CONFIGURATION OF WAZUH AS ENDPOINT DETECTION AND RESPONSE

NT534.P21.ANTT

MSc. Nguyễn Duy

Nhóm 6

22520645 - Nguyễn Phan Hữu Khánh

22520677 - Nguyễn Hồ Nhật Khoa

22520720 - Nguyễn Thanh Kiệt

Content

1. Context
2. Technology Trends
3. Objectives
4. Business && non-business requirement
5. Architecture
6. Demo

Context

STT	Painpoint	Description
1	Visibility attacks	Thiếu khả năng nhìn toàn diện các vector tấn công
2	Detection attacks	Khó quan sát advanced threats, attack chains
3	Response attacks	Manual response khiến quá trình restore bị delay
4	Alert fatigue	FP nhiều gây khó khăn cho việc quan sát, phân tích
5	Using human resources	Sử dụng nhân lực không hiệu quả

Technology Trends

STT	Painpoint	Trends
1	Visibility attacks	Unified Dashboard
2	Detection attacks	Kết hợp nhiều engine AV,HIDS,Vul Management, Threat Intelligence
3	Response attacks	Playbooks
4	Alert fatigue	Prioritize alerts
5	Using human resources	Security Tier 2,3

Objectives

- Xây dựng được kiến trúc cơ sở hạ tầng với môi trường ảo để minh họa
- Minh họa automatic response với custom script kết hợp VirusTotal
- Minh họa các detection engines: AV,HIDS,Vul Management
- Minh họa threat intelligence với MITRE ATT&CK trong cuộc tấn công APT

