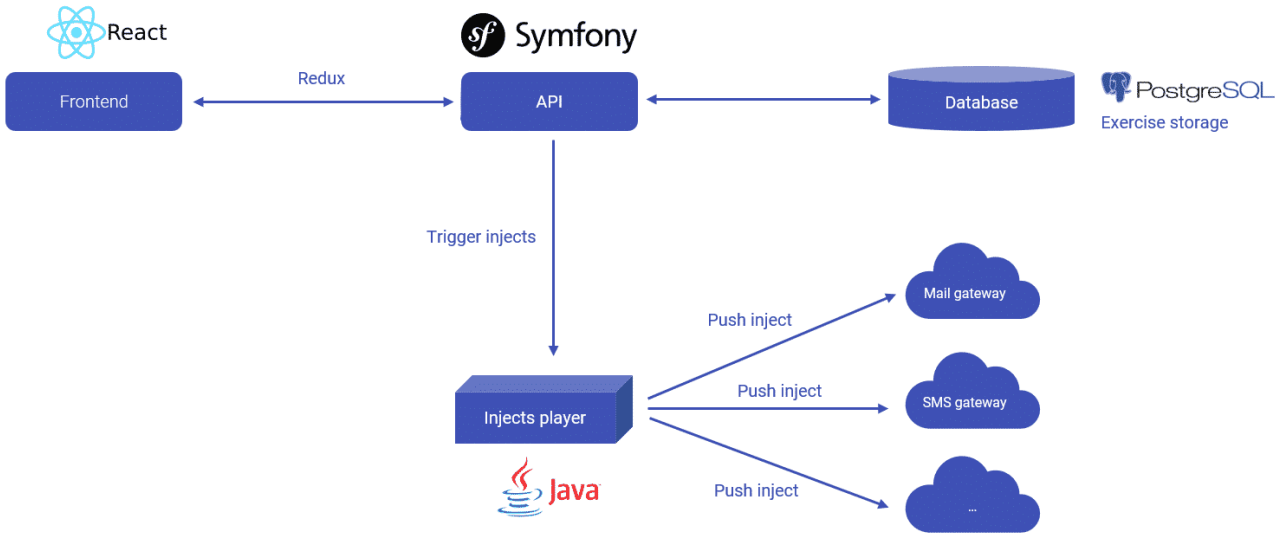
OpenCTI : le projet origine ANSSI rallie Thales et Gatewatcher

C'est officiel depuis quelques jours : Thales s'est rallié à Luatix*. Le groupe français est devenu membre sponsor de cette association à but non lucratif née voilà quatre ans.

Luatix a pris sous son aile deux projets *open source*. Le plus ancien trouve ses racines en 2016. Son nom : **OpenEx**. Il s'agit d'une plate-forme de planification et d'orchestration d'exercices de crise. La première bêta était sortie en mars 2017, parallèlement à la création de l'association.

> *Lancement de l'association Luatix ! Recherche et développement en #CyberSécurité #InfoSec #GestionDeCrise https://t.co/xbj3gKwvII*
>
> *— Luatix (@LuatixHQ) March 13, 2017*

La première version majeure était sortie à l'été 2018. La deuxième est arrivée il y a quelques semaines. Elle a notamment ajouté le SSO, les galeries de documents et le *geofencing*.



