AIL Project

How to Improve and Support Your Threat Intelligence Process

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy
alexandre.dulaunoy@circl.lu

info@circl.lu

November 7, 2023

Background

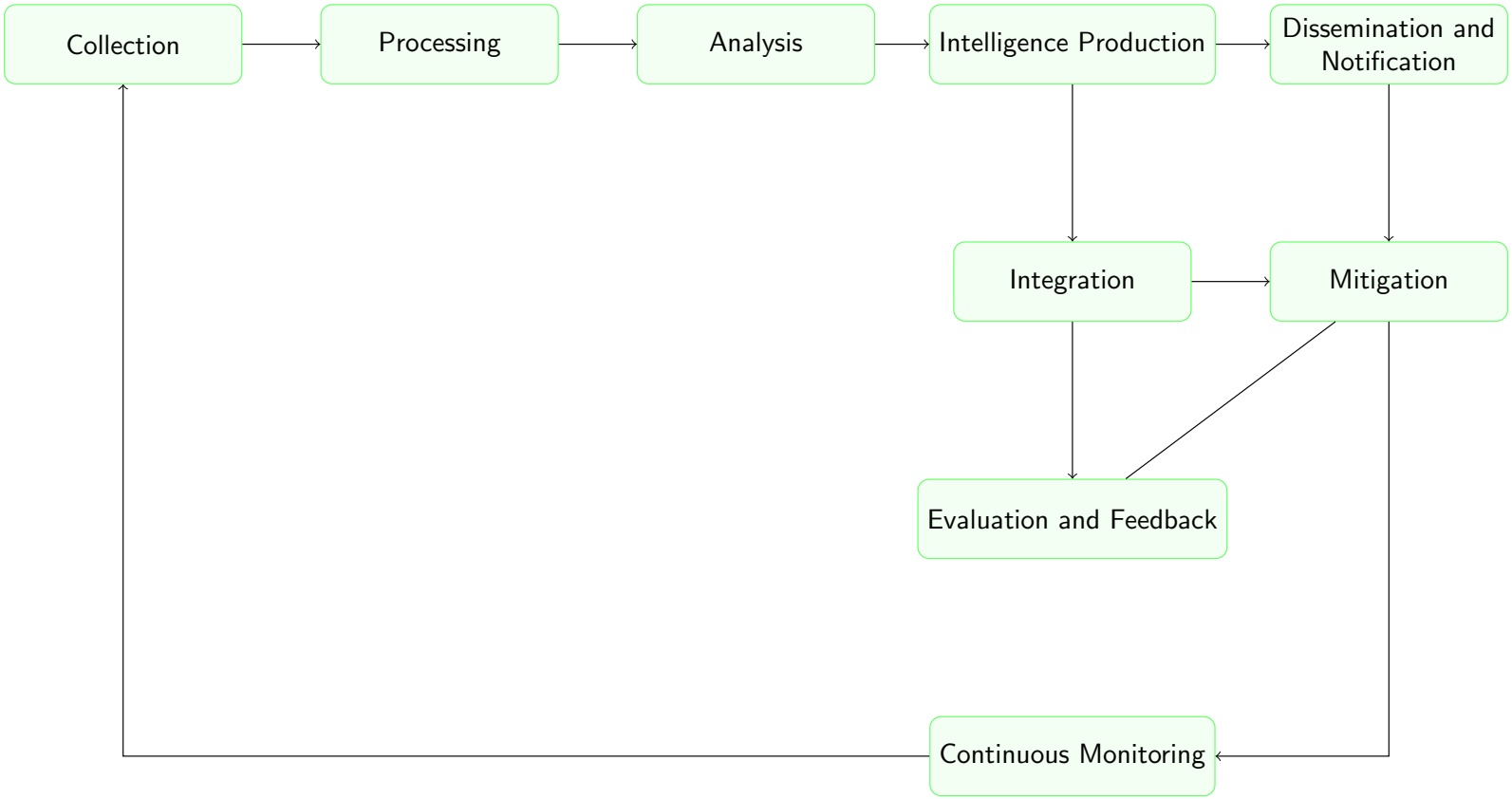
- Over the past five years, we have developed the AIL project[1] to fulfill our needs at CIRCL in intelligence gathering and analysis.
- As AIL gained popularity, an increasing number of users began integrating it into their **threat intelligence processes and workflows**.
- In this presentation, we outline some of the processes where AIL can serve as a valuable tool, **facilitating and enhancing the work of intelligence analysts**.

