IntelOwl Project

“making the life of cyber security analysts easier”

The Honeynet Workshop - Denmark ‘24

Say “hi” to the team :)

IntelOwl Maintainers		
Matteo Lodi	@matte_lodi	mlodic
Simone Berni	@0ssig3no	0ssigeno
Daniele Rosetti	@magicross94	drosetti

certego

Threat Intelligence Team

HN/P

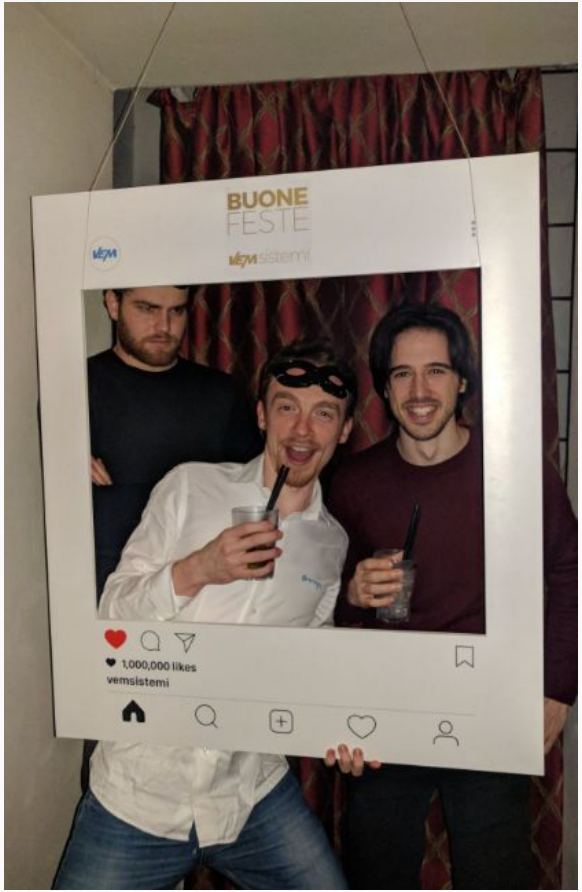
Members

Intel owl

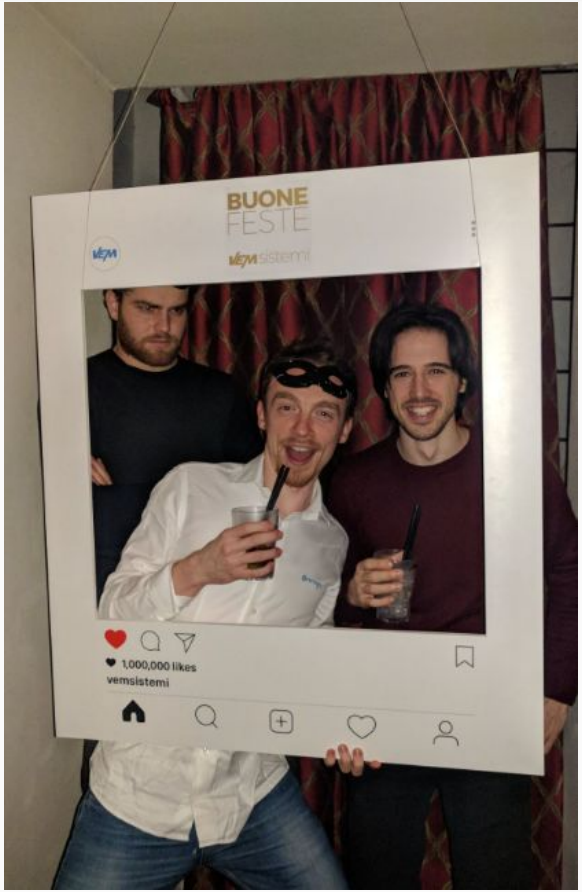
Who are you?

Intel owl

Enjoying myself in the Cyber Security field!



Enjoying myself in the Cyber Security field!

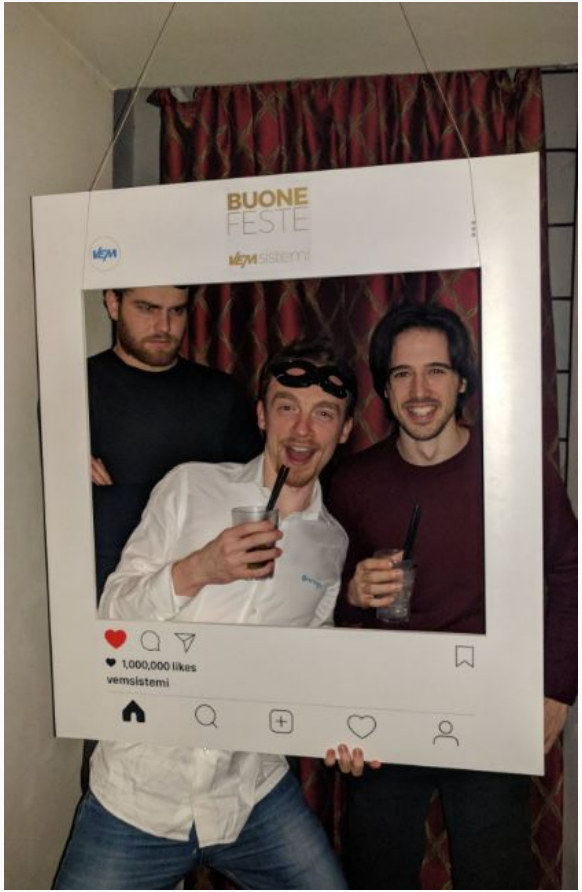


I have the best colleagues ever!

Intel owl

Enjoying myself in the Cyber Security field!

I'll never stop learning!



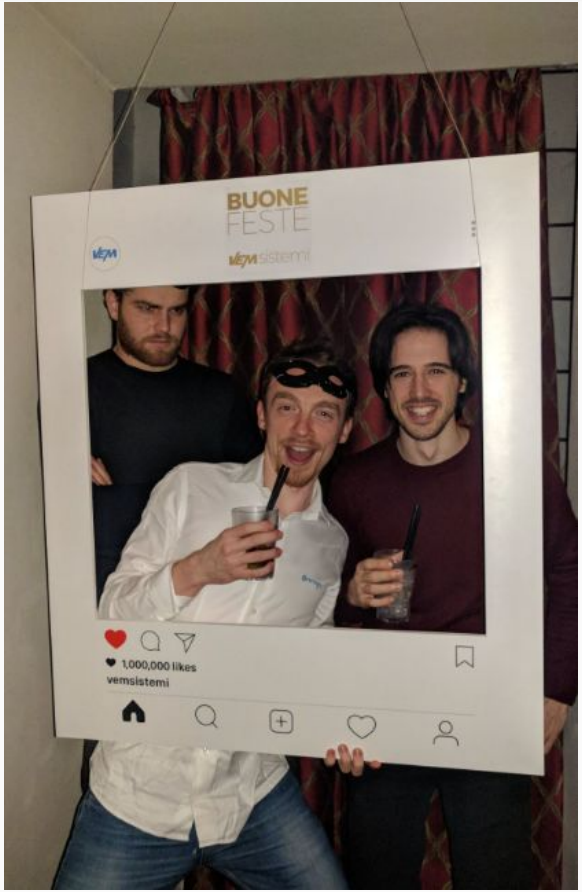
I have the best colleagues ever!

Intel owl

Enjoying myself in the Cyber Security field!

I'll never stop learning!

We are like superheroes!



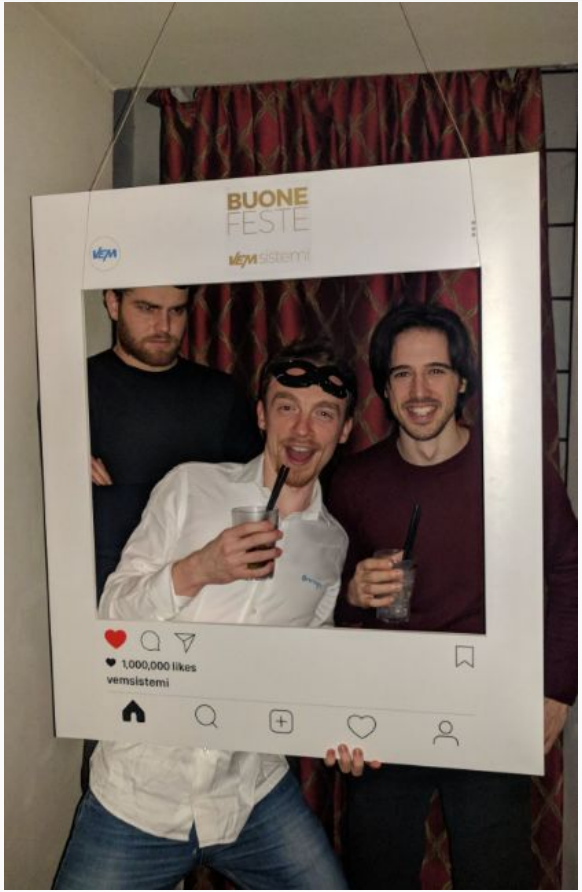
I have the best colleagues ever!

Intel owl

Enjoying myself in the Cyber Security field!

I'll never stop learning!

We are like superheroes!

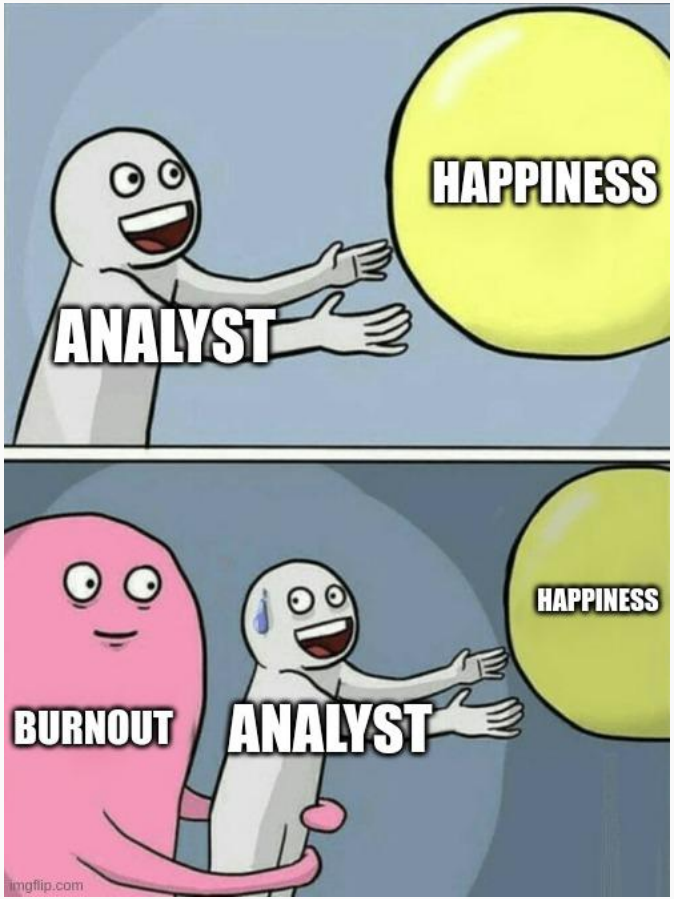


I have the best colleagues ever!

This is my dream job!

Intel owl

Unveil the reality



Intel owl

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

Burnout: the hidden cyber security threat

Workers are exhausted and constantly on edge.

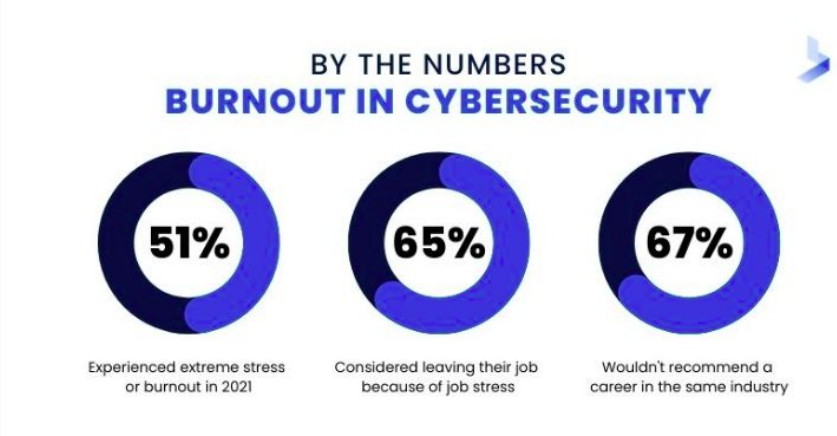
By Emily Chantiri on Sep 27 2023 04:06 PM

ref: AECS

83% of IT Security Professionals Say Burnout Causes Data Breaches

September 20, 2023 3 Min Read

ref: DarkReading



ref: Bitlyft

Automate, automate, automate

2017:

- Working in a little team of cyber security analysts
- Overwhelmed by security alerts
- Stuck in repetitive and boring tasks
- Burnt-out myself

Automate, automate, automate

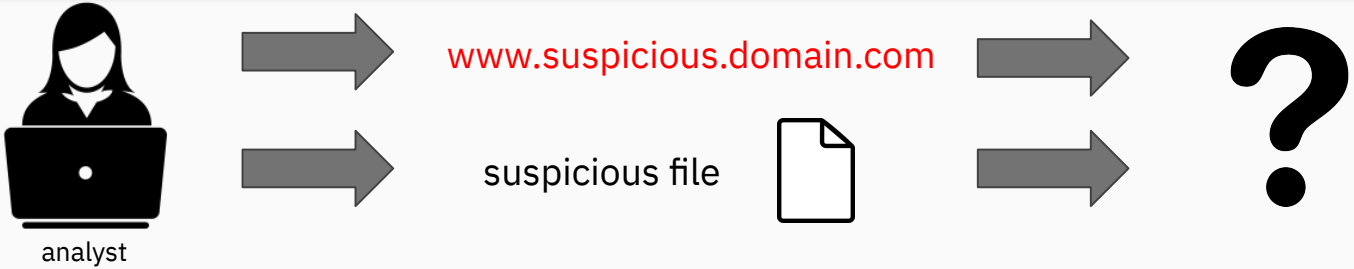
2017:

- Working in a little team of cyber security analysts
- Overwhelmed by security alerts
- Stuck in repetitive and boring tasks
- Burnt-out myself

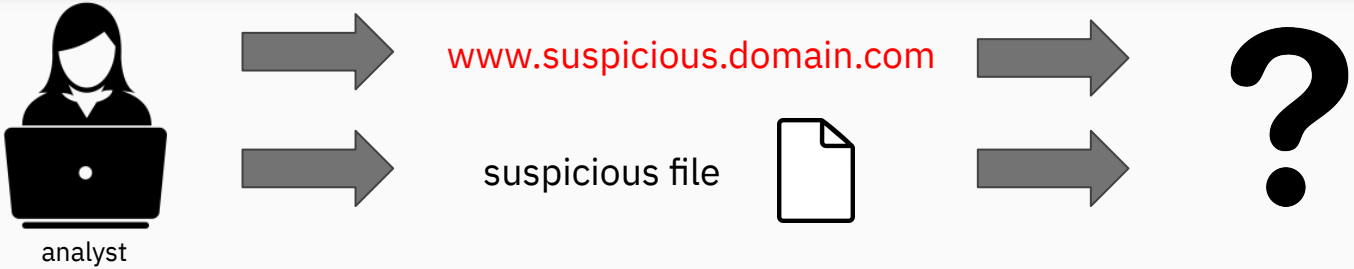
We needed to start to **automate** our most common workflows.

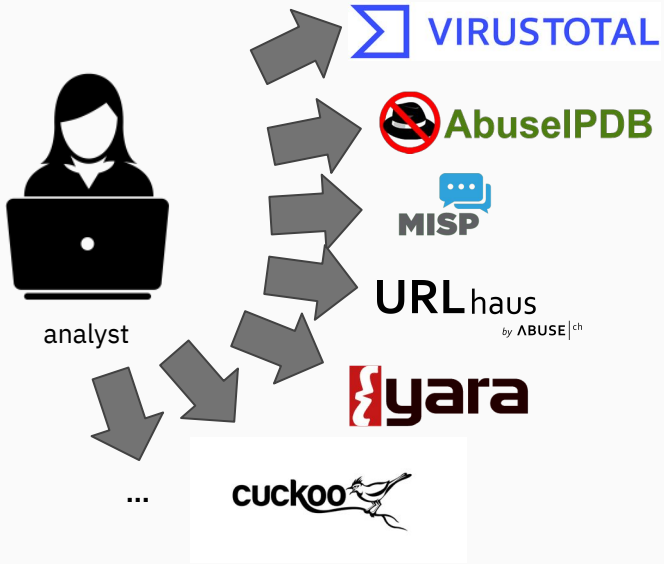
Intel owl

The bottleneck: acquisition of threat intelligence context



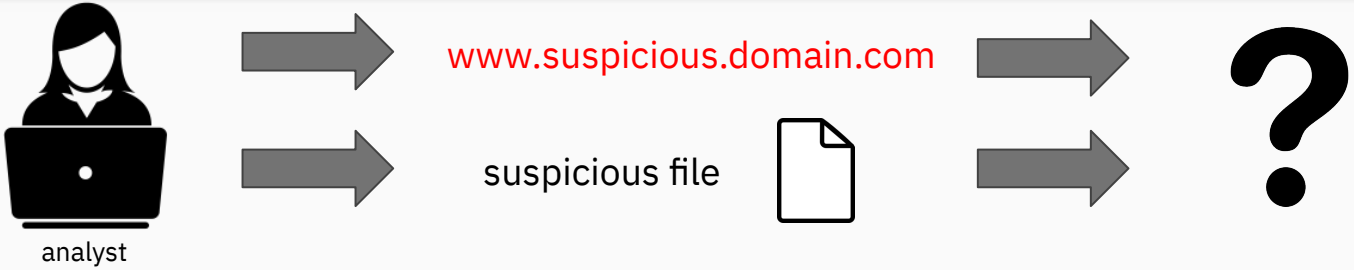
The bottleneck: acquisition of threat intelligence context

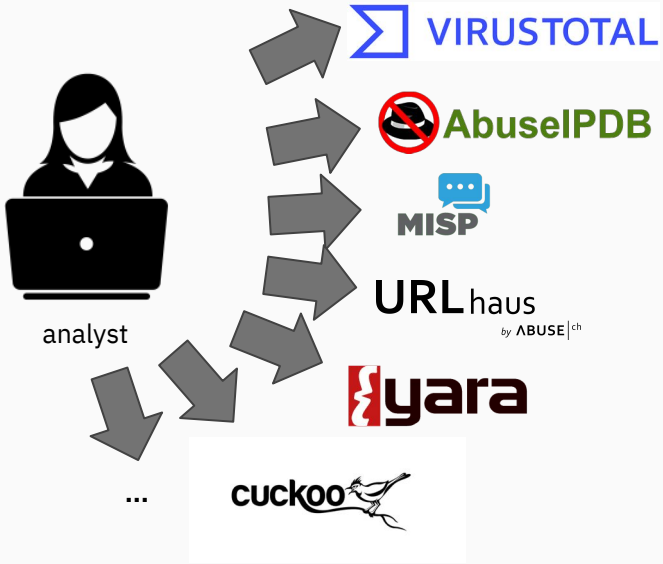


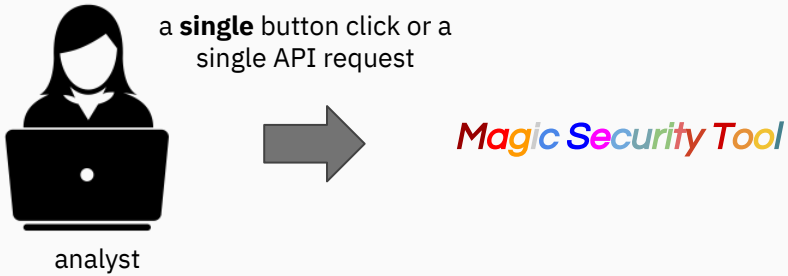


Intel owl

The bottleneck: acquisition of threat intelligence context







Intel owl

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

Intel owl

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

Intel owl

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

Intel owl

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

Intel owl

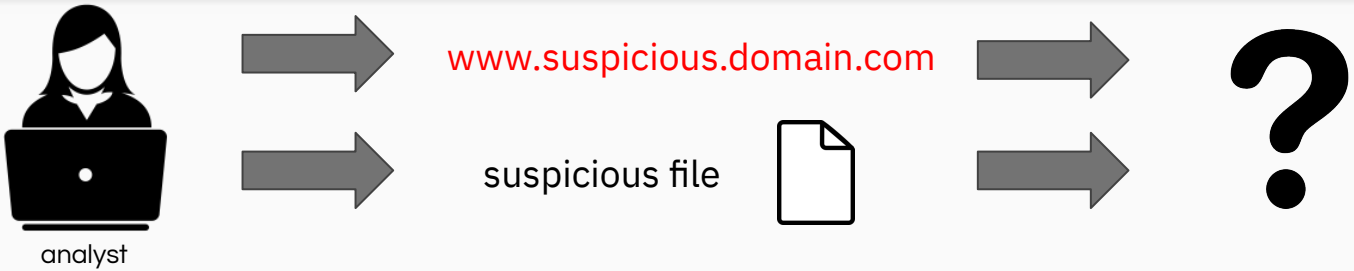
IntelOwl was born

Intel owl

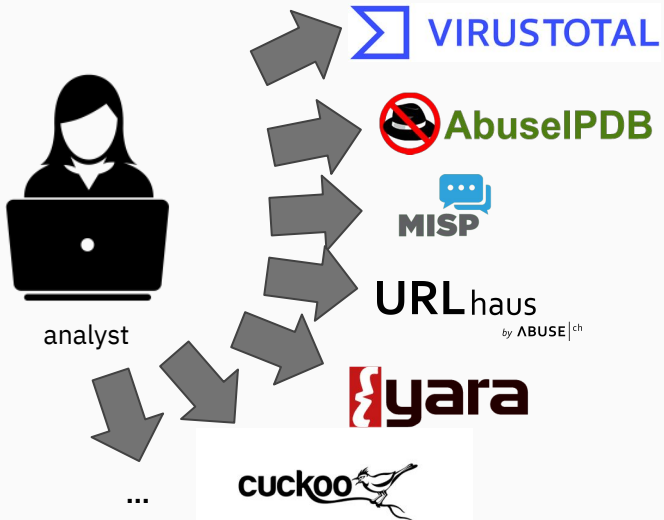
Born in Certego at the start of 2020, it is a great example of a successful Open Source project: right now it is one of the most popular Threat Intel projects on GitHub (>3k stars).

