GIÁM SÁT & ỨNG PHÓ SỰ CỐ AN TOÀN MẠNG

Chương 2. Hệ thống giám sát an toàn thông tin mạng

1. Thu thập dữ liệu
2. Phân tích dữ liệu
3. Tìm kiếm các mối đe dọa

1. Thu thập dữ liệu
2. Phân tích dữ liệu
3. Tìm kiếm các mối đe dọa

Thu thập dữ liệu

❑ Chuyên gia phân tích dữ liệu giỏi cần biết rõ:

- Các nguồn dữ liệu họ có
- Nơi lấy được dữ liệu
- Cách thu thập dữ liệu
- Lý do thu thập
- Những gì có thể làm với dữ liệu đó

Thu thập dữ liệu

- Thu thập và phân tích dữ liệu là một công việc vô cùng quan trọng và mất nhiều thời gian.
- Nhiều tổ chức thường không hiểu đầy đủ về dữ liệu của họ.
- Không có cách tiếp cận có cấu trúc để xác định các nguy cơ có thể đến với tổ chức.
- Hậu quả:
  - Sử dụng dữ liệu tùy biến có sẵn để xây dựng chương trình > Lượng dữ liệu quá lớn > Không đủ tài nguyên > Lọc dữ liệu bằng nhân công hoặc các công cụ phân tích không hiệu quả.

Applied Collection Framework

- Là khung làm việc được xây dựng để làm giảm sự phức tạp của việc thu thập dữ liệu.
- Giúp tổ chức đánh giá các nguồn dữ liệu cần tập trung trong quá trình thu thập dữ liệu.
- Gồm bốn giai đoạn:

Xác định nguy cơ

- Thay vì chỉ xác định các nguy cơ chung, cần xác định các mối nguy cơ cụ thể vào mục tiêu của tổ chức
- Các nguy cơ thường tác động đến:

- Tính bảo mật
- Tính toàn vẹn
- Tính sẵn sàng

- Từ nguy cơ đã xác định > thấy được các kỹ thuật và công nghệ cần sử dụng để giải quyết

- Máy chủ web (web server)
- Máy chủ cơ sở dữ liệu (database server)
- Máy chủ lưu trữ tệp tin (file server),...

Định lượng rủi ro

- Khi xác định được một danh sách các nguy cơ, cần xác định xem nguy cơ nào cần được ưu tiên
- Thực hiện bằng cách tính toán rủi ro gây ra bởi các nguy cơ tiềm ẩn:

Ảnh hưởng (I) * Xác suất (P)=Rủi ro (R)

- Ảnh hưởng là tác động của nguy cơ đến tổ chức
- Xác suất là khả năng nguy cơ xuất hiện
- Mức độ rủi ro mà nguy cơ gây ra đối với sự an toàn của mạng

Xác định nguồn dữ liệu

- Đi từ nguy cơ có hệ số rủi ro cao nhất, và xem xét khả năng nguy cơ có thể bị khai thác
- Ví dụ, để kiểm tra nguy cơ tấn công máy chủ lưu trữ tệp tin, cần:
  - Xác định cấu trúc của máy chủ
  - Vị trí trên mạng
  - Người có quyền truy cập
  - Đường dẫn mà dữ liệu đi vào
- Dựa vào đó để kiểm tra cả hai nguồn dữ liệu dựa trên mạng và dựa trên máy chủ

Ví dụ

- Dựa trên mạng:
  - Máy chủ lưu trữ tệp tin VLAN – Dữ liệu bắt gói tin
  - Máy chủ lưu trữ tệp tin VLAN – Dữ liệu phiên
  - Máy chủ lưu trữ tệp tin VLAN – Dữ liệu cảnh báo IDS
  - Upstream Router – Dữ liệu nhật ký tường lửa
- Dựa trên máy chủ:
  - Máy chủ lưu trữ tệp tin – Dữ liệu nhật ký sự kiện OS
  - Máy chủ lưu trữ tệp tin – Dữ liệu cảnh báo virus
  - Máy chủ lưu trữ tệp tin – Dữ liệu cảnh báo HIDS

Chọn lọc dữ liệu

- Liên quan đến các bước kỹ thuật chiều sâu và cần phải xem xét tất cả các nguồn dữ liệu riêng để xác định giá trị của nó.
  - Ví dụ: Chi phí cho việc lưu trữ, xử lý và quản lý một nguồn dữ liệu có thể lớn hơn nhiều so với giá trị mà nó mang lại, thì đó không phải là nguồn dữ liệu tốt
- Cần phân tích chi phí/lợi ích của các nguồn dữ liệu
  - Tài nguyên phần cứng, phần mềm, nhân công, việc tổ chức và lưu trữ dữ liệu,…
  - Số lượng dữ liệu và thời gian lưu trữ dữ liệu
  - Cần phải giảm tối thiểu chi phí lưu trữ dữ liệu và tăng tối đa độ quan tâm về dữ liệu hữu ích dùng trong việc phân tích

Chọn lọc dữ liệu

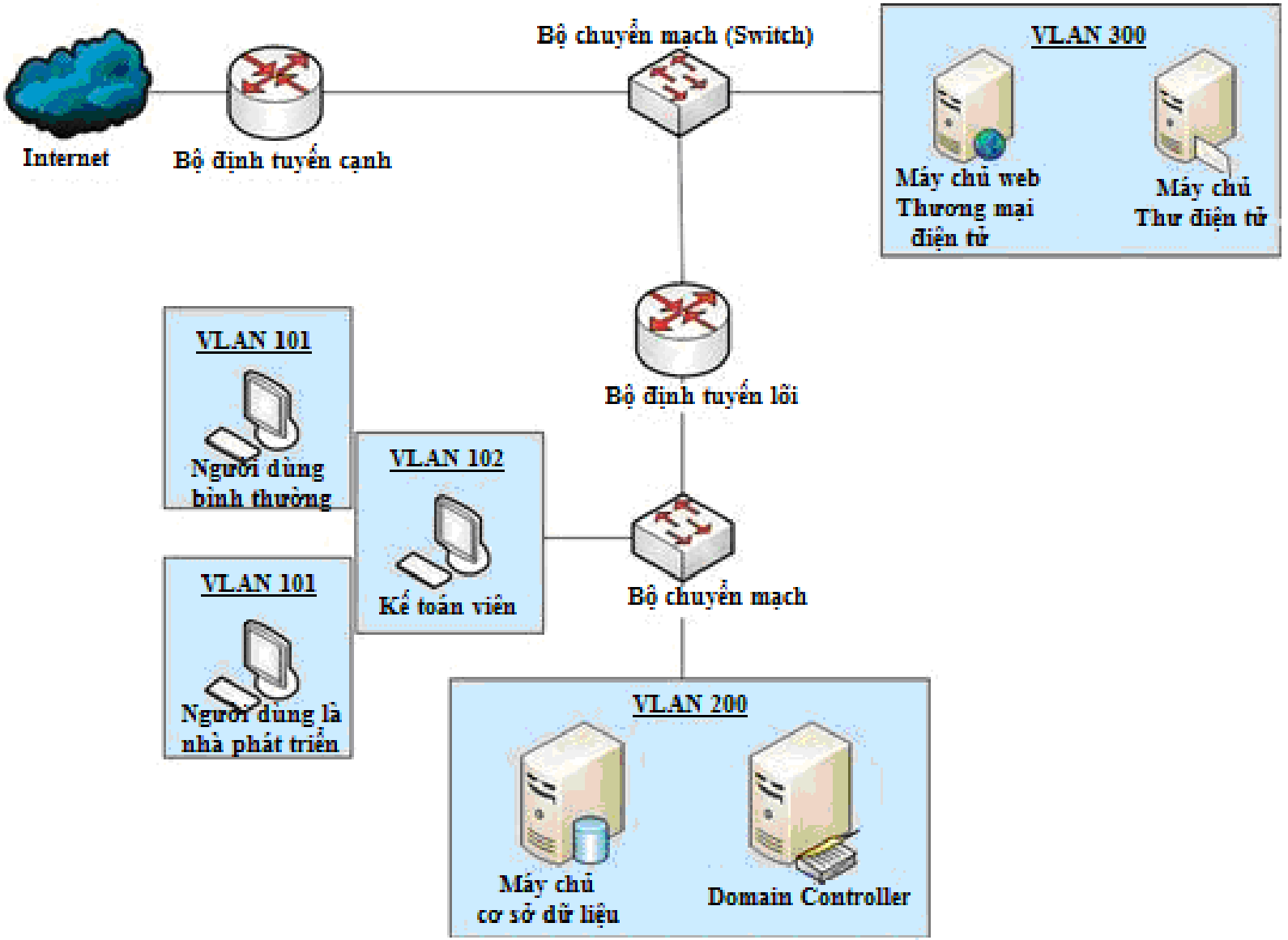
- Trên cơ sở đó, xây dựng cơ sở hạ tầng thích hợp cho việc thu thập dữ liệu.
- Dữ liệu liên tục được thu thập, được sử dụng cho phát hiện xâm nhập và phân tích theo sự phát triển hệ thống mạng của tổ chức, và sẽ luôn cần phải xem xét lại chiến lược thu thập dữ liệu.

