IntelOwl Project

“making the life of cyber security analysts easier”

The Honeynet Workshop - Denmark ‘24

Say “hi” to the team :)

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

certego

Threat Intelligence Team

HN/P

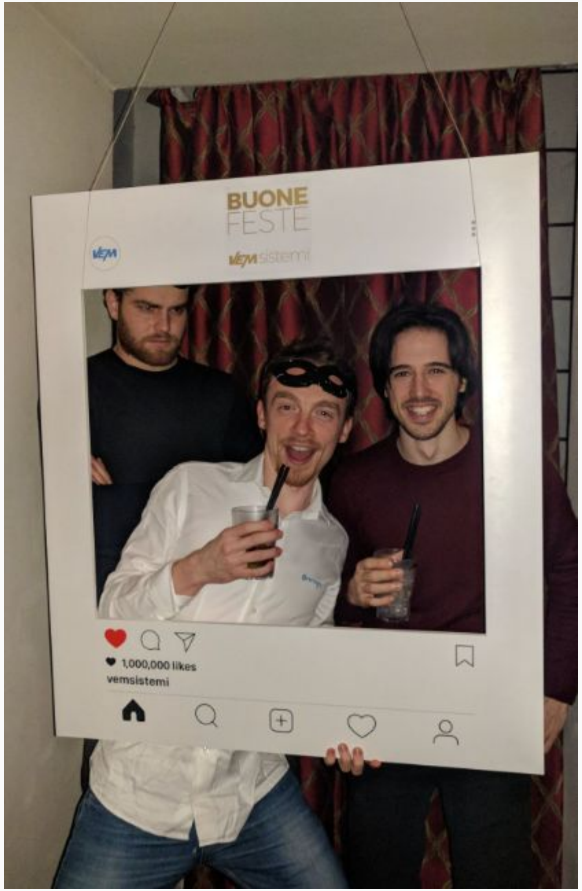
Members

Who are you?

Enjoying myself in the Cyber Security field!

I'll never stop learning!

We are like superheroes!

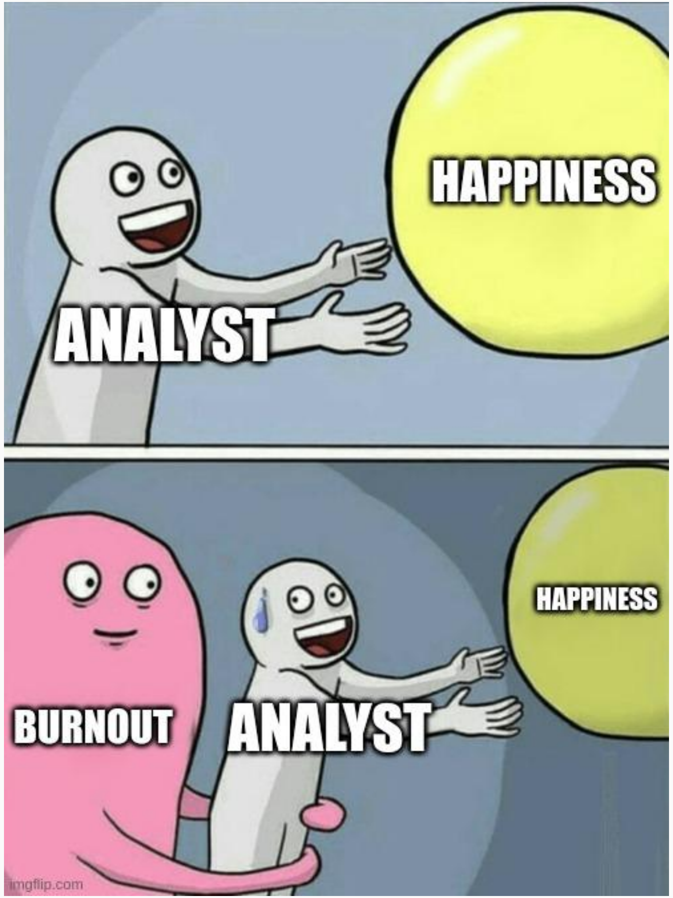


I have the best colleagues ever!

This is my dream job!

Intel Owl

Unveil the reality

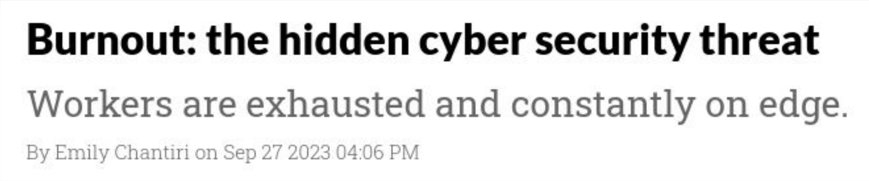


Unveil the reality

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

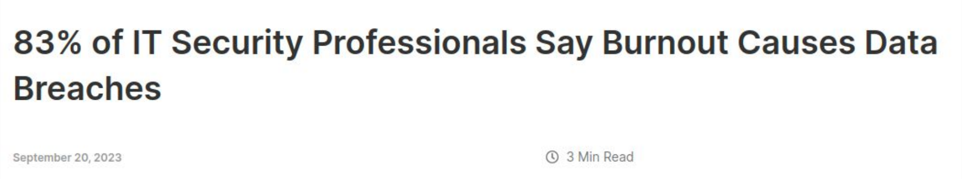


Burnout: the hidden cyber security threat

Workers are exhausted and constantly on edge.

By Emily Chantiri on Sep 27 2023 04:06 PM

ref: AECS

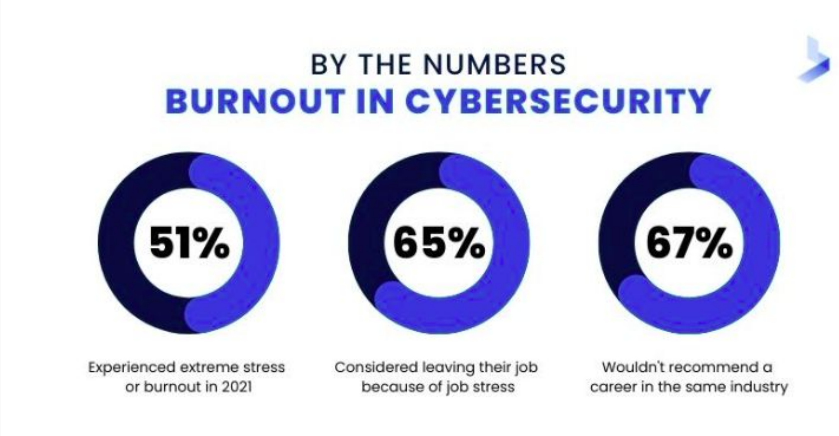


83% of IT Security Professionals Say Burnout Causes Data Breaches

September 20, 2023

3 Min Read

ref: DarkReading



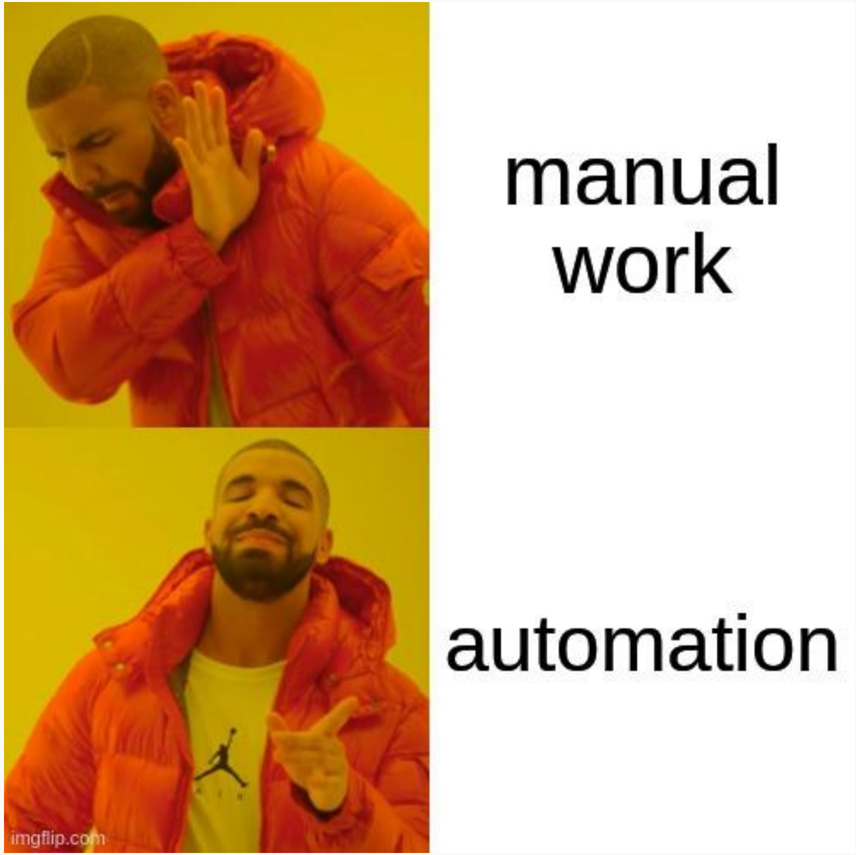
ref: Bitlyft

Automate, automate, automate

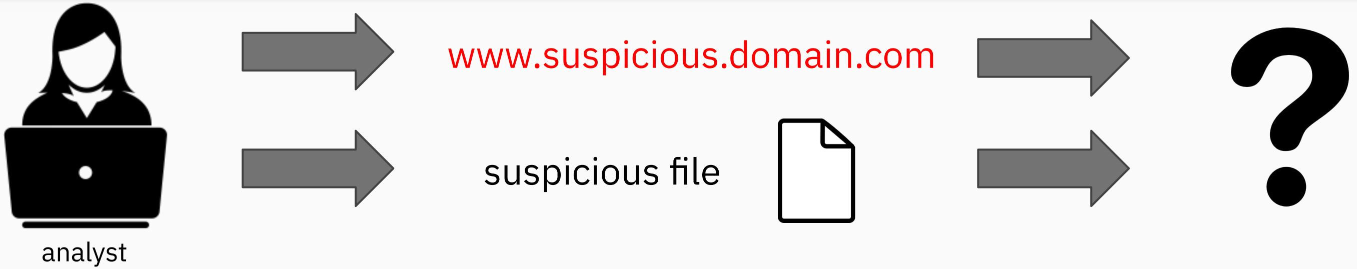
2017:

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

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



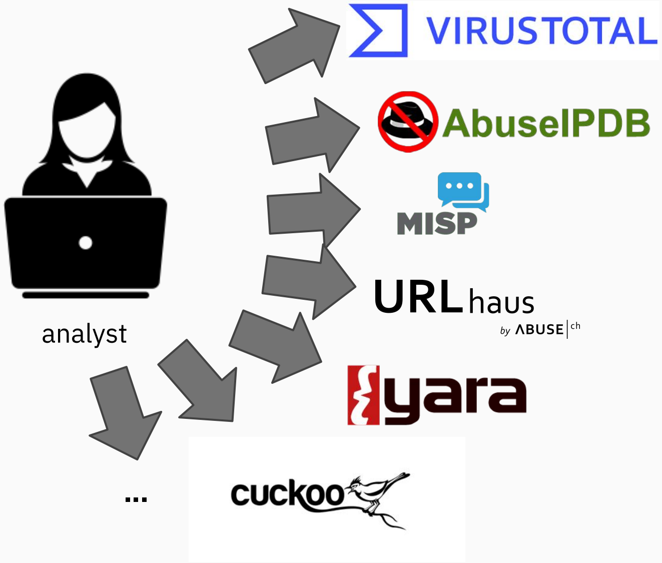
The bottleneck: acquisition of threat intelligence context



www.suspicious.domain.com

suspicious file

analyst



analyst

VIRUSTOTAL

AbuseIPDB

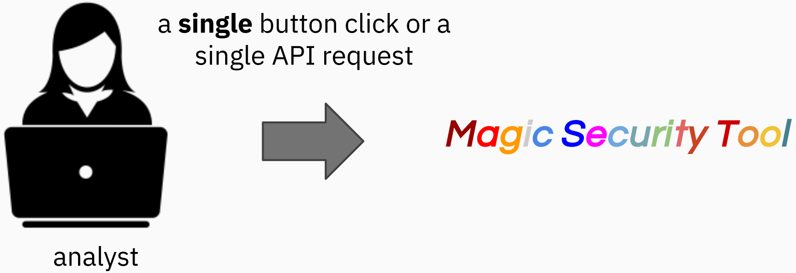
MISP

URLhaus by ABUSE|ch

yara

cuckoo

...



a **single** button click or a single API request

analyst

Magic Security Tool

We were looking for a tool

Our requirements were:

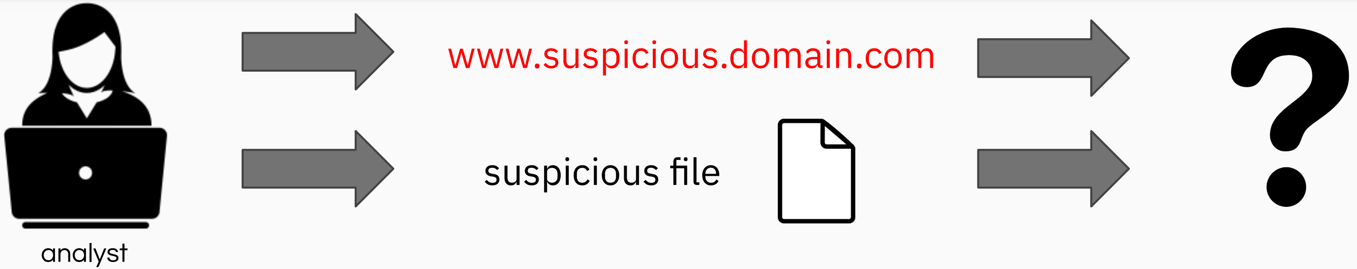
- Automated extraction of threat intelligence data from different sources
- Full-featured Web Application with user-friendly interface
- Client library for easy integrations with other security tools
- High possibility of customization to allow different use cases
- High level of scalability and speed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

IntelOwl was born

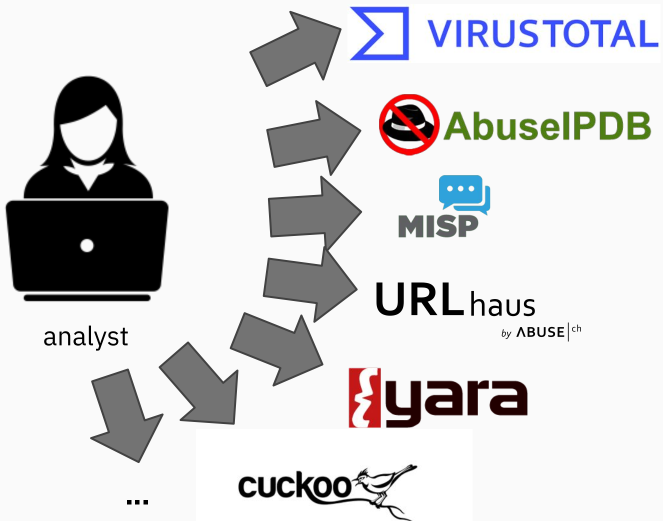
Born in Certego at the start of 2020, it is a great example of a successful Open Source project: right now it is one of the most popular Threat Intel projects on GitHub (>3k stars).