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

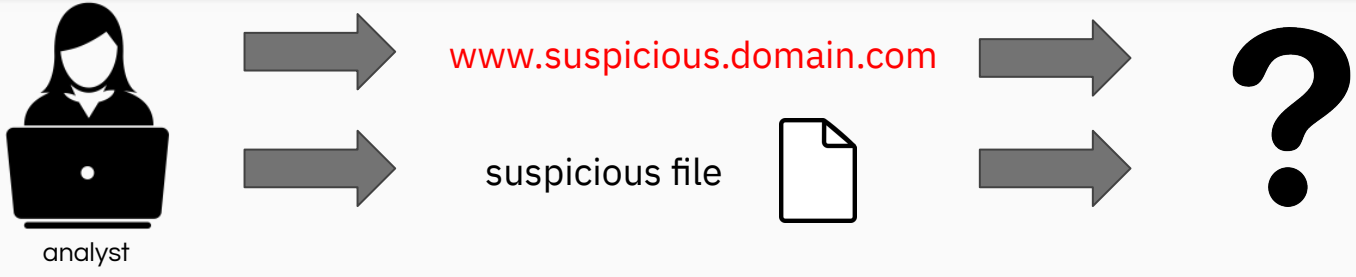
IntelOwl solution



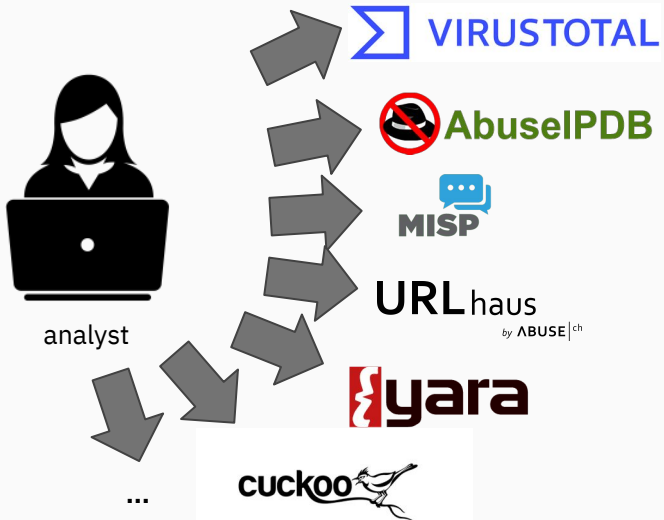
WithOUT Intel Owl



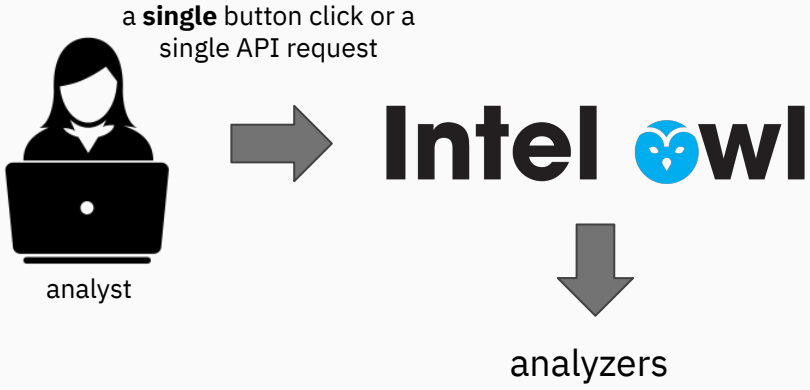
IntelOwl solution



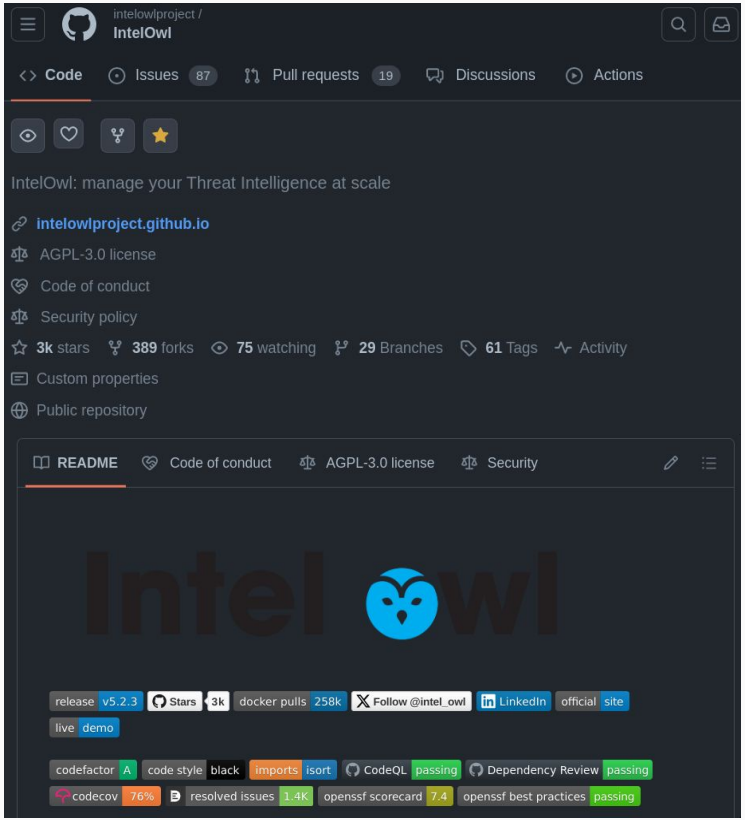
WithOUT Intel Owl



With Intel Owl



IntelOwl Repository & Tech Stack

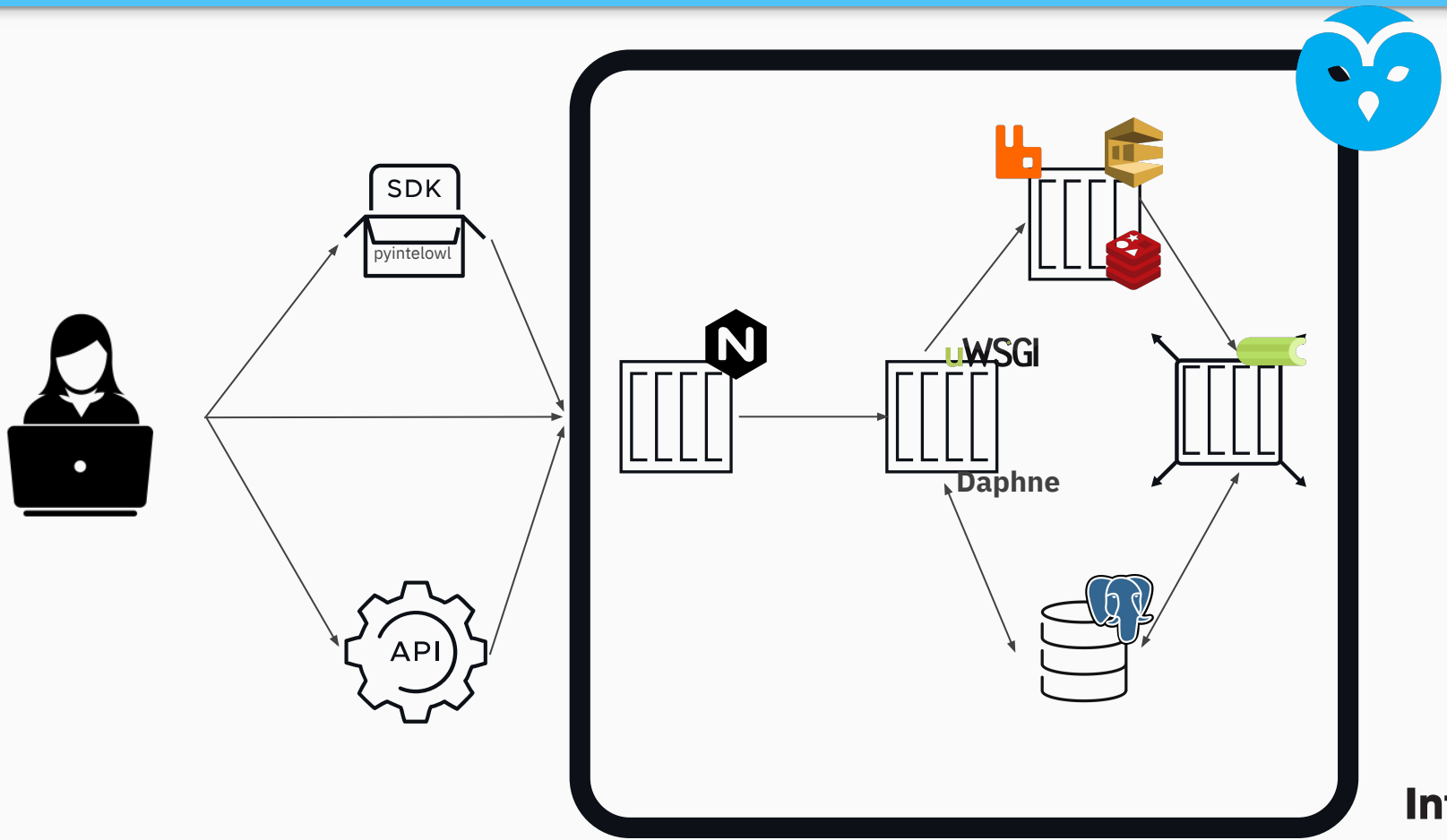


The most common (and open source) technologies and framework are used and we keep them constantly updated:

- Docker
- Python3
- ReactJS
- Django ecosystem
- Celery
- PostgreSQL
- ElasticSearch
- Nginx
- Uwsgi
- Daphne
- Rabbit-MQ/SQS/Redis

Intel owl

IntelOwl: Infrastructure Architecture



Intel owl

IntelOwl: Installation

IT'S YOUR TIME TO TRY! Follow the steps below!

get the slides of the workshop here!

Follow the official documentation (which we strive to keep up to date):

```
# clone the IntelOwl project repository
git clone https://github.com/intelowlproject/IntelOwl
cd IntelOwl/

# this can solve some installation problems
./initialize.sh

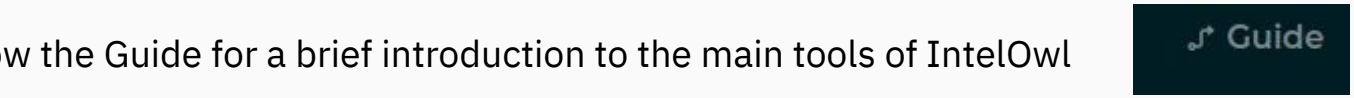
# verify installed dependencies and start the app
./start prod up OR
.env ->
```COMPOSE_PROJECT_NAME=intelowl
COMPOSE_FILE=docker/default.yml:docker/redis.override.yml:docker/postgres.override.yml```

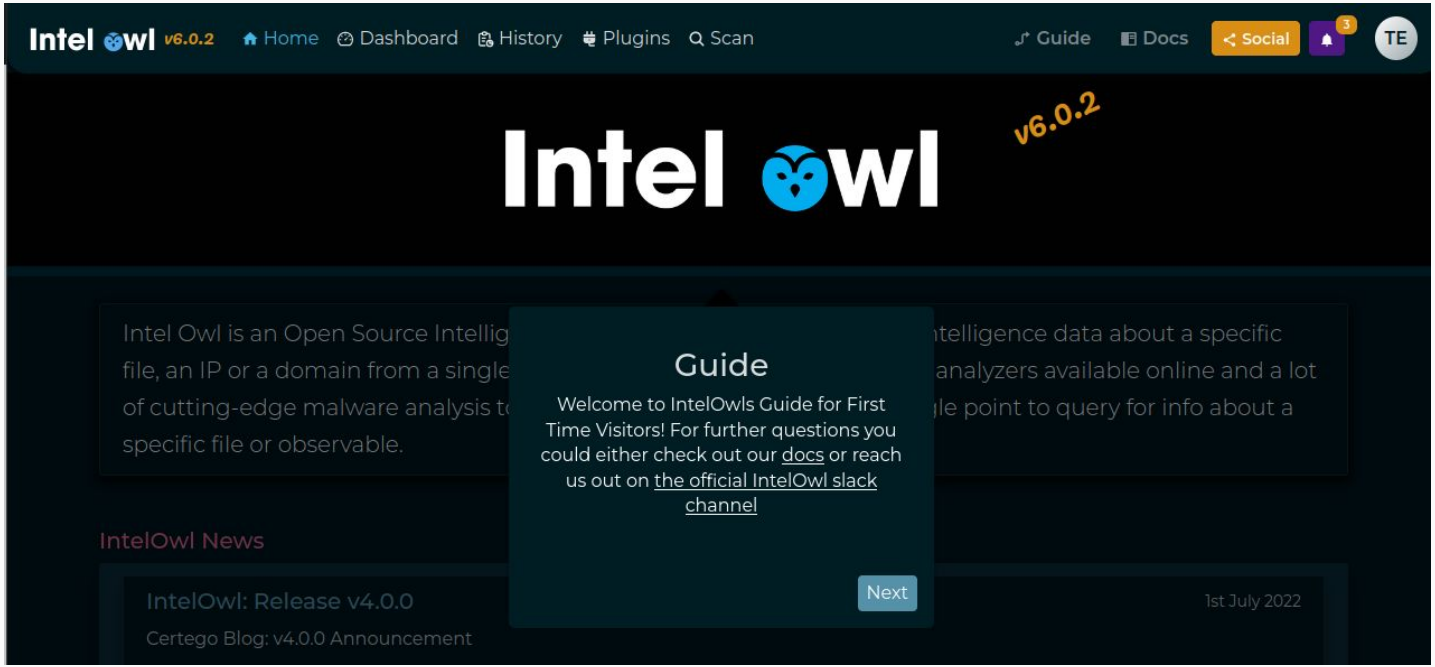
# now the application is running on http://localhost:80

# create a super user
```
```

IntelOwl Kick-off: Guide

Let’s Follow the Guide for a brief introduction to the main tools of IntelOwl



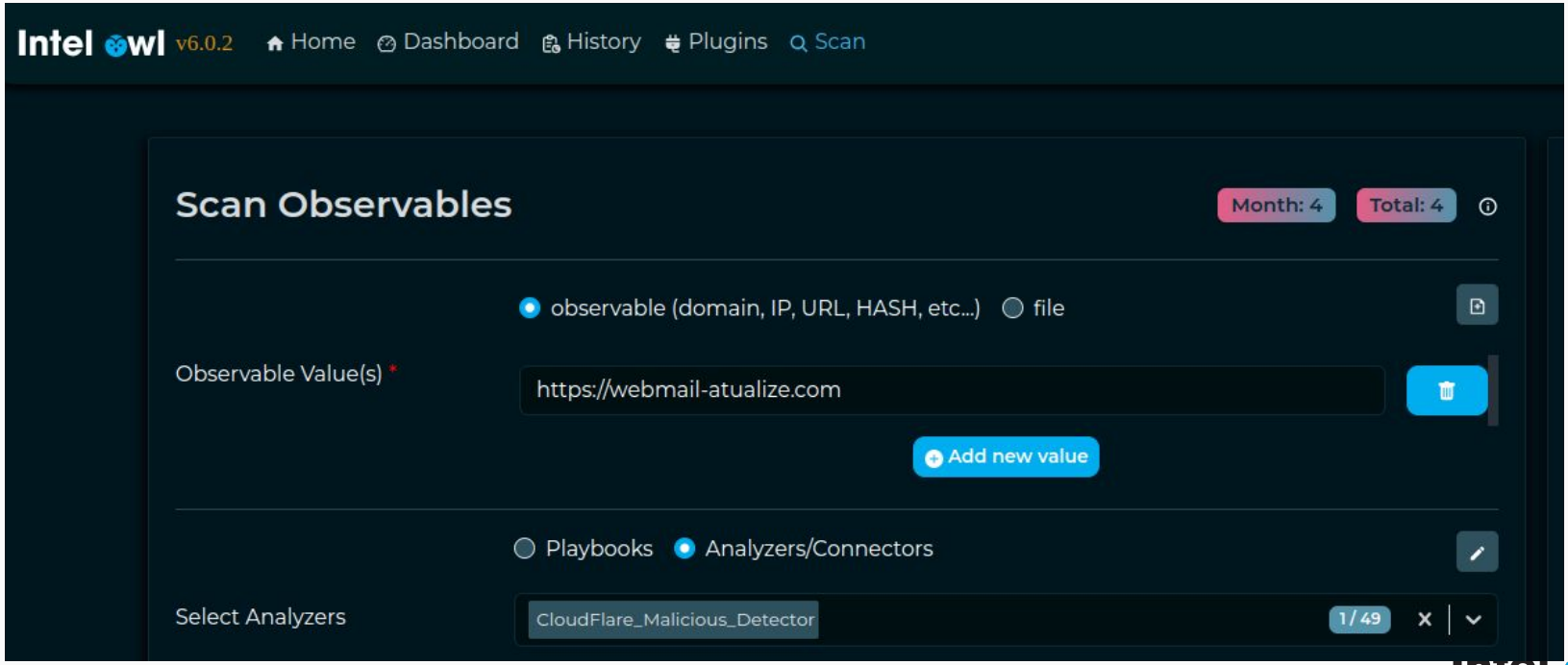


Intel owl

IntelOwl: Observables Analysis

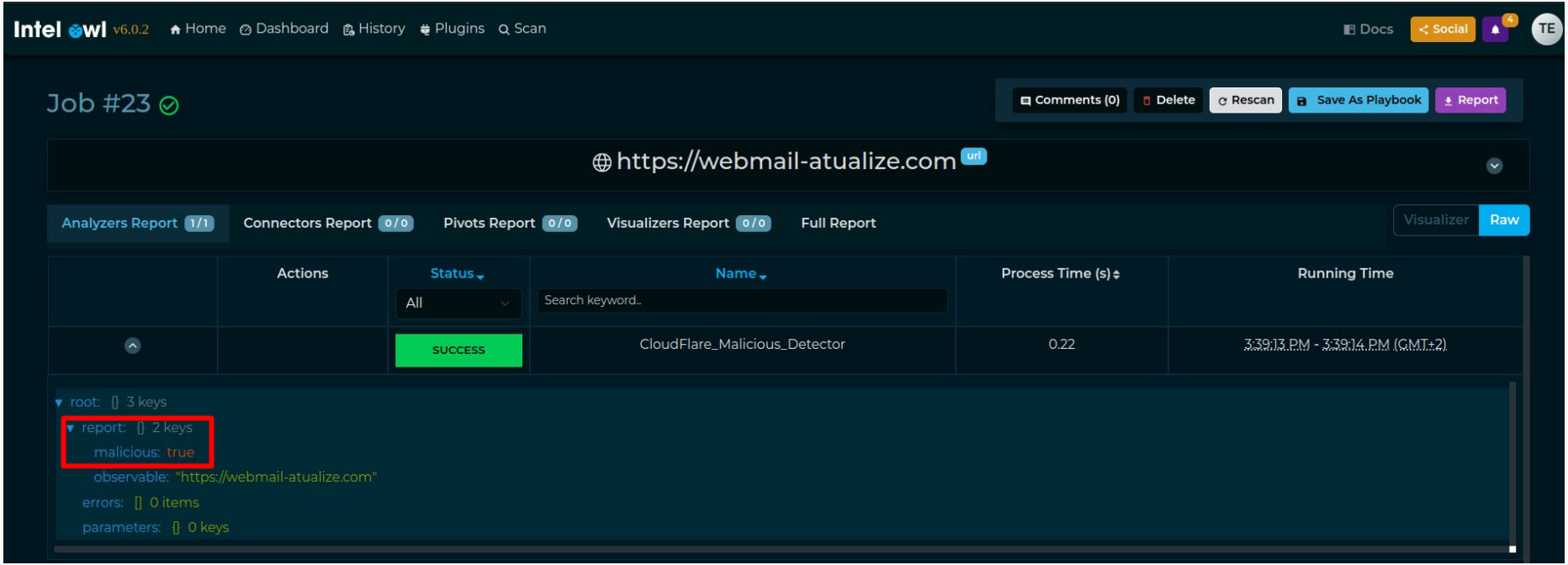
IntelOwl - Observables Analysis

IT'S YOUR TIME TO TRY:
Analyze *https://webmail-atualize.com* with analyzer *CloudFlare_Malicious_Detector*
What did you get?



IntelOwl - Observables Analysis

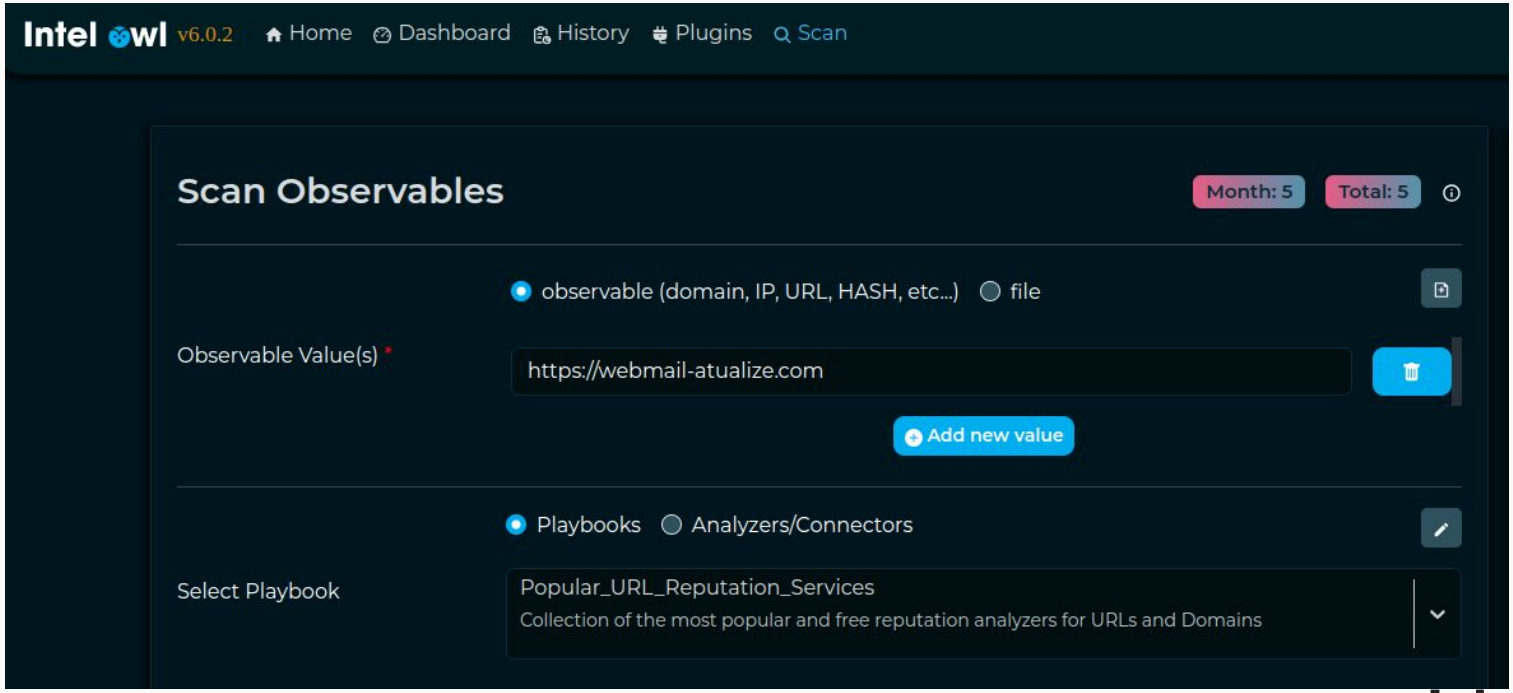
You can check the raw data extracted by the external service where we looked for.



