Cyber-threat intelligence (CTI) and OSINT 3

Group 10
Lê Viết Tài Mẫn – 20521593
Hoàng Thanh Lâm – 20521513
Vũ Hoàng Thạch Thiết – 20521957
Phạm Văn Xuân – 20522184

01.Context and overview of ETIP

Context:

- OSINT: (Open Source Intelligence) data is security data collected from available open sources.
- TIPs (Threat Intelligence Platforms). These platforms help companies gather, link, and analyze security data from a variety of sources to help build defenses.

Problem:

- Unstructured data from multiple natural sources. TIPs require data to be filtered and processed before being analyzed and shared.

Propose:

- ETIP architectures secure data collected from multiple sources and links the data.
- Thereby diversifying security data, building a defense system.

Overview:

- ETIP (Enriched Threat Intelligence Platform)
- ETIP extends the ability to import and share information of internal detection and monitoring
- A solution to improve the quality assessment of security data.
- A process of linking related security data from multiple internal detection sources and monitoring
- Calculate threat score for each Indicator of Compromised (IoC)
- Deploy the platform
- Security data is leveraged from OSINT and collected from various sources such as firewalls, IDS,…
- This information is analyzed to build defense mechanisms.

02.Architecture of ETIP

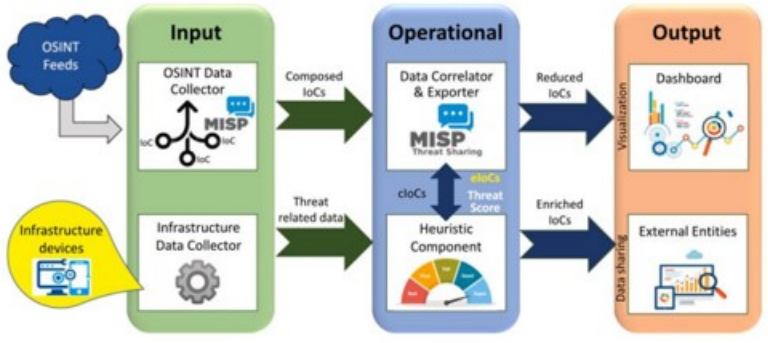
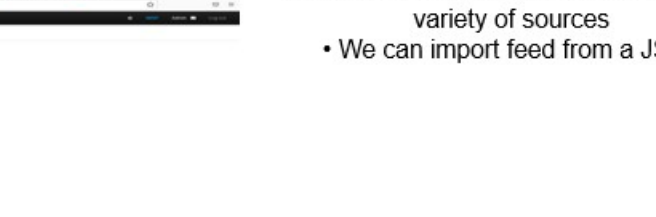


Fig. 1. The Enriched Threat Intelligence Platform architecture.

