TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
Khoa Mạng máy tính & Truyền thông

Host-based IDPS

NT204 – Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập

GV: Đỗ Hoàng Hiển

hiendh@uit.edu.vn

Nội dung hôm nay…

Host-based IDPS

Hôm nay có gì?

Host-based IDPS

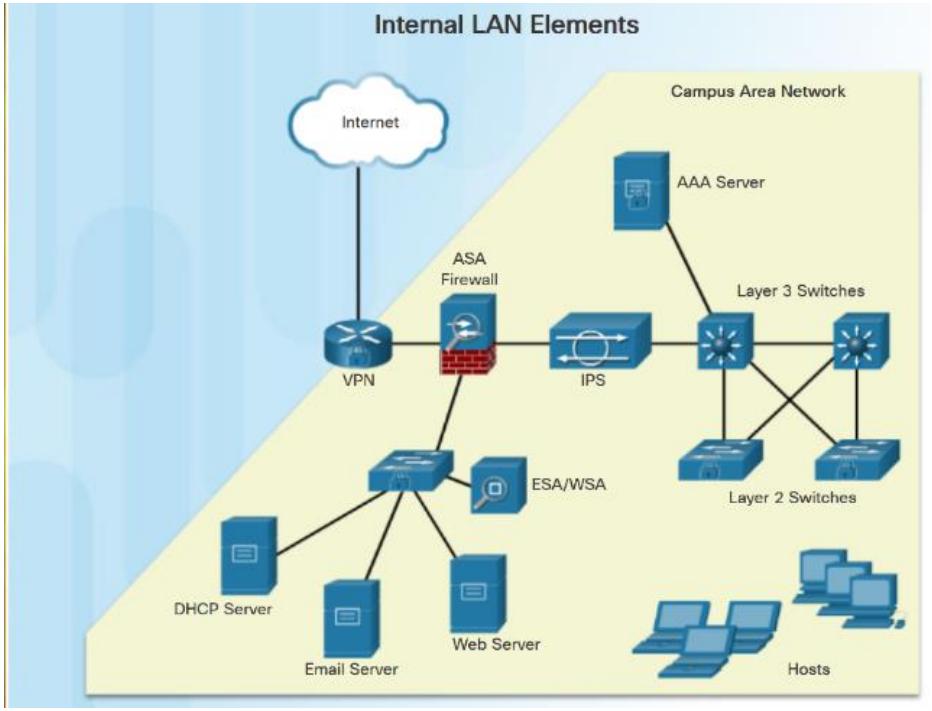
Tài liệu:

- NIST, Chương 7

Tổng quan

Endpoint Security

- 2 thành phần trong mạng LAN cần được bảo vệ:
  - **Endpoint** – Các hosts thường là các laptop, máy bàn, máy in, server, các điện thoại IP, ...
  - **Hạ tầng mạng** – Các thiết bị trong hạ tầng LAN kết nối các endpoint, thường bao gồm switch, thiết bị không dây, các thiết bị thoại IP...



Ref: Cisco CCNA CyberOps

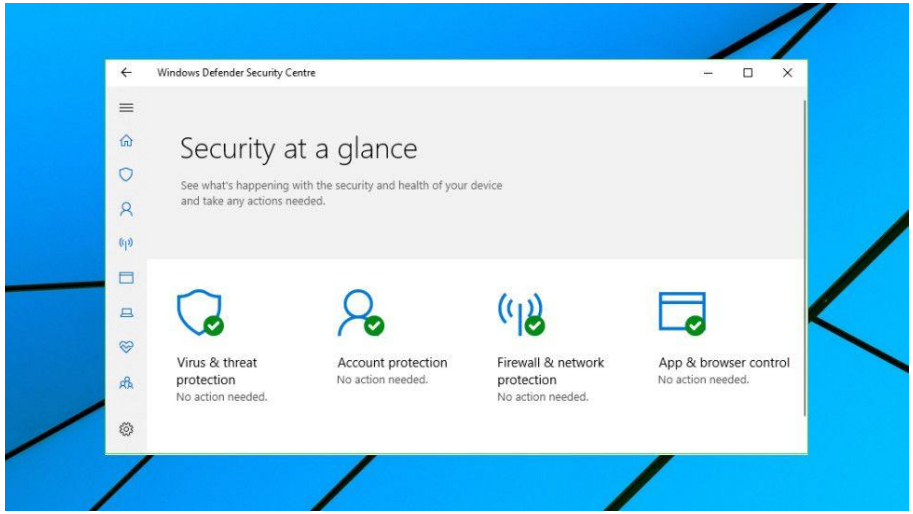
Làm sao để bảo vệ các endpoint?