Xây dựng SIEM

- Thiết lập một hệ thống SIEM cho cửa hàng bán lẻ trực tuyến, sử dụng trang web. Toàn bộ doanh thu là từ việc bán hàng qua trang web
- Sơ đồ mạng gồm:

- Máy chủ truy nhập công khai trong một DMZ, nằm phía trong bộ định tuyến
- Người dùng và máy chủ mạng nội bộ ở các VLAN khác nhau bên trong bộ định tuyến lõi
- Chưa có bất kỳ cảm biến nào do chưa xác định được nhu cầu thu thập dữ liệu

Xây dựng NSM


Internet
Bộ định tuyến cạnh
Bộ chuyển mạch (Switch)
VLAN 300
Máy chủ web
Thương mại
điện tử
Máy chủ
Thư điện tử
Bộ định tuyến lõi
VLAN 101
Người dùng
bình thường
VLAN 102
Kế toán viên
VLAN 101
Người dùng là
nhà phát triển
Bộ chuyển mạch
VLAN 200
Máy chủ
cơ sở dữ liệu
Domain Controller

Bước 1 – Xác định nguy cơ

- Tính bảo mật: trang web thu thập và lưu trữ các thông tin của khách hàng trong CSDL.
  - Có thể bị tấn công vào CSDL qua trang web
- Tính sẵn sàng: Kẻ tấn công có thể thực hiện một cuộc tấn công làm cho trang web thương mại điện tử không tiếp cận được với khách hàng
  - Tấn công từ chối dịch vụ
- Tính toàn vẹn: Kẻ tấn công có thể thực hiện một cuộc tấn công trong đó cho phép họ dùng ứng dụng web một cách không có chủ ý
  - Ví dụ: mua sản phẩm mà không có giao dịch về tiền

Bước 2 – Định lượng rủi ro

Nguy cơ	Ảnh hưởng	Xác suất	Rủi ro
Đánh cắp thông tin thẻ tín dụng của khách hàng – tấn công ứng dụng web	4	4	16
Đánh cắp thông tin thẻ tín dụng của khách hàng – tấn công người dùng nội mạng	4	2	8
Làm gián đoạn các dịch vụ thương mại điện tử – DoS	4	2	8
Làm gián đoạn các dịch vụ thương mại điện tử – tấn công tài sản bên ngoài	5	3	15
Làm gián đoạn các dịch vụ thương mại điện tử – tấn công tài sản nội mạng	5	2	10
Sử dụng dịch vụ thương mại điện tử không chủ ý – tấn công ứng dụng web	2	4	8
Sử dụng dịch vụ thương mại điện tử không chủ ý – tấn công tài sản nội mạng	2	1	2

Bước 2 – Định lượng rủi ro

Nguy cơ	Ảnh hưởng	Xác suất	Rủi ro
Đánh cắp thông tin thẻ tín dụng của khách hàng – tấn công ứng dụng web	4	4	16
Đánh cắp thông tin thẻ tín dụng của khách hàng – tấn công người dùng nội mạng	4	2	8
Làm gián đoạn các dịch vụ thương mại điện tử – DoS	4	2	8
Làm gián đoạn các dịch vụ thương mại điện tử – tấn công tài sản bên ngoài	5	3	15
Làm gián đoạn các dịch vụ thương mại điện tử – tấn công tài sản nội mạng	5	2	10
Sử dụng dịch vụ thương mại điện tử không chủ ý – tấn công ứng dụng web	2	4	8
Sử dụng dịch vụ thương mại điện tử không chủ ý – tấn công tài sản nội mạng	2	1	2

Bước 3 – Xác định nguồn dữ liệu

❑Với nguy cơ: Đánh cắp thông tin thẻ tín dụng của khách hàng – tấn công ứng dụng web.

- Thu thập và kiểm tra các giao dịch máy chủ web với người dùng bên ngoài để phát hiện ra những hành vi bất thường

➢ có thể đặt một bộ cảm biến ở cạnh mạng

- Thu thập dữ liệu nhật ký ứng dụng cụ thể của các máy chủ web
- Kiểm tra các giao dịch đến máy chủ cơ sở dữ liệu

➢ cần đặt một cảm biến thứ hai có khả năng hiển thị trong mạng nội bộ

- Thu thập dữ liệu về các bản ghi ứng dụng cụ thể của các máy chủ cơ sở dữ liệu

Bước 3 – Xác định nguồn dữ liệu

- Kế hoạch này tạo ra danh sách các nguồn dữ liệu như sau:
  - Dữ liệu bắt gói tin đầy đủ, dữ liệu phiên, dữ liệu kiểu chuỗi trong gói tin, sử dụng NIDS qua cảm biến DMZ.
  - Dữ liệu bắt gói tin đầy đủ, dữ liệu phiên, dữ liệu kiểu chuỗi trong gói tin, sử dụng NIDS qua cảm biến nội mạng.
  - Dữ liệu nhật ký ứng dụng máy chủ web
  - Dữ liệu nhật ký ứng dụng máy chủ cơ sở dữ liệu

Bước 3 – Xác định nguồn dữ liệu

- Với nguy cơ: Làm gián đoạn các dịch vụ thương mại điện tử – tấn công tài sản bên ngoài.
  - Có thể bao gồm cả tấn công ứng dụng web.
  - Có hai tài sản bên ngoài cần bảo vệ là máy chủ web, và máy chủ thư điện tử
  - Dữ liệu nhật ký tường lửa là nguồn dữ liệu điều tra rất hữu ích.
  - ➢ cần có một cảm biến để thu thập dữ liệu qua giao diện mạng.
  - Cần thu thập nhật ký cụ thể của ứng dụng, bao gồm nhật ký máy chủ web, cơ sở dữ liệu và thư điện tử.

Bước 3 – Xác định nguồn dữ liệu

- Kế hoạch này tạo ra danh sách các nguồn dữ liệu như sau:
  - Dữ liệu nhật ký tường lửa cạnh mạng
  - Dữ liệu bắt gói tin đầy đủ, dữ liệu phiên, dữ liệu kiểu chuỗi trong gói tin, sử dụng NIDS qua cảm biến DMZ
  - Dữ liệu nhật ký ứng dụng máy chủ cơ sở dữ liệu
  - Dữ liệu nhật ký ứng dụng máy chủ thư điện tử
  - Dữ liệu nhật ký bảo mật và hệ điều hành của máy chủ thư điện tử và máy chủ web
  - Dữ liệu cảnh báo chống virus và dữ liệu cảnh bảo HIDS của máy chủ thư điện tử và máy chủ web

