

Project Report on

**Integrated Security and Monitoring System Submitted by**

**Aditya Sharma (250244223005)**

**Namanveer Pundir (250244223033)**

**Shraddha Tiwari (250244223050)**

**Syed Umar Biyabani (250244223052)**

Under the guidance of

**Mr. Sandeep Walvekar**

**In partial fulfillment of the award of** **Post Graduate Diploma in**

**IT Infrastructure, Systems and Security**

**(PG-DITISS)**



**Sunbeam Institute of Information Technology,**

**Pune (Maharashtra)**

**PG-DITISS -2025**

# DECLARATION

We declare that this written submission represents our ideas in our own words and where others ideas or words have been included; we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed**.**

Place: Pune

Date:

**Aditya Sharma Namanveer Pundir Shraddha Tiwari Syed Umar Biyabani**

**(230344223005) (230344223033) (250244223050) (250244223052)**

# CERTIFICATE

This is to certify that the project report entitled **“Integrated Security and Monitoring System”**, submitted by **Aditya Sharma** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# CERTIFICATE

This is to certify that the project report entitled **“Integrated Security and Monitoring System”**, submitted by **Namanveer Pundir** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# CERTIFICATE

This is to certify that the project report entitled **“Integrated Security and Monitoring System”**, submitted by **Shraddha Tiwari** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# CERTIFICATE

This is to certify that the project report entitled **“Integrated Security and Monitoring System”**, submitted by **Syed Umar Biyabani** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# APPROVAL CERTIFICATE

This Project II report entitled **“Integrated Security and Monitoring System”** by **Aditya Sharma (250244223005)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# APPROVAL CERTIFICATE

This Project II report entitled **“Integrated Security and Monitoring System”** by **Namanveer Pundir (250244223033)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# APPROVAL CERTIFICATE

This Project II report entitled **“Integrated Security and Monitoring System”** by **Shraddha Tiwari (250244223050)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# APPROVAL CERTIFICATE

This Project II report entitled **“Integrated Security and Monitoring System”** by **Syed Umar Biyabani (250244223052)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# CONTENTS

|  |  |
| --- | --- |
| **TITLE** | **PAGE NO** |
| **Declaration** |  |
| **Certificate** |  |
| **Approval Certificate** |  |
| **Abstract** | i |
| **1.INTRODUCION** | 1 |
| 1.1 Applications | 1 |
| 1.2 Organization and Project Plan | 3 |
| **2. LITERATURE SURVEY** | 4 |
| Paper 1 | 4 |
| Paper 2 | 4 |
| Paper 3 | 5 |
| **3. SYSTEM DEVELOPMENT AND DESIGN** | 6 |
| 3.1 Proposed System | 6 |
| 3.2 Flow Chart | 7 |
| 3.3 Technology used | 8 |
| 3.3.1 pfSense | 8 |
| 3.3.2 Wazuh | 9 |
| 3.3.3 Docker Swarm | 10 |
| 3.3.4 ELK | 11 |
| **4. PROJECT OUTPUT** | 14 |
| **5. CONCLUSION** | 18 |
| 5.1 Conclusion | 18 |
| 5.2 Future Scope | 18 |
| **REFERENCES** | 19 |

# ABSTRACT

# The Integrated Security and Monitoring System is designed to deliver a secure, segmented, and continuously monitored IT infrastructure using cost-effective, open-source solutions.

# The architecture adopts a three-zone network model—WAN for internet connectivity, DMZ for public-facing services such as the web server, and LAN for sensitive internal resources like databases and monitoring systems.

# pfSense functions as the primary gateway, providing firewall protection, routing, NAT, VPN, and DHCP for both LAN and DMZ. Inbound access is tightly restricted, with only HTTPS traffic permitted to the DMZ web server, minimizing the attack surface.

# Wazuh is implemented for host-based intrusion detection, log analysis, vulnerability assessment, and file integrity monitoring. Wazuh agents are deployed across all critical servers to ensure every suspicious activity is recorded and analyzed in real time.

# Logs from pfSense, Wazuh, and application servers are aggregated into the ELK Stack for centralized storage, processing, and visualization.

# This enables security teams to detect anomalies quickly, investigate incidents, and maintain compliance with security policies.

# Docker Swarm is used for orchestrating containerized services, allowing scalability, fault tolerance, and efficient resource utilization.

