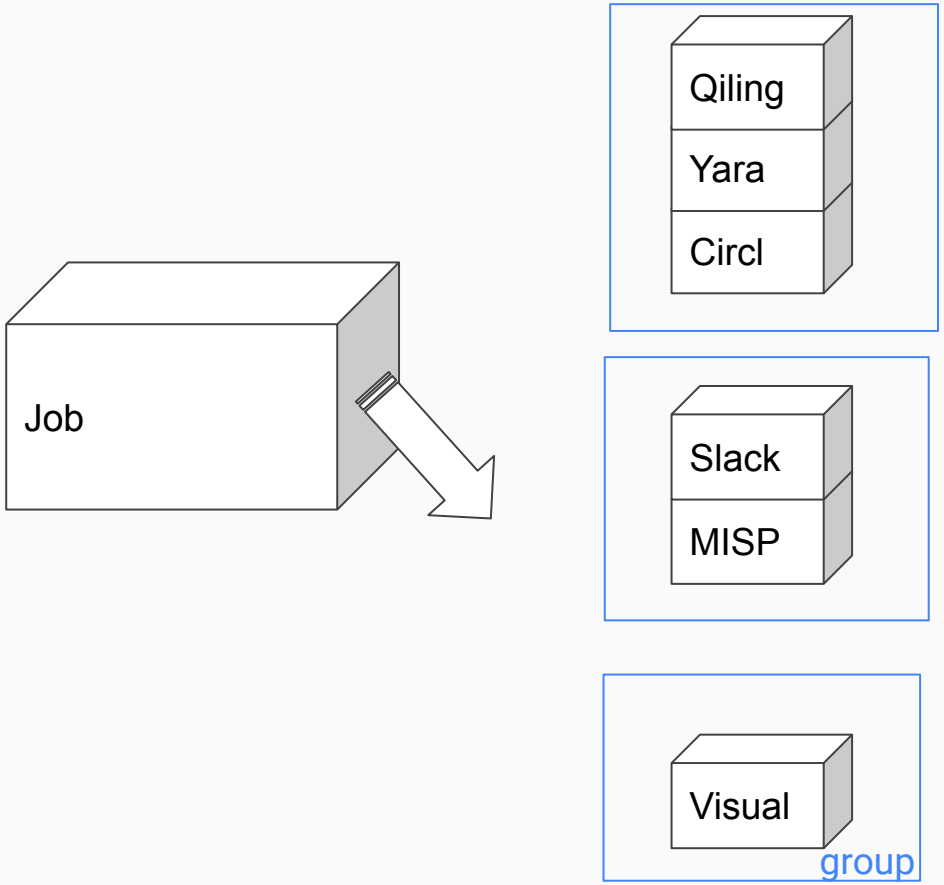
IntelOwl: Software Architecture



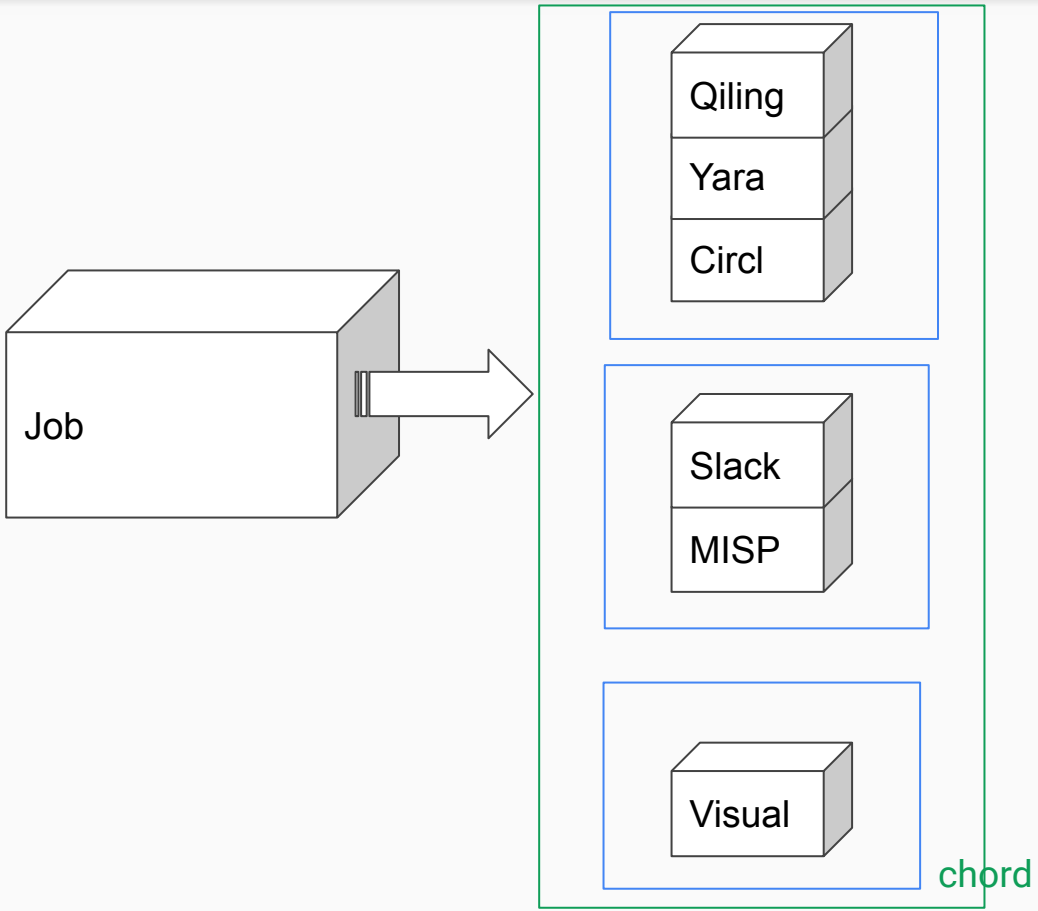
IntelOwl: Software Architecture



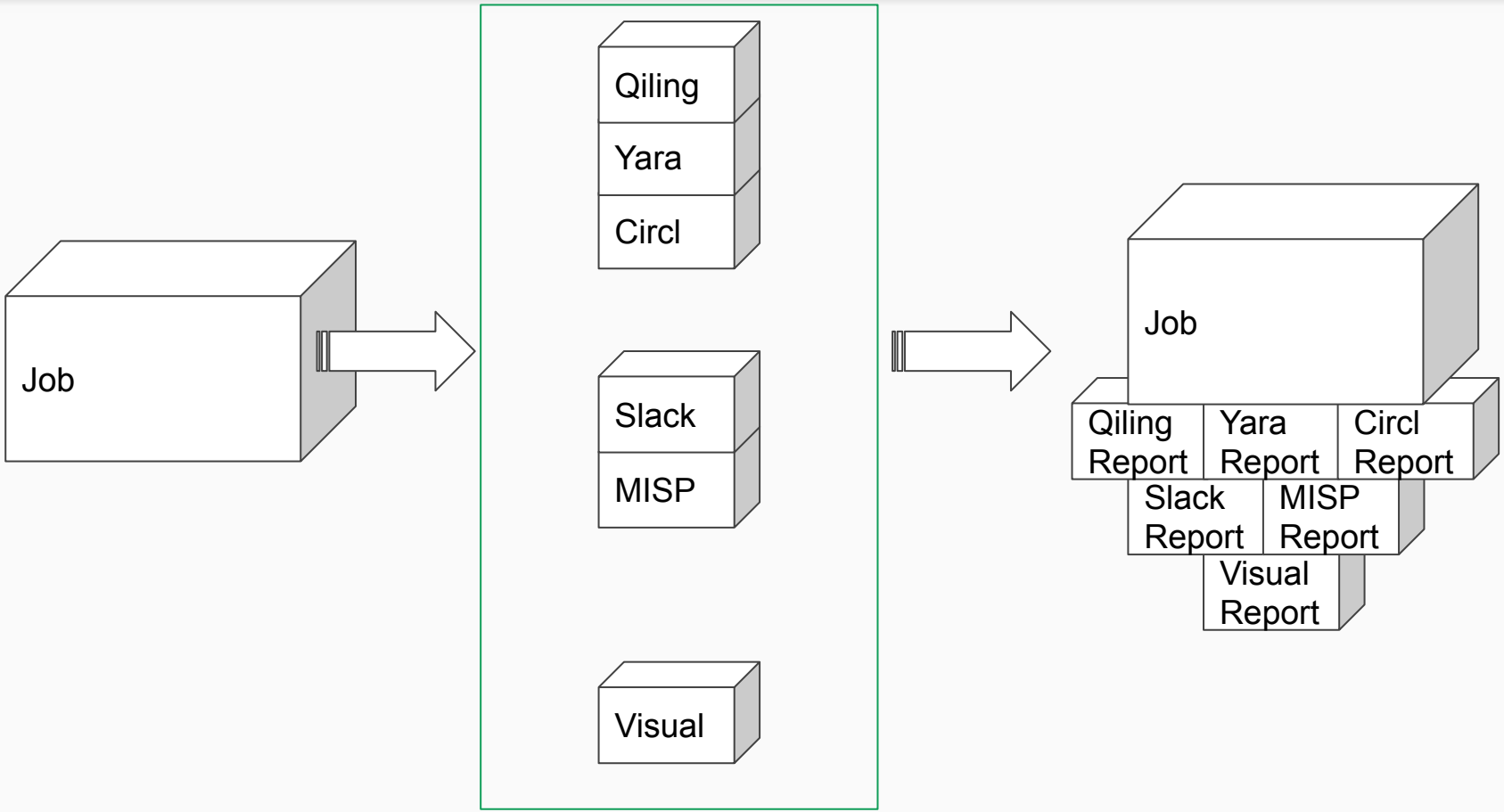
IntelOwl: Software Architecture



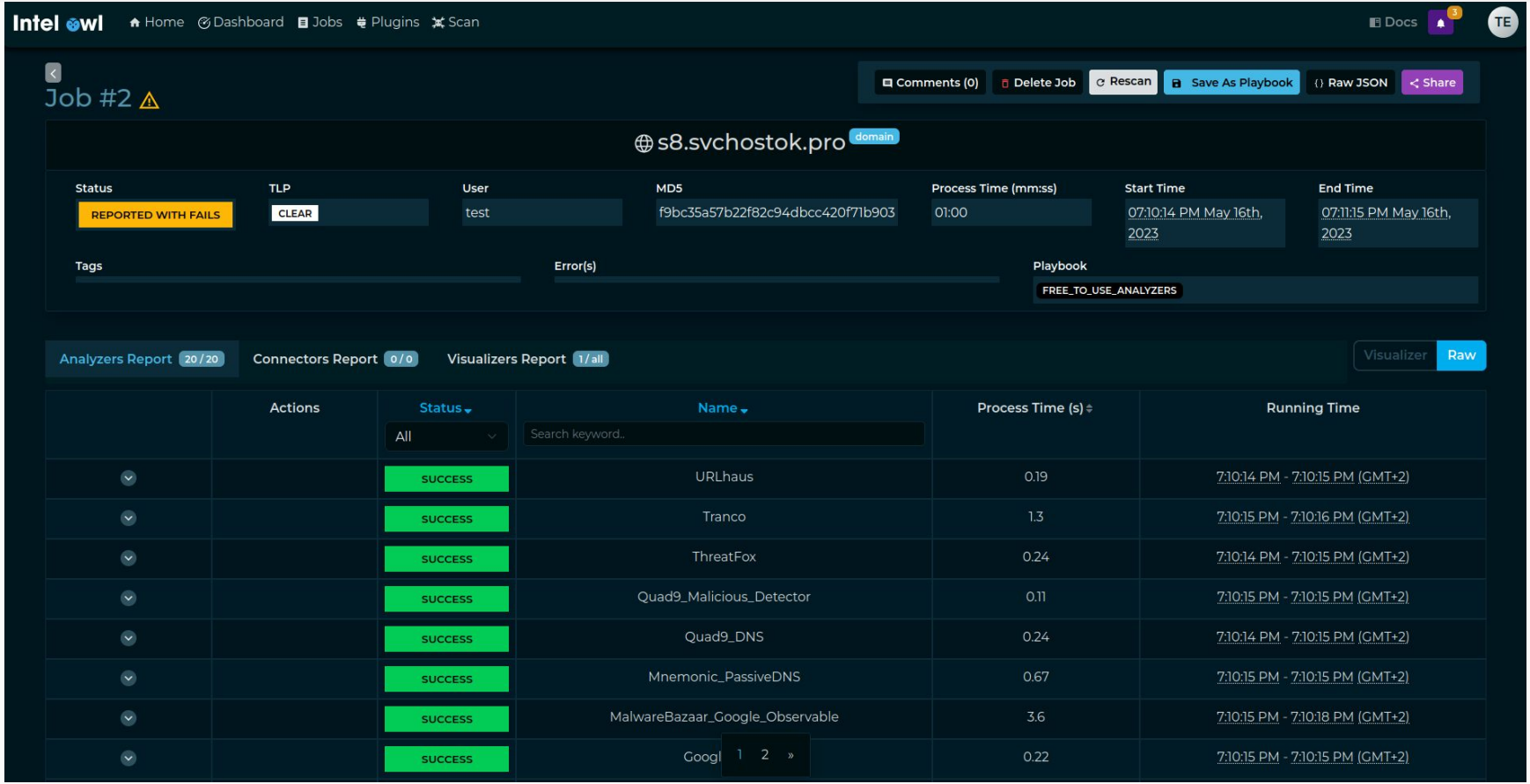