[1] `https://www.ail-project.org/`

AIL overview

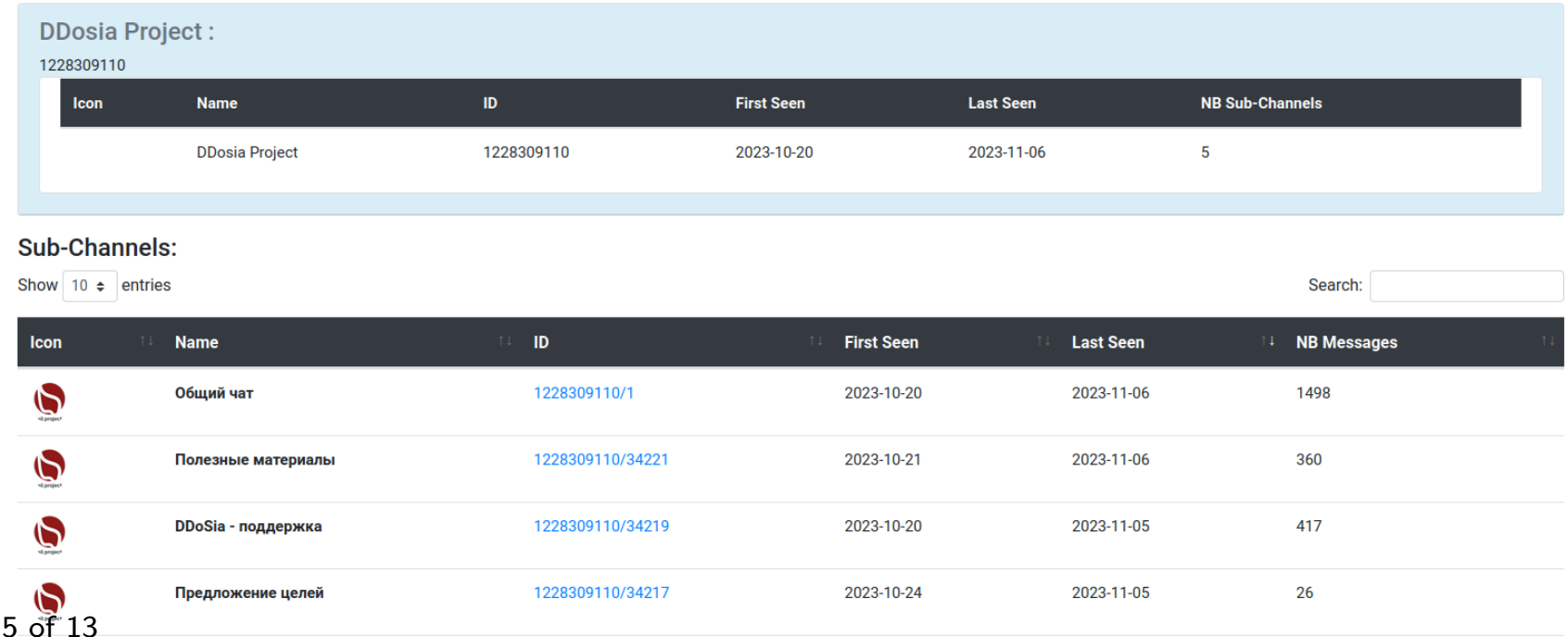
- The AIL Project is an open-source framework comprising various modules designed for the **collection, crawling, digging, and analysis of unstructured data**.
- AIL features an extensible Python-based framework for the **analysis of unstructured information**, collected either through an advanced Crawler manager or from various feeders, including social networks and custom feeders.
- AIL also provides support for actively **crawling Tor** hidden services, as well as crawling protected websites and forums by utilizing pre-recorded session cookies.

Threat Intelligence Process at CIRCL



Collection - automate collection

- Collecting data from various chat sources can be a **tedious task for analysts**.
- AIL offers a set of feeders (e.g., Telegram, Discord, etc.) that can be used to subscribe to chat channels.
- All the **collected messages are then processed and analyzed** within the AIL's *processing* and *analysis* stages.



