



IntelOwl Project

Making the life of cyber security analysts easier



Daniele Rosetti

Administrator and frontend maintainer

drosetti 



Threat Intelligence Team

Cyber security analysts problem

Cyber security analysts are:

- understaffed
- overworked
- working 24/7

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](#)

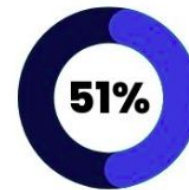
83% of IT Security Professionals Say Burnout Causes Data Breaches

September 20, 2023

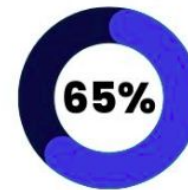
🕒 3 Min Read

ref: [DarkReading](#)

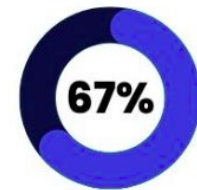
BY THE NUMBERS BURNOUT IN CYBERSECURITY



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](#)

Automate, automate, automate

- Overwhelmed by security alerts
- Stuck in repetitive and boring tasks
- Burnt-out myself

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

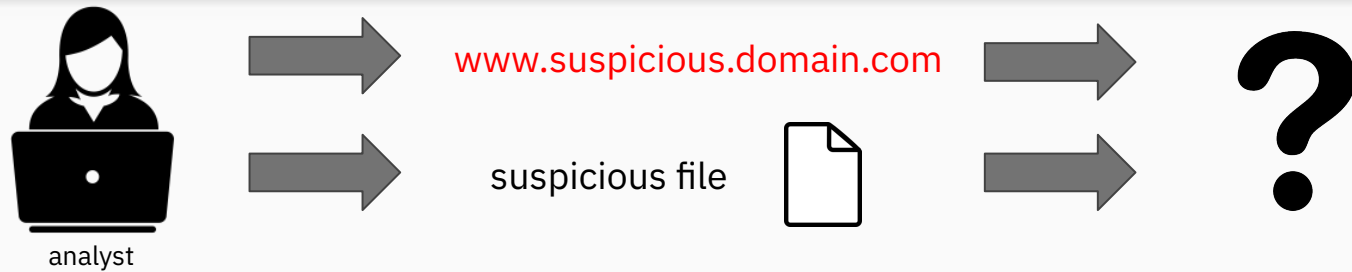


manual
work

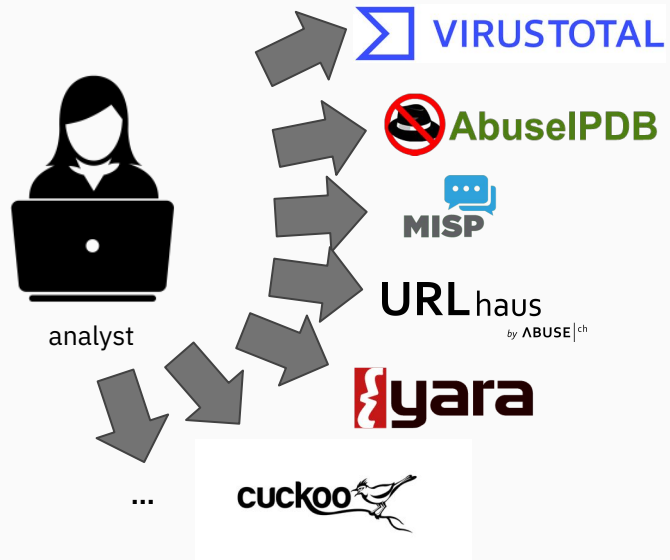
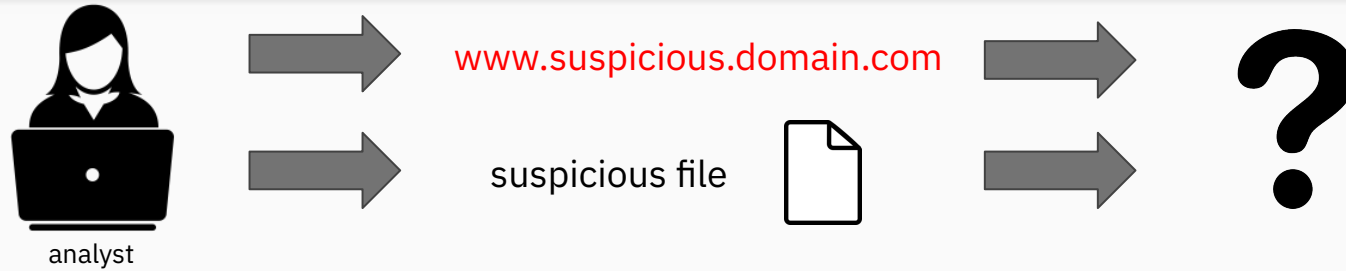