IntelOwl: Software Architecture



IntelOwl: Software Architecture



IntelOwl: Job Result (Raw Data)



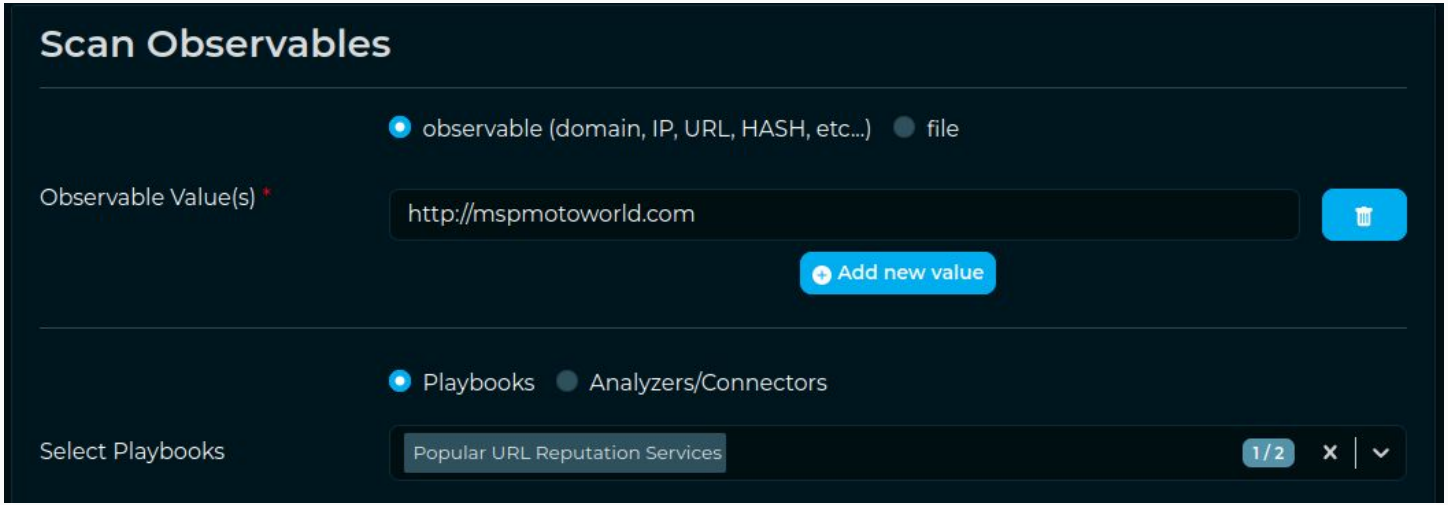
IntelOwl example use case

IntelOwl example use case: Phishing verification (1 / 3)