DDosia Project :

1228309110

Icon	Name	ID	First Seen	Last Seen	NB Sub-Channels
	DDosia Project	1228309110	2023-10-20	2023-11-06	5

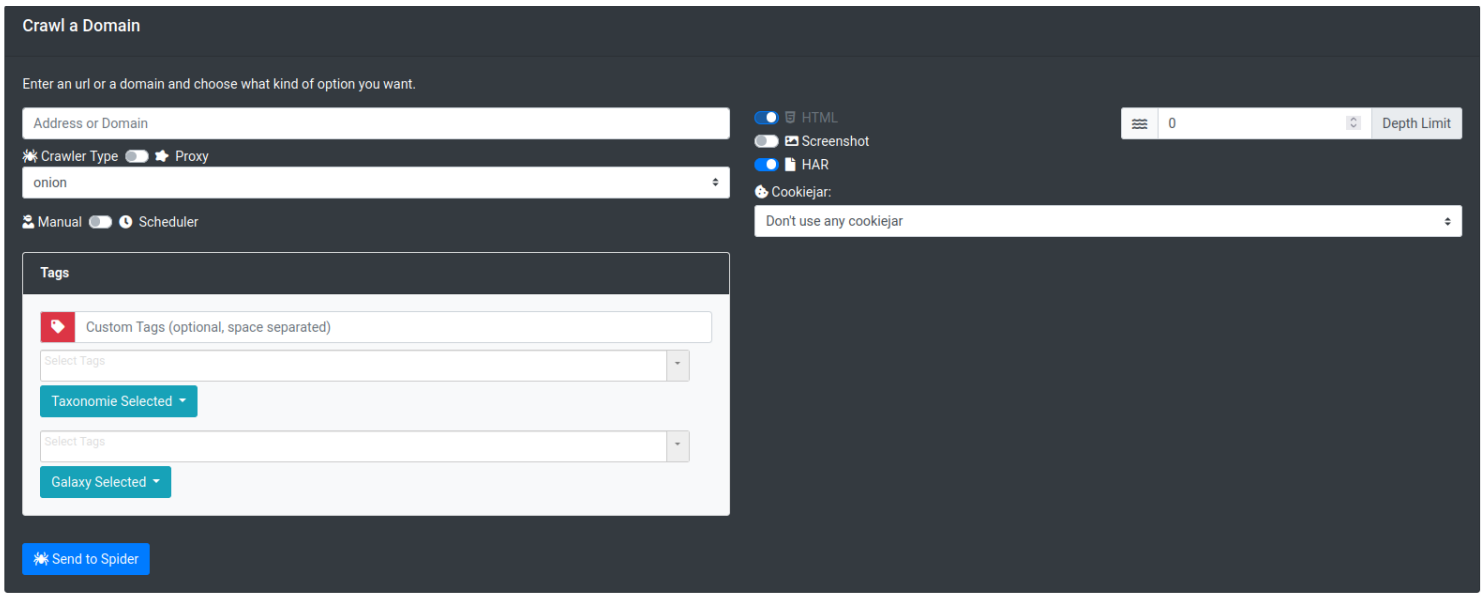
Sub-Channels:

Show 10 entries Search:

Icon	Name	ID	First Seen	Last Seen	NB Messages
	Общий чат	1228309110/1	2023-10-20	2023-11-06	1498
	Полезные материалы	1228309110/34221	2023-10-21	2023-11-06	360
	DDoSia - поддержка	1228309110/34219	2023-10-20	2023-11-05	417
	Предложение целей	1228309110/34217	2023-10-24	2023-11-05	26

Collection - automate crawling

- Crawling can be a challenging task, for example, gathering all the blog posts from ransomware groups[2], which can be demanding for an analyst.
- AIL offers a crawling feature that can **initiate regular crawls using a standard spawned browser**.