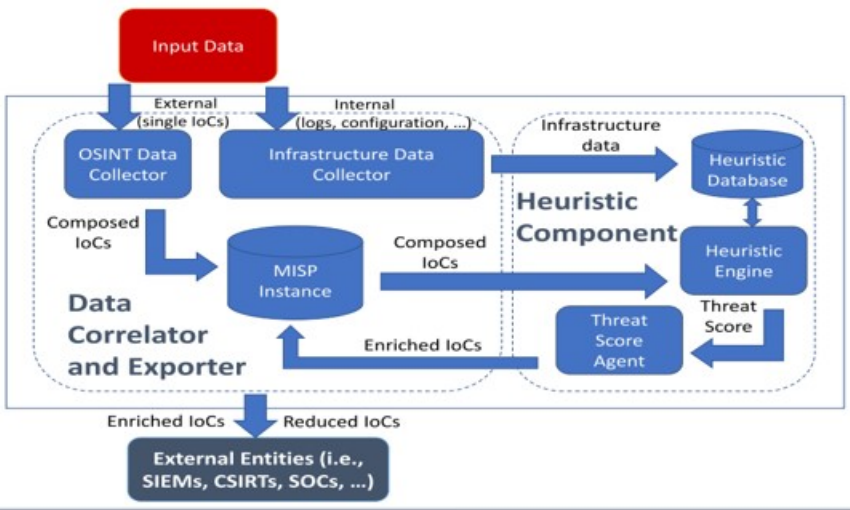
03.Architecturaldetails

Input Module

OSINT Data Collector



Operation Module



Output Module

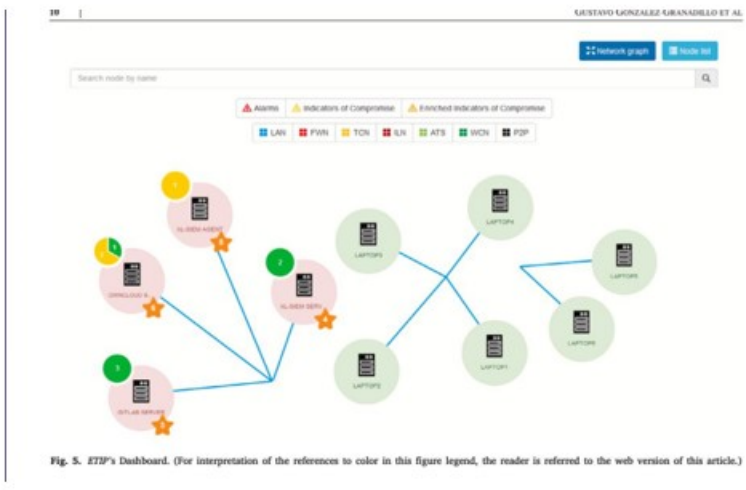
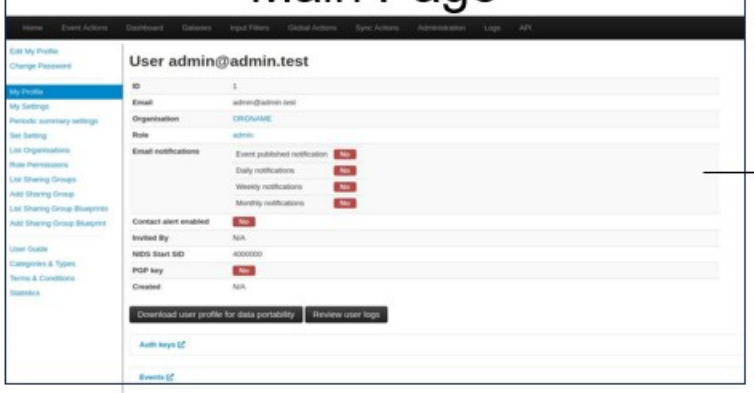


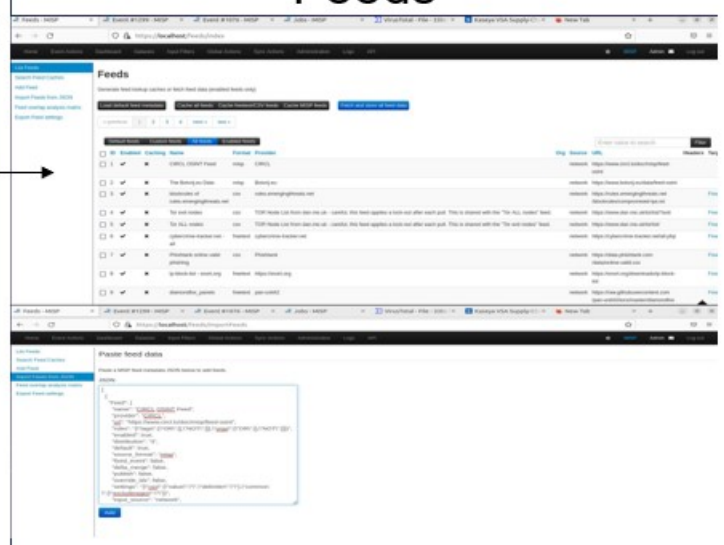
Fig. 5. *ETIP*'s Dashboard. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