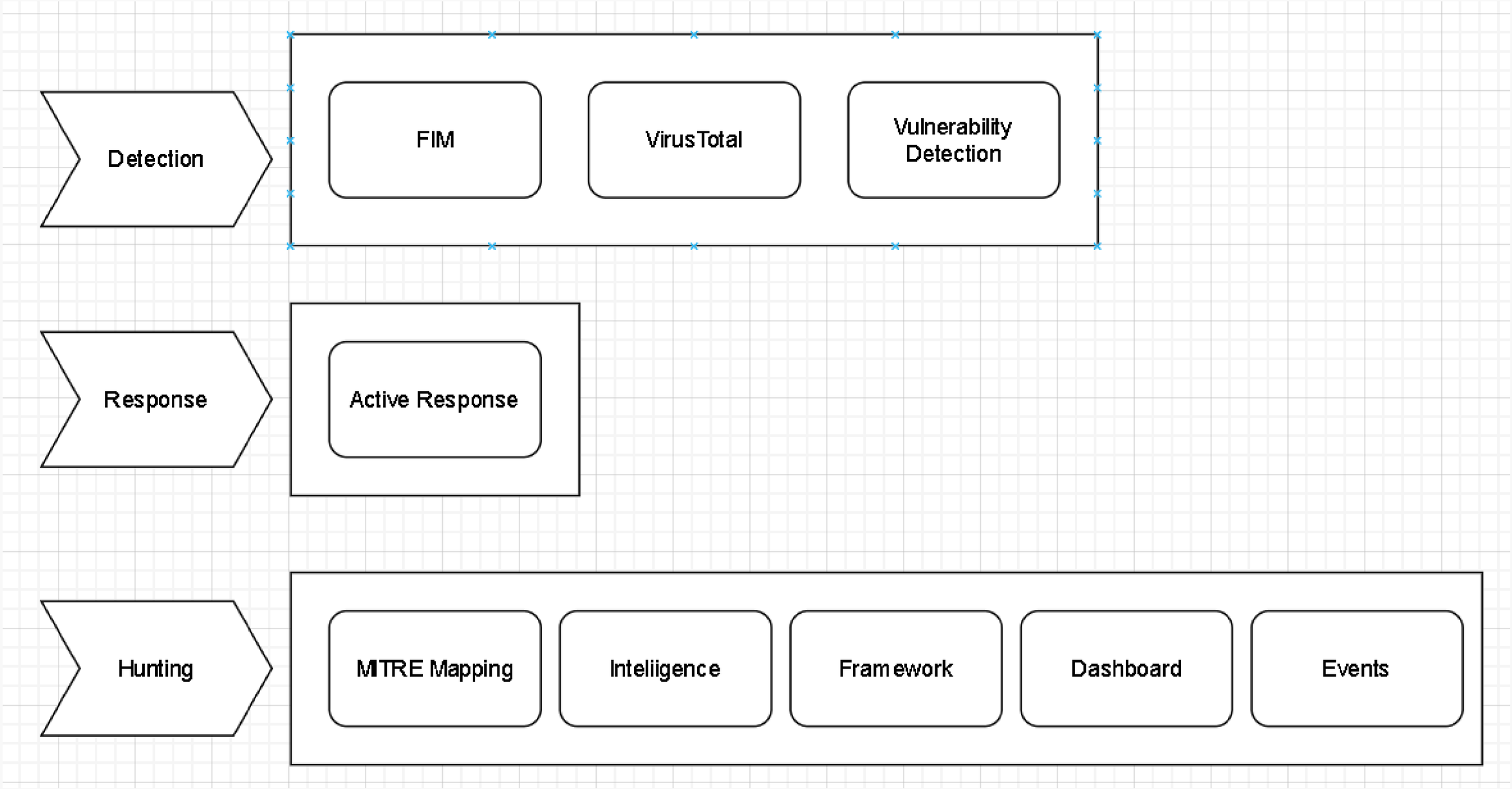
Requirement

STT	Business	Description
1	Visibility attacks	• Custom một dashboard để có khả năng hiển thị toàn diện các cuộc tấn công vào endpoint
2	Detection attacks	• Sử dụng nhiều detection engine kết hợp MITRE framework để nhận biết chuỗi tấn công phức tạp.
3	Response attacks	• Dùng pre-defined playbooks để phản hồi tự động khi có alert
4	Alert fatigue	• Phản hồi theo mức độ ưu tiên của alert
5	Using human resources	• Tăng hiệu suất trong response và threat intelligence