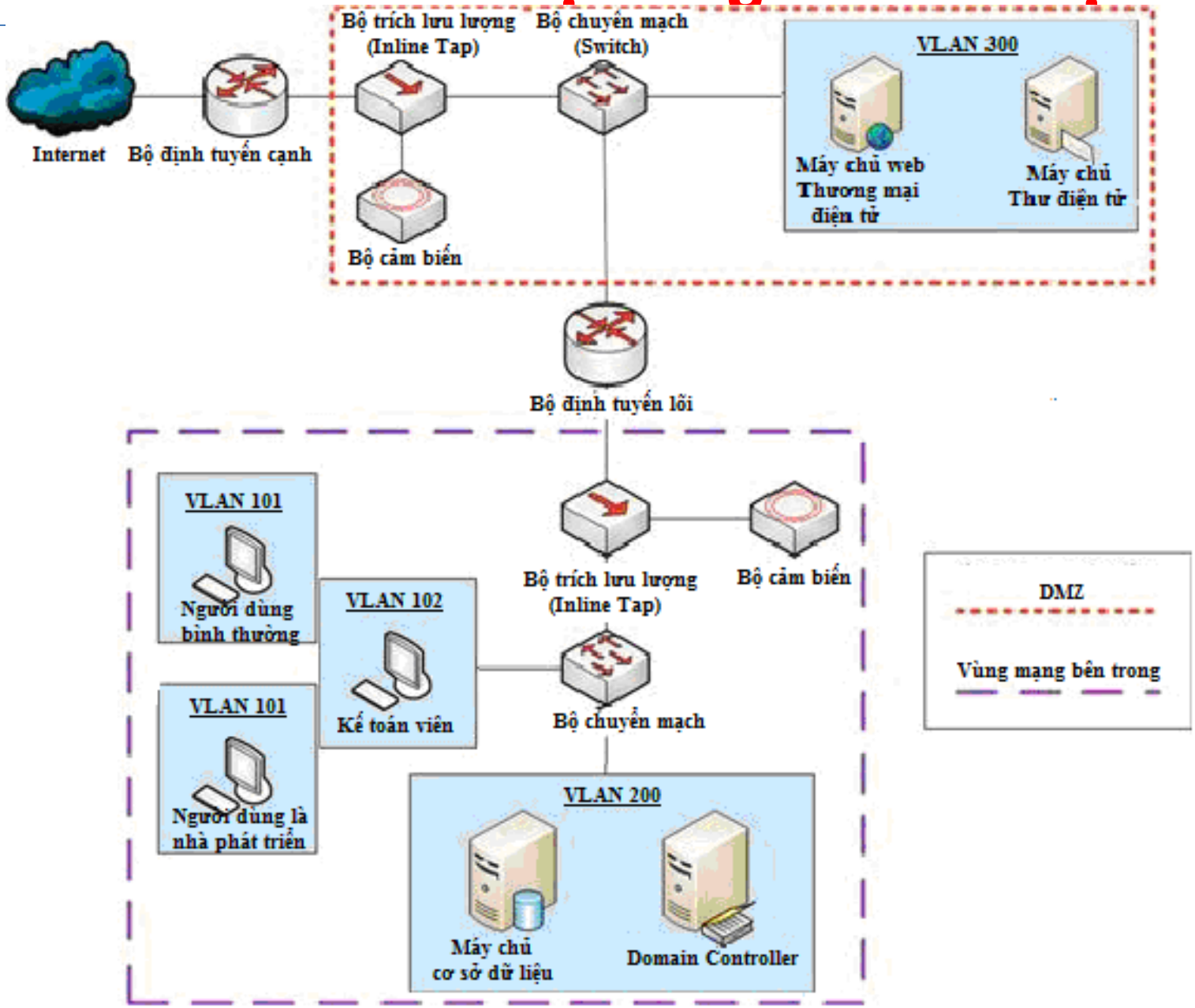
Bước 3 – Xác định nguồn dữ liệu

- Với nguy cơ: Làm gián đoạn các dịch vụ thương mại điện tử – tấn công tài sản nội mạng.
  - Chỉ có các máy chủ trong VLAN 200 và những người dùng là nhà phát triển trong VLAN 103 là có quyền truy nhập vào DMZ từ bên trong mạng
  - ➢ cần triển khai một cảm biến ở bên trong mạng để thu thập các dữ liệu từ các thiết bị này
  - Nếu kẻ tấn công chiếm được quyền sử dụng máy của người dùng là nhà phát triển trong nội mạng, hắn sẽ có quyền truy nhập đến DMZ, tác động đến DNS
  - cần thu thập dữ liệu của các hệ thống có liên quan và các nhật ký bảo mật từ các bộ định tuyến nội mạng

Bước 3 – Xác định nguồn dữ liệu

- Kế hoạch này tạo ra danh sách các nguồn dữ liệu như sau:
  - Dựa trên mạng:
  - ➢ Dữ liệu nhật ký tường lửa bên cạnh mạng, bên trong mạng
  - ➢ Dữ liệu bắt gói tin đầy đủ, dữ liệu phiên qua cảm biến DMZ và cảm biến nội mạng
  - Dựa trên máy chủ:
  - ➢ Nhật ký dữ liệu máy chủ web, cơ sở dữ liệu, và ứng dụng điều khiển miền.
  - ➢ Dữ liệu nhật ký bảo mật, Dữ liệu cảnh báo chống vi-rus và cảnh bảo HIDS máy chủ web, VLAN 200 và VLAN 103

Bước 3 – Xác định nguồn dữ liệu



Bước 4 – Chọn lọc dữ liệu

- Dựa trên mạng:
  - Dữ liệu nhật ký tường lửa bên cạnh mạng
    - Bên trong→Từ chối bên ngoài
  - Dữ liệu nhật ký tường lửa bên trong (lõi mạng)
    - Bên ngoài→Cho phép/Từ chối bên trong
    - Bên trong→Từ chối bên ngoài
  - Cảm biến DMZ – Dữ liệu bắt gói tin đầy đủ
    - Bên ngoài→Các cổng web bên trong
    - Bên ngoài→Các cổng thư điện tử bên trong
    - Bên trong→Các cổng thư điện tử bên ngoài
  - Cảm biến DMZ – Dữ liệu phiên
    - Tất cả các bản ghi

Bước 4 – Chọn lọc dữ liệu

- Dựa trên mạng:
  - Cảm biến DMZ – NIDS
    - Các luật tập trung vào tấn công ứng dụng web: SQL injection, XSS,...
    - Các luật tập trung vào tấn công máy chủ web và máy chủ thư điện tử
    - Cảm biến DMZ –NIDS dựa trên bất thường
    - Các luật tập trung vào những bất thường trong nội dung thư và web
  - Cảm biến nội mạng – Dữ liệu bắt gói tin đầy đủ
    - Bên trong→Các IP máy chủ web
    - Bên trong→Nhà phát triển VLAN 103
    - Bên ngoài→Máy chủ VLAN 200

Bước 4 – Chọn lọc dữ liệu

- Dựa trên mạng:
  - Cảm biến nội mạng – Dữ liệu phiên
    - Tất cả các bản ghi
  - Cảm biến nội mạng – Dữ liệu kiểu chuỗi trong gói tin
    - Nhà phát triển VLAN 103→Bên ngoài
  - Cảm biến nội mạng – NIDS
    - Các luật tập trung vào tấn công cơ sở dữ liệu
    - Các luật tập trung vào tấn công và các hoạt động quản trị bộ điều khiển miền
    - Các luật phần mềm độc hại chung
    - Các luật tập trung vào tương tác cơ sở dữ liệu bất thường

Bước 4 – Chọn lọc dữ liệu

- Dựa trên máy chủ:
  - Dữ liệu nhật ký máy chủ thư điện tử, máy chủ web, máy chủ cơ sở dữ liệu và ứng dụng điều khiển miền
    - Máy chủ thư điện tử – Tạo và sửa đổi tài khoản
    - Máy chủ web – Các giao dịch từ miền con xử lý thanh toán
    - Máy chủ web – Các giao dịch từ miền con quản trị
    - Máy chủ cơ sở dữ liệu – Tạo và sửa đổi tài khoản
    - Máy chủ cơ sở dữ liệu – Các giao dịch thanh toán
    - Máy chủ cơ sở dữ liệu – Các giao dịch quản trị

Bước 4 – Chọn lọc dữ liệu

- Dựa trên máy chủ:
  - Dữ liệu nhật ký bảo mật và hệ điều hành máy chủ thư điện tử, máy chủ web, VLAN 200 và VLAN 103
    - Tạo và sửa đổi tài khoản
    - Các thông báo phần mềm được cài đặt
    - Các thông báo cập nhật hệ thống
    - Thông báo khởi động lại hệ thống
  - Dữ liệu cảnh báo chống virus máy chủ thư điện tử, máy chủ web, VLAN 200 và VLAN 103
    - Tất cả dữ liệu cảnh báo
  - Dữ liệu cảnh báo HIDS máy chủ thư điện tử, máy chủ web và VLAN 103 Alert Data

