DFIR-IRIS.org

Plateforme de réponse sur incident collaborative

Paul Amicelli - Théo Letailleur
SSTIC 2022

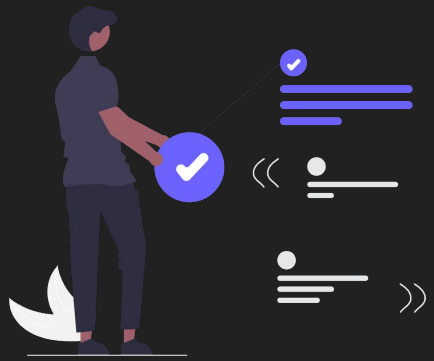
Qui sommes-nous ?

Incident responder
Paul Amicelli
@White_Kernel

Incident responder
Théo Letailleur
@ekt0

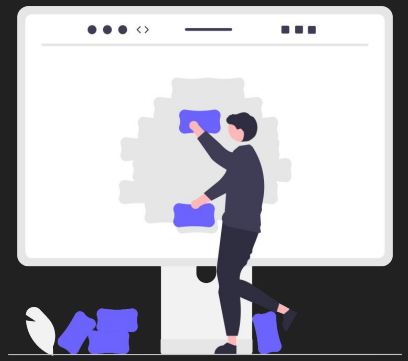
CSIRT Airbus
Cybersecurity

Problématiques



Tracer les **éléments** rencontrés durant l'**investigation**

Partager **efficacement** les informations entre analystes



Traiter les **tâches répétitives** et redondantes

Les solutions alternatives

Solutions open-source et gratuites

TheHive (v4)