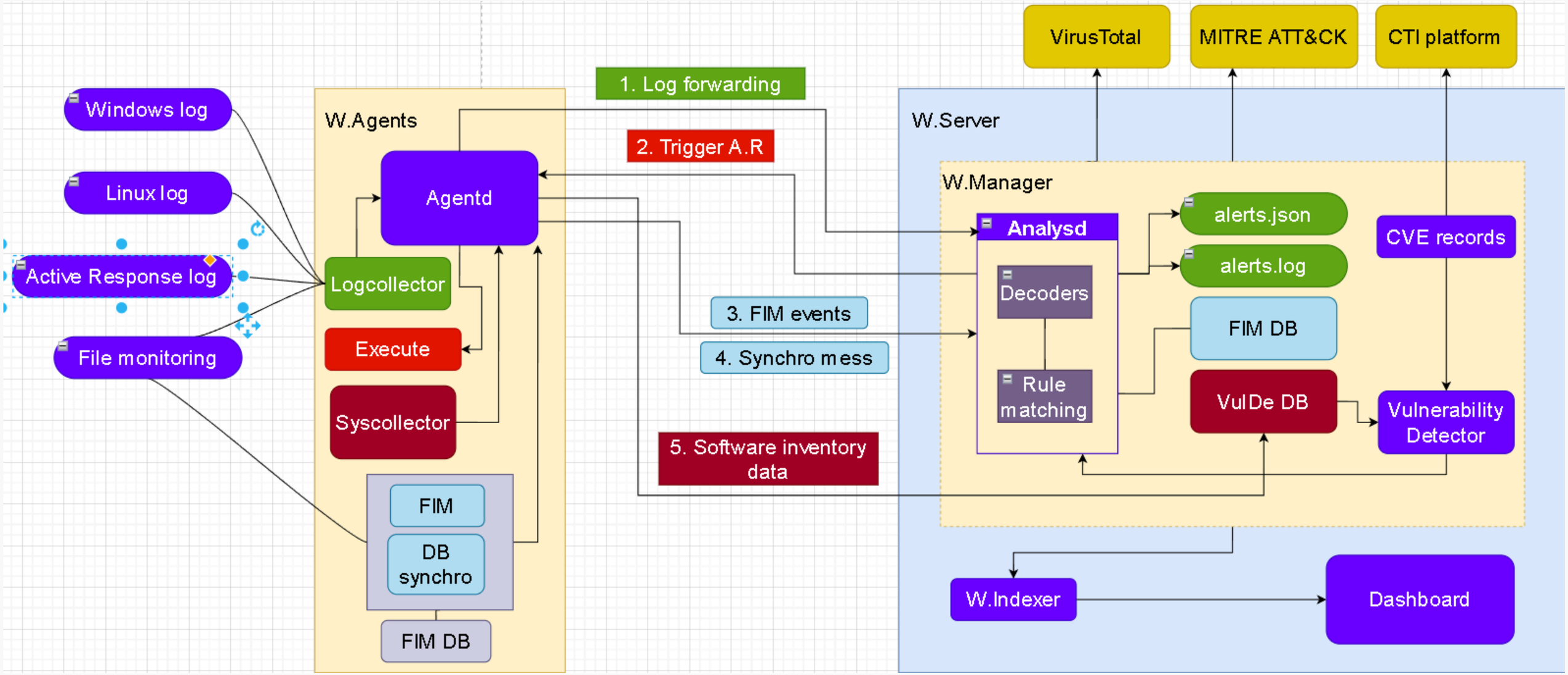
Requirement

STT	Non-business	Description
1	Business Volume: - Users: Y1, Y2, Y3 - Concurrence users: Y1, Y2, Y3	• Users: Y1=80, Y2=100, Y3=120 • Concurrence users: Y1=60, Y2=80, Y3=100
2	Define: - RTO - RPO	• RTO <= 2 giờ • RPO <= 1 giờ
3	Backup & Restore	• Dữ liệu được backup cần phải được mã hoá • 7-days snapshot, cold storage 90 ngày • Khôi phục trong vòng 1 giờ
4	Computing & Storage: Y1, Y2, Y3	• Y1: 8 vCPU/32GB RAM/5TB storage • Y2: 12 vCPU/48GB RAM/8TB storage • Y3: 16 vCPU/64GB RAM/12TB storage

