XÂY DỰNG ĐỒ THỊ TRI THỨC DỰA TRÊN HỌC MÁY TỪ THÔNG TIN ĐE DỌA MẠNG ĐỂ XÁC ĐỊNH NGUỒN GỐC APT

Tô Thị Mỹ Âu[1]

[1] Trường ĐH Công Nghệ Thông Tin

What ?

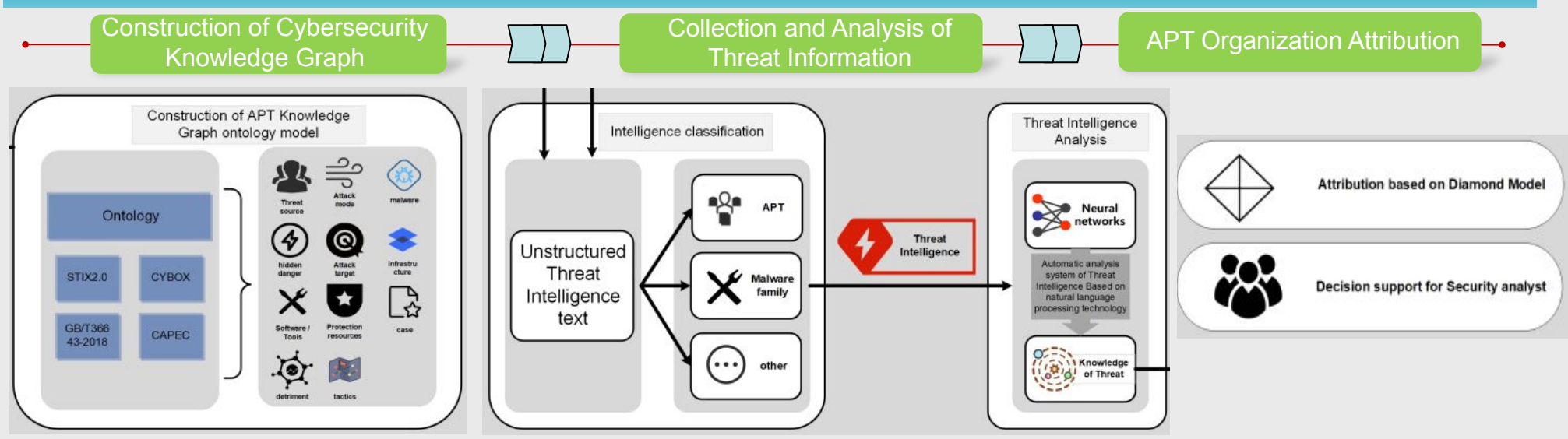
Giới thiệu một khung đồ thị tri thức từ thông tin mối đe dọa mạng để xác định nguồn gốc APT, trong đó có:

- Đề xuất một phương pháp tự động hóa trích xuất và phân loại các thực thể mạnh mẽ.
- Tổng hợp cơ sở dữ liệu CTI từ nhiều nguồn khác nhau.
- Đánh giá một số phương pháp trích xuất dữ liệu.

Why ?

- Tống công APT ngày càng trở nên tinh vi hơn, việc xác định nguồn gốc mối đe dọa là một chiến lược phòng thủ quan trọng để chống lại các mối dọa APT. Việc xác định nguồn gốc APT bằng phân tích các nguồn thủ công khác nhau không mang lại hiệu quả cao. Vì vậy, phương pháp trích xuất tự động để xác định nguồn gốc APT là một vấn đề đang được quan tâm trong lĩnh vực an ninh mạng.
- Hầu hết các nghiên cứu đều tập trung vào các **dữ liệu có cấu trúc hơn** là các **nguồn mở không cấu trúc**.

Overview



Description

1. Construction of Cybersecurity Knowledge Graph

- Cấu trúc ontology tóm tắt một tập hợp các quan hệ ngữ nghĩa phù hợp cho việc phân tích tổ chức APT. bằng cách trích xuất các kỹ thuật phân tích và các mối quan hệ logic đầu mối được đề cập trong báo cáo APT.

