CIRCL
Computer Incident
Response Center
Luxembourg

Flow your management

https://github.com/flowintel/flowintel

David Cruciani - david.cruciani@circl.lu

October, 2025

CIRCL https://www.circl.lu

Me - David Cruciani

- CIRCL since 2021
- Software Engineer, Forensics Analyst
- https://github.com/DavidCruciani
- Love Cycling

FlowIntel - What & Why

FlowIntel is an open-source *incident & forensic case management platform*.

- Day-to-day CSIRT / SOC work still relies on spreadsheets, generic ticketing tools, or expensive closed platforms.
- There was **no vendor-neutral, open source** alternative focused on *security operations workflows*.
- FlowIntel fills that gap: structure investigations, keep evidence organised, and accelerate collaboration.

FlowIntel - Who

Facts

- Co-funded by **CIRCL** (Computer Incident Response Center Luxembourg) and the **European Union**.
- As a pivotal open source case management for the **CIRCL** toolset such as MISP or AIL.
- Source code: https://github.com/flowintel/flowintel

Who Is It For?

- **Security analysts / responders** needing lightweight but powerful case & task handling.
- **Threat intelligence teams** enriching cases with MISP data.
- **Forensic investigators** documenting acquisitions, analysis steps and findings.
- **Any organisation or individual** wanting a simple way to manage incident-like workflows.
- Lower barrier than specialised tools - FlowIntel exposes only what you need as a security analyst.

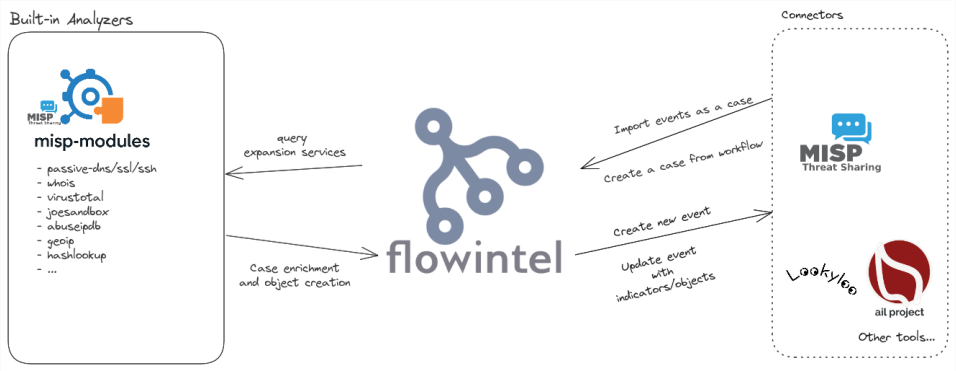
What Can You Do With FlowIntel ?

- **Track** cases, tasks, subtasks and their status.
- **Organise** notes, evidence, timelines and reports.
- **Collaborate**: shared workspace, templates.
- **Plan** with a built-in calendar & to-do management.
- **Notifications / Reminders** for task assignments and upcoming deadlines
- **Automate** via the REST **API** and connectors.
- **Explore** statistics across all cases and tasks
- **Build** your own plugins and workflows.
- **Integrate** with MISP
- . . . and more as the community grows.

FlowIntel and MISP

- **Import** MISP events as new cases.
- **Leverage** galaxies & taxonomies for classification.
- **Use** MISP-modules as on-demand analysers.
- **Export** cases to MISP when needed.
- **Support** for multiple MISP instances side by side
- **Attach** MISP-Object directly to cases

FlowIntel Interactions



FlowIntel sits between your analysts and your intelligence sources: ingest from MISP and other systems, enrich inside the platform, and push consolidated intelligence back out.

Time to test !

https://github.com/flowintel/flowintel

Thank You for listening !!