Rapport du openCTI

OpenCTI
Cyber Threat Intelligence

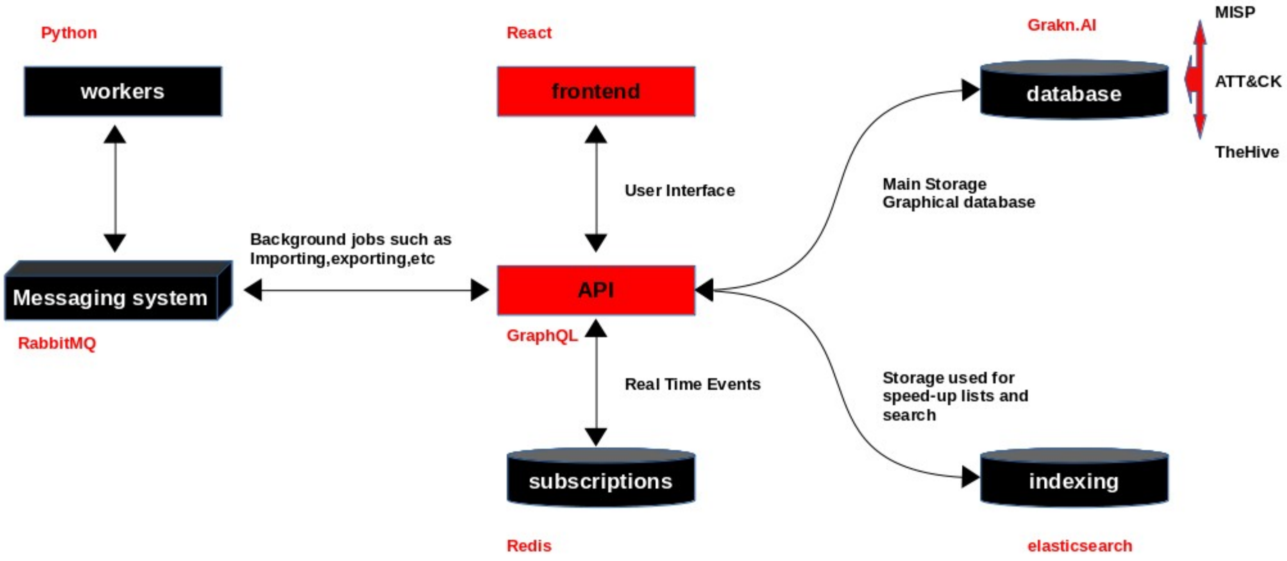
Version 1 le 01/07 2019

I. Objectif

openCTI is an open source platform for organizations to manage (stock & structure & visualize) cyber-threat intelligence.

II. Architecture

The openCTI platform replies on several external databases and services to work.



X. Annexes

STIX2: Structured Threat Information eXpression, a structured langage for Cyber Threat Intelligence.
UX : User eXpression design
MISP: Malware Information Sharing Platform and Threat Sharing.
TheHive: Security Incident Response Platform for **SOC & CSIRT & CERT.**
ATT&CK: Catalog of techniques and tactics that describe post-compromise adversary behavior.
TTP:Tactics, Techniques and Procedures
Luatix:Association for cybersecurity and crisis management