IntelOwl Project

Making the life of cyber security analysts easier

Intel owl

whoami

Daniele Rosetti

Administrator and frontend maintainer

drosetti

certego

Threat Intelligence Team

Intel owl

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.

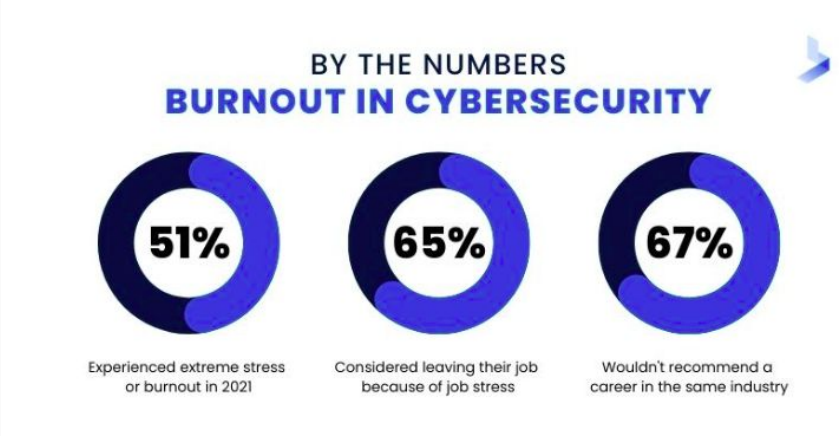
By Emily Chantiri on Sep 27 2023 04:06 PM

ref: AECS

83% of IT Security Professionals Say Burnout Causes Data Breaches

September 20, 2023 3 Min Read

ref: DarkReading



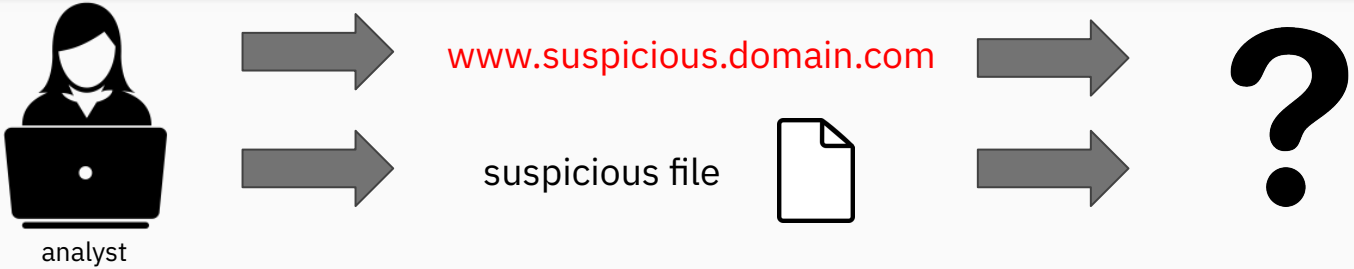
ref: Bitlyft

Automate, automate, automate

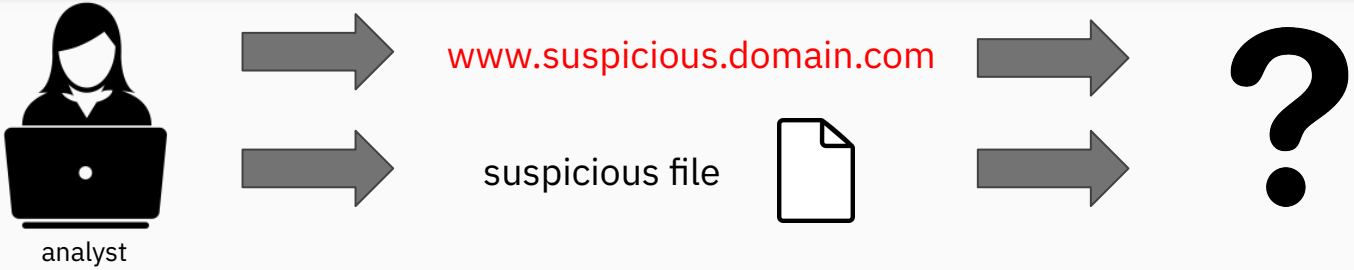
- Overwhelmed by security alerts
- Stuck in repetitive and boring tasks
- Burnt-out myself

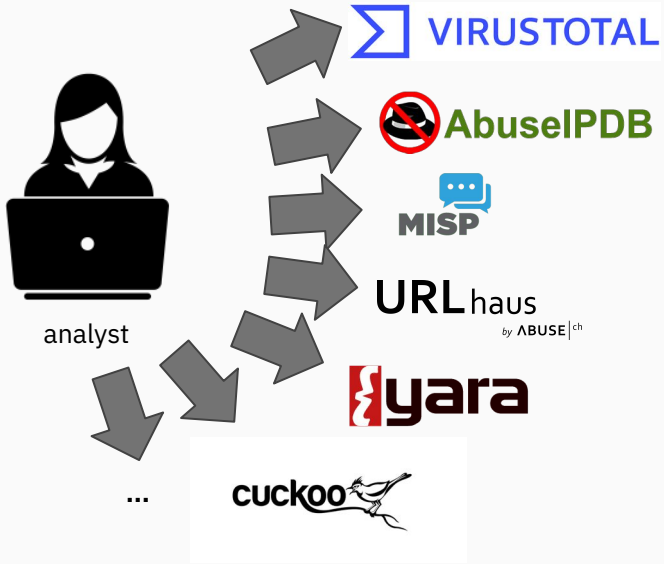
We needed to start to **automate** our most common workflows.