4 bước chính: **Discover → Inventory → Monitor → Protect**

Bộ giải pháp Host-based security – gồm antivirus, anti-phishing (chống lừa đảo), safe browsing, Host-based intrusion prevention system (HIDPS), firewall và chức năng ghi log

Host-based Malware Protection

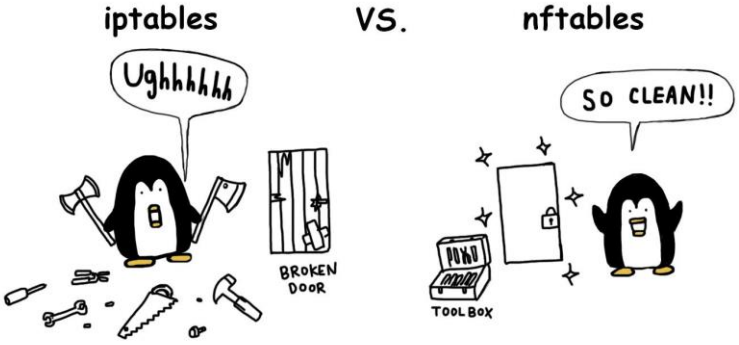
- Các phần mềm Antimalware/antivirus.
  - **Signature-based** – Phát hiện các đặc điểm khác nhau của những file malware đã biết
  - **Heuristics-based** – Phát hiện các tính năng chung thường được sử dụng bởi các loại malware
  - **Behavior-based** – dựa trên việc phân tích các hành vi đáng ngờ



Tổng quan

Host-based Firewall

- **Host-based firewall** là các chương trình phần mềm kiểm soát traffic đi vào và đi ra một máy tính/thiết bị
- Host-based firewall bao gồm:
  - **Windows Firewall** – sử dụng hướng tiếp cận profile-based để cấu hình hoạt động của firewall
  - **Iptables** – cho phép cấu hình các rule kiểm soát truy cập trên các hệ thống Linux
  - **Nftables** – kế thừa từ iptables, nftables là ứng dụng firewall cho Linux sử dụng 1 máy ảo đơn giản trong kernel Linux
  - **TCP Wrapper cho các thiết bị Linux –** hệ thống kiểm soát truy cập và ghi log dựa trên rule