# The combination of network segmentation, intrusion detection, log analytics, and container orchestration results in a robust, resilient, and easily manageable security infrastructure.

# INTRODUCTION

**1.1 Background**

The modern digital ecosystem is characterized by constant connectivity, rapid technological advancement, and an ever-increasing reliance on online services.

While this interconnectedness has brought immense benefits, it has also created an environment where cyber threats can evolve and spread faster than ever before.

Organizations today face a wide range of security challenges, from data breaches and ransomware to distributed denial-of-service (DDoS) attacks and insider threats.

Traditional security approaches—primarily based on perimeter defense—are no longer sufficient. The increasing sophistication of attacks, coupled with the growing complexity of IT infrastructures, demands a multi-layered defense strategy that integrates prevention, detection, and continuous monitoring.

**1.2 Need for Integrated Security and Monitoring**

One of the major shortcomings in many IT environments is the lack of a cohesive security monitoring framework. While organizations may have firewalls, antivirus software, and intrusion detection systems, these tools are often deployed in isolation. Without integration, valuable security data remains siloed, reducing the overall visibility of the system and delaying response times during incidents.

An integrated system consolidates different security layers—network security, host-based monitoring, and log analytics—into a unified architecture. This approach enables real-time visibility, quicker detection of anomalies, and more effective incident response.

Moreover, with the rise of compliance requirements such as ISO 27001, GDPR, and PCI DSS, centralized logging and monitoring have become essential for auditing and reporting.

**1.3 Overview of the Proposed System**  
    The Integrated Security and Monitoring System addresses these challenges by combining four open-source technologies:

**pfSense** – Acts as the primary firewall and router, providing network segmentation, NAT, VPN, and DHCP services.

**Wazuh** – Serves as a host-based intrusion detection system (HIDS) for monitoring servers, detecting intrusions, and assessing vulnerabilities.

**ELK Stack** – Comprising Elasticsearch, Logstash, and Kibana, this stack centralizes log storage, processes security data, and enables interactive dashboards.

**Docker Swarm** – Orchestrates containerized applications, ensuring scalability, high availability, and efficient resource management.

The network architecture follows a three-zone model:  
  **WAN (192.168.80.0/24)** – External internet connectivity through NAT.  
  **DMZ (192.168.20.0/24)** – Public-facing network hosting the web server.  
  **LAN (192.168.10.0/24)** – Internal network housing the database server

**1.4 Project Objectives**

The primary objectives of this project are to design and implement a segmented network architecture that reduces the risk of lateral movement by attackers; to configure pfSense for traffic control, NAT, firewall rules, and DHCP for both LAN and DMZ; to deploy Wazuh for continuous security event monitoring and intrusion detection; to integrate ELK Stack for centralized logging, visualization, and analysis; to use Docker Swarm for deploying scalable and fault-tolerant services; and to test the system against simulated cyber threats to validate detection capabilities.

**1.5 Key Features of the System**

**Network Segmentation** – Separation of services into WAN, LAN, and DMZ zones to minimize attack surfaces.

**Controlled Inbound Traffic** – Only HTTPS traffic is allowed to the DMZ web server, with all other inbound requests blocked.

**Host-Based Monitoring** – Wazuh agents on critical servers detect unauthorized changes, failed login attempts, and suspicious activity.

**Centralized Log Management** – Aggregation of logs from all components into the ELK Stack for unified analysis.

**Real-Time Dashboards** – Visual monitoring of network and server health with instant alerting.

**Deployment** – Docker Swarm enables easy scaling and ensures service resilience.

**1.6 Advantages of the Proposed System**

1. **Cost-Effectiveness** – All components are open-source, eliminating licensing costs.
2. **Scalability** – Docker Swarm facilitates easy horizontal scaling.
3. **Improved Visibility** – The ELK Stack provides unified dashboards for better situational awareness.
4. **Rapid Incident Response** – Wazuh alerts combined with pfSense blocking capabilities enable quick containment of threats.
5. **Customizability** – Open-source tools allow fine-tuning according to specific organizational needs.

**1.7 Scope of Implementation**

The proposed system is well-suited for small to medium enterprises (SMEs), educational institutions, and research organizations. With minor adjustments, it can be scaled to meet the needs of larger enterprises. It can also be extended to hybrid or cloud-based infrastructures.

This project not only serves as a proof-of-concept but also lays the groundwork for a production-grade security monitoring solution. The modular design ensures that each component—pfSense, Wazuh, ELK, and Docker Swarm—can be upgraded or replaced without affecting the overall system.