Intel owl

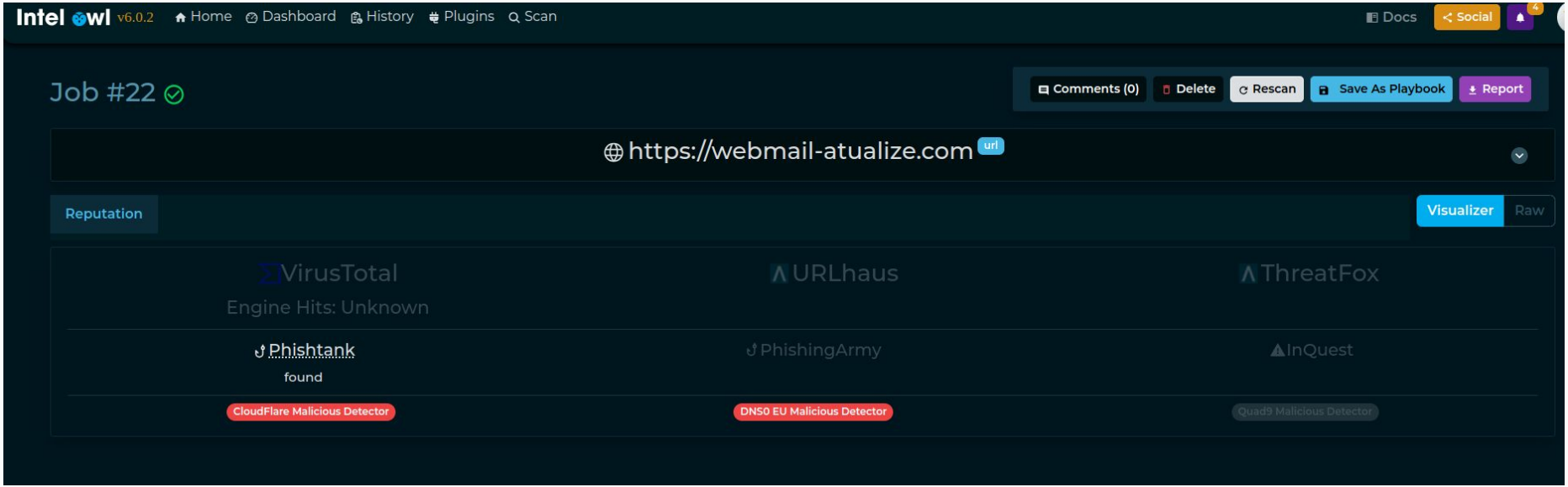
IntelOwl - Observables Analysis

IT'S YOUR TIME TO TRY:
Analyze *https://webmail-atualize.com* with the playbook *Popular_URL_Reputation_Services*
What did you find?



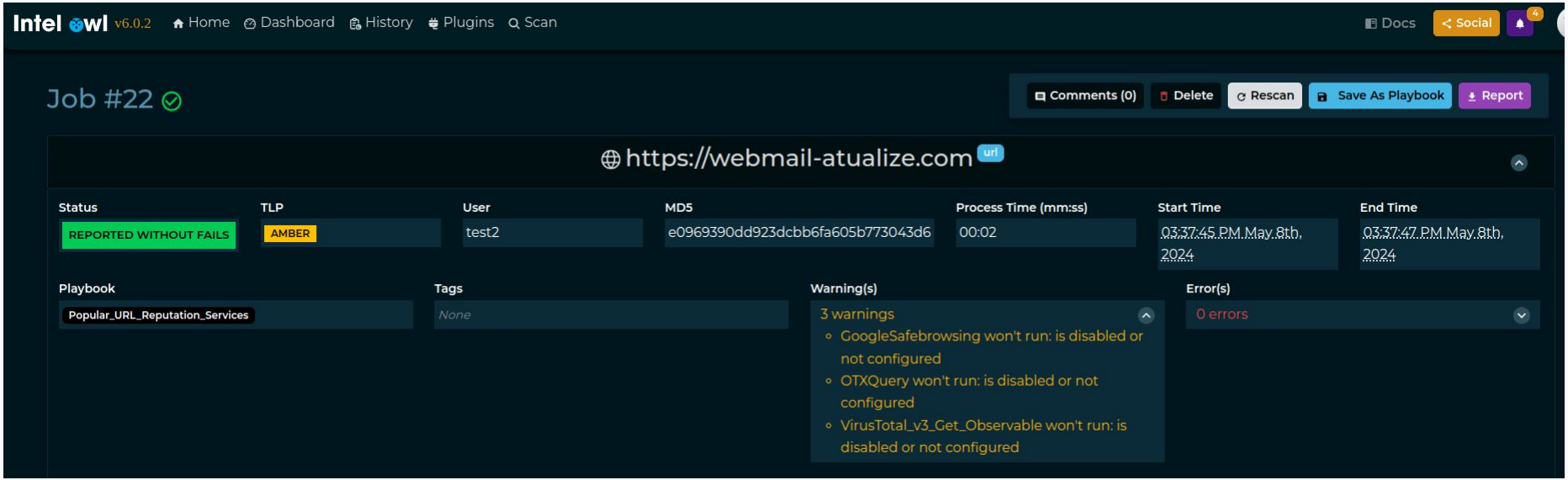
IntelOwl - Observables Analysis

You get a different and more “user-friendly” visualization. This is an example of a **Visualizer,** another type of Plugin. Visualizers are designed to run after the *analyzers*. The visualizer adds logic after the computations, allowing to show the final result in a different way than merely the list of reports. They can be customized and you can create your own personal visualizations.



IntelOwl - Observables Analysis

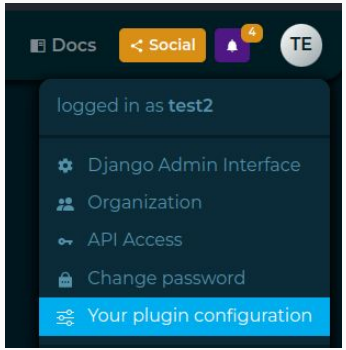
Some of the analyzers available in the playbook where not executed.
This happened because they require API keys to access their online services.

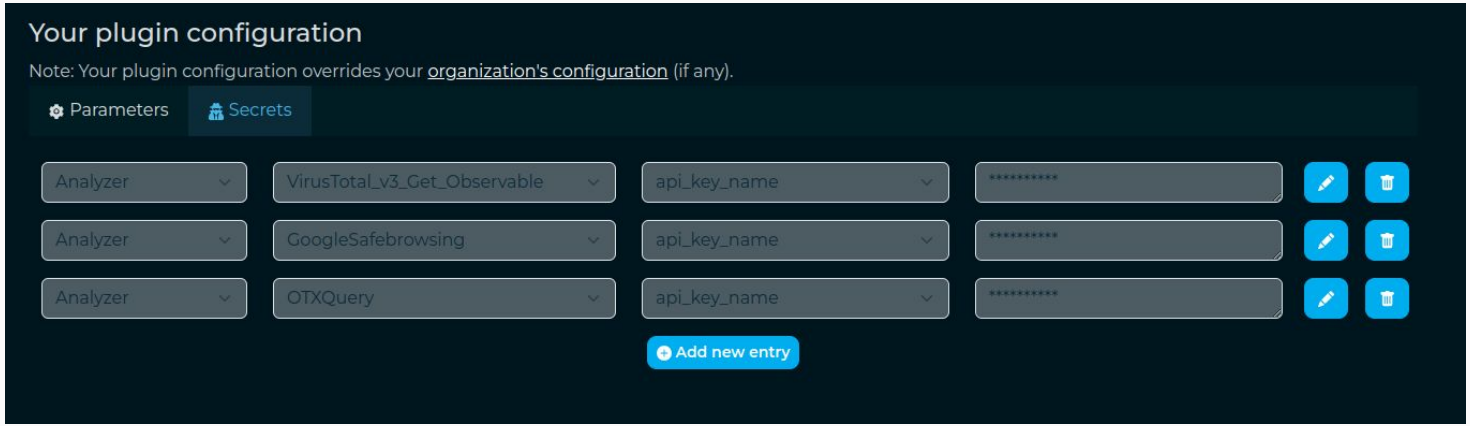


IntelOwl - Observables Analysis

Let’s configure those Analyzers!
IT’S YOUR TIME TO TRY:

- Register to Google Cloud, VirusTotal, OTX Alienvault to get the keys
- Add the keys as Secrets in the “Plugin Configuration” section



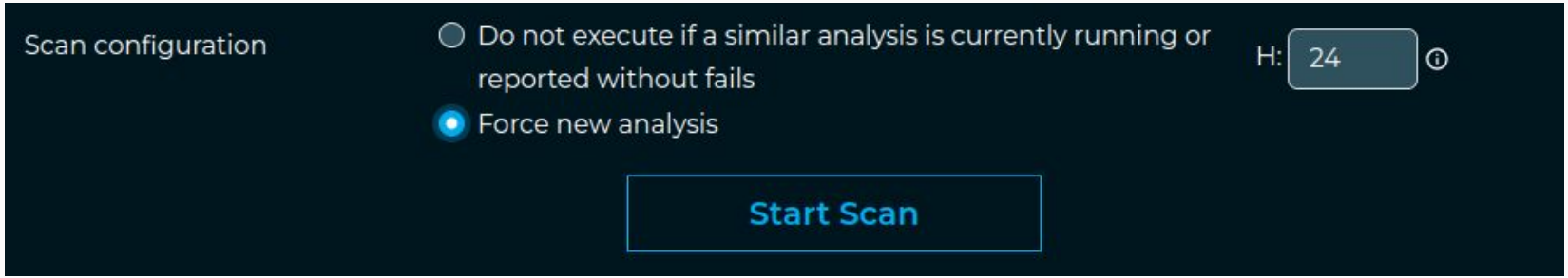


IntelOwl - Observables Analysis

IT'S YOUR TIME TO TRY:

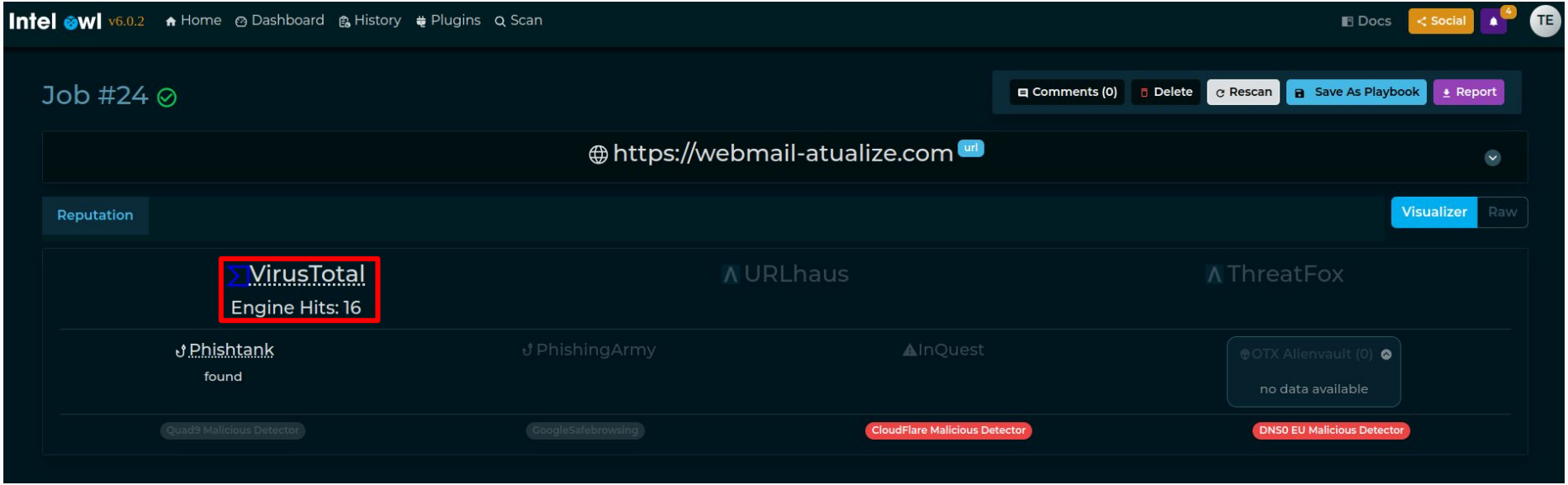
- Force a new analysis of *https://webmail-atualize.com* with the playbook *Popular_URL_Reputation_Services*. This is needed cause otherwise IntelOwl saves the computation and show you instantly the same old analysis. There is a default of 24 hours cache. Two ways to do that:
  - Button "Rescan" from the Old Analysis 

  - Select the Checkbox "Force new analysis" from the "Scan Page"



IntelOwl - Observables Analysis

This time we have more results thanks to the new configured Analyzers!

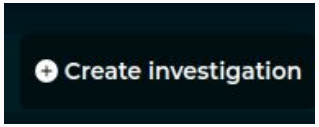


Intel owl

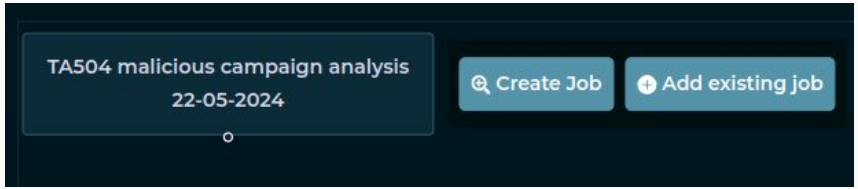
IntelOwl - Observables Analysis

IT'S YOUR TIME TO TRY:

- Let's do another analysis with the same Playbook for the URL *https://dnjja.com/login.php*, related to the same phishing campaign we are analyzing
- What did you find?
- Create a new Investigation with the button from the *History* page



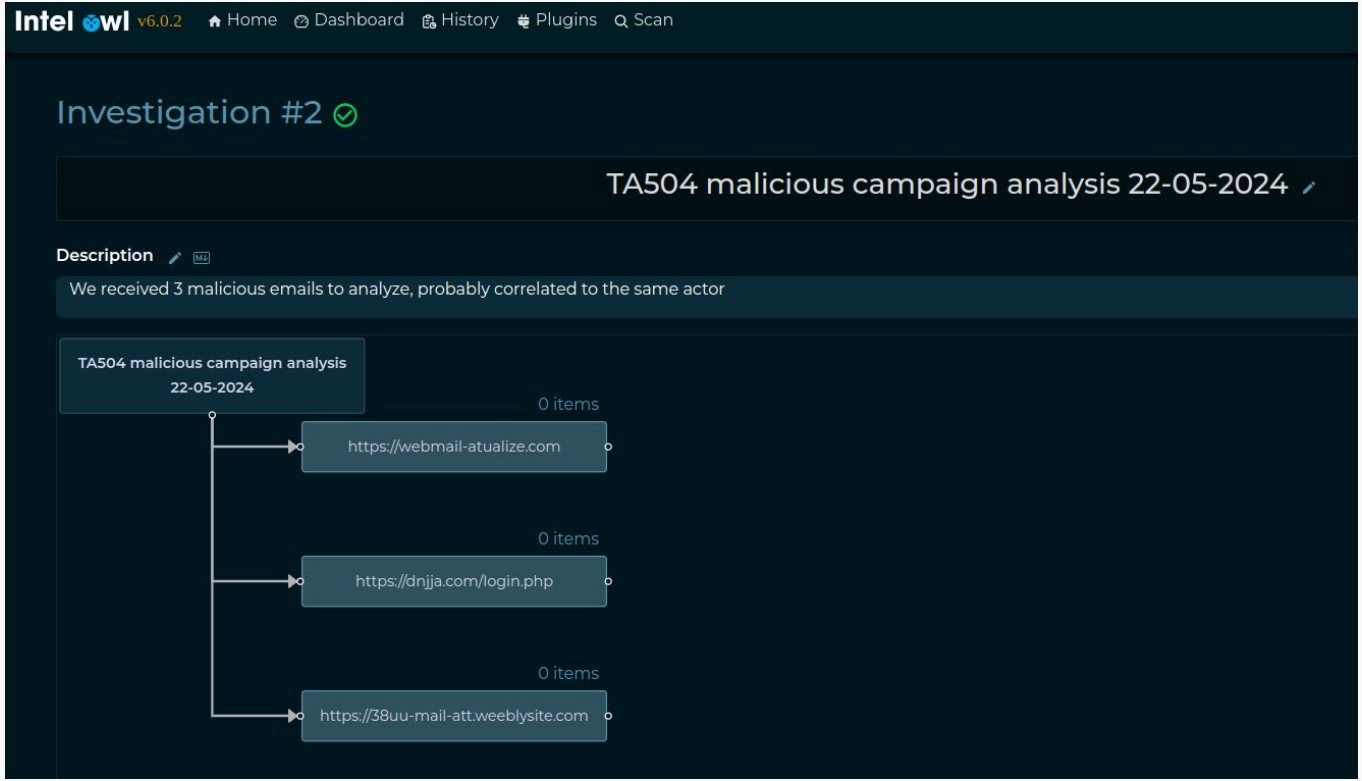
- Describe the malicious campaign
- Connect the analysis of the 2 URLs into the same Investigation by adding them via the "Add existing Job" button



- Add a new Job into the same investigation for a third found URL *https://38uu-mail-att.weeblysite.com/* by using the "Create Job" button

IntelOwl - Observables Analysis

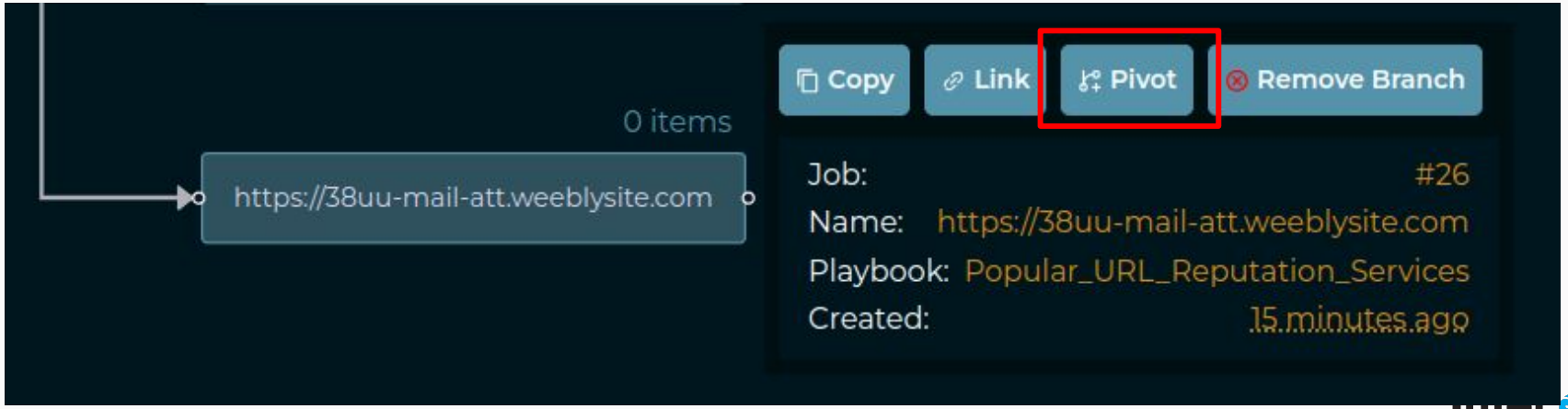
At this point you should have your Investigation compiled with 3 different URL analysis.



IntelOwl - Observables Analysis

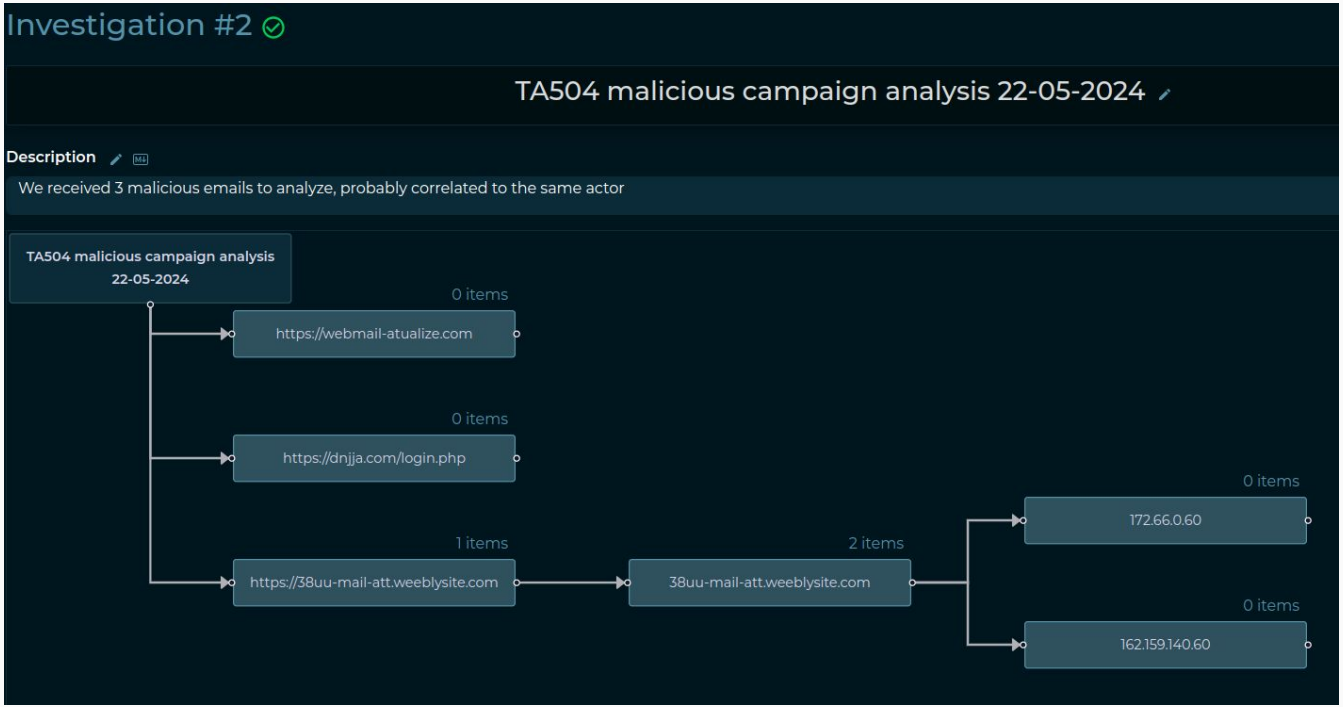
Let's get additional Information from the *https://38uu-mail-att.weeblysite.com* URL. IT'S YOUR TIME TO TRY:

- *Pivot* from that URL to Extract more information about it. This will link the new analysis to the same the investigation.
  - Leverage the "Pivot" button to analyze the domain (remove https://) via a different Playbook called *DNS* to extract the resolved IP addresses.
  - *Pivot* from the found IP addresses by leveraging a different "Pivot" button. You can find this button by hovering the IP addresses in the DNS Playbook visualization
  - Analyze those IP addresses with the *Popular_IP_Reputation_Services* Playbook.



IntelOwl - Observables Analysis

Now you should have a similar Investigation. Thanks to the “Pivot” feature, it is possible to create a Flow of analysis related to one another.



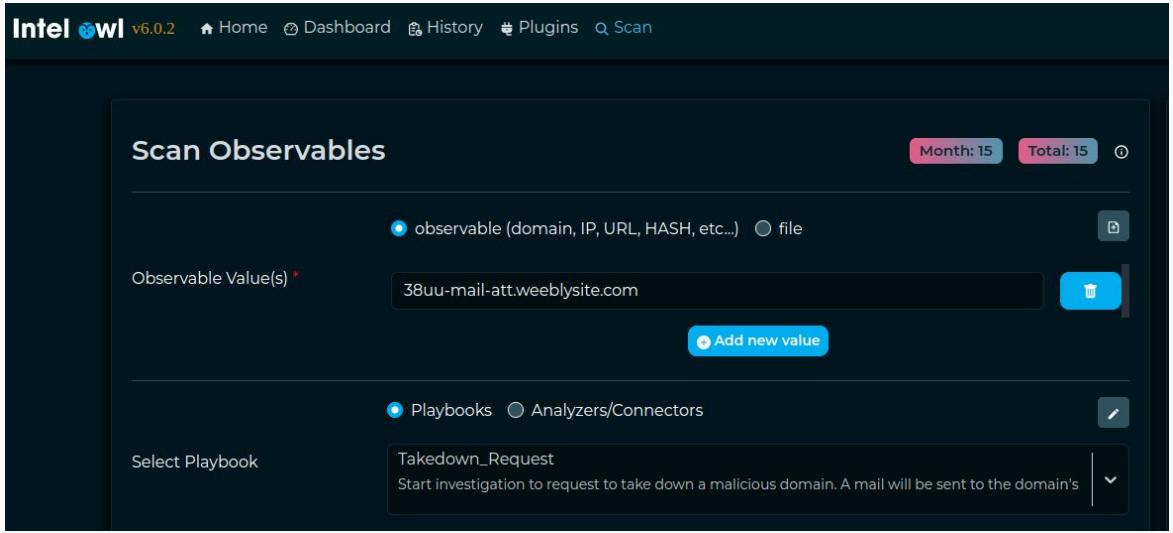
IntelOwl: Use Cases

IntelOwl - TakeDown Use Case

Thanks to the collected information, now we are sure that those domains are malicious and should be taken down by the host providers. How to automate the TakeDown Request?