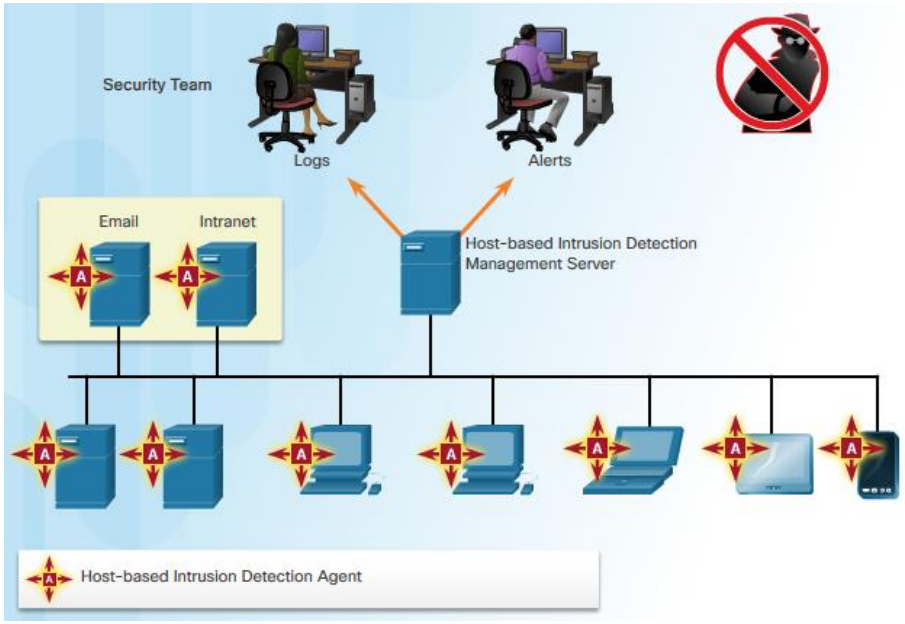


Tổng quan

Host-based IDPS

Host-based IDPS theo dõi các đặc điểm của 1 host và các sự kiện xảy ra trong host đó (trong mạng LAN) để nhận biết các hành vi đáng ngờ

- Theo dõi các traffic mạng có dây và không dây (chỉ cho host/server đó)
- Theo dõi *log hệ thống, tiến trình đang chạy, các file, các hoạt động truy cập và thay đổi file, thay đổi trong cấu hình hệ thống và ứng dụng, registry (Windows)*
- Đánh giá traffic do host đó tạo ra
- Không lắng nghe các gói tin khi chúng đi vào mạng LAN



