



# IntelOwl Project

*“making the life of cyber security analysts easier”*

The Honeynet Workshop - Denmark '24

Intel owl

Say “hi” to the team :)



IntelOwl Maintainers



Matteo Lodi

@matte\_lodi

mlodic

Simone Berni

@Ossig3no

Ossigeno

Daniele Rosetti

@magicross94

drosetti



Threat Intelligence Team



Members

Intel owl

Who are you?



# Enjoying myself in the Cyber Security field!



# Enjoying myself in the Cyber Security field!



# Enjoying myself in the Cyber Security field!

I'll never stop learning!



I have the best colleagues ever!

# Enjoying myself in the Cyber Security field!

I'll never stop learning!

We are like superheroes!



I have the best colleagues ever!

# Enjoying myself in the Cyber Security field!

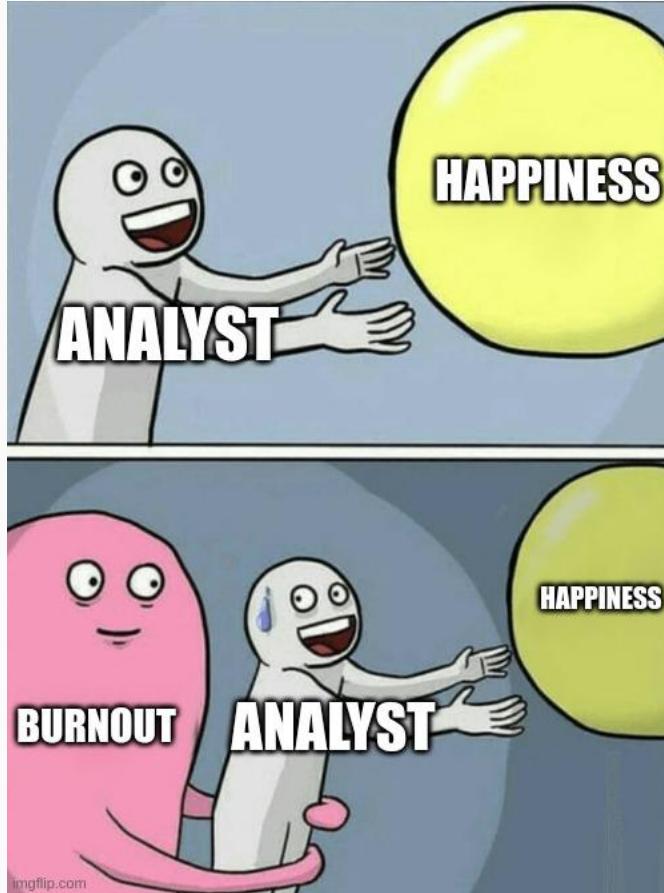
I'll never stop learning!

We are like superheroes!



I have the best colleagues ever!

This is my dream job!



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](#)

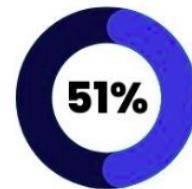
**83% of IT Security Professionals Say Burnout Causes Data Breaches**

September 20, 2023

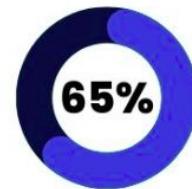
3 Min Read

ref: [DarkReading](#)

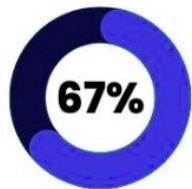
### BY THE NUMBERS BURNOUT IN CYBERSECURITY



Experienced extreme stress or burnout in 2021



Considered leaving their job because of job stress



Wouldn't recommend a career in the same industry

ref: [Bitlyft](#)

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.



imgflip.com

manual  
work

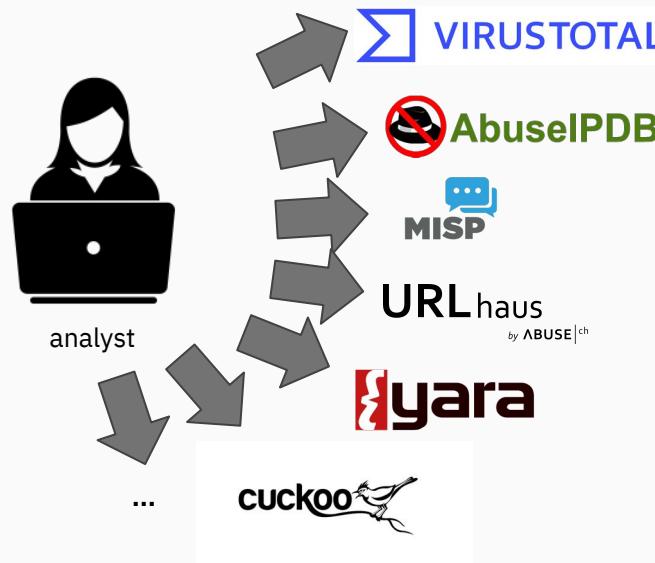
automation

Intel owl

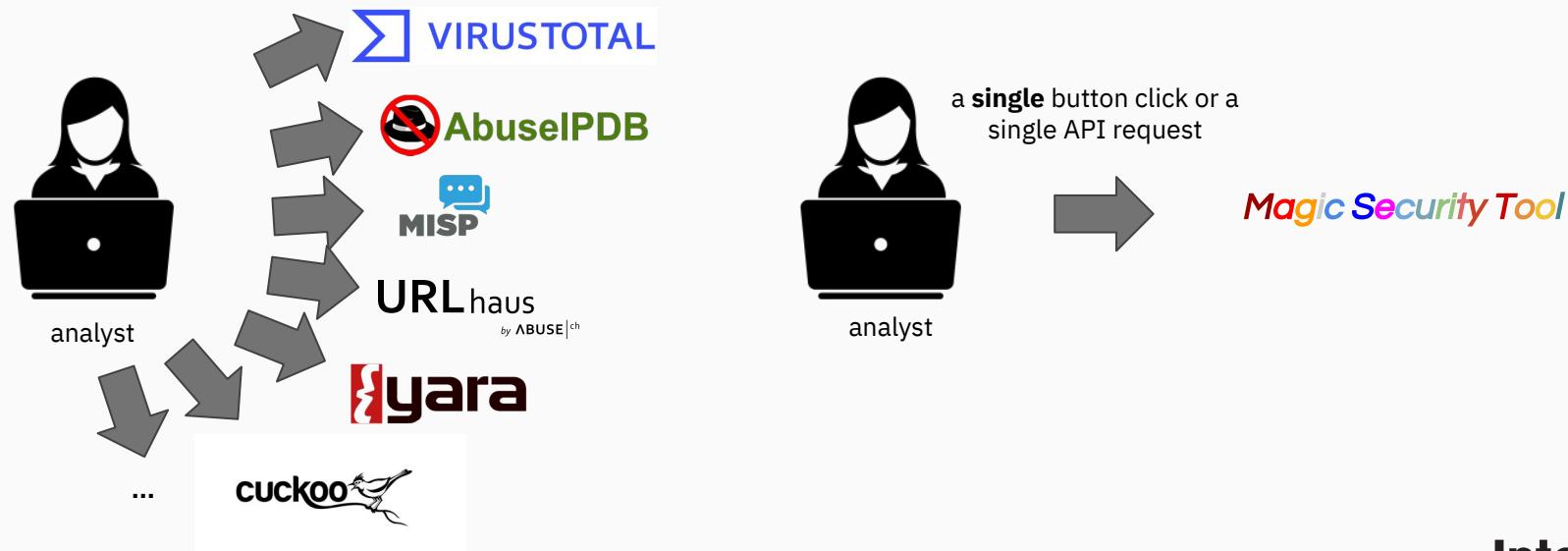
# The bottleneck: acquisition of threat intelligence context



# 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



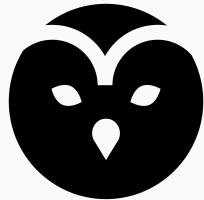
# We were looking for a tool

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 

The word "Intel" is in a large, bold, black sans-serif font. To the right of a thin vertical line, there is a blue circular icon containing a white owl's head, which is part of the IntelOwl logo.

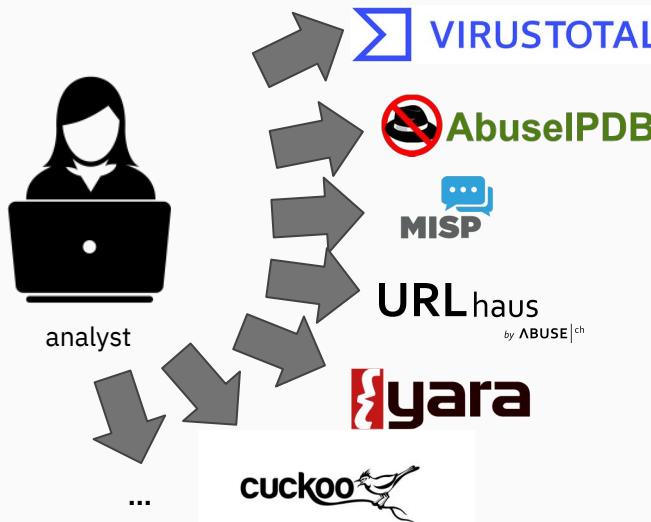
Born in Certego at the start of 2020, it is a great example of a successful Open Source project: right now it is one of the most popular Threat Intel projects on GitHub (>3k stars).