04.Demo

Main Page

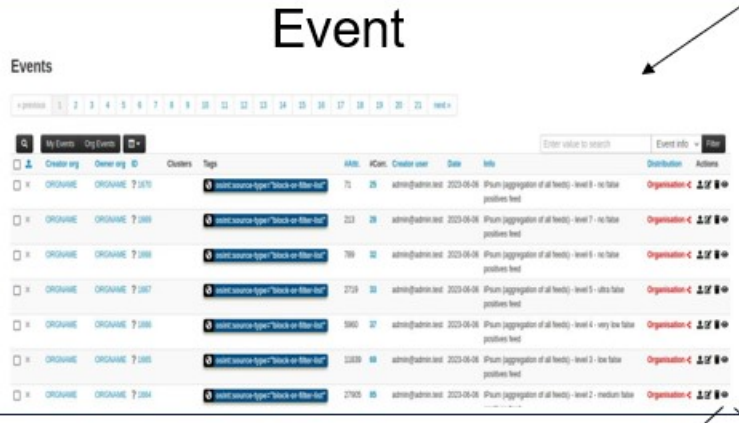


Feeds



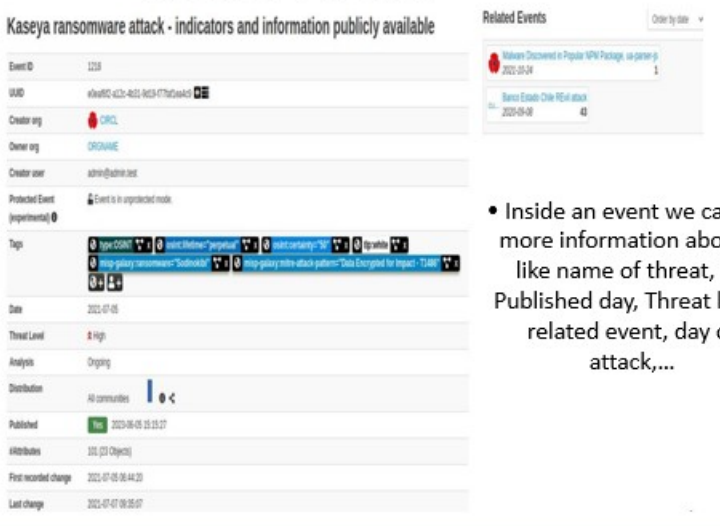
- Information sources that provide data on threats and cybersecurity metrics
- These feeds are typically created and maintained by cybersecurity organizations, security service providers, or the cybersecurity community
- Provide information about events, identifiers and information related to threats, including malicious IP, malicious domain, malicious code, attack signature, APT. This information is collected from a variety of sources
- We can import feed from a JSON

Event



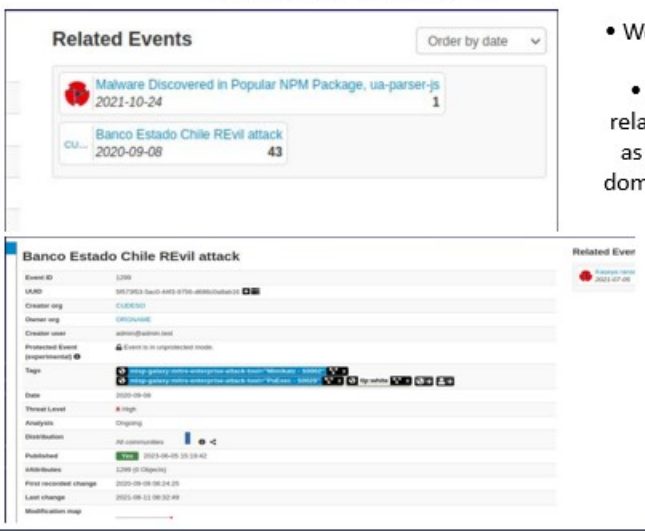
- Event contain information related to network security factors and indicators, such as attacks malicious code, attacker information, malicious code sample, attack campaigns,...
- Taken from feeds we provided, containing meta data about known ransomware, malware,...
- MISP categorizes event for easier analysis
- Creator org: Here we can see who is responsible for collecting all that data and putting it in to MISP
- Tags: Used to categorize and tag events to enhance search, filtering and sorting

Inside Event



- Inside an event we can see more information about it like name of threat, ID, Published day, Threat level, related event, day of attack,...

Inside Event



- We can see attack event that related to this attack
- Maybe this attack event related to another event such as using common malicious domains, common commands, similar payloads,...