

# AIL Project

## How to Improve and Support Your Threat Intelligence Process



**CIRCL**

Computer Incident  
Response Center  
Luxembourg

Alexandre Dulaunoy

[alexandre.dulaunoy@circl.lu](mailto:alexandre.dulaunoy@circl.lu)

[info@circl.lu](mailto:info@circl.lu)

November 6, 2023

# Background

---

- Over the past five years, we have developed the AIL project<sup>1</sup> 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**.

---

<sup>1</sup><https://www.ail-project.org/>

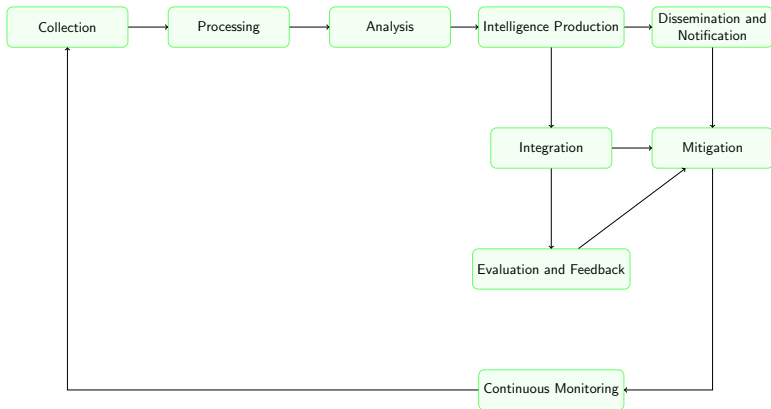
## AIL overview

---

- 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

---



## 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>