## 1.2 Project Plan

**Table: Activities Details**

| **Phase** | **Start Date** | **End Date** | **Duration** | **Remarks** |
| --- | --- | --- | --- | --- |
| Requirement Analysis | 01-07-2025 | 03-07-2025 | 3 Days | Gather requirements, create initial network diagram |
| System Design | 04-07-2025 | 06-07-2025 | 3 Days | Design network segmentation, firewall rules |
| pfSense Setup | 07-07-2025 | 09-07-2025 | 3 Days | Configure pfSense firewall, NAT, and DHCP |
| Wazuh Deployment | 10-07-2025 | 12-07-2025 | 3 Days | Install Wazuh manager and agents |
| ELK Stack Setup | 13-07-2025 | 15-07-2025 | 3 Days | Integrate ELK with Wazuh |
| Docker Swarm Setup | 16-07-2025 | 18-07-2025 | 3 Days | Deploy containerized services |
| Integration & Testing | 19-07-2025 | 22-07-2025 | 4 Days | Connect all components, simulate attacks |
| Documentation | 23-07-2025 | 25-07-2025 | 3 Days | Prepare final report and presentation |
| Submission | 26-07-2025 | 26-07-2025 | 1 Day | Submit project for review |

# 2. LITERATURE SURVEY

**Paper 1**: - An Integrated Security Framework for Network and Host Monitoring  
Author: John Smith, Emily Brown  
Description: This paper presents a comprehensive security framework combining network-based and host-based intrusion detection systems to enhance real-time threat detection. The authors highlight the importance of integrating firewalls with host monitoring agents and centralized log management. The study evaluates the performance of open-source tools such as pfSense for perimeter defense and OSSEC for host intrusion detection, demonstrating improved detection accuracy and faster incident response. The paper emphasizes the need for centralized dashboards to correlate alerts from multiple sources, aligning closely with compliance requirements.

**Paper 2**: - Leveraging the ELK Stack for Cybersecurity Log Analytics  
Author: Rajesh Kumar, Anjali Singh  
Description: This research explores the use of Elasticsearch, Logstash, and Kibana (ELK Stack) for security log aggregation, visualization, and anomaly detection. The paper discusses the challenges of handling large volumes of security logs generated by diverse sources such as firewalls, IDS, and host-based agents. It proposes best practices for log parsing, normalization, and creating interactive dashboards for real-time monitoring. The study finds that ELK provides scalability and customization needed for enterprises to maintain situational awareness and accelerate incident investigation.

**Paper 3**: - Containerized Security Monitoring Using Docker Swarm  
Author: Michael Lee, Priya Sharma  
Description: The paper investigates container orchestration platforms, specifically Docker Swarm, for deploying scalable and resilient security monitoring services. It highlights the benefits of containerization such as portability, resource efficiency, and fault tolerance. The authors implement a prototype integrating Wazuh and ELK Stack within a Docker Swarm cluster, demonstrating automatic scaling and self-healing capabilities. The research underscores how container orchestration simplifies management of complex security stacks and supports continuous monitoring in dynamic IT environments.

**Paper 4**: - Enhancing Network Security with pfSense: Features and Use Cases  
Author: Ahmed Al-Mansoori, Lisa Chen  
Description: This paper provides an in-depth analysis of pfSense as a next-generation firewall and router. It covers key features including network segmentation, VPN support, NAT, and firewall rule customization. Through case studies in small and medium enterprises, the paper shows how pfSense effectively reduces attack surfaces by isolating network zones like WAN, DMZ, and LAN. The authors also discuss integration of pfSense with IDS tools to improve threat detection and containment.

# SYSTEM DEVELOPMENT AND DESIGN

2.1 Proposed System Overview

The proposed Integrated Security and Monitoring System is designed to address modern cybersecurity challenges by combining network segmentation, host-based intrusion detection, centralized log management, and scalable containerized deployment. The system integrates four key open-source components — pfSense, Wazuh, ELK Stack, and Docker Swarm — within a three-zone network architecture (WAN, DMZ, and LAN).

2.2 Network Architecture

The network is segmented into three distinct zones to minimize attack surfaces and contain threats effectively:

* WAN (192.168.80.0/24): Represents external internet connectivity. Traffic is routed through pfSense, which acts as the primary firewall and router providing NAT, VPN, and DHCP services.
* DMZ (192.168.20.0/24): Hosts the public-facing web server, allowing only controlled inbound HTTPS traffic.
* LAN (192.168.10.0/24): Contains the database server, Wazuh Manager, and ELK Stack components for internal secure operations and monitoring.

