SIEM

Security Information and Event Management

Nhóm 4

Đinh Lê Thành Công – 22520167

Hồ Hoàng Diệp – 22520249

AGENDA

- Context
- Technology Trends
- Project Objectives (Scope & Out of Scope)
- Business Requirements & Non-Business Requirements
- Architectures (Function / Application / Data / Infrastructure)
- Scenarios Demo

CONTEXT

Pain point 1

Detection attacks

Too many alert and high rate FP when using Rule-based detection
And lack of context enrichment
Advanced attacks often bypass the rules

Pain point 2

Scalability & performance

SIEM fails to ingest and analyze large volumes of log data in real time, causing delays in detection and response

Pain point 3

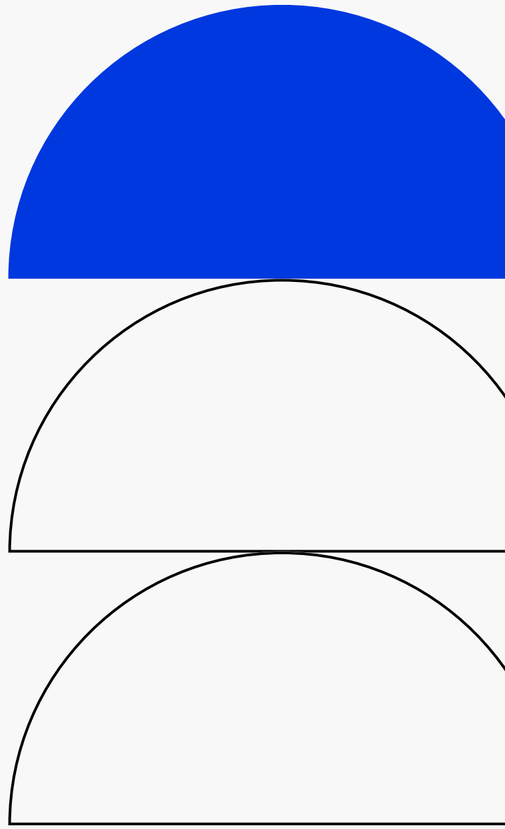
Manual Incident Response

Do not automatically after alerting: open ticket, send mail, block firewall...

Pain point 4

Cost, Maintenance and Human resources

High-fee License, storage for log, more employee for maintenance.



TECHNOLOGY TRENDS

Pain point 1: Detection attacks

→ **Integrate AI/ML and UEBA for behavioral detection**

Pain point 2: Scalability & performance → Using Cloud-native SIEM to ingest millions of events per second without backlog

Pain point 3: Manual Incident Response → SOAR và automation playbook (isolate host, block IP, kill processes)

Pain point 4: Cost, Maintenance and Human resources → Automation was used to deploy log agents, network extraction, and configuration of data sources.

PROJECT OBJECTIVES

In Scope

- Log Ingestion & Parsing
- Elasticsearch – Data Storage & Search Module
- Detection – Setup Rules & Alert Module
- Visualization & Dashboard
- Integration with SOAR System combined with playbook

Out Scope

- Dark web monitoring
- Cloud or Hybrid SIEM
- User and Entity Behavior Analytics (UEBA)
- Data Loss Prevention & File Integrity Monitoring
- Detection based on MITRE ATT&CK