[2] `https://www.ransomlook.io/`

Processing - extracting selector/patterns

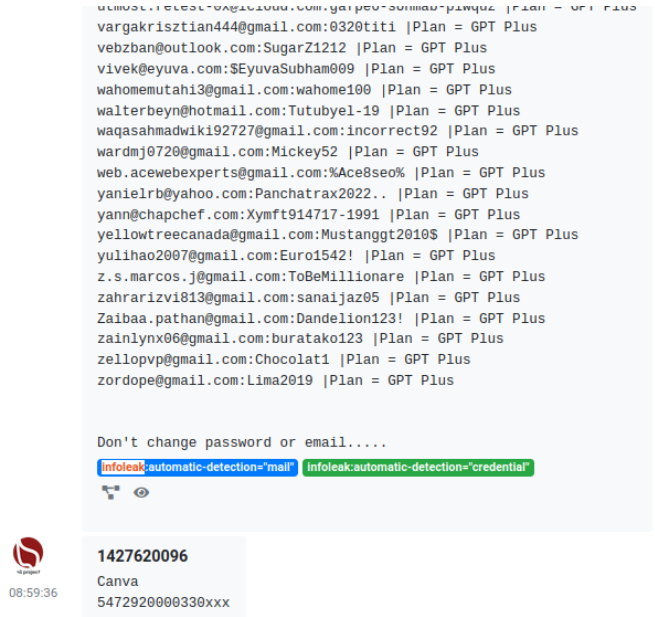
- Detecting specific search patterns in a large dataset, such as a significant ransomware leak, can be challenging for analysts.
- AIL includes a **rich set of existing search patterns** (e.g. IBAN) along with default Yara rules, and you have the ability to create custom ones.

Type	ID	Extracted
tag	infoleak:automatic-detection="onion"	https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr https://3vynrelomm3k43lqhetkztg2o25eif4hr
tag	infoleak:automatic-detection="iban"	ES5221004423650200138506
tracker	13ac3e24-e922-4d50-a08b-4b746b08a672	BEGIN PKCS7
	ERROR	Donaciones Audiocinemateca Donaciones

Showing 1 to 4 of 4 entries

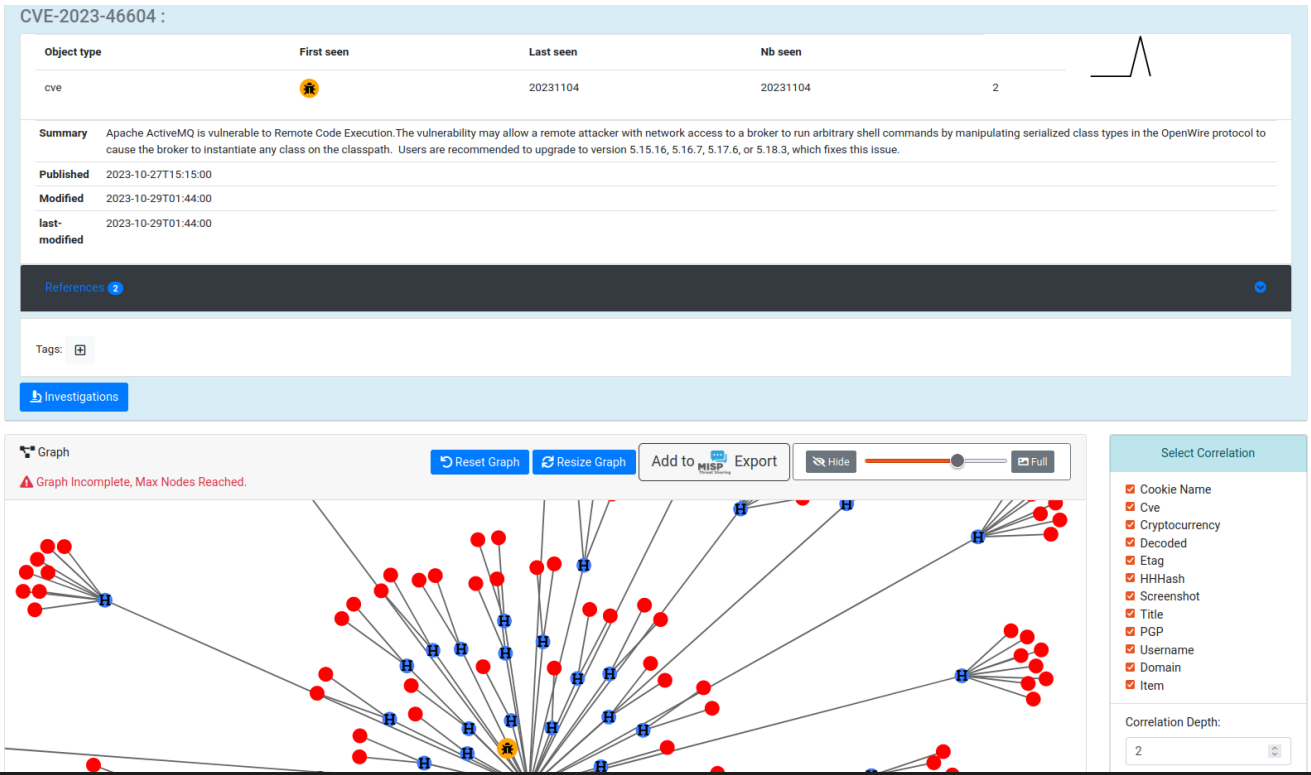
Analysis - automatic detection from collection

