ETIP

An Enriched Threat Intelligence Platform for improving OSINT correlation, analysis, visualization and sharing capabilities

Ngữ cảnh:

* OSINT ( Open Source Intelligence) data là dữ liệu bảo mật thu thập được từ những nguồn mở có sẵn.
* TIPs (Threat Intelliegence Platforms). Những platform này giúp cho các công ty tập hợp, liên kết và phân tích những dữ liệu bảo mật từ nhiều nguồn khác nhau để hợ trỗ xây dựng hệ thống phòng thủ.

Vấn đề:

* Nhưng những dữ liệu không có kiến trúc (unstructured data) từ nhiều nguồn tự nhiên. TIPs yêu cầu dữ liệu phải được lọc, xử lý trước khi được phân tích và chia sẻ.

Đề Xuất:

* ETIP kiến trúc hoá được dữ liệu bảo mật được thu thập từ nhiều nguồn và liên kết hoá được dữ liệu
* Từ đó đa dạng hoá được dữ liệu bảo mật, xây dựng hệ thống phòng thủ.

Tổng quan:

Nội dung chính của EITP

* ETIP mở rộng khả năng nhập (import) và chia sẻ thông tin của internal detection và hệ thống giám sát.
* Một giải pháp để nâng cao việc đánh giá chất lượng những dữ luệ bảo mật.
* Một tiến trình liên kết các dự liệu bảo mật có liên quan đến nhau từ nhiều nguồn internal detection và hệ thống giám sát.
* Tính toán threat score cho từng Indicator of Compromised (IoC)
* Triển khai platform

Kiến trúc ETIP (Enriched Threat Intelligence Platform)

* Các dữ liệu bảo mật được tận dụng từ OSINT và thu thập từ các nguồn khác nhau như firewall, IDS, IPS,… dữ liệu được liên kết, đánh giá và được thể hiện như là một threat score
* Những thông tin này được phân tích để xây dựng cơ chế phòng thủ.

Các thuật ngữ chính:

* Indicator of Compromise: là dữ liệu liên quan đến bảo mật. Dữ liệu này được thư thập được từ system log hoặc file, và nó xác định có khả năng độc hại đến mạng và hệ thống
* Composed Indicator of Compromise:

Là sự liên kết, tích hợp các dự liệu liên quan từ các nguồn khác nhau.

* Enriched Indicator of Compromise:

Kết quả của bước này là hán threat score

* Reduced Indicator of Compromise:

Nhưng thông tin liên quan nhất đến bảo mật được triết xuất từ eIoC. Vì nhưng thông tin dư thừa lớn và khó trực quan

Kiến trúc của ETIP

Diagram

Description automatically generated with medium confidence

Có 3 modules:

* Input module:

thu thập security events (OSINT feeds và infrastructure data), cho ra kết quả IoCs và threat data

* Operational module:

dữ liệu từ OSINT và threat data được đối chiếu và đánh giá

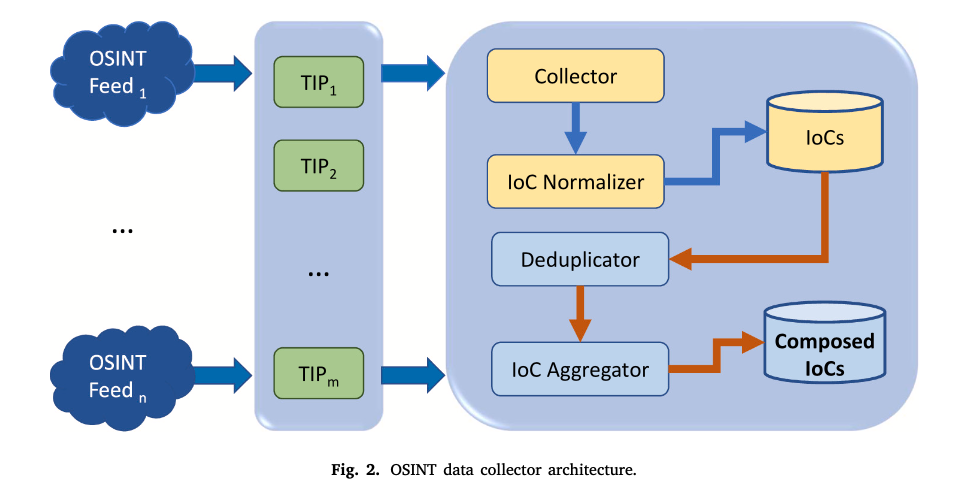
* Output module:

Cho ra kết quả trực quan và chia sẻ những dữ liệu bảo mật.

