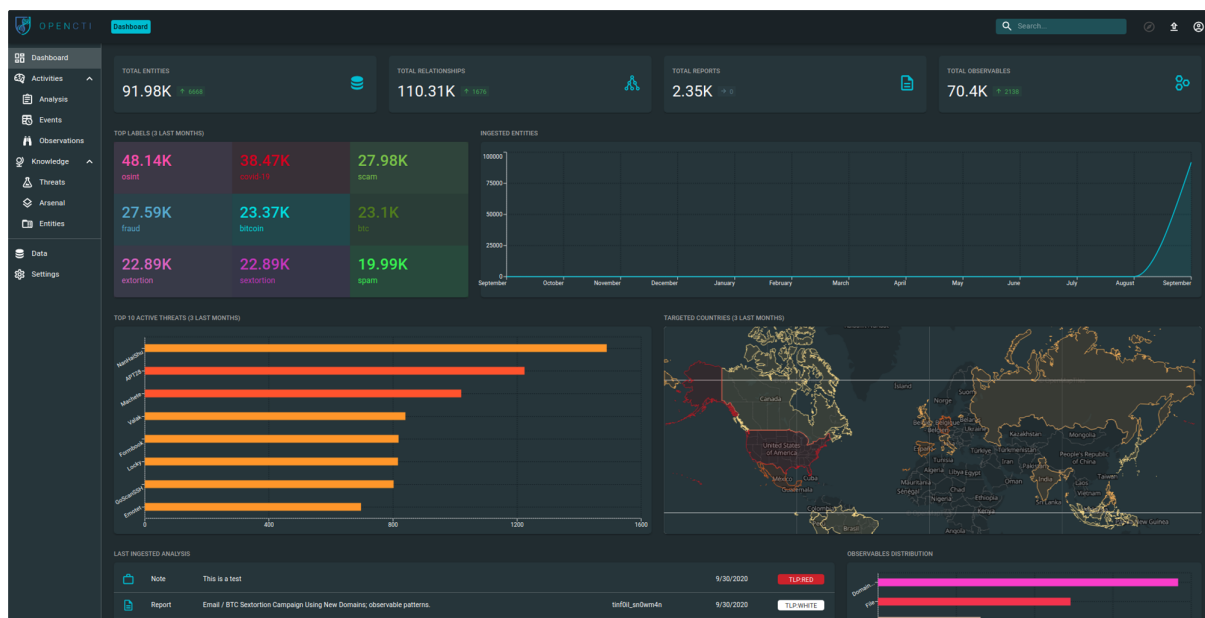




Introduction

OpenCTI is an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables. It has been created in order to structure, store, organize and visualize technical and non-technical information about cyber threats.

The data is structured using a knowledge schema based on the [STIX2 standards](#). It has been designed as a modern web application including a [GraphQL API](#) and an UX oriented frontend. Also, OpenCTI can be integrated with other tools and applications such as [MISP](#), [TheHive](#), [MITRE ATT&CK](#) etc.



Objective

The goal is to create a comprehensive tool allowing users to integrate technical information (such as TTPs and observables) and non-technical information (such as suggested attribution, victimology, sector of activity and localization), while linking each piece of information to its primary source (a report, a MISP event, etc.) and providing features such as links between each piece of information, first and last seen dates, levels of confidence and description fields. The tool is able to use the [MITRE ATT&CK framework](#) (through a [dedicated connector](#)) to help structure the data. The user can also chose to implement its own datasets.

Once data has been integrated within OpenCTI by the analysts, new relations [may be inferred](#) from existing ones to facilitate the understanding and the representation of this information. This allow the user to extract and leverage meaningful knowledge from the raw data.

OpenCTI not only allows [imports](#) but also [exports of data](#) under different formats (CSV, STIX2 bundles, etc.). [Connectors](#) are currently under development to accelerate interactions between the tool and other platforms.

Demonstration

If you wish to discover how the OpenCTI platform is working, a [demonstration instance](#) is available and open to everyone. This instance is reset every night and is based on open source reference data maintained by the OpenCTI developers.

Releases download

The releases are available on the [GitHub releases page](#). You can also access to the [rolling release package](#) generated from the master branch of the repository.

Installation

You have 3 options to install the OpenCTI platform, depending on your needs:

-  [Aucun accès](#)
-  [Using Docker](#)
-  [Manual deployment](#)

Community

Status & bugs

Currently OpenCTI is under heavy development. If you wish to report bugs or ask for new features, you can directly use the [GitHub issues module](#).

Discussion

If you need support or you wish to engage a discussion about the OpenCTI platform, feel free to join us on our [Slack channel](#). You can also send us an email to contact@opencti.io.

About

OpenCTI is a product powered by the collaboration of the [French national cybersecurity agency \(ANSSI\)](#), the [CERT-EU](#) and the [Luatix](#) non-profit organization.

 Next section, the  [Architecture](#) page.