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

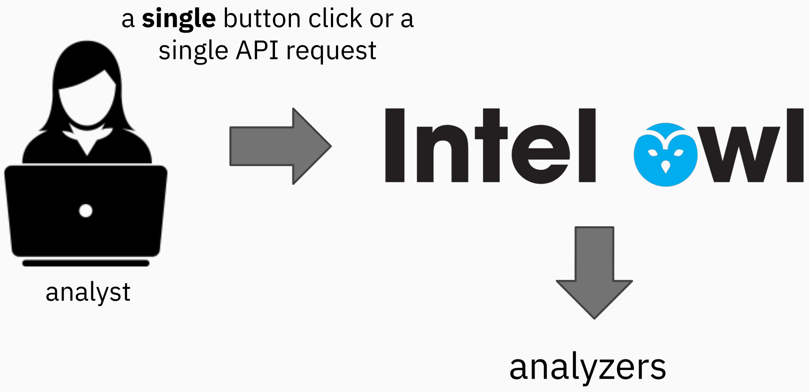
IntelOwl solution



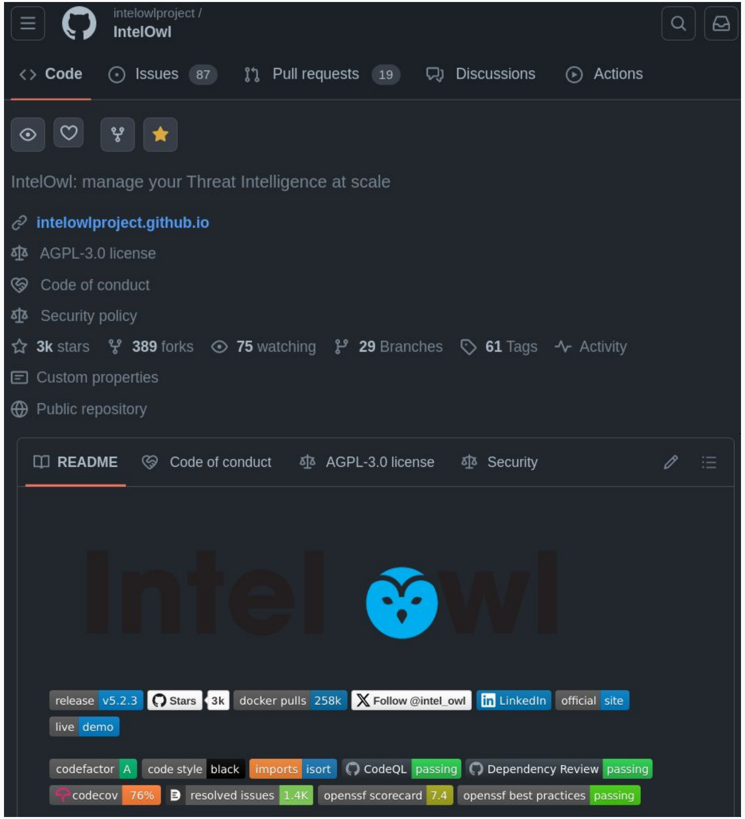
WithOUT Intel Owl



With Intel Owl


a **single** button click or a single API request

IntelOwl Repository & Tech Stack



intelowlproject /
IntelOwl

Code · Issues 87 · Pull requests 19 · Discussions · Actions

IntelOwl: manage your Threat Intelligence at scale

intelowlproject.github.io
AGPL-3.0 license
Code of conduct
Security policy
3k stars · 389 forks · 75 watching · 29 Branches · 61 Tags · Activity
Custom properties
Public repository

README · Code of conduct · AGPL-3.0 license · Security

Intel Owl

release v5.2.3 · Stars 3k · docker pulls 258k · Follow @intel_owl · LinkedIn · official site · live demo

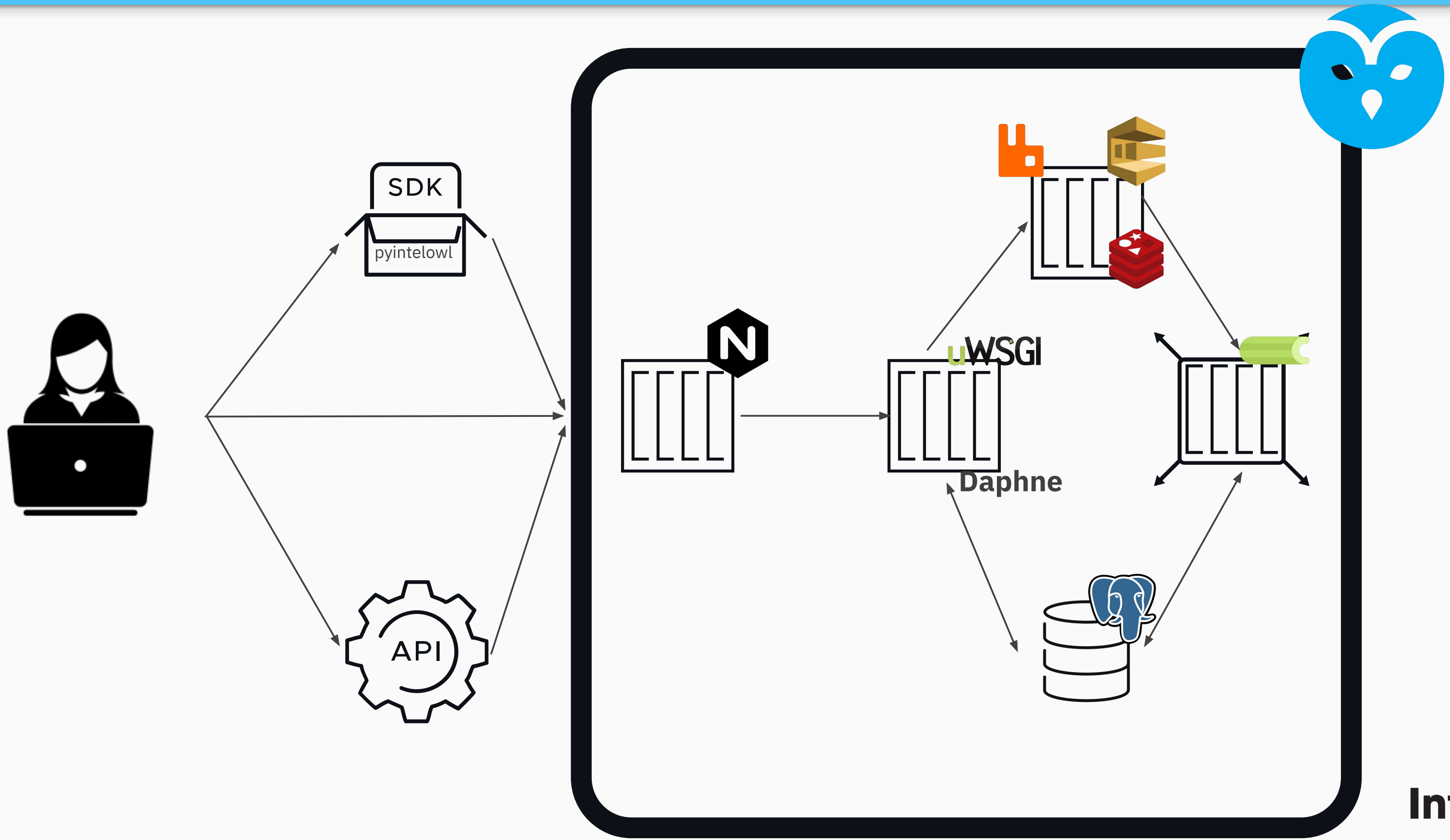
codefactor A · code style black · imports isort · CodeQL passing · Dependency Review passing · codecov 76% · resolved issues 1.4K · openssf scorecard 7.4 · openssf best practices passing

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

- Docker
- Python3
- ReactJS
- Django
- Django Rest Framework
- Celery
- PostgreSQL
- ElasticSearch
- Nginx
- Uwsgi
- Rabbit-MQ/SQS/Redis

Intel Owl

IntelOwl: Infrastructure Architecture



Intel Owl

IntelOwl: Installation

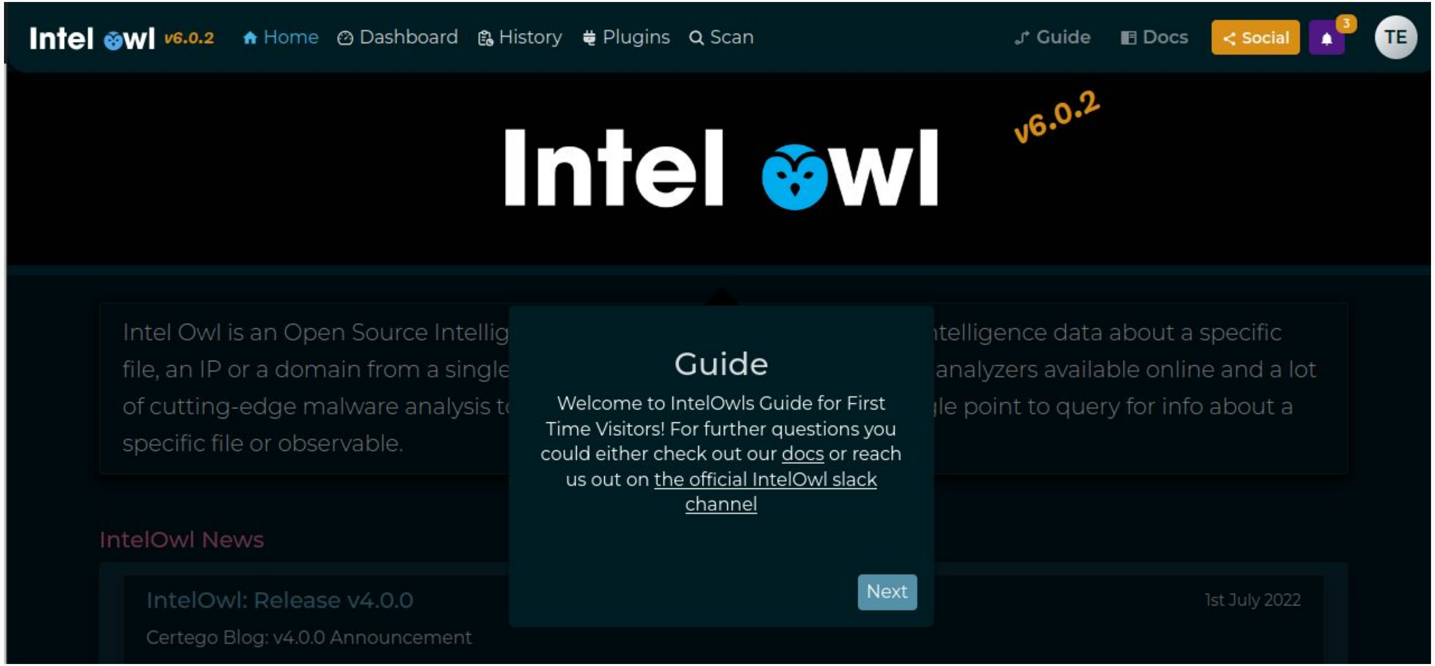
IT’S YOUR TIME TO TRY! Follow the steps below!

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/

# verify installed dependencies and start the app
./start prod up
# now the application is running on http://localhost:80