automation

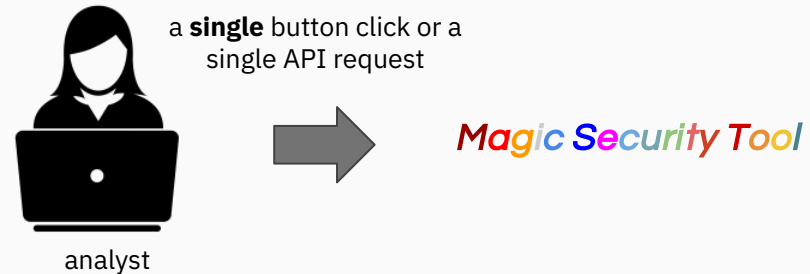
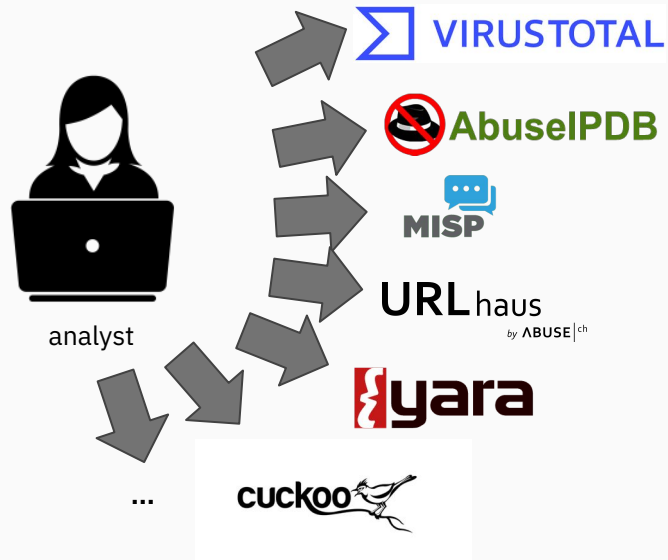
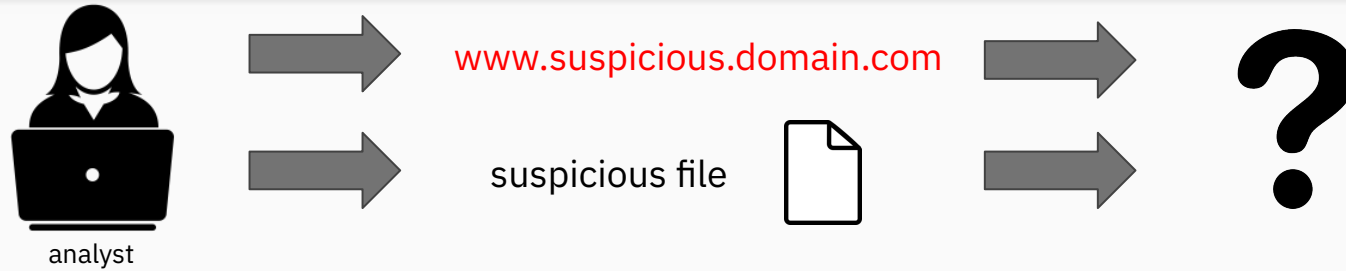
The bottleneck: acquisition of threat intelligence context