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

# IntelOwl solution



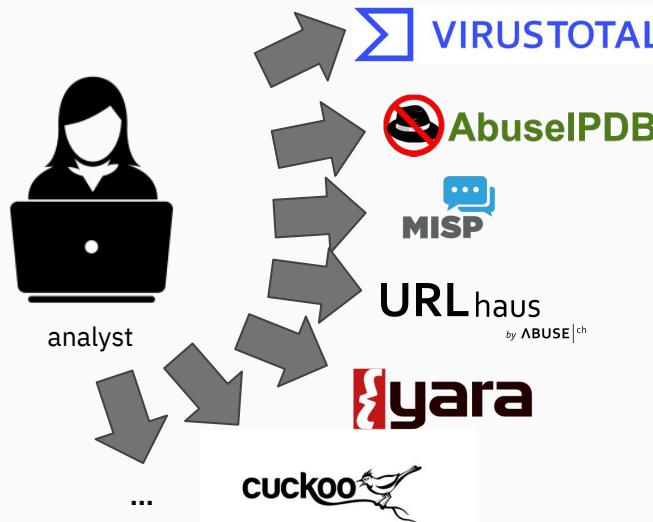
**WithOUT** Intel Owl



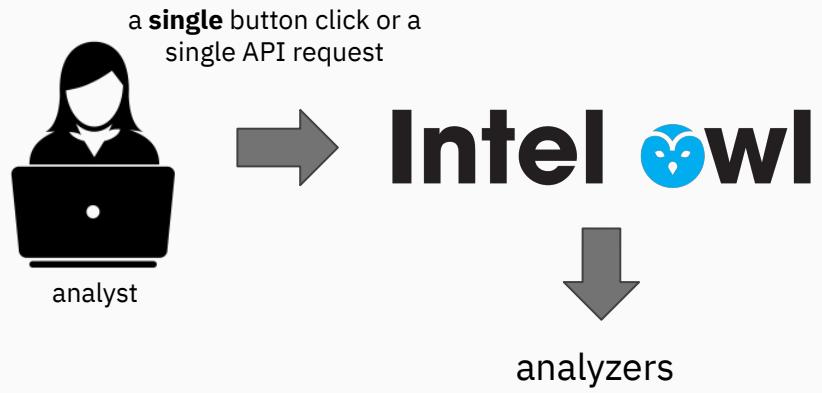
# IntelOwl solution



**WithOUT** Intel Owl



**With** Intel Owl





# IntelOwl Repository & Tech Stack

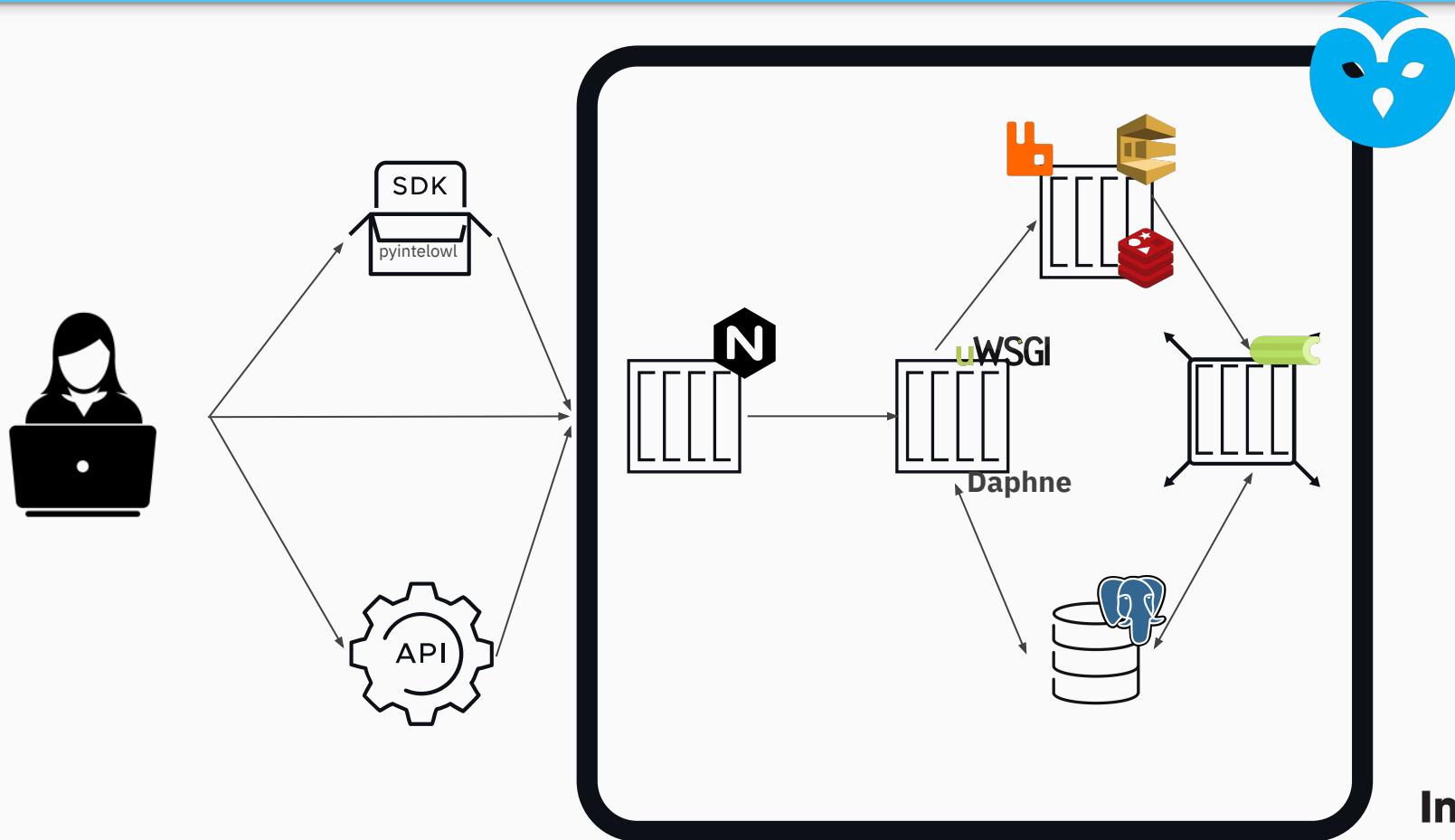
The screenshot shows the GitHub repository page for IntelOwl. The repository has 3k stars, 389 forks, 75 watching, 29 branches, and 61 tags. It includes links to the README, Code of conduct, AGPL-3.0 license, and Security. The README features the Intel Owl logo. Below the README are sections for releases (v5.2.3), stars (3k), docker pulls (258k), and social links (Follow @intel\_owl, LinkedIn, official site). There is also a live demo button. At the bottom, there are status indicators for codefactor, code style, imports, isort, CodeQL, Dependency Review, codecov (76%), resolved issues (1.4k), openssf scorecard (7.4), and openssf best practices (passing).

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



# IntelOwl: Infrastructure Architecture



# IntelOwl: Installation



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

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
```

get the slides of the workshop here!



# IntelOwl Kick-off: Guide



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

↗ Guide

The screenshot shows the IntelOwl web interface at version v6.0.2. The top navigation bar includes links for Home, Dashboard, History, Plugins, Scan, Guide (which is highlighted), Docs, Social, Notifications (with 3 notifications), and TE. The main header features the Intel Owl logo with a blue owl icon and the text "v6.0.2" above it. A central callout box is titled "Guide" and contains the text: "Welcome to IntelOwl's Guide for First Time Visitors! For further questions you could either check out our [docs](#) or reach us out on the [official IntelOwl slack channel](#)". Below this box are three smaller cards: one about IntelOwl being an open-source intelligence tool, another about IntelOwl News (mentioning release v4.0.0 and Certego Blog), and a third about intelligence data analysis. At the bottom right, there is a date stamp of "1st July 2022".

Intel Owl is an Open Source Intelligence file, an IP or a domain from a single of cutting-edge malware analysis to specific file or observable.

Guide

Welcome to IntelOwl's Guide for First Time Visitors! For further questions you could either check out our [docs](#) or reach us out on the [official IntelOwl slack channel](#)

IntelOwl News

IntelOwl: Release v4.0.0

Certego Blog: v4.0.0 Announcement

Next

1st July 2022



# 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?

Intel owl v6.0.2    Home    Dashboard    History    Plugins    Scan

## Scan Observables

Month: 4    Total: 4    [View Log](#)

observable (domain, IP, URL, HASH, etc...)     file

Observable Value(s) \* [Add new value](#) [Delete](#)

https://webmail-atualize.com

Playbooks     Analyzers/Connectors [Edit](#)

Select Analyzers [CloudFlare\\_Malicious\\_Detector](#)

1 / 49 [X](#) [▼](#)

Intel owl



# IntelOwl - Observables Analysis

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

Job #23 ✓

Comments (0) Delete Rescan Save As Playbook Report

https://webmail-atualize.com url

Analyzers Report 1/1 Connectors Report 0/0 Pivots Report 0/0 Visualizers Report 0/0 Full Report Visualizer Raw

	Actions	Status	Name	Process Time (s)	Running Time
		All	CloudFlare_Malicious_Detector	0.22	3:39:13 PM - 3:39:14 PM (GMT+2)