1. Thu thập dữ liệu
2. Phân tích dữ liệu
3. Tìm kiếm các mối đe dọa

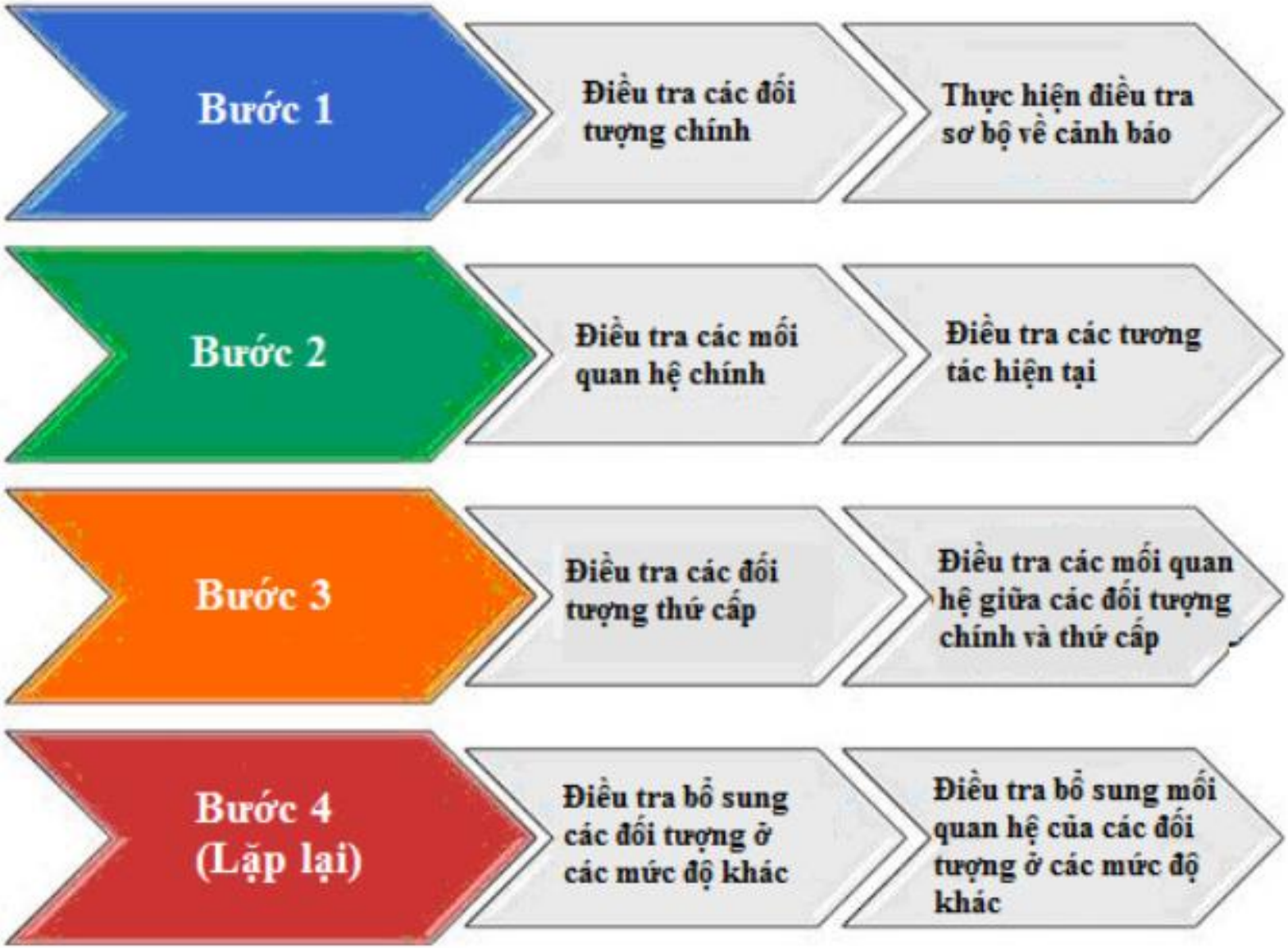
Phân tích dữ liệu

- Là một cách tiếp cận có hệ thống dùng để giải thích nội dung dữ liệu thông qua quá trình sắp xếp, phân loại và xác định chủ đề.
- Quy trình phân tích gồm 3 phần:
  - Đầu vào
  - Điều tra
  - Đầu ra

Phương pháp phân tích

- Điều tra quan hệ.
  - Dựa trên việc xác định các mối quan hệ tuyến tính giữa các thực thể
- Chuẩn đoán khác biệt.

Quy trình điều tra quan hệ



Điều tra các đối tượng chính và thực hiện điều tra sơ bộ các cảnh báo

- Xác định đối tượng (máy chủ, máy tính…)
- Xác định cảnh báo là thật hay giả, nếu các cảnh báo là thật thì thu thập tiếp các thông tin như IP, domain, tài nguyên tin cậy và nguy hiểm

Điều tra mối quan hệ chính và tương tác hiện tại

- Điều tra mối quan hệ trước đó cũng như hiện tại của máy tính tấn công và máy tính cần bảo vệ như hai máy đã từng liên lạc, nếu có thì cổng, giao thức và dịch vụ nào?
- Điều tra kỹ lưỡng các kết nối bằng cách thu thập dữ liệu PCAP, thực hiện phân tích gói, trích xuất các tập tin để phân tích phần mềm độc hại, tạo thống kê dữ liệu phiên…

Điều tra các đối tượng thứ cấp và mối quan hệ

- Xác định các đối tượng thứ cấp.
- Xác định mối quan hệ giữa các đối tượng thứ cấp và đối tượng chính

Điều tra bổ sung về quan hệ của các đối tượng

- Việc điều tra các đối tượng và các mối quan hệ nên được lặp lại nhiều lần khi cần thiết có thể đòi hỏi thêm các đối tượng mức 3, mức 4.
- Nên đánh giá các đối tượng và các mối quan hệ một cách đầy đủ trên cơ sở mỗi cấp độ trước khi chuyển sang mức kế tiếp để tránh mất các thông tin quan trọng

Examples

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	2014-08-26 11:20:49	192.168.204.139	49647	176.102.38.75	80	6	ET CURRENT_EVENTS Fiesta EK randomized javascript Ga
RT	11	2014-08-26 11:20:52	192.168.204.139	49654	64.202.116.154	80	6	ET CURRENT_EVENTS Fiesta URI Struct
RT	8	2014-08-26 11:20:53	64.202.116.154	80	192.168.204.139	49654	6	ET CURRENT_EVENTS Fiesta Flash Exploit Download
RT	6	2014-08-26 11:20:55	64.202.116.154	80	192.168.204.139	49662	6	ET CURRENT_EVENTS DRIVEBY Incognito libtiff PDF Explo
RT	6	2014-08-26 11:20:55	64.202.116.154	80	192.168.204.139	49662	6	ET WEB_CLIENT PDF With Embedded File
RT	6	2014-08-26 11:20:55	64.202.116.154	80	192.168.204.139	49662	6	ETPRO WEB_CLIENT Adobe PDF Memory Corruption /Ff
RT	6	2014-08-26 11:20:55	64.202.116.154	80	192.168.204.139	49662	6	ET CURRENT_EVENTS Fiesta PDF Exploit Download
RT	6	2014-08-26 11:20:55	64.202.116.154	80	192.168.204.139	49662	6	ET CURRENT_EVENTS PDF /XFA and PDF-1.[0-4] Spec Viol
RT	17	2014-08-26 11:20:54	64.202.116.154	80	192.168.204.139	49663	6	ET CURRENT_EVENTS Fiesta SilverLight Exploit Download
RT	3	2014-08-26 11:21:49	192.168.204.139	49694	64.202.116.154	80	6	ET CURRENT_EVENTS Unknown - Java Request - gt 60cha

Examples

- Bước 1: Điều tra các đối tượng chính và thực hiện điều tra sơ bộ cho thấy:
  - IP Attacker: 192.0.2.5
  - IP Victim: 172.16.16.20
  - PDF được tải về, giá trị MD5 của PDF được 23% engine phát hiện virus cho rằng là mã độc

=> Quyết định điều tra tiếp.

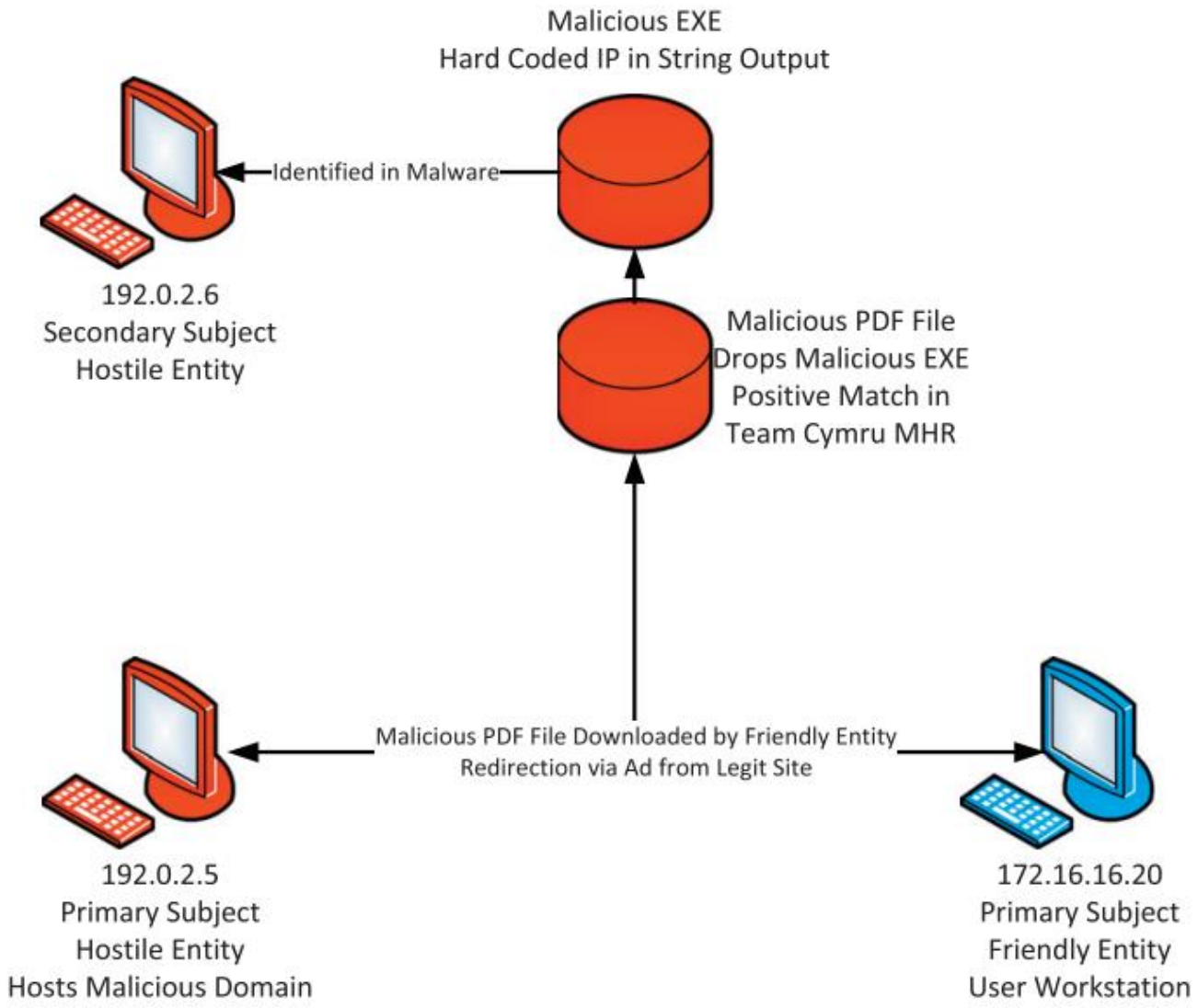
Bước 1 (Tiếp)