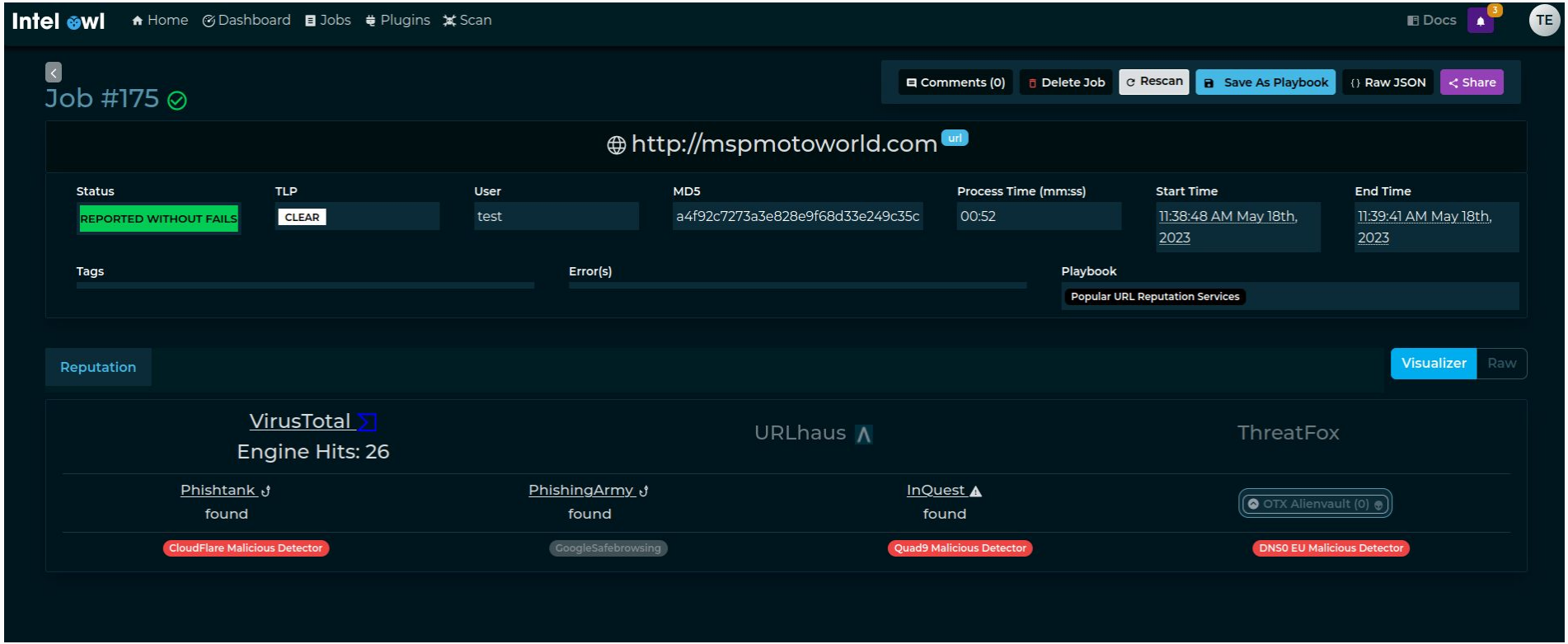
You get a link to an URL inside a suspicious email. Could it be phishing?

IntelOwl is integrated with tons of external services which can be queried to understand whether an URL is malicious or not and which kind of threat it poses: Reputation Services, DNS Resolvers, WHOIS services, Passive DNS services, URL Sandboxes, Threat Intel Platforms, Information Sharing Platforms, etc

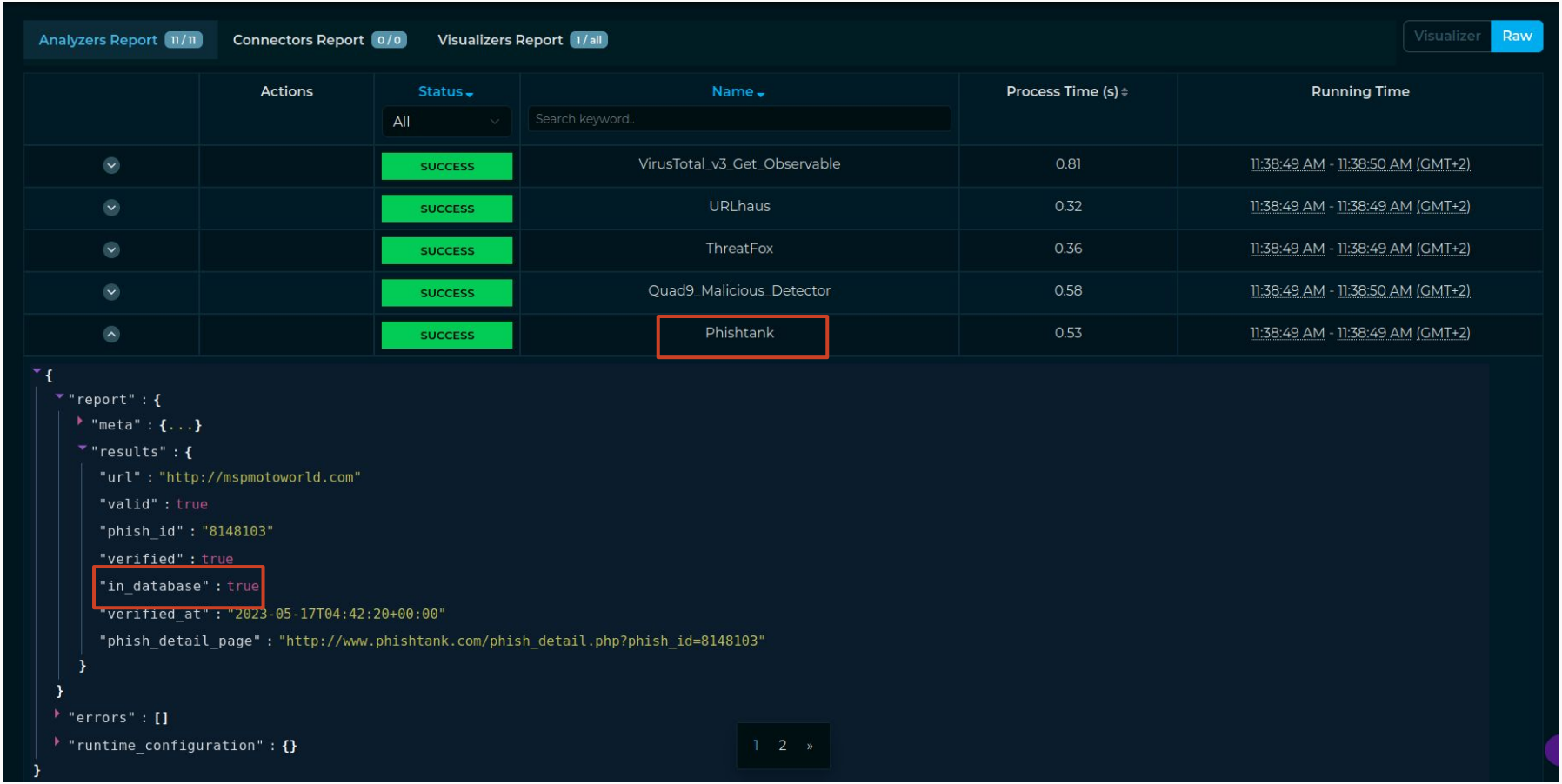
Those are all pre-built in the default installation.