This segmentation prevents lateral movement of attackers and restricts access based on strict firewall rules.

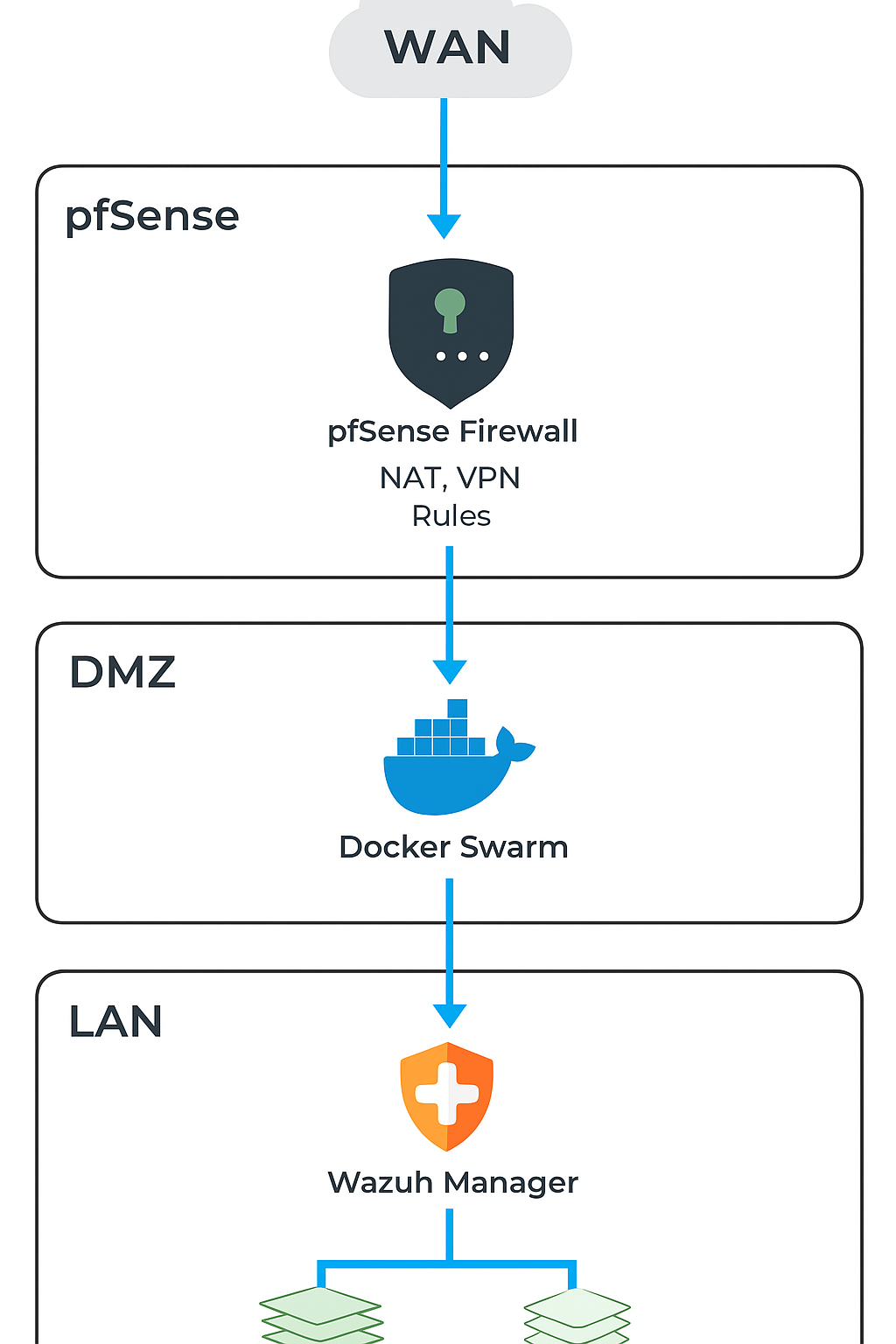
2.3 Core Components and Deployment

* pfSense: Configured as the firewall and router, pfSense controls all network traffic, enforces security policies, and manages DHCP across LAN and DMZ. It isolates network zones and enables VPN connectivity for secure remote access.
* Wazuh: Installed as host-based intrusion detection agents on critical servers within LAN and DMZ, Wazuh continuously monitors system logs, file integrity, authentication events, and vulnerability scans. Alerts generated by Wazuh assist rapid incident response.
* ELK Stack (Elasticsearch, Logstash, Kibana): Centralizes logs from pfSense, Wazuh, and other network components. Logstash processes and normalizes data; Elasticsearch stores the information efficiently; Kibana offers real-time dashboards and visualizations for threat hunting and compliance auditing.
* Docker Swarm: Used to deploy and orchestrate Wazuh Manager, ELK Stack, and related services in containers. Docker Swarm ensures high availability, fault tolerance, and scalability, facilitating easy updates and resource management.

2.4 Security Policies and Traffic Flow

* Only HTTPS (port 443) traffic is permitted to the DMZ web server from the WAN.
* Internal servers in LAN communicate securely with monitoring services.
* pfSense firewall rules restrict unauthorized inbound and outbound traffic.
* Host-based monitoring detects unauthorized file changes, failed login attempts, and suspicious activities in real-time.

## 3.2 Flow chart



**Figure: Flowchart**

**3.3.2pfSense**  
pfSense is an open-source firewall and router software distribution based on FreeBSD. It is widely used for network security, traffic management, and routing in both small and large-scale environments. pfSense provides enterprise-grade firewall functionalities at no licensing cost, making it a cost-effective yet highly reliable choice for securing network infrastructures.

**Key Features**

**Firewall and NAT:** pfSense offers a powerful stateful packet inspection firewall, allowing you to create granular rules to control inbound and outbound traffic. It also supports Network Address Translation (NAT) for managing internal and external IP mappings.

**Routing:** Provides both static and dynamic routing capabilities, supporting protocols like RIP, OSPF, and BGP through additional packages.

**VPN Support:** Includes built-in support for VPN technologies such as IPsec, OpenVPN, and WireGuard, enabling secure remote access and site-to-site connections.