The bottleneck: acquisition of threat intelligence context



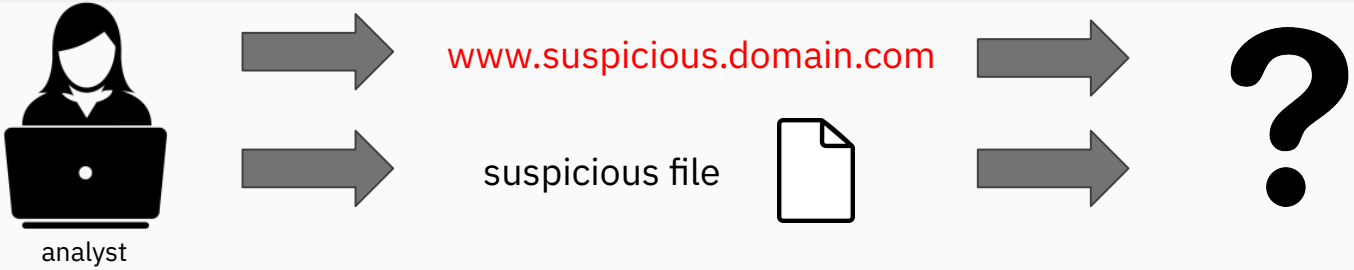
The bottleneck: acquisition of threat intelligence context