- Friendly Intelligence for 172.16.16.20
  - Máy trạm của người dùng đang chạy Win7
  - Hệ thống không mở các cổng dịch vụ nào cả
  - Người dùng hệ thống này thường lướt web
- Hostile Intelligence for 192.0.2.5
  - Kiểm tra IP Blacklist với http://www.ipvoid.com/ trả về 0 kết quả
  - Kiểm tra IP Blacklist với http://www.urlvoid.com/ trả về 5 kết quả cho tên miền nơi các tập tin PDF được tải về
  - 192.0.2.5 không liên lạc với máy nào khác trong hệ thống mạng victim

(Example) Bước 2 – Điều tra mối quan hệ chính và tương tác hiện tại

- Tải và phân tích các gói tin trong khoảng thời gian có cảnh báo (10p trước và 10p sau cảnh báo)
- Thực hiện phân tích và xác định được:
  - Victim đã chuyển hướng tới máy tính độc hại từ 1 quảng cáo của bên thứ 3 trên một trang web hợp pháp
  - Victim tải tệp tin về và ngừng kết nối tới máy chủ lưu trữ 192.0.2.5
  - Tải tệp tin lên Cuckoo sandbox để thực hiện phân tích mã độc tự động chỉ ra PDF có chứa mã thực thi và tệp thực thi có chứa địa chỉ IP 192.0.2.6, ngoài ra không còn thông tin nào khác

(Example) Bước 2 – Điều tra mối quan hệ chính và tương tác hiện tại



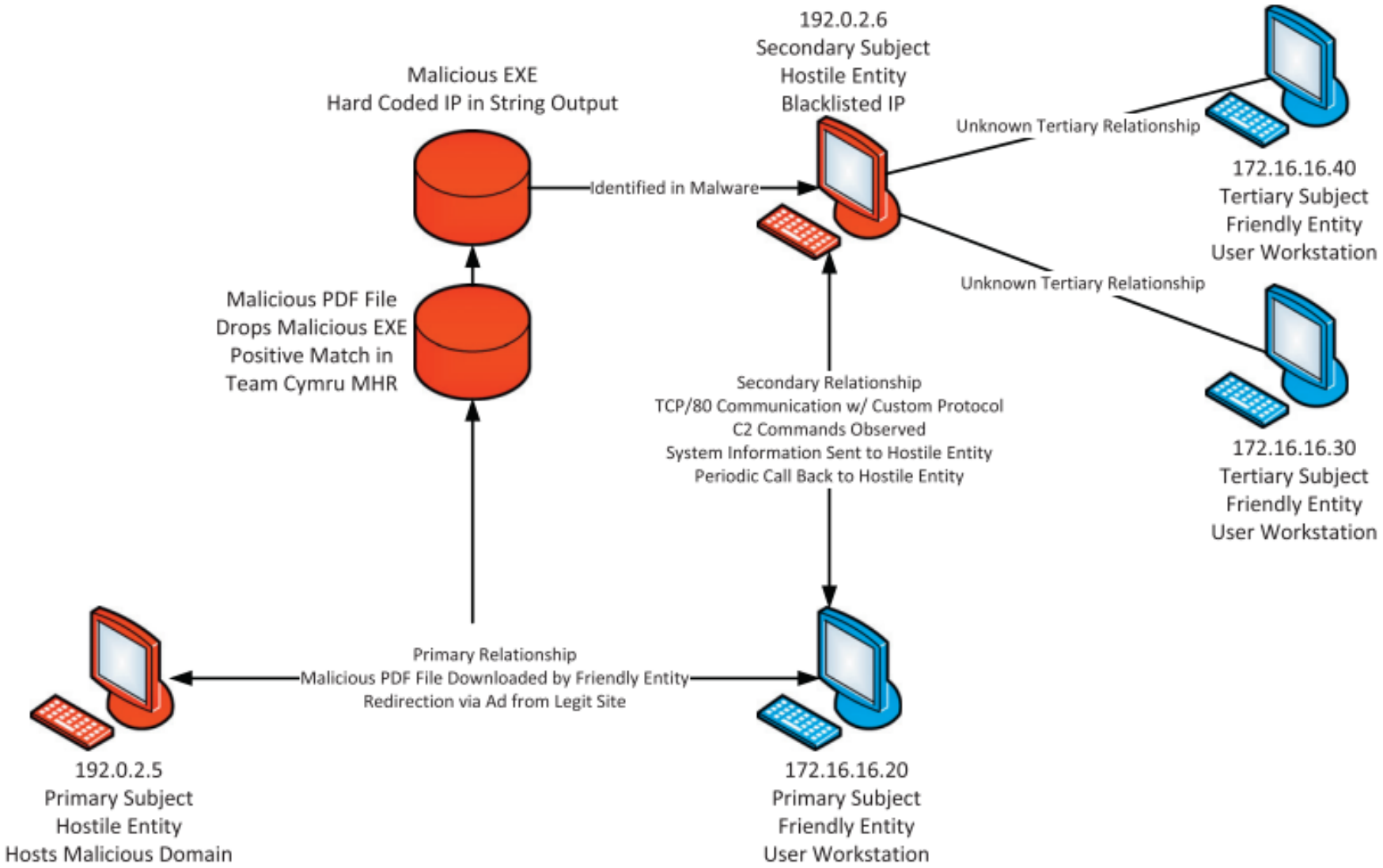
(Example) Bước 3 – Điều tra các đối tượng thứ cấp và mối quan hệ

- Xác định được đối tượng thứ cấp có IP 192.0.2.6
- Hostile Intelligence for 192.0.2.6:
  - http://www.ipvoid.com/ trả về 2 kết quả
  - Dữ liệu NetFlow cho thấy victim (172.16.16.20) đã liên lạc với máy tính này sau 30p kể từ cảnh báo ban đầu
  - Dữ liệu NetFlow chỉ ra 2 máy tính trong hệ thống mạng của victim cũng giao tiếp với IP này theo định kỳ với lưu lượng thấp với IP lần lượt 172.16.16.30 và 172.16.16.40
  - Các máy giao tiếp qua cổng 80 bằng một giao thức sửa đổi cho phép gửi thông tin từ victim về máy chủ độc hại

(Example) Bước 3 – Điều tra các đối tượng thứ cấp và mối quan hệ

- Trong một số trường hợp, việc điều tra có thể kết thúc ở đây với thông báo sự cố là 172.16.16.20 đã bị tấn công và 2 máy khác trong hệ thống cũng có thể bị đã bị tấn công trước đó.