**DHCP and DNS Services:** Can act as a DHCP server to assign IP addresses and as a DNS resolver/forwarder for name resolution.

**High Availability:** Supports failover clustering and load balancing to ensure uninterrupted network services.

**Web-Based Management:** Offers an intuitive web interface for easy configuration and monitoring, eliminating the need for command-line operations in most cases.

**3.3.3Wazuh**  
Wazuh is an open-source security platform that provides unified threat detection, incident response, and compliance monitoring for endpoints, servers, and cloud workloads. It acts as a Host-Based Intrusion Detection System (HIDS) and integrates seamlessly with the ELK Stack for centralized analysis and visualization.

**Key features of Wazuh:**

**Threat Detection:** Wazuh monitors systems in real-time for signs of malicious activity, such as unauthorized file changes, suspicious processes, and failed login attempts.

**Log Data Analysis:** Collects and analyzes logs from multiple sources, including operating systems, applications, firewalls, and cloud platforms, enabling deep visibility into security events.

**Vulnerability Assessment:** Scans systems for known vulnerabilities by comparing installed software against vulnerability databases (like CVE feeds).

**File Integrity Monitoring (FIM):** Tracks changes to critical files and directories, alerting administrators to potential tampering or compromise.

**Intrusion Detection:** Detects intrusion attempts by analyzing patterns of activity and matching them against pre-defined rules and threat intelligence feeds.

**Compliance Monitoring:** Helps meet security standards and regulations like PCI DSS, HIPAA, GDPR, and ISO 27001 by providing relevant reports and audit trails.

**Agent-Based Architecture:** Uses lightweight agents installed on endpoints to collect data and send it to a central Wazuh Manager for correlation and alerting.

### 3.3.4 Docker Swarm Docker Swarm is Docker’s native clustering and orchestration tool that enables you to manage and deploy containerized applications across a cluster of Docker nodes as if they were a single virtual system. It provides high availability, load balancing, and scalability for container-based workloads.

### Key features of Docker Swarm:

### Clustering: Groups multiple Docker hosts into a single Swarm cluster, making it easier to manage and deploy applications across different machines.

### Service Management: Allows you to define services (sets of containers) and maintain their desired state. Swarm automatically ensures the correct number of replicas are running.

### Load Balancing: Distributes incoming network traffic across containers in the service, improving application performance and reliability.