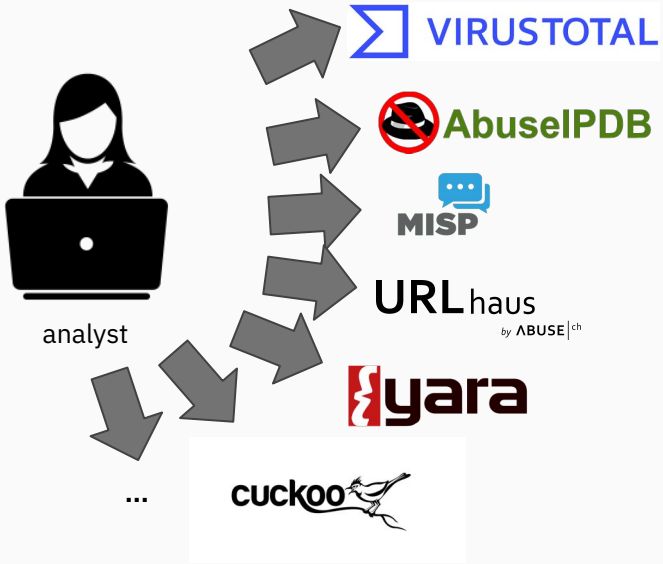


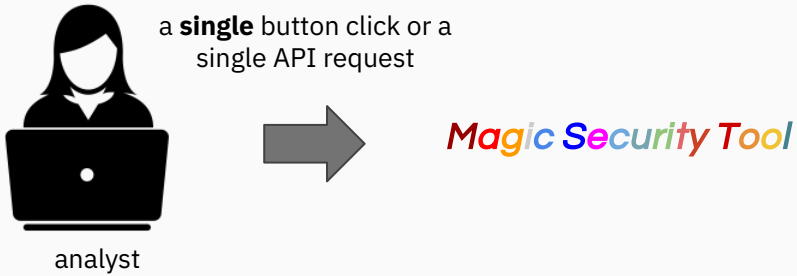


Intel owl

The bottleneck: acquisition of threat intelligence context







Intel owl

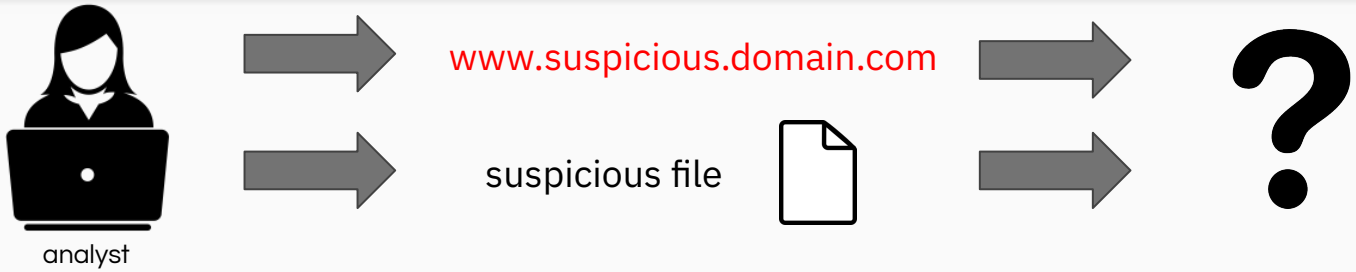
IntelOwl was born

Intel owl

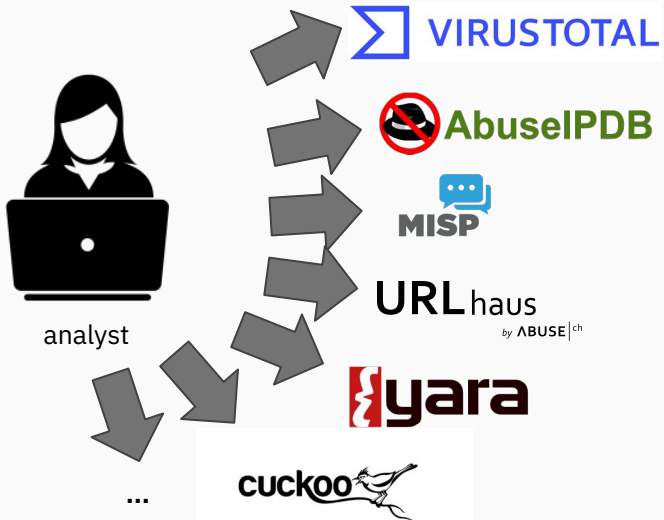
Born in Certego at the start of 2020, it is a great example of a successful Open Source