USE CASE/OPENCTI

Filigran

Intelligence-driven defense against disinformation

For the Threat Intelligence community, defending against disinformation and Foreign Information Manipulation & Interference (FIMI) requires efficient knowledge sharing.

Filigran Capabilities

OpenCTI is one of the most advanced and effective solutions for combating disinformation, widely used by organizations around the world today.

EFFORTLESS DATA INGESTION

The existing process of importing disinformation data from scattered sources is often manual and time-consuming, resulting in wasted time, analyst fatigue, reduced coverage, and delayed response to emerging threats.

OpenCTI streamlines this process by leveraging established CTI techniques. Features like **CSV mapper** and **bulk creation** allow defender teams to efficiently import diverse datasets from spreadsheets or databases. **Modeling on OpenCTI** transforms unstructured information into structured data thanks to various entities. Analysts can extract more valuable insights semi-automatically from reports while saving time from repetitive tasks.

UNIFIED DATA CONSOLIDATION

Disinformation data often suffers from duplication and inconsistencies caused by overlapping reports and repeated imports.

RECURRING PAIN POINTS

FRAGMENTED DATA SOURCE

Scattered data sources hinder effective modeling of disinformation threats and incidents

OVERWHELMING DATA VOLUME

The large volume of data obscures trends and relationships among actors, targets, and campaigns

LIMITED COLLABORATION ACROSS STAKEHOLDERS

Sharing insights and experiences is difficult when stakeholders use varied research approaches and methodologies

SILOED RESPONSES

Disinformation responses are often isolated and uncoordinated, weakening collective efforts against disinformation

OpenCTI resolves these issues with **automatic de-duplication** and offers **manual merge capabilities**, ensuring clean and unified datasets. By adhering to standards like **DISARM** and **STIX**, OpenCTI guarantees the consistency across datasets, reducing friction in analysis and sharing while fostering better collaboration.

ENHANCED DATA ANALYSIS

It is struggle for defenders to interpret vast amounts of data. OpenCTI addresses this with **graph visualizations**, allowing users to map entities, observables, and relationships in disinformation campaigns.

Customizable dashboards and the **investigation module** further allow users to pivot on any knowledge, enabling comprehensive exploration and analysis of connections between entities and relationships. By making critical insights both accessible and actionable, OpenCTI significantly accelerates decision-making.

SEAMLESS COLLABORATION AND SHARING

Collaboration is essential in combating disinformation, yet sharing actionable intelligence efficiently across teams and organizations remains a challenge.

OpenCTI supports various sharing mechanisms including TAXII, Live stream, CSV Feed, connectors... It automatically structures and categorizes all information, ensuring clarity and consistency.

In addition, **the dashboards on OpenCTI are sharable across teams and organizations**, even with external collaborators who do not have an account. This gives researchers and analysts the flexibility to present investigation results, enabling effortless cooperation and wide-scale intelligence sharing.

Use case outcomes

OpenCTI enables the defender community to use threat intelligence techniques to better manage and combat against disinformation, especially FIMI threats:

CLEAR VISION OF FIMI TRENDS

OpenCTI ensures quality datasets and knowledge subsystems as well as the ability to produce accurate key indicators over time.

CONCISE CATEGORIZATION OF FIMI DATA & ANALYSIS

Frameworks like STIX 2.1 and DISARM ensure structured data format which facilitates the sharing of threat intelligence.

KNOWLEDGE GRAPH AND RELATIONSHIPS

Easily visualize activity clusters and common characteristics.

© Filigran 2024 All rights reserved.