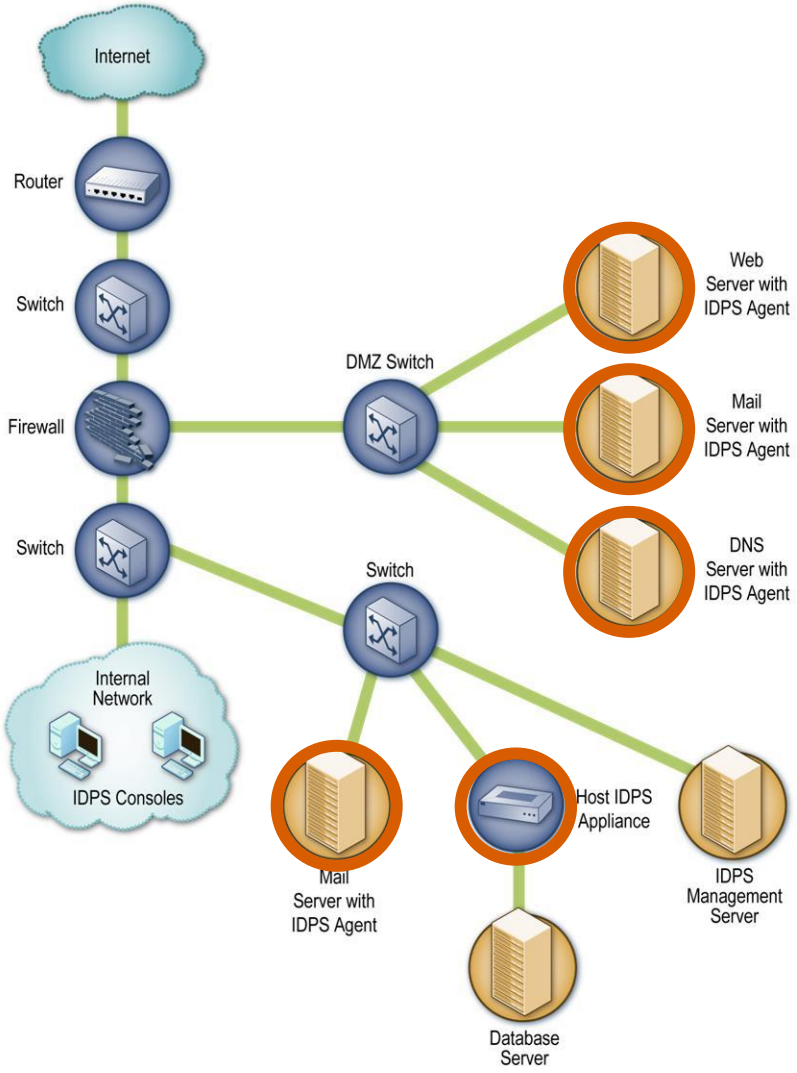
Các thành phần

- **Agent**: phần mềm hoặc phần cứng chuyên dụng, thực hiện theo dõi các hoạt động trên 1 host, gửi dữ liệu đến các server quản lý
- Mỗi agent thường được thiết kế cụ thể để bảo vệ:
  - **Một server:** theo dõi hệ điều hành của server, một số ứng dụng phổ biến
  - **Một client host (máy bàn hay laptop):** theo dõi hệ điều hành và các ứng dụng client phổ biến như e-mail client, trình duyệt web, ...
  - **Một dịch vụ ứng dụng:** theo dõi một dịch vụ ứng dụng, như Web server hoặc server cơ sử dữ liệu (*còn được gọi là application-based IDPS)*
- Thường được triển khai trên các host quan trọng như **các server có thể được truy cập từ internet** và **các server chứa thông tin quan trọng**

HIDPS

Kiến trúc mạng

- Agent được triển khai trên các host đang có trong mạng của tổ chức, *thay vì sử dụng một mạng quản lý riêng*
- Hầu hết các sản phẩm HIDPS mã hoá giao tiếp để tránh việc bị nghe lén khi truy cập các thông tin quan trọng
- Agent dựa trên phần cứng thường được triển khai **inline** ngay phía trước host cần được bảo vệ



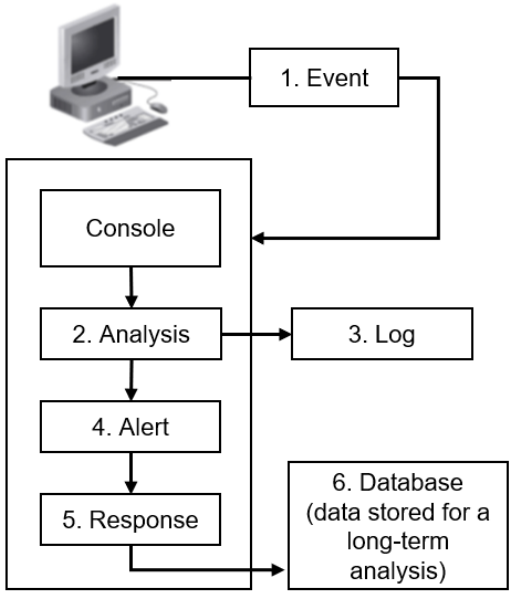
Cần đặt các agent ở đâu?

- Có thể triển khai agent trên hầu hết các server và máy bàn/ laptop
- Thường dùng để phân tích các hoạt động mà **các biện pháp kiểm soát an ninh khác không theo dõi được**
  - **Ví dụ:** network-based IDPS sensor không thể phân tích các hoạt động trong các kết nối mạng được mã hoá, nhưng host-based IDPS agent cài đặt trên các endpoint có thể theo dõi các hoạt động sau khi giải mã
- Cần xem xét điều kiện gì khi lựa chọn vị trí cho các agent?
  - ***Chi phí** triển khai, vận hành và theo dõi các agent*
  - *Các **hệ điều hành** và **ứng dụng** được agent hỗ trợ*
  - ***Tầm quan trọng** của dữ liệu hoặc dịch vụ trên các host*
  - ***Khả năng hỗ trợ** các agent của hạ tầng*

Các kiến trúc Host

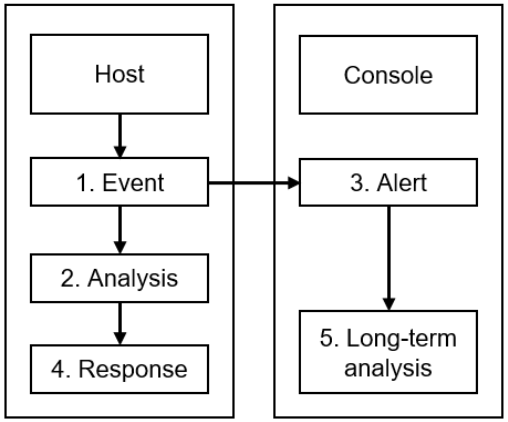
- Cấu hình HIDPS
  - **Cấu hình tập trung**
    - Các agent gửi tất cả dữ liệu đến 1 vị trí trung tâm
    - Hiệu suất của host không bị ảnh hưởng bởi IDPS
    - Các cảnh báo có thể không theo thời gian thực