project: right now it is one of the most popular Threat Intel projects on GitHub (>4k stars).

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

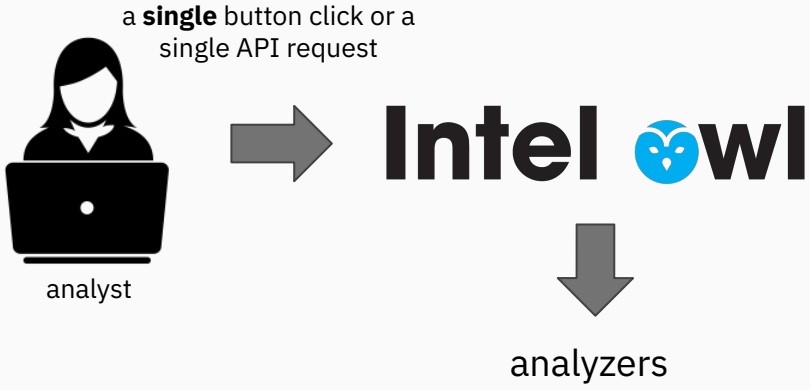
IntelOwl solution



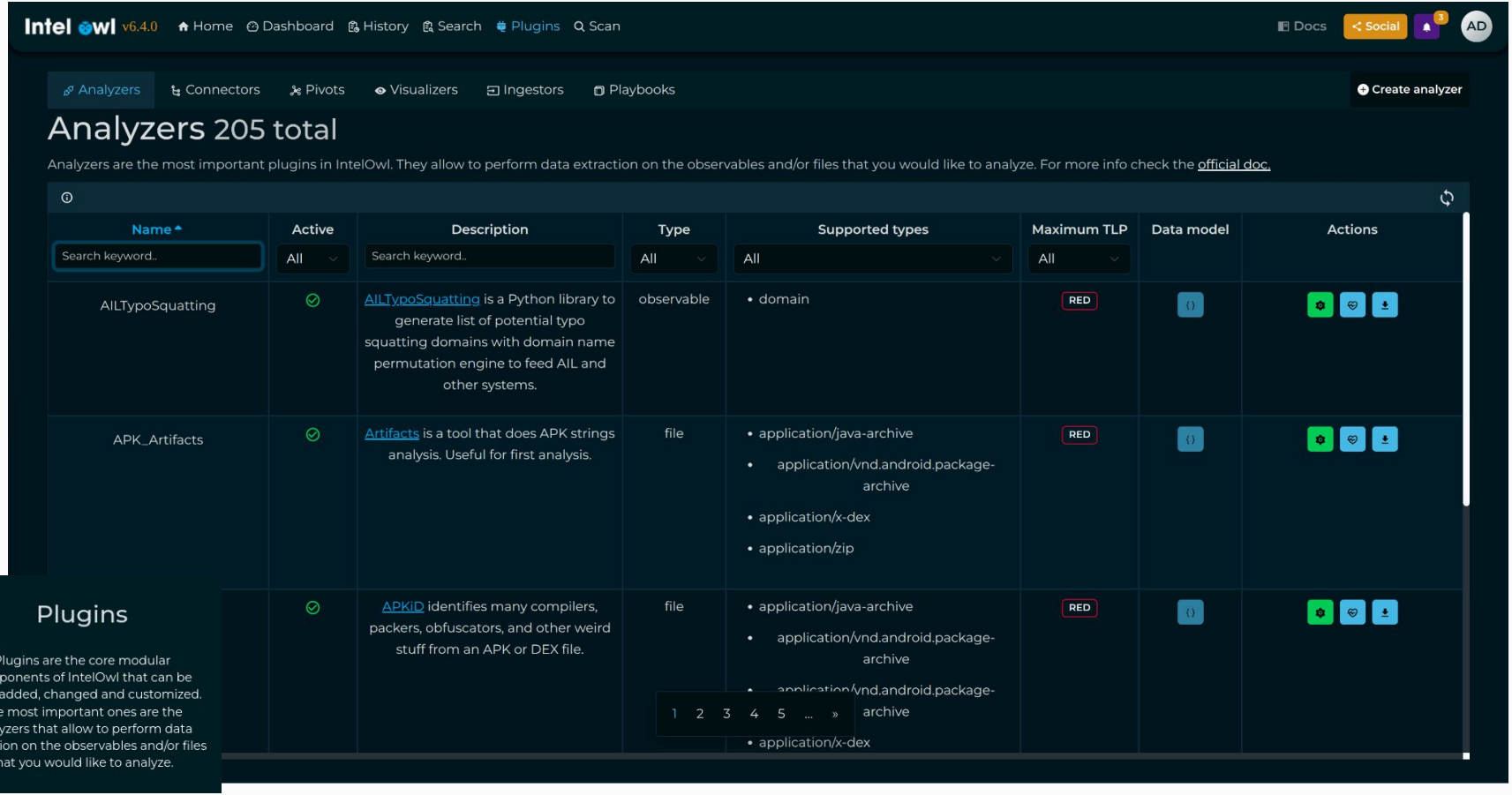
WithOUT Intel Owl



With Intel Owl



IntelOwl: Plugins



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.