IntelOwl example use case: Phishing verification (2 / 3)



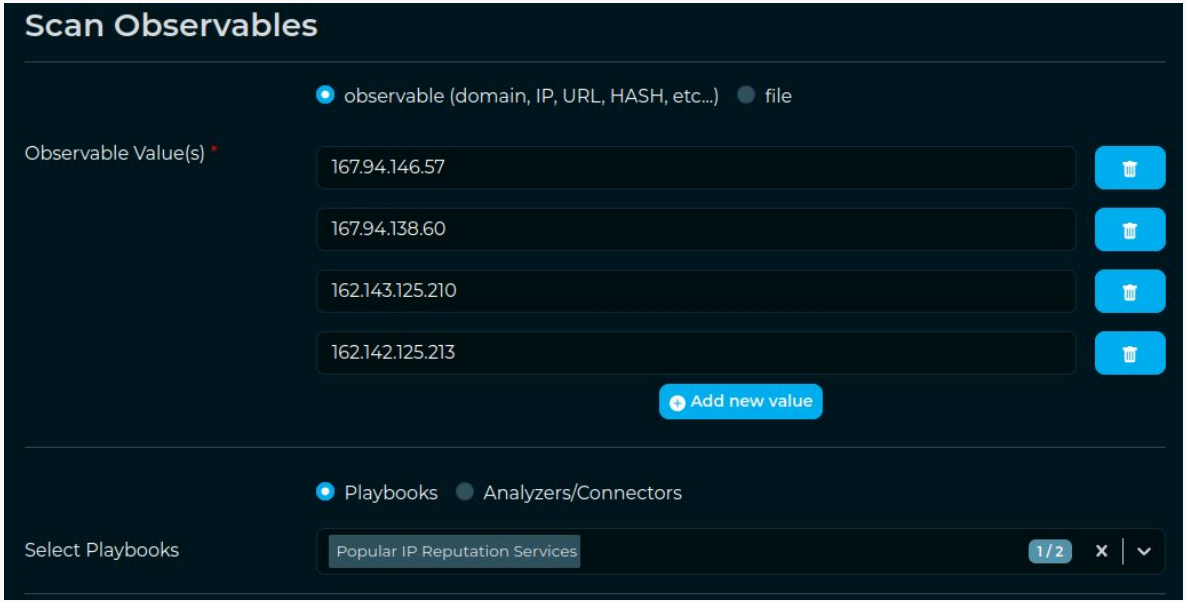
IntelOwl example use case: Phishing verification (3 / 3)



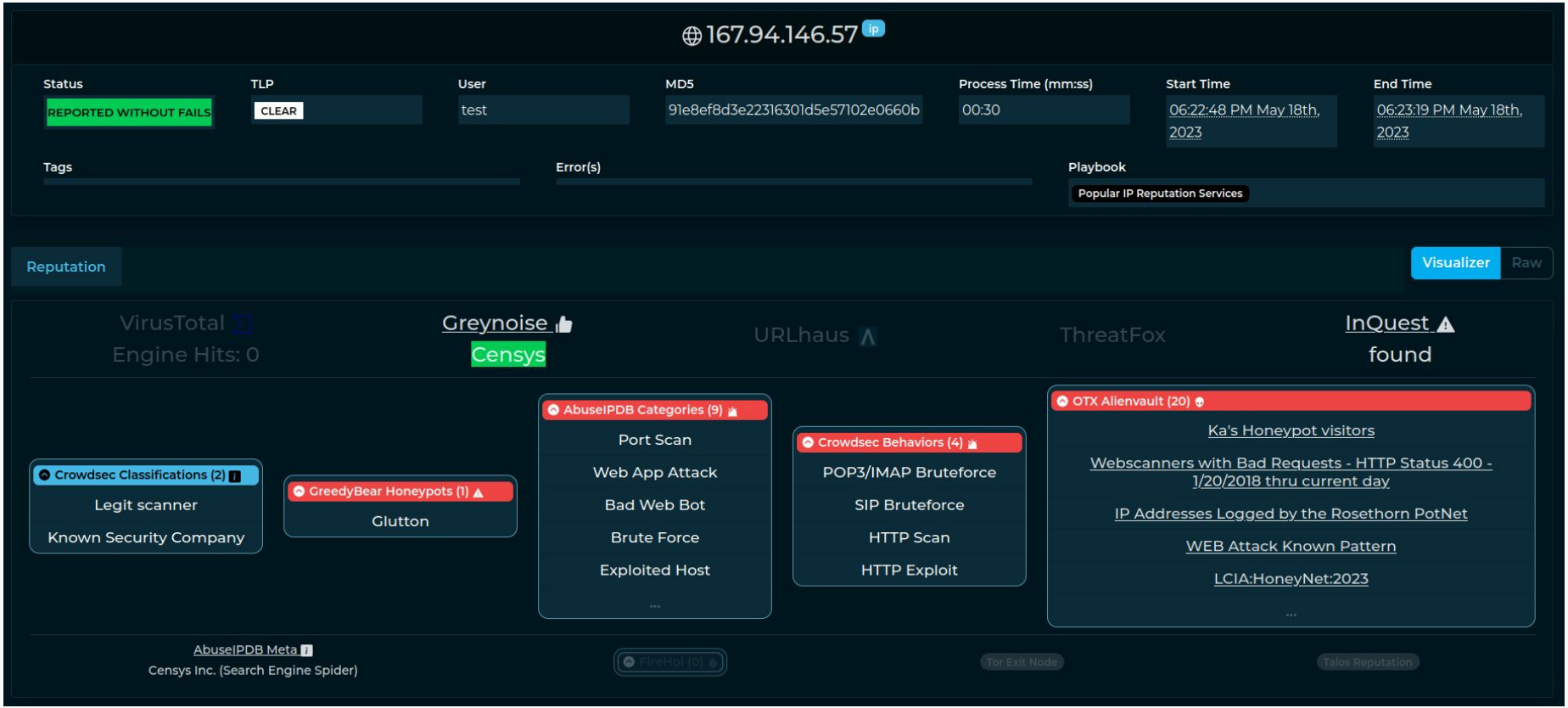
IntelOwl example use case: Filtering of legit connections (1 / 3)

You get a list of IP addresses that have been doing a lot of connections against your infrastructure. Are they legit scanners (crawlers like GoogleBot) or are they known to be abused?

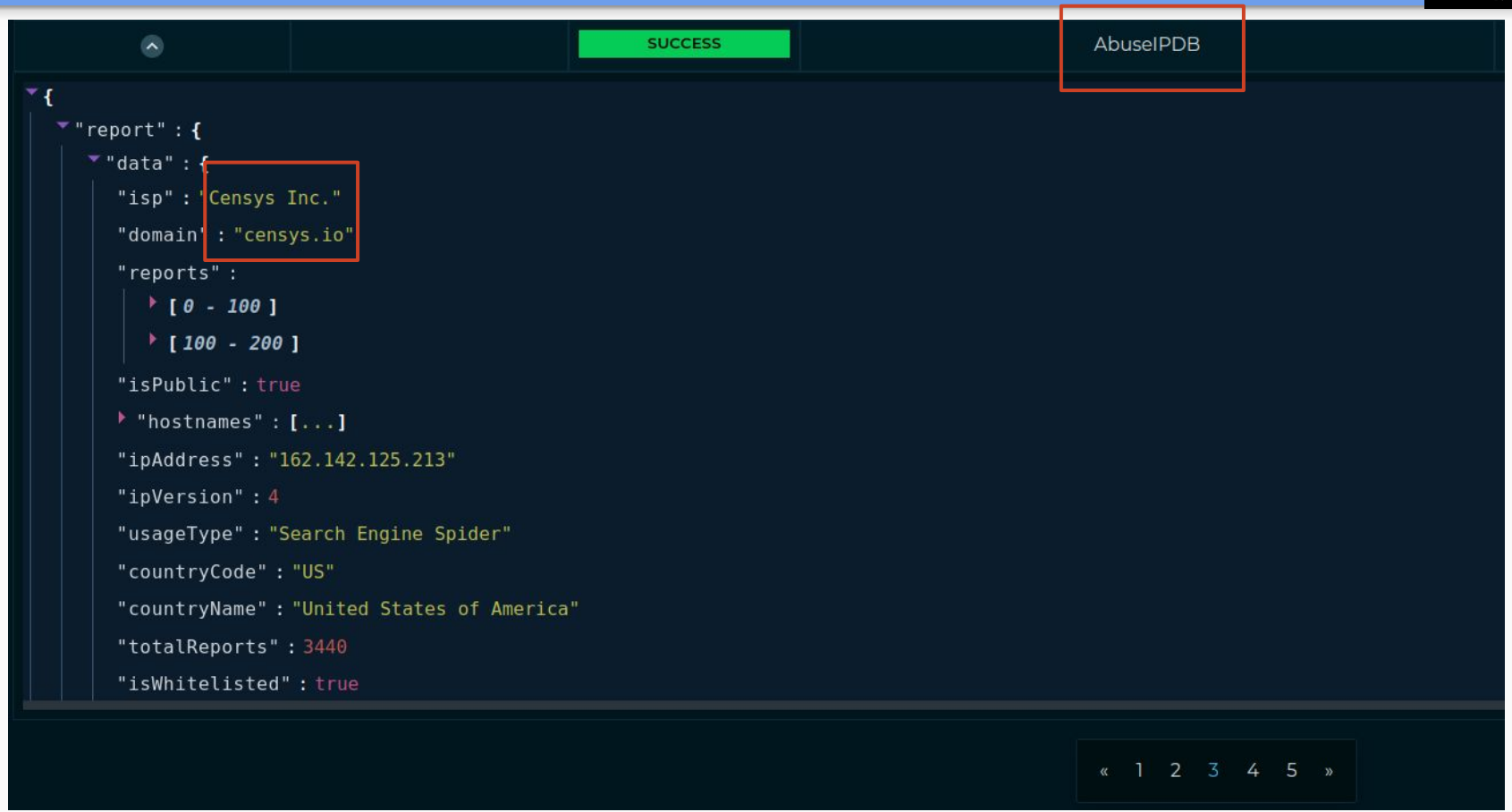
IntelOwl is integrated with tons of external services which can be queried to understand whether an IP address is malicious or not and which kind of threat it poses: Reputation Services, DNS Resolvers, Passive DNS services, Threat Intel Platforms, Information Sharing Platforms, etc