OpenCTI : une option made in France

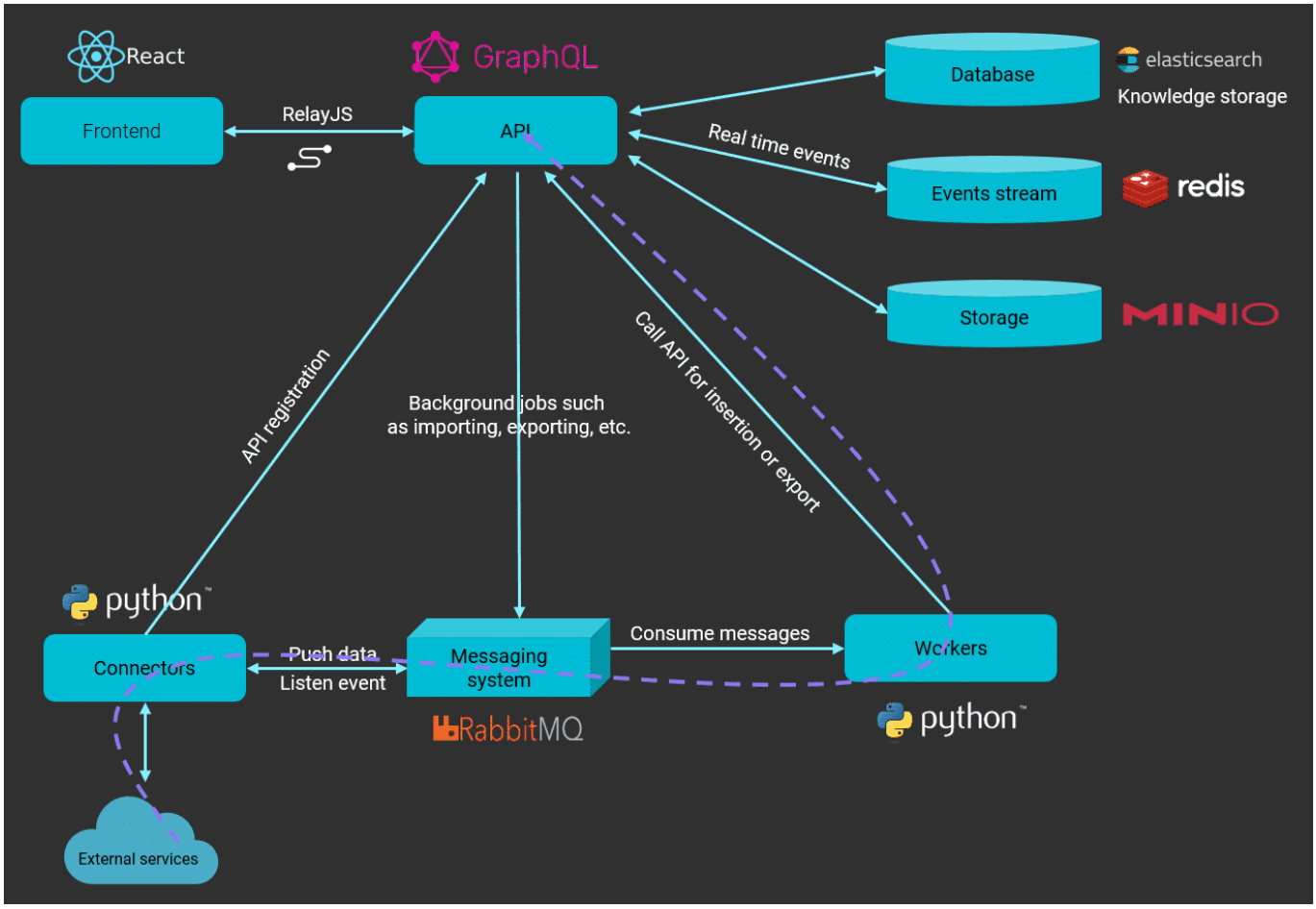
L'autre projet fait l'objet d'un développement plus soutenu. Sous le nom OpenCTI (Open Cyber Threat Intelligence), il vise à développer une plate-forme d'analyse de la cybermenace. L'ANSSI en est à l'origine et l'a mis en *open source* à la mi-2019.

Les liens entre l'ANSSI et Luatix sont multiples. L'agence fait notamment partie de la gouvernance de l'association. Et cette dernière a pour président Samuel Hassine, ancien directeur du