The bottleneck: acquisition of threat intelligence context



The bottleneck: acquisition of threat intelligence context



IntelOwl was born

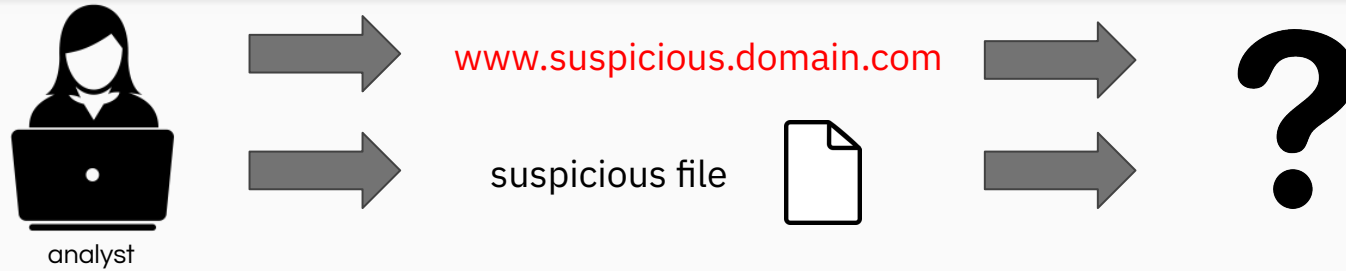


Intel owl

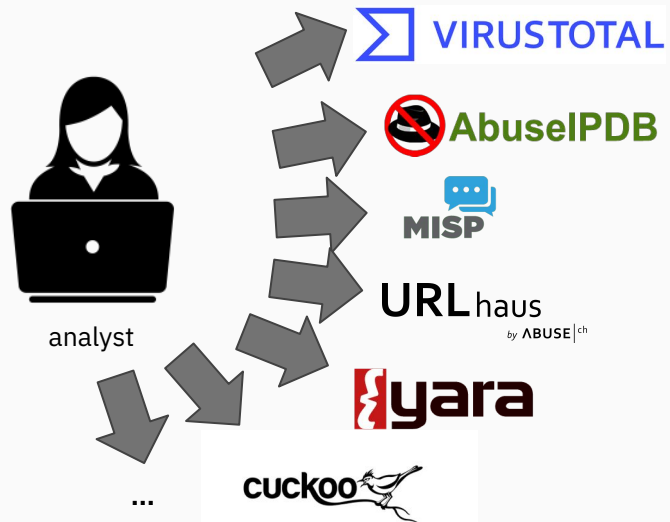
Born in Certego at the start of 2020, it is a great example of a successful Open Source project: right now it is one of the most popular Threat Intel projects on GitHub (>4k stars).

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

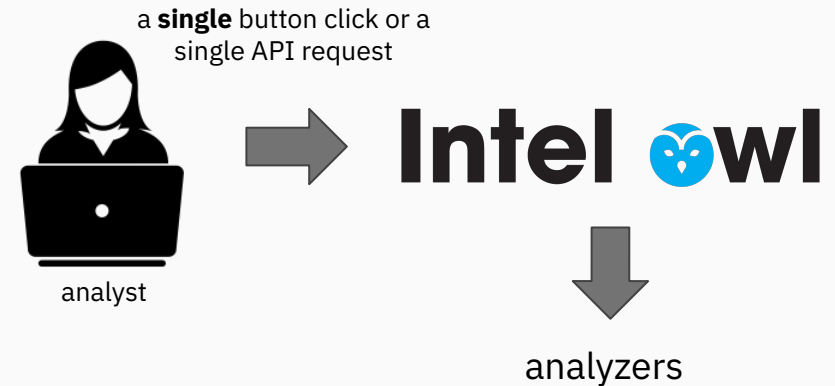
IntelOwl solution



Without Intel Owl



With Intel Owl



IntelOwl: Plugins

Intel Owl v6.4.0

Home Dashboard History Search Plugins Scan

Docs Social 3 AD

Analyzers

Connectors Pivots Visualizers Ingestors Playbooks

Create analyzer

Analyzers 205 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](#).

Name	Active	Description	Type	Supported types	Maximum TLP	Data model	Actions
AILTypoSquatting	✓	AILTypoSquatting is a Python library to generate list of potential typo squatting domains with domain name permutation engine to feed AIL and other systems.	observable	• domain	RED	()	
APK_Artifacts	✓	Artifacts is a tool that does APK strings analysis. Useful for first analysis.	file	• application/java-archive • application/vnd.android.package-archive • application/x-dex • application/zip	RED	()	
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	RED	()	

Plugins

Plugins are the core modular components of IntelOwl that can be easily added, changed and customized. The most important ones are the Analyzers that allow to perform data extraction on the observables and/or files that you would like to analyze.