IntelOwl example use case: Filtering of legit connections (2 / 3)



IntelOwl example use case: Filtering of legit connections (3 / 3)



IntelOwl example use case: Suspicious File Analysis (1 / 4)

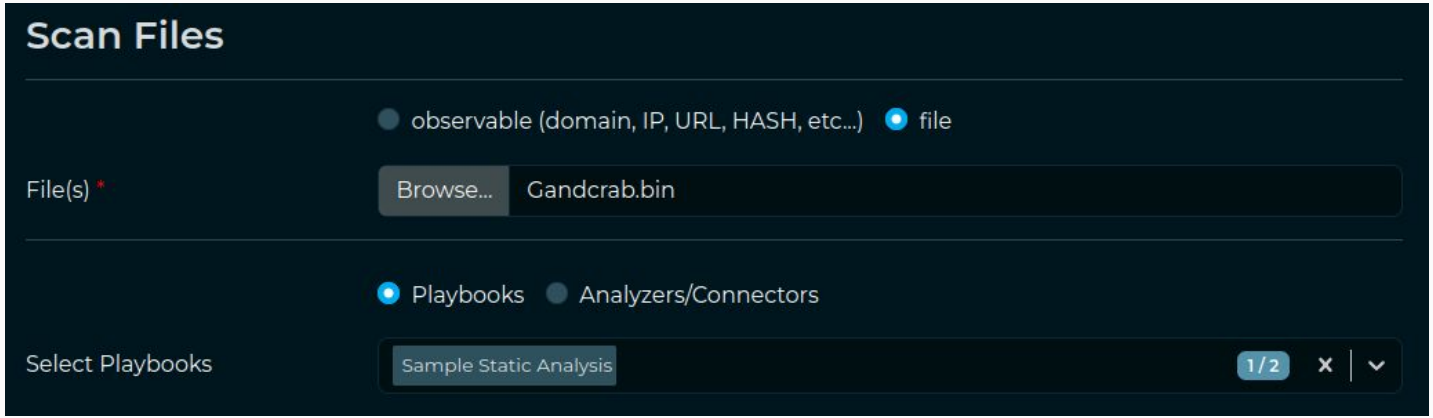
You get a possible malicious file and you need to understand more about it.

IntelOwl embeds a high number of open source file analysis tools: Yara, ClamAV, Exiftools, PdfId, Oletools, PeFile, Mandiant's Tools (Floss, Speakeasy, Stringsifter, CAPA), Quark Engine, Qiling, etc.

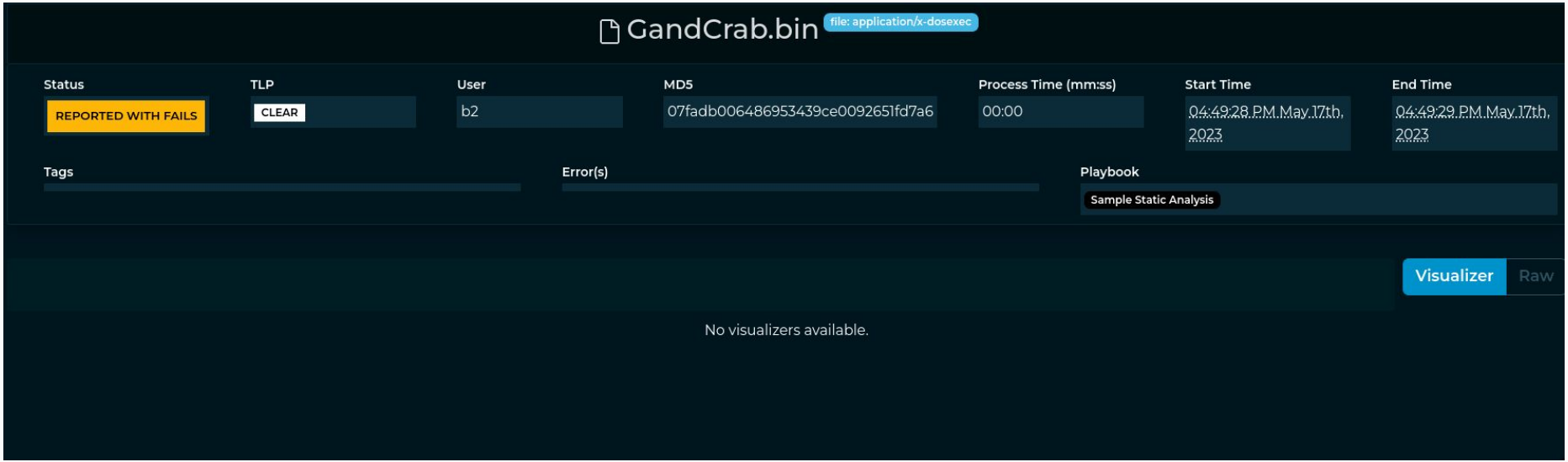
To leverage them all, you have to execute IntelOwl with an optional Docker container:

```
# start the app
python3 start.py prod up --malware_analysis_tools
```

Moreover IntelOwl is able to send either the sample or the hash only to external services for further analysis: VirusTotal, Intezer, etc