    ➔ Yêu cầu ít CPU, RAM, ổ cứng trên các host



  - **Cấu hình phân tán**
    - Việc xử lý các sự kiện được phân tán giữa host và console
    - Host tạo và phân tích sự kiện theo thời gian thực
    - Giảm hiệu suất trên các host

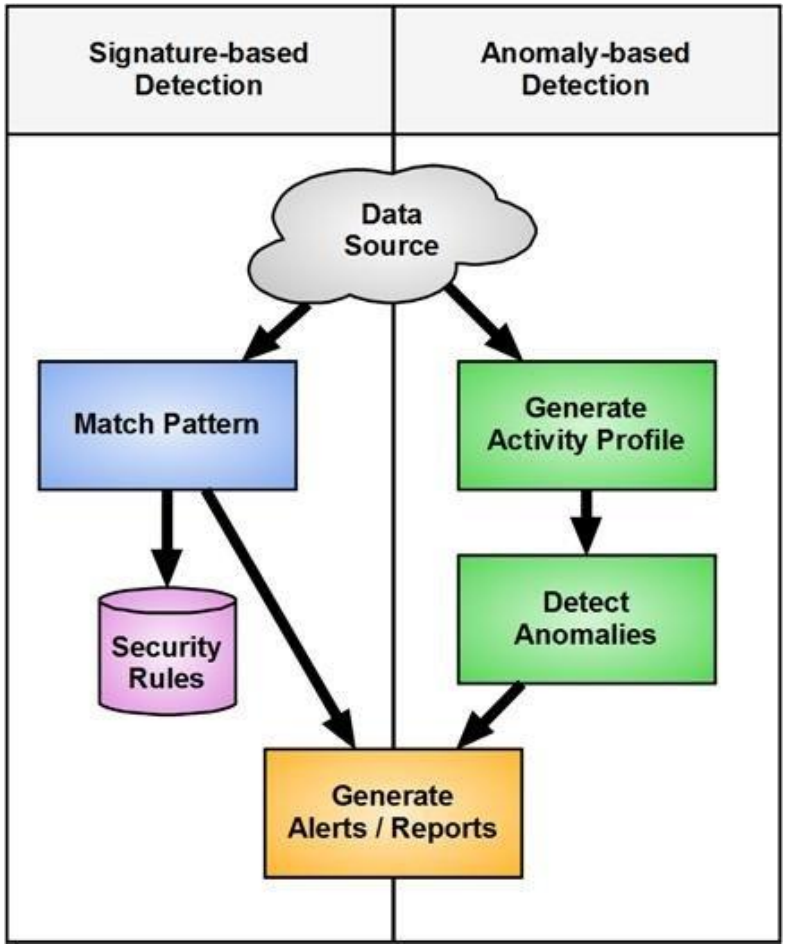
    ➔ Các host nên được trang bị tối đa CPU, RAM, ổ cứng



Ref: Guide to Network Defense and Countermeasures Second Edition

Hoạt động của HIDPS

- HIDPS có khả năng ngăn chặn tấn công do sử dụng signature để phát hiện các xâm nhập đã biết và ngăn chúng ảnh hưởng đến hệ thống
  - **Signature-based –** Hành vi bình thường được định nghĩa bằng các rule hoặc các hành vi vi phạm các rule đã định nghĩa trước
- Có thể kết hợp chiến lược khác để phát hiện các xâm nhập qua mặt được kỹ thuật phát hiện signature-based:
  - **Anomaly-based** – Hành vi của host được so sánh với một mô hình baseline đã được học trước (các ngưỡng)



Khả năng phát hiện tấn công

- **Khả năng phát hiện tấn công**
  - **Các loại sự kiện phát hiện được:** chủ yếu dựa trên các kỹ thuật phát hiện sau:
    - **Phân tích code:** xác định các hành động đáng ngờ bằng cách phân tích các lần thực thi mã code
      - **Phân tích hoạt động của code:** thực thi code trong **sandbox** để phân tích hành vi của nó
      - **Phát hiện Buffer overflow:** tìm các đặc điểm đặc trưng, như một chuỗi các instruction hay hành vi truy cập vào vùng nhớ khác vốn không được cấp phát cho tiến trình đó
      - **Theo dõi lệnh gọi hệ thống (System call):** biết ứng dụng hay tiến trình nào nên gọi ứng dụng hay tiến trình nào khác hoặc thực hiện các hành động nhất định. Agent có thể giới hạn driver nào có thể được load, để ngăn việc cài đặt rookit hoặc các tấn công khác
      - **Danh sách ứng dụng và thư viện:** để giới hạn các ứng dụng, thư viện cũng như phiên bản nhất định nào có thể được dùng