1 2 3 4 5 ... »

archive

IntelOwl: How to use the platform



IntelOwl: Phishing verification

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

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

Those are all pre-built in the default installation.

IntelOwl: Scan

IntelOwl v6.4.0

[Home](#) [Dashboard](#) [History](#) [Search](#) [Plugins](#) [Scan](#)

[Docs](#) [Social](#)

3

AD

Scan Observables

Month: 0 Total: 0

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

Observable Value(s) *

google.com, 8.8.8.8, https://google.com, 1d5920f4b44b27a802bd77c4f0536f5

Add new value

☒ Playbooks ☐ Analyzers/Connectors

Select Playbook

Select...

TLP

☐ CLEAR ☒ GREEN ☐ AMBER ☐ RED

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

Advanced settings

Start Scan

Recent Scans

0 total

No recent scans available

IntelOwl: Phishing verification

IntelOwl v6.4.0

Home Dashboard History Search Plugins Scan

Docs Social 3 AD

Scan Observables

Month: 12 Total: 12

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

file

Observable Value(s) *

amazmoon.com

Add new value

Playbooks

Analyzers/Connectors

Select Playbook

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

TLP

CLEAR

GREEN

AMBER

RED

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

Advanced settings

Start Scan

Recent Scans

5 total

0-0lx-merchandise.554217.xyz

score: 6

Playbook: Popular_URL_Reputation_Services TLP: AMBER
Finished: 8 minutes ago User: admin

hamstercoin.lol

score: 6

Playbook: Popular_URL_Reputation_Services TLP: AMBER
Finished: 9 minutes ago User: admin

onsblogs.sbs

score: 6

Playbook: Popular_URL_Reputation_Services TLP: AMBER
Finished: 9 minutes ago User: admin

IntelOwl: Phishing verification

Intel OwlHomeDashboardHistorySearchPluginsScanDocsSocialAD

Job #45

Comments (0) Delete Rescan Save As Playbook Report

Similar Investigations: 1

Investigation: Custom investigation: 3 jobs

amazmoon.com domain

Analyzers Report 5/5

Connectors Report 0/0

Pivots Report 0/0

Visualizers Report 1/1

Full Report

Visualizer Raw

	Actions	Status	Name	Process Time (s)	Running Time
		All	Search keyword...		
		SUCCESS	VirusTotal_v3_Get_Observable	0.88	12:21:53 PM - 12:21:54 PM (GMT+2)
		SUCCESS	Tranco	1.7	12:21:53 PM - 12:21:55 PM (GMT+2)
		SUCCESS	Phishtank	0.69	12:21:53 PM - 12:21:54 PM (GMT+2)
		SUCCESS	PhishingArmy	0.09	12:21:53 PM - 12:21:53 PM (GMT+2)

```
1 {
2   "report": {
3     "link": "https://phishing.army/download/phishing_army_blocklist.txt",
4     "found": true
5   },
6   "data_model": null,
7   "errors": [],
8   "parameters": {}
9 }
```

IntelOwl: Phishing verification

IntelOwl v6.4.0 [Home](#) [Dashboard](#) [History](#) [Search](#) [Plugins](#) [Scan](#) [Docs](#) [Social](#) [AD](#)

Job #44

[Comments \(0\)](#) [Delete](#) [Rescan](#) [Save As Playbook](#) [Report](#)

Similar Investigations:
0

amazmoon.com [domain](#)