Business Requirement

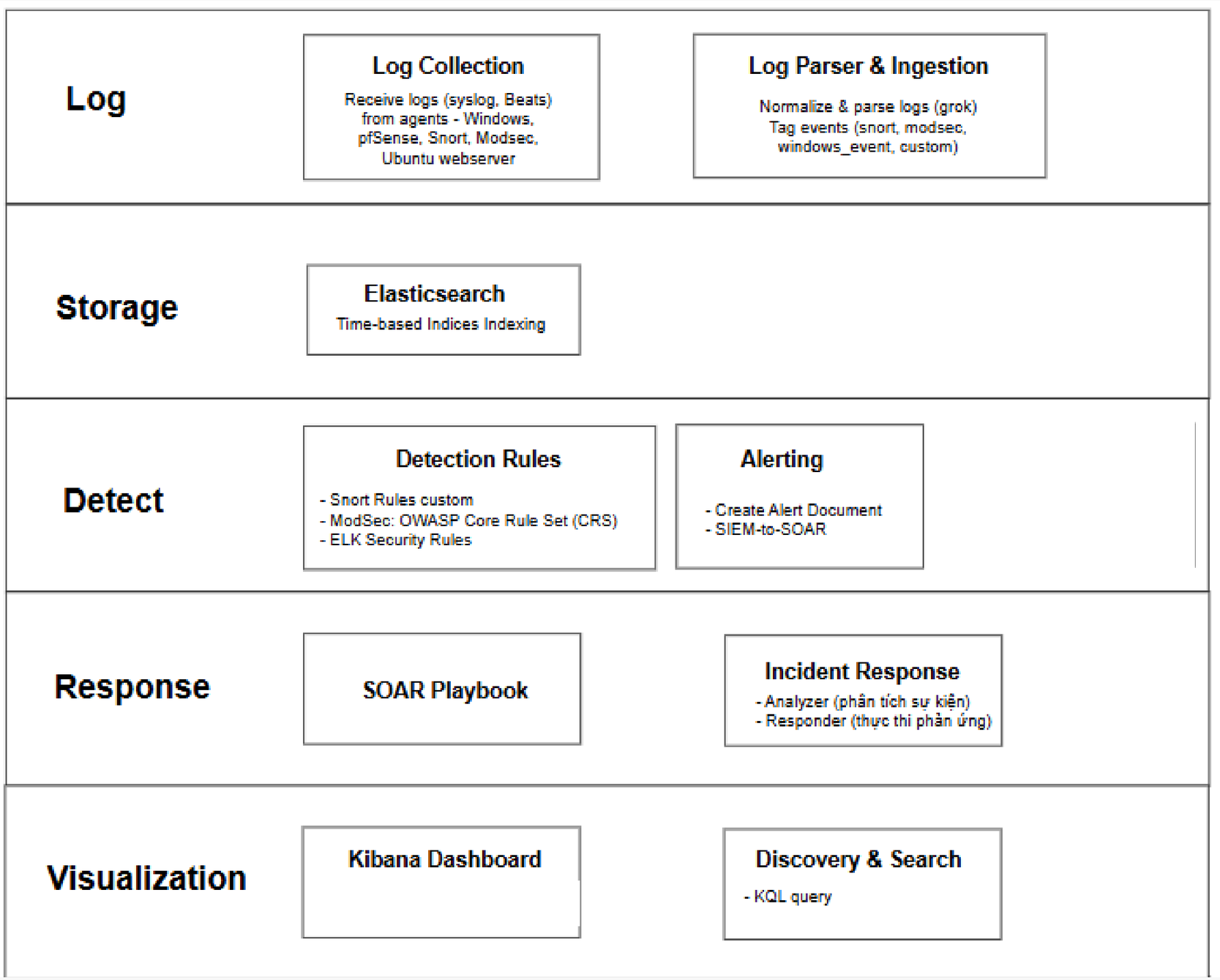
No.	Business Requirements	Solution
1	**Real-time Threat Detection**	Correlation rules, anomaly detection (SIEM rules, Snort rules...)
2	**Unified Log Visibility**	Log shippers (Filebeat, Winlogbeat, syslog)
3	**Accurate and Flexible Log Parsing**	Parsing firewall/WAF logs by Grok patterns in Logstash, custom pipelines
4	**Incident Response Enablement**	Intergration with SOAR (e.g., Cortex, TheHive) using playbook
5	**Security Posture Reporting**	Dashboards and executive reports (e.g. Kibana)