- Processing automatically collected information can be a challenging task.
- AIL processes all the collected items for any **hunting rules and utilizes MISP taxonomies to tag the matching information**.



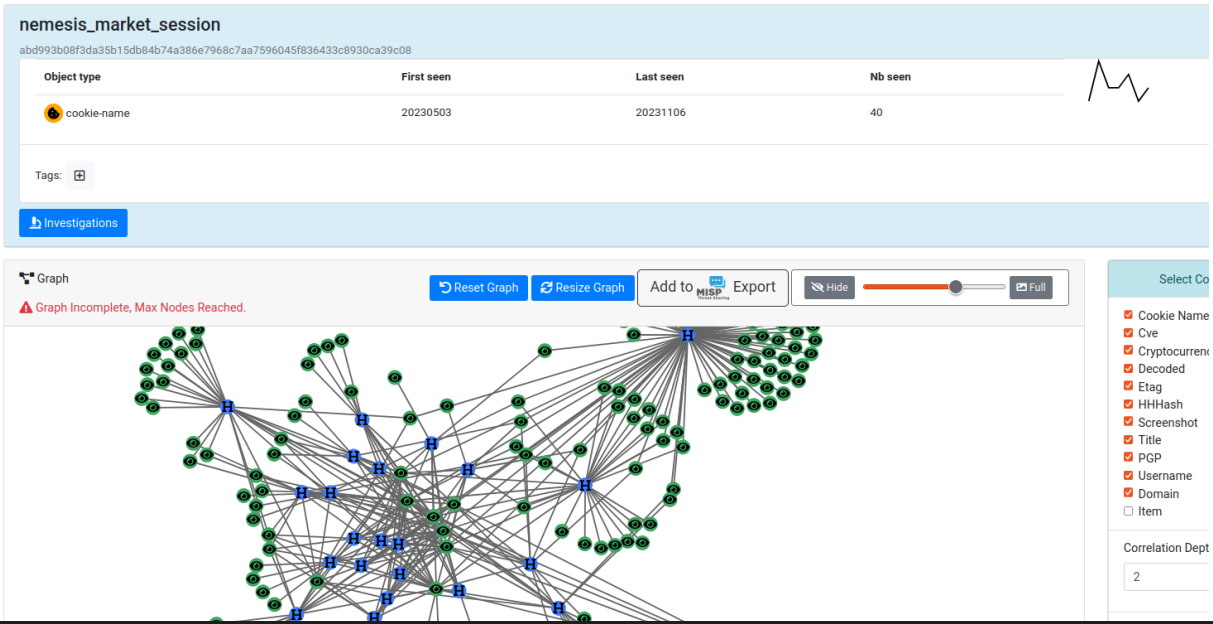
Analysis - evaluating vulnerability severity/risk

- What is the visibility, usage, mentions, or risk of a vulnerability observed in forums, channels, pastes, or websites?
- AIL can assist you in determining the severity/risk level or in **reviewing the usage of a vulnerability** (e.g., the number of PoCs).



