DFIR-IRIS.org

Collaborative incident response platform

Paul Amicelli - Théo Letailleur
Pass The SALT 2022

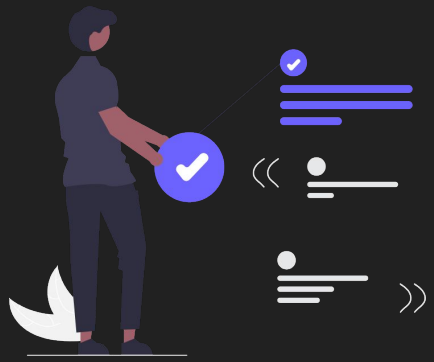
Whoami

Incident responder
Paul Amicelli
@White_Kernel

Incident responder
Théo Letailleur
@ekt0

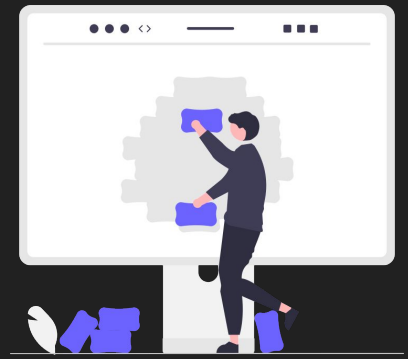
CSIRT Airbus
Cybersecurity

Problems



Track **elements** observed during the investigation

Effectively **share pieces of information** between analysts



Handle **repetitive** and **redundant** tasks

Alternative solutions

- The free and open-source ones


TheHive (v4)


FIR

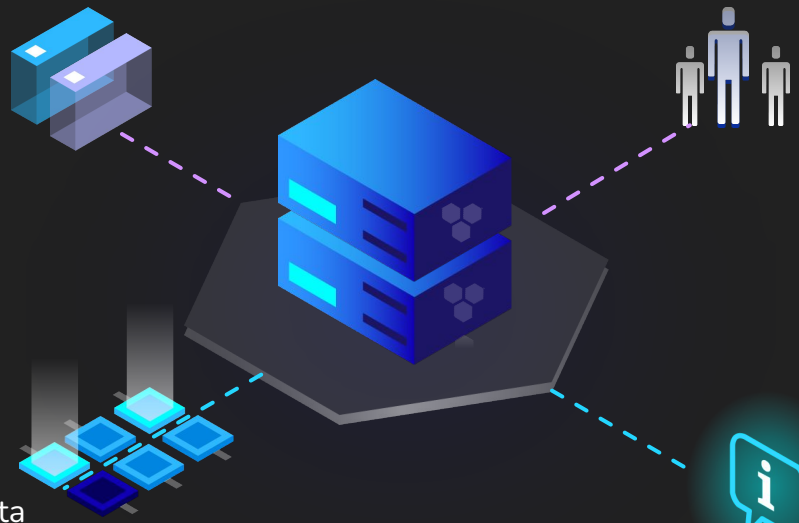

Catalyst

DFIRTrack


Aurora

DFIR-IRIS

Python web app
Portable, extensible and pluggable thanks to an open API and modules