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

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

# Have fun!
```

IntelOwl Kick-off: Guide

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



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

…telligence data about a specific … analyzers available online and a lot … le point to query for info about a

Guide

Welcome to IntelOwls 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

Next

IntelOwl: Release v4.0.0

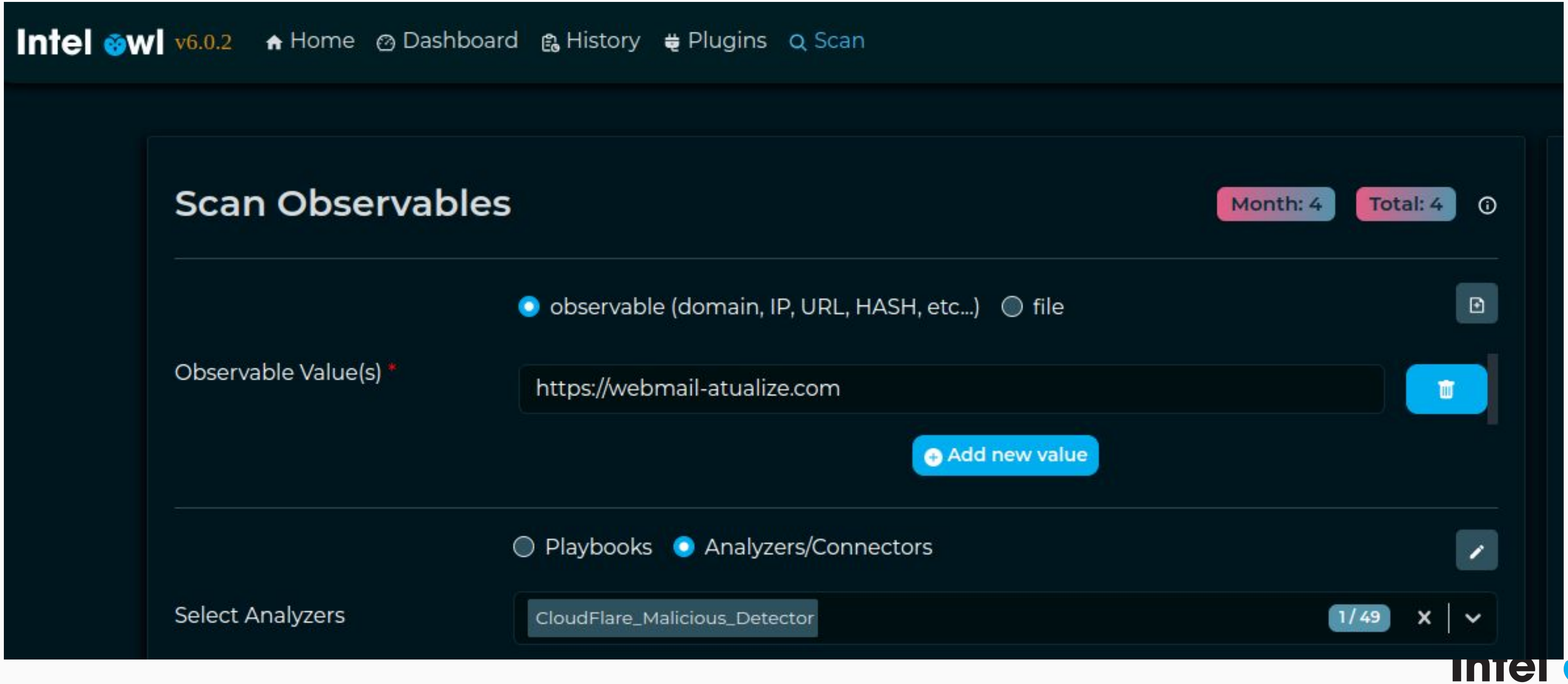
Certego Blog: v4.0.0 Announcement

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?



Scan Observables

Month: 4 Total: 4

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

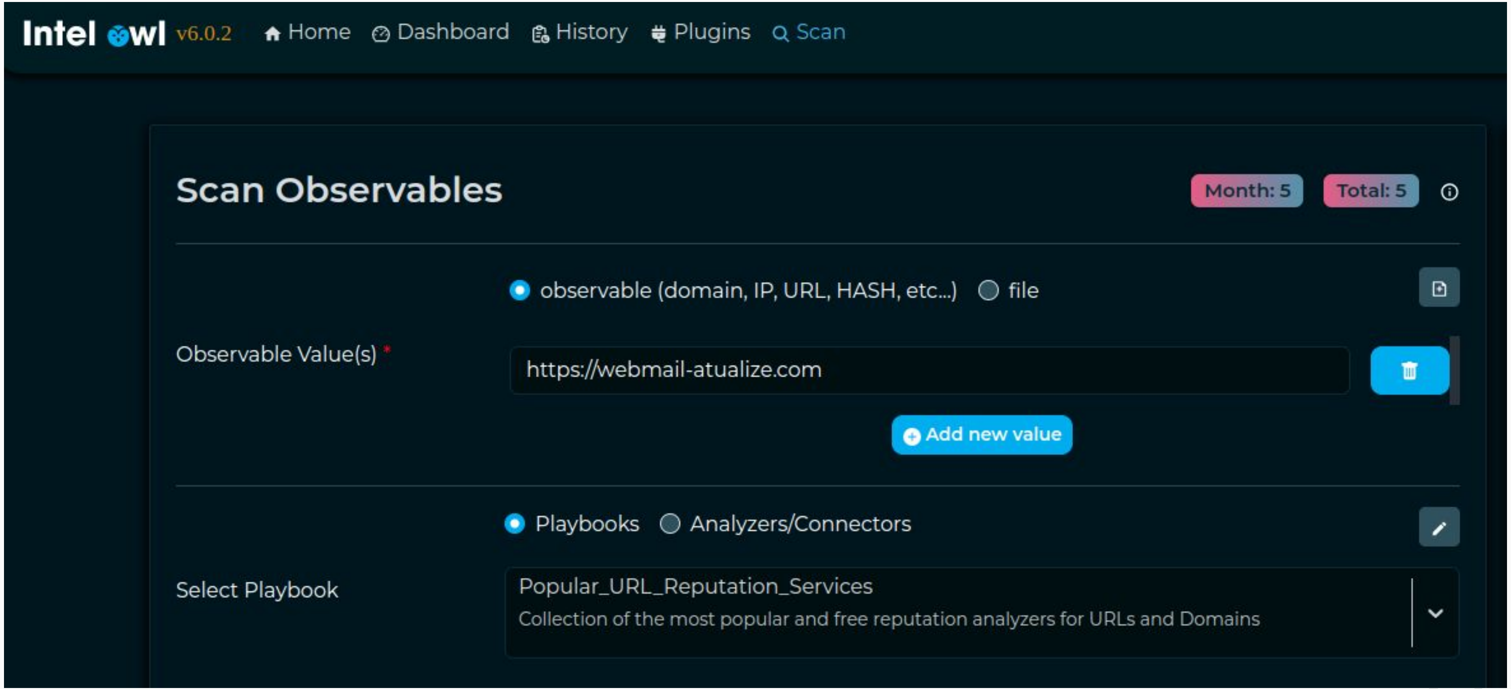
Observable Value(s) *: https://webmail-atualize.com

○ Playbooks ● Analyzers/Connectors

Select Analyzers: CloudFlare_Malicious_Detector 1/49

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?



Scan Observables

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

Observable Value(s) *: https://webmail-atualize.com

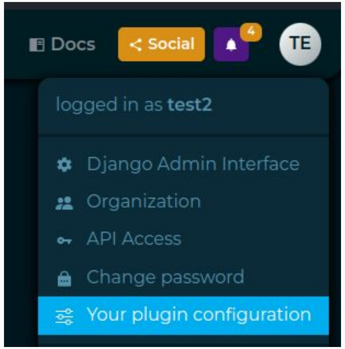
● Playbooks ○ Analyzers/Connectors

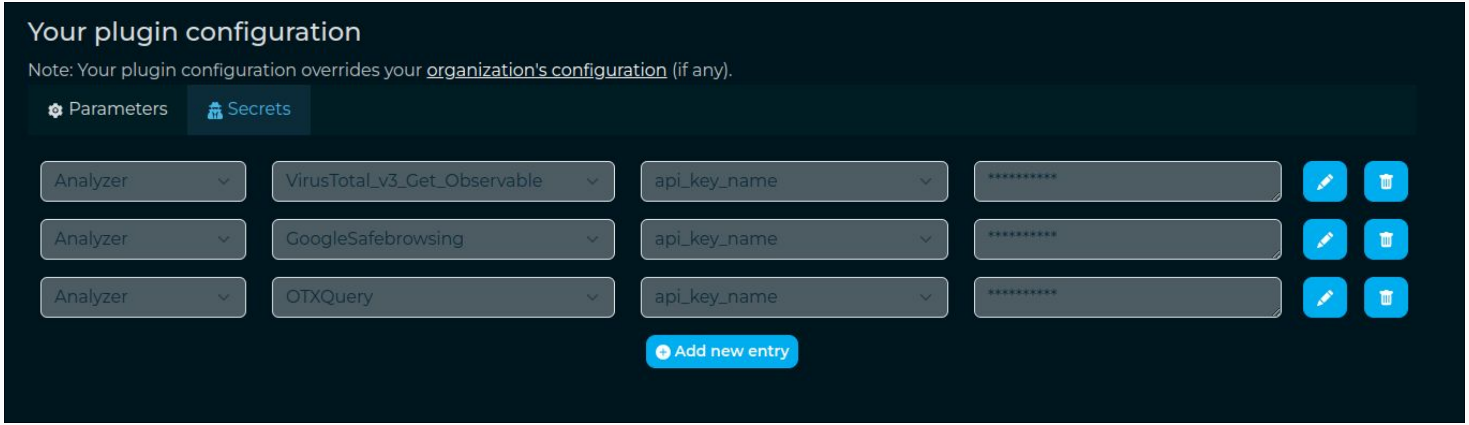
Select Playbook: Popular_URL_Reputation_Services
Collection of the most popular and free reputation analyzers for URLs and Domains

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




Your plugin configuration

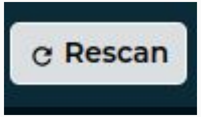
Note: Your plugin configuration overrides your organization's configuration (if any).

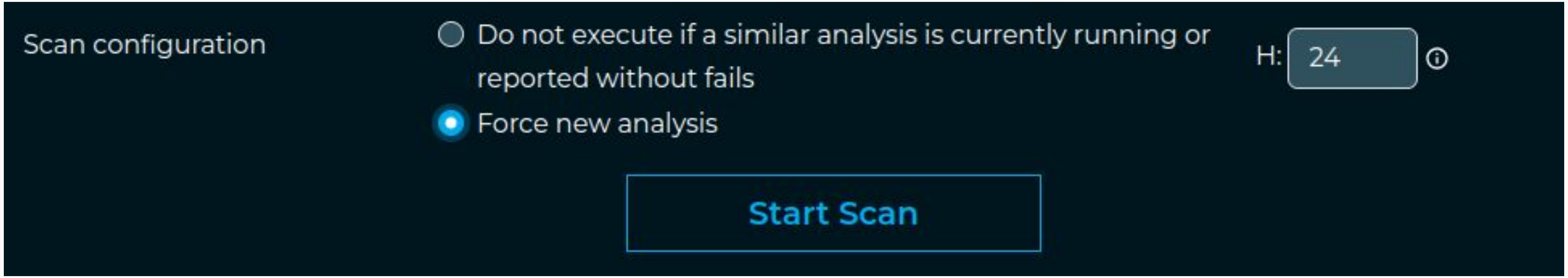
Analyzer	VirusTotal_v3_Get_Observable	api_key_name	***********
Analyzer	GoogleSafebrowsing	api_key_name	***********
Analyzer	OTXQuery	api_key_name	***********

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”





Scan configuration

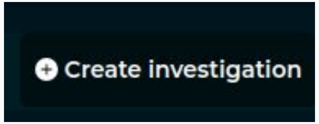
○ Do not execute if a similar analysis is currently running or reported without fails   H: 24

● Force new analysis

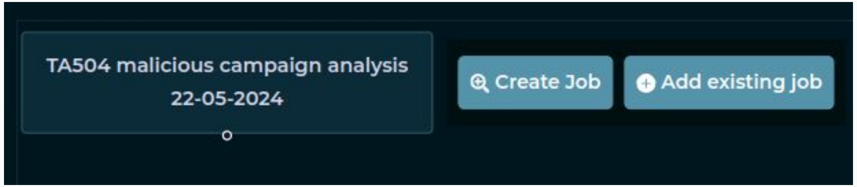
IntelOwl - Observables Analysis

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

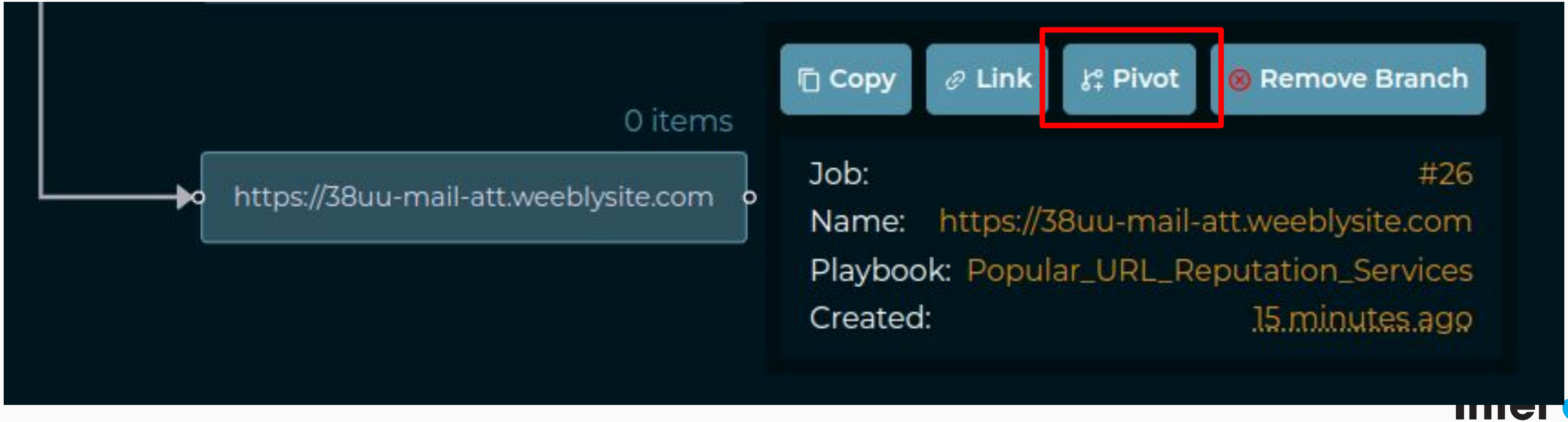

TA504 malicious campaign analysis
22-05-2024

- 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

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.



Job: #26
Name: https://38uu-mail-att.weeblysite.com
Playbook: Popular_URL_Reputation_Services
Created: 15 minutes ago

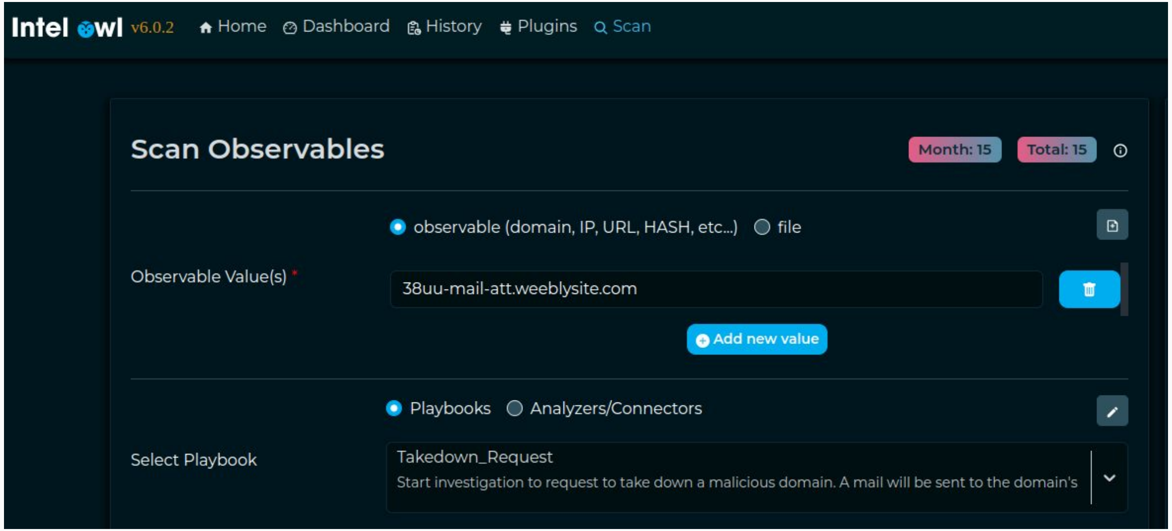
IntelOwl: Use Cases

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?



Scan Observables

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

Observable Value(s) *: 38uu-mail-att.weeblysite.com

● Playbooks ○ Analyzers/Connectors

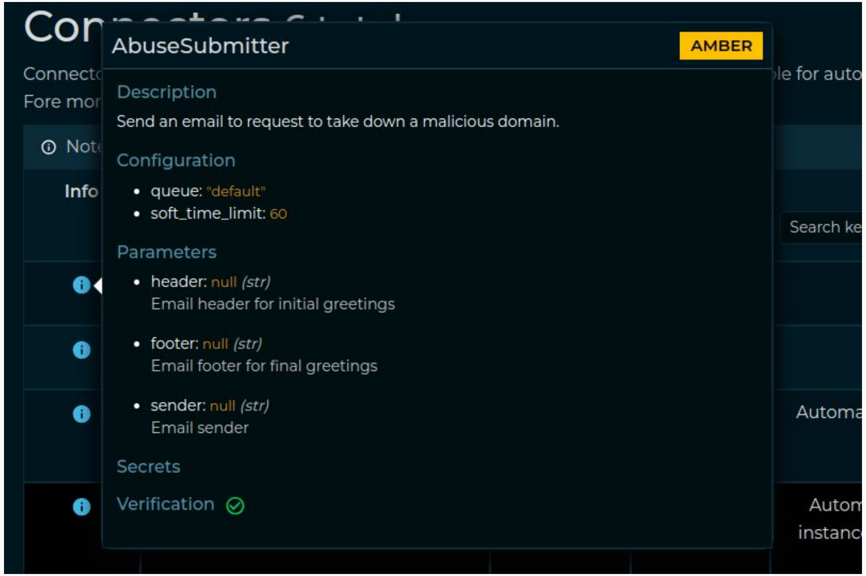
Select Playbook: Takedown_Request
Start investigation to request to take down a malicious domain. A mail will be sent to the domain's

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.



AbuseSubmitter AMBER

Description

Send an email to request to take down a malicious domain.

Configuration

- queue: "default"
- soft_time_limit: 60

Parameters

- header: null *(str)*
  Email header for initial greetings
- footer: null *(str)*
  Email footer for final greetings
- sender: null *(str)*
  Email sender

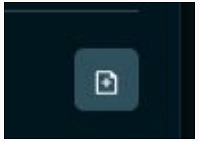
Secrets

Verification ✓

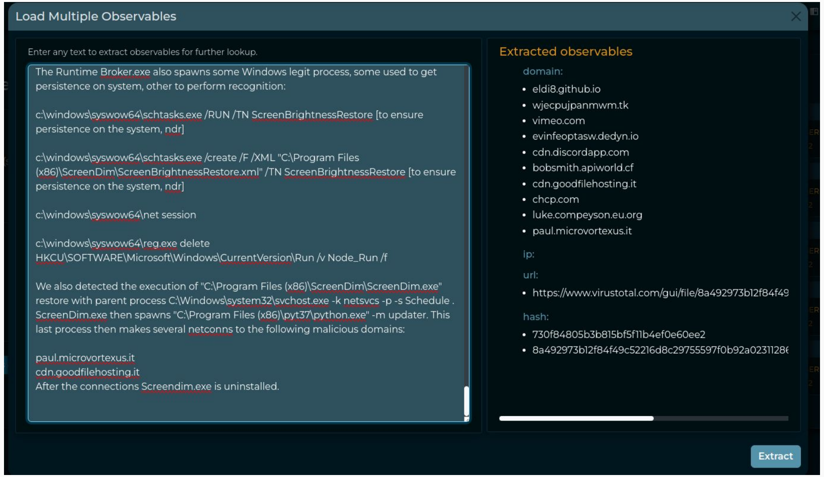
IntelOwl - Blog Post Analysis Use Case

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 /f

We also detected the execution of "C:\Program Files (x86)\ScreenDim\ScreenDim.exe"
restore with parent process C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule .
ScreenDim.exe then spawns "C:\Program Files (x86)\pyt37\python.exe" -m updater. This
last process then makes several netconns to the following malicious domains:

paul.microvortexus.it
cdn.goodfilehosting.it
After the connections Screendim.exe is uninstalled.
```