Khả năng phát hiện tấn công

- **Khả năng phát hiện tấn công**
  - **Các loại sự kiện phát hiện được (tt)**:
    - **Phân tích lưu lượng mạng:** phân tích các ứng dụng thông dụng, client e-mail phổ biến, trích xuất các file gửi bởi các ứng dụng như email, web và các file gửi peer-to-peer
    - **Lọc lưu lượng mạng:** thường bao gồm 1 tường lửa host-based có thể giới hạn lưu lượng ra và vào cho mỗi ứng dụng trên hệ thống để ngăn chặn các truy cập trái phép và các hành vi vi phạm chính sách
    - **Theo dõi hệ thống file** (file system): Kiểm tra tính toàn vẹn của file, kiểm tra các đặc điểm của file, theo dõi các truy cập file
    - **Phân tích log**: theo dõi và phân tích các log của OS và ứng dụng để phát hiện hành vi bất thường
    - **Theo dõi cấu hình mạng**: theo dõi các cấu hình mạng hiện tại và phát hiện các thay đổi trên các cấu hình này

HIDPS - Các khả năng bảo mật

Khả năng phát hiện tấn công

- **Độ chính xác:**

  Thách thức hơn với HIDPS (vì nhiều kỹ thuật phát hiện tấn công, như phân tích log hay theo dõi file system, không có kiến thức về ngữ cảnh các sự kiện diễn ra)

  ➔ Sử dụng kết hợp nhiều kỹ thuật phát hiện thường có thể đạt được khả năng phát hiện chính xác hơn so với sử dụng 1 hoặc một vài kỹ thuật

- **Tuỳ chỉnh**

  Kết nối tự động HIDPS với các hệ thống quản lý thay đổi là **không khả thi**

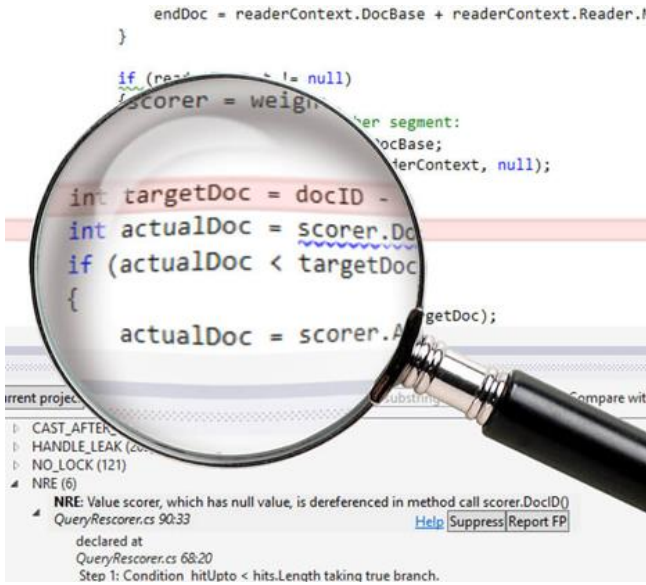
  ➔ Quản trị viên có thể thường xuyên xem các record quản lý các thay đổi và thay đổi các cấu hình host và các policy trên HIDPS để ngăn false positive

  - Các policies có thể linh hoạt được cài đặt trên một hoặc nhóm các host
  - Hỗ trợ whitelist và blacklist
  - Tuỳ chỉnh các cảnh báo, ví dụ xác định hành động phản ứng cần được thực hiện với mỗi cảnh báo

Khả năng ngăn chặn tấn công

Có các khả năng ngăn chặn khác nhau tuỳ vào kỹ thuật phát hiện được sử dụng:

- **Phân tích code:** ngăn việc code được thực thi, bao gồm các malware hoặc ứng dụng không có quyền; ngăn các ứng dụng mạng gọi shell
- **Phân tích lưu lượng mạng:** ngăn việc xử lý các lưu lượng mạng đi vào host hoặc ngăn các lưu lượng mạng đi ra khỏi host
- **Lọc lưu lượng mạng:** ngăn các truy cập trái phép và các hành vi vi phạm chính sách
- **Theo dõi hệ thống file:** ngăn việc truy cập, thay đổi, ghi đè, hoặc xoá file, từ đó có thể ngăn việc cài đặt malware cũng như các tấn công có truy cập file không phù hợp



Các khả năng khác

- **Giới hạn các thiết bị removable:** giới hạn sử dụng các thiết bị removable, cả dạng USB và truyền thống
- **Giám sát các thiết bị nghe nhìn:** giám sát các host khi kích hoạt hoặc sử dụng các thiết bị nghe nhìn, như microphone, camera, điện thoại IP,…
- **Host Hardening:** gỡ bỏ app không cần thiết; khóa port, dịch vụ không cần thiết; khóa/thay đổi tài khoản/mật khẩu mặc định,...
- **Theo dõi trạng thái tiến trình:** Một số sản phẩm theo dõi trạng thái các tiến trình/dịch vụ đang chạy trên host, nếu phát hiện đã dừng, các sản phẩm này có thể tự động khởi chạy lại chúng
- **Làm sạch (sanitize) lưu lượng mạng**: Một số agent, thường là loại triển khai dựa trên phần cứng, có thể làm sạch lưu mạng theo dõi được

Quản lý

- **Triển khai**
  - **Kiểm tra và triển khai các thành phần:** Sau khi đánh giá các thành phần của host-based IDPS trên môi trường thử nghiệm, các tổ chức nên triển khai trên một vùng thí điểm nhỏ trong mạng sản xuất
  - **Bảo vệ các thành phần:** Nếu như các server quản lý và console cần chứng thực với mỗi agent để quản lý và thu thập dữ liệu từ chúng, thì doanh nghiệp nên đảm bảo rằng cơ chế chứng thực có thể quản lý và bảo mật đúng cách
- **Vận hành**
  - ***Tương tự như các công nghệ IDPS điển hình***
  - Một số agent có khả năng định kỳ kiểm tra cập nhật trên server quản lý và tự động lấy về để cài đặt/áp dụng các cập nhật đó

Các hạn chế

- **Độ trễ khi tạo cảnh báo và báo cáo tập trung:**
  - Một số kỹ thuật được sử dụng để định kỳ xác định các sự kiện vốn đã diễn ra hoặc chỉ sử dụng theo giờ hoặc thậm chí chỉ vài lần trong ngày, tạo ra độ trễ đáng kể trong việc xác nhận các sự kiện nhất định nào đó
  - Nhiều host-based IDPS được thiết kế để chuyển cảnh báo đến server quản lý định kỳ, chứ không theo thời gian thực
- **Sử dụng tài nguyên của host:** Hoạt động trên agent có thể làm chậm các hoạt động khác như kết nối mạng và sử dụng hệ thống file
- **Xung đột với các cơ chế kiểm soát an ninh đang có:** ví dụ personal firewall, nếu có các chức năng bị trùng lặp

HIDPS

Ưu điểm và Nhược điểm

- **Ưu điểm:**
  - Phát hiện các sự kiện trên hệ thống host, phát hiện thay đổi trong các file, bộ nhớ và ứng dụng
  - Có thể xử lý lưu lượng đã bị mã hoá (encrypted) để phát hiện các tấn công mà NIDS không thể phát hiện
  - Có thể so sánh các record lưu trong log theo dõi
- **Nhược điểm:**
  - Thêm vấn đề quản lý, cần triển khai agent trên mỗi host muốn giám sát
  - Có thể chịu các tấn công trực tiếp hoặc tấn công vào host, dễ bị 1 số tấn công DoS
  - Cần một không gian ổ đĩa lớn, có thể ảnh hưởng đến hiệu suất của host