IntelOwl: How to use the platform

Intel owl

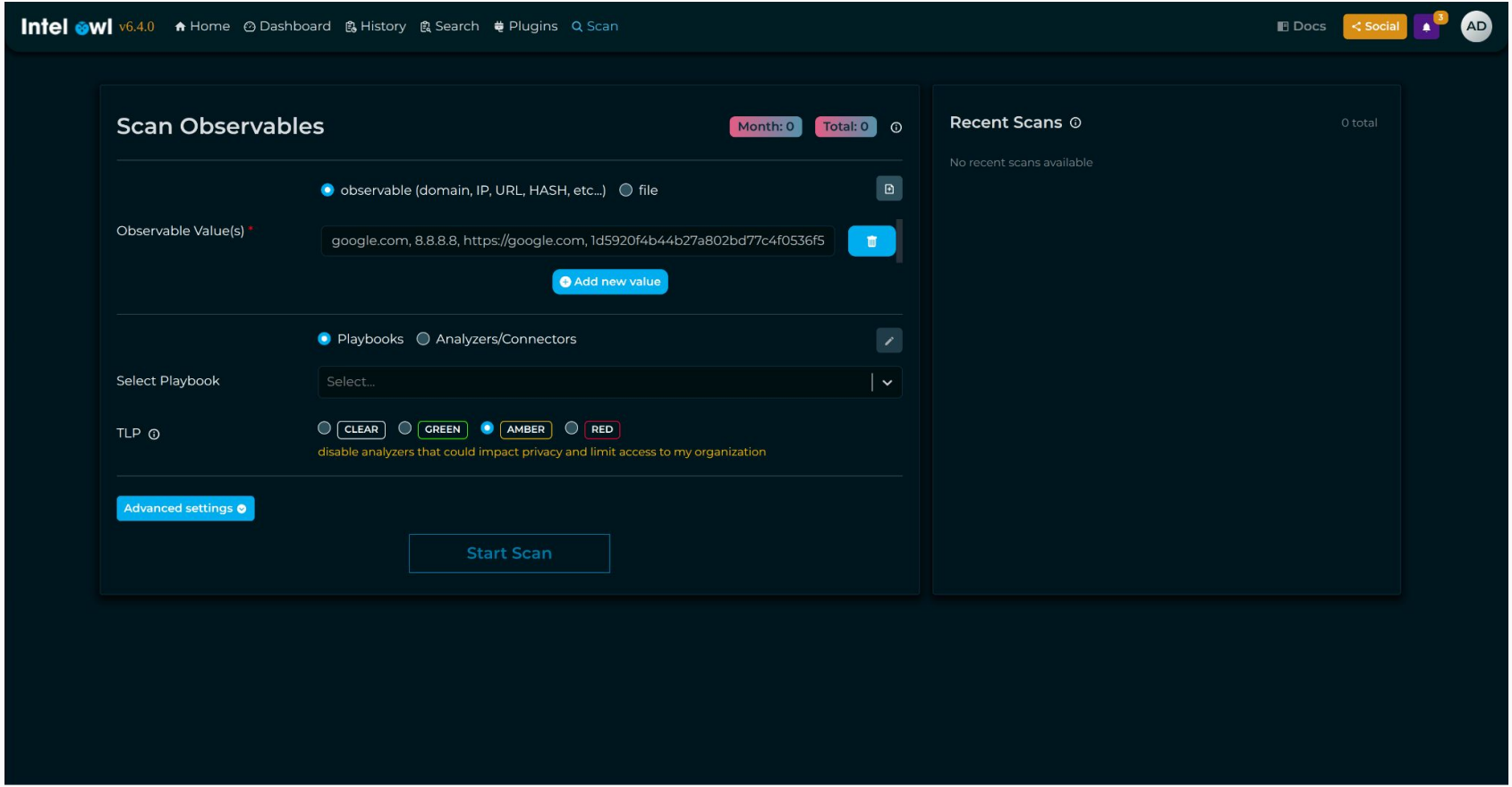
IntelOwl: Phishing verification

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

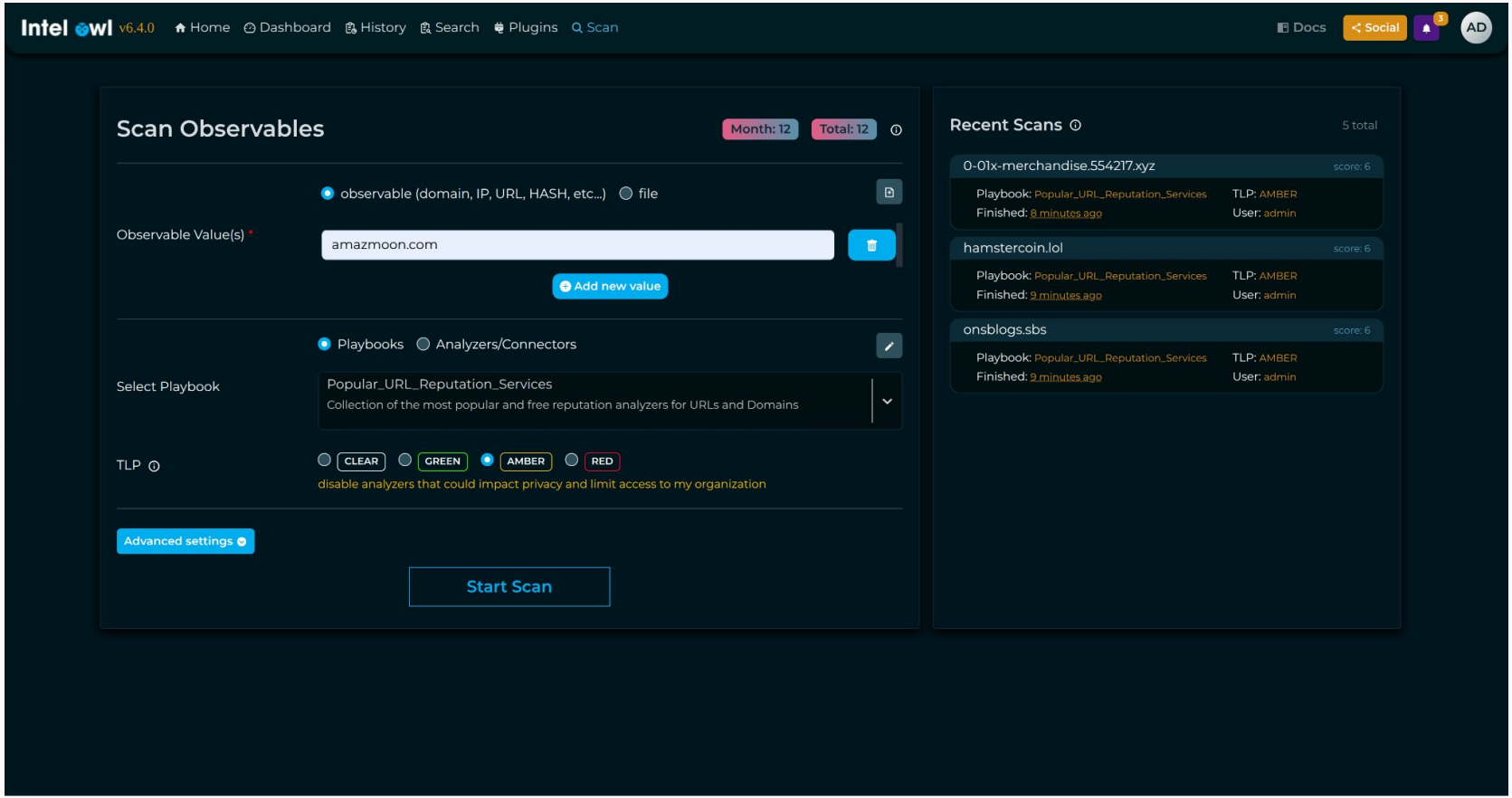
IntelOwl is integrated with tons of external services which can be queried to understand whether an URL is malicious or not and which kind of threat it poses: Reputation Services, DNS Resolvers, WHOIS services, Passive DNS services, URL Sandboxes, Threat Intel Platforms, Information Sharing Platforms,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

Those are all pre-built in the default installation.