Reputation

VisualizerRaw

VirusTotal
Engine Hits: 12

Tranco Rank

Phishtank

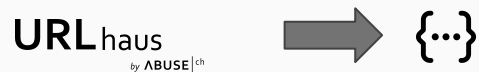
PhishingArmy
found

InQuest



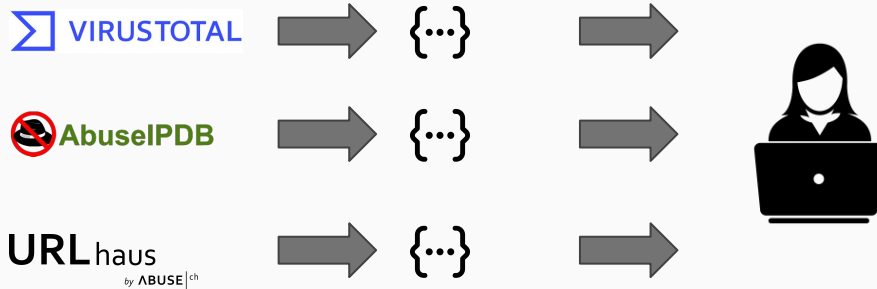
IntelOwl: Data Model

Each analyzer generates a JSON report with a different structure, keys and data.



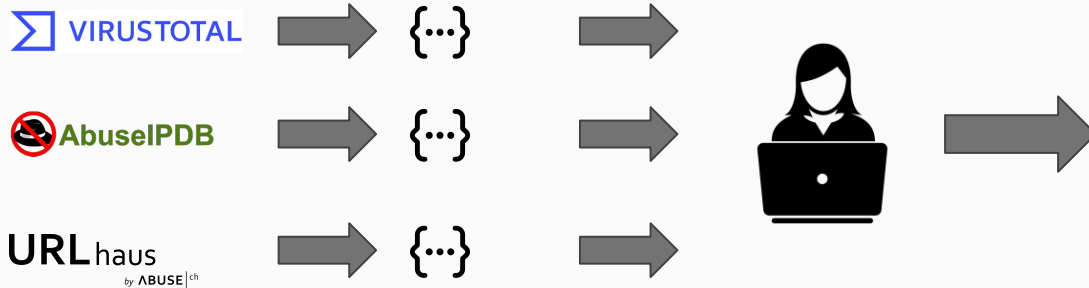
IntelOwl: Data Model

Users need to read them...



IntelOwl: Data Model

...And **understand** them



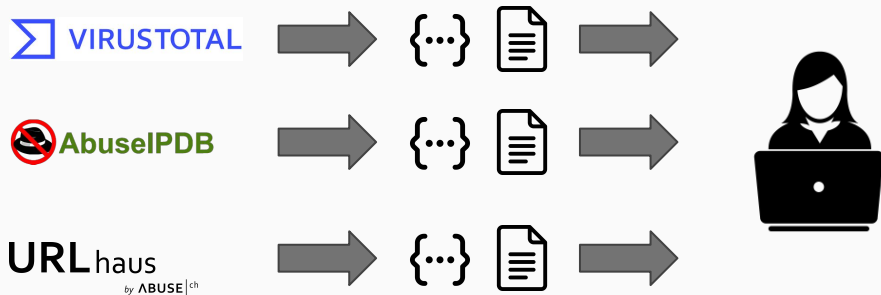
IntelOwl: Data Model

Data model allows analyzers to normalize the output.



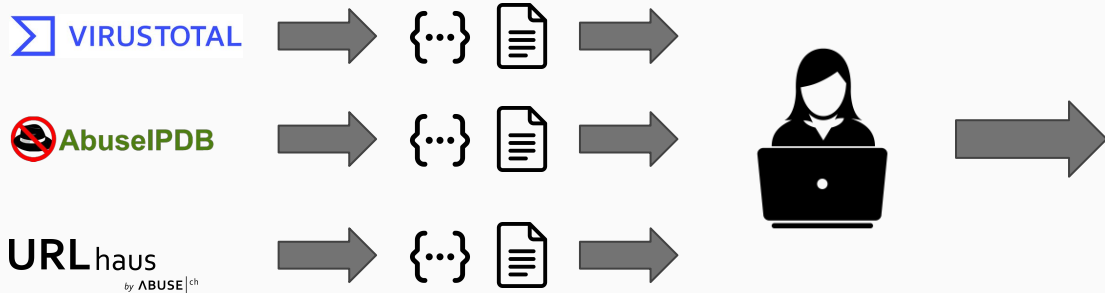
IntelOwl: Data Model

In this way the analyst just needs to understand the data model format.



IntelOwl: Data Model

In this way the life of security analysts is easier.