```
root: [] 3 keys
  report: [] 2 keys
    malicious: true
  observable: "https://webmail-atualize.com"
  errors: [] 0 items
  parameters: [] 0 keys
```



# 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?

The screenshot shows the IntelOwl web interface with the following details:

- Header:** Intel owl v6.0.2, Home, Dashboard, History, Plugins, Scan.
- Section:** Scan Observables
- Observables:** observable (domain, IP, URL, HASH, etc...) (selected), file.
- Observable Value(s):** https://webmail-atualize.com (input field with a trash icon) and a button to Add new value.
- Playbooks/Analyzers:** Playbooks (selected), Analyzers/Connectors.
- Select Playbook:** Popular\_URL\_Reputation\_Services (selected). Description: Collection of the most popular and free reputation analyzers for URLs and Domains.

# 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.

Intel owl v6.0.2    Home    Dashboard    History    Plugins    Scan    Docs    Social    4

Job #22

Comments (0)    Delete    Rescan    Save As Playbook    Report

Reputation

Visualizer    Raw

↳ VirusTotal  
Engine Hits: Unknown

↳ Phishtank  
found

CloudFlare Malicious Detector

URLhaus

↳ PhishingArmy

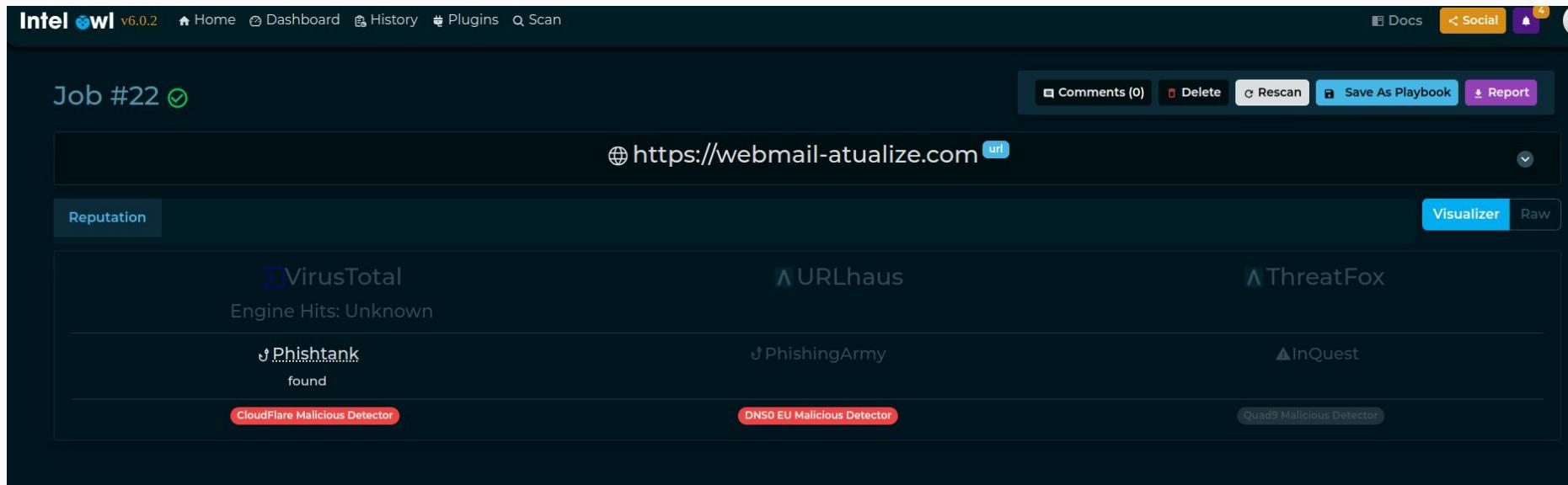
DNS0 EU Malicious Detector

ThreatFox

InQuest

Quad9 Malicious Detector

https://webmail-atualize.com





# IntelOwl - Observables Analysis

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

Intel Owl v6.0.2    Home    Dashboard    History    Plugins    Scan    Docs    Social    4

### Job #22

⊕ <https://webmail-atualize.com> url

Status	TLP	User	MD5	Process Time (mm:ss)	Start Time	End Time
REPORTED WITHOUT FAILS	AMBER	test2	e0969390dd923dcbb6fa605b773043d6	00:02	03:37:45 PM May 8th, 2024	03:37:47 PM May 8th, 2024

Playbook: Popular\_URL\_Reputation\_Services    Tags: None

**Warning(s)**

- 3 warnings
- GoogleSafebrowsing won't run: is disabled or not configured
- OTXQuery won't run: is disabled or not configured
- VirusTotal\_v3\_Get\_Observable won't run: is disabled or not configured

**Error(s)**

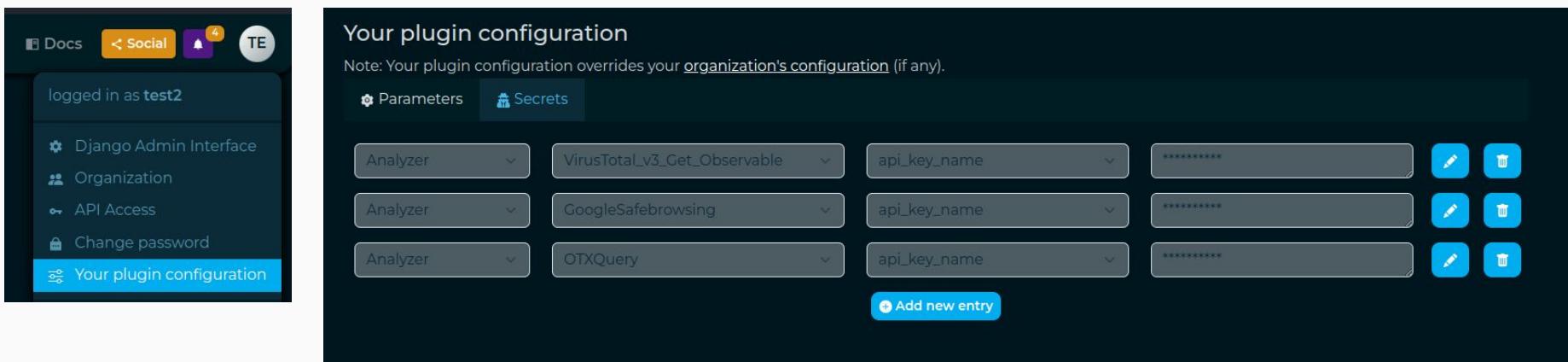
- 0 errors

# 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



The screenshot shows the IntelOwl Django Admin interface. On the left, there is a sidebar with the following navigation items:

- Docs
- Social (with a notification count of 4)
- TE
- logged in as test2
- Django Admin Interface
- Organization
- API Access
- Change password
- Your plugin configuration (highlighted in blue)

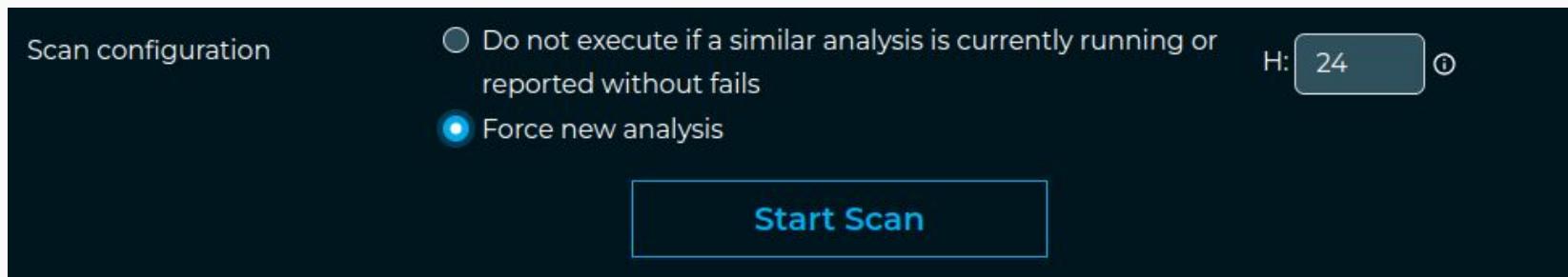
The main content area is titled "Your plugin configuration". It contains a note: "Note: Your plugin configuration overrides your [organization's configuration](#) (if any)." Below this, there are three rows of configuration fields. Each row consists of a dropdown menu labeled "Analyzer", a dropdown menu with a value, a dropdown menu labeled "api\_key\_name", and a redacted input field. To the right of each row are edit and delete icons.

Analyzer	Value	api_key_name	Secret Value	Action
VirusTotal_v3_Get_Observable			*****	 
GoogleSafebrowsing			*****	 
OTXQuery			*****	 

[Add new entry](#)

## 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”



Scan configuration

Do not execute if a similar analysis is currently running or reported without fails

Force new analysis

H: 24  ⓘ

**Start Scan**

A screenshot of the IntelOwl web interface. The top navigation bar is blue with the IntelOwl logo. Below it, the main title is "IntelOwl - Observables Analysis". The slide content is titled "IT'S YOUR TIME TO TRY:" followed by a bullet-point list. The list item about forcing a new analysis is illustrated with a screenshot of the "Scan configuration" section. This section has a dark background. On the left, it says "Scan configuration". In the center, there are two radio buttons: one for "Do not execute if a similar analysis is currently running or reported without fails" and one for "Force new analysis", which is selected and highlighted with a blue outline. To the right of these buttons is a "H:" label followed by a "24" input field with a small info icon, and a "Start Scan" button at the bottom.



# IntelOwl - Observables Analysis

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

Intel owl v6.0.2    Home    Dashboard    History    Plugins    Scan    Docs    Social    Notifications (4)    TE

Job #24

https://webmail-atualize.com

Reputation    Visualizer    Raw

**VirusTotal**  
Engine Hits: 16

URLhaus

ThreatFox

Phishtank found

PhishingArmy

InQuest

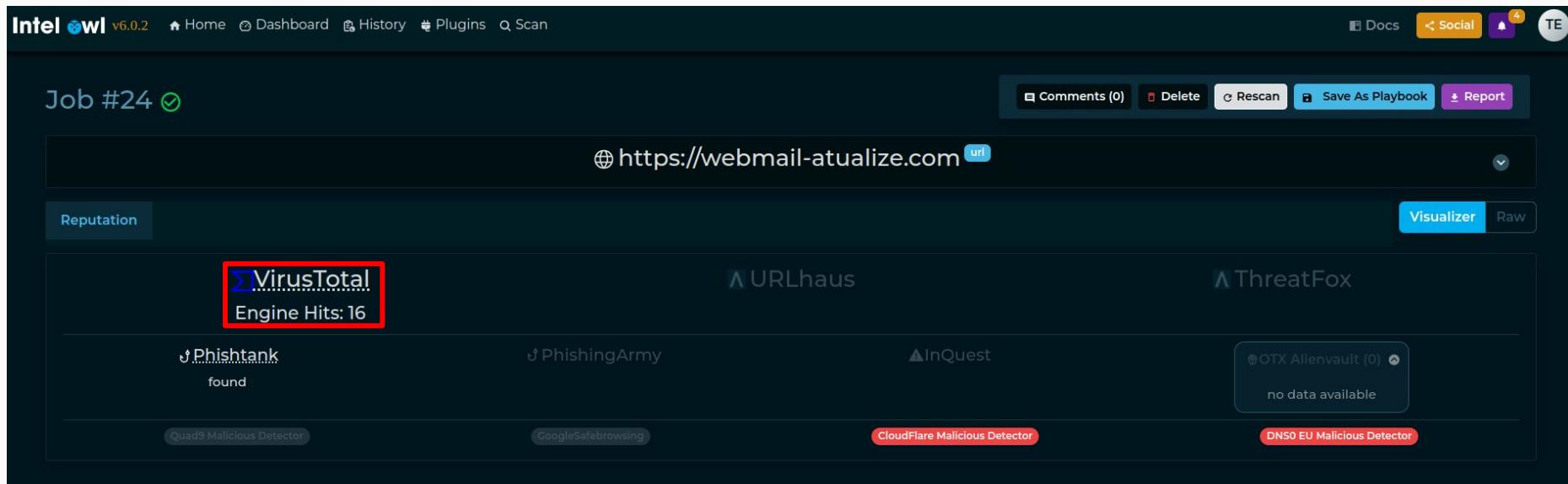
OTX AlienVault (0)  
no data available

Quad9 Malicious Detector

GoogleSafebrowsing

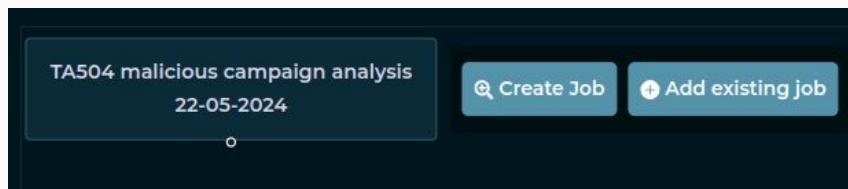
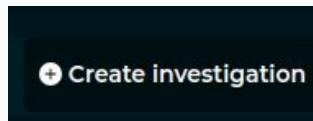
CloudFlare Malicious Detector

DNSO EU Malicious Detector



## IT'S YOUR TIME TO TRY:

- Let's do another analysis with the same Playbook for the URL <https://dnja.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.

Intel owl v6.0.2 Home Dashboard History Plugins Scan

## Investigation #2

### TA504 malicious campaign analysis 22-05-2024

Description  

We received 3 malicious emails to analyze, probably correlated to the same actor

TA504 malicious campaign analysis  
22-05-2024

0 items

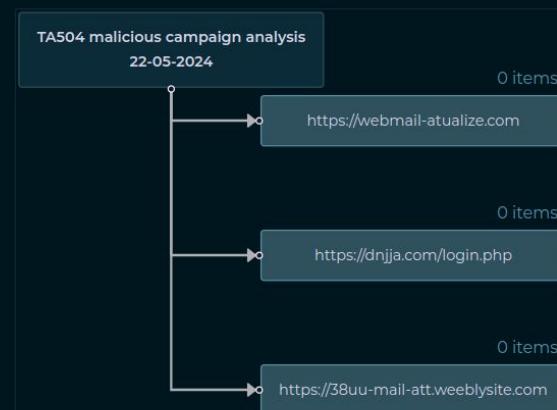
https://webmail-atualize.com

0 items

https://dnjja.com/login.php

0 items

https://38uu-mail-att.weeblysite.com



Intel owl

# 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.

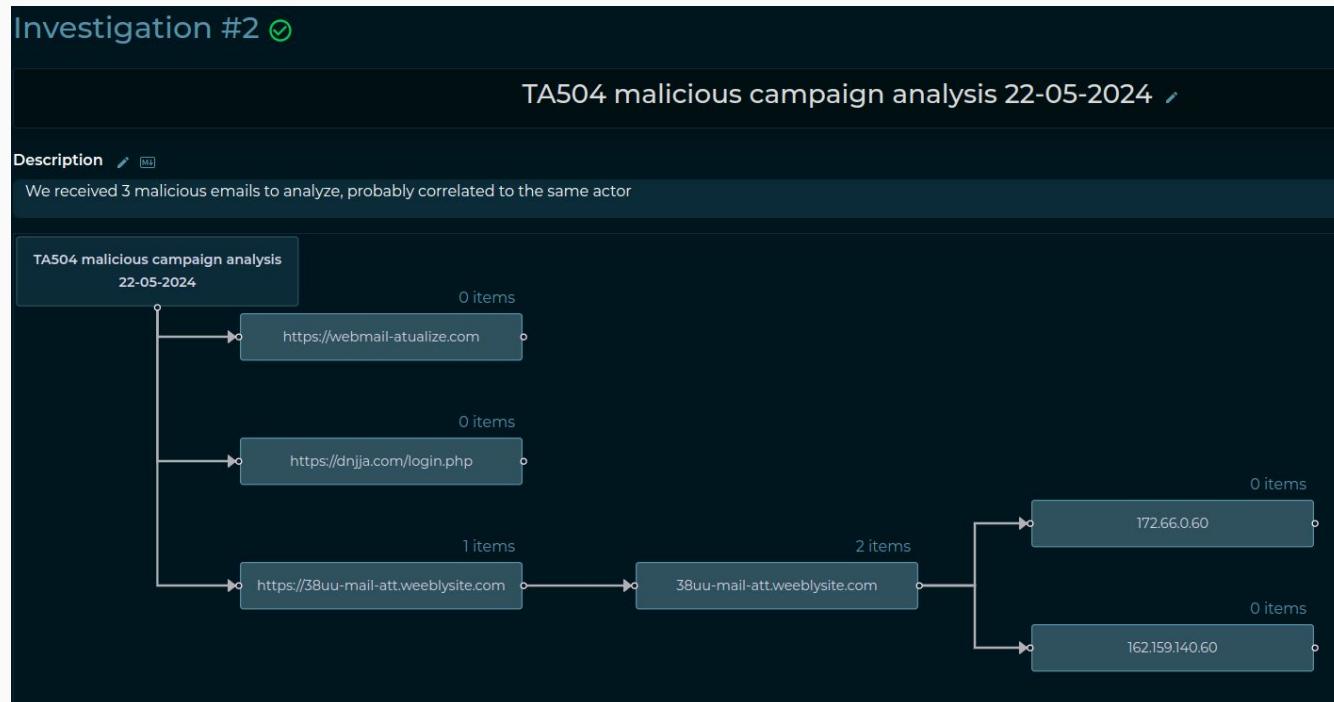
The screenshot shows a dark-themed IntelOwl interface. On the left, there is a visualization of a network graph with nodes and edges. A specific node is highlighted with a red arrow pointing to it, containing the URL <https://38uu-mail-att.weeblysite.com>. To the right of this visualization, the text "0 items" is displayed. Below the URL node, there is a summary card with the following details:

- Job: #26
- Name: <https://38uu-mail-att.weeblysite.com>
- Playbook: Popular\_URL\_Reputation\_Services
- Created: 15.minutes.ago

At the top of the card, there are four buttons: "Copy", "Link", "**Pivot**" (which is highlighted with a red box), and "Remove Branch".

# 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?

The screenshot shows the IntelOwl v6.0.2 web interface. At the top, there's a navigation bar with links for Home, Dashboard, History, Plugins, and Scan. Below the navigation is a search bar and a date range selector showing "Month: 15" and "Total: 15".

The main area is titled "Scan Observables". It has two tabs: "observable (domain, IP, URL, HASH, etc...)" (selected) and "file". A text input field contains the value "38uu-mail-att.weeblysite.com". Below the input is a blue button labeled "+ Add new value".

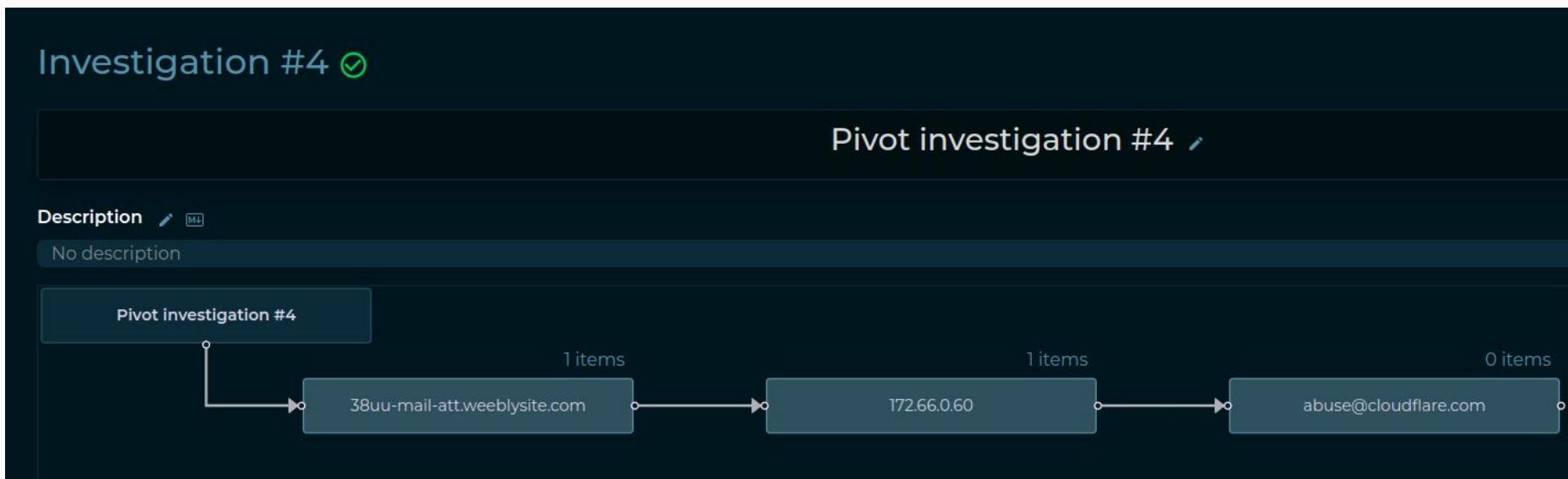
Further down, there are two more tabs: "Playbooks" (selected) and "Analyzers/Connectors". A dropdown menu is open under "Select Playbook", showing the option "Takedown\_Request". A tooltip for this option states: "Start investigation to request to take down a malicious domain. A mail will be sent to the domain's".

In the bottom right corner of the screenshot, the IntelOwl logo is visible.

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.

The screenshot shows the IntelOwl v6.0.2 interface. At the top, there is a navigation bar with links for Home, Dashboard, History, Plugins, and Scan. Below the navigation bar, the title "Job #34" is displayed. On the right side, an email address "abuse@cloudflare.com" is shown with a "generic" label. The main content area features a table with columns for Actions, Status, and Name. The "Actions" column contains icons for "Edit" and "Delete". The "Status" column shows "FAILED". The "Name" column lists "AbuseSubmitter". Below the table, there is a detailed log section:

- root: [] 3 keys
- report: [] 0 keys
- errors: [] 1 item
  - O: "AbuseSubmitter' object has no attribute 'sender'"
- parameters: [] 0 keys

# 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.

### Job #34

Comments (0) Delete Rescan Save As Playbook Report

Investigation Overview

abuse@cloudflare.com generic

Status FAILED	TLP AMBER	User test2	MDS 9d201efa0f28509e77b137e62a5c5e8a	Process Time (mm:ss) 00:00	Start Time 04:51:03 PM May 8th, 2024	End Time 04:51:03 PM May 8th, 2024
Playbook Send_Abuse_Email	Tags None	Warning(s) 0 warnings	Error(s) 0 errors			

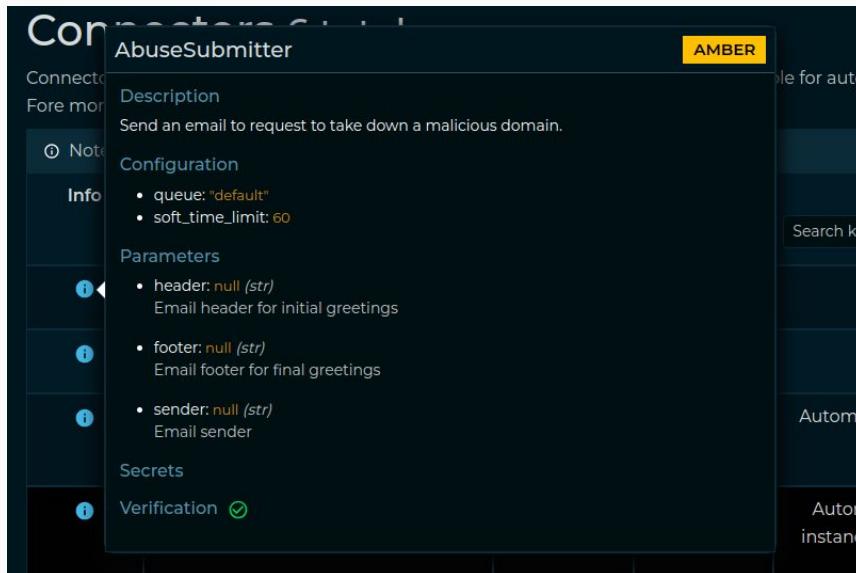
ANALYZERS COMPLETED Reported 0/0 → CONNECTORS COMPLETED Reported 1/1 → PIVOTS COMPLETED Reported 0/0 → VISUALIZERS COMPLETED Reported 0/0

# 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



Job #43 0

Investigation Overview abuse@cloudflare.com generic

Analyzers Report 0/0 Connectors Report 1/1 Pivots Report 0/0 Visualizers Report 0/0 Full Report

	Actions	Status	Name	Pro
		All	Search keyword..	
▲		SUCCESS	AbuseSubmitter	

▼ root: [] 3 keys

▼ report: [] 4 keys

▼ to: [] 1 item

O: "abuse@cloudflare.com"

body: "Hello Abuse Team, Domain 38uu-mail-att.weeblysite.com has been detected as malicious by our team. We kindly request you to take it down." from: "takedown@honeynet.org"

subject: "Takedown domain request for 38uu-mail-att.weeblysite.com"

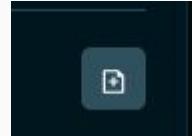
# IntelOwl - Blog Post Analysis Use Case

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)



Load Multiple Observables

Enter any text to extract observables for further lookup.

The Runtime Broker.exe also spawns some Windows legit process, some used to get persistence on system, other to perform recognition.