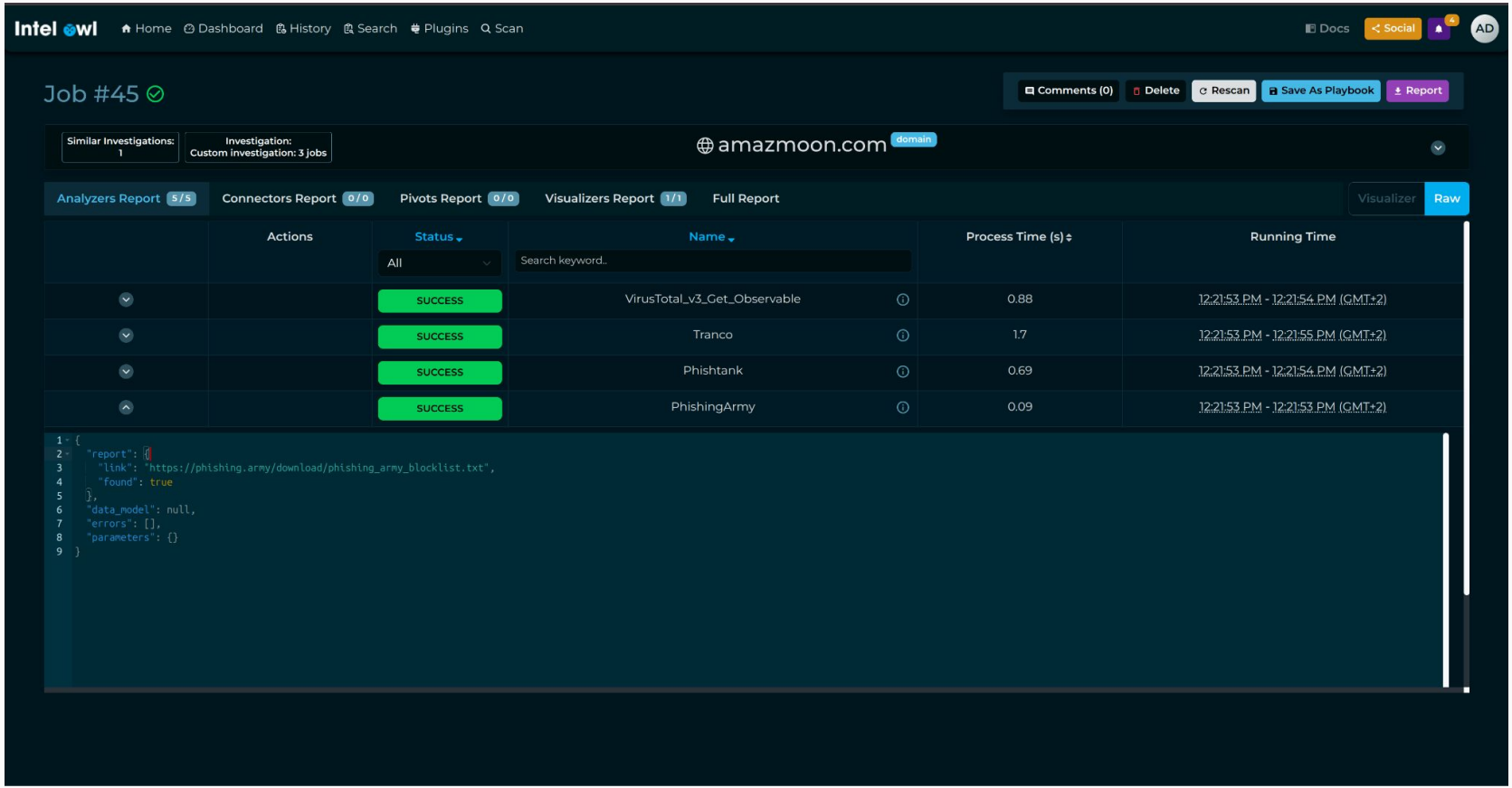
IntelOwl: Scan



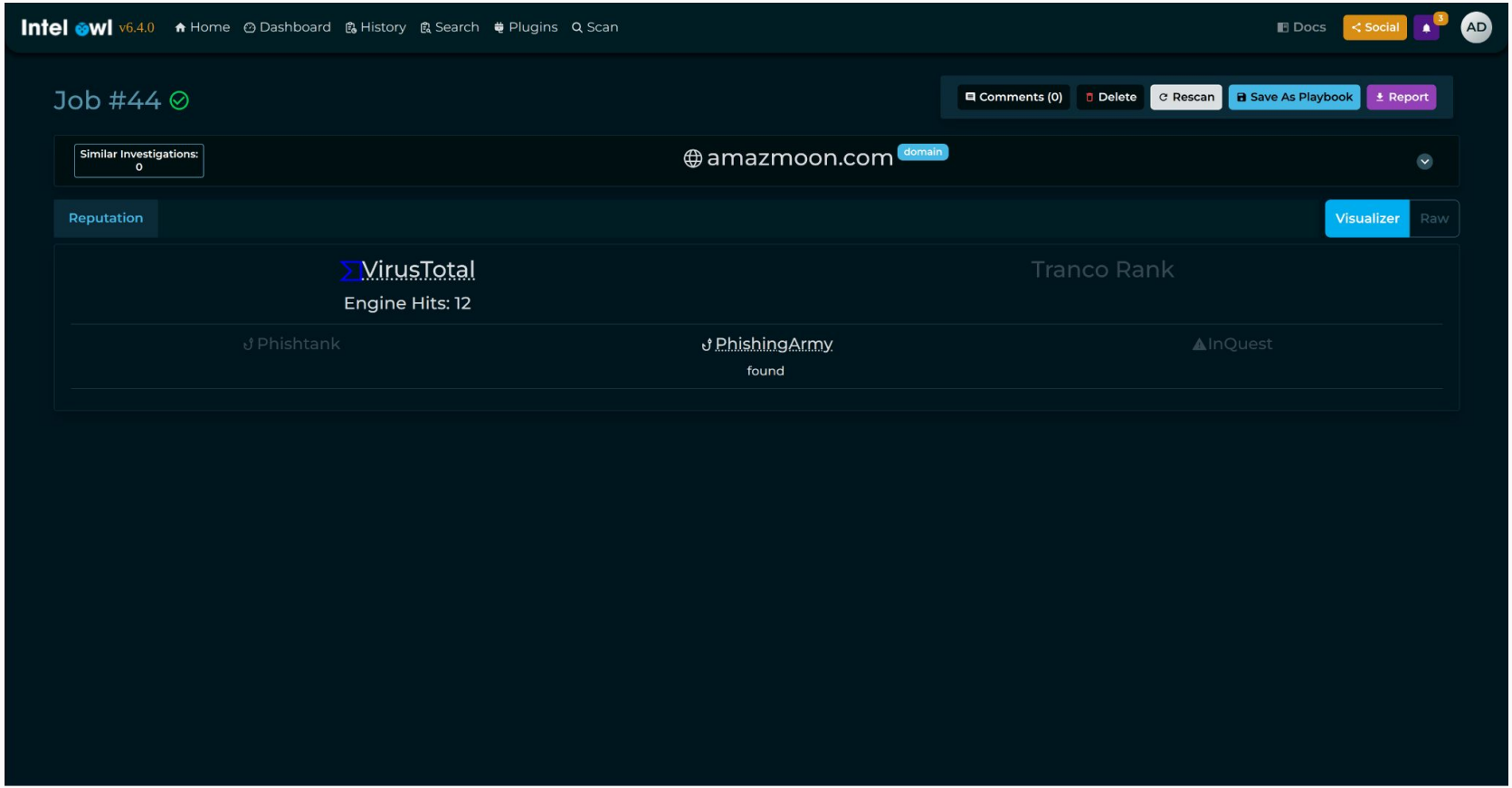
IntelOwl: Phishing verification



IntelOwl: Phishing verification



IntelOwl: Phishing verification

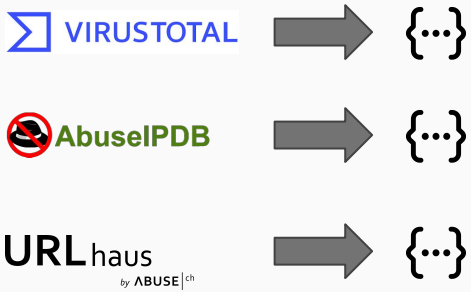


IntelOwl: Roadmap

Intel owl

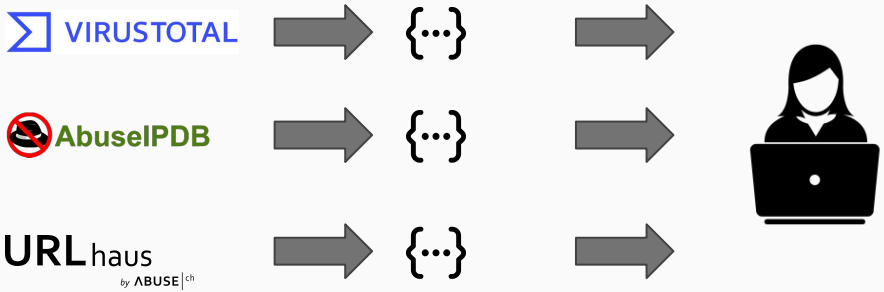
IntelOwl: Data Model

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