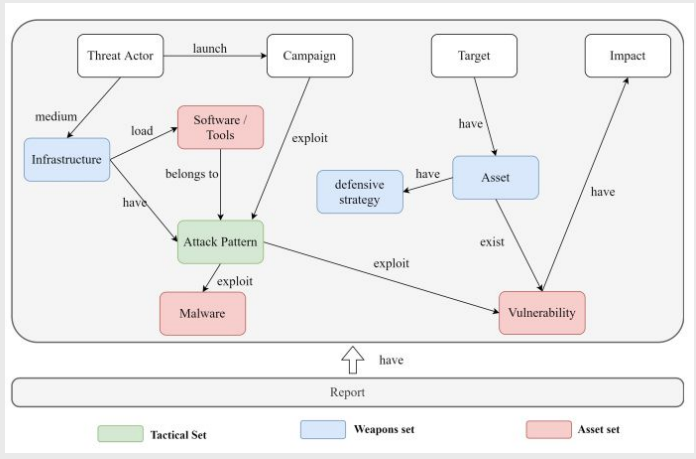


Figure 1. Cấu trúc ontology.

2. Collection and Analysis of Threat Information

- Xây dựng nguồn thông tin có khả năng mở rộng.
- thông tin tình báo, dữ liệu không liên quan sẽ được lọc.
- Loại thông tin về mối đe dọa được được trích xuất tự động bằng cách kết hợp cơ sở tri thức và Công nghệ NLP.

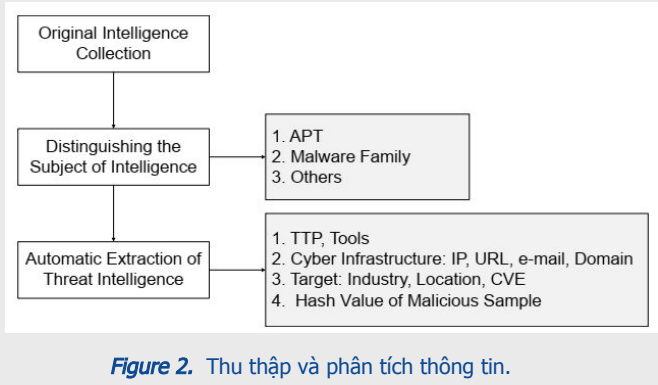


Figure 2. Thu thập và phân tích thông tin.

3. APT Organization Attribution

- Sử dụng Diamond model để ghi lại nguồn gốc APT để tạo ra nhiều thông tin tình báo hơn.
- Mô hình hỗ trợ xây dựng chiến lược năng lực răn đe và phòng thủ trong an ninh mạng.
- Diamond model mô tả đối thủ sử dụng cơ sở hạ tầng khả năng triển khai cho nạn nhân, trong 4 yếu tố cơ bản: **Adversary**,**Victim**, **Capability**, **Infrastructure**.

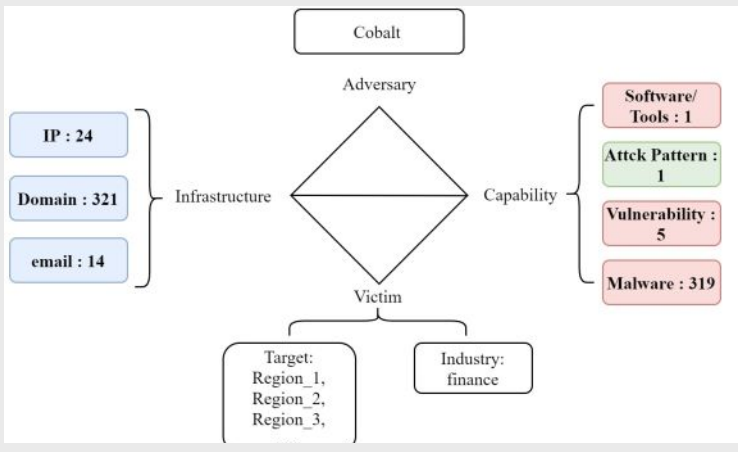


Figure 3. Xây dựng nguồn gốc APT.

NII

Tô Thị Mỹ Âu – Trường Đại học Công Nghệ Thông Tin
TEL : 0357181661 Email : auttm.18@grad.uit.edu.vn