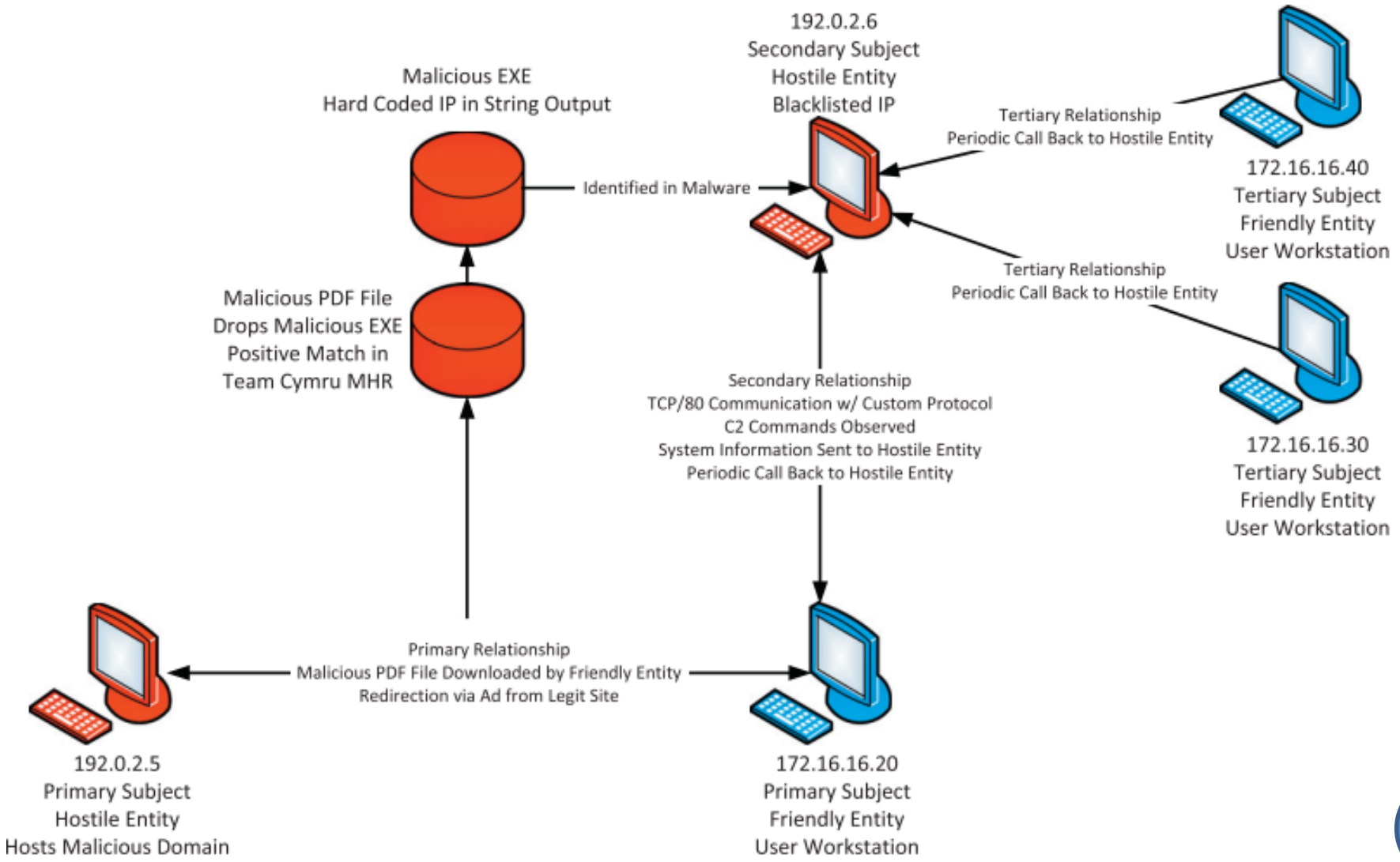
(Example) Bước 3 – Điều tra các đối tượng thứ cấp và mối quan hệ



(Example) Bước 4 – Điều tra bổ sung quan hệ của các đối tượng

- Trong một số trường hợp, việc điều tra có thể kết thúc ở đây với thông báo sự cố là 172.16.16.20 đã bị tấn công và 2 máy khác trong hệ thống cũng có thể bị đã bị tấn công trước đó.
- Thực hiện kiểm tra các gói dữ liệu truyền giữa các máy tính mức 3 (172.16.16.30 và 172.16.16.40) cho thấy nó cũng tham gia và hành vi callback tới máy chủ độc hại
  - Xác định được các máy tính được bảo vệ ở mức ba cũng bị tổn hại

(Example) Bước 4 – Điều tra bổ sung quan hệ của các đối tượng



(Example) Tổng kết sự cố

- Kịch bản này được dựa trên một sự cố thực sự xảy ra trong một doanh nghiệp.
- Việc sử dụng quy trình phân tích hệ thống để xác định các máy tính và xây dựng các mối quan hệ giữa chúng không chỉ cho phép chúng ta xác định liệu một tấn công xảy ra hay không, mà còn cho chúng ta tìm các máy tính khác cũng đã bị tổn hại nhưng không được xác định trong các cảnh báo ban đầu.

Chuẩn đoán khác biệt

- Bước 1: Xác định và liệt kê các dấu hiệu.
- Bước 2: Xem xét và đánh giá chuẩn đoán phổ biến nhất đầu tiên.
- Bước 3: Liệt kê tất cả chuẩn đoán có thể cho các dấu hiệu đã biết
- Bước 4: Đánh giá mức ưu tiên trong danh sách ứng viên theo mức độ nghiêm trọng
- Bước 5: Loại bỏ các điều kiện ứng viên và bắt đầu với cái nghiêm trọng nhất

Bước 1: Xác định và liệt kê các dấu hiệu

Các dấu hiệu sau đây được quan sát qua cảnh báo IDS và điều tra các dữ liệu đã có:

1. Một máy chủ tin cậy bắt đầu gửi lưu lượng đến một địa chỉ IP ở Nga
2. Dữ liệu được gửi đều đặn sau mỗi 10 phút
3. Giao thức HTTPS được sử dụng để truyền tải dữ liệu

Bước 2: Xem xét đánh giá chuẩn đoán thường thấy nhất đầu tiên

Các dấu hiệu sau đây được quan sát qua cảnh báo IDS và điều tra các dữ liệu đã có:

1. Một máy chủ tin cậy bắt đầu gửi lưu lượng đến một địa chỉ IP ở Nga
2. Dữ liệu được gửi đều đặn sau mỗi 10 phút
3. Giao thức HTTPS được sử dụng để truyền tải dữ liệu

Bước 3: Liệt kê tất cả phán đoán có thể cho các dấu hiệu đã biết

- Truyền thông bình thường
- Nhiễm mã độc
- Dữ liệu bị rò rỉ từ máy tính bị tấn công
- Cấu hình sai

Bước 4: Sắp xếp danh sách ưu tiên theo mức độ nghiêm trọng

- Ưu tiên 1: Số liệu rò rỉ từ máy tính bị tấn công (cao nhất)
- Ưu tiên 2: Nhiễm mã độc
- Ưu tiên 3: Cấu hình sai
- Ưu tiên 4: Liên lạc bình thường

Bước 5: Loại bỏ dần các phán đoán

- Ưu tiên 1: Dữ liệu rò rỉ từ máy tính bị tấn công
- Ưu tiên 2: Nhiễm mã độc
- Ưu tiên 3: Cấu hình sai
- Ưu tiên 4: Truyền thông bình thường

Thực hiện các phương pháp phân tích

- Nên lựa chọn Tiến hành chuẩn đoán hay Điều tra mối quan hệ?

Lưu ý trong quá trình phân tích

- Luôn đặt ra các giả định
- Cần phải lưu ý về dữ liệu
- Nên làm việc theo nhóm
- Không đánh động tin tặc
- Các gói tin là nguồn dữ liệu tốt
- Wireshark chỉ là một công cụ phân tích
- Cần thực hiện phân loại sự kiện rõ ràng
- Quy tắc 10