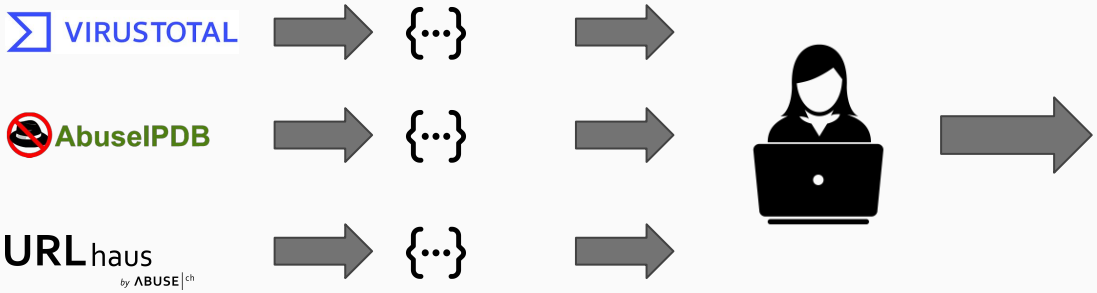
IntelOwl: Data Model

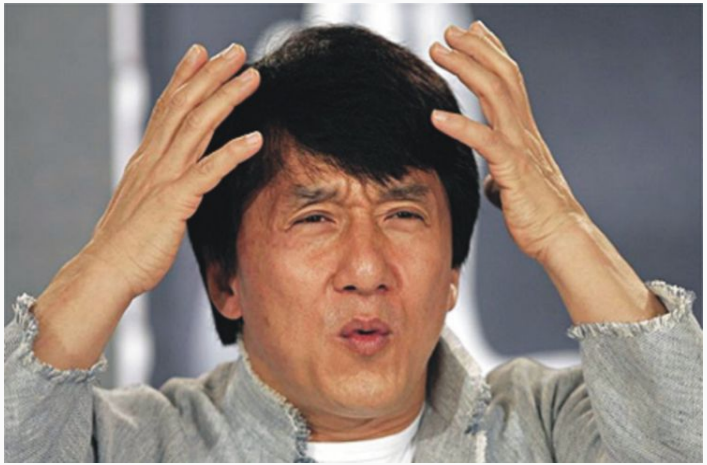
Users need to read them...



IntelOwl: Data Model

...And **understand** them

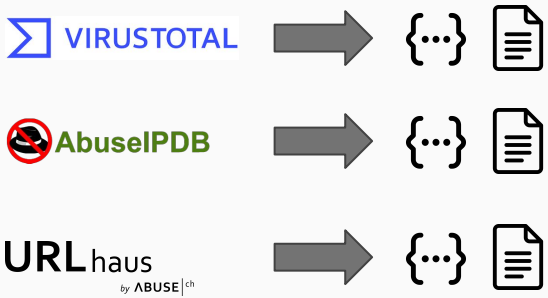




Intel owl

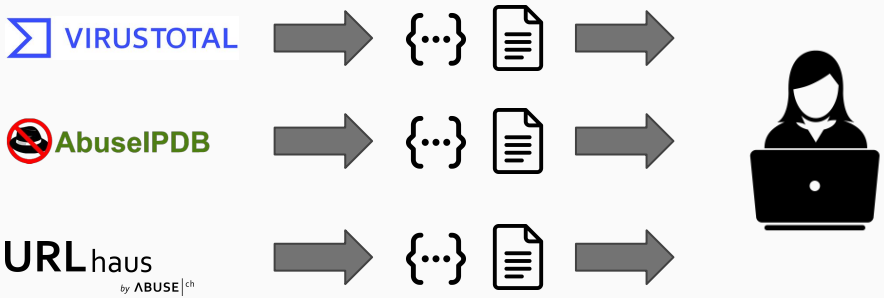
IntelOwl: Data Model

Data model allows analyzers to normalize the output.