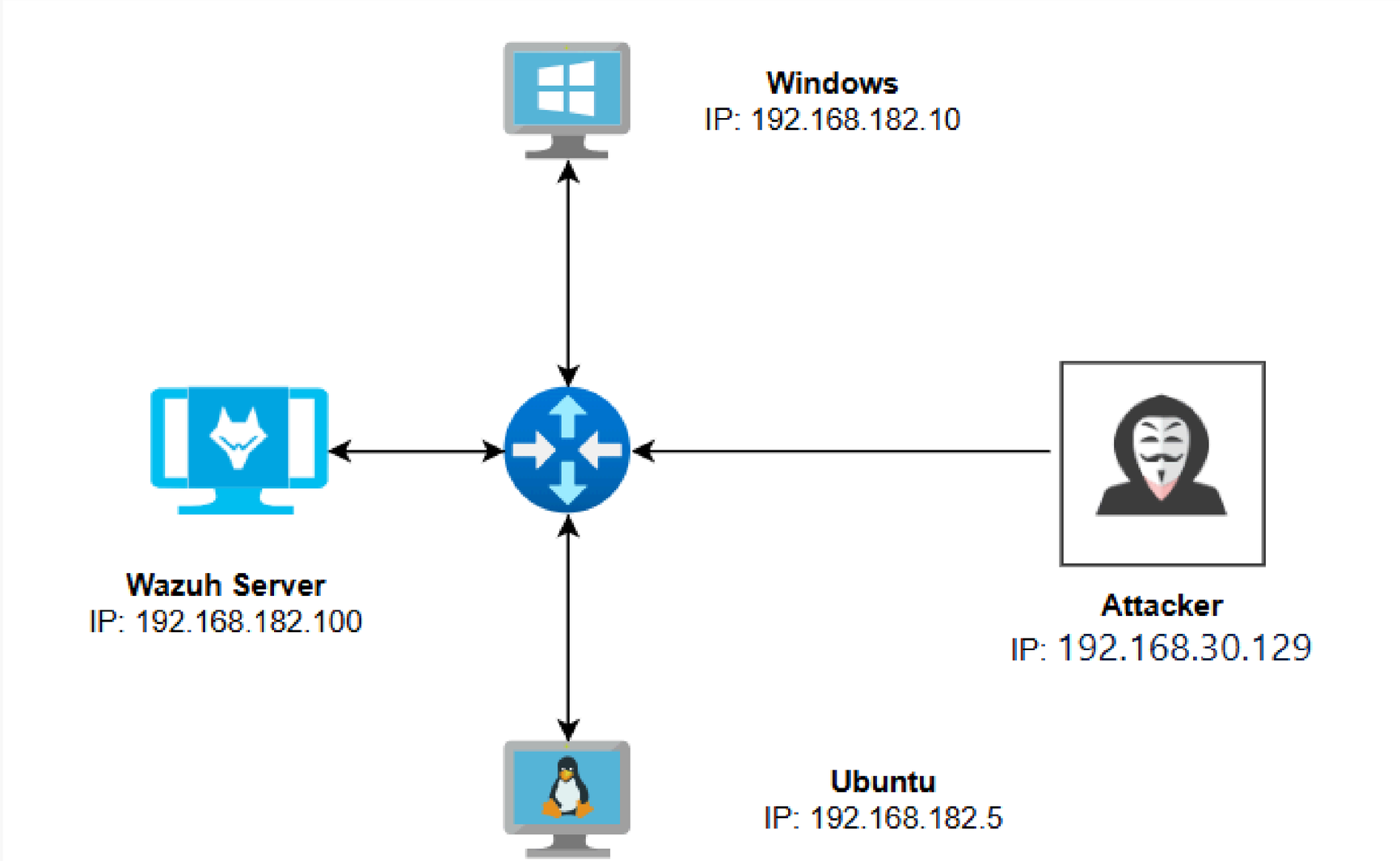
Architecture - functionality



Architecture - data



Architecture - infrastructure



Scenario

Kịch bản 1: Blocking SSH Brute-force Attacks with Wazuh Active Response

Cấu hình Wazuh để phát hiện các địa chỉ IP thực hiện nhiều lần đăng nhập SSH thất bại. Khi phát hiện tấn công brute-force, hệ thống tự động thực thi Active Response để chặn IP tấn công sau 3 lần thử sai, ngăn truy cập tiếp theo và ghi log sự kiện trên Dashboard.

Kịch bản 2: Detecting and removing malware using VirusTotal integration

Cấu hình Wazuh để tích hợp VirusTotal và giám sát thư mục bằng FIM. Khi có tập tin mới được thêm vào, Wazuh gửi hash của tập tin lên VirusTotal để kiểm tra. Nếu tập tin bị đánh dấu là độc hại, Wazuh tự động kích hoạt Active Response để xóa tập tin khỏi hệ thống, đồng thời ghi log kết quả xử lý trên Dashboard.

Scenario

Kịch bản 3: OS Vulnerability Detection

Cấu hình Wazuh để tự động quét và phát hiện các lỗ hổng bảo mật tồn tại trong phần mềm hệ điều hành. Sau khi cài đặt một phiên bản phần mềm có chứa lỗ hổng (CVE), hệ thống nhanh chóng ghi nhận, phân tích và hiển thị cảnh báo chi tiết về mã CVE, mức độ nghiêm trọng và tên phần mềm liên quan ngay trên Dashboard

Kịch bản 4: Detecting APT attack chain with MITRE framework

Wazuh được cấu hình để sử dụng Sysmon trên Windows nhằm phát hiện khi PsExec tạo service PSEXESVC (dấu hiệu của privilege escalation). Rule của Wazuh được ánh xạ với MITRE ATT&CK ID T1543.003 để hiển thị thông tin tactic và technique trên Dashboard, hỗ trợ điều tra và phản ứng nhanh.

Thank you
for watching