IT'S YOUR TIME TO TRY:

- Takedown Request of 38uu-mail-att.weeblysite.com via the *TakeDown_Request* Playbook
- What happened? Did it work?



IntelOwl - TakeDown Use Case

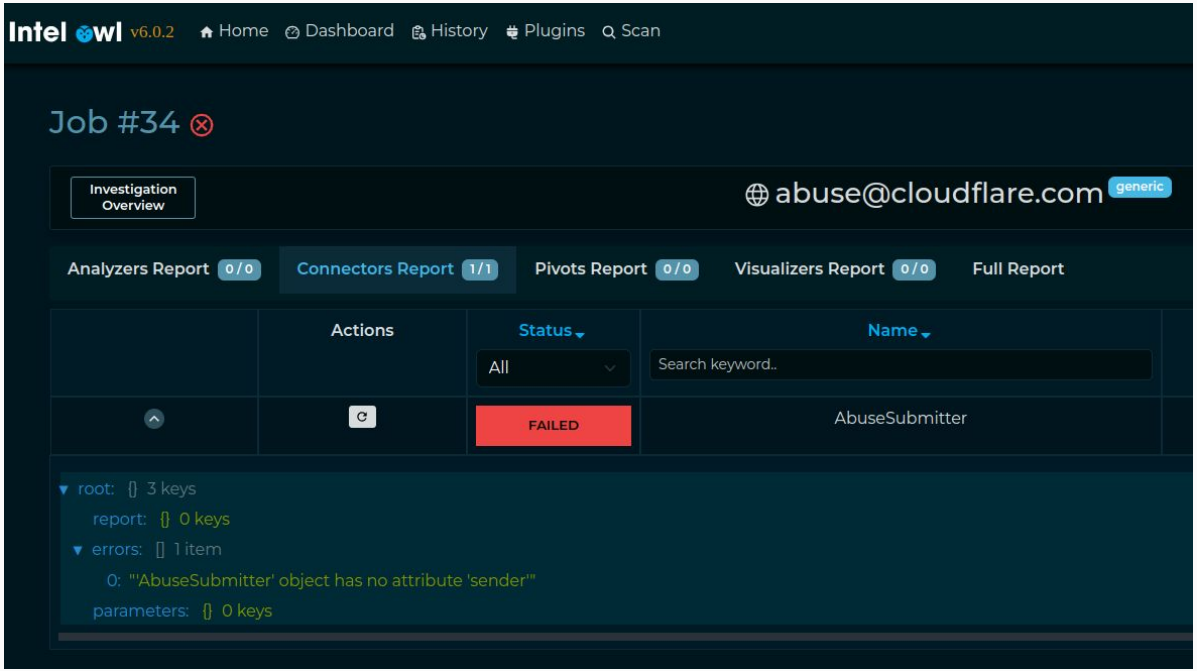
This Playbook has performed *automatic Pivots*:

- First, the Domain has been resolved to the IP address
- Then, the IP address has been analyzed to retrieve the Abuse Email for its Hosting Provider.
- Finally, an automatic email has been sent to the found Email

However, the last step failed. Why did that happen?

IntelOwl - TakeDown Use Case

We did not configure the *AbuseSubmitter* **Connector** with the parameters required to send the Email to the hosting provider.



IntelOwl - TakeDown Use Case

Ok but what's a **Connector**?

Connector is another type of Plugin. Connectors are designed to run after every successful analysis and are used mainly to send information to other platforms, like Threat-Sharing Platforms (MISP, OpenCTI, etc)

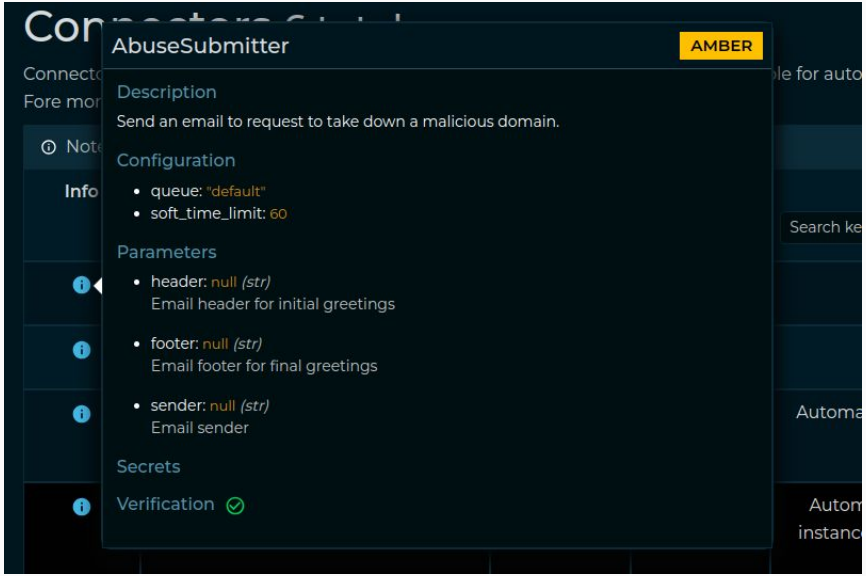
In the Analysis Pipeline, Connectors act as the second stage. You can always see how the pipeline worked by looking at the additional information of a specific Job.

IntelOwl - TakeDown Use Case

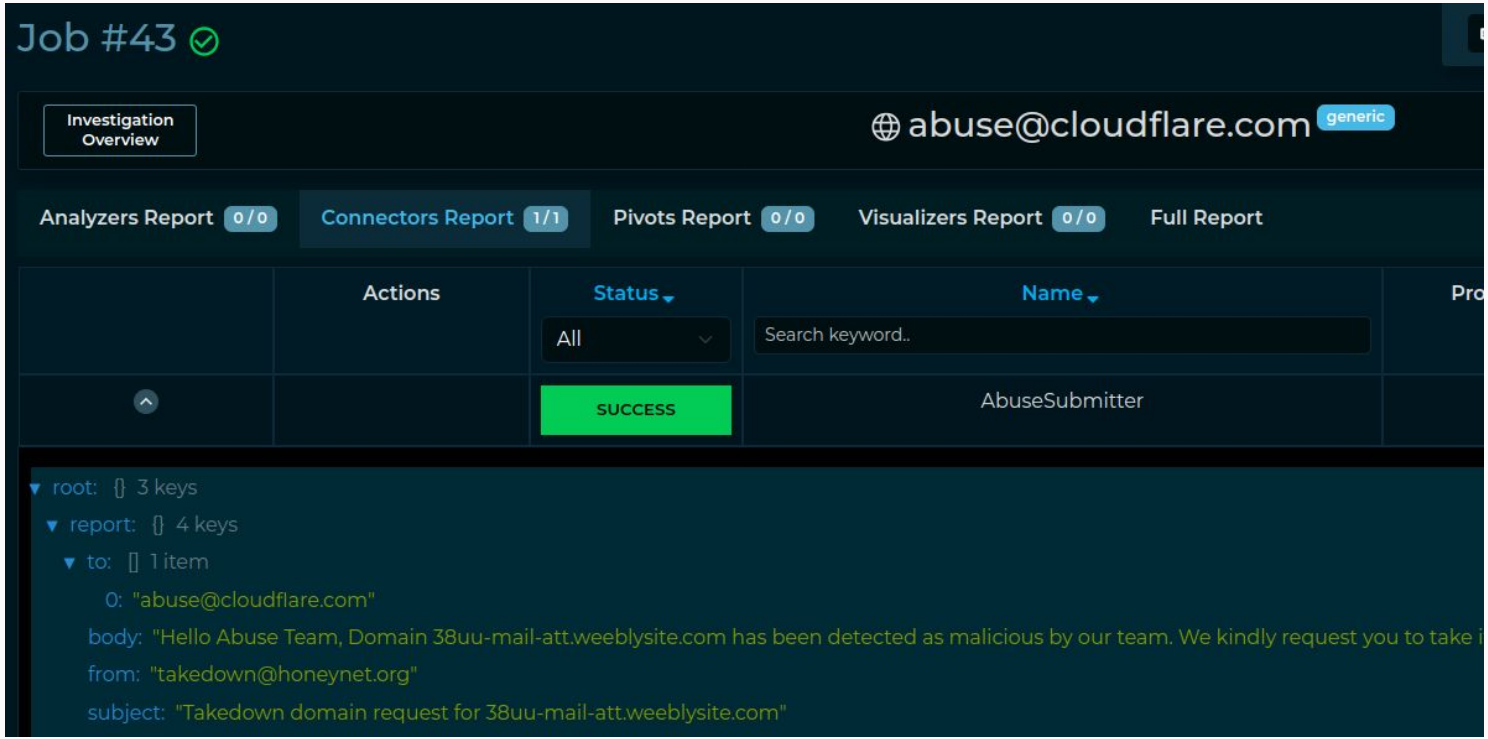
IT’S YOUR TIME TO TRY:

- configure the *AbuseSubmitter* Connector with the required Parameters
- Execute the TakeDown request again.

Don’t worry! The TakeDown Request won’t be sent if you are running IntelOwl in DEBUG mode, as you should by default.

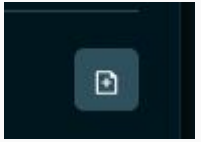


IntelOwl - TakeDown Use Case

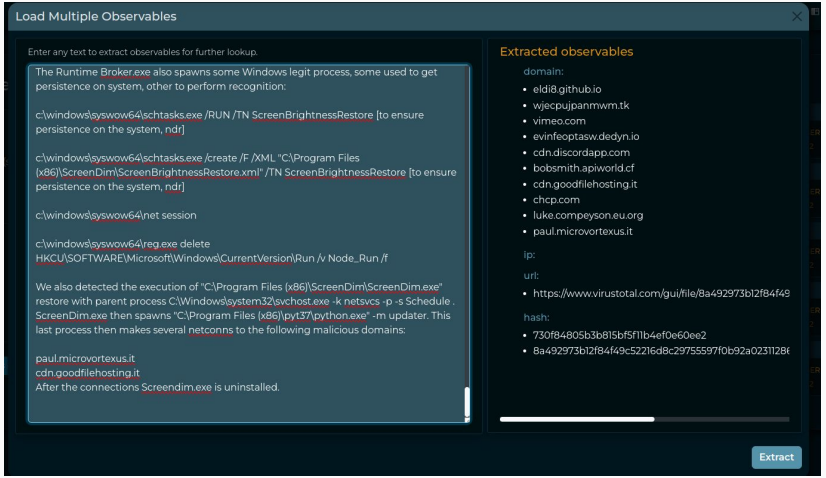


IntelOwl - Blog Post Analysis Use Case

Let’s say you are reading from a Blog Post of a Security Provider a report regarding an emerging threat.
You want to easily extract all the IOCs cited from that blog post and analyze them in IntelOwl to get more context about them.
Example: Certego Blog
IT’S YOUR TIME TO TRY:



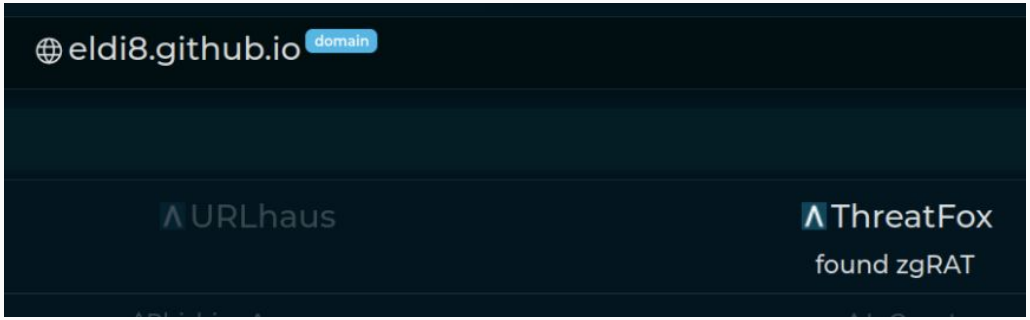
- Copy/Paste the Blog content into the Multi-Analysis Section of the “Scan” page.
- Remove the URLs you don’t want to analyze, like the VT link.
- Analyze the extracted observables.
- How many are already known to be malicious?
- Which threat is it? (understand it from the IntelOwl output)



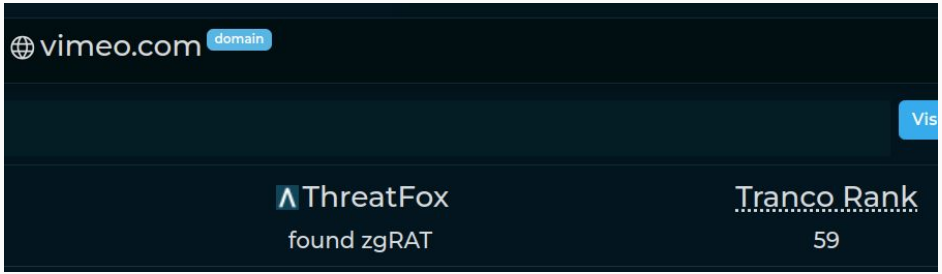
IntelOwl - Blog Post Analysis Use Case

- Not all of them are malicious:
  - *vimeo.com*, *cdn.goodfilehosting.it* and *cdn.discordapp.com* are abused services
  - *paul.microvortexus.it* is not known
- Other domains are evidence for a threat reported as **zgRAT** (Threatfox report)

eldi8.github.io has been found in the Threatfox Intelligence Database



vimeo.com is a high ranked domain. This means that the Threatfox Report is a False positive Report



IntelOwl - Connect your Instance to MISP

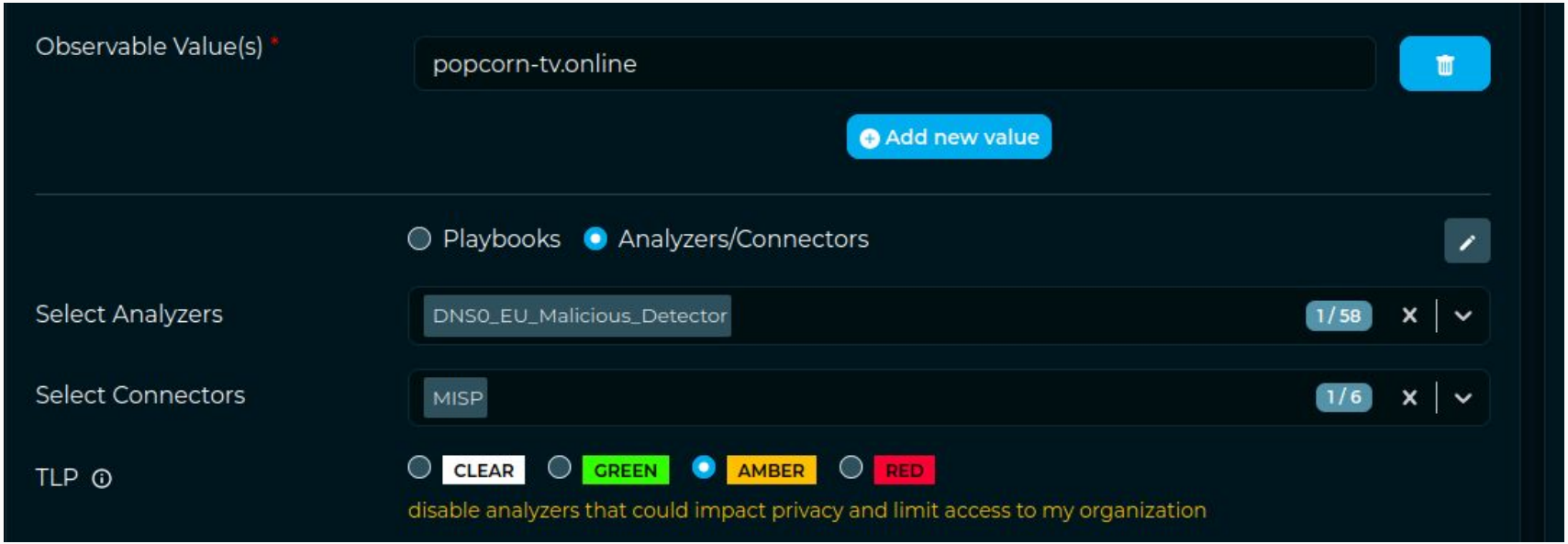
Let’s say we want to share our analysis to a different platform of any kind. We can either build a new Connector or leverage an already existing one.
IT’S YOUR TIME TO TRY:

- Download and Install a Dockerized MISP Instance from this Github repo
- Follow the instructions in the repo to start a new MISP instance in a fast way. Remember to change the docker-compose file to host the service into a different port than 80 that is already used by IntelOwl
- Generate an API key in the “Profile” section of the MISP
- Add a Plugin Configuration in IntelOwl for the MISP (API key and URL)
- Check if everything works as expected via the “Health Check” button from the “Plugin” page 
- Now we are ready to try the connector!

IntelOwl - MISP Export Use Case

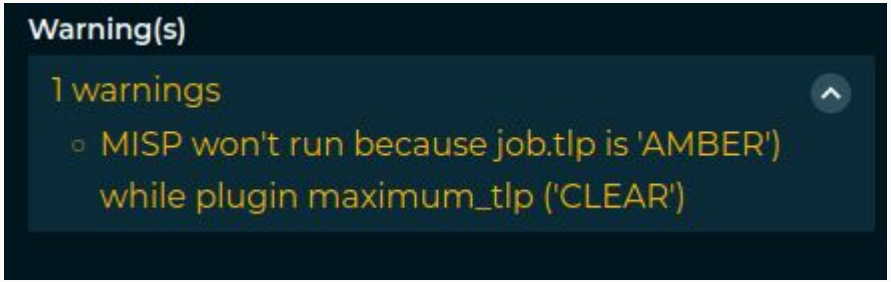
IT'S YOUR TIME TO TRY:

- Analyze the domain *popcorn-tv.online* with the analyzer *DNS0_EU_Malicious_Detector* and the connector *MISP*
- What happened, did it work?



IntelOwl - MISP Export Use Case

It seems the MISP connector hasn't been executed. Why?



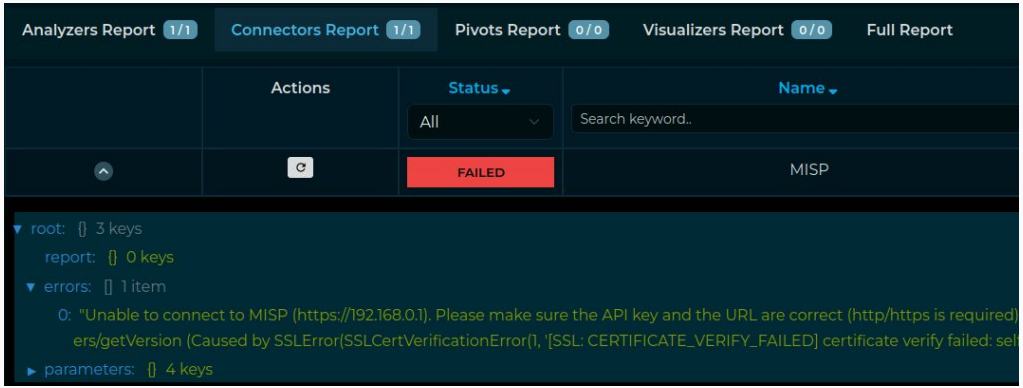
In IntelOwl there is the concept of TLP. Considering that the connector would have sent externally the data extracted by our analysis, only a TLP:CLEAR value is allowed. This is the default and can be changed.

IT'S YOUR TIME TO TRY:

- Let's analyze it again:
  - Flag the "Force new analysis" flag
  - Select the TLP: CLEAR
- Did it work now?

IntelOwl - MISP Export Use Case

It seems the MISP connector hasn't been executed again. Why?



By default, SSL verification is enabled but this is a local instance and we do not want to check it for this case. To do that, we have to change the Parameter used by the MISP connector. 2 ways to do that:

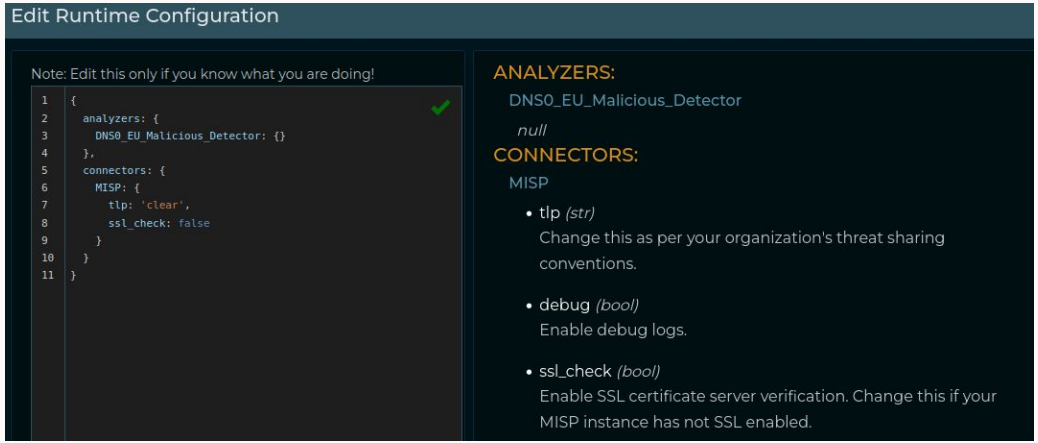
- Change the Parameter in the "Plugin Config" section. This is permanent for every other time you use the MISP connector
- Change the Parameter at "Runtime". In this way you change that parameter **only** for the Scan that you are about to do. To make this change, click the "Runtime configuration" button in the "Scan" page.