Non-Business Requirement

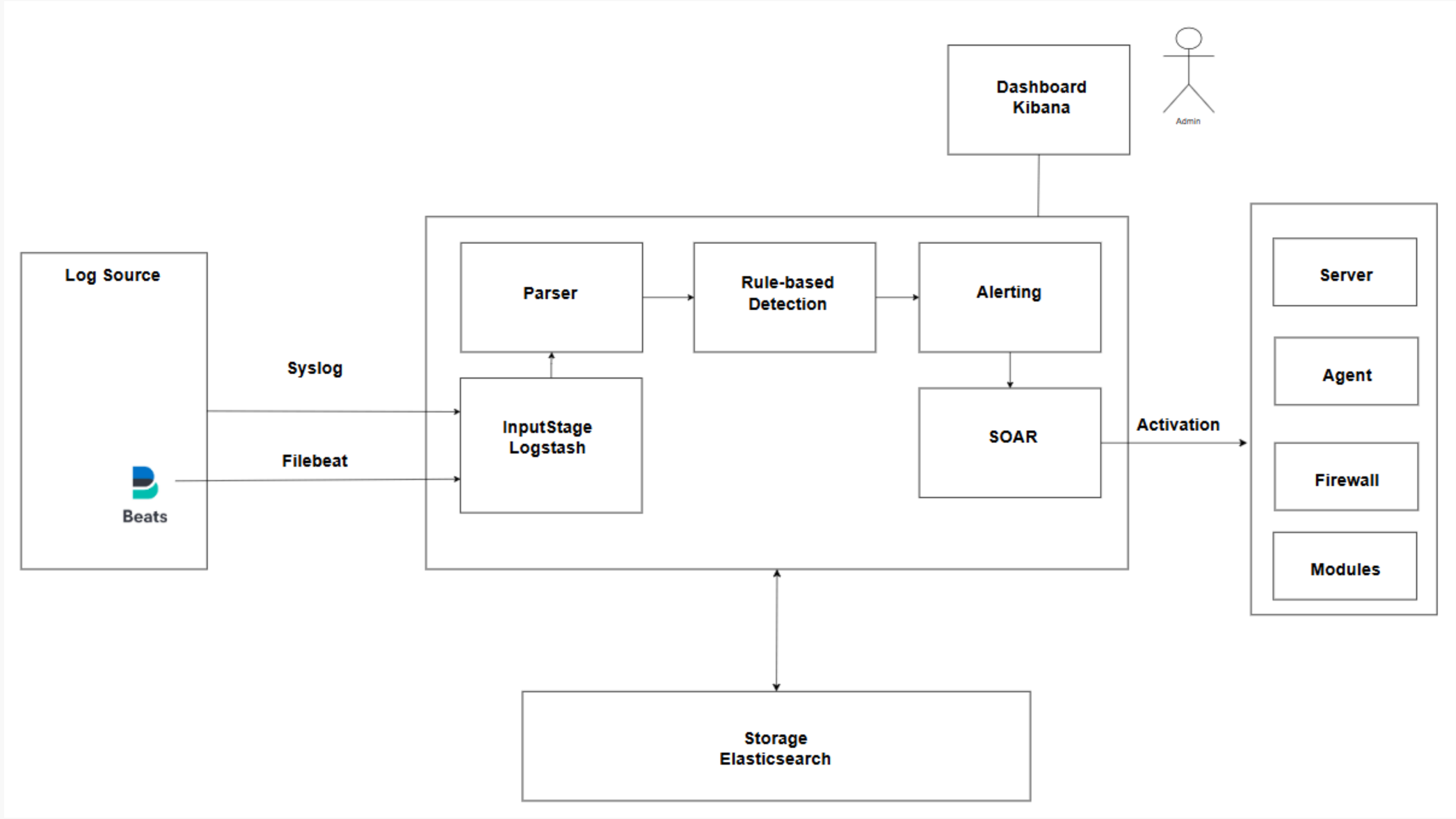
No.	Non-Business Requirements	Description
1	**Performance**	Logstash pipelines and tested ingestion from ModSecurity, Snort, etc. Real-time alerts working
2	**Network Security**	Use of pfSense to network segmentation, NAT and isolate internal SIEM components for public exposure
3	**Application Security**	Cortex integrates with TheHive to run analyzers (e.g., VirusTotal) and responders (e.g., block IP). Access to these tools is role-based.