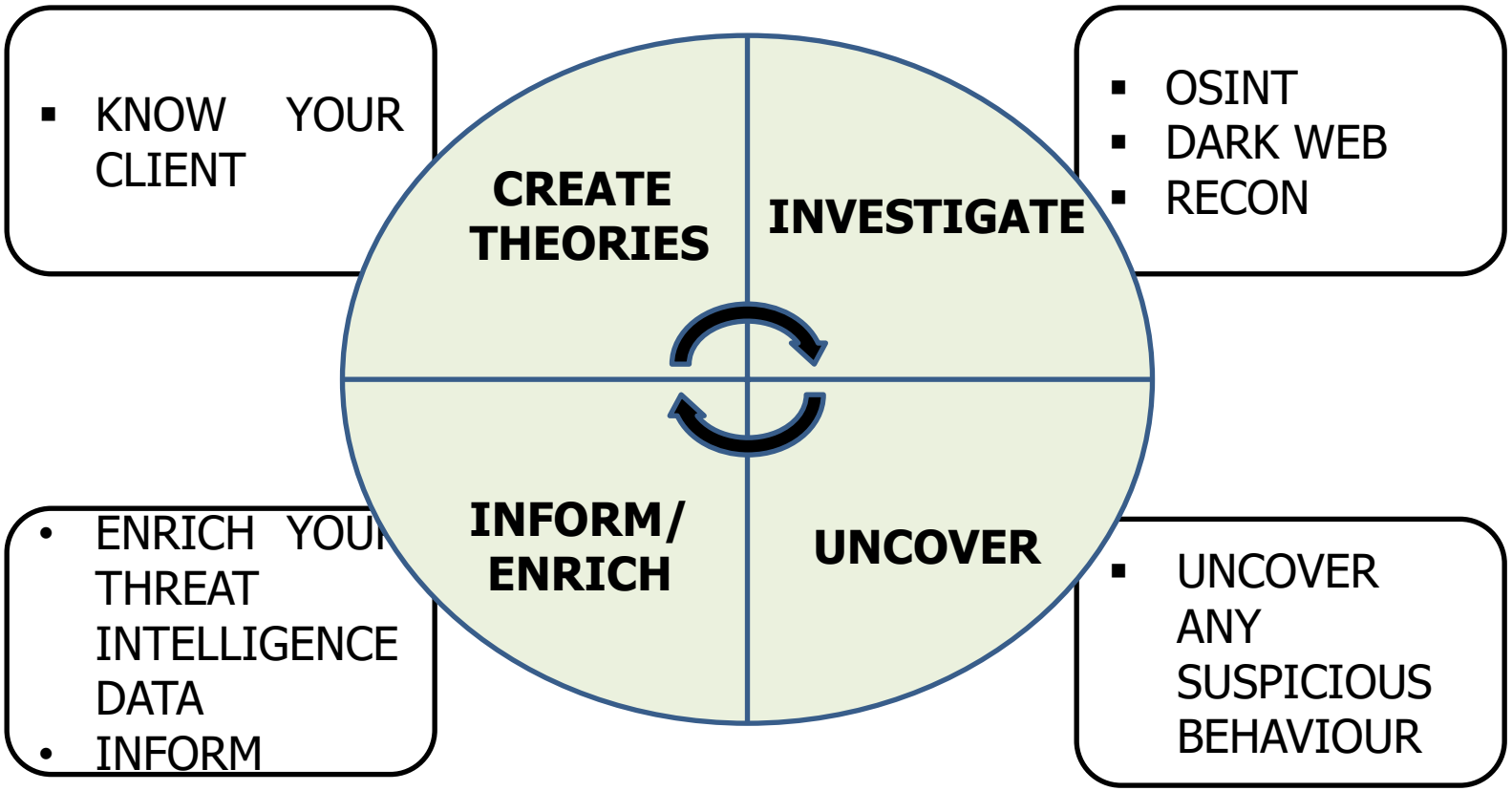
1. Thu thập dữ liệu
2. Phân tích dữ liệu
3. Tìm kiếm các mối đe dọa

Cyber Threat Hunting

- Các giải pháp bảo mật thông thường (FW, IDPS, SIEM) thường điều tra dựa trên bằng chứng sau khi có cảnh báo.
- Cyber Threat Hunting - là quá trình tìm kiếm và điều tra chủ động, lặp đi lặp lại nhằm phát hiện và cô lập các mối đe dọa trước khi có cảnh báo.

Cyber Threat Hunting

- Threat Hunting có thể được thực hiện thủ công hoặc tự động hóa 1 phần.
- Các nhóm tìm kiếm thường đặt ra một giả thuyết và sau đó sẽ chứng minh giả thuyết đó là đúng hoặc sai.



Kỹ thuật

Host Analysis	Network Analysis	Threat Intelligence
Persistence mechanism	Lateral Movement	STIX
Privilege Escalation	C2	TAXII
Code Execution	Beacon patterns	Active/ Passive defence
Exploit	Payload Delivery	OSINT

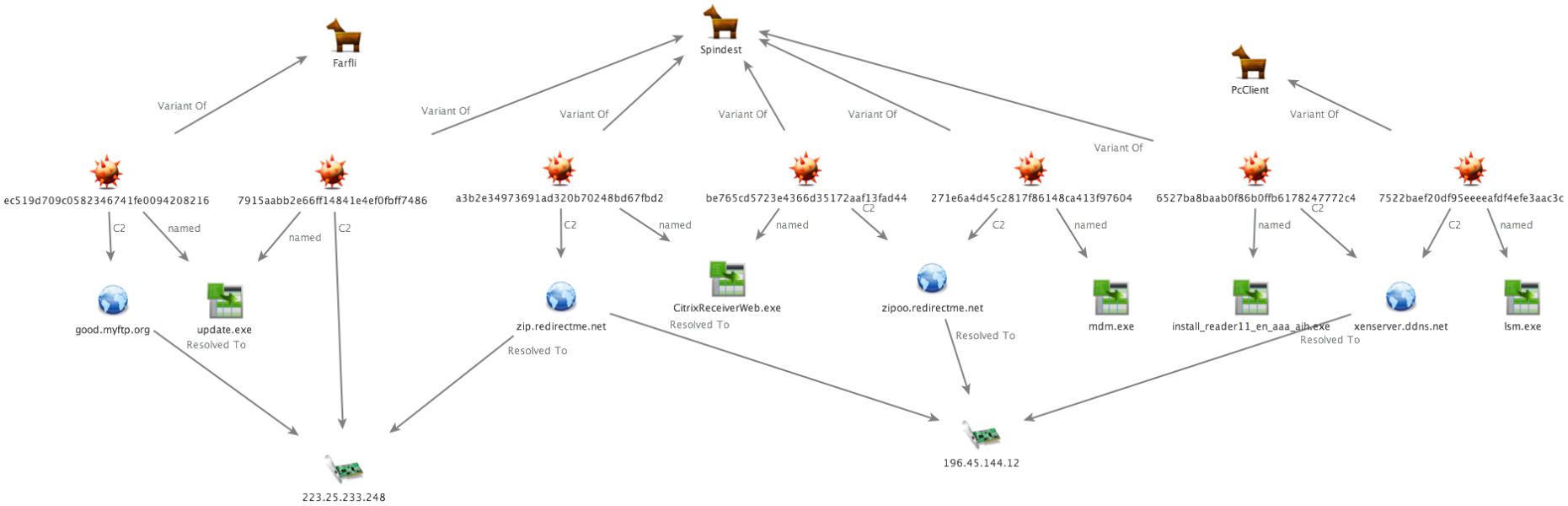
Kỹ thuật

- Tìm kiếm IOC (Indicator of Compromise)
- Tìm kiếm TTP (Tactics, Techniques and Procedures)
- Tìm kiếm hành vi bất thường

Tìm kiếm IOC

- Dễ dàng tự động hóa
- Chỉ tìm kiếm được các mối đe dọa đã biết

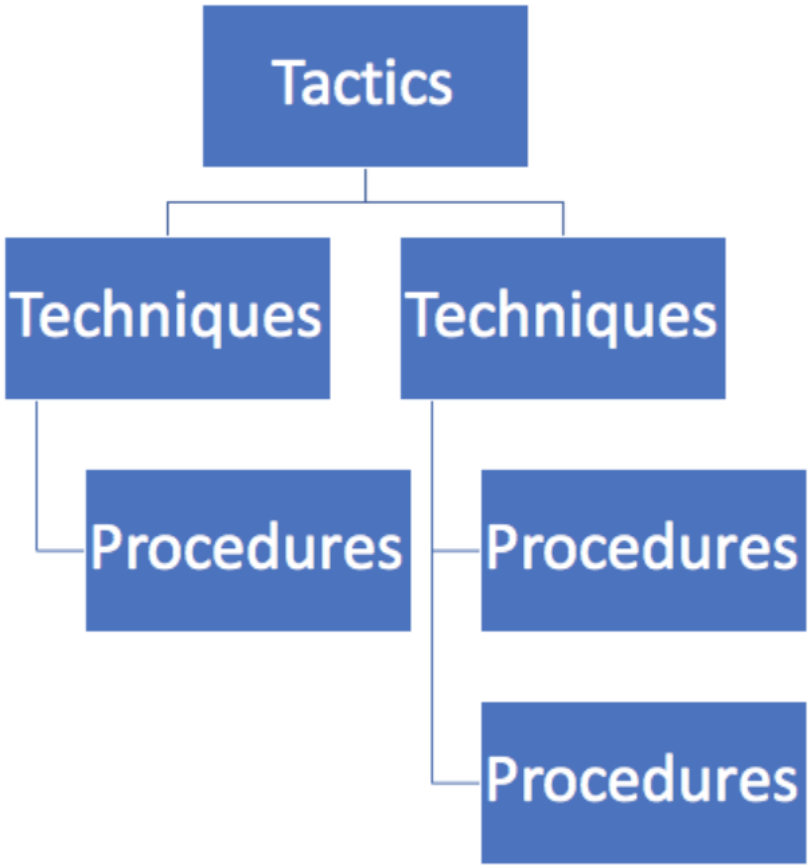
Example - IOC for APT Group Nitro



SHA256	0a1103bc90725d4665b932f88e81d39eafa5823b0de3ab146e2d4548b7da79a0
MD5	7915aabb2e66ff14841e4ef0fbff7486
File Name	update.exe
File Size	106496
First Seen	2014-07-24 11:54:02
C2 IP	223.25.233.248