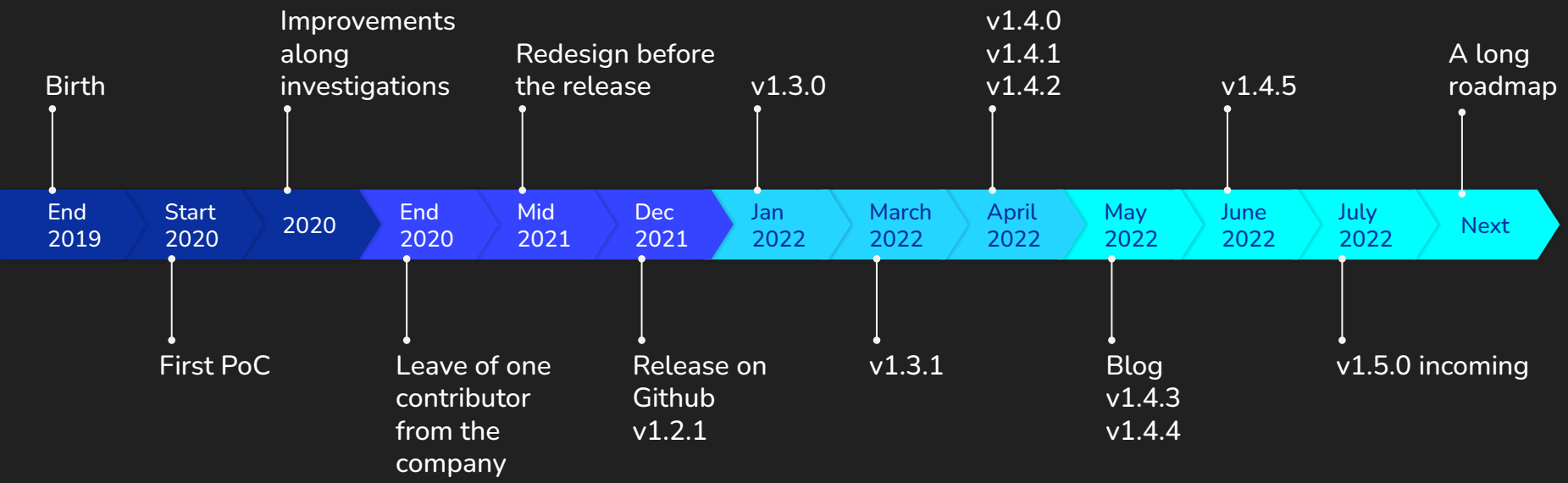


Collaboration
Collaborative editing, notes, tasks, information sharing

Automation
with report generation, data ingestion and enrichment

Tracking
IOCs, assets, timeline, evidence, follow up

DFIR-IRIS - Background



Demonstration

The future

1. **Authentication** OpenID Connect, and multi-factor
2. **Authorizations** (access control and roles)
3. New **modules and integrations**
4. TTP functionality
5. Workshops? Governance?
6. And even more on docs.dfir-iris.org/roadmap

https://matrix.to/#/#dfir-iris:matrix.org

Join us!

https://github.com/dfir-iris

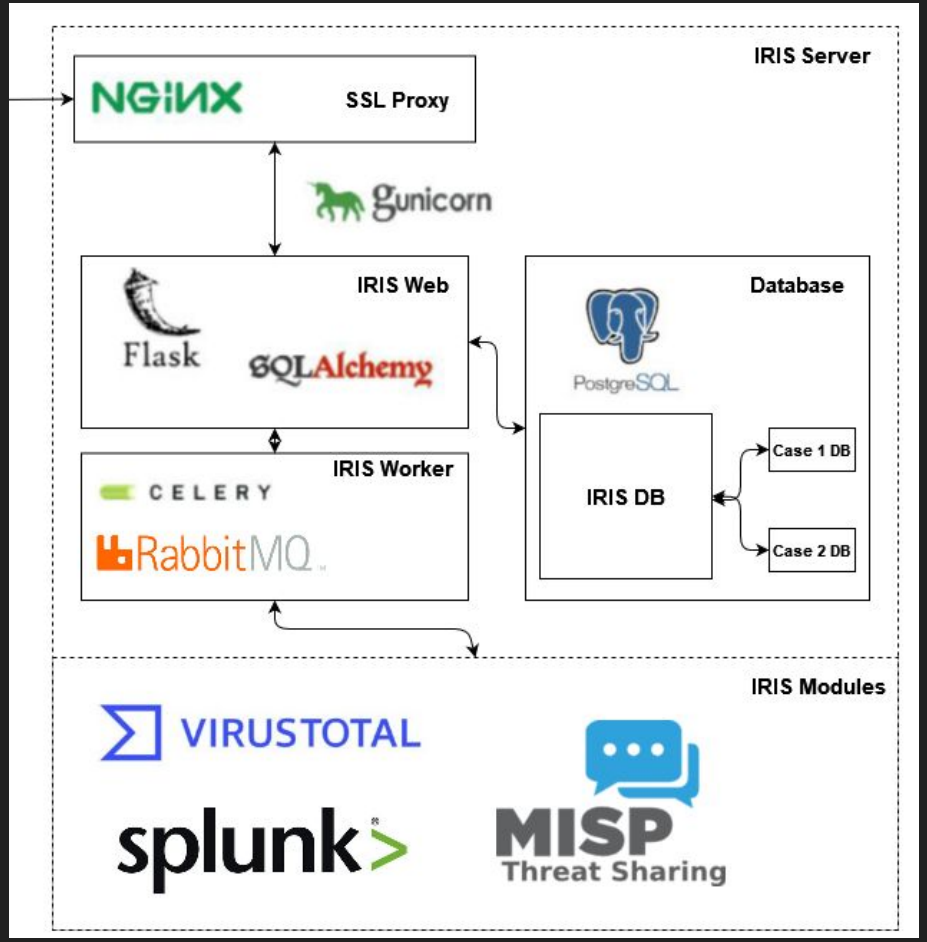
https://discord.gg/76tM6QUJza

https://twitter.com/dfir_iris

Annexe - Architecture

Architecture segregated into Docker components

- Flask for the web service
- SQLAlchemy and PostgreSQL for the database
- Celery and RabbitMQ the data processing from modules
- Nginx for the reverse proxy



Annexe - DFIR-IRIS in numbers

~971,3 commits

68 issues

47 pull requests

9 versions release

7 contributors

6 new modules

and 1613930339 coffees