THYNK UNLIMITED

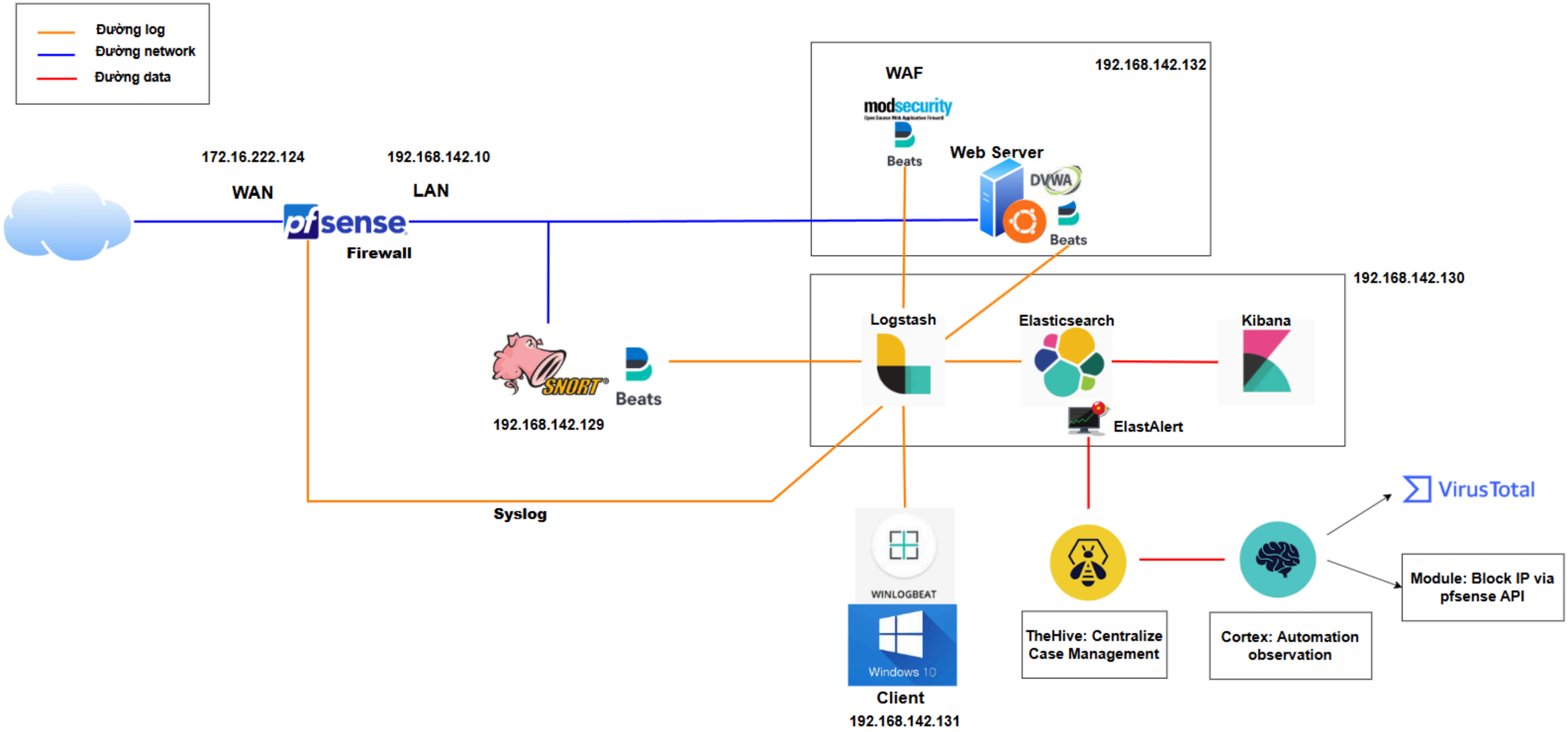
Function Architecture



Application/Data Architecture



Infrastructure Architecture



DEMO

- LOG COLLECTION, LOG INGESTION & PARSING
- SEARCHING & INVESTIGATION
- ALERTING
- VISUALIZATION & DASHBOARD
- DETECTION AND RESPONSE (SQL INJECTION & XSS)