IntelOwl: User Events

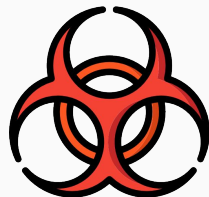
User events allow users to generate reports about analyzables.



Analyst

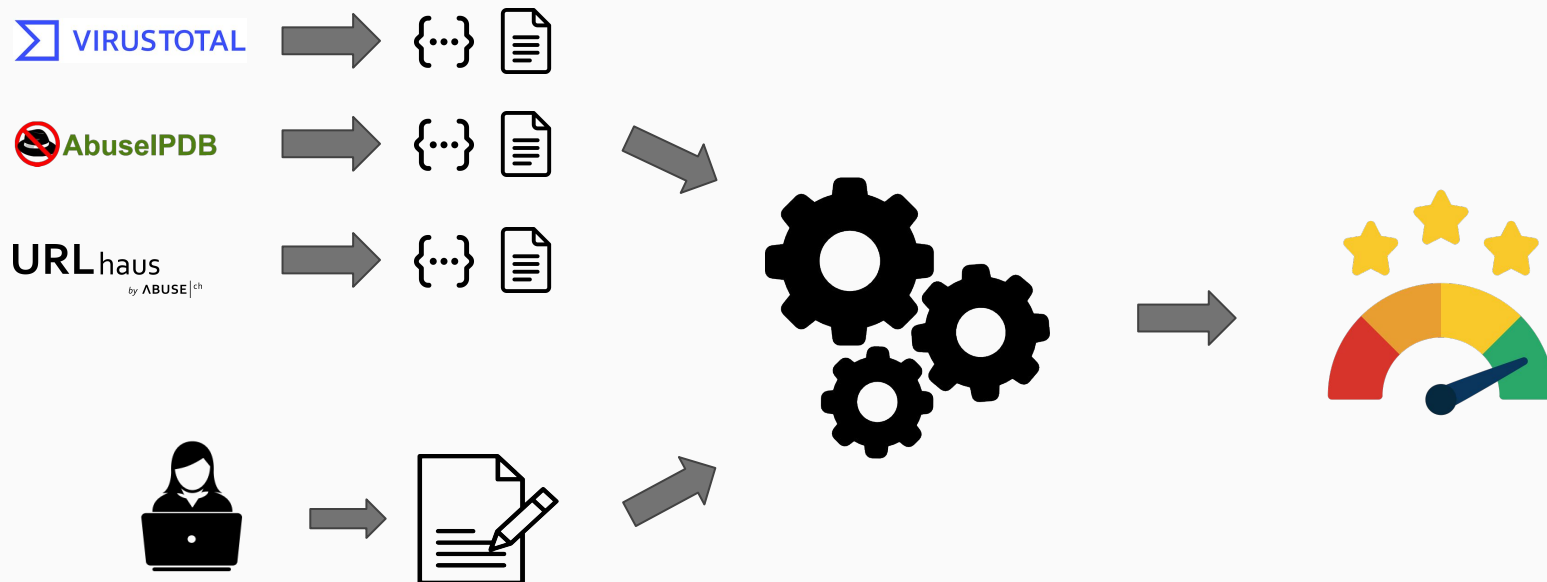


User
event



IntelOwl: Engine

Engine combines analyzer's data models and user reports to provide an evaluation of the analysis.



IntelOwl: Recap

- IntelOwl is a Data Extraction Platform. It helps analysts to retrieve data from several sources.
- The goal for this year is to give a system to evaluate the data.

IntelOwl: Recap

- IntelOwl is a Data Extraction Platform. It helps analysts to retrieve data from several sources.
- The goal for this year is to give a system to evaluate the data.
- IntelOwl is an open source. Every contributor is welcome!
- IntelOwl is part of Google summer of code



IntelOwl: Recap

- IntelOwl is a Data Extraction Platform. It helps analysts to retrieve data from several sources.
- The goal for this year is to give a system to evaluate the data.
- IntelOwl is an open source every contributor is welcome!
- IntelOwl is part of Google summer of code



Give us YOUR ideas!



@intel_owl



intelowlproject/IntelOwl



Thank you for listening!

The icons were collected from: [FlatIcon](#)
Memes were generated with [Imgflip](#)

Intel  owl