Tìm kiếm TTP

- TTP mô tả hành vi của một hoặc nhiều tác nhân đe dọa.
  - Tactics (Chiến thuật) – Mô tả hành vi tác nhân đe dọa đang muốn cố gắng thực hiện (Ví dụ: Chiếm quyền điều khiển) → *Dự đoán tấn công sắp tới.*



Tìm kiếm TTP

➢Techniques (Kỹ thuật) – Công nghệ sử dụng để tấn công nhằm đạt được mục tiêu của chiến thuật đề ra (Ví dụ: Sử dụng phishing để chiếm quyền điều khiển)

→ *Xác định cách thức đối phó.*

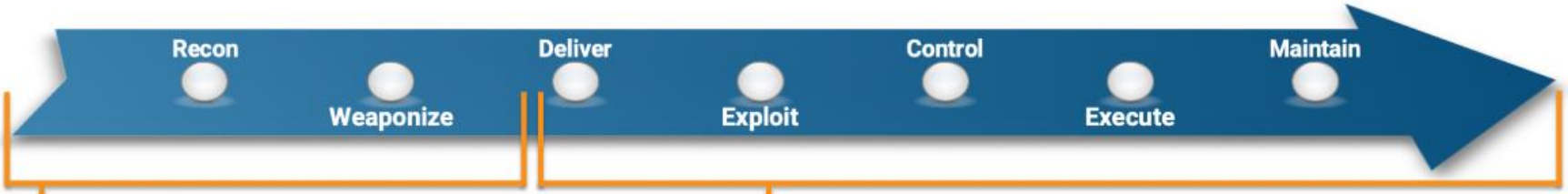
Tìm kiếm TTP

- Procedures (Thủ tục) – Quy trình thực hiện tấn công (Ví dụ để thực hiện phishing thì sẽ bao gồm rất nhiều các bước như tìm kiếm thông tin, gửi mail độc hại…)

→ *Xác định được cách thức cuộc tấn công diễn ra.*

MITRE ATT&CK Framework

https://attack.mitre.org/



PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People, Organizational

Weakness Identification
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ATT&CK for Enterprise

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Impact

Example

- Tactics: Privilege
- Techniques: Access Token

Last Modified: 2019-10-09 18:48:31.906000

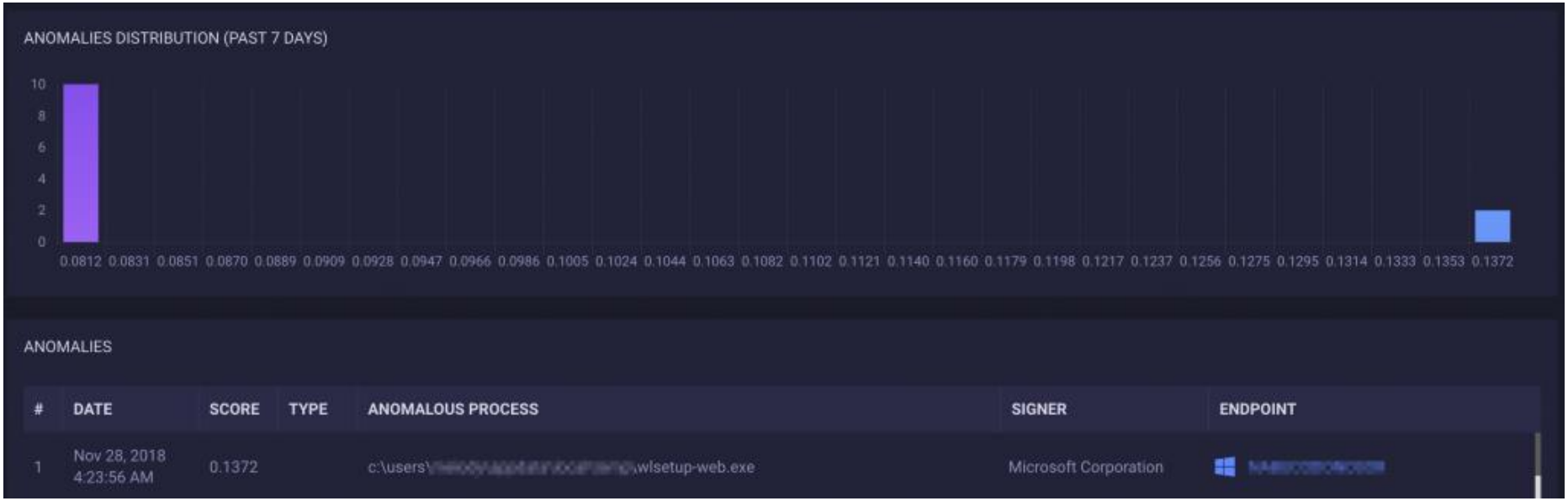
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium
Supply Chain	Execution through	Bootkit	Elevated Execution with	Compile After Delivery	Exploitation for Credential	Network Share	Pass the Ticket	Data Staged	Domain Generation	Scheduled

Tìm kiếm TTP

- Ưu Điểm
  - Tính Toàn Diện và Cập Nhật
  - Tăng Cường Hiệu Quả Phòng Thủ
- Nhược Điểm
  - Yêu Cầu Chuyên Môn Cao
  - Độ Phức Tạp

Tìm kiếm theo hành vi

- Đòi hỏi khả năng giám sát hành vi thông qua trích xuất và phân tích hành vi ở cấp độ endpoint
- Có khả năng tự động hóa hoàn toàn
- Phát hiện sớm các mối đe dọa không có trong lịch sử dữ liệu

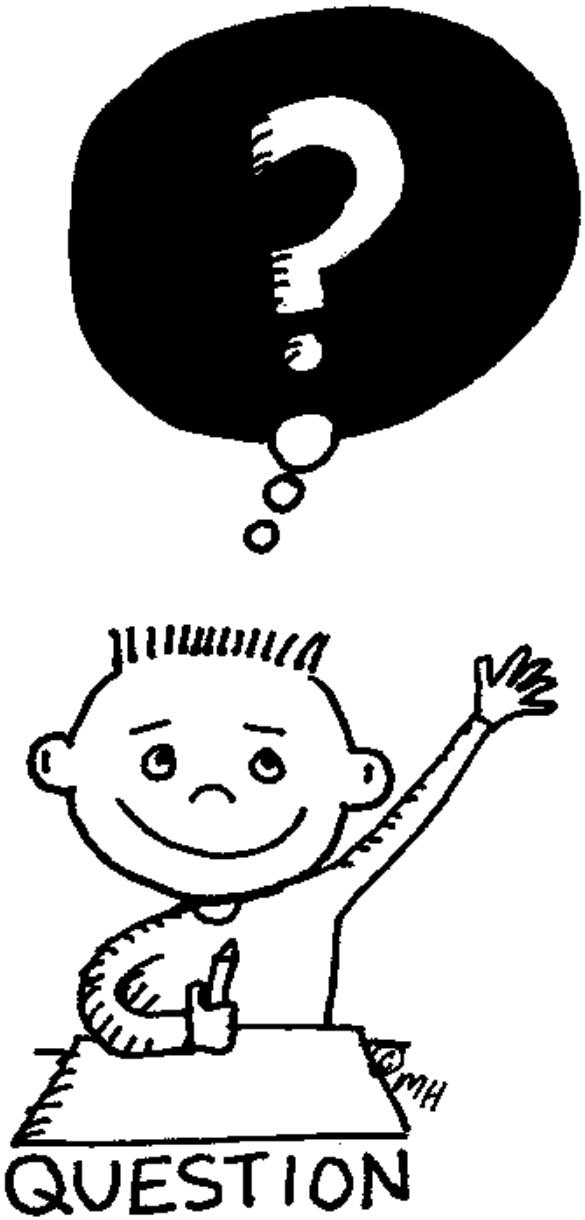


Threat Hunting Platform

- Thu thập, quản lý, chia sẻ dữ liệu
- Phát hiện và phân tích các mối đe dọa nâng cao
- Giao diện trực quan, hỗ trợ các kỹ thuật tự động
- Kết nối các nhóm tìm kiếm

Threat Hunting Platform

- **Commercial**
  - Sqrrl, Splunk, …
  - Mantix4
  - Exabeam
  - Infocyte HUNT
  - …
- **Open Source**
  - MISP, OpenCTI
  - RedHunt OS
  - CHIRON
  - MaliceIO
  - …


QUESTION