IntelOwl - MISP Export Use Case

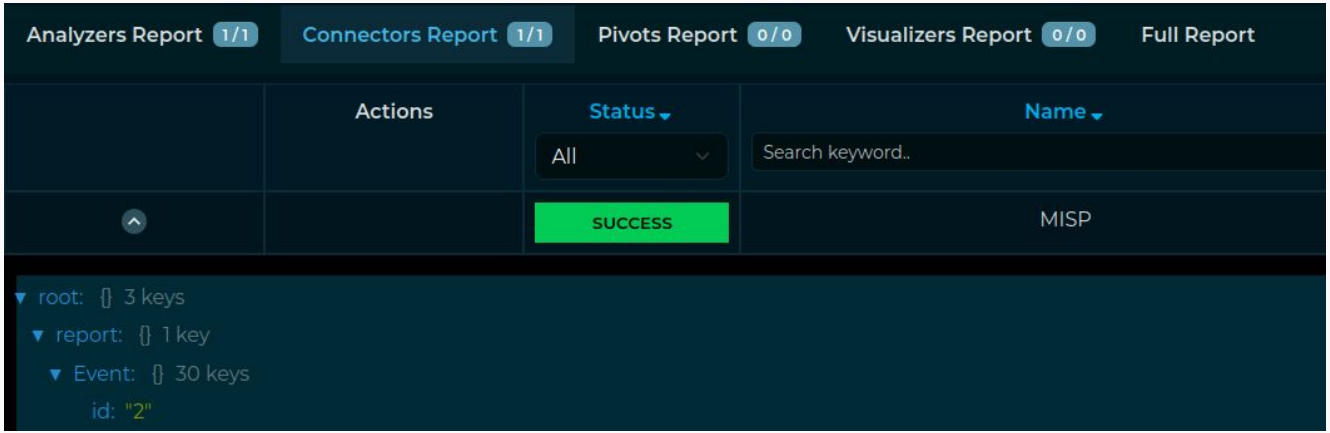
IT'S YOUR TIME TO TRY:

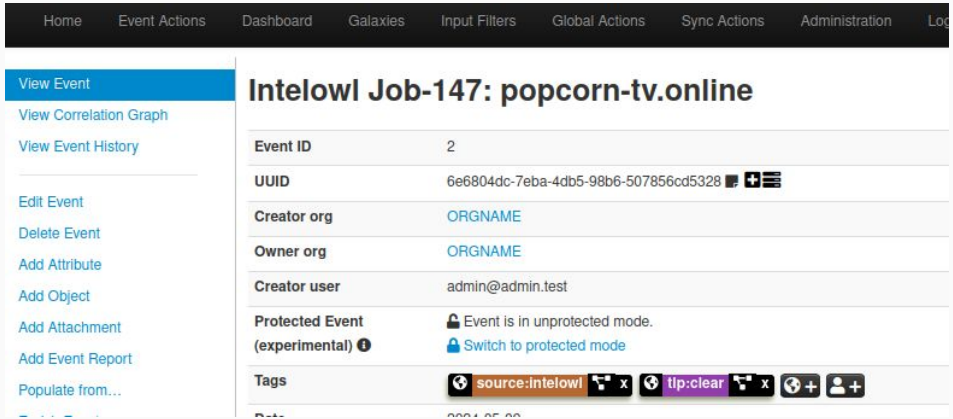
- Let's analyze it again:
  - Flag the "Force new analysis" flag
  - Select the TLP: CLEAR
  - Change the *ssl_check* Parameter to *false* in the Runtime Configuration

- Did it work now?



IntelOwl - MISP Export Use Case





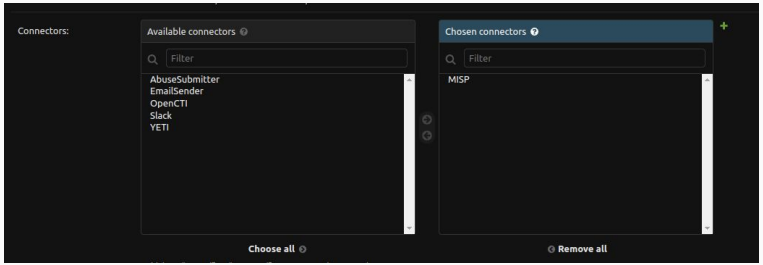
IntelOwl - MISP Export Use Case (EXTRA)

Let’s say we want to add the MISP connector to a Playbook that we use to automatically export all the analysis.

Right now this can be done only by administrators from the Django Admin section.

IT’S YOUR TIME TO TRY:

- Go to the Django Admin
- Go to the “Playbook configs” section.
- Select the Playbook you want to change. For instance *Popular_URL_Reputation_Services*.
- Add the MISP to the “Chosen connectors” section.
- Click the “Save” button.
- Now analyze *popcorn-tv.online* with the playbook *Popular_URL_Reputation_Services*
- You can see your results into your MISP!

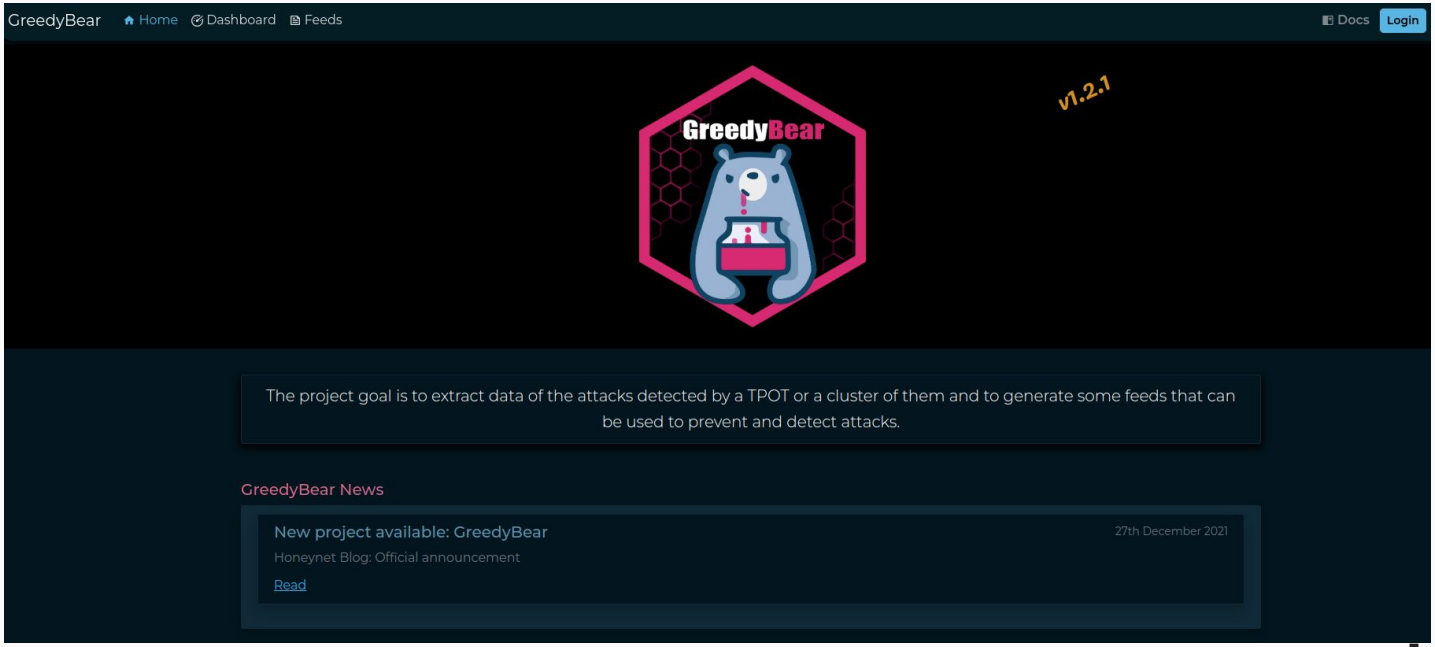


IntelOwl - GreedyBear Integration

In IntelOwl you can find an Analyzer for a specific service called GreedyBear.

Greedybear is a Threat Intel Platform for T-POTs. You can find the public instance hosted by Honeynet here.

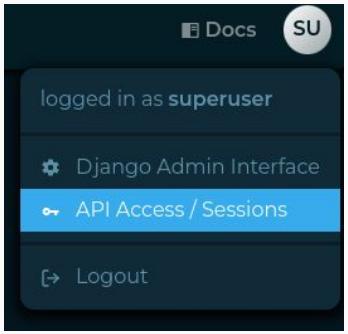
You can extract a lot of information regarding malicious IP addresses belonging to botnets here!

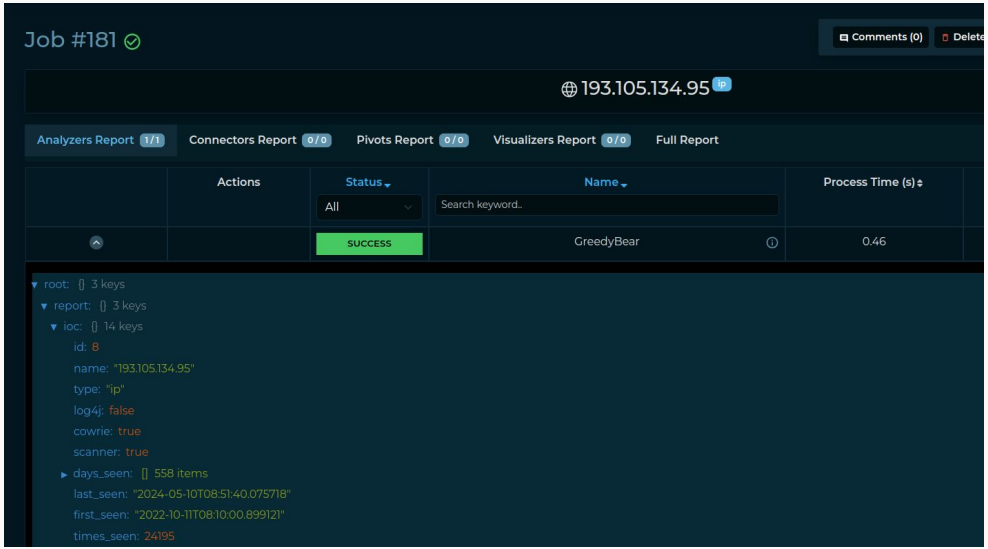


IntelOwl - GreedyBear Integration

IT'S YOUR TIME TO TRY:

- Request user creation by contacting us on Twitter.
- Login to your account and generate an API key from the "API Access" section.
- Configure the *GreedyBear* Analyzer API Key in IntelOwl from the "Plugin Configuration" section.
- Analyze the IP address *193.105.134.95* in IntelOwl with the *GreedyBear* Analyzer.





IntelOwl: Files Analysis

IntelOwl File Analysis

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: Y*ara, 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:

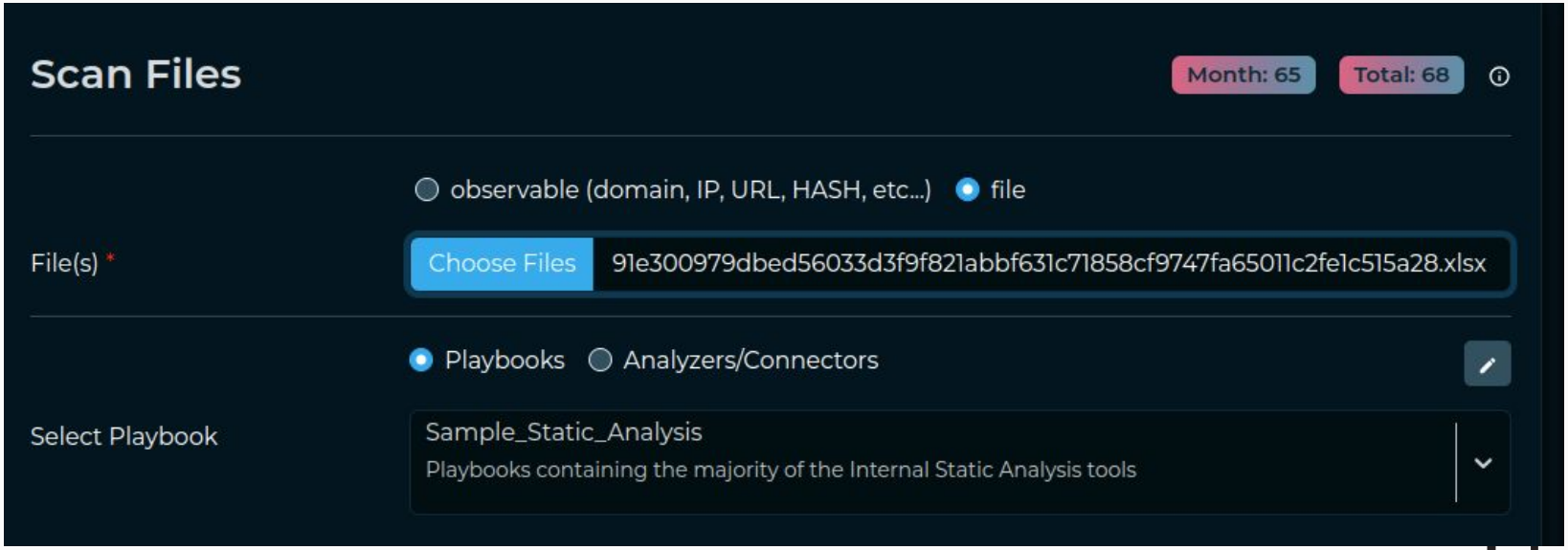
```
./start prod down && ./start prod up --malware_tools_analyzers
```

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

IntelOwl File Analysis - Static Analysis - XLS

IT'S YOUR TIME TO TRY:

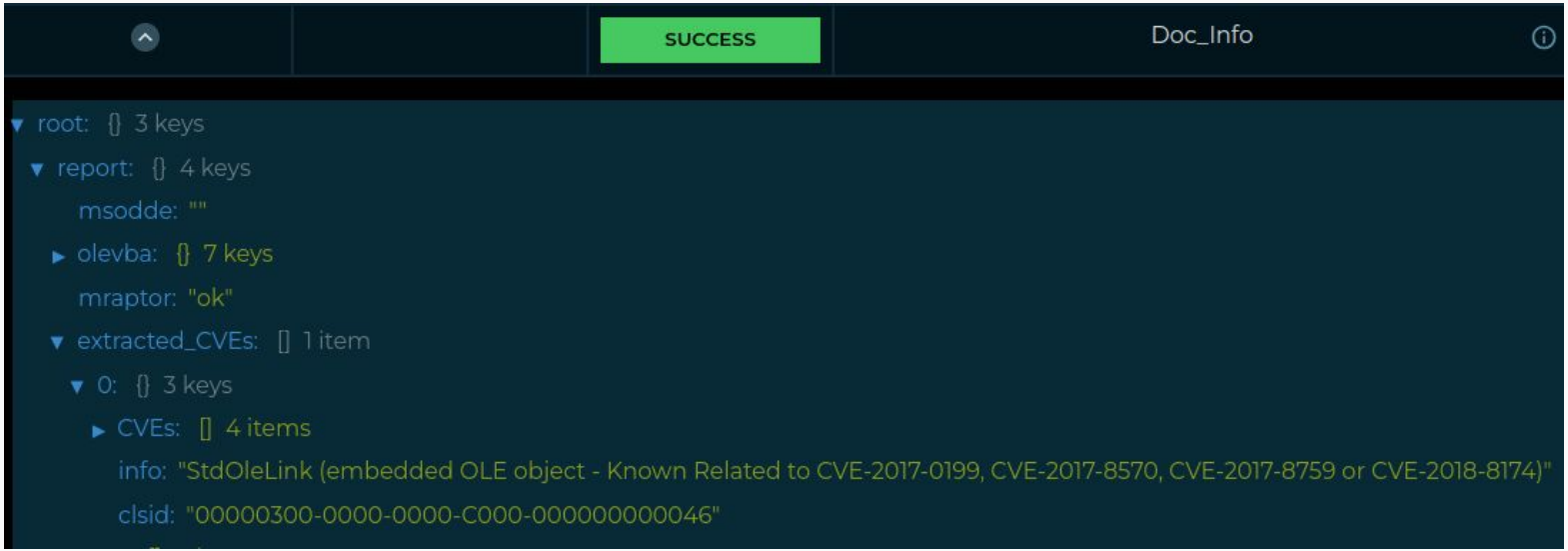
- Leverage the *Sample_Static_Analysis* Playbook (requires no configuration) to analyze the following file extracted from MalwareBazaar: XLS sample
- What did you find?



IntelOwl File Analysis - Static Analysis - XLS

This Playbook has no Visualizer attached. We need to check out all the Analyzers Reports for useful results:

- *Doc_Info* found different things:
  - possible exploit of known vulnerabilities
  - encrypted file with the default password “VelvetSweatshop” (Read-Only mode)



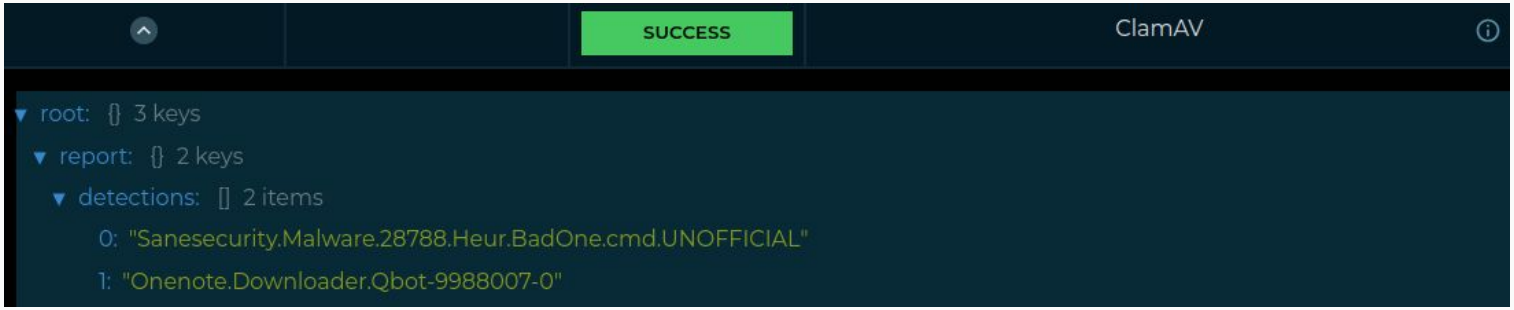
IntelOwl File Analysis - Static Analysis Exercise

- IT'S YOUR TIME TO TRY:
- Use the *Sample_Static_Analysis* Playbook to analyze different type of files to explore all the static analyzers available in IntelOwl.
  - OneNote file
  - PDF file
  - Javascript file
  - APK file
  - Portable Executable file
- Find some "evidence" of maliciousness for each file.

IntelOwl File Analysis - Static Analysis - OneNote

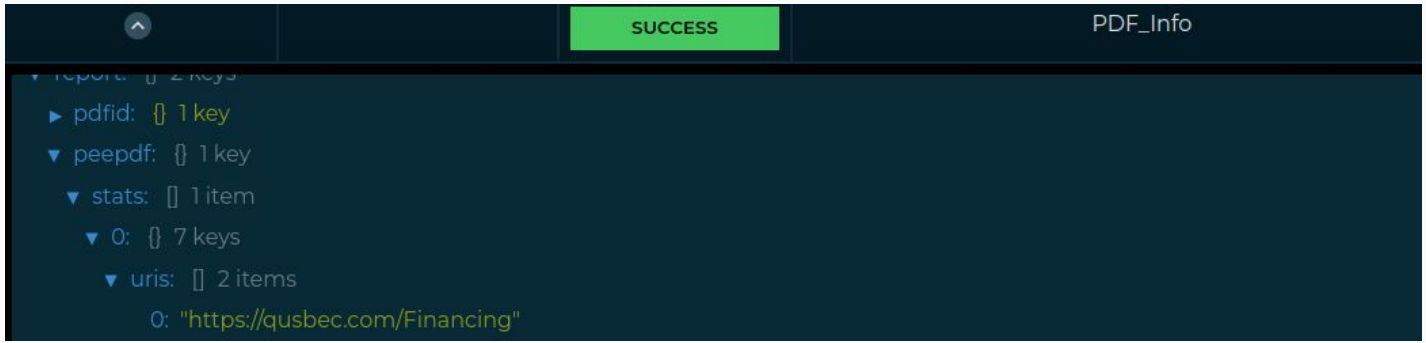
- Specific *OneNote_Info* analyzer does not provide too much useful information
- *ClamAV* detects it
- *Yara* finds an anomaly in the OneNote file structure

PLEASE NOTE! IntelOwl automatically downloads *Yara* and *ClamAV* open source rules and keep them updated. But you can add your own custom signatures for *Yara* and *ClamAV*. Check the docs.



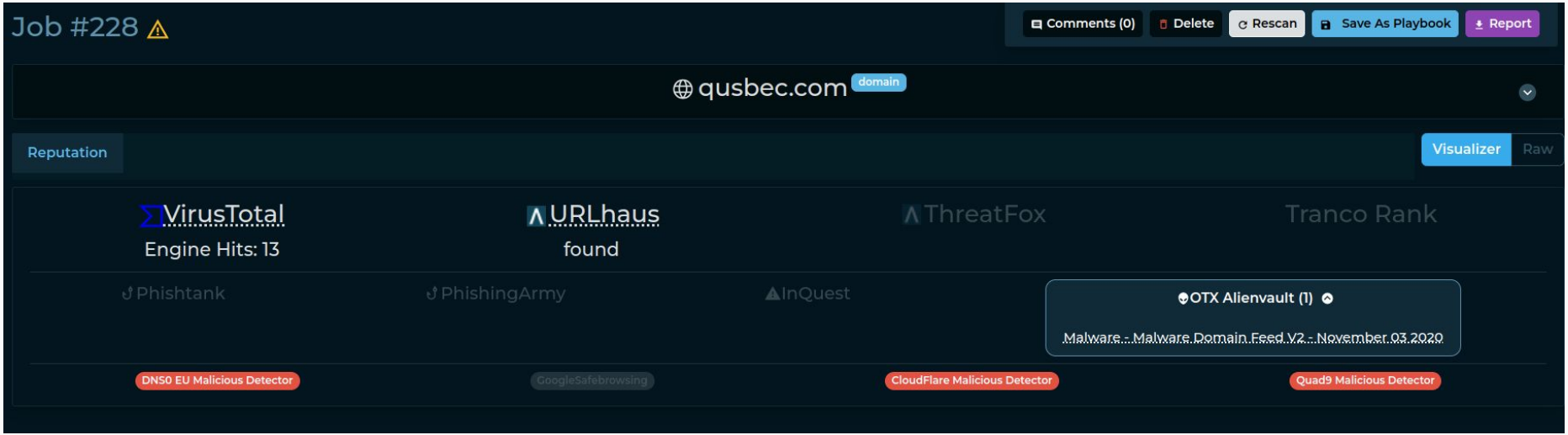
IntelOwl File Analysis - Static Analysis - PDF

- Specific *PDF_Info* analyzer extracts a suspicious embedded URL
- *ClamAV* detects it as malicious
- *Yara* detects it as a MalDoc



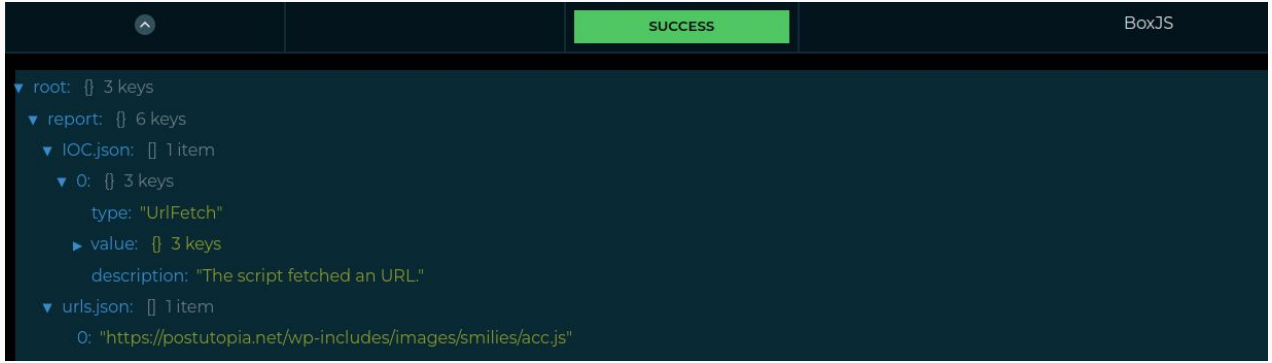
IntelOwl File Analysis - Static Analysis - PDF

- The URL extracted from the *PDF_Info* Analyzer (*qusbec.com*) is known to be malicious