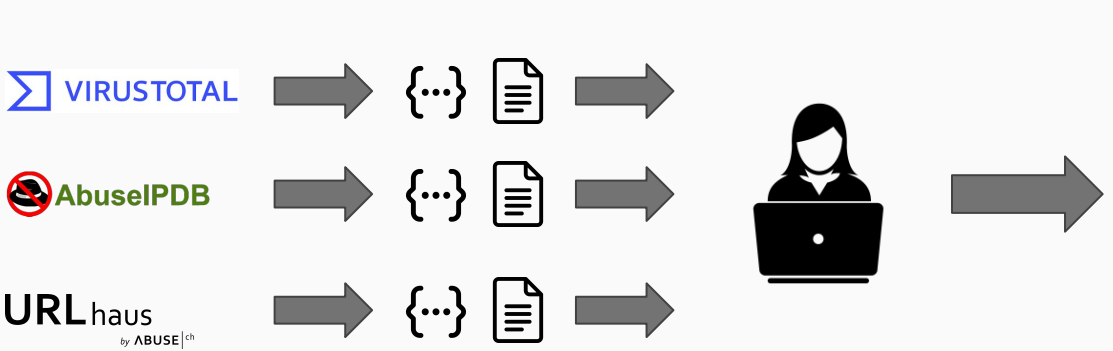
IntelOwl: Data Model

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.



Intel owl

IntelOwl: User Events

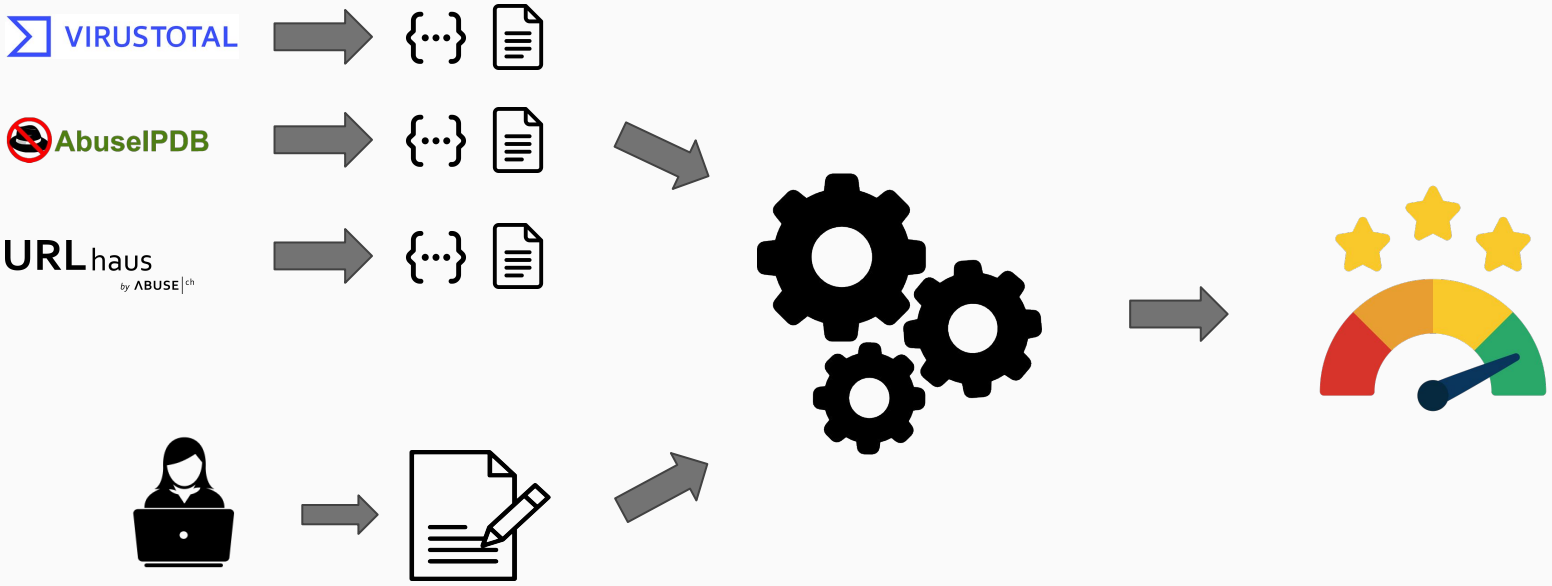
User events allow users to generate reports about analyzables.

Analyst

User event

IntelOwl: Engine

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



Intel owl

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

Intel owl

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

@intel_owl

intelowlproject/IntelOwl

Thank you for listening!

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

Intel owl