Extracted observables

domain:

- eldi8.github.io
- wjecpujpanmwm.tk
- vimeo.com
- evinfeoptasw.dedyn.io
- cdn.discordapp.com
- bobsmith.apiworld.cf
- cdn.goodfilehosting.it
- chcp.com
- luke.compeyson.eu.org
- paul.microvortexus.it

ip:

url:

- https://www.virustotal.com/gui/file/8a492973b12f84f49

hash:

- 730f84805b3b815bf5f11b4ef0e60ee2
- 8a492973b12f84f49c52216d8c29755597f0b92a0231128

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:

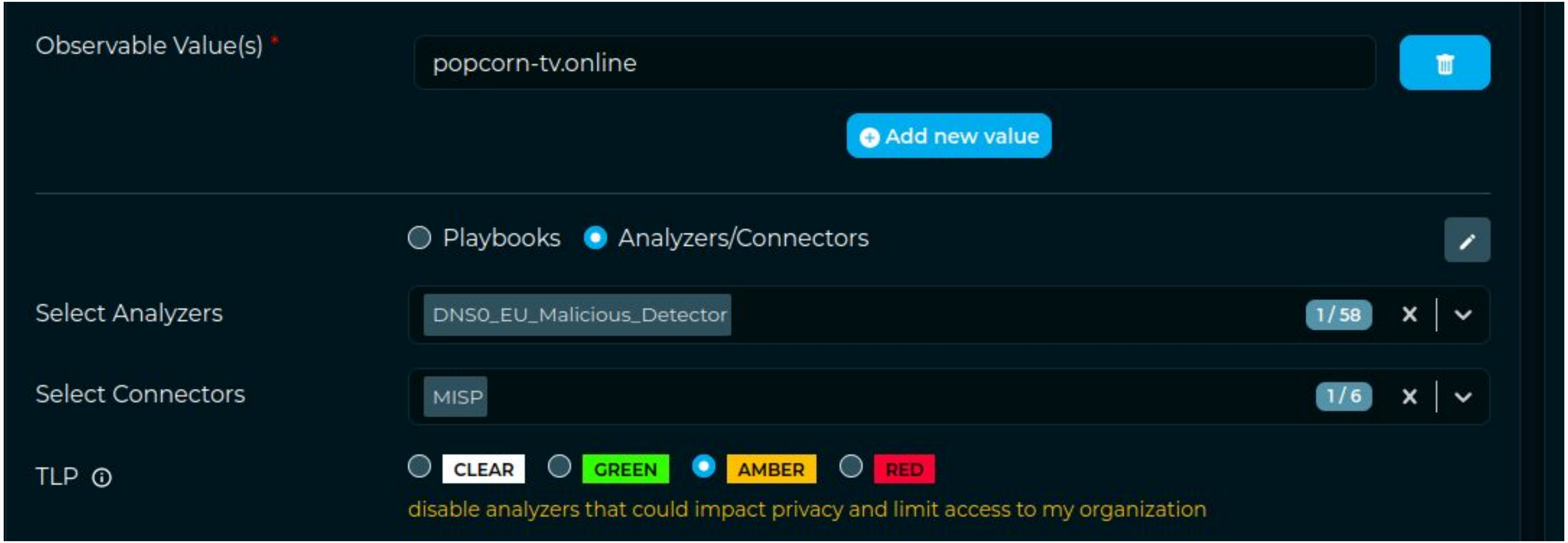
- Download and Install a Dockerized MISP Instance from this [Github repo]
- Follow the instructions in the repo to start a new MISP instance in a fast way. Remember to change the docker-compose file to host the service into a different port than 80 that is already used by IntelOwl
- Generate an API key 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?



Observable Value(s) *: popcorn-tv.online

○ Playbooks ● Analyzers/Connectors

Select Analyzers: DNS0_EU_Malicious_Detector 1/58

Select Connectors: MISP 1/6

TLP: ○ CLEAR ○ GREEN ● AMBER ○ RED

disable analyzers that could impact privacy and limit access to my organization

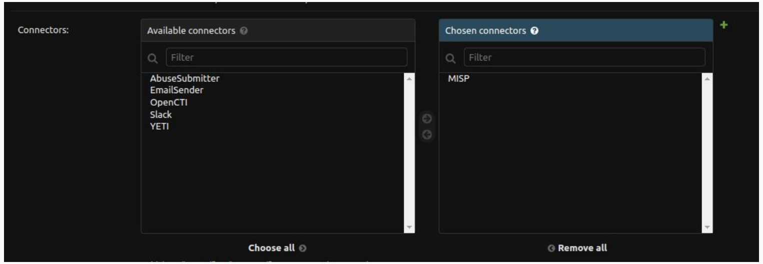
IntelOwl - MISP Export Use Case (EXTRA)

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!


Connectors:

Available connectors: AbuseSubmitter, EmailSender, OpenCTI, Slack, YETI

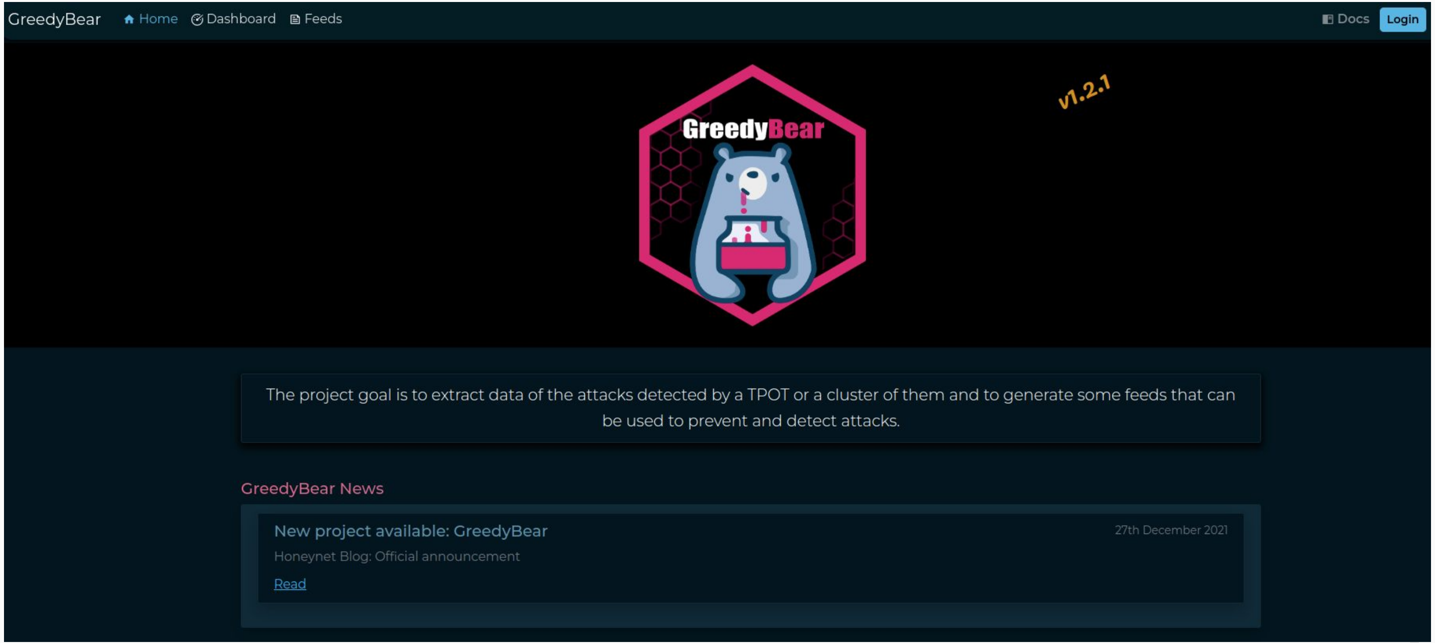
Chosen connectors: MISP

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!



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.