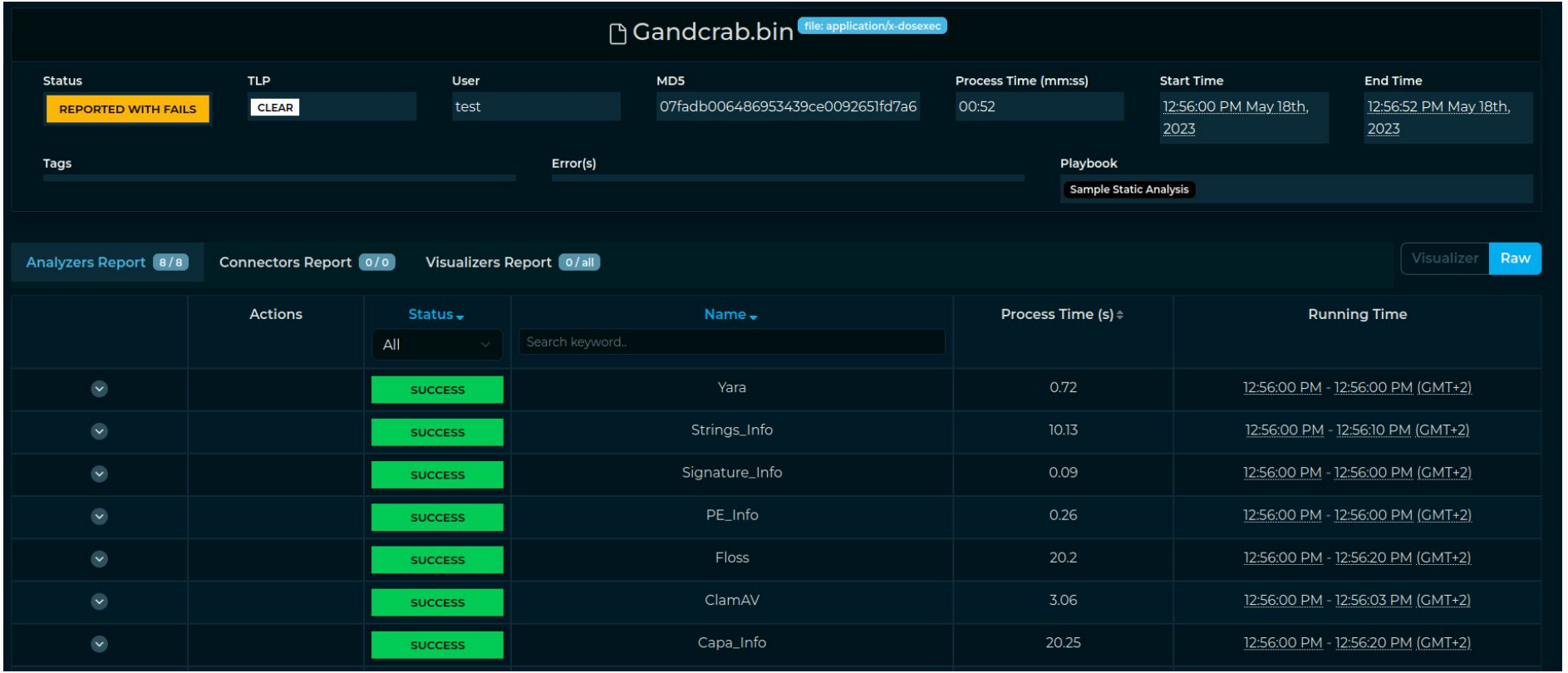


IntelOwl example use case: Suspicious File Analysis (2 / 4)



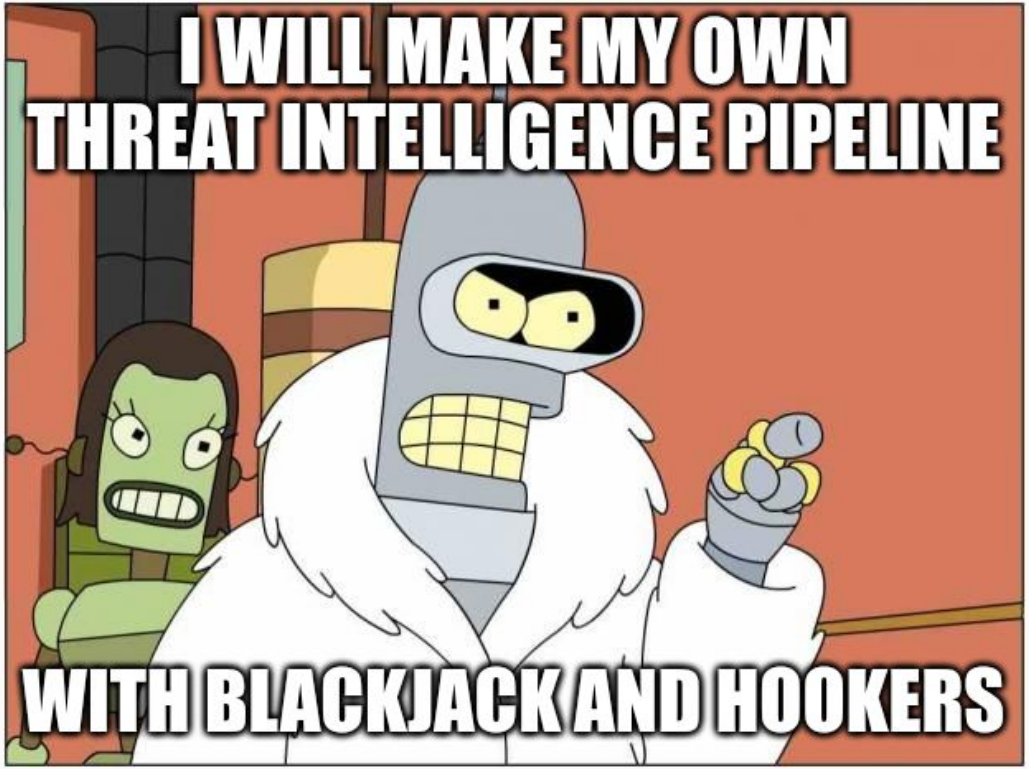
IntelOwl example use case: Suspicious File Analysis (2 / 4)

IntelOwl example use case: Suspicious File Analysis (3 / 4)

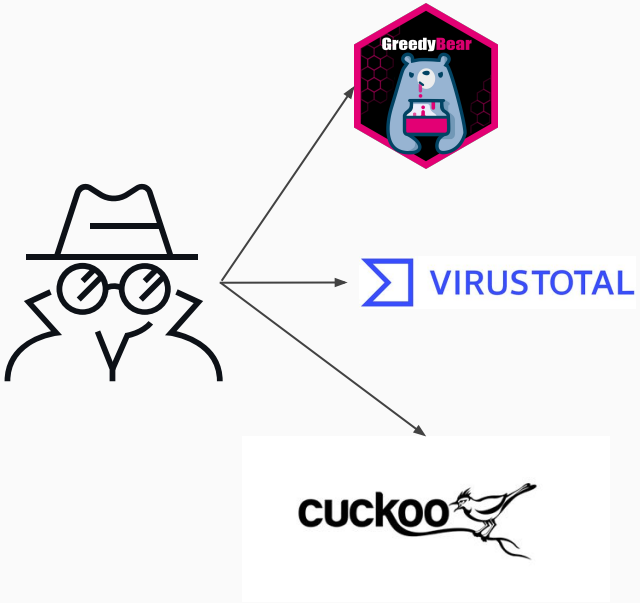


IntelOwl example use case: Suspicious File Analysis (4 / 4)

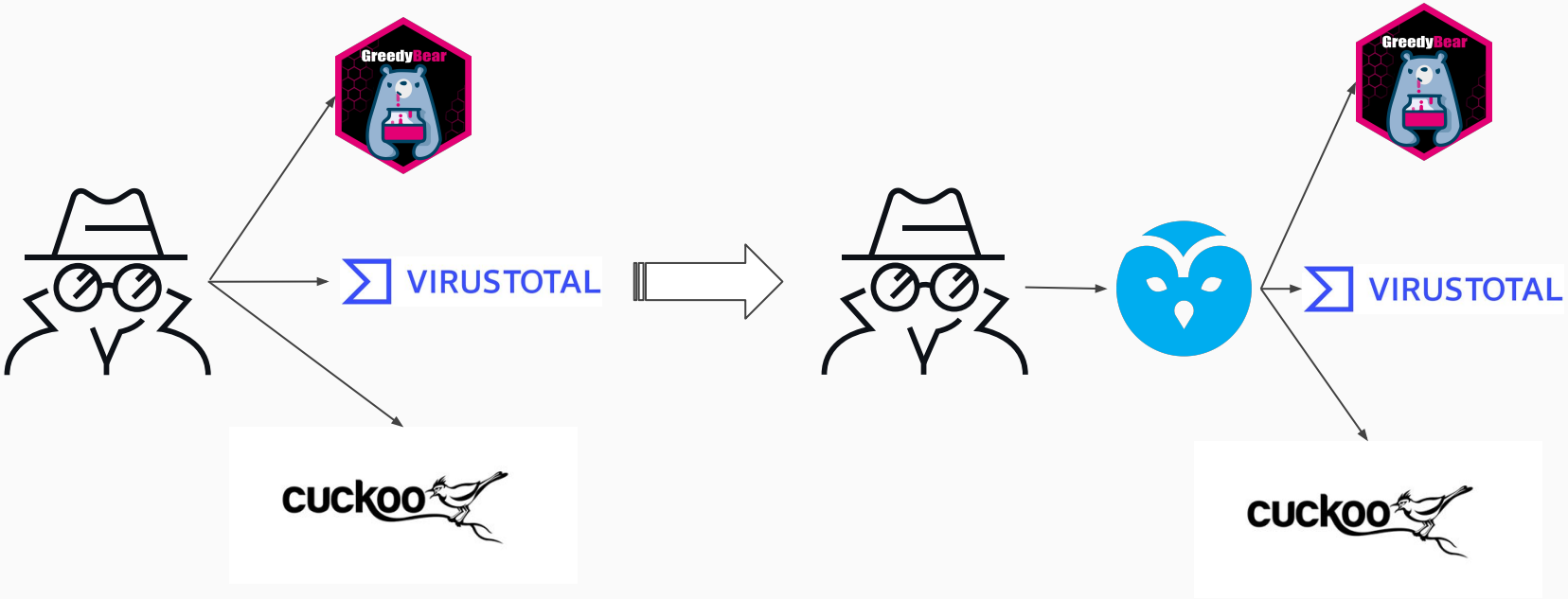
IntelOwl example use case: Suspicious File Analysis (4 / 4)