Input module:

Được chia ra 2 loại:

1. OSINT data collector



+ OSINT Feeds: Thành phần này được cấu hình từ nhiều nguồn OSINT về các sự kiện bảo mật ( cyber-attacks, malware domains, vulnerabilty exploitation, IP blacklist)

+ TIPs: Các TIPs khác nhau thu thập nhiều nguồn OSINT khác nhau, tăng sự đa dạng.

+ collector: Đầu ra của các TIP khác nhau, dưới dạng một IOC

+ IOC normalizer: thành phần IOC được thu thập với nhiều dạng format khắc nhau. Cần đưa về một format, và lưu trữ trong một database. MISP chuẩn hoá quá trình này và đưa về dạng MISP format.

+ Deduplicator: Do các IOC có thể giống nhau trong database, nên có thể deduplicate.

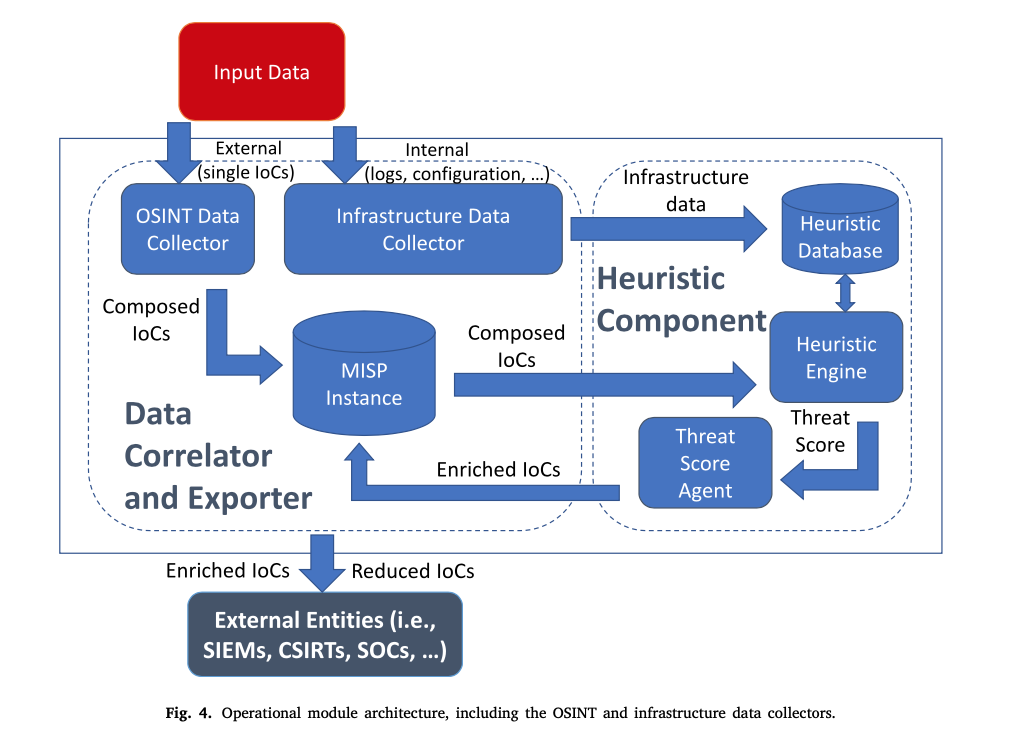
+ IoC Aggregator: Tích hợp các IoC lại với nhau. Các IoC có thể khác nhau nhưng lại chứa những thông tin liên quan. Tích hợp lại và tạo thành một IoC mới ( new composed IoC)

1. Infrastructure data collector

+ Thu thập dữ liệu từ system log như hashes, signature, Ips, domains, URLs). Có thể lấy từ những nguồn như ( event logs, system logs, server logs, Web logs, application logs từ firewall, ids, honeypots, security sensor)

Operation module

Module này dựa vào MISP, có chức năng liên kết các thông tin với nhau.



Gồm 2 thành phần chính

+ Data correlator & Exporter: là một instance của MIPs, có chức năng liên kết thông tin với nhau.

+ Heuristic component: thực hiện tự phân tích ( heuristic analysis), với mục đích tính toán Threat Score.

Output module

* Có chức năng chính là hiển thị những thông tin IoC ở dạng graph

Dashboard – graphical representation

A screenshot of a computer

Description automatically generated with medium confidence

Figure 5 thể hiện các node. Các node gồm alarm và IoC tương tự

Phần alarm bao gồm những số lượng issues, IP source và IP destination, và bản miêu tả của issue.

Phần IoC bao gồm số lượng lỗ hổng được phát hiện, threat score, bản miêu tả lổ hổng và các application liên quan.

Phần bên phải của dashboard gồm các nodes của infastructure.