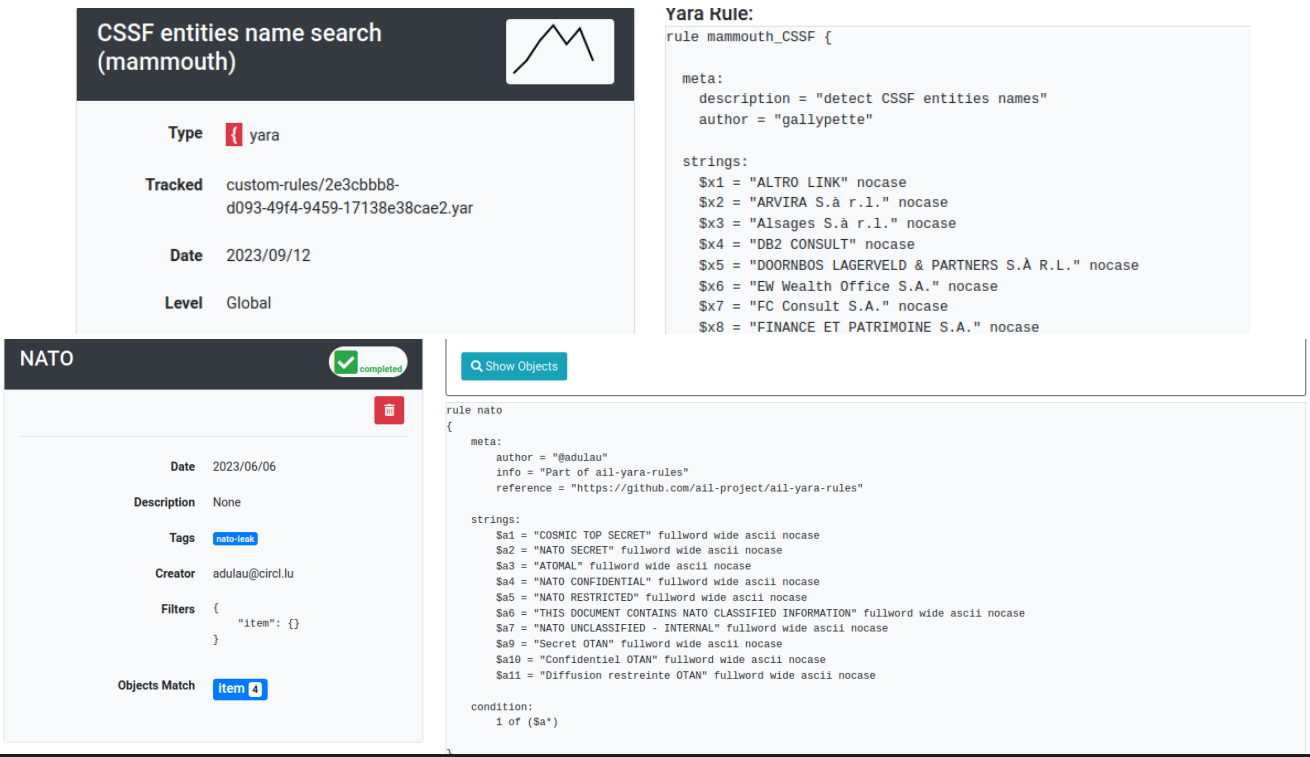
Dissemination - distributing analysis

- AIL exports data using the **MISP standard format** and offers complete integration with MISP to facilitate the dissemination of data.
- All the context within AIL uses the **MISP taxonomies and galaxy**.
- The insights provided by AIL are often used as complementary information for threat intelligence reports and landscapes.



Evaluation/Integration - review search rules on real dataset

- Reviewing matching rules on a large dataset, such as extensive ransomware leaks, can be cumbersome.
- AIL provides a "retro-hunt" functionality to search and **evaluate your Yara rules**.



Conclusion

- While AIL can be a valuable tool for **organisations dealing with data leaks and information breaches**, it's important to remember that it is primarily designed for information leak analysis and not for the entire threat intelligence process.
- Organizations should use **AIL in conjunction with other threat intelligence solutions** and processes to establish a comprehensive threat intelligence strategy.
- AIL is an open-source project, and if you discover modules that could assist in your processes, please let us know or contribute directly.

Links

- AIL project `https://github.com/ail-project` (**all components including feeders and crawler infrastructure**)
- AIL framework `https://github.com/ail-project/ail-framework` (**analysis framework**)
- Training materials and slide deck `https://github.com/ail-project/ail-training`