I WILL MAKE MY OWN
THREAT INTELLIGENCE PIPELINE
WITH BLACKJACK AND HOOKERS

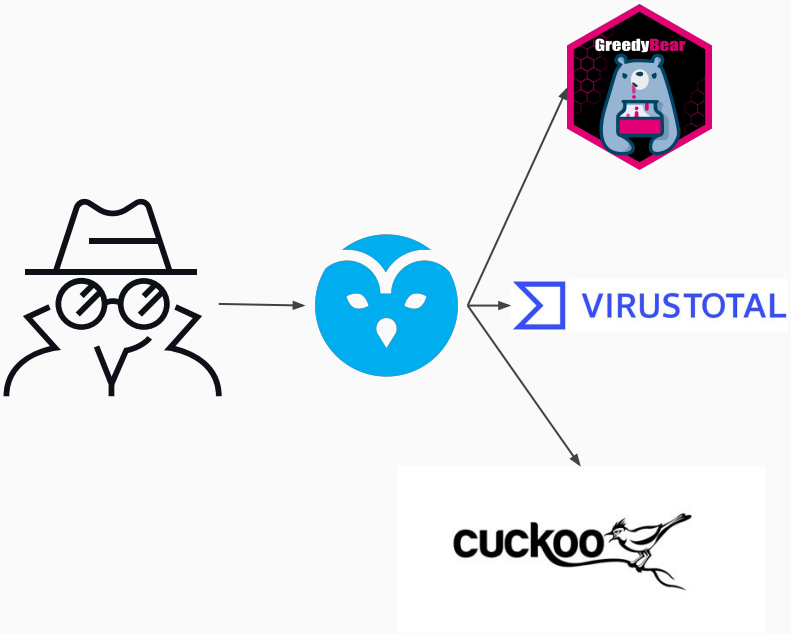
A Threat Intelligence pipeline with IntelOwl (1 / 3)



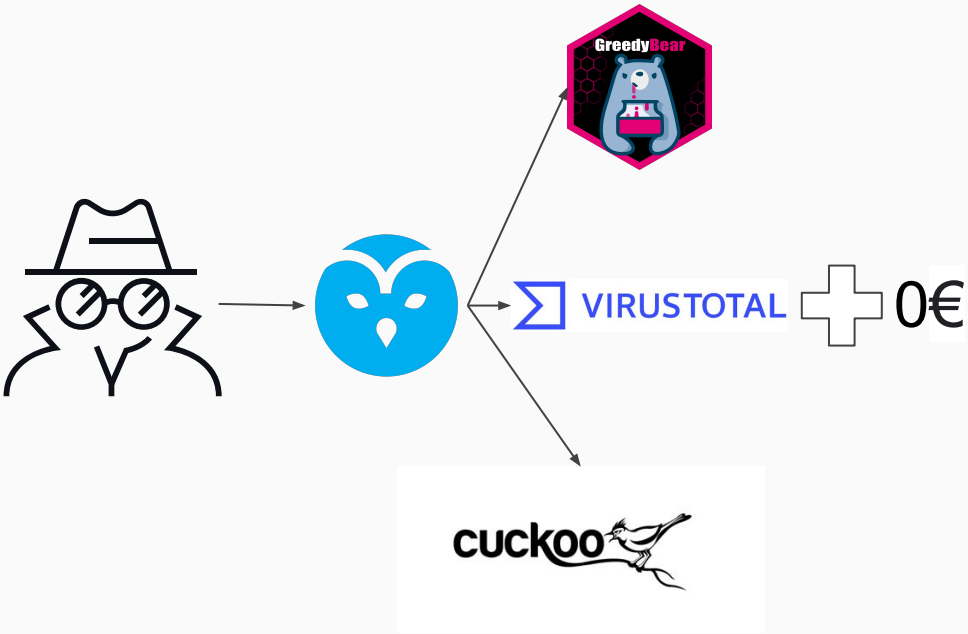
A Threat Intelligence pipeline with IntelOwl (1 / 3)



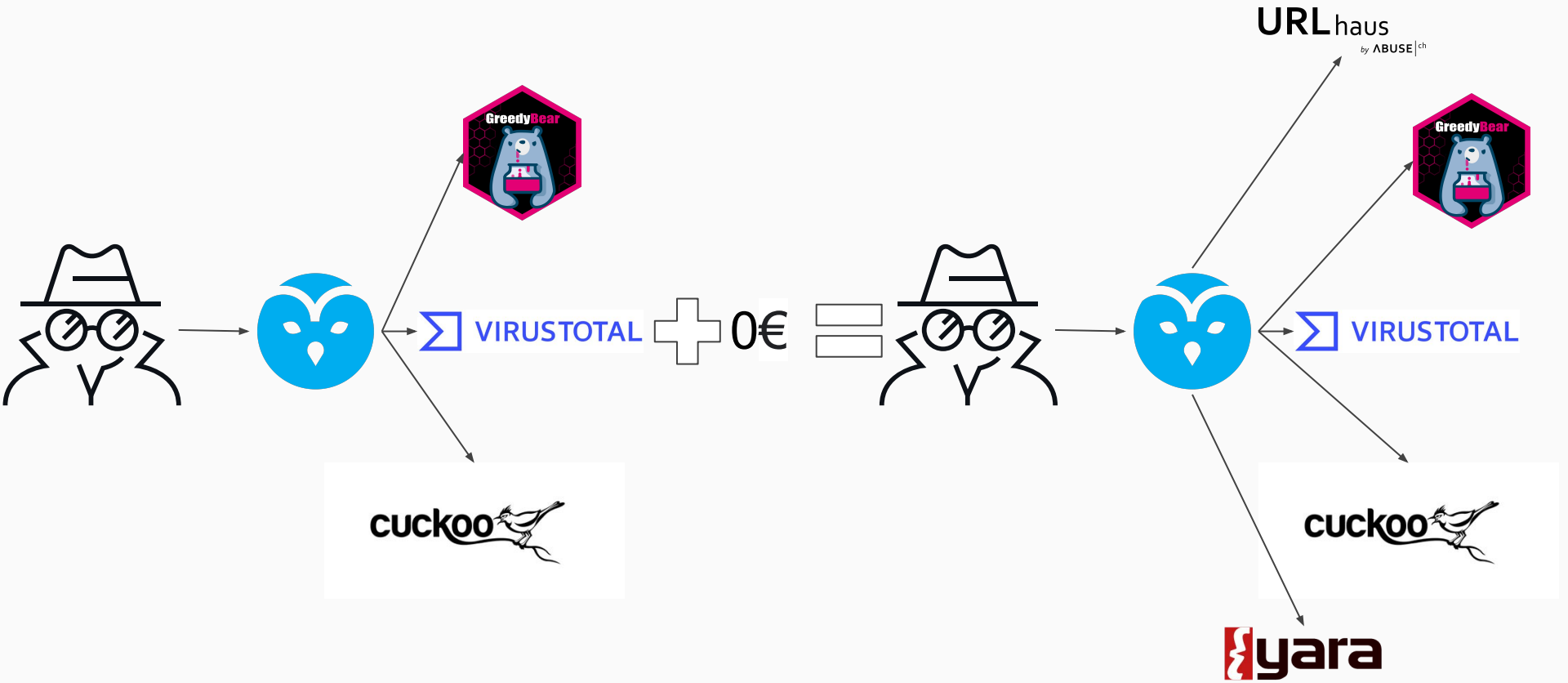
A Threat Intelligence pipeline with IntelOwl (2 / 3)