Đánh giá điểm số mối đe doạ ( Threat Score Evaluation)

* Threat score evaluation là một phần của heuristic component có sử dụng threat score function.
* Giai đoạn phân tích đánh giá threat score evaluation bao gồm:

+ Source Indentification: xác định nguồn cung cấp thông tin từ đâu ( như là security logs, databases, report data, OSINT data sources,…)

+Heuristic Identification: Xác định những features từ input data. Những features (như là vulnerabilites, events, faults, errors,…). Những ví dụ heuristics: CVE( common vulnerability exposure), IP source/destination, port source/destination, timestamp

+ Threshold definition: định nghĩa một mức ngưỡng threshold ( e.g 0-5) cho tất cả input data nếu data có chứa CVE

+ Score Computation: Tính toán score

+ Training period: một tập hợp test được kiểm tra trong quá trình training để đánh giá cho việc score computation

+ Engine Calibration: để giảm độ biến thiên (false positive, false negative)

+ Final test: kiểm tra một lần nữa.

Threat Score Function

Heuristic-based threat score bao gồm cả những score riêng lẻ để thể hiện cho mức độ được ưu tiên và mức độ liên quan đến bảo mật từ OSINT/ infrastructure

* Weighted Mean là hàm được lựa chọn để tính toán threat score

Có những ưu điểm sau:

+ đơn giản và dễ

+ tránh những kết quả không xác định.

+ mỗi một score có một weight riêng dựa vào source và những thông tin liên quan.

Hàm Threat Score Function

A picture containing font, white, graphics, typography

Description automatically generated

Threat Score = Tổng tất cả individual heuristic value (Xi) sau đó x với weight factor (Pi ). Weight được xem như là criteria (relevace, accuracy, timeliness, variety).

Cp là completeness parameter

Cp = A picture containing text, font, white, typography

Description automatically generated

Kết quả của threat score từ 0 <= TS <= 5

0 <= TS <= 1: very  low level of priority

1 <= TS <= 2: a low level of priority

2 <= TS <= 3: a medium level of priority

3 <= TS <= 4: a high level of priority

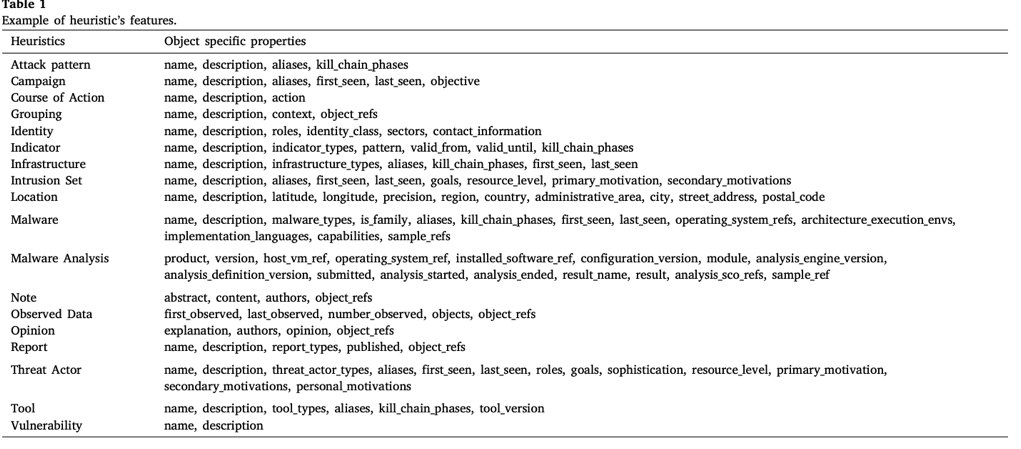
4 <= TS <= 5: a very high level of priority

Heuristic features and values

(phân tích Xi)

Heuristic feature Xi để thể hiện dưới dạng:

* Attack pattern: thông tin miêu tả đe doạ tấn công mục tiêu ( types of tatics, techniques/ procedures describing threat attempt to compromise targets)
* Identiy: xác định đối tượng đe dọa
* Indicator: những dấu hiệu để nhận diện hành vi độc hại
* Malware: malicous code
* Tool: những chương trình hợp lệ có thể bị lợi dụng để tấn công bảo mật
* Vulnerability: những sai sót trong chương trình có thể bị tấn công trực tiếp



Ví dụ: Những properties cụ thể cho từng heuristic feature

A picture containing text, screenshot, font, document

Description automatically generated

Một ví dụ cụ thể heuristic’s feature: vulnerability

Weighting criteria

Thành phần thứ hai của threat score là weight Pi

A picture containing text, receipt, font, screenshot

Description automatically generated

A Case study: MySQL server vulnerability

A picture containing text, screenshot, font, receipt

Description automatically generated

Đánh giá các thành phần của ETIP và phân tích kết quả

* Để hình thành threat score của một Composed IoC là bao gồm kết hợp nhiều threat score của nhiều IoC khác nhau.
* Giai đoạn này bao gồm: collecting phase, aggregating phase, sharing phase, TS evaluation phase