Nhóm 4

SIEM (Security Information and Event Management)

Elastic Stack

(ELK) Elasticsearch, Kibana & Logstash

Hồ Hoàng Diệp 22520249

Đinh Lê Thành Công 22520167

Overview

Elastic Stack (ELK Stack) là công cụ mạnh mẽ dùng để thu thập, xử lý, lưu trữ, tìm kiếm và hiển thị dữ liệu log hoặc event

1. **Elasticsearch** - là công cụ search engine, chức năng chính là lưu trữ và lập chỉ mục dữ liệu log hoặc event theo thời gian thực

2. **Logstash** - công cụ thu thập và xử lý log từ nhiều nguồn khác nhau. Nhận log từ các nguồn như syslog, filebeat,... Phân tích, định dạng (grok, mutate, kv...), lọc và chuyển đổi dữ liệu (parsing)

3. **Kibana** - công cụ giao diện web để trực quan hóa dữ liệu được lưu trong Elasticsearch. Chức năng chính là vẽ dashboard, biểu đồ; tạo truy vấn, alert và phân tích hành vi bảo mật

Modules

1. Log Collection: Thu thập log từ nhiều nguồn
2. Log Ingestion & Parsing: Nhận và xử lý log
3. Data Storage & Search Module (Elasticsearch)
4. Detection - Setup Rules & Alert Module
5. Visualization & Dashboard (Kibana)
6. Threat Intelligence Module