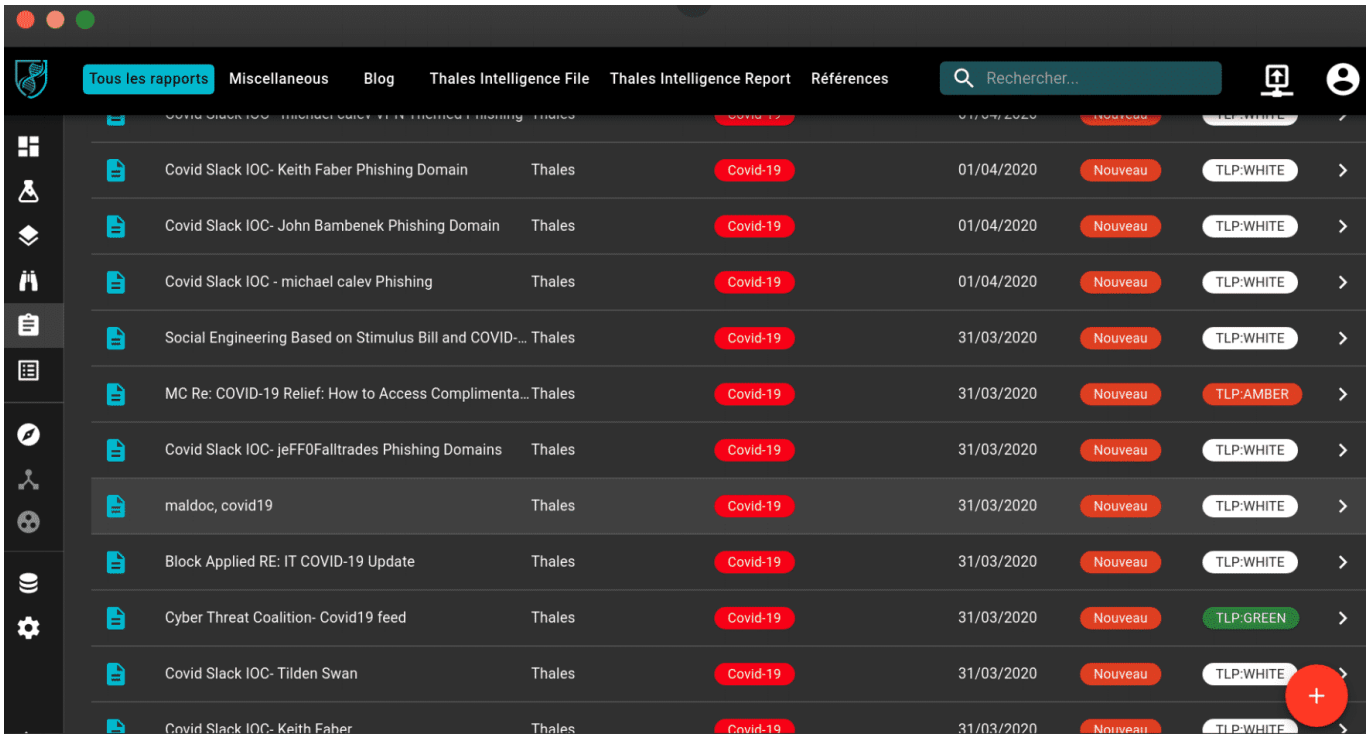
renseignement sur les menaces au sein de cette même ANSSI.

OpenCTI exploite un modèle de données basé sur le format STIX2. Mais on l'a enrichi avec Grakn (base de données de graphes) pour prendre en charge les relations imbriquées.

