Cyber Threat Intelligence

Detects, classifies and helps mitigate cyberspace threats to an organisation's IT assets

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

The purpose of the tool is to continuously expose the earliest indication of cyber risks to an organization's network from deep and dark web fora and markets, as well as private messaging groups.
Without the tool, analysts will have to cope with a lot of manual work, regarding:

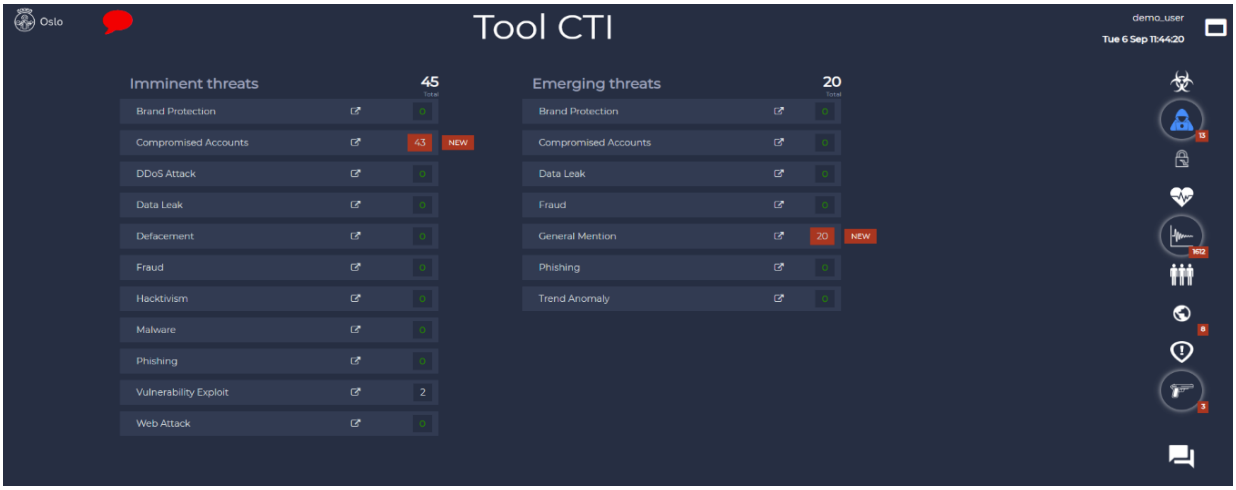
- Collecting domain, IP and third-party data
- Indexing, tagging and metadata analysis of collected data
- Extracting relevant data and restructuring and packaging for data storage in a database maintained by the tool provider (Cybersixgill)

With the tool, you are able to:

- Receive and use a queue of asset-based alerts
- Conduct offline and discreet investigation of ongoing threats and events in cyberspace
- Receive contextual information of – and mitigate – the threats to the organization (who, where, what)

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: IT specialists tasked with giving Security Operations Center operators and other stakeholders (government officials, senior level management, etc.) early notice of possible threats posed to the organization's assets.
- **What are the critical situations for deployment**: Regular: scans would typically be performed daily. The tool provides comprehensive insights into the nature and source of cyber threats, and as these can emerge rapidly it essential to keep up to date.



HOW DOES IT WORK?

There are 3 main steps:

1. **Data collection** – Finding all relevant sources, sign-in closed access forums and groups, and inquire the data (by crawling).
2. **Data processing and analysis** – The tool runs several processes on every newly collected item: indexing, enrichment, tagging, entity extraction, metadata, restructuring and saving the data into a database.
3. **Data lake query** – Automated and manual processes are running on our extensive database of cyber incidents and threat actors' activity.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.