Technology Stack Overview

Firewall - Pfsense

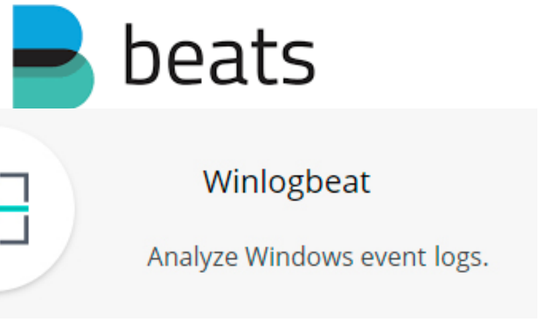
IDS mode Inline - Snort

Web Server (Apache) - DVWA

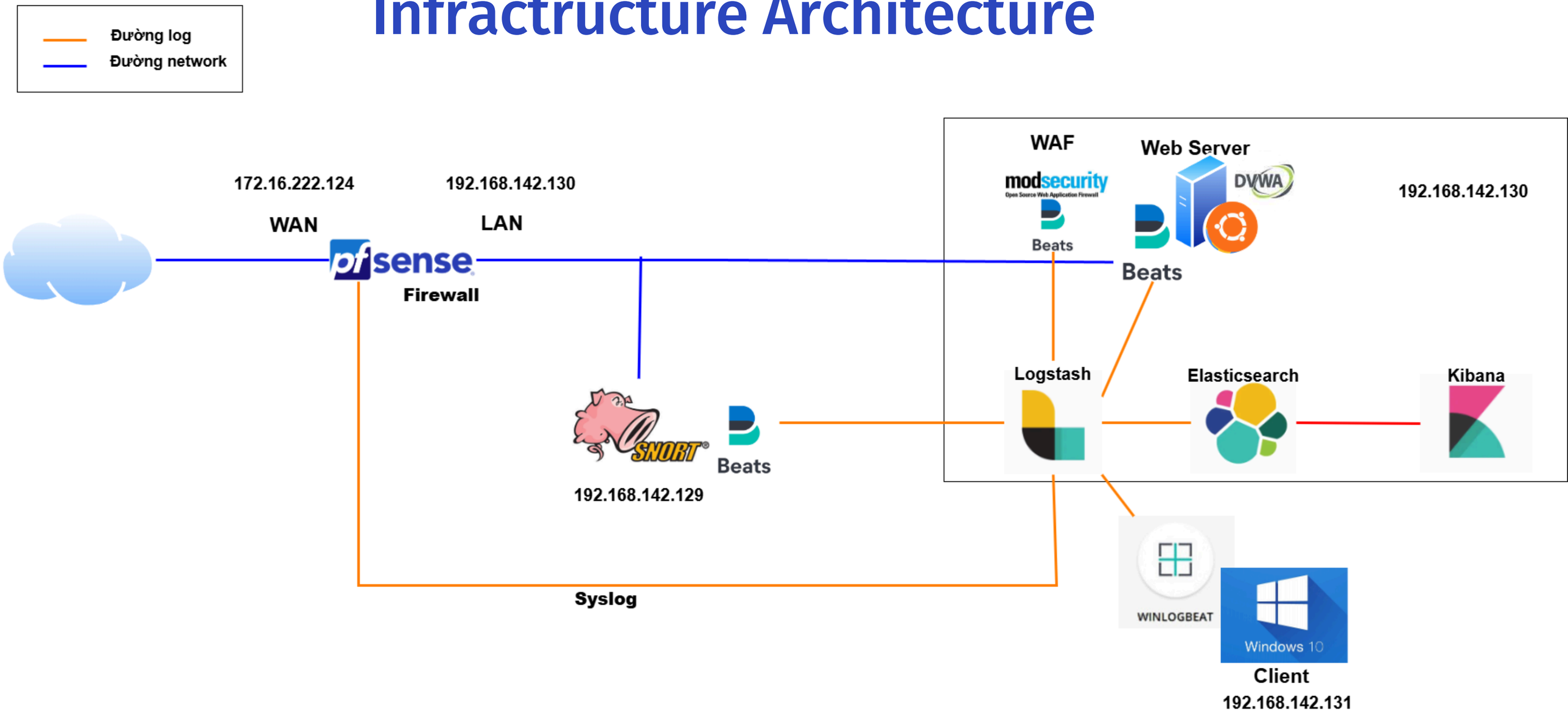
WAF - Modsecurity

Client - Windows 10

Elasticsearch Logstash Kibana



Infractructure Architecture



Demo 1
Log Collection

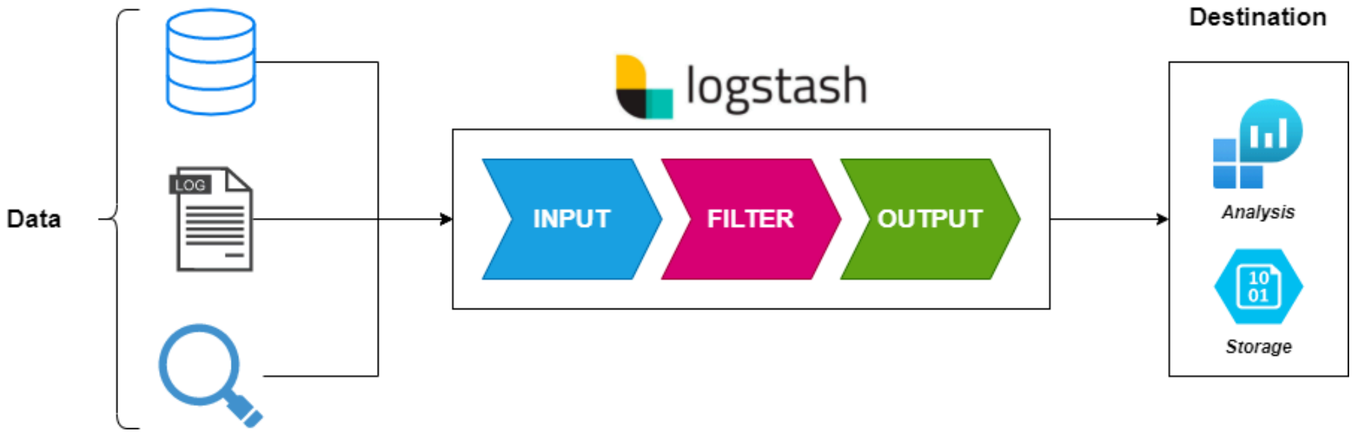
Filebeat: Thu thập log file từ hệ thống, ứng dụng, Apache

Winlogbeat: Thu thập Windows Event Log (Security, System, App...)

Syslog: Thu thập log trực tiếp từ các thiết bị trong mạng như firewall

Demo 2: Log Ingestion & Parsing (logstash)

- ***Input:*** Log được thu thập sẽ gửi đến Logstash.
- ***Filter:*** giai đoạn phân tích, trích xuất, định dạng lại log.
  Một số plugin filter phổ biến:
  - grok: tách chuỗi log bằng regex.
  - mutate: đổi tên, xóa, chuyển đổi dữ liệu.
  - kv: phân tích key=value.
  - geoip: thêm thông tin địa lý từ IP.
  - date: chuẩn hóa thời gian.



- ***Output:*** Sau khi xử lý, Logstash sẽ gửi dữ liệu đến nơi lưu trữ hoặc các hệ thống khác. Thông thường là gửi đến Elasticsearch để phân tích bằng Kibana

Demo 3: Elasticsearch - Data Storage & Search Module

- Vai trò chính: Lưu trữ, lập chỉ mục (index), tìm kiếm dữ liệu log/event
- Cách tổ chức dữ liệu trong Elasicsearch:
  - Index - mỗi loại log có thể là 1 index riêng
  - Document là một bản ghi log - được lưu trữ ở dạng JSON.
  - Field: từng thuộc tính trong document
- Hỗ trợ truy vấn bằng DSL hoặc KQL

Demo 4: Detection - Setup Rules & Alert Module

Detection Rules

- KQL-based Rule: Cho phép viết truy vấn trên index giống như tìm kiếm trong Kibana
- Thiết lập về Threshold

Alerting

- Khi có log match với Rule, các thông này sẽ được thông báo và lưu trữ riêng cho tới khi được xử lý
- Hỗ trợ gửi cảnh báo về email & Slack

Demo 5 Visualization & Dashboard (Kibana)

Vai trò: Trực quan hóa log, event và các alert.

- Giám sát trạng thái theo thời gian thực
- Phân tích và điều tra các sự kiện bất thường
- Xây dựng security reports dễ hiểu

Kiban cung cấp nhiều loại biểu đồ và công cụ mạnh mẽ: Line/Area/Bar Chart, Map, Pie Chart...

Dashborad tập hợp các visualization giúp quan sát toàn cảnh hệ thống