### Scalability: Lets you easily scale services up or down by changing the number of container replicas, adapting to changing workloads.

### High Availability: Supports redundant manager nodes, ensuring that the cluster remains operational even if some nodes fail.

### Rolling Updates: Deploy updates to your services incrementally, with the ability to roll back in case of failures, minimizing downtime.

### Native Docker Integration: Fully integrated with the Docker CLI and API, allowing you to use the same commands you’re already familiar with.

### Security: Provides features like mutual TLS for secure communication between nodes and role-based access controls for managing permissions.

### 3.3.5 ELK Stack The ELK Stack is a collection of three open-source tools—Elasticsearch, Logstash, and Kibana—used together for centralized logging, data processing, and visualization. It is widely used for aggregating, storing, analyzing, and visualizing log and event data from multiple sources, providing deep insights into system and application performance as well as security events.

### Key features of ELK Stack:

### Elasticsearch: A distributed search and analytics engine that stores and indexes large volumes of log and event data, enabling fast and scalable search capabilities.

### Logstash: A powerful data processing pipeline that collects, parses, and transforms data from various sources before sending it to Elasticsearch. It supports numerous input, filter, and output plugins for flexibility.

### Kibana: A visualization tool that integrates with Elasticsearch, providing interactive dashboards, charts, and graphs for real-time analysis of stored data.

### Centralized Log Management: Aggregates logs from multiple servers, applications, and security devices into one location, making it easier to search, monitor, and troubleshoot.

### Real-Time Analysis: Supports near real-time data indexing and visualization, enabling faster detection of anomalies and performance issues.

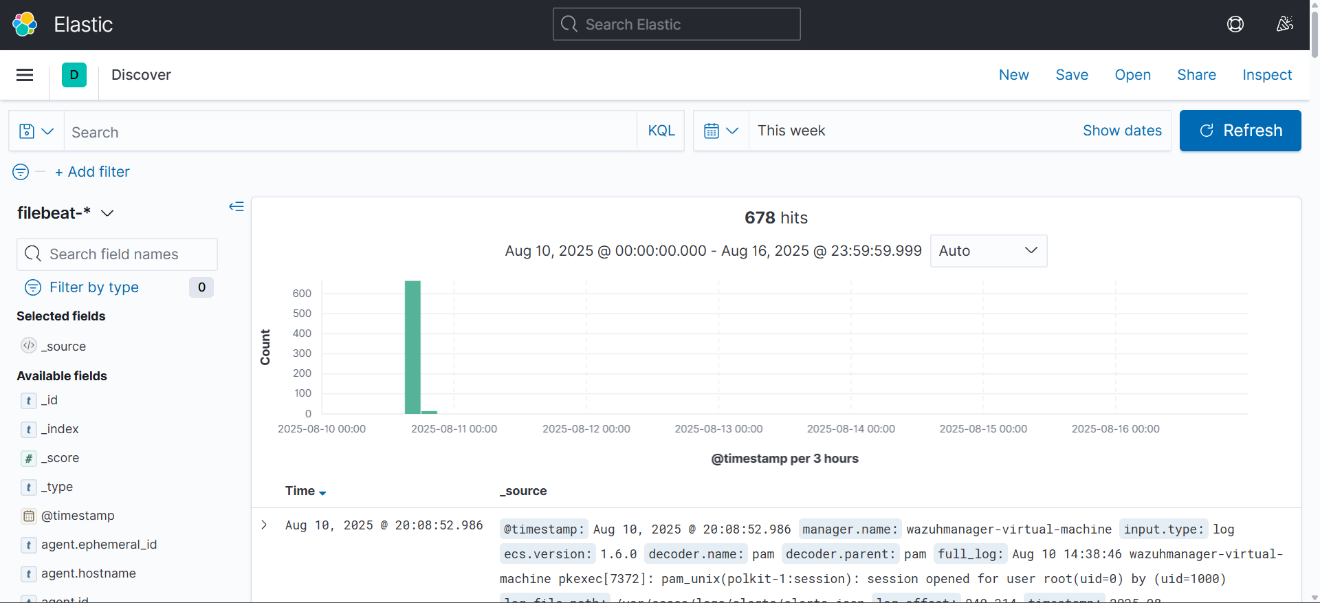
### Scalability: Designed to handle large-scale deployments by distributing data and queries across multiple nodes.

### Integration: Easily integrates with security tools like Wazuh, firewalls, and cloud services for unified monitoring.