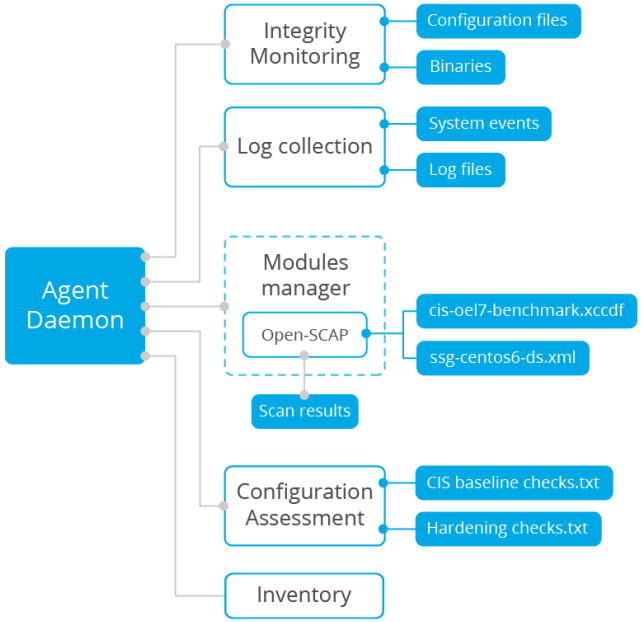
Một số nền tảng HIDPS

- Hầu hết HIDPS sử dụng phần mềm trên host và một số chức năng quản lý bảo mật tập trung cho phép tích hợp với các dịch vụ theo dõi an ninh mạng và threat intelligence.
  - **Ví dụ**: Cisco AMP, AlienVault USM, Tripwire, Wazuh, và Open Source HIDS SECurity (OSSEC)
  - OSSEC sử dụng server quản lý trung tâm và các agents cài đặt trên các host riêng biệt

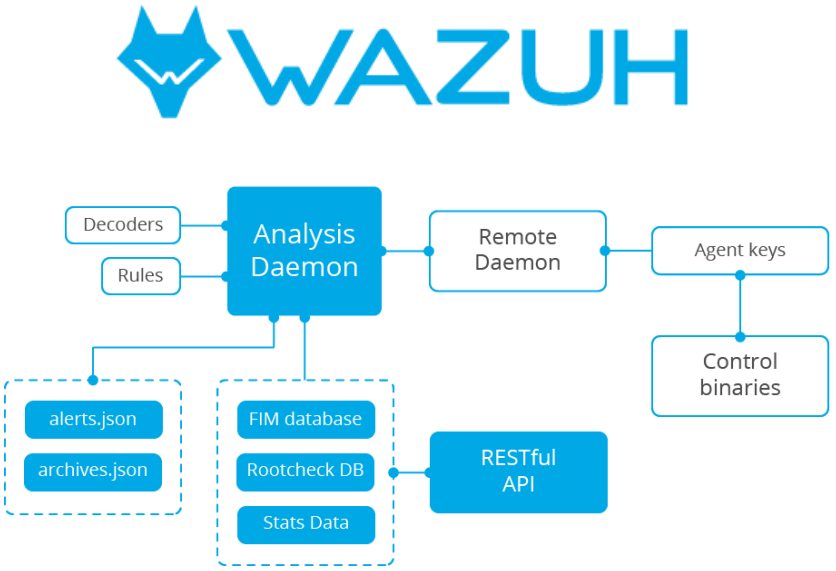
HIDPS

Wazuh – Nền tảng bảo mật mã nguồn mở toàn diện

Security Analytics | Intrusion Detection | Log Data Analysis | File Integrity Monitoring | Vulnerability Detection | Configuration Assessment | Incident Response | Regulatory Compliance | Cloud Security | Containers Security



Wazuh agent



Wazuh server

Nhắc lại

Chuẩn bị cho tuần sau…

- Hôm nay: **Host-based IDPS**

- Chuẩn bị cho buổi sau: **Security Monitoring, SIEM, SOC**
  - *SIEM: Security information and event management*
  - *SOC: Security operations center*
    - Theo khoá học CCNA Cybersecurity Operation

Câu hỏi/thắc mắc nếu có???

Today end, **See you next week!**