GreedyBear News

New project available: GreedyBear

27th December 2021

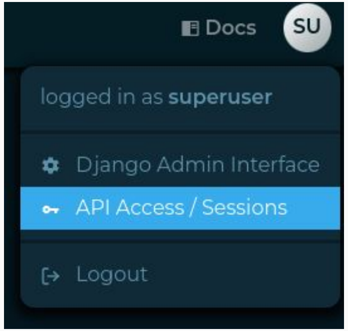
Honeynet Blog: Official announcement

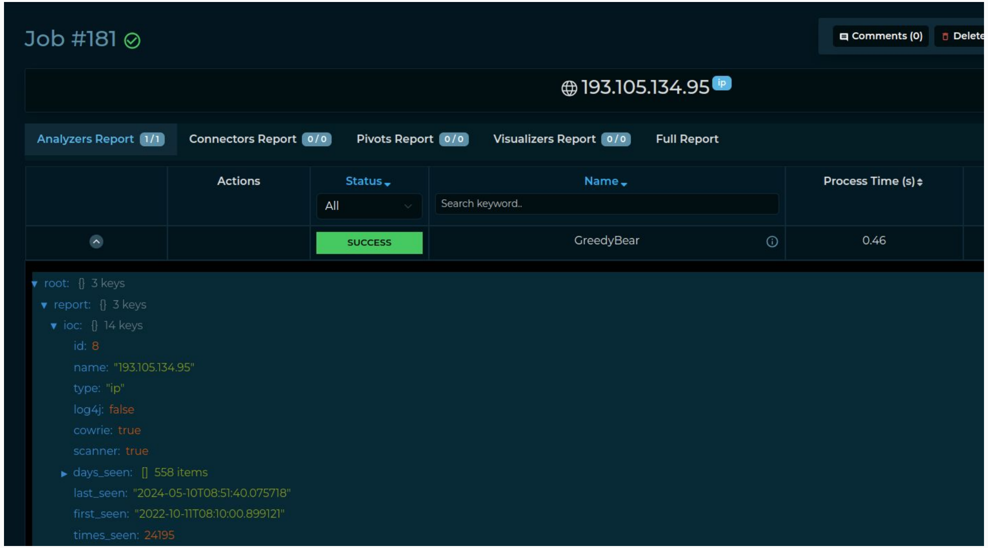
Read

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

193.105.134.95 ip

	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: "2024-05-10T08:51:40.075718"
        first_seen: "2022-10-11T08:10:00.899121"
        times_seen: 24195
```

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:

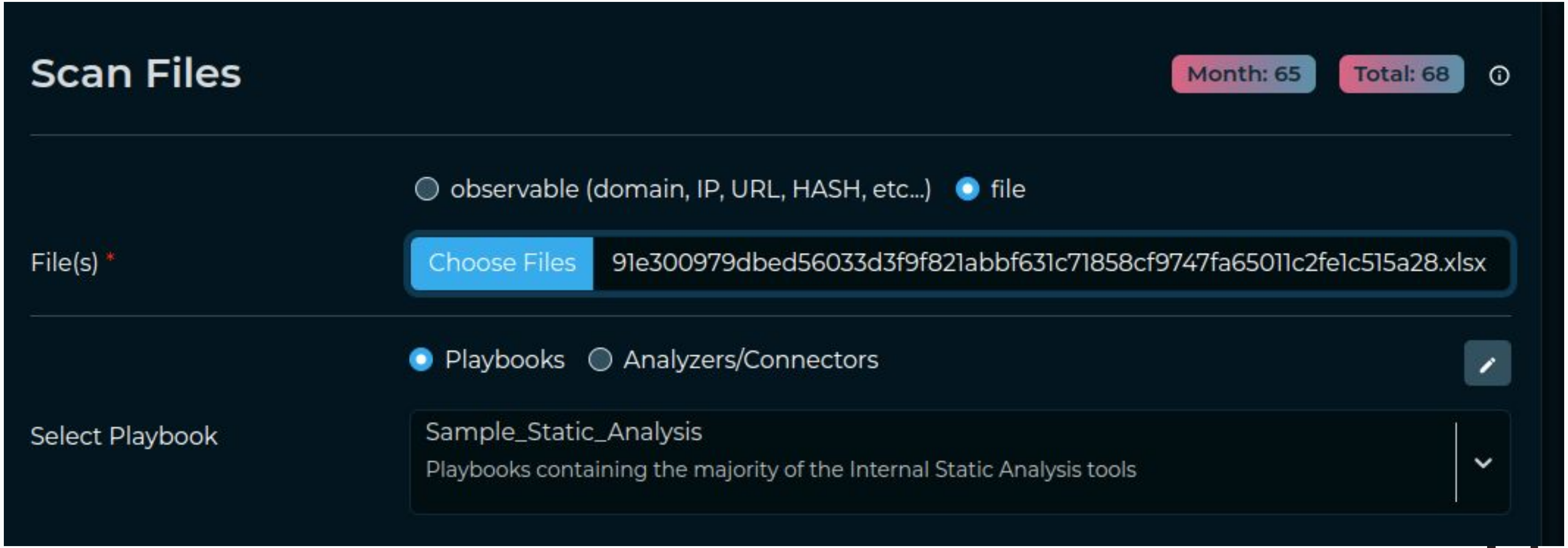
```
./start prod down && ./start prod up --malware_tools_analyzers
```

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?



Scan Files

Month: 65 Total: 68

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

File(s) *: Choose Files 91e300979dbed56033d3f9f821abbf631c71858cf9747fa65011c2fe1c515a28.xlsx

● Playbooks ○ Analyzers/Connectors

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

IntelOwl File Analysis - Static Analysis Exercise

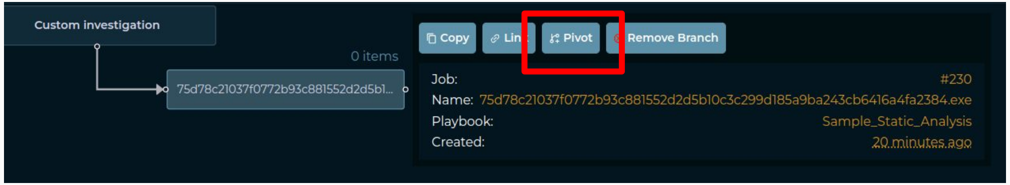
- IT’S YOUR TIME TO TRY:
- Use the *Sample_Static_Analysis* Playbook to analyze different type of files to explore all the static analyzers available in IntelOwl.
  - OneNote file
  - PDF file
  - Javascript file
  - APK file
  - Portable Executable file
- Find some “evidence” of maliciousness for each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

IntelOwl File Analysis - EXE

IT’S YOUR TIME TO TRY:

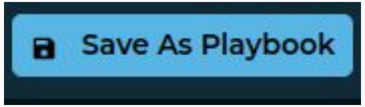
Let’s get a second opinion with online services. Pick the ones that you like the most. Some suggestions are VirusTotal, Intezer, FileScan, Triage, HybridAnalysis, MWDB, etc. Then:

- 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.



Job: #230
Name: 75d78c21037f0772b93c881552d2d5b10c3c299d185a9ba243cb6416a4fa2384.exe
Playbook: Sample_Static_Analysis
Created: 20 minutes ago

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



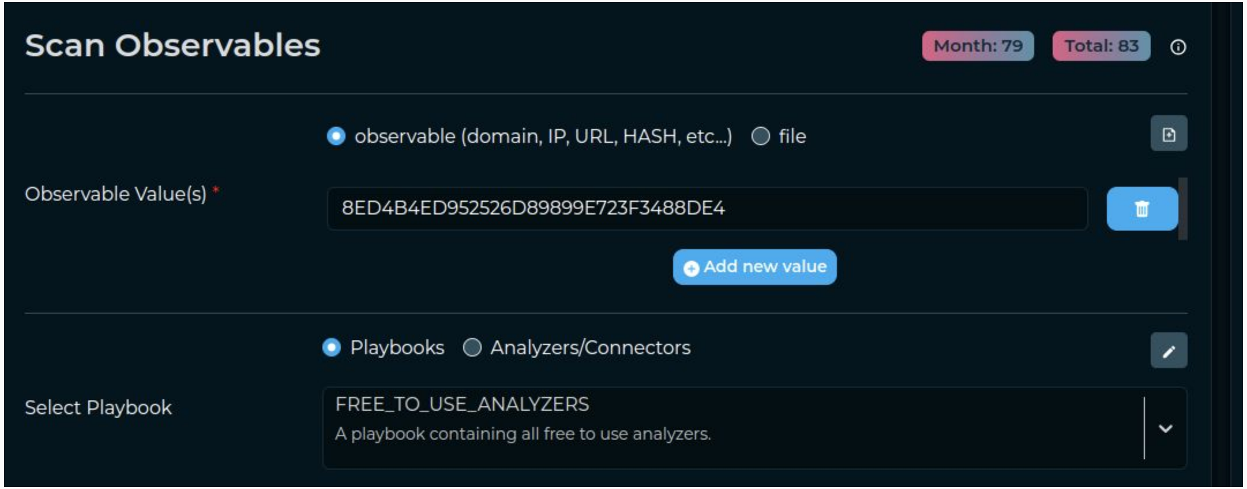
- Use the 2 Playbooks (static and dynamic analysis) in a chain again to associate another sample of AgentTesla to the same Investigation. We’ll try with this one.

IntelOwl File Analysis - 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?



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.

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.

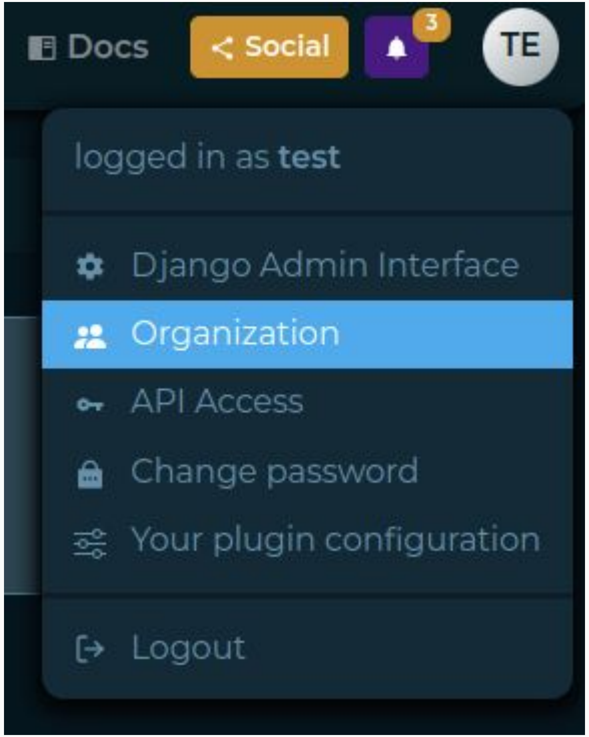
See the docs for more info about it.

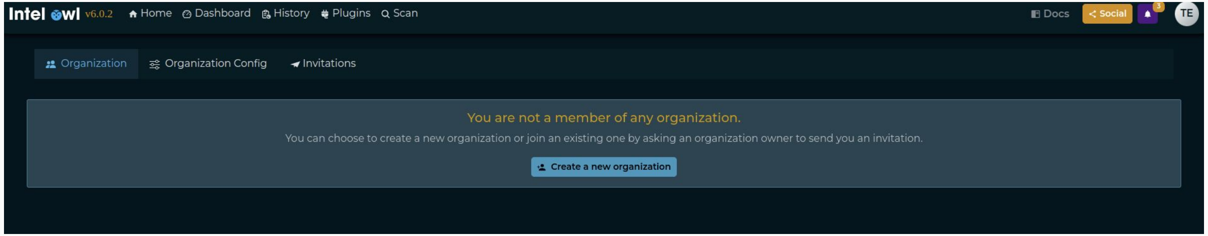
IT’S YOUR TIME TO TRY:

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

IntelOwl: Organizations

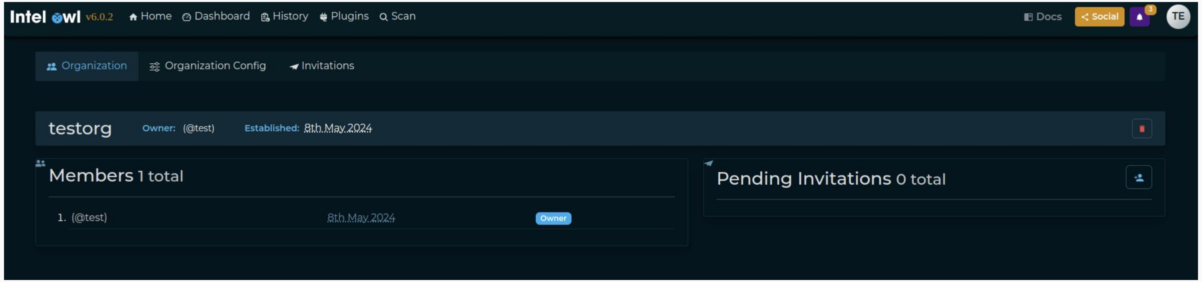
IntelOwl Organizations: Create a new organization





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.



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

Members 1 total

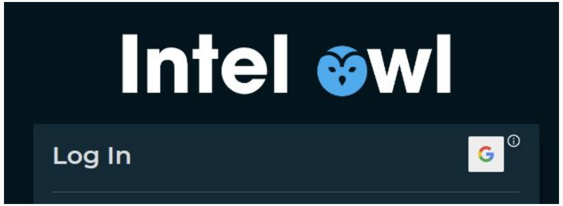
1. (@test) 8th May 2024 Owner

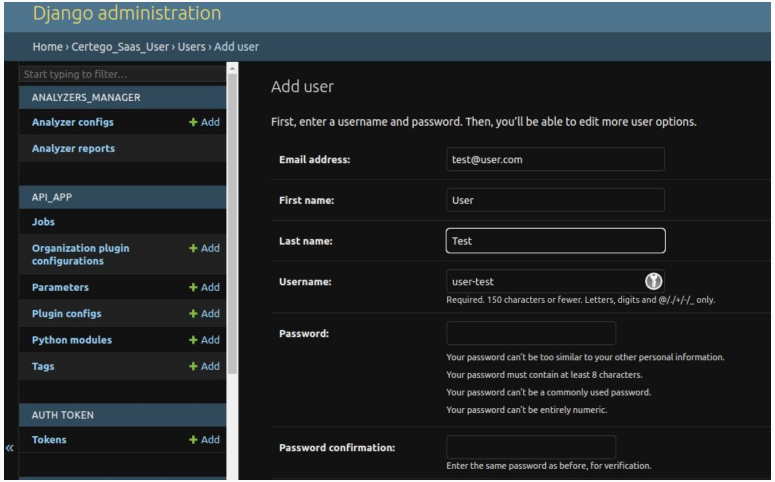