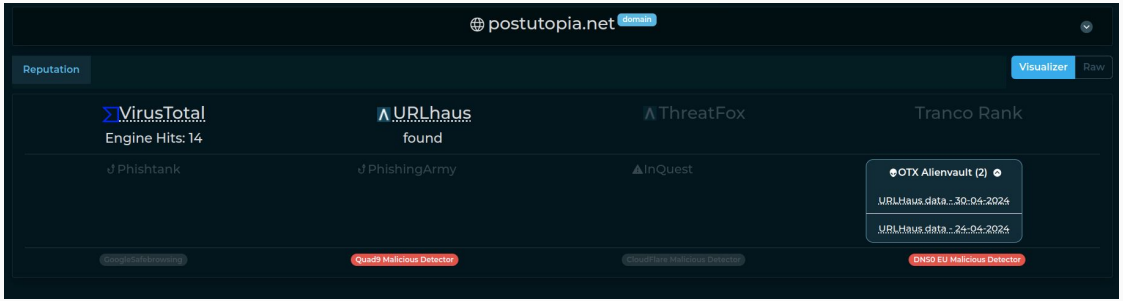


IntelOwl File Analysis - Static Analysis - Javascript

- Specific *BoxJS* analyzer extracts a suspicious embedded URL

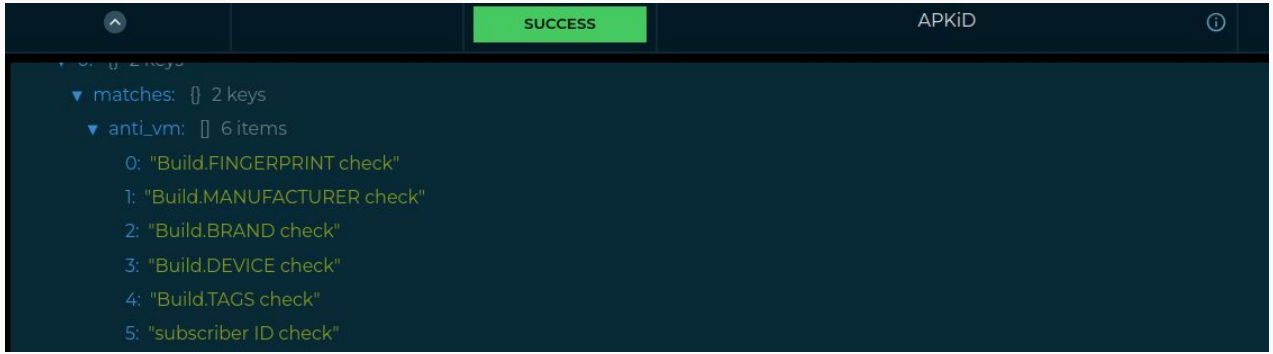


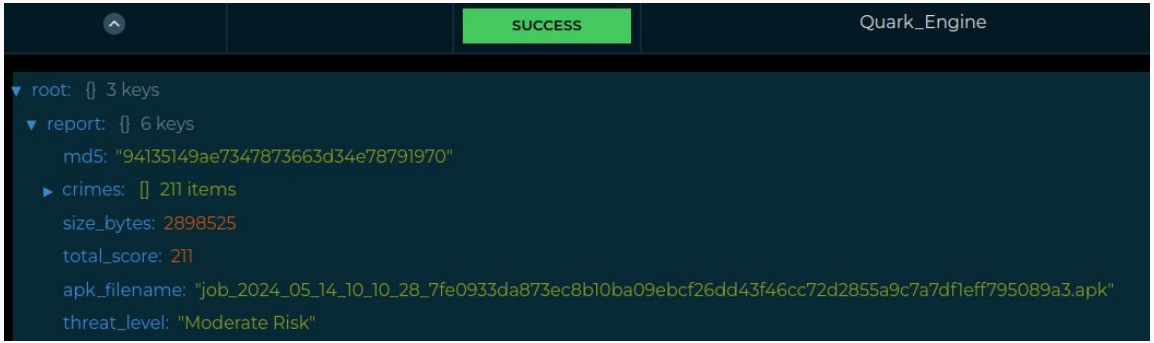
- The URL extracted from the *PDF_Info* Analyzer (*postutopia.net*) is known to be malicious



IntelOwl File Analysis - Static Analysis - APK

- Specific *APKiD* analyzer found some *anti_vm* checks.
- Specific *Quark_Engine* analyzer found a lot of *crimes* (detection rules) and evaluated the sample as "Moderate Risk"

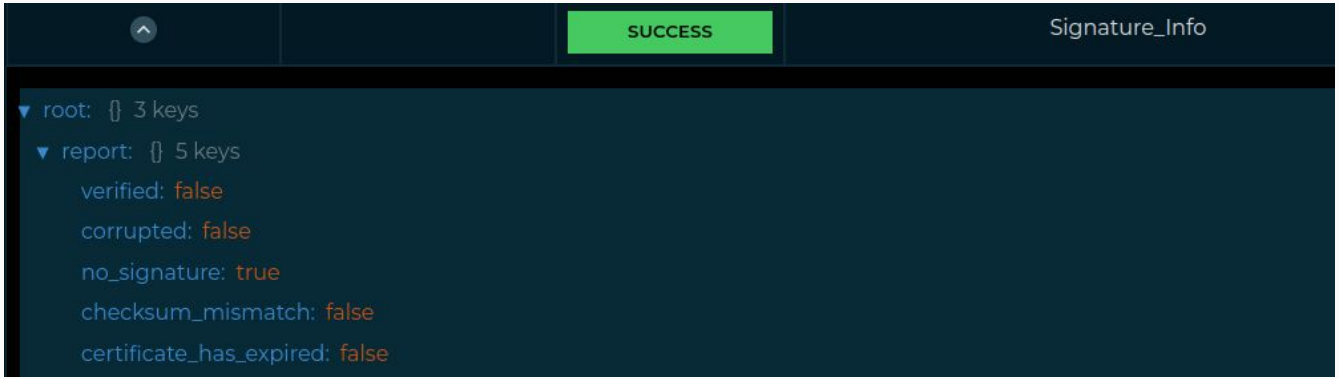




IntelOwl File Analysis - Static Analysis - EXE

- Specific *Signature_Info* analyzer tells you that the file is not signed
- Specific *PE_Info* file detects some anomalies
- Specific *CAPA_Info* and *Blint* find few anomalies
- *ClamAV* detects it

But we did not get enough information to understand better what it does.

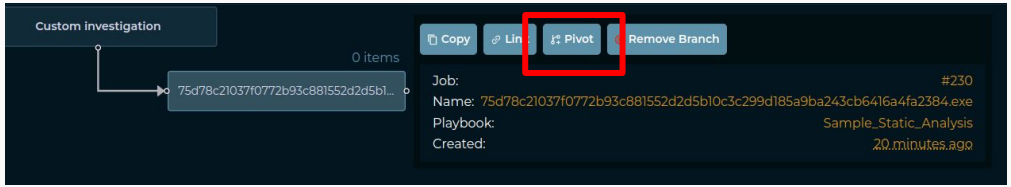


IntelOwl File Analysis - EXE

IT'S YOUR TIME TO TRY:

Let's get a second opinion with online services. Pick the ones that you like the most. Some suggestions are VirusTotal, Intezer, FileScan, Triage, HybridAnalysis, MWDB, etc. Then:

- Configure the secrets of the services you chose in your Plugin Configuration.
- Create a new Investigation with the static analysis you have done earlier.
- *Pivot* from Static Analysis to Analyze the File Again with the Analyzers you chose.

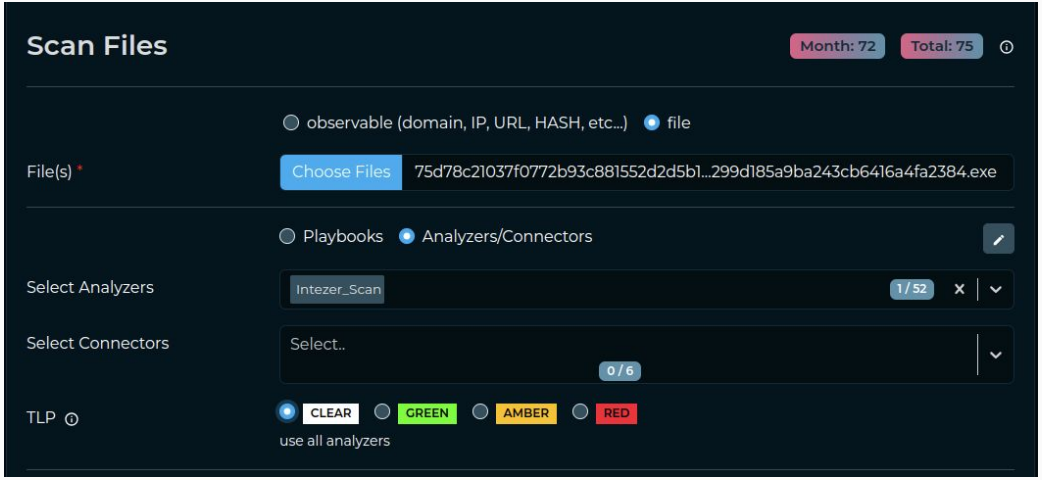


- Create a new Playbook so you can replicate that type of analysis again and call it *Dynamic_Analysis.*

- Use the 2 Playbooks (static and dynamic analysis) in a chain again to associate another sample of AgentTesla to the same Investigation. We'll try with this one.

IntelOwl File Analysis - EXE

We chose *Intezer_Scan* as Dynamic Analyzer and that sample has been found known malicious by that service!



Let’s analyze the second sample!

IntelOwl File Analysis - EXE

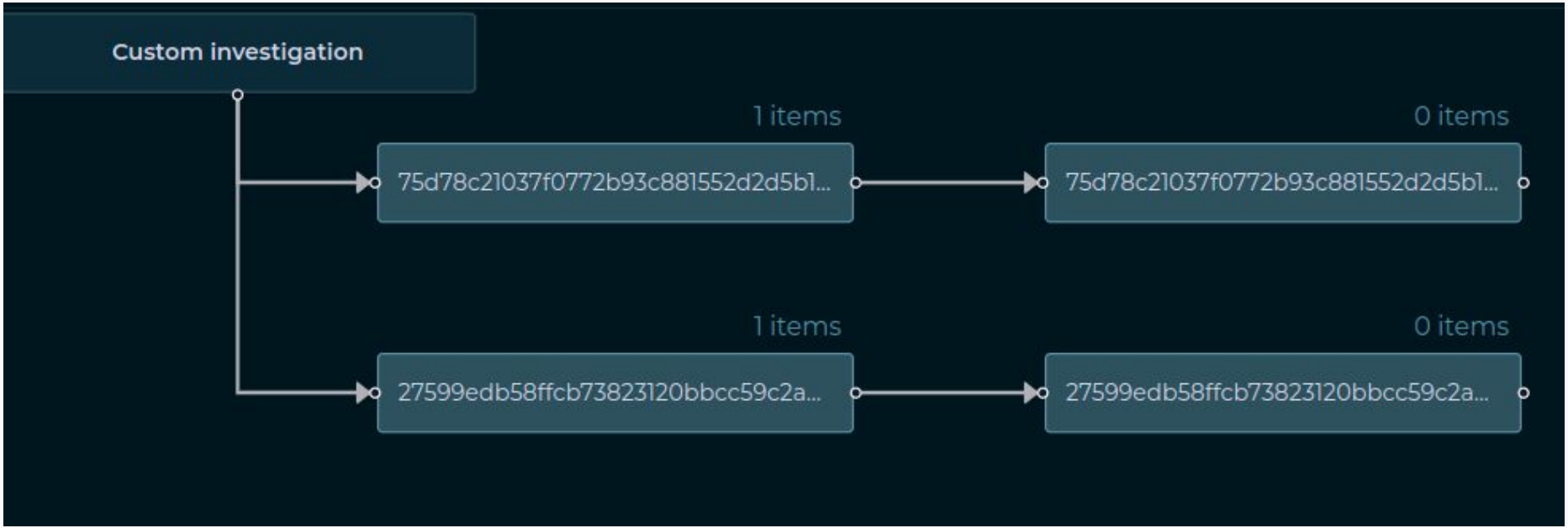
- Specific *Signature_Info* analyzer tells you that the file is not signed
- This time *Capa_Info* provides more useful guesses on the capabilities of the executable.
- *Strings_Info* shows randomic Strings as an indication of strong obfuscation or encryption
- There's no *ClamAV* detection

We are most probably working with a packed sample with anti-analysis features.

Dynamic Analysis could reveal its true identity. Let's do it with the new created Playbook!

IntelOwl File Analysis - EXE

Final Investigation Schema

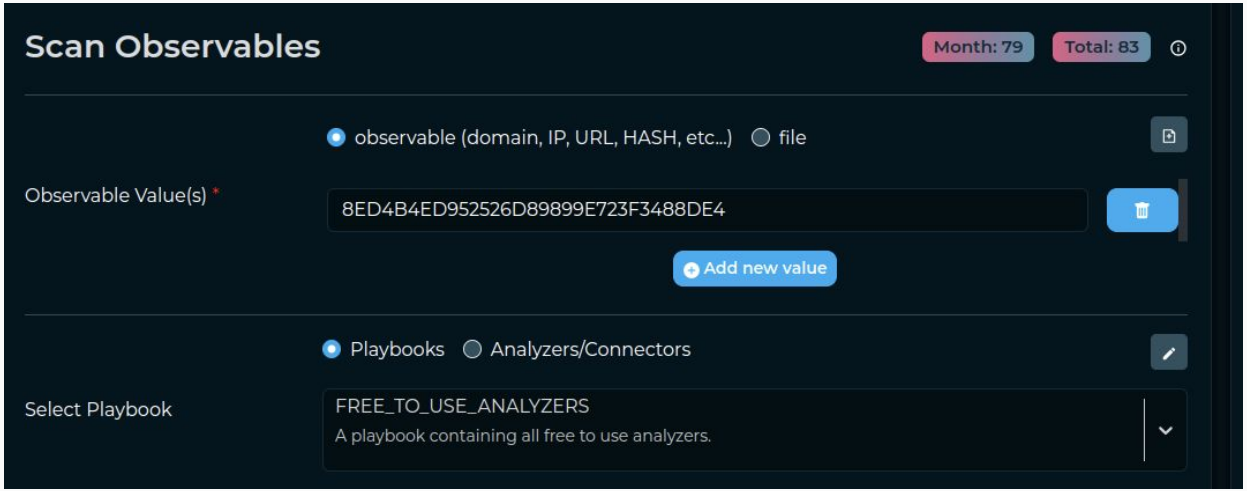


IntelOwl File Analysis - Hash

It may happen that you gets an hash of a file but you don’t have the sample itself. How to proceed?

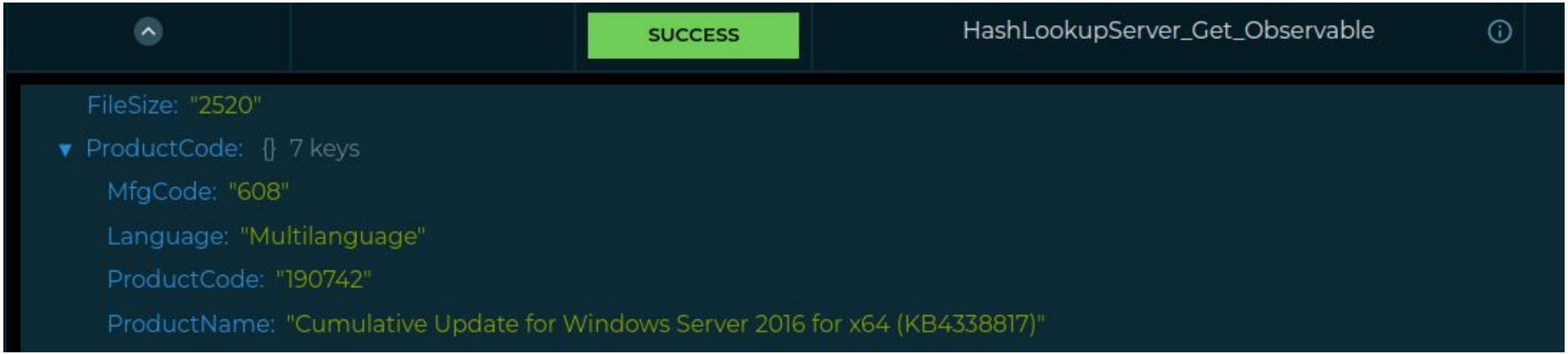
IT’S YOUR TIME TO TRY:

- Analyze an Hash found in the wild: *8ED4B4ED952526D89899E723F3488DE4* with the default *FREE_TO_USE_ANALYZERS* Playbook.
- What did you find?



IntelOwl File Analysis - Hash

- The Specific *HashLookupServer* analyzer found it in a list of Trusted hashes.



IntelOwl File Analysis - PCAP

IntelOwl embeds some analyzers dedicated to PCAP files: *HFinger* and *Suricata*.

Suricata is available in an additional container. Let's spin it up:

```
./start prod down --malware_tools_analyzer  && ./start prod up --pcap_analyzers
```

Once loaded, *Suricata* will download the open source signatures automatically and it will update them periodically. Plus, you can add your own signatures. This is a good way to test your own signatures.

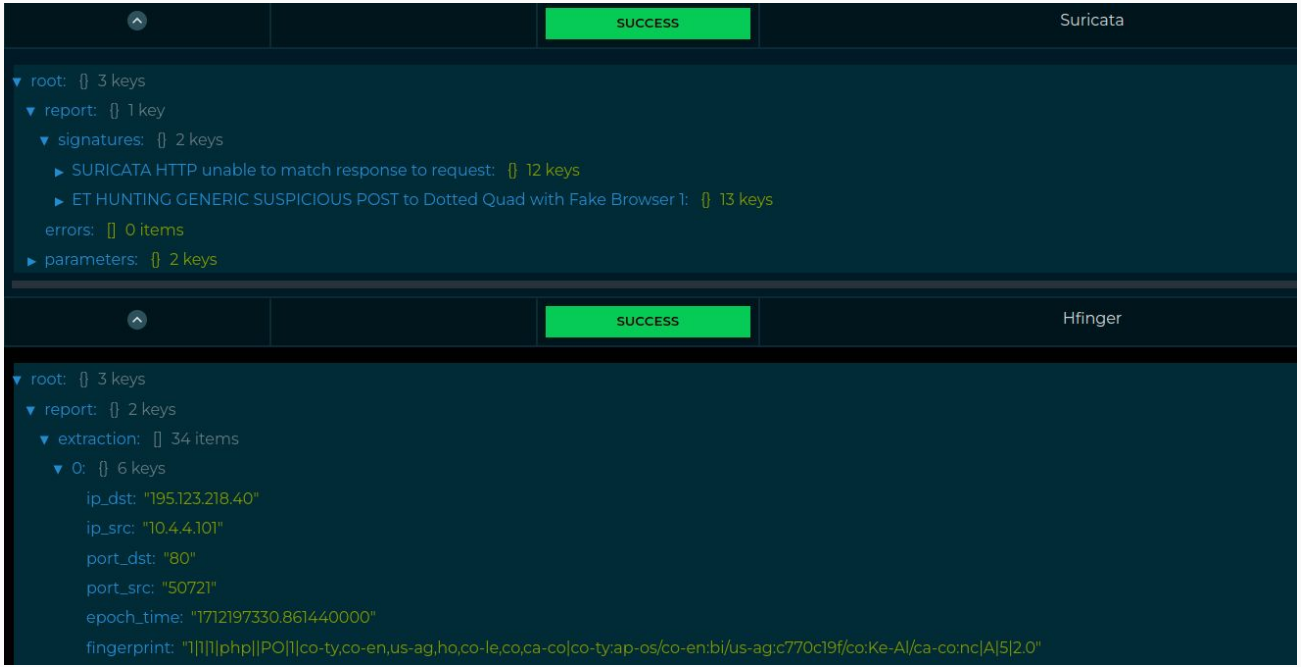
See the docs for more info about it.

IT'S YOUR TIME TO TRY:

- Analyze the PCAP you can download in this link with the default Playbook *PCAP_Analysis*.
- What did you find?

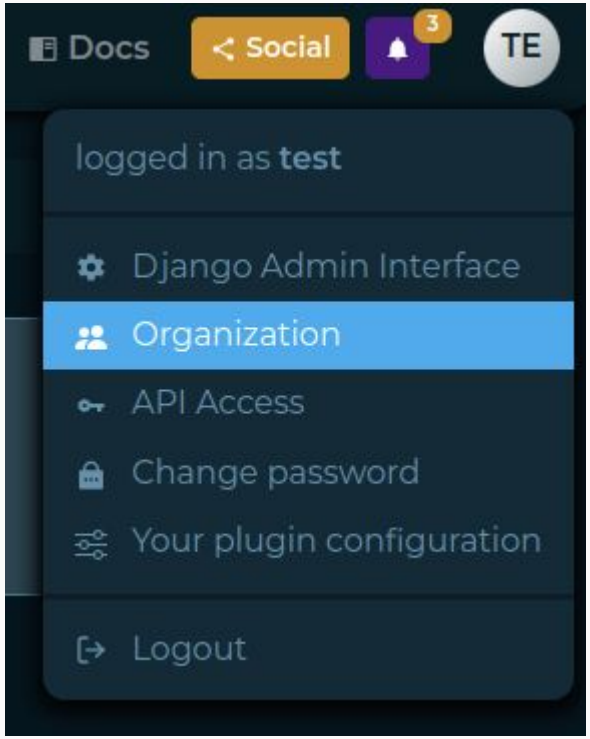
IntelOwl File Analysis - PCAP

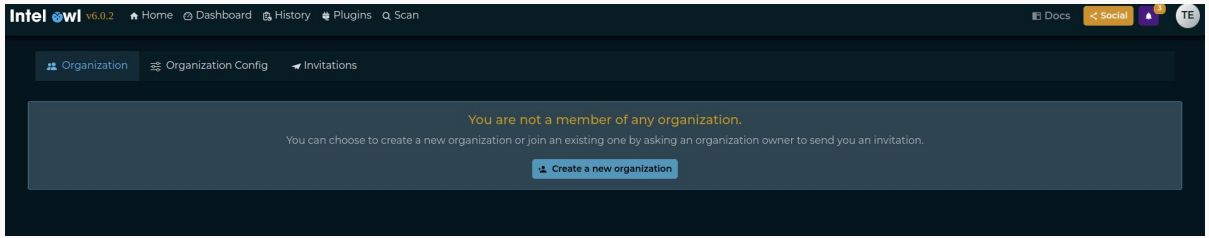
- *Suricata* triggered 2 Signatures, one of them very suspicious
- *HFinger* generated 11 different fingerprints to use