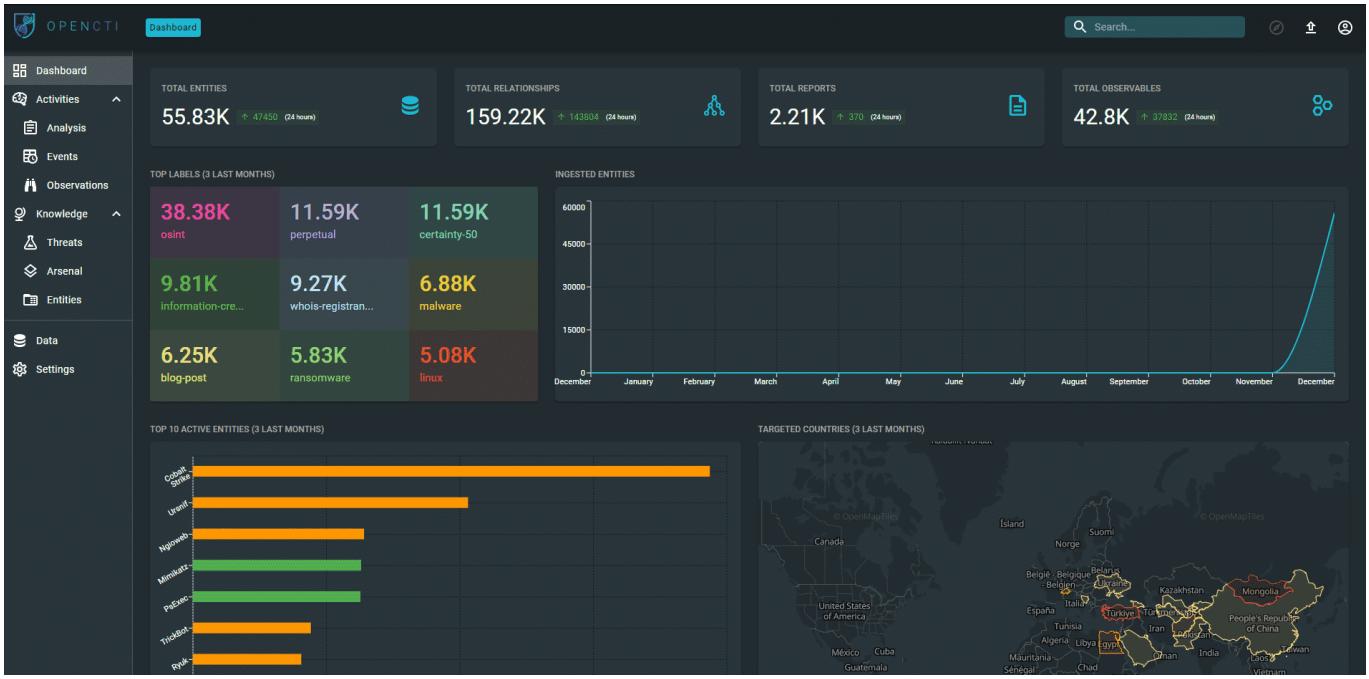
La plate-forme propose des fonctionnalités d'exploration et de corrélation (si A=B et B=C, alors A=C). Elle s'articule autour d'une API GraphQL. La jonction avec les services externes se fait au travers de connecteurs Python et du gestionnaire RabbitMQ.



Thales a déployé, voilà près d'un an, sa première instance de prod. Elle vise le secteur de la santé, dans le contexte de la crise Covid. Quant à l'ANSSI, elle a publié en début d'année sa « doctrine » d'utilisation, axée plus particulièrement sur les processus d'intégration de données.



Les [dernières mises à jour] d'OpenCTI ont, entre autres, renforcé l'isolation des accès et la visualisation de données. Prochains chantiers : le *pub/sub*, la *data science* ou encore la connexion aux SIEM.



À la mémoire d'Olympe

Luatix évolue sous l'égide de la [fondation] Citeum, aux côtés d'une autre association : Limeo. Celle-ci doit porter d'autres projets ouverts, mais dans les infrastructures cloud, la *data science* et la blockchain. Elle en compte pour le moment deux à son portefeuille. [D'une part], un packaging de déploiement local de Zotero (logiciel de gestion de références). [De l'autre], des outils de gestion et

de visualisation pour le *token* GHOST.

> *Hello world !! Introducing Citeum & our tool to manage @LuatixHQ and @LimeoHQ organizations !!. Discover why we will create Citeum and what are the next steps, to promote and develop Open Source apps and Open Standards !. https://t.co/WbulEGYJRl*
>
> *— Citeum (@CiteumHQ) January 8, 2021*

Limeo a existé bien avant Luatix. Son premier porte-drapeau fut Olympe. L'hébergeur associatif, financé par des dons et des partenariats, avait fermé ses portes en juin 2016, près de neuf ans après sa création.

> *#Olympe aux RMLL 2015 à #Beauvais ! Toujours plus d'ouverture et de softs Open Source, des surprise pour la rentrée. pic.twitter.com/gVppBpBgiH*
>
> *— Limeo (@LimeoHQ) July 4, 2015*

** Gatewatcher vient aussi de rejoindre la boucle.*

Illustration principale © Rawpixel.com – Adobe Stock