FIR

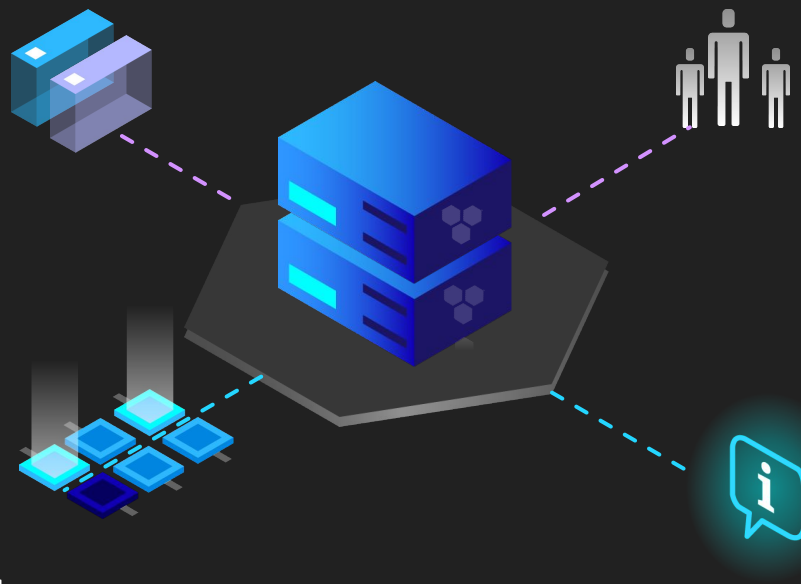
Catalyst

DFIRTrack

Aurora

DFIR-IRIS

App Web Python
portable, extensible et intégrable grâce une API et des modules

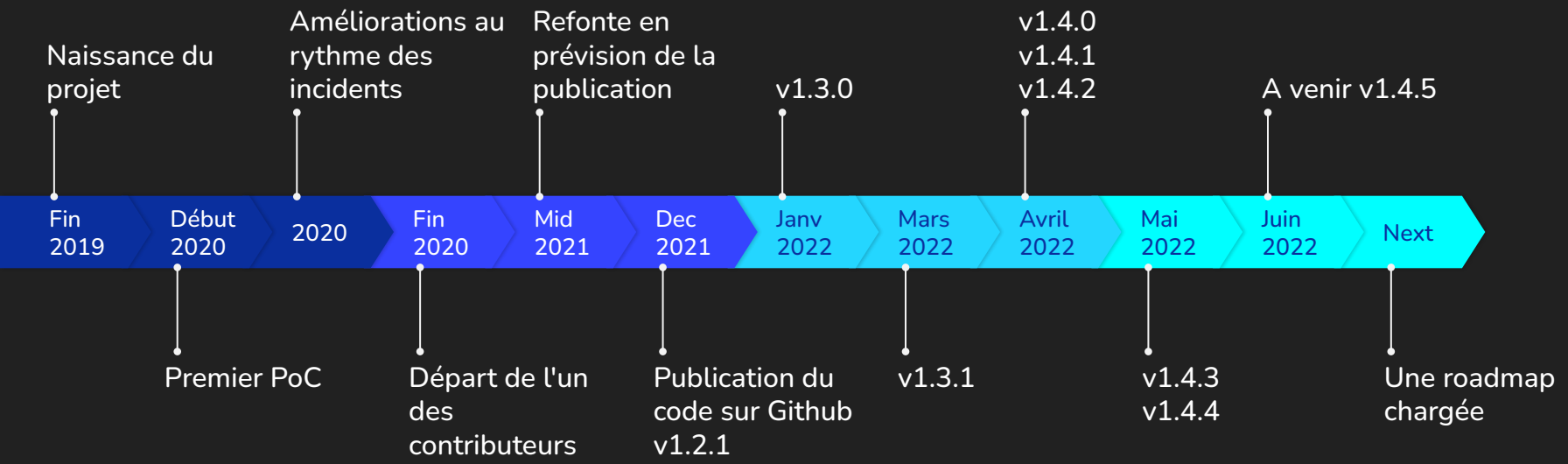


Collaboration
Edition collaborative, notes, tâches, partage des informations

Automatisation
avec générations de rapports, ingestion de données et enrichissement

Traçabilité
IOCs, assets, timeline, preuves, main courante

DFIR-IRIS - Historique



Démonstration

Le futur

1. **Authentification** OpenID Connect, et multi-facteur
2. **Autorisations** (contrôle d'accès et rôles)
3. Nouveaux **modules et intégrations**
4. Fonctionnalité de **TTP**
5. Workshops ? Gouvernance ?

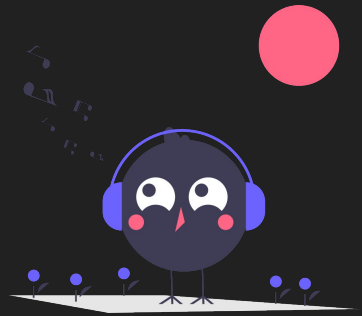
"Objectif Lune"

Rejoignez-nous !

https://github.com/dfir-iris

https://discord.gg/76tM6QUJza

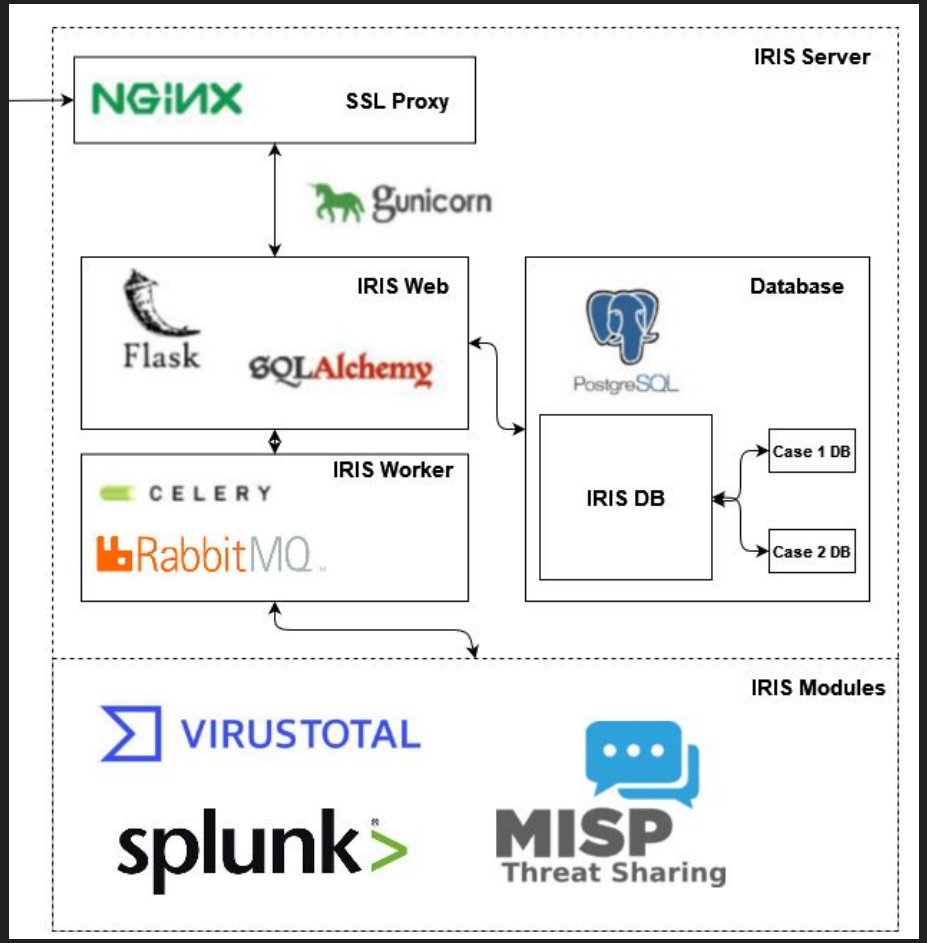
https://twitter.com/dfir_iris



Annexe - Architecture

Architecture séparée en composants Docker

- Flask pour le service web
- SQLAlchemy et PostgreSQL pour la base de données
- Celery et RabbitMQ pour le traitement des données des modules
- Nginx pour le reverse proxy



Annexe - DFIR-IRIS en chiffres

~800 commits

62 issues

47 pull requests

8 versions release

7 contributeurs

4 nouveaux modules

et 16180339 cafés