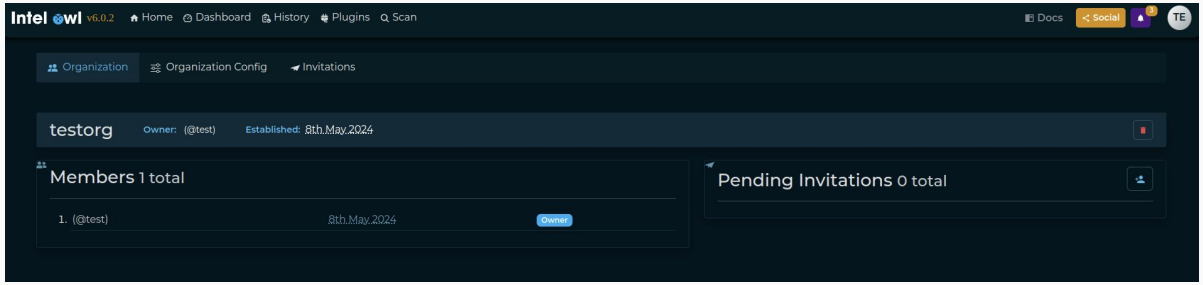


IntelOwl: Organizations

IntelOwl Organizations: Create a new organization



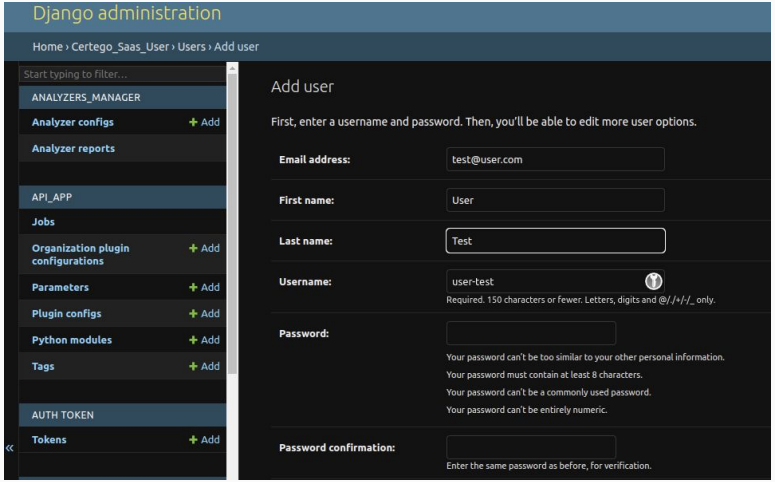




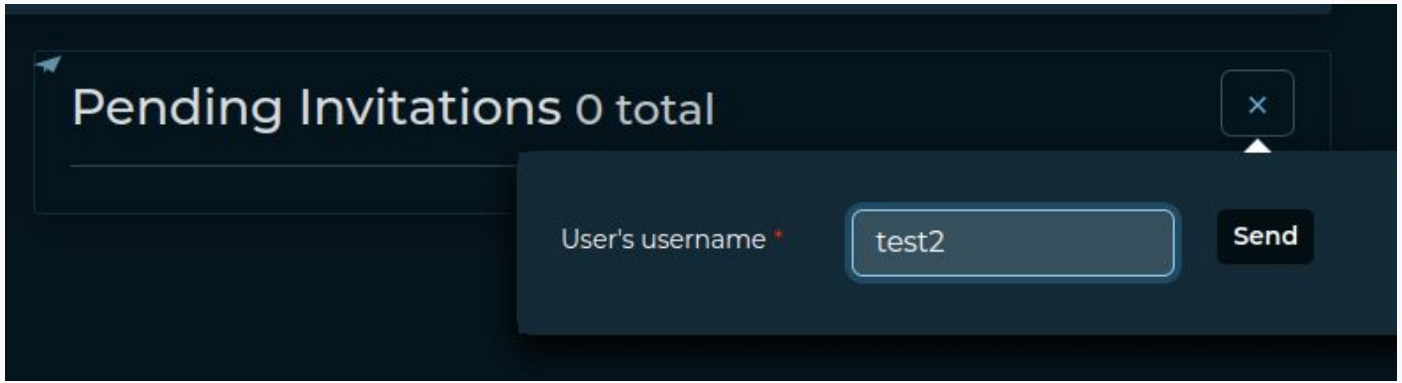
IntelOwl Organizations: Create a new user

Create a new user:

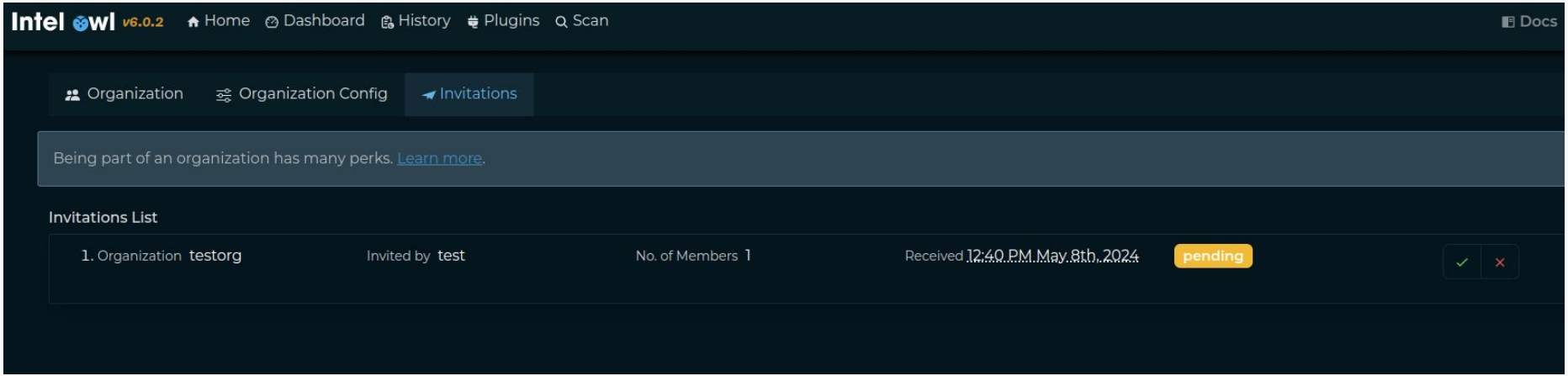
- Automatically by configuring one of the following:
  - Google Oauth2
  - LDAP
  - Radius
- Manually:
  - Django Admin
  - Django Createsuperuser command

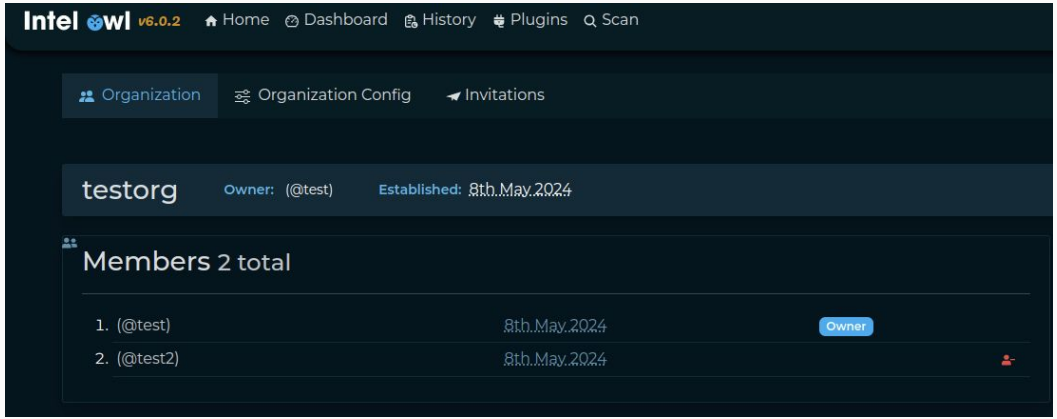


IntelOwl Organizations: Invite a new user



IntelOwl Organizations: New user accepts the invitation

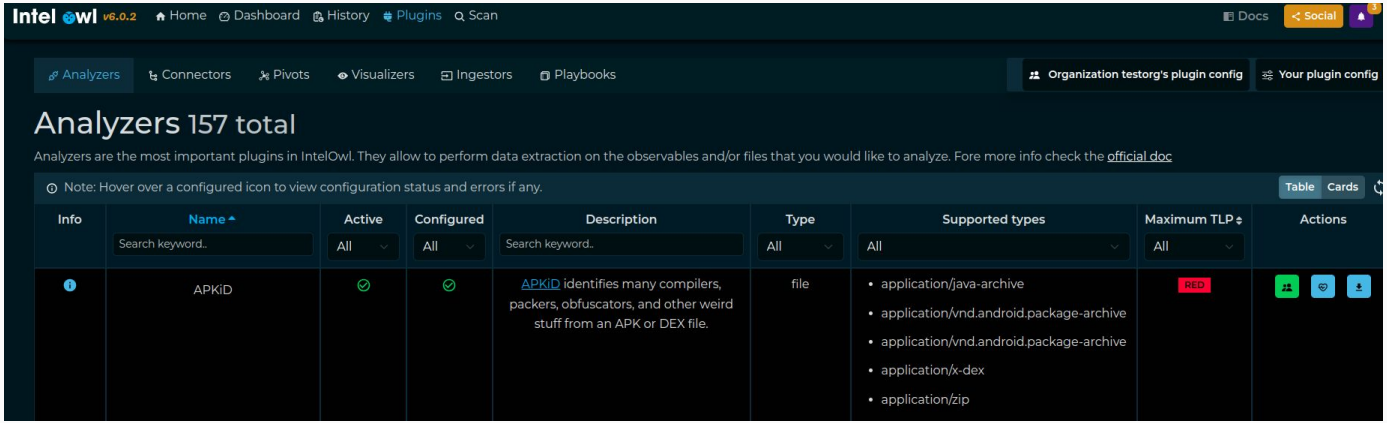


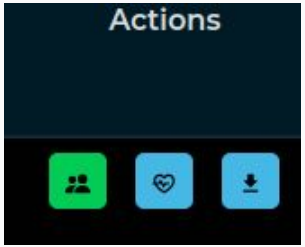


IntelOwl Organizations: Organization Plugin configuration

IntelOwl Organizations: Disable Plugin for entire Organization

This can be useful in case you don’t want your users to use a specific plugin for various reasons (performance, permissions, etc).





Intel owl

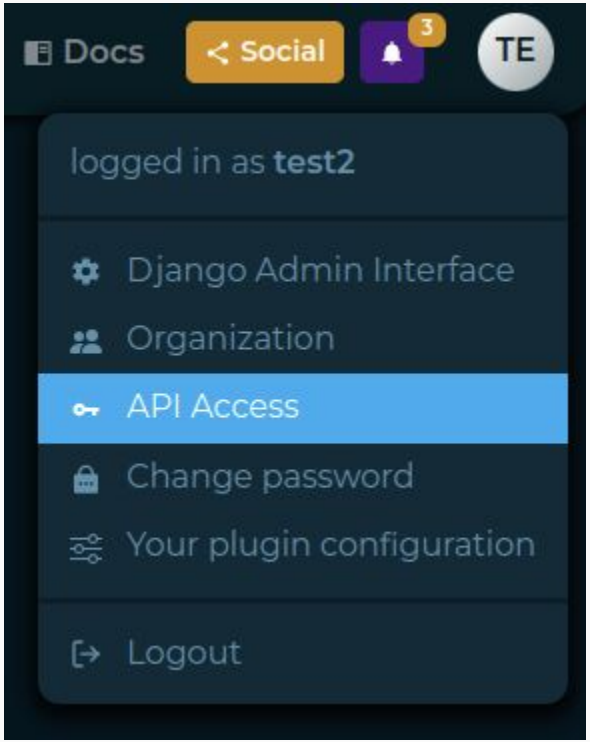
IntelOwl Organizations - Exercise

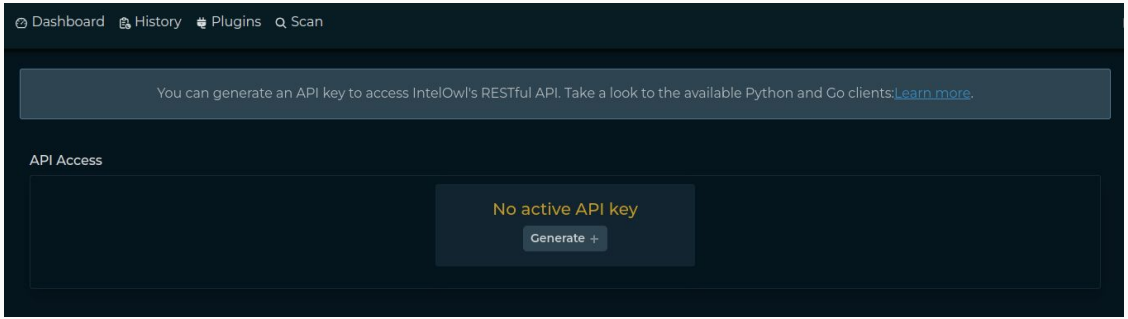
IT'S YOUR TIME TO TRY! Follow the steps below!

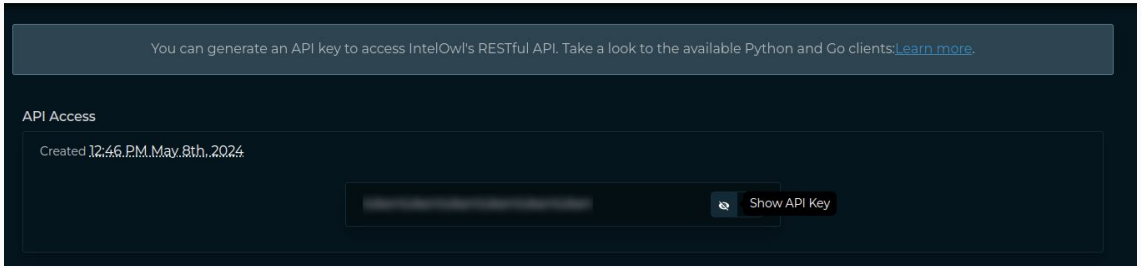
- Organizations
  - Create a new organization
  - Create a new user
  - Invite a new user
  - The new user accepts the invitation
  - Generate a secret for VirusTotal for your entire organization
  - Disable Capa_Info Plugin for your entire organization

IntelOwl: Integrations

IntelOwl Integrations: generate your API key







IntelOwl Integrations: PyIntelOwl CLI Example

PyIntelOwl can be installed locally and used as a CLI:

- `git clone git@github.com:intelowlproject/pyintelowl.git`
- `python3 -m venv venv && source venv/bin/activate && python3 setup.py install`

Configure the CLI to interact with an IntelOwl Instance:

- `pyintelowl config set`
- `pyintelowl config get`

Try to analyze an observable from the CLI with the Playbook:

- `pyintelowl analyse playbook-observable www.test.com Popular_URL_Reputation_Services -p`

View results:

- `pyintelowl jobs view <job_id>`

IntelOwl Integrations: Using it as a library

PyIntelOwl can be installed as a Python requirement and used as a library.

DFIR-IRIS Integration example

Example script:

```
from pyintelowl import IntelOwl, IntelOwlClientException

obj = IntelOwl(
    "5d031089fe0dcaccc1f65c382c20f1e7",  # api key
    "http://localhost:80",
)

try:
    query_result =
    obj.send_observable_analysis_request(observable_name="scanme.org")

except IntelOwlClientException as e:
    logger.exception(e)
```

Intel owl

IntelOwl Integrations - Exercise

IT'S YOUR TIME TO TRY! Follow the steps below!

- Integrations
  - Generate your own API Key via the GUI
  - Install PyIntelOwl
  - Configure PyIntelOwl CLI
  - Execute Your First Analysis via PyIntelOwl CLI
    - Analyze the IP address *120.46.66.113* with the Playbook *Popular_IP_Reputation_Services*, by adding the Tag *honeynet* and with TLP: CLEAR
  - Write a Simple Python Script to create your first Analysis via the PyIntelOwl Library
    - Analyze the IP address *138.201.222.158* with the Playbook *Popular_IP_Reputation_Services*, by adding the Tag *honeynet* and with TLP: CLEAR

IntelOwl: Create custom Plugins!

IntelOwl - Create custom plugins!

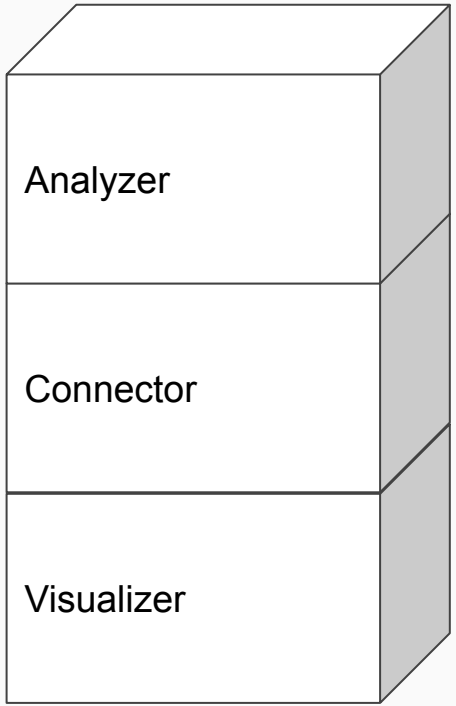
In this part of the workshop we want you to try to create new custom plugins.
We want this to be more interactive as possible. Please tell us your ideas and doubts and we'll guide you.

Schedule:

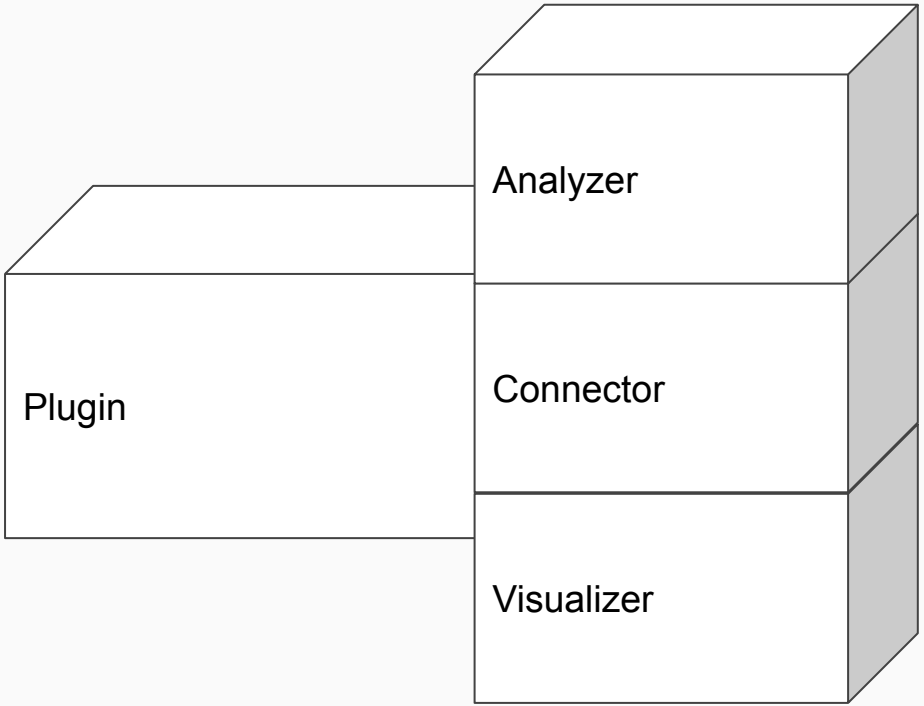
- First, we briefly explain the Plugin Framework and talk about the Software Architecture of IntelOwl
- Then, IT'S CHALLENGE TIME! Everyone choose which type of challenge they want:
  - If you have a specific use case in mind, tell us and we'll come to you to make a plan together of what can be done in the platform. Then, you will have your time to try to create it.
  - If you don't have anything in mind, we'll propose one of our challenges.

THIS IS A CONTEST! :)
Open a Pull Request to the IntelOwl Github Repo with your personal addition!
At the end of the Workshop we'll review the PR and select the best one!
The winner will win a fantastic and unique IntelOwl - Honeynet Swag :)

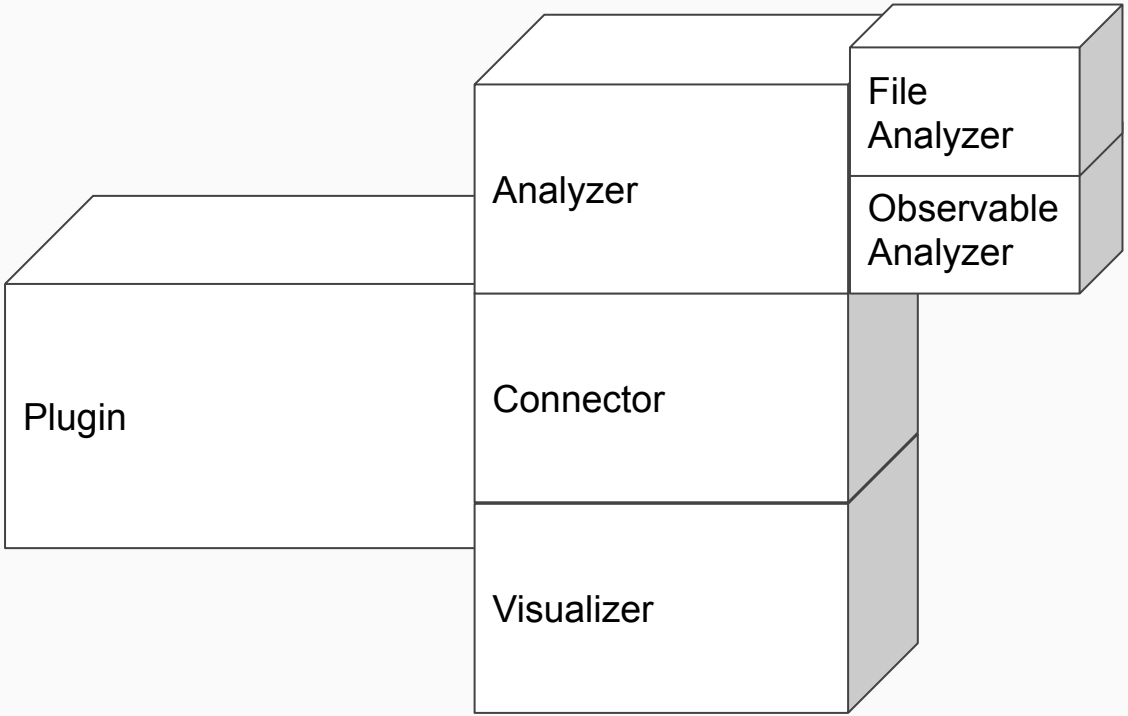
IntelOwl - Software Architecture



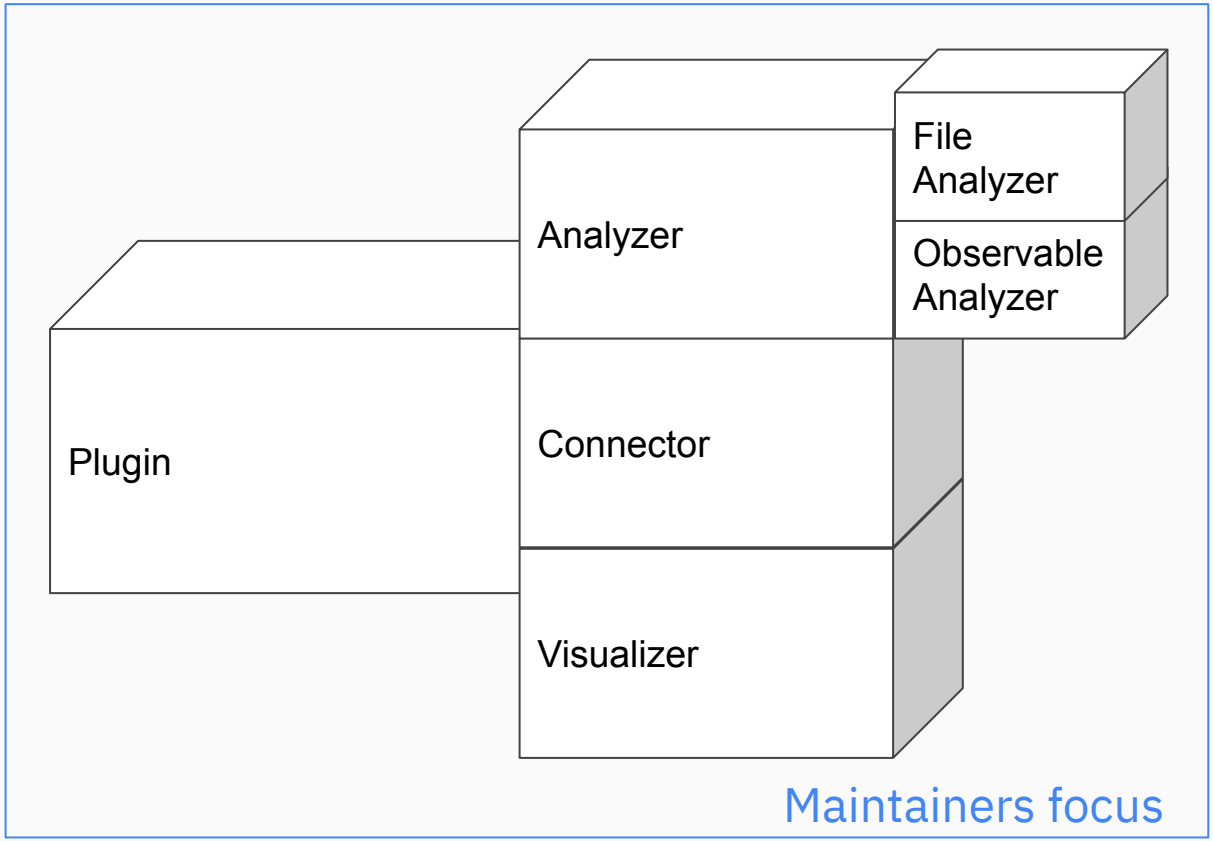
IntelOwl - Software Architecture



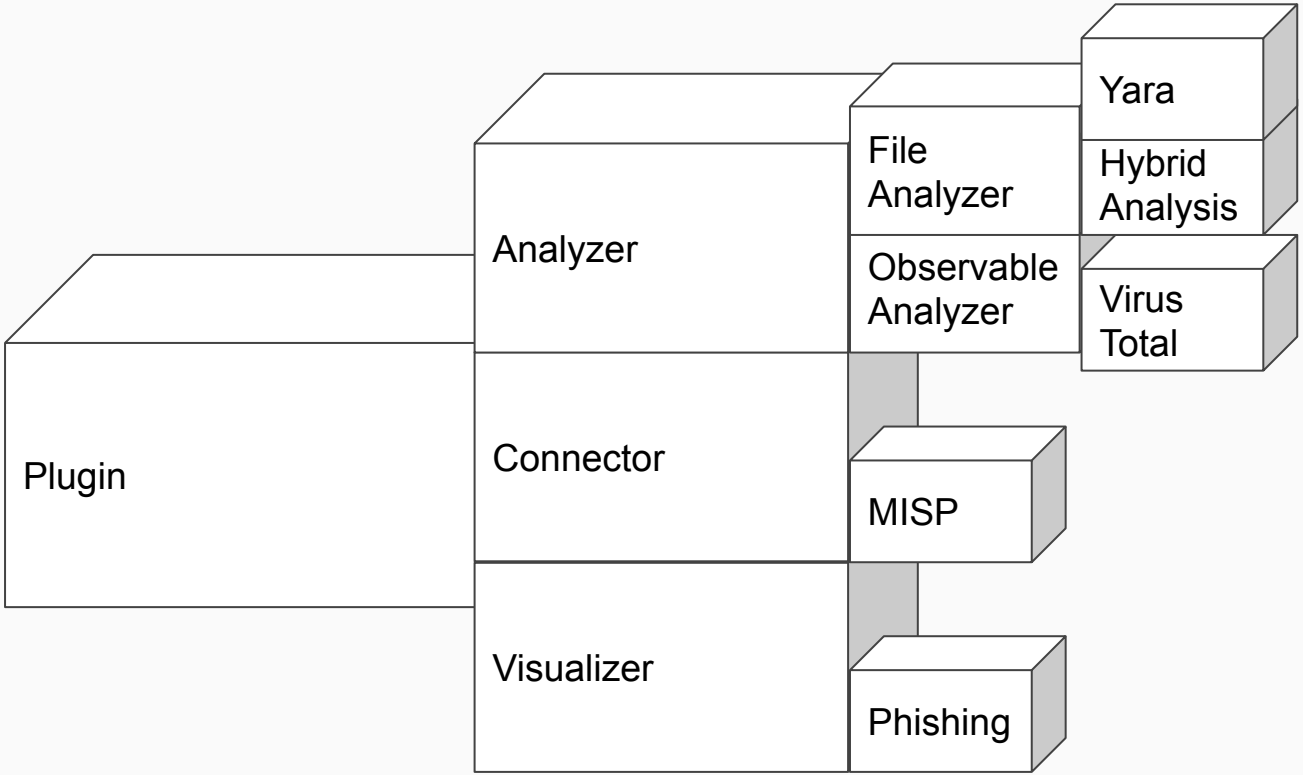
IntelOwl - Software Architecture



IntelOwl - Software Architecture

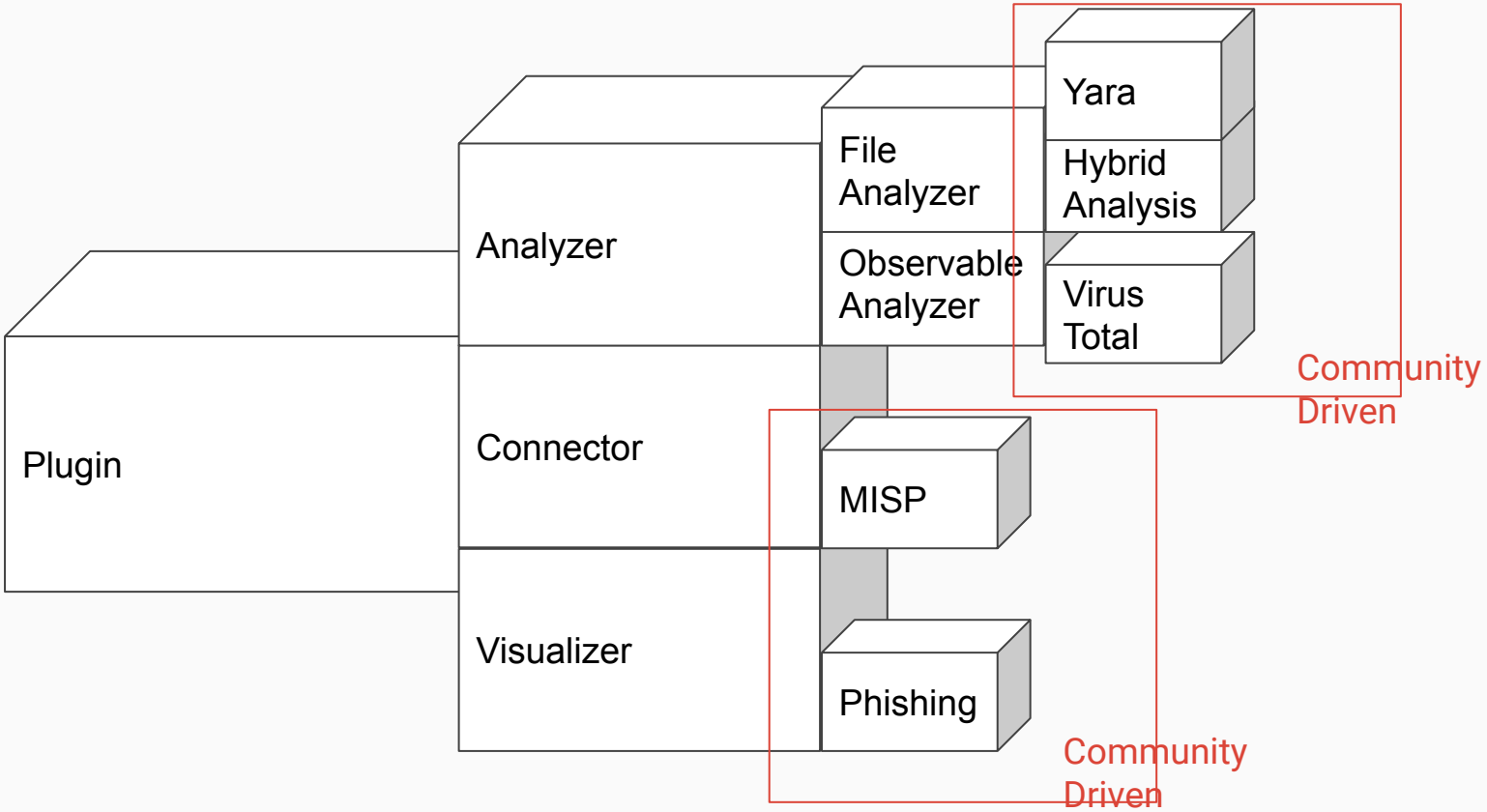


IntelOwl - Software Architecture



Intel owl

IntelOwl - Software Architecture



IntelOwl - Software Architecture

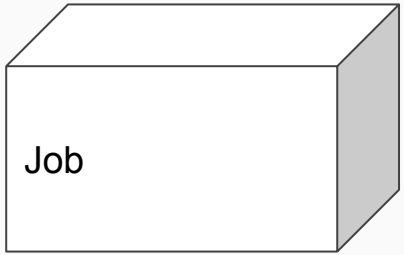
Plugin

Community Driven

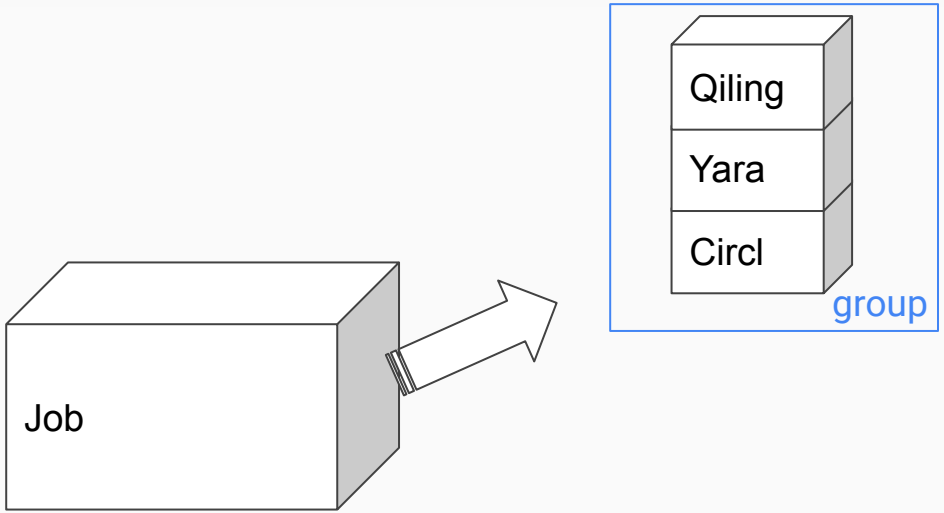
Driven

Intel owl

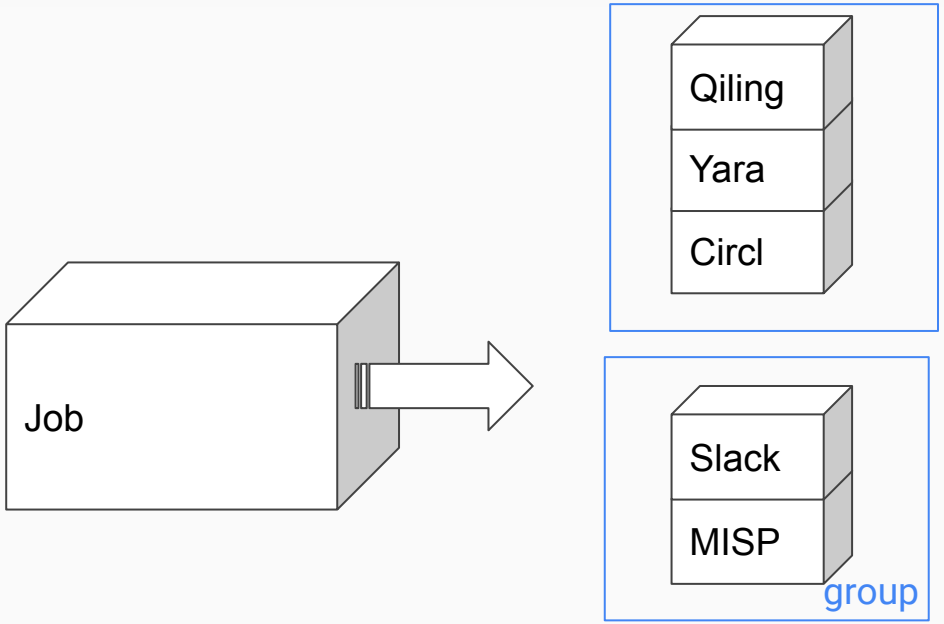
IntelOwl - Software Architecture



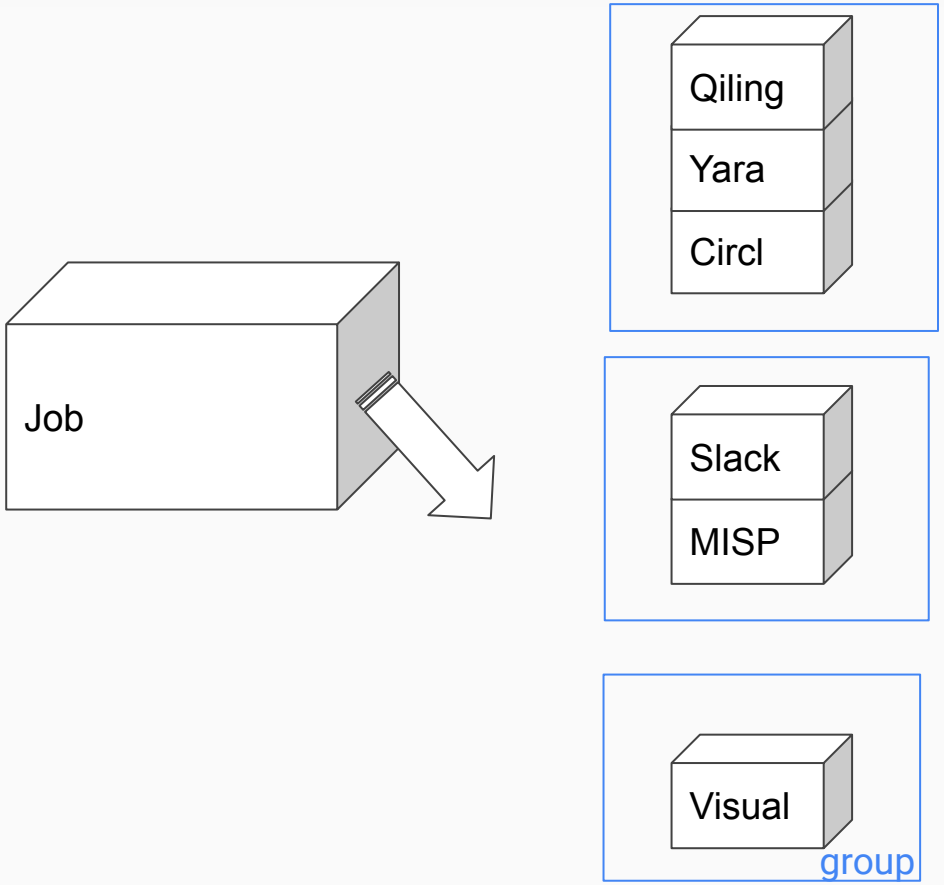
IntelOwl - Software Architecture



IntelOwl - Software Architecture

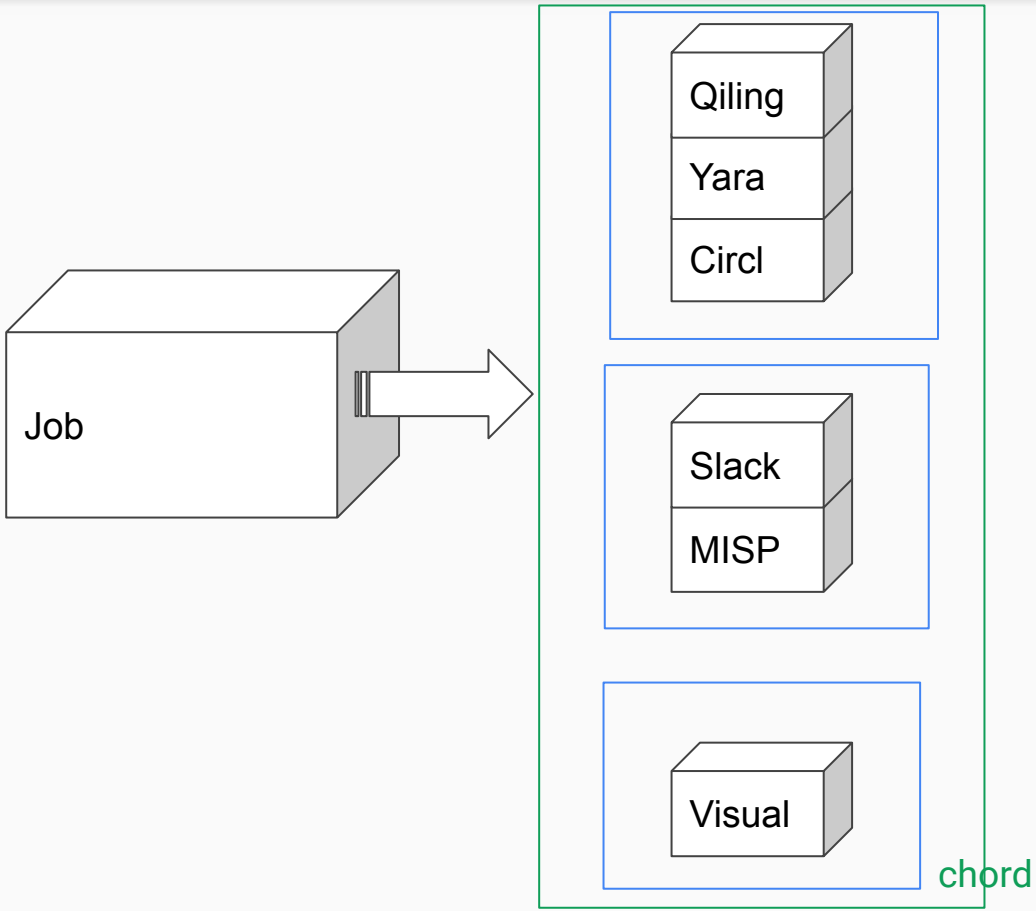


IntelOwl - Software Architecture



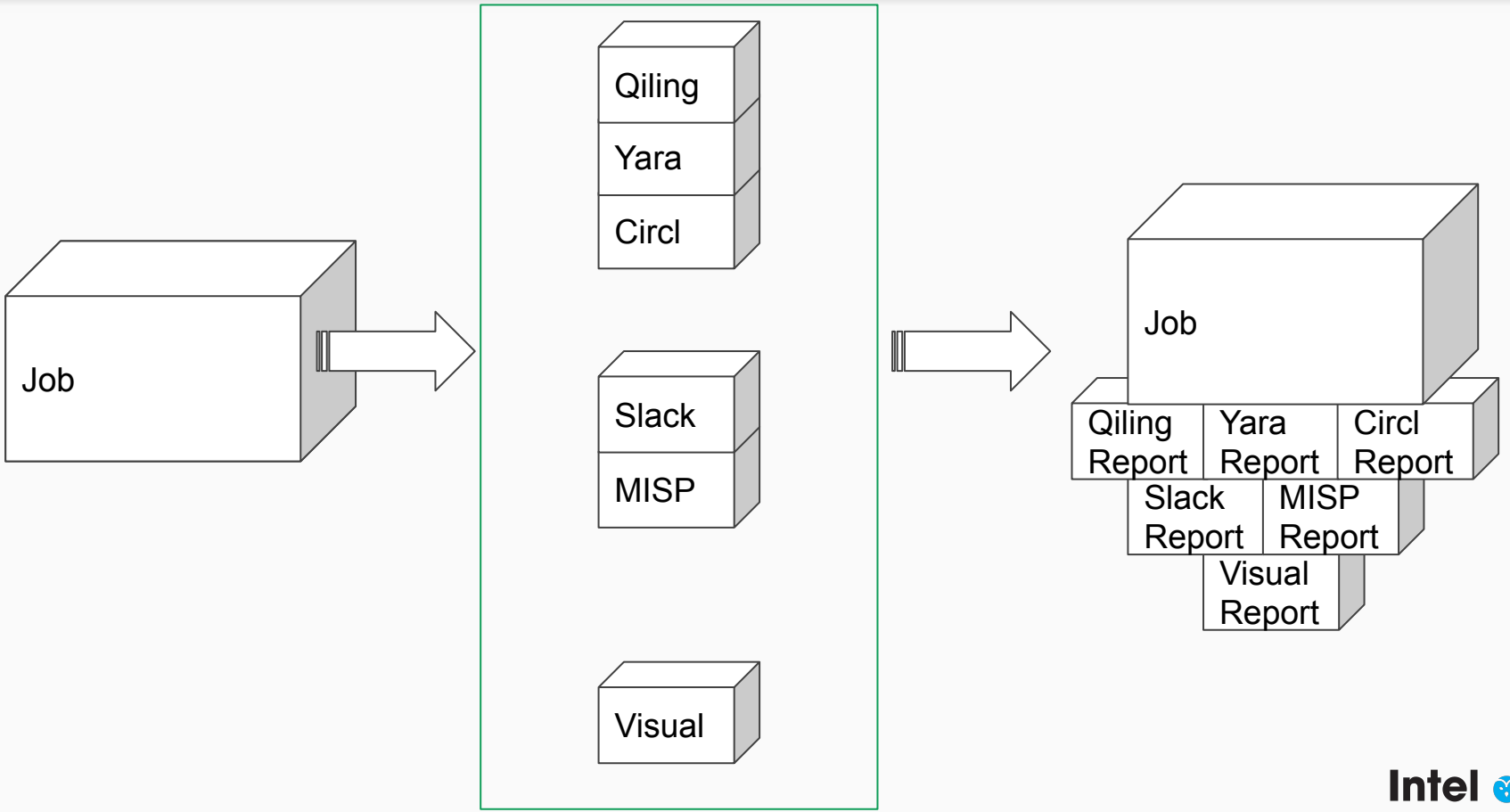
Intel owl

IntelOwl - Software Architecture



Intel owl

IntelOwl - Software Architecture



Intel owl

IntelOwl - Create a new custom Plugin!

How to start? Follow our extensive Documentation!

- How to setup Development. Focus on initialization and the backend part.
- How to add a new Plugin. There is a guide for every type of plugin.
- How to test the application. You need to execute IntelOwl in development mode: `./start test up`

As soon as you are ready, please feel free to open a draft PR into the main Github Repository so we can help you to finalize your PR better!

IntelOwl - Create a new custom Plugin! (Page 1 / 2)

This is the list of ideas that we have for your Plugin Challenge!

Plugin ideas (D=difficulty):

- (D=easy): Write a new **Observable Analyzer** for CleanBrowsing DNS (Ref):
  - Similar to other DNS checker Analyzer that we used during the workshop, we need to understand whether this DNS service blocks the analyzed domain or not.
  - Additional Task: Add this new Analyzer to the already existing Playbooks *Dns* and *Popular_URL_Reputation_Services*. Then, update their own **Visualizers** to show this new info.
- (D=easy): Write a new **File Analyzer** for MobSF (Ref):
  - leverage their library and the JSON output option to extract info via this tool for Android apps
  - Additional Task: Create a custom **Visualizer** for this tool.

Check the next page for other ideas.

IntelOwl - Create a new custom Plugin! (Page 2 / 2)

Other plugin ideas (D=difficulty):

- (D=medium): Write a new default **Playbook** that includes the File Analysis services or tools for Dynamic Analysis already available in IntelOwl. Choose the ones you like the most.
    - Additional Task: Create another **Playbook** that runs a few static analysis tools of your choice and then connect a new **Pivot** for the previously created Dynamic Analysis Playbook. This flows allows the user to choose which files deserve a dynamic analysis based on specific traits extracted from the static analysis of your choice.
- (D=medium): Write a new **Visualizer** for the already existing *Static_Sample_Analysis* Playbook (Ref)
    - The ideal Visualizer would have a main page with the most important information at the top
    - Additional task: add more “tabs” to visualize results for some mime type specific analyzers (one Tab for PDF info, one for DOC info, one for APK info, etc)

Thank you for attending!

@intel_owl

intelowlproject/IntelOwl

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

Intel owl