Pending Invitations 0 total

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




Django administration

Home › Certego_Saas_User › Users › Add user

Start typing to filter...

ANALYZERS_MANAGER

- Analyzer configs + Add
- Analyzer reports

API_APP

- Jobs
- Organization plugin configurations + Add
- Parameters + Add
- Plugin configs + Add
- Python modules + Add
- Tags + Add

AUTH TOKEN

- Tokens + Add

Add user

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

Email address: test@user.com

First name: User

Last name: Test

Username: user-test

Required. 150 characters or fewer. Letters, digits and @/./+/-/_ only.

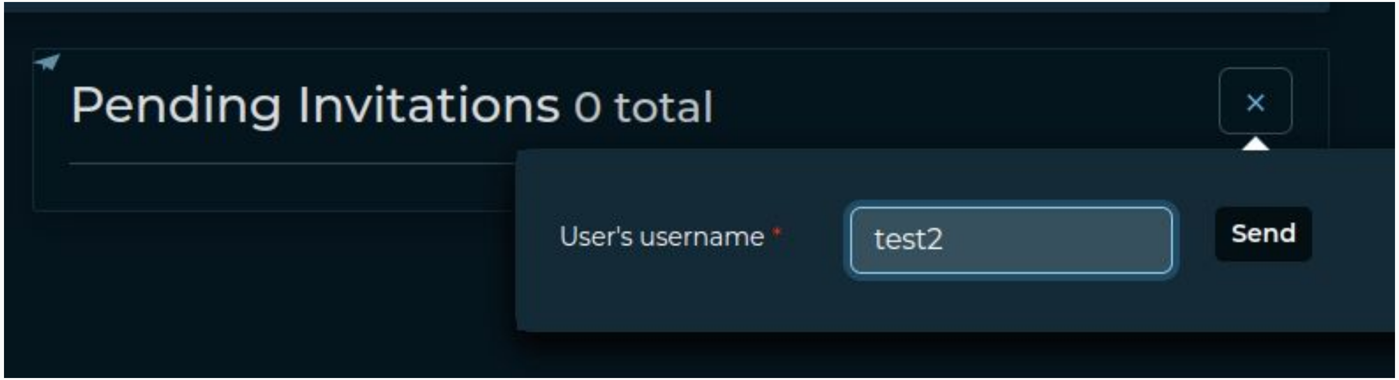
Password:

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.

Password confirmation:

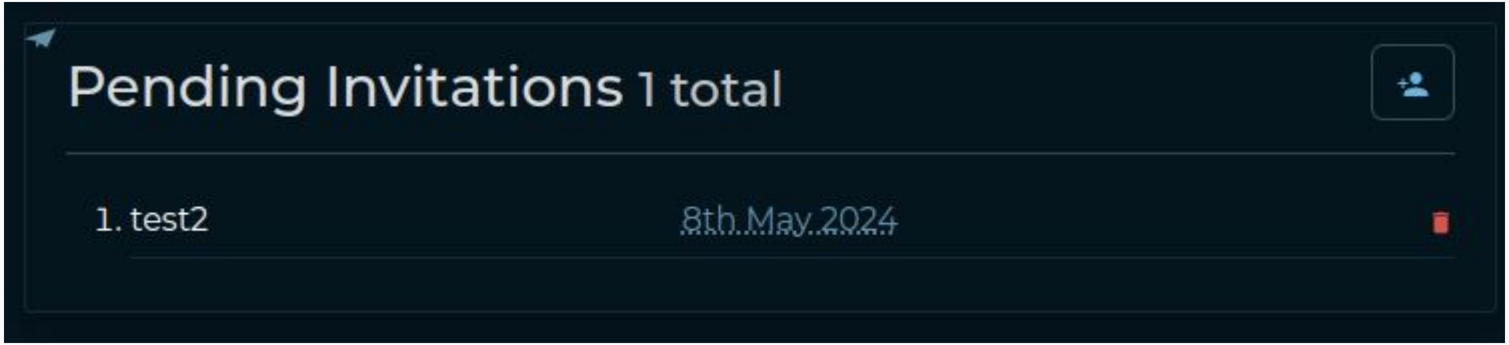
Enter the same password as before, for verification.

IntelOwl Organizations: Invite a new user



Pending Invitations 0 total

User's username * test2 Send

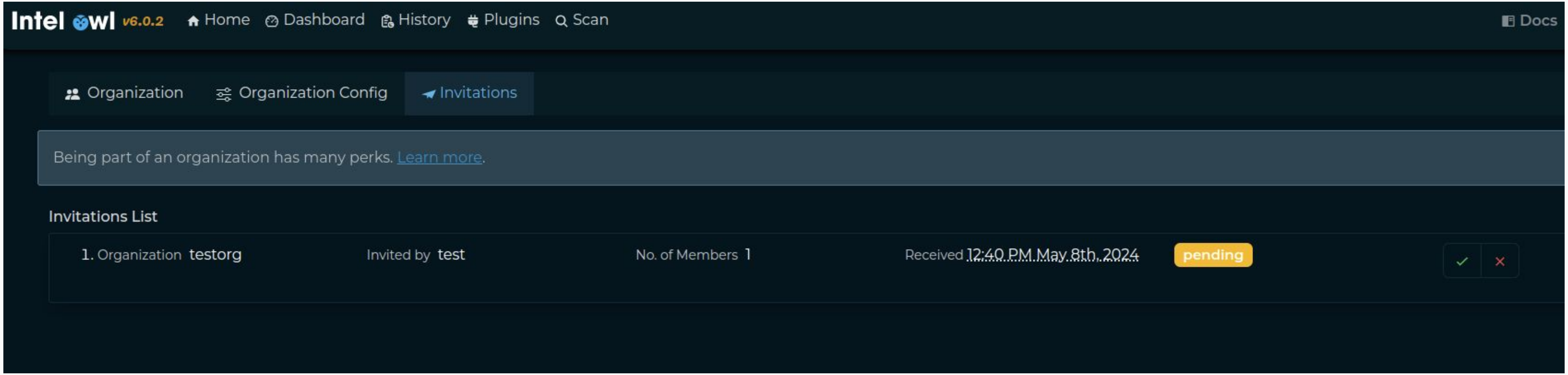


Pending Invitations 1 total

1. test2 8th May 2024

Intel Owl

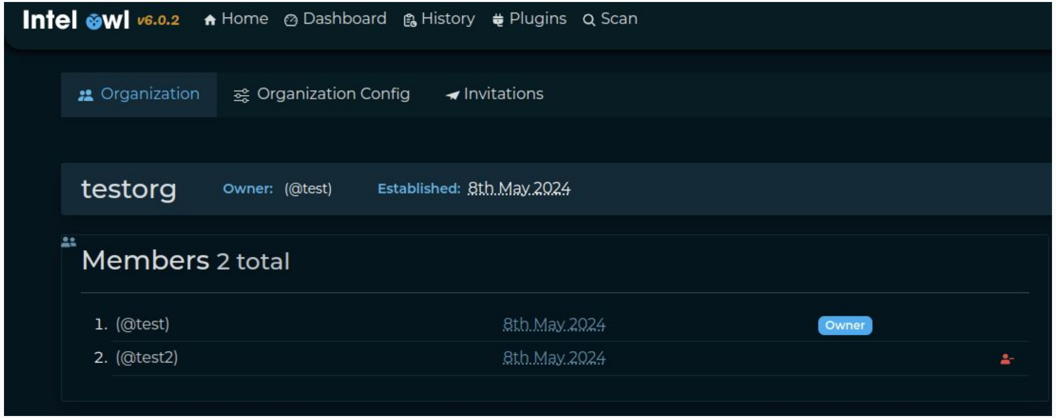
IntelOwl Organizations: New user accepts the invitation



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 ✓ ✕

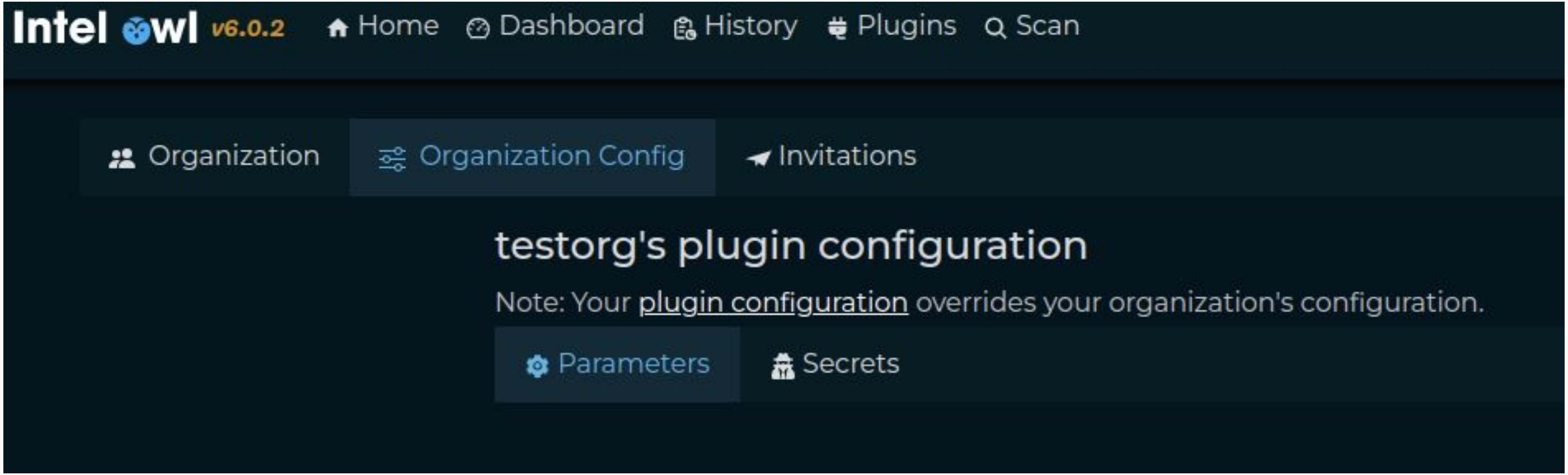


testorg Owner: (@test) Established: 8th May 2024

Members 2 total

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

IntelOwl Organizations: Organization Plugin configuration

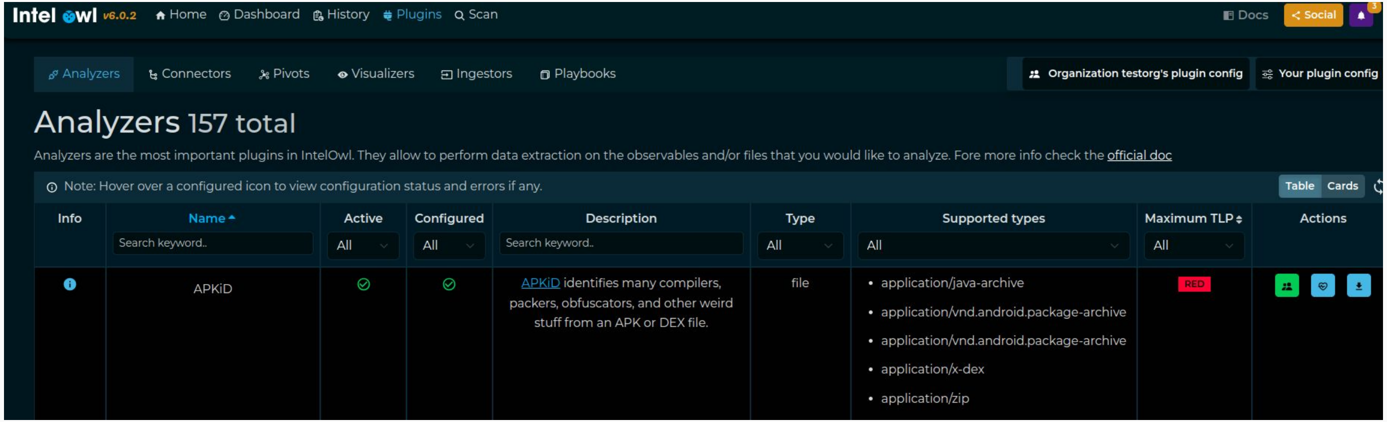


testorg's plugin configuration

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

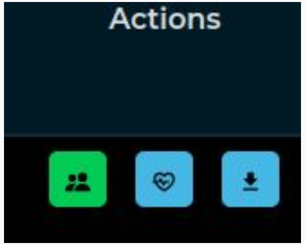


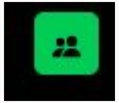
Analyzers 157 total

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. Fore 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
	Search keyword..	All	All	Search keyword..	All	All	All	
ⓘ	APKiD	✓	✓	APKiD identifies many compilers, packers, obfuscators, and other weird stuff from an APK or DEX file.	file	application/java-archive application/vnd.android.package-archive application/vnd.android.package-archive application/x-dex application/zip	RED	





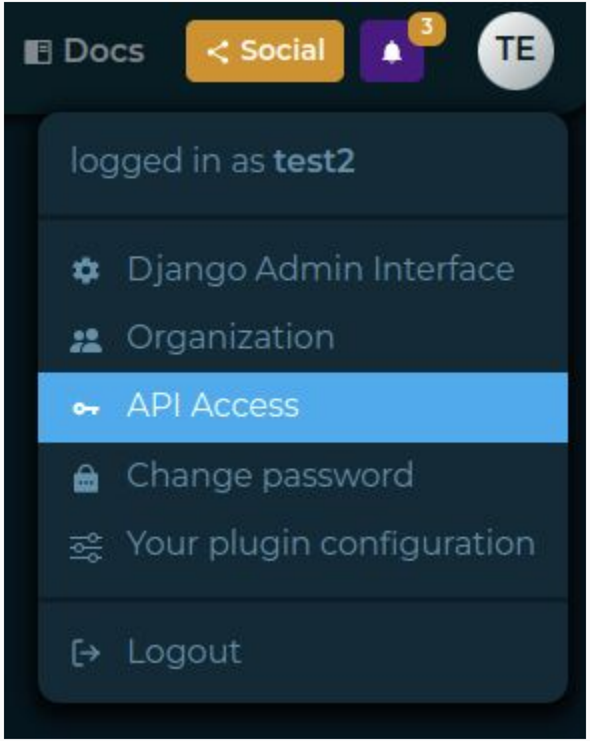
IntelOwl Organizations - Exercise

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

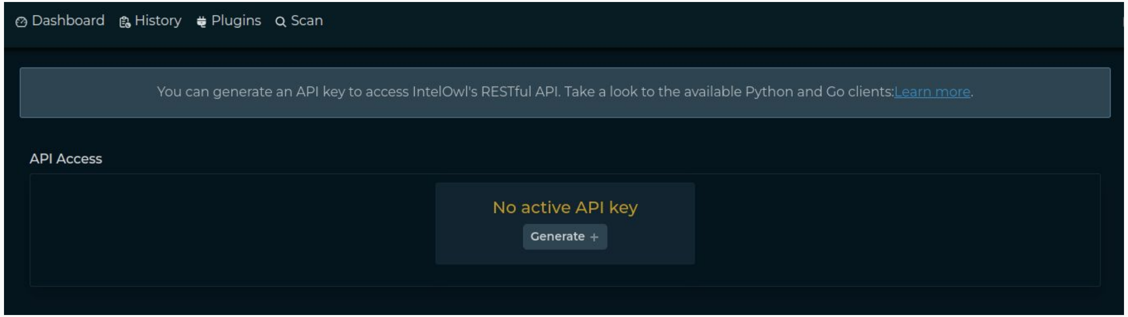
- Organizations
  - Create a new organization
  - Create a new user
  - Invite a new user
  - The new user accepts the invitation
  - Generate a secret for VirusTotal for your entire organization
  - Disable Capa_Info Plugin for your entire organization

IntelOwl: Integrations

IntelOwl Integrations: generate your API key



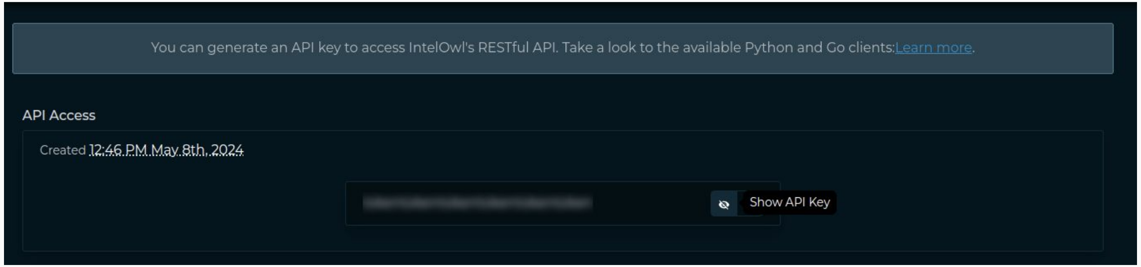
logged in as **test2**



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



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]

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)
```