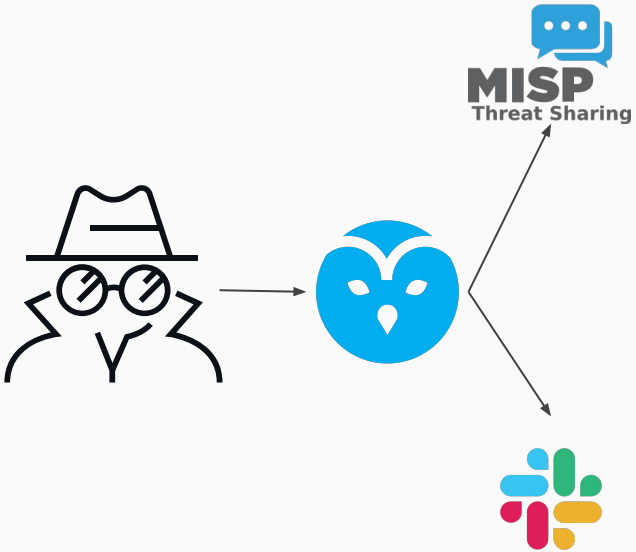
A Threat Intelligence pipeline with IntelOwl (2 / 3)



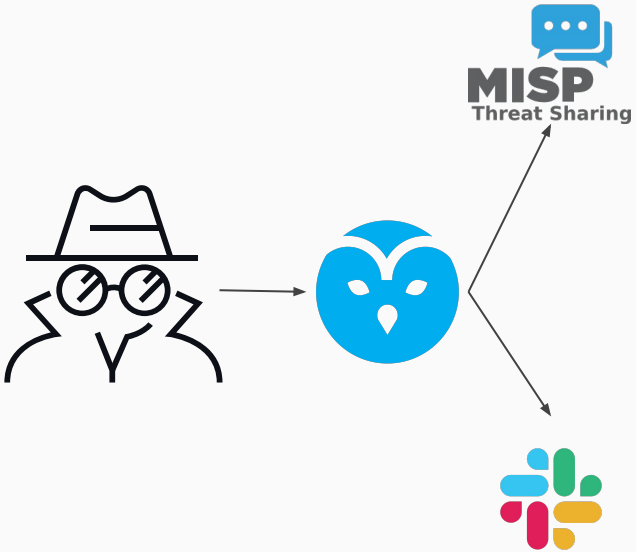
A Threat Intelligence pipeline with IntelOwl (2 / 3)

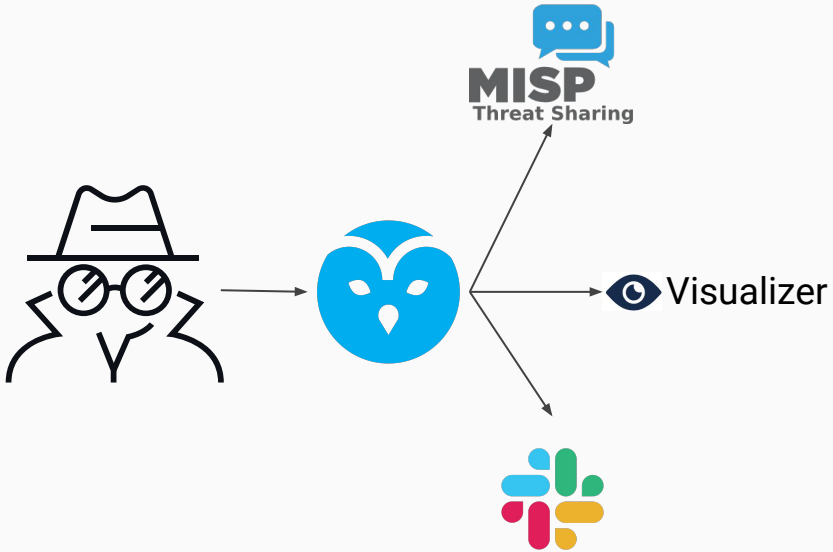


A Threat Intelligence pipeline with IntelOwl (3 / 3)



A Threat Intelligence pipeline with IntelOwl (3 / 3)





IntelOwl and Google Summer of Code

Since the very beginning of this project we participated in the **Google Summer of Code** under the umbrella of The Honeynet Project! (3 years, 6 successfully completed projects!)

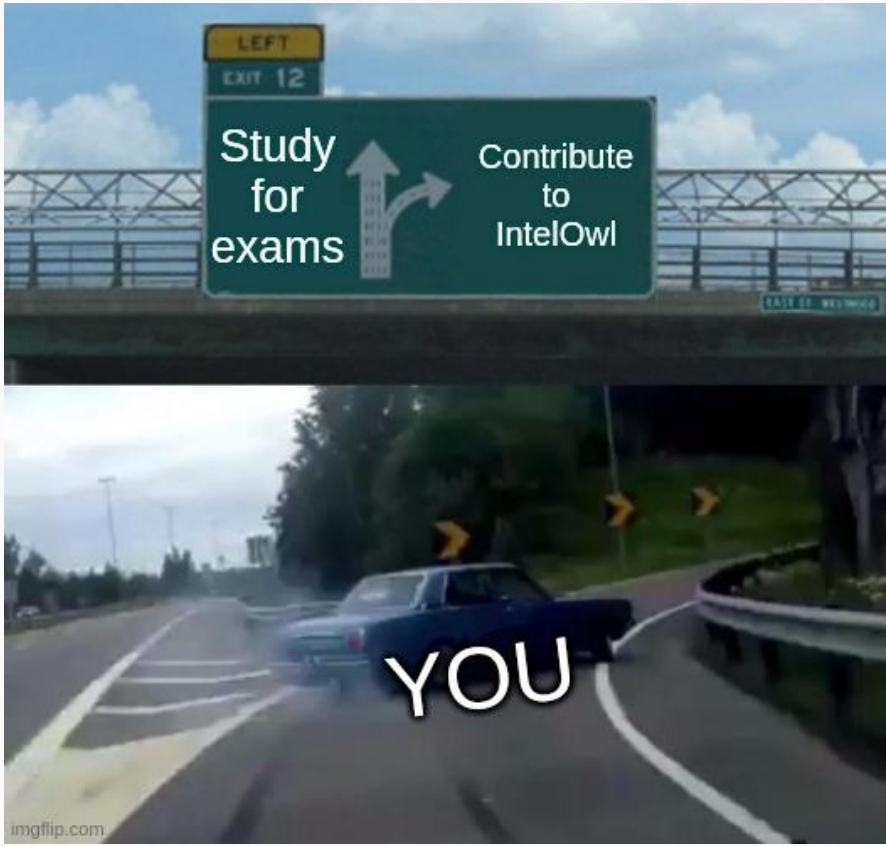
We are participating this year too!

Google Summer of Code

We have selected 2 new contributors this year and they have just started to work for their projects:

- *Abheek Tripathy* is working on creating a new official website for IntelOwl!
- *Shivam Purohit* is working on adding new features like 2FA, Single Sign On with Github, etc

Stay tuned for GSoC 2024!



IntelOwl Future Plans

We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

IntelOwl Future Plans

We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results~~ -> *IntelOwl v5 released!*

IntelOwl Future Plans

We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results~~ -> *IntelOwl v5 released!*
- Investigation Framework:
  - Workflows of Analysis (SOAR-like)

IntelOwl Future Plans

We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results~~ -> *IntelOwl v5 released!*
- Investigation Framework:
  - Workflows of Analysis (SOAR-like)
- Support for Cluster Deployments:
  - Docker Swarm
  - Kubernetes
- New Plugins Types:
  - Ingestors
  - Scanners

IntelOwl Future Plans

We are planning to add new critical features in IntelOwl to transform it from a Data Extraction Platform to a complete **Investigation Platform**:

- ~~Aggregated and simplified visualization of analyzers results~~ -> *IntelOwl v5 released!*
- Investigation Framework:
  - Workflows of Analysis (SOAR-like)
- Support for Cluster Deployments:
  - Docker Swarm
  - Kubernetes
- New Plugins Types:
  - Ingestors
  - Scanners
- **Give us YOUR ideas!**
- **Follow us on Twitter, Linkedin and Github!**

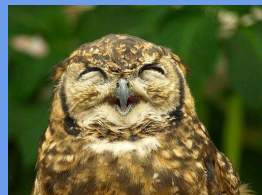
Any help is welcome and valuable!

The icons were collected from: Flaticon
Memes were generated with Imgflip

Thank you for listening!

@matte_lodi @0ssig3no

intelowlproject/IntelOwl



This presentation was reviewed and built together with our awesome team:
Daniele Rosetti and Pietro Delsante