```
c:\windows\syswow64\schtasks.exe /RUN /TN ScreenBrightnessRestore [to ensure persistence on the system, ndr]
```

```
c:\windows\syswow64\schtasks.exe /create /F /XML "C:\Program Files (x86)\ScreenDim\ScreenBrightnessRestore.xml" /TN ScreenBrightnessRestore [to ensure persistence on the system, ndr]
```

```
c:\windows\syswow64\net session
```

```
c:\windows\syswow64\reg.exe delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Node_Run /#
```

We also detected the execution of "C:\Program Files (x86)\ScreenDim\ScreenDim.exe" restore with parent process C:\Windows\system32\svchost.exe -k netsvc -p -s Schedule. ScreenDim.exe then spawns "C:\Program Files (x86)\pyt137\python.exe" -m updater. This last process then makes several netconn to the following malicious domains:

```
paul.microvortex.us.it
cdn.goodfilehosting.it
```

After the connections ScreenDim.exe is uninstalled.

Extract

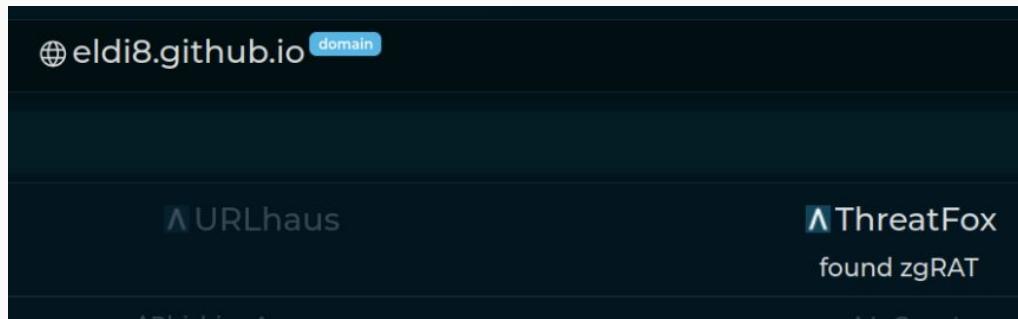
Extracted observables

- domain:
  - elid8.github.io
  - wjeepuijanwmwtk
  - vimeo.com
  - evinfoptasv.dedyn.io
  - cdn.discordapp.com
  - bobsmith.apworld.cf
  - cdn.goodfilehosting.it
  - chcp.com
  - luke.compeyson.eu.org
  - paul.microvortex.us.it
- ip:
  - 730f84805b3b815bf1b4ef0e60ee2
  - 8a492973b12f84f49c52216d8c2975597fb92a0231128
- url:
  - https://www.virustotal.com/gui/file/8a492973b12f84f49c52216d8c2975597fb92a0231128
- hash:
  - 730f84805b3b815bf1b4ef0e60ee2
  - 8a492973b12f84f49c52216d8c2975597fb92a0231128

# IntelOwl - Blog Post Analysis Use Case

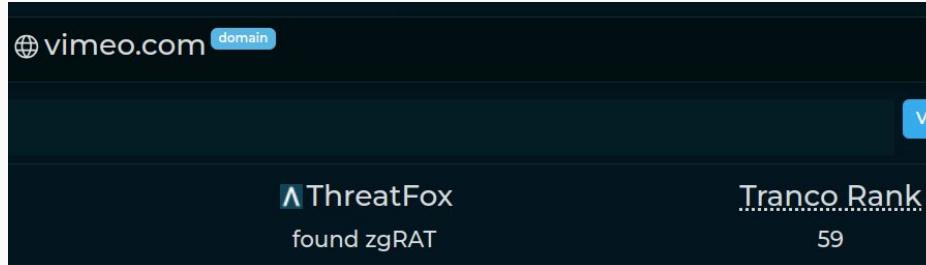
- Not all of them are malicious:
  - *vimeo.com,cdn.goodfilehosting.it* and *cdn.discordapp.com* are abused services
  - *paul.microvortexus.it* is not known
- Other domains are evidence for a threat reported as **zgRAT** (Threatfox report)

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



The screenshot shows a Threatfox report for the domain `eldi8.github.io`. On the left, there's a link to URLhaus. On the right, it says "ThreatFox found zgRAT".

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



The screenshot shows a Threatfox report for the domain `vimeo.com`. It includes a link to ThreatFox which found zgRAT, and a link to Tranco Rank which is 59.

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?

Observable Value(s) \*

 trash icon  
+ Add new value

---

Playbooks  Analyzers/Connectors edit icon

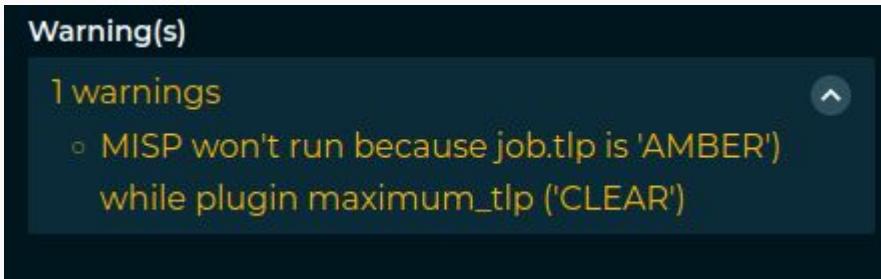
Select Analyzers  1/58 X | ▼

Select Connectors  1/6 X | ▼

TLP info icon  CLEAR  GREEN  AMBER  RED  
disable analyzers that could impact privacy and limit access to my organization

# 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?

	Actions	Status	Name
	All	FAILED	MISP

root: [] 3 keys  
report: [] 0 keys  
errors: [] 1 item  
0: "Unable to connect to MISP (https://192.168.0.1). Please make sure the API key and the URL are correct (http/https is required)  
ers/getVersion [Caused by SSLError[SSLCertVerificationError], [SSL: CERTIFICATE\_VERIFY\_FAILED] certificate verify failed: self signed certificate in certificate chain]"  
parameters: [] 4 keys

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?



Edit Runtime Configuration

Note: Edit this only if you know what you are doing!

```
1  {
2    analyzers: {
3      DNS0_EU_Malicious_Detector: {}
4    },
5    connectors: {
6      MISP: {
7        tlp: 'clear',
8        ssl_check: false
9      }
10    }
11 }
```

**ANALYZERS:**  
DNS0\_EU\_Malicious\_Detector  
null

**CONNECTORS:**  
MISP

- `tlp (str)`  
Change this as per your organization's threat sharing conventions.
- `debug (bool)`  
Enable debug logs.
- `ssl_check (bool)`  
Enable SSL certificate server verification. Change this if your MISP instance has not SSL enabled.



# IntelOwl - MISP Export Use Case

Analyzers Report 1/1 Connectors Report 1/1 Pivots Report 0/0 Visualizers Report 0/0 Full Report

	Actions	Status ▾	Name ▾
		All	Search keyword..
		SUCCESS	MISP

▼ root: {} 3 keys  
  ▼ report: {} 1 key  
    ▼ Event: {} 30 keys  
      id: "2"

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs

**View Event**

[View Correlation Graph](#)  
[View Event History](#)

---

[Edit Event](#)  
[Delete Event](#)  
[Add Attribute](#)  
[Add Object](#)  
[Add Attachment](#)  
[Add Event Report](#)  
[Populate from...](#)

**Intelowl Job-147: popcorn-tv.online**

Event ID	2
UUID	6e6804dc-7eba-4db5-98b6-507856cd5328
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	<a href="#">source:intelowl</a> <a href="#">x</a> <a href="#">ip:clear</a> <a href="#">x</a> <a href="#">+</a> <a href="#">+</a>

# 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!

A screenshot of the Django Admin interface showing two panels for managing connectors. The left panel, titled 'Available connectors', lists several connectors: AbuseSubmitter, EmailSender, OpenCTI, Slack, and YETI. The right panel, titled 'Chosen connectors', shows a single connector selected: MISP. Both panels include a 'Filter' input field and a 'Choose all' or 'Remove all' button at the bottom.

# IntelOwl - GreedyBear Integration



In IntelOwl you can find an Analyzer for a specific service called [GreedyBear](#).

**Greedybear** is a Threat Intel Platform for [T-POT](#)s. You can find the public instance hosted by Honeynet [here](#).

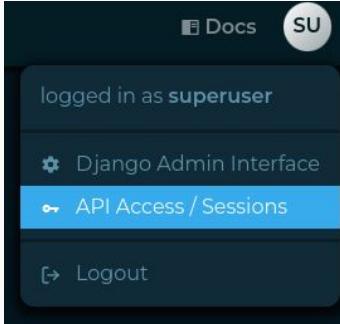
You can extract a lot of information regarding malicious IP addresses belonging to botnets here!

The screenshot shows the GreedyBear web application. At the top, there's a navigation bar with links for Home, Dashboard, Feeds, Docs, and Login. The central feature is a large logo of a blue bear holding a pink honey pot, set against a pink hexagonal background. To the right of the logo, the text "v1.2.1" is displayed. Below the logo, a dark box contains the text: "The project goal is to extract data of the attacks detected by a TPOT or a cluster of them and to generate some feeds that can be used to prevent and detect attacks." At the bottom, there's a "GreedyBear News" section with a card for a "New project available: GreedyBear Honeynet Blog: Official announcement" dated "27th December 2021".

# 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.



Job #181

Comments (0) Delete

193.105.134.95

Analyzers Report 1/1 Connectors Report 0/0 Pivots Report 0/0 Visualizers Report 0/0 Full Report

	Actions	Status	Name	Process Time (s)
	All	SUCCESS	GreedyBear	0.46

root: [] 3 keys

report: [] 3 keys

ioc: [] 14 keys

id: 8

name: "193.105.134.95"

type: "ip"

log4j: false

cowrie: true

scanner: true

days\_seen: [] 558 items

last\_seen: "2024-10-11T08:51:40.075718"

first\_seen: "2022-10-11T08:10:00.899121"

times\_seen: 24195

# IntelOwl: Files 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: *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 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

## 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?

### Scan Files

Month: 65    Total: 68    ⓘ

observable (domain, IP, URL, HASH, etc...)    file

File(s) \*  91e300979dbed56033d3f9f821abbf631c71858cf9747fa65011c2fe1c515a28.xlsx

Playbooks    Analyzers/Connectors

Select Playbook   
Playbooks containing the majority of the Internal Static Analysis tools

# 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)

SUCCESS

Doc\_Info

```
▼ root: {} 3 keys
  ▼ report: {} 4 keys
    msodde: ""
    ▶ olevba: {} 7 keys
      mraptor: "ok"
    ▼ extracted_CVEs: [] 1 item
      ▼ 0: {} 3 keys
        ▶ CVEs: [] 4 items
          info: "StdOleLink (embedded OLE object - Known Related to CVE-2017-0199, CVE-2017-8570, CVE-2017-8759 or CVE-2018-8174)"
          clsid: "00000300-0000-0000-C000-000000000046"
```

# 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.](#)

SUCCESS

ClamAV

```
▼ root: {} 3 keys
  ▼ report: {} 2 keys
    ▼ detections: [] 2 items
      0: "Sanesecurity.Malware.28788.Heur.BadOne.cmd.UNOFFICIAL"
      1: "OnenoteDownloader.Qbot-9988007-0"
```

SUCCESS

Yara

```
date: "2025-02-14"
author: "Nicholas Dhaeyer - @DhaeyerWolf"
reference: "https://blog.didierstevens.com/2023/01/22/analyzing-malicious-onenote-documents/"
description: "OneNote files that contain embedded files that are not pictures."
```



# 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

SUCCESS

PDF\_Info

```
▶ report: [2 keys]
  ► pdfid: {} 1 key
  ▼ peepdf: {} 1 key
    ▼ stats: [] 1 item
      ▼ 0: {} 7 keys
        ▼ uris: [] 2 items
          0: "https://qusbec.com/Financing"
```

SUCCESS

Yara

```
▼ 4: {} 7 keys
  url: "https://github.com/Yara-Rules/rules.git"
  ▶ meta: {} 3 keys
    path: "/opt/deploy/files_required/yara/yara-rules_rules/maldocs/Maldoc_PDF.yar"
  ▶ tags: [] 2 items
    match: "invalid_trailer_structure"
```



# IntelOwl File Analysis - Static Analysis - PDF

- The URL extracted from the *PDF\_Info Analyzer* ([qusbec.com](http://qusbec.com)) is known to be malicious

Job #228 ⚠

Comments (0) Delete Rescan Save As Playbook Report

Reputation Visualizer Raw

qusbec.com domain

VirusTotal Engine Hits: 13

URLhaus found

ThreatFox

Tranco Rank

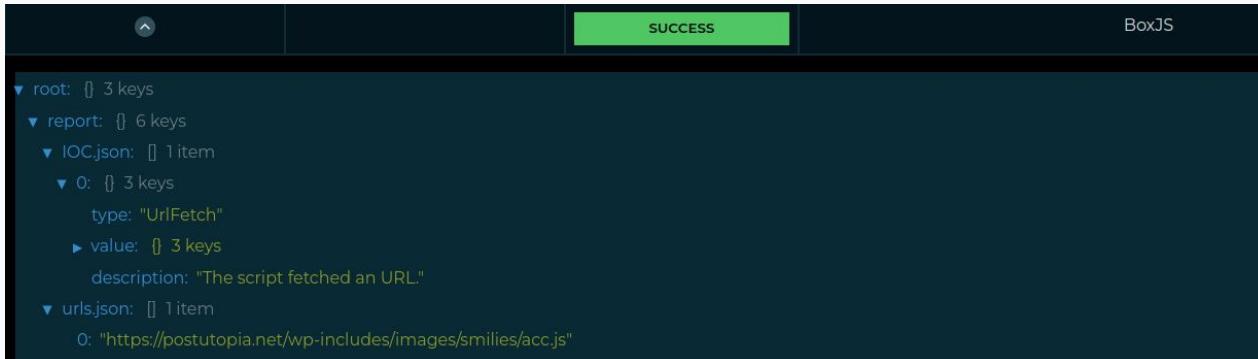
Phishtank PhishingArmy InQuest OTX AlienVault (I) Malware...Malware.Domain.Feed.V2...November.03.2020

DNS0 EU Malicious Detector GoogleSafebrowsing CloudFlare Malicious Detector Quad9 Malicious Detector

Intel owl

# IntelOwl File Analysis - Static Analysis - Javascript

- Specific BoxJS analyzer extracts a suspicious embedded URL



```
▶ root: {} 3 keys
  ▶ report: {} 6 keys
    ▶ IOC.json: {} 1 item
      ▶ 0: {} 3 keys
        type: "UrlFetch"
        ▶ value: {} 3 keys
          description: "The script fetched an URL."
    ▶ urls.json: {} 1 item
      0: "https://postutopia.net/wp-includes/images/smilies/acc.js"
```

- 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”

APKID

SUCCESS

```
matches: {} 2 keys
  anti_vm: [] 6 items
    0: "Build.FINGERPRINT check"
    1: "Build.MANUFACTURER check"
    2: "Build.BRAND check"
    3: "Build.DEVICE check"
    4: "Build.TAGS check"
    5: "subscriber ID check"
```

Quark\_Engine

SUCCESS

```
root: {} 3 keys
  report: {} 6 keys
    md5: "94135149ae7347873663d34e78791970"
    crimes: [] 211 items
      size_bytes: 2898525
      total_score: 211
    apk_filename: "job_2024_05_14_10_10_28_7fe0933da873ec8b10ba09ebcf26dd43f46cc72d2855a9c7a7df1eff795089a3.apk"
    threat_level: "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.

```
SUCCESS
Signature_Info

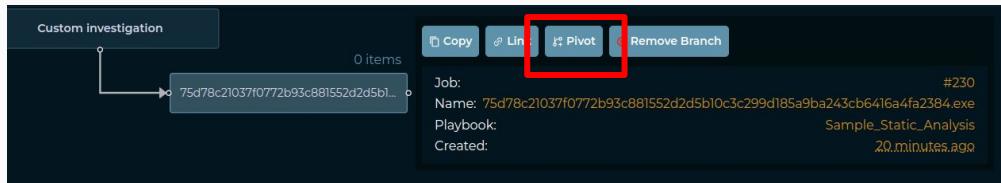
▼ root: {} 3 keys
  ▼ report: {} 5 keys
    verified: false
    corrupted: false
    no_signature: true
    checksum_mismatch: false
    certificate_has_expired: false
```

# 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!

**Scan Files**

Month: 72 Total: 75

observable (domain, IP, URL, HASH, etc...)  file

File(s) \*  75d78c21037f0772b93c881552d2d5b1...299d185a9ba243cb6416a4fa2384.exe

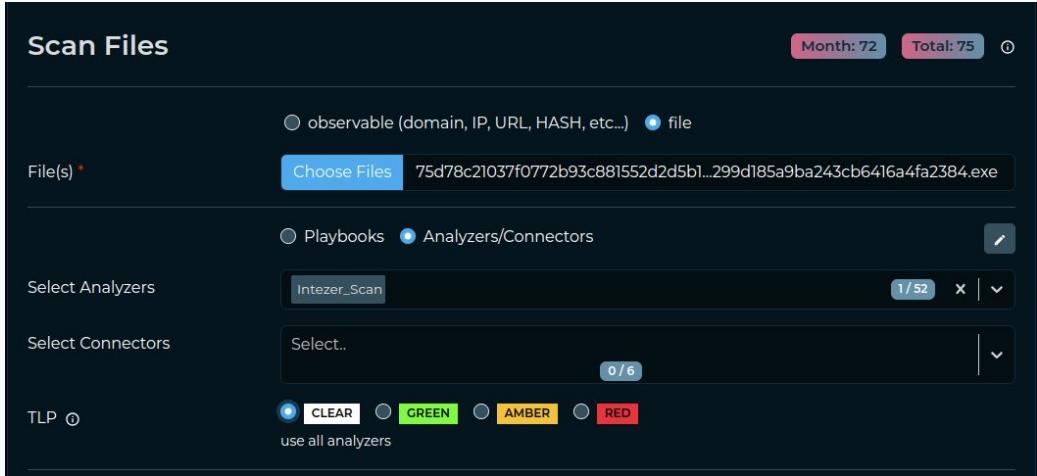
Playbooks  Analyzers/Connectors

Select Analyzers  1 / 52

Select Connectors  0 / 6

TLP

use all analyzers



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!

The screenshot shows the IntelOwl interface with the 'Capa\_Info' tab selected. A green 'SUCCESS' button is visible at the top. Below it, a list of API calls and their counts is displayed:

- ▶ PEB access: {} 3 keys
- ▶ contain loop: {} 3 keys
- ▶ get file size: {} 3 keys
- ▶ delay execution: {} 3 keys
- ▶ parse PE header: {} 3 keys
- ▶ terminate process: {} 3 keys
- ▶ create or open file: {} 3 keys
- ▶ read file on Windows: {} 3 keys
- ▶ write file on Windows: {} 3 keys
- ▶ set environment variable: {} 3 keys
- ▶ create process on Windows: {} 3 keys
- ▶ get geographical location: {} 3 keys

A navigation bar at the bottom right shows pages 1 and 2.

# IntelOwl File Analysis - EXE

## Final Investigation Schema



# IntelOwl File Analysis - Hash

It may happen that you get a 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?

**Scan Observables**

Month: 79 Total: 83 ⓘ

observable (domain, IP, URL, HASH, etc...)  file

Observable Value(s) \*

8ED4B4ED952526D89899E723F3488DE4

Playbooks  Analyzers/Connectors

Select Playbook

FREE\_TO\_USE\_ANALYZERS  
A playbook containing all free to use analyzers.



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

SUCCESS

HashLookupServer\_Get\_Observable

FileSize: "2520"

▼ ProductCode: {} 7 keys

- MfgCode: "608"
- Language: "Multilanguage"
- ProductCode: "190742"
- ProductName: "Cumulative Update for Windows Server 2016 for x64 (KB4338817)"

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

The screenshot shows two separate analysis results from the IntelOwl interface.

**Suricata:**

- root: {} 3 keys
  - report: {} 1 key
    - signatures: {} 2 keys
      - SURICATA HTTP unable to match response to request: {} 12 keys
      - ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1: {} 13 keys
    - errors: {} 0 items
  - parameters: {} 2 keys

**Hfinger:**

- root: {} 3 keys
  - report: {} 2 keys
    - extraction: {} 34 items
      - 0: {} 6 keys
        - ip\_dst: "195.123.218.40"
        - ip\_src: "10.4.4.101"
        - port\_dst: "80"
        - port\_src: "50721"
        - epoch\_time: "1712197330.861440000"
        - fingerprint: "1|||php||PO||co-ty,co-en,us-ag,ho,co-le,co,ca-co||co-ty:ap-os/co-en:bi/us-ag:c770c19f/co:Ke-Al/ca-co:nc|A|5|2.0"

# IntelOwl: Organizations



# IntelOwl Organizations: Create a new organization

The screenshot shows the Django Admin interface for IntelOwl. At the top, there are navigation links: 'Docs', 'Social' (with a notification badge '3'), and a circular profile icon labeled 'TE'. Below the header, a sidebar lists several options: 'Django Admin Interface', 'Organization' (which is highlighted in blue), 'API Access', 'Change password', and 'Your plugin configuration'. At the bottom of the sidebar is a 'Logout' button.

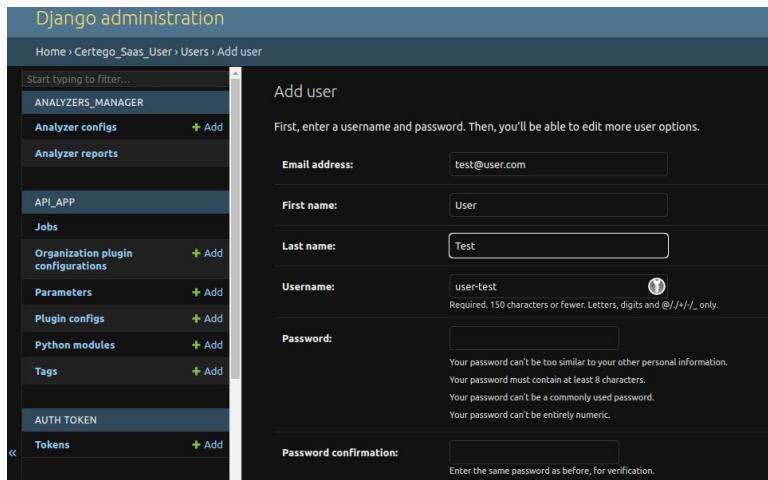
The screenshot shows the 'Organization' creation page in IntelOwl. The header includes the IntelOwl logo (v6.0.2), navigation links ('Home', 'Dashboard', 'History', 'Plugins', 'Scan'), and a search bar. Below the header, there are three tabs: 'Organization' (selected), 'Organization Config', and 'Invitations'. A message states: 'You are not a member of any organization. You can choose to create a new organization or join an existing one by asking an organization owner to send you an invitation.' A 'Create a new organization' button is visible.

The screenshot shows the details of an organization named 'testorg'. The header is identical to the previous screenshot. The main content area displays the organization's name, 'Owner: (@test)', and 'Established: 8th May, 2024'. Below this, there are two sections: 'Members 1 total' and 'Pending Invitations 0 total'. The 'Members' section lists one member: '1. (@test)' established on '8th May, 2024' with the role 'Owner'. The 'Pending Invitations' section is currently empty.

# 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



 A screenshot of the Django administration interface showing the "Add user" form. The left sidebar lists various models: ANALYZERS\_MANAGER, Analyzer config, Analyzer reports, API\_APP, Jobs, Organization plugin configurations, Parameters, Plugin configs, Python modules, Tags, and AUTH TOKEN. The main form fields include "Email address" (test@user.com), "First name" (User), "Last name" (Test), "Username" (user-test), "Password", and "Password confirmation". Validation messages for the password field are visible on the right.
 

Django administration

Home > Certego\_Saas\_User > Users > Add user

Add user

First, enter a username and password. Then, you'll be able to edit more user options.

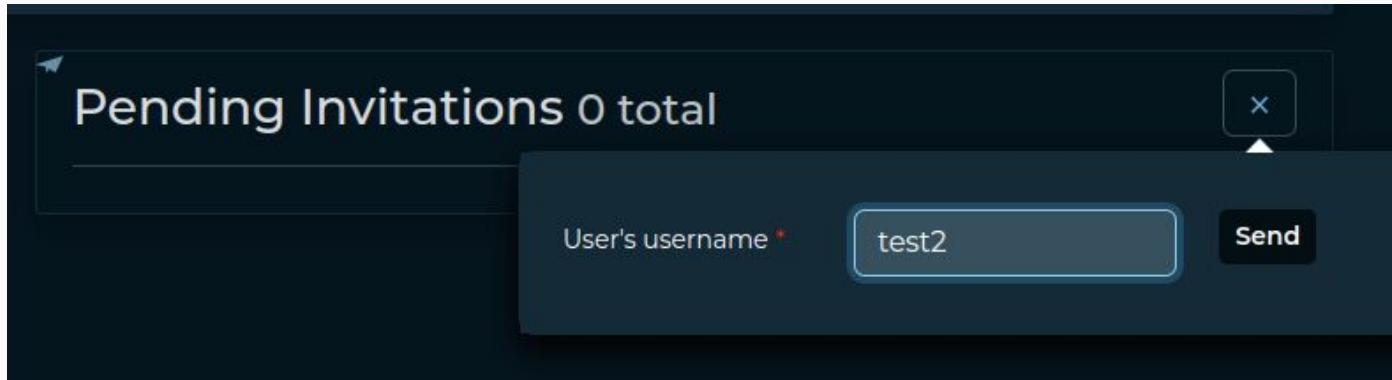
Email address:	<input type="text" value="test@user.com"/>
First name:	<input type="text" value="User"/>
Last name:	<input type="text" value="Test"/>
Username:	<input type="text" value="user-test"/> <small>Required: 150 characters or fewer. Letters, digits and @/./+/-/_ only.</small>
Password:	<input type="password"/> <small>Your password can't be too similar to your other personal information. Your password must contain at least 8 characters. Your password can't be a commonly used password. Your password can't be entirely numeric.</small>
Password confirmation:	<input type="password"/> <small>Enter the same password as before, for verification.</small>

Pending Invitations 0 total

User's username \*

Send

X



Pending Invitations 1 total

1. test2 8th May 2024

+  
Red





# IntelOwl Organizations: New user accepts the invitation

Intel owl v6.0.2 Home Dashboard History Plugins Scan Docs

Organization Organization Config Invitations

Being part of an organization has many perks. [Learn more.](#)

Invitations List

1. Organization testorg	Invited by test	No. of Members 1	Received 12:40 PM May 8th, 2024	Pending
<input checked="" type="checkbox"/> <input type="checkbox"/>				

Intel owl v6.0.2 Home Dashboard History Plugins Scan

Organization Organization Config Invitations

testorg Owner: (@test) Established: 8th May 2024

Members 2 total

1. (@test)	8th May 2024	Owner
2. (@test2)	8th May 2024	



# IntelOwl Organizations: Organization Plugin configuration

Intel owl v6.0.2    Home    Dashboard    History    Plugins    Scan

Organization    Organization Config    Invitations

## testorg's plugin configuration

Note: Your plugin configuration overrides your organization's configuration.

Parameters    Secrets

# 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).

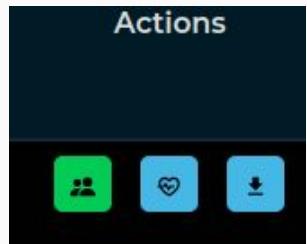
**Intel owl v6.0.2** Home Dashboard Plugins Scan Docs Social

Analyzers 157 total

Analyzers are the most important plugins in IntelOwl. They allow to perform data extraction on the observables and/or files that you would like to analyze. For more info check the [official doc](#)

Note: Hover over a configured icon to view configuration status and errors if any.

Info	Name	Active	Configured	Description	Type	Supported types	Maximum TLP	Actions
	APKID	✓	✓	APKID identifies many compilers, packers, obfuscators, and other weird stuff from an APK or DEX file.	file	<ul style="list-style-type: none"> <li>application/java-archive</li> <li>application/vnd.android.package-archive</li> <li>application/vnd.android.package-archive</li> <li>application/x-dex</li> <li>application/zip</li> </ul>	RED	  



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

Docs Social 3 TE

logged in as **test2**

- Django Admin Interface
- Organization
- API Access**
- Change password
- Your plugin configuration
- Logout

Dashboard History Plugins Scan

You can generate an API key to access IntelOwl's RESTful API. Take a look to the available Python and Go clients: [Learn more](#).

API Access

No active API key

[Generate +](#)

You can generate an API key to access IntelOwl's RESTful API. Take a look to the available Python and Go clients: [Learn more](#).

API Access

Created 12:46 PM May 8th, 2024

[REDACTED] [Show 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)
```

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!

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:

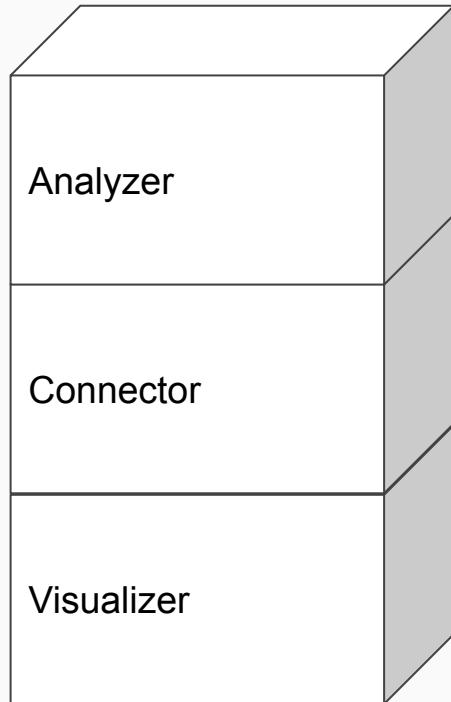
- First, we briefly explain the Plugin Framework and talk about the Software Architecture of IntelOwl
- Then, IT'S CHALLENGE TIME! Everyone choose which type of challenge they want:
  - If you have a specific use case in mind, tell us and we'll come to you to make a plan together of what can be done 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.

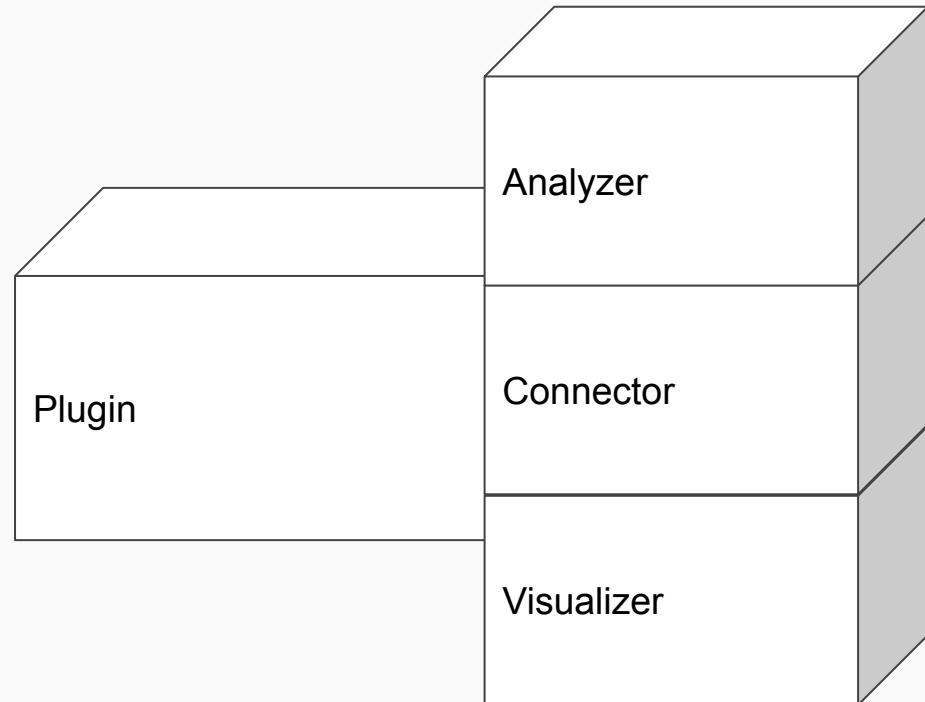
THIS IS A CONTEST! :)

Open a Pull Request to the [IntelOwl Github Repo](#) with your personal addition!

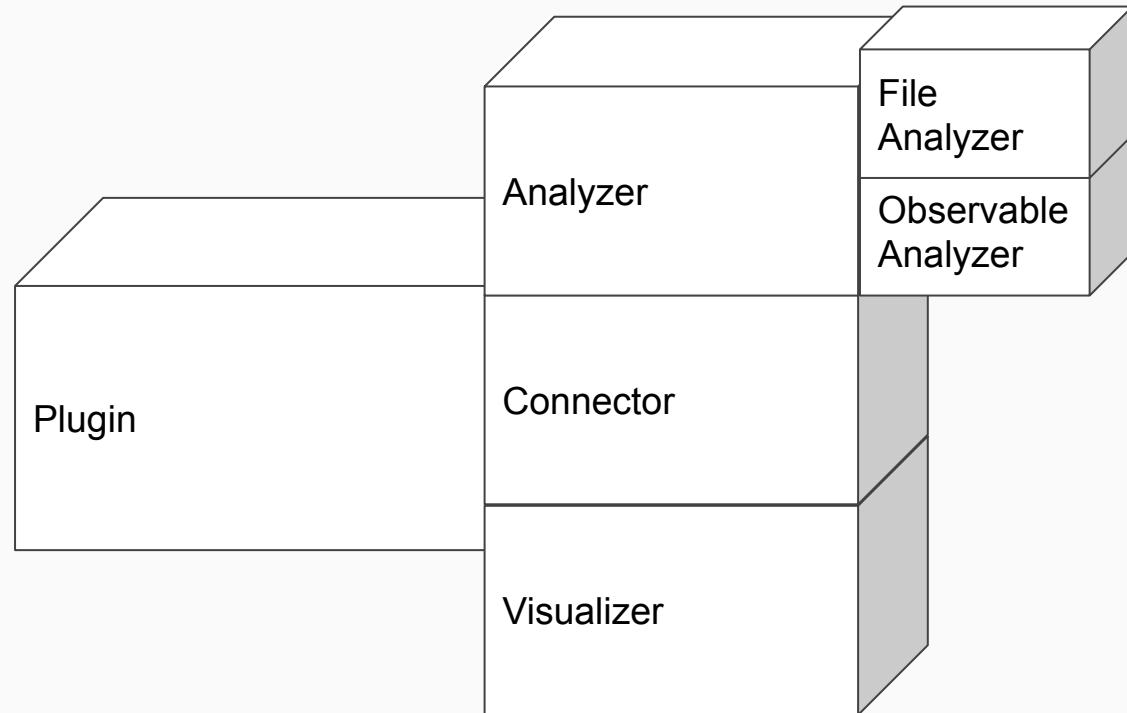
At the end of the Workshop we'll review the PR and select the best one!

**The winner will win a fantastic and unique IntelOwl - Honeynet Swag :)**

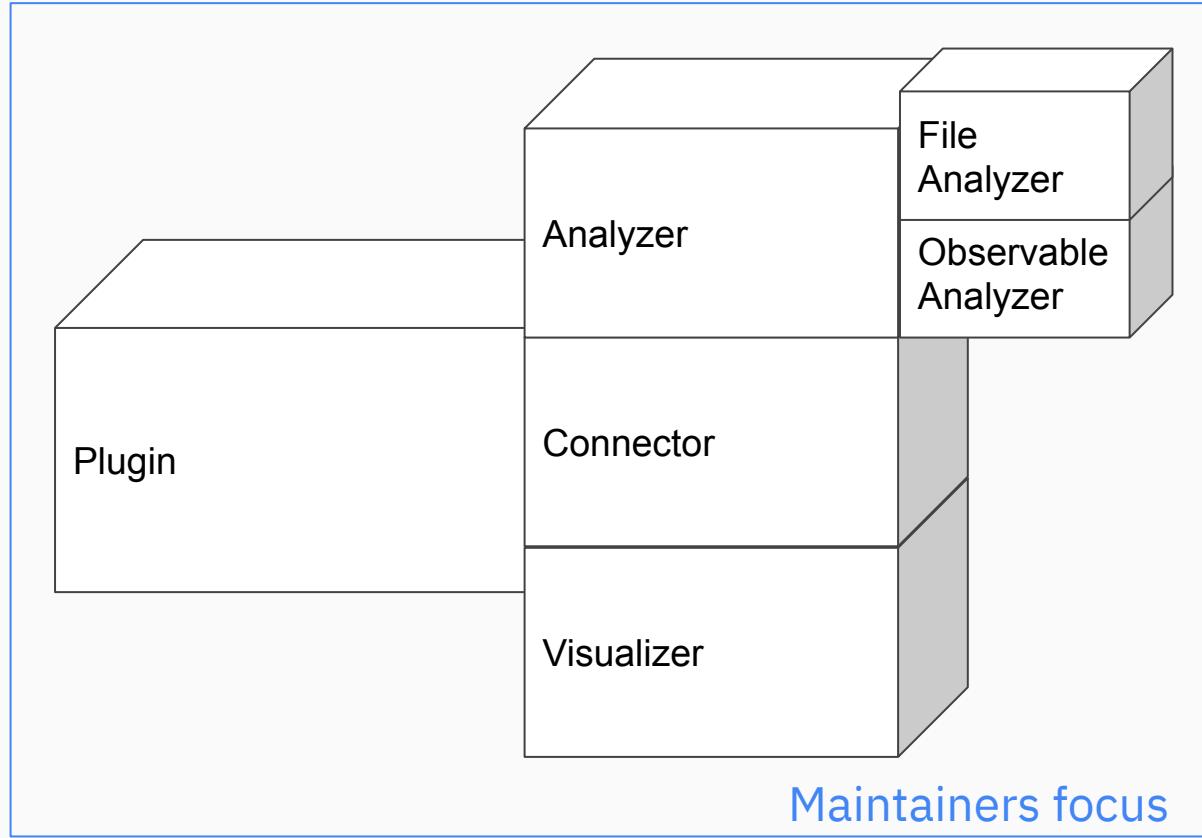




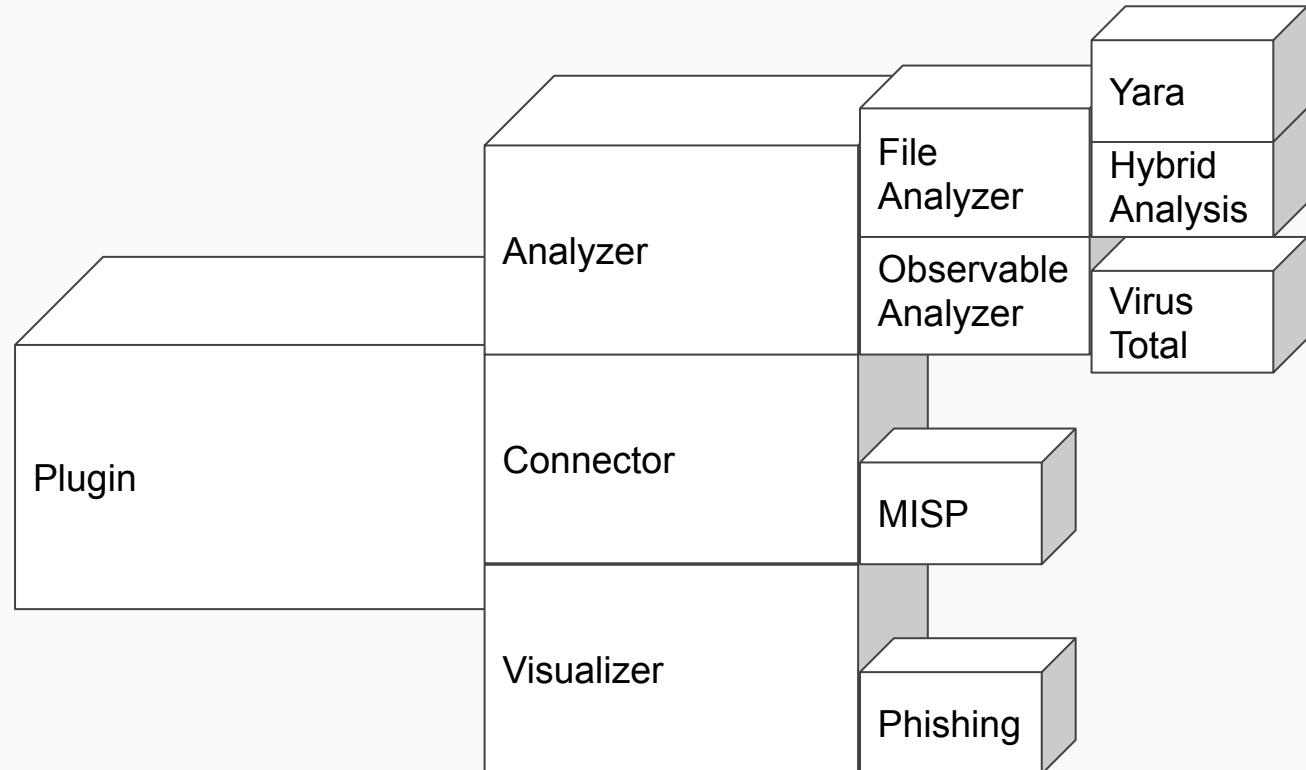
# IntelOwl - Software Architecture



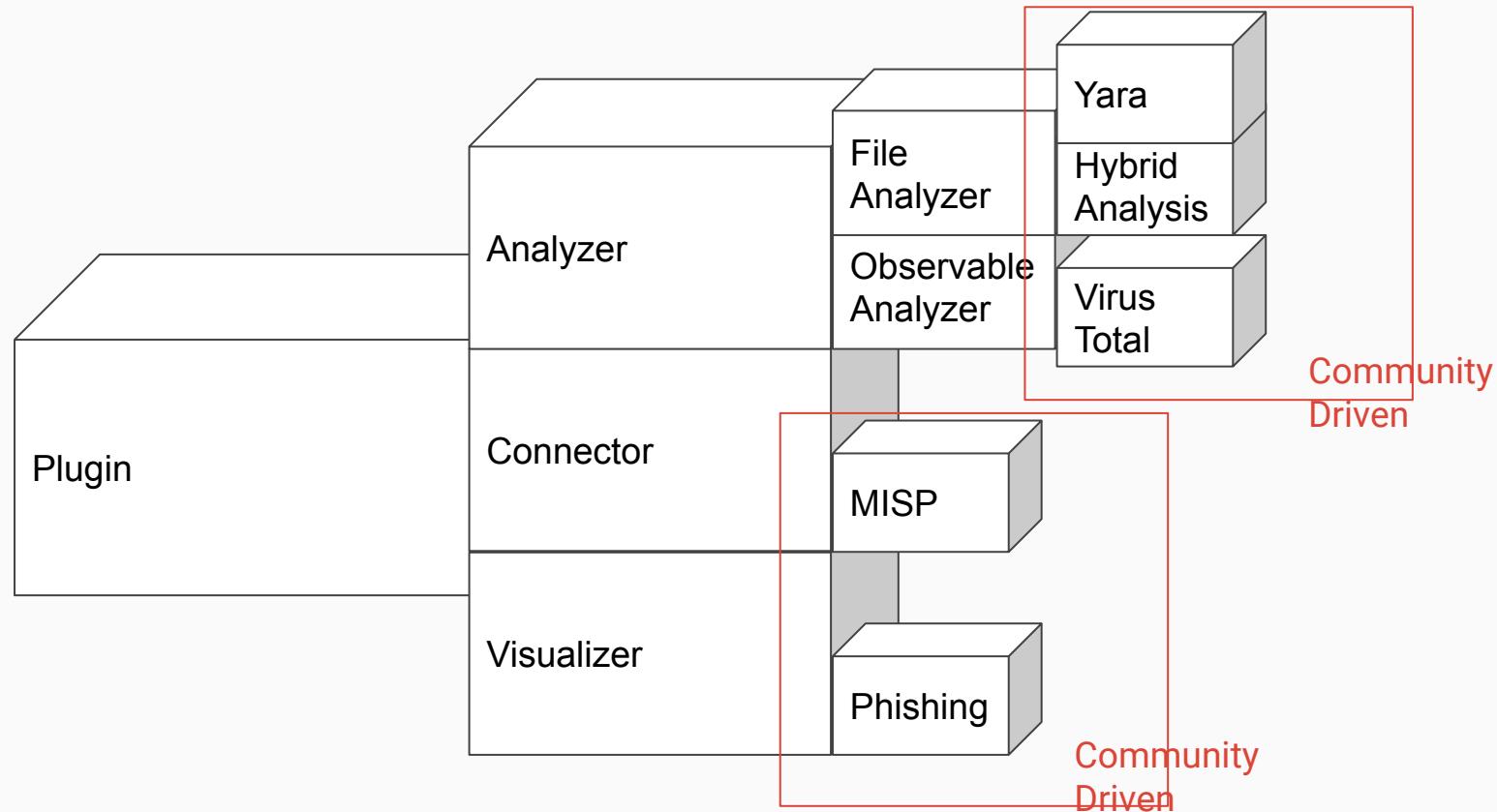
# IntelOwl - Software Architecture



# IntelOwl - Software Architecture

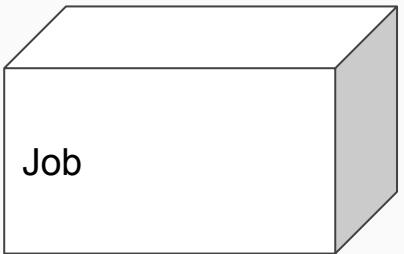


# IntelOwl - Software Architecture

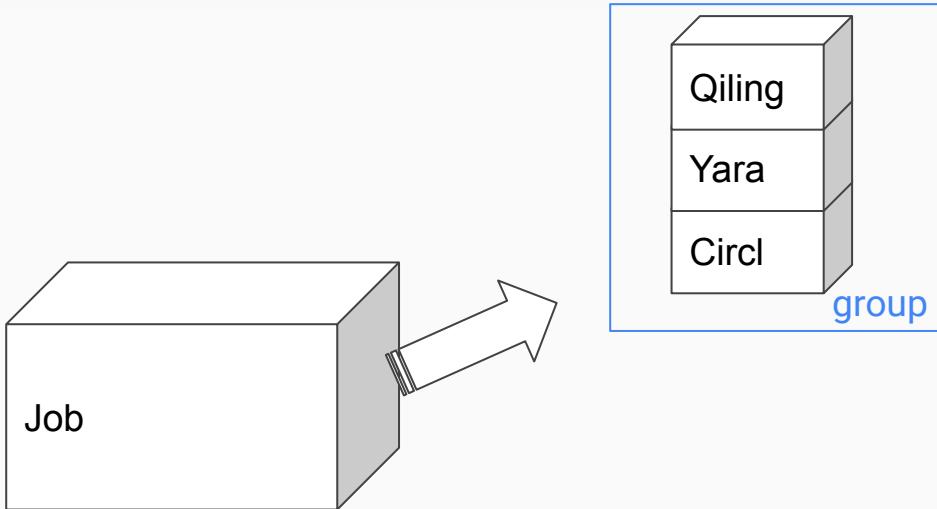




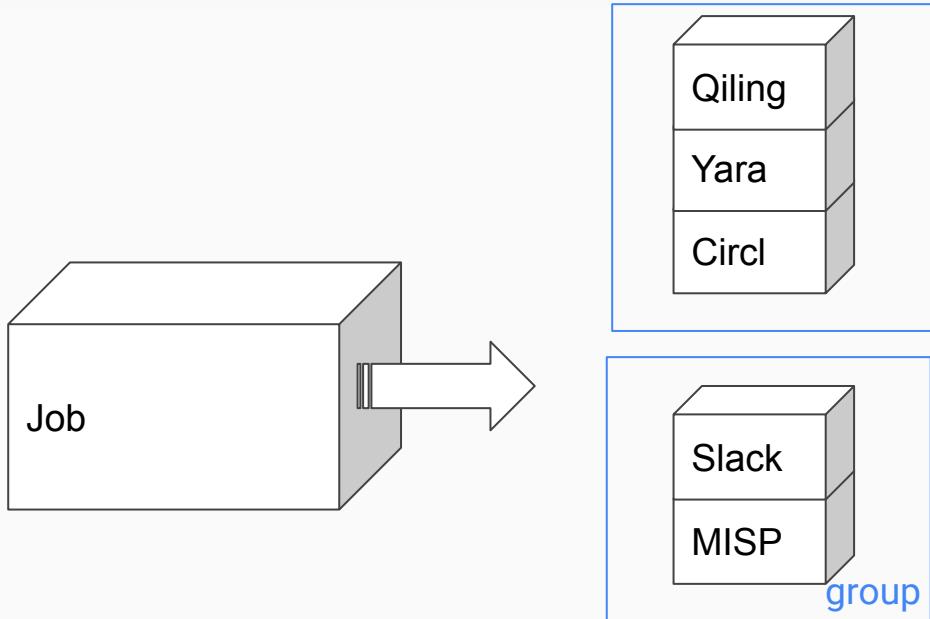
Driven



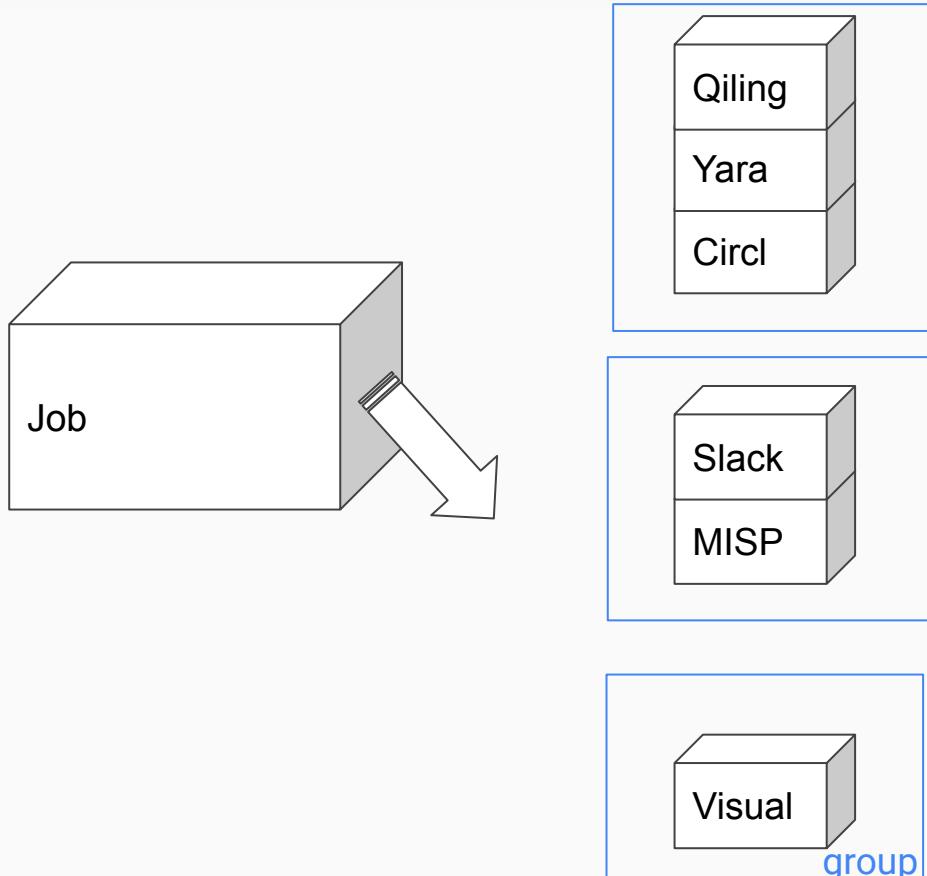
# IntelOwl - Software Architecture



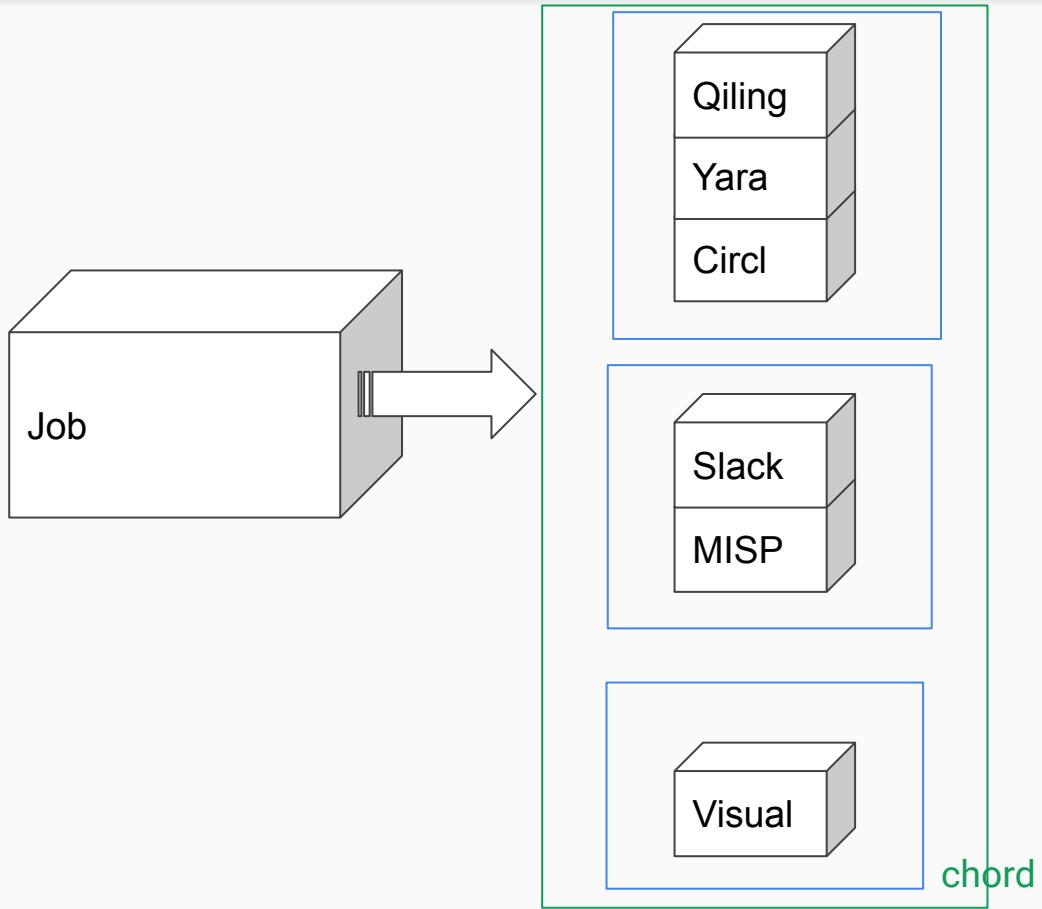
# IntelOwl - Software Architecture



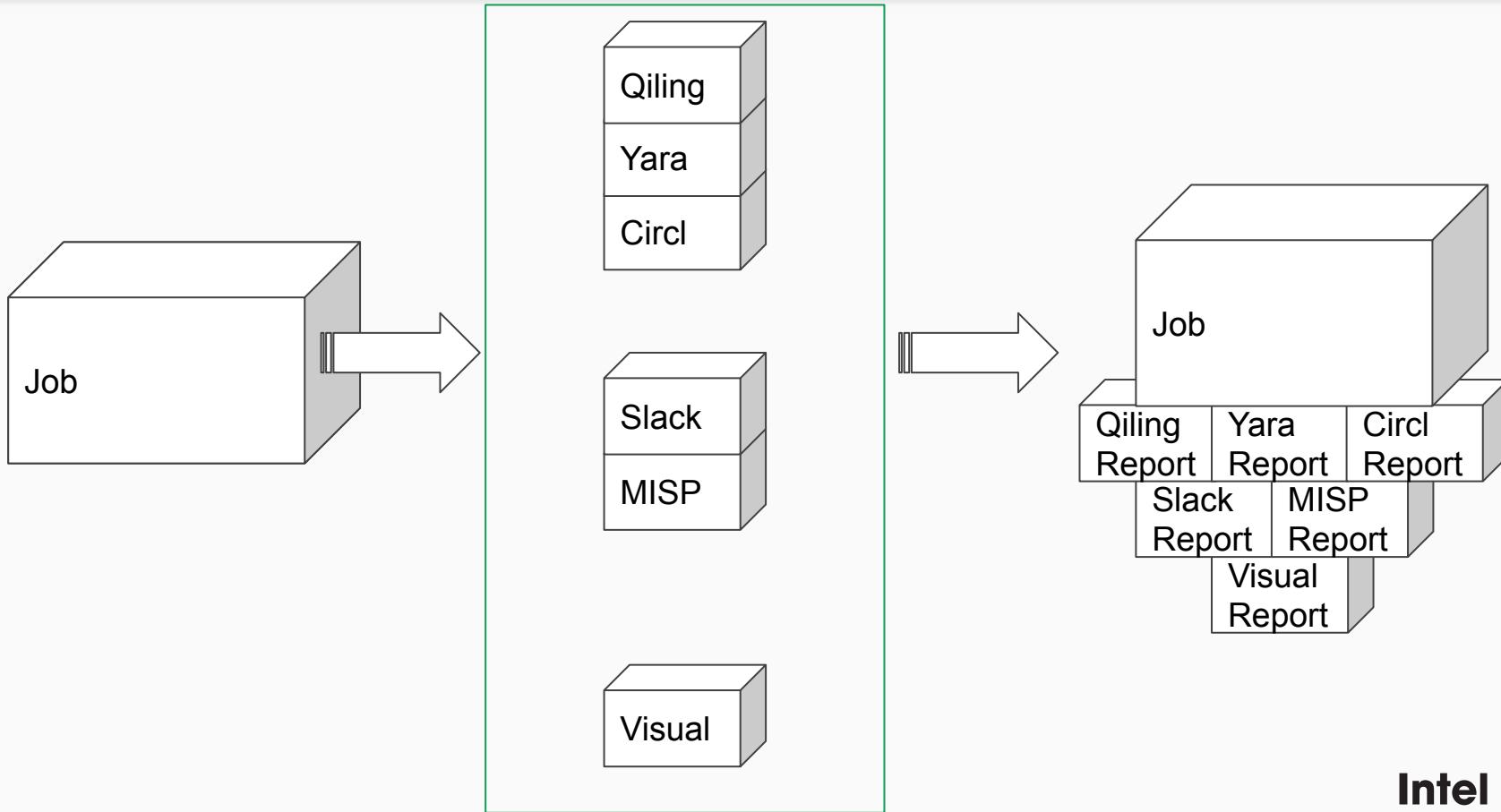
# IntelOwl - Software Architecture



# IntelOwl - Software Architecture



# IntelOwl - Software Architecture



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!

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.

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