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!

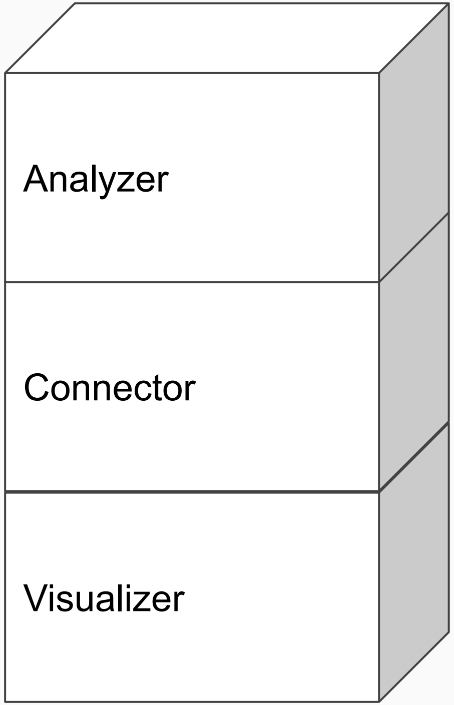
In this part of the workshop we want you to try to create new custom plugins.
We want this to be more interactive as possible. Please tell us your ideas and doubts and we'll guide you.

Schedule:

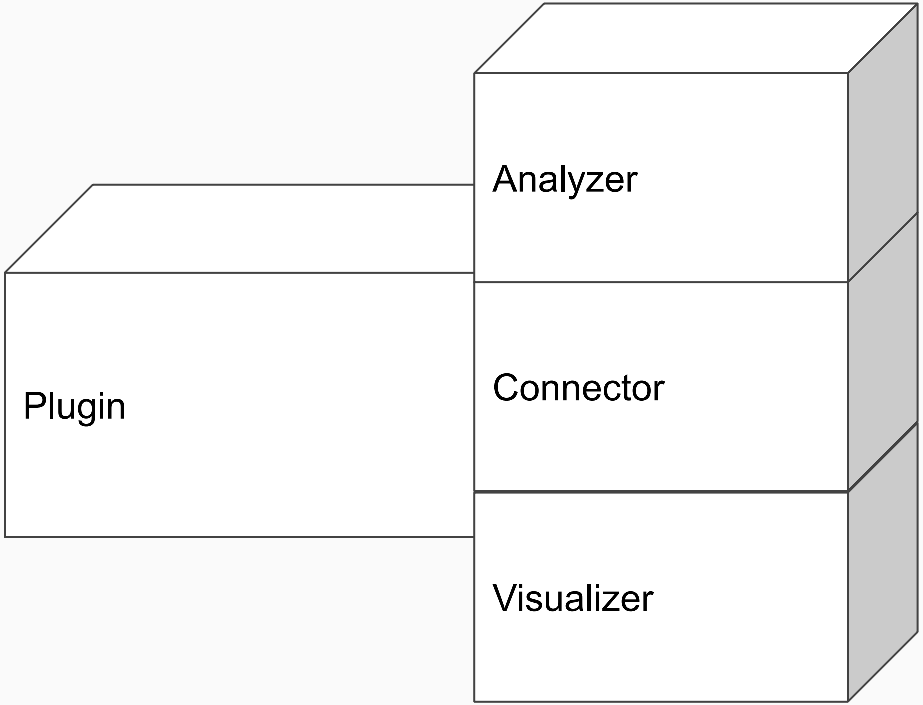
- First, we briefly explain the Plugin Framework and talk about the Software Architecture of IntelOwl
- Then, IT'S CHALLENGE TIME! Everyone choose which type of challenge they want:
  - If you have a specific use case in mind, tell us and we'll come to you to make a plan together of what can be done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

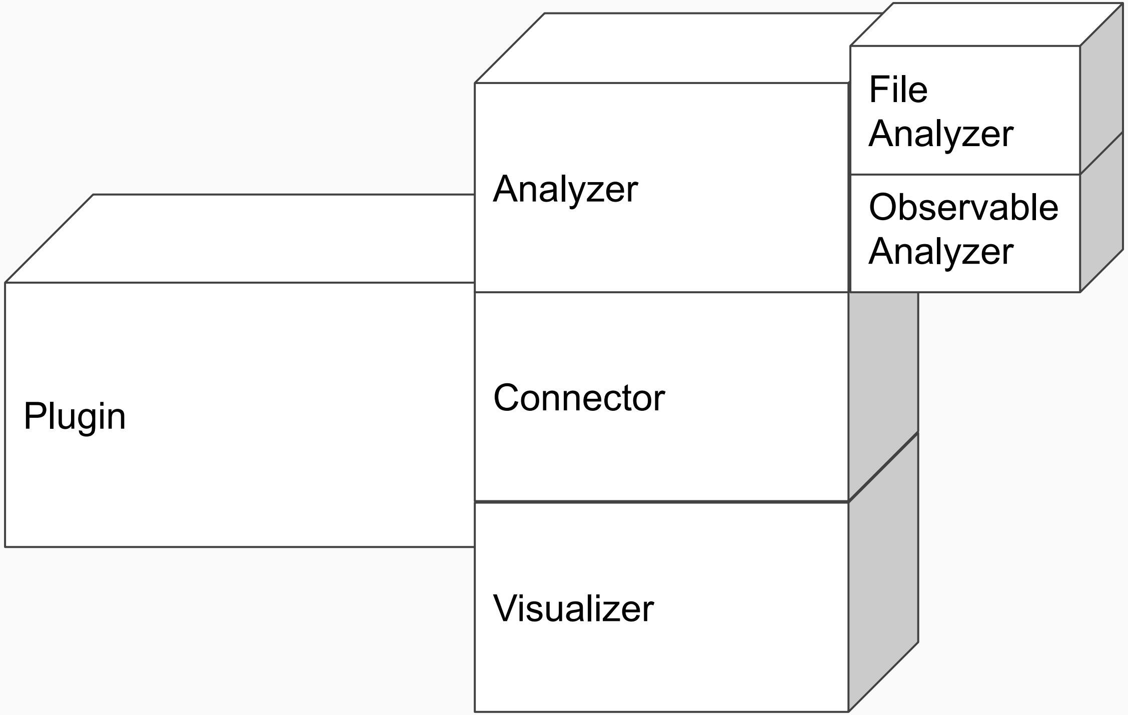
IntelOwl - Software Architecture



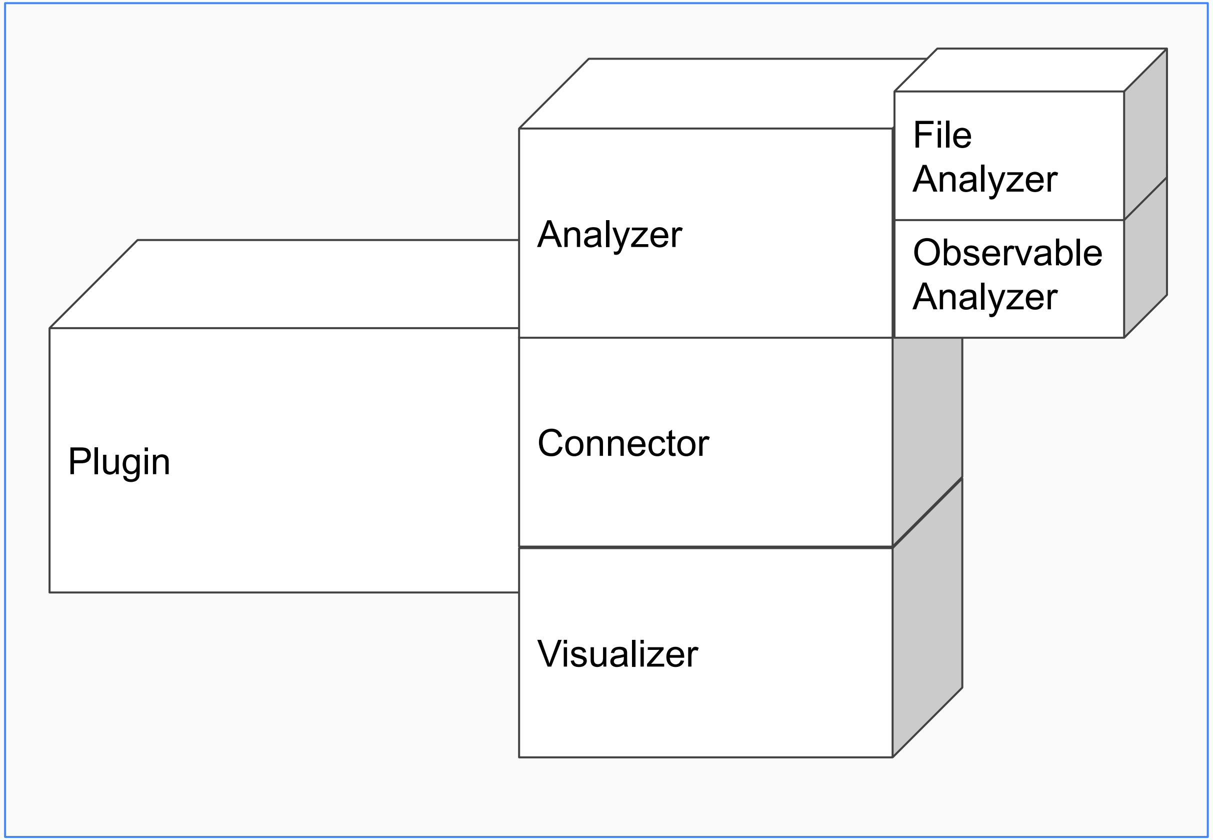
IntelOwl - Software Architecture



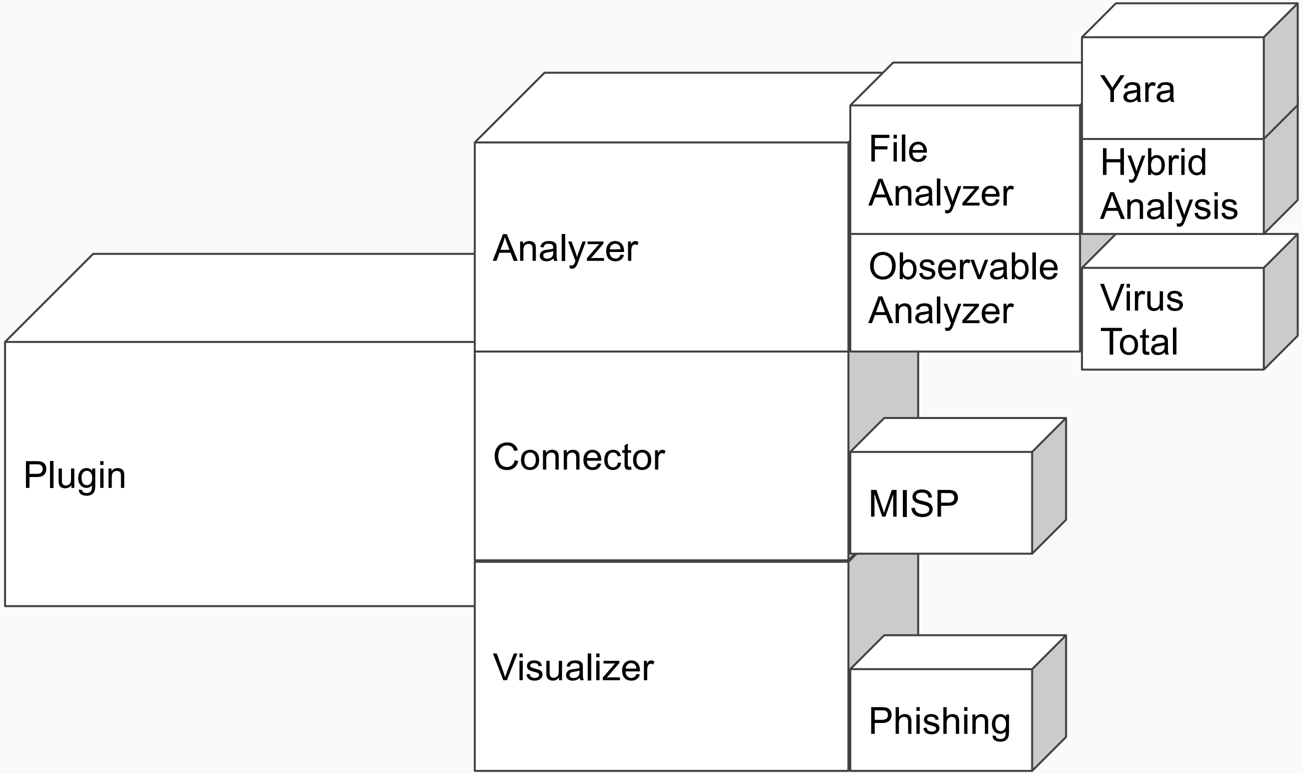
IntelOwl - Software Architecture



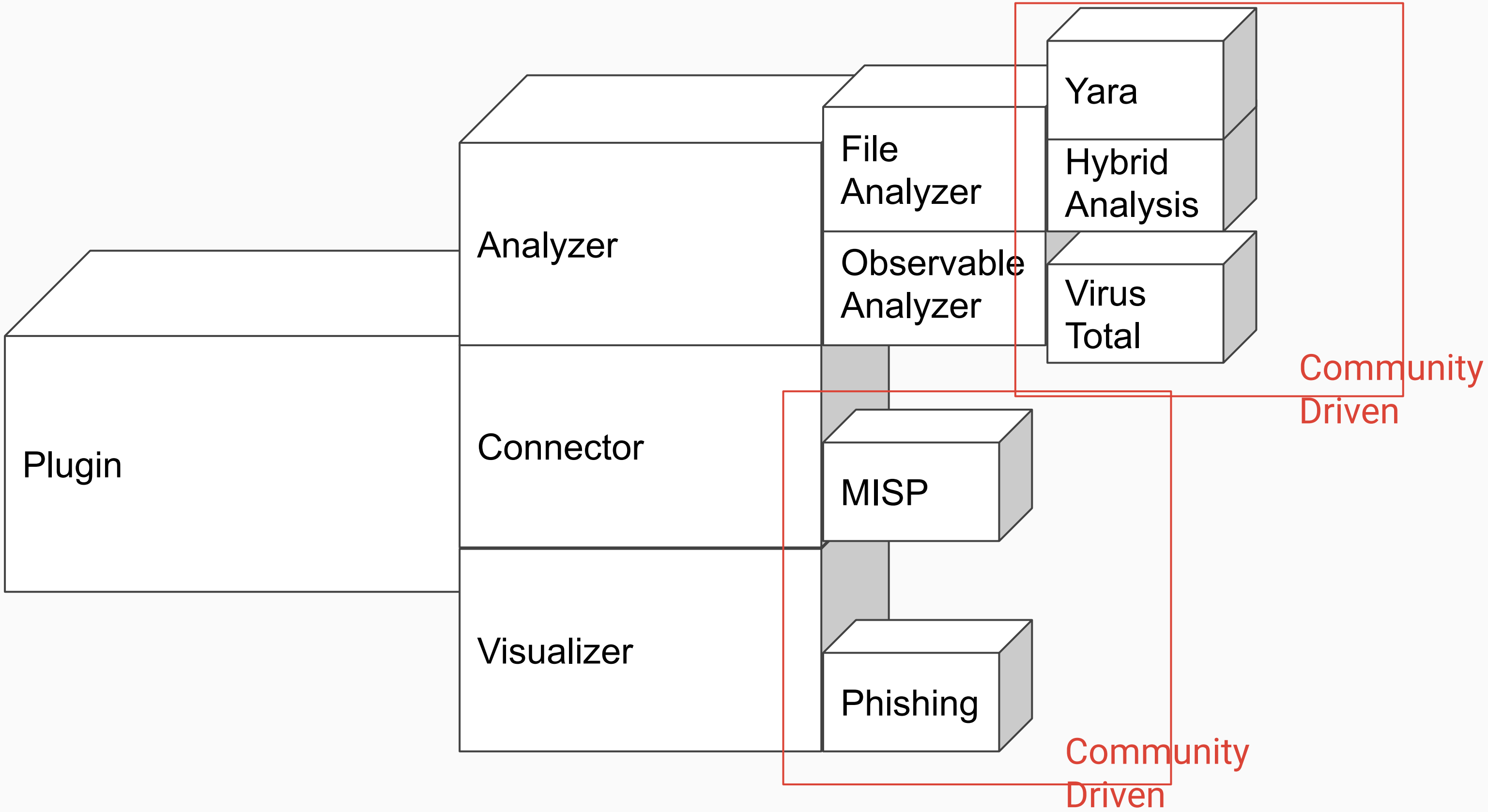
IntelOwl - Software Architecture



IntelOwl - Software Architecture



IntelOwl - Software Architecture



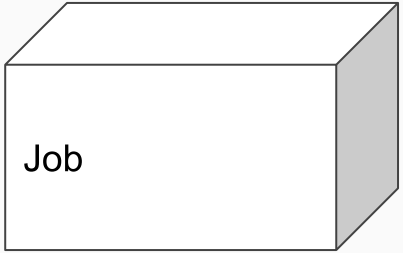
IntelOwl - Software Architecture

Plugin

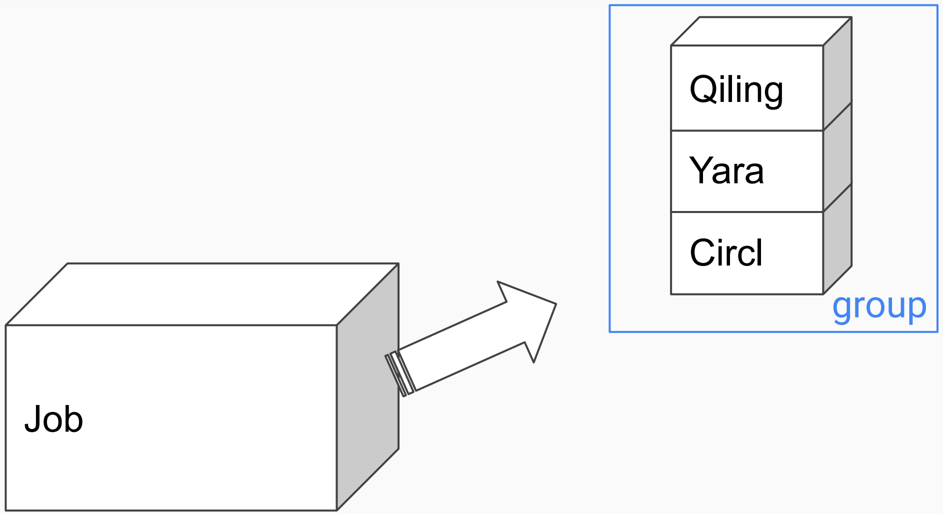
Community Driven

Driven

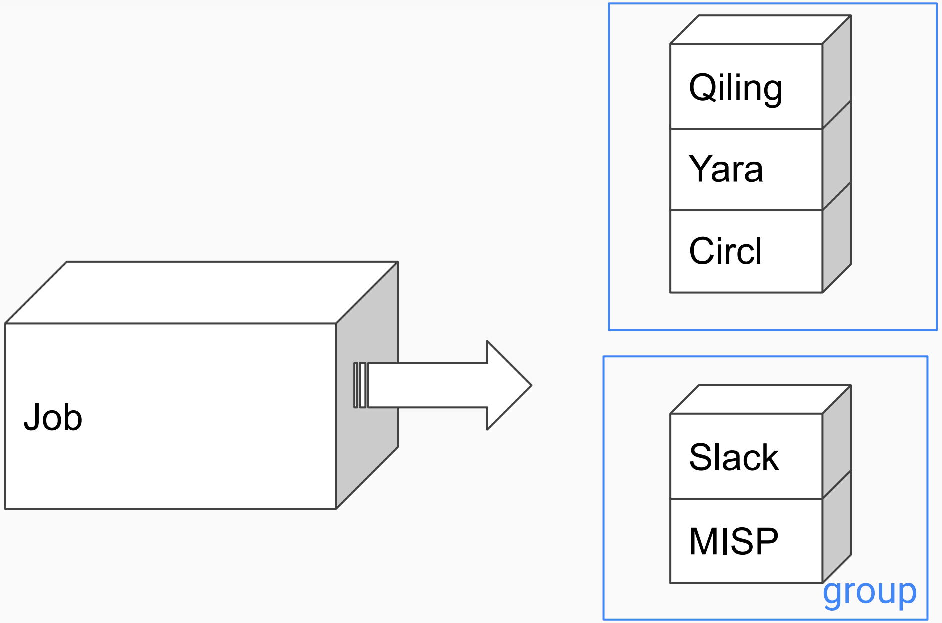
IntelOwl - Software Architecture



IntelOwl - Software Architecture

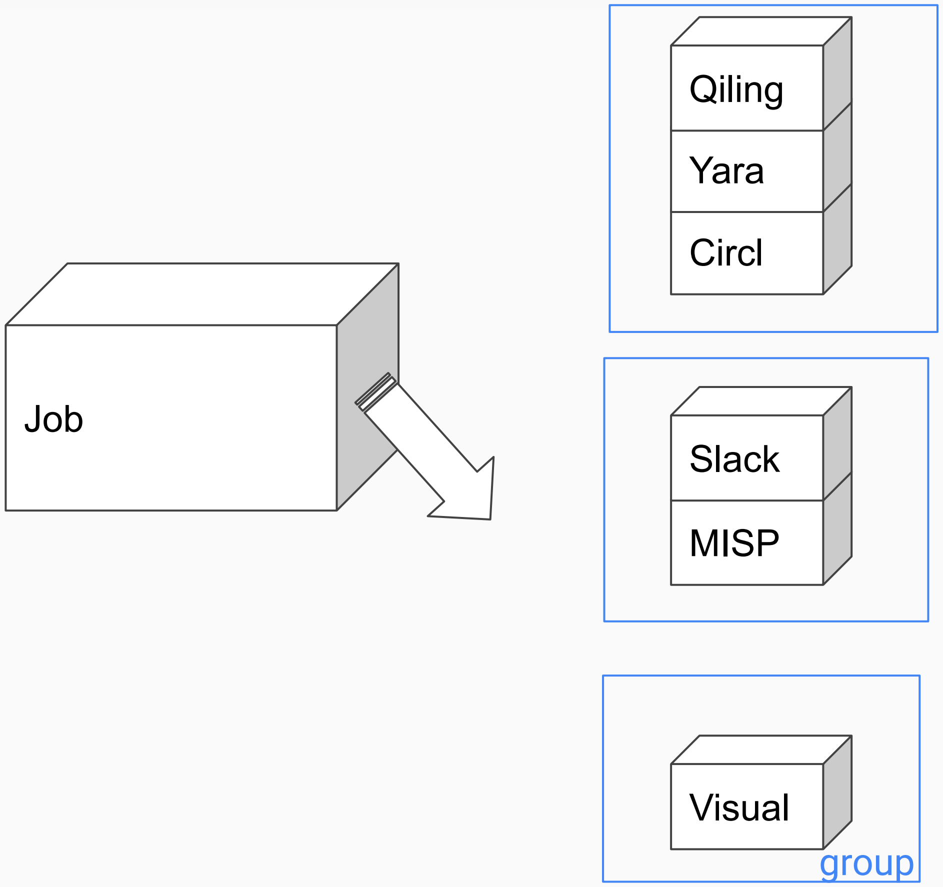


IntelOwl - Software Architecture

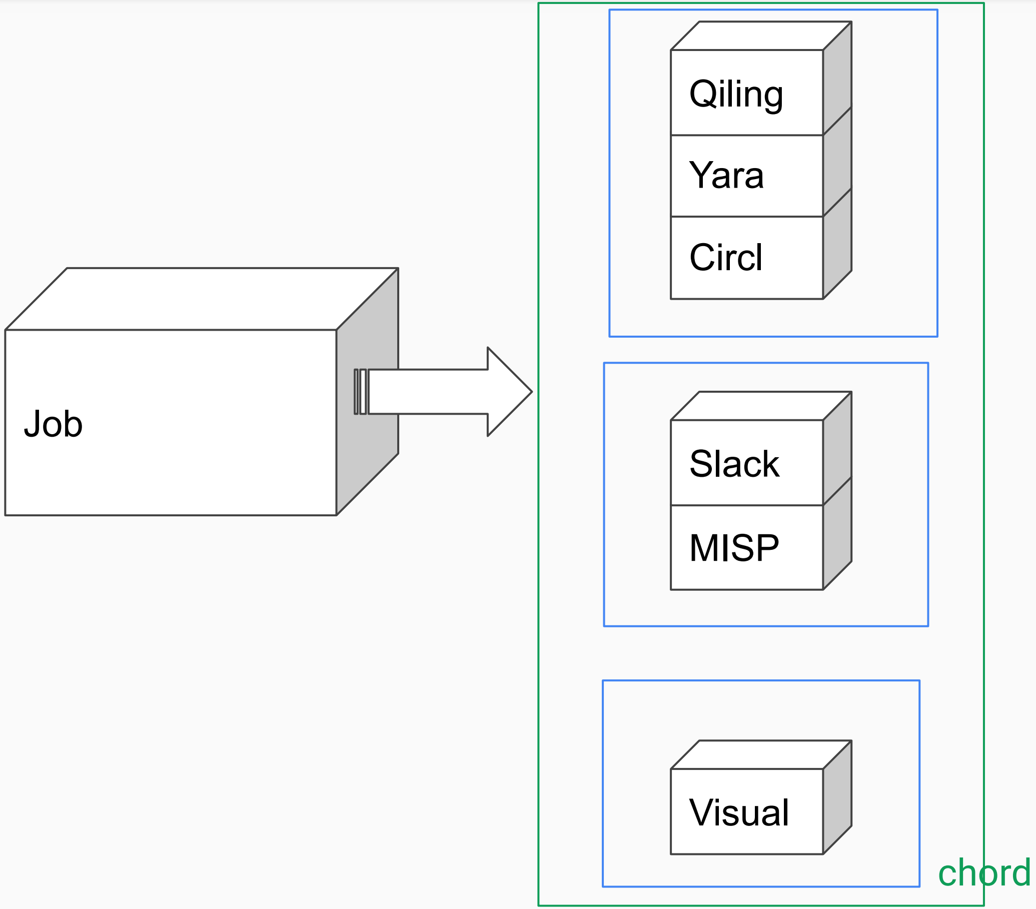


Intel Owl

IntelOwl - Software Architecture

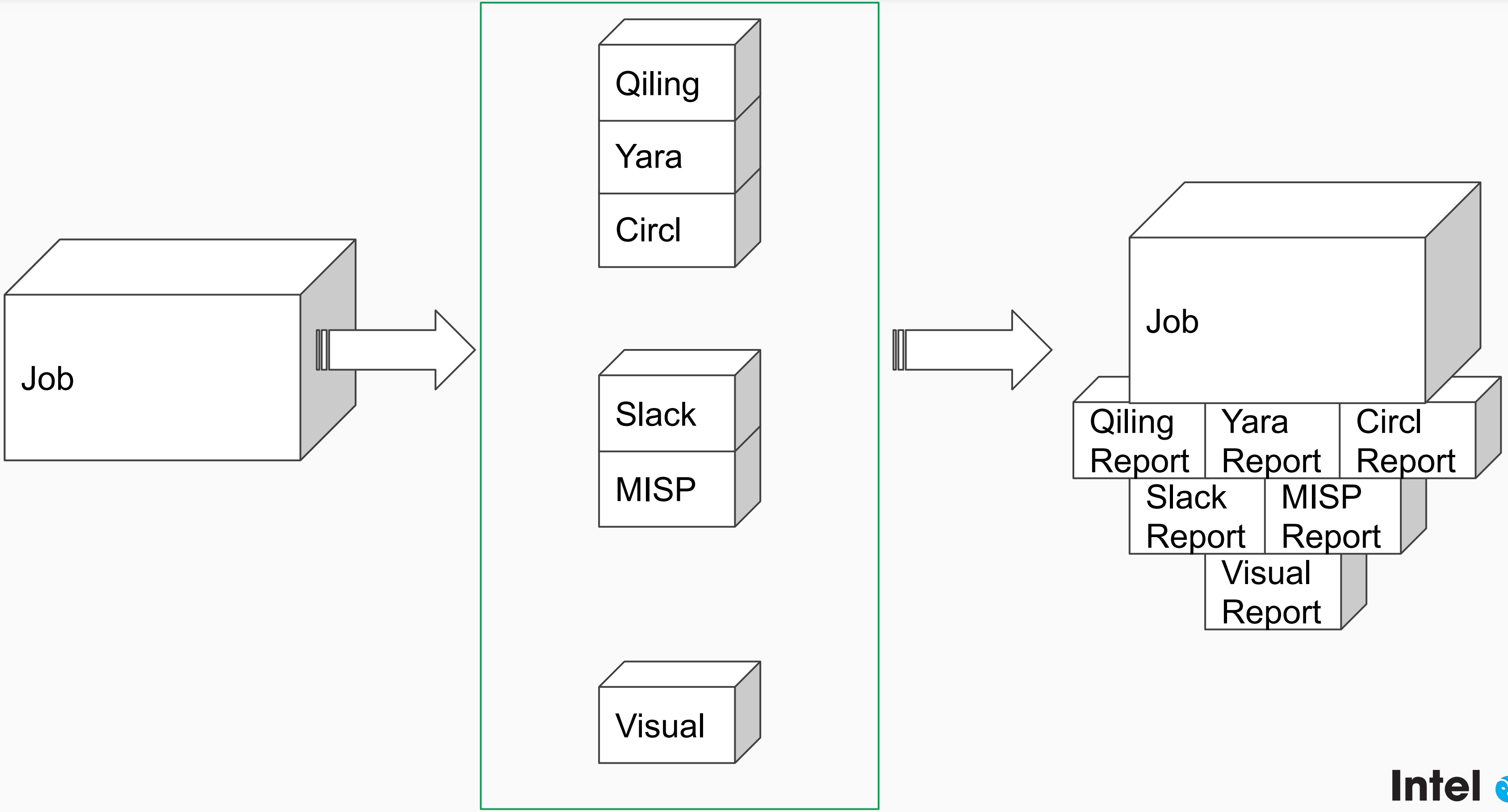


IntelOwl - Software Architecture



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!

𝕏 @intel_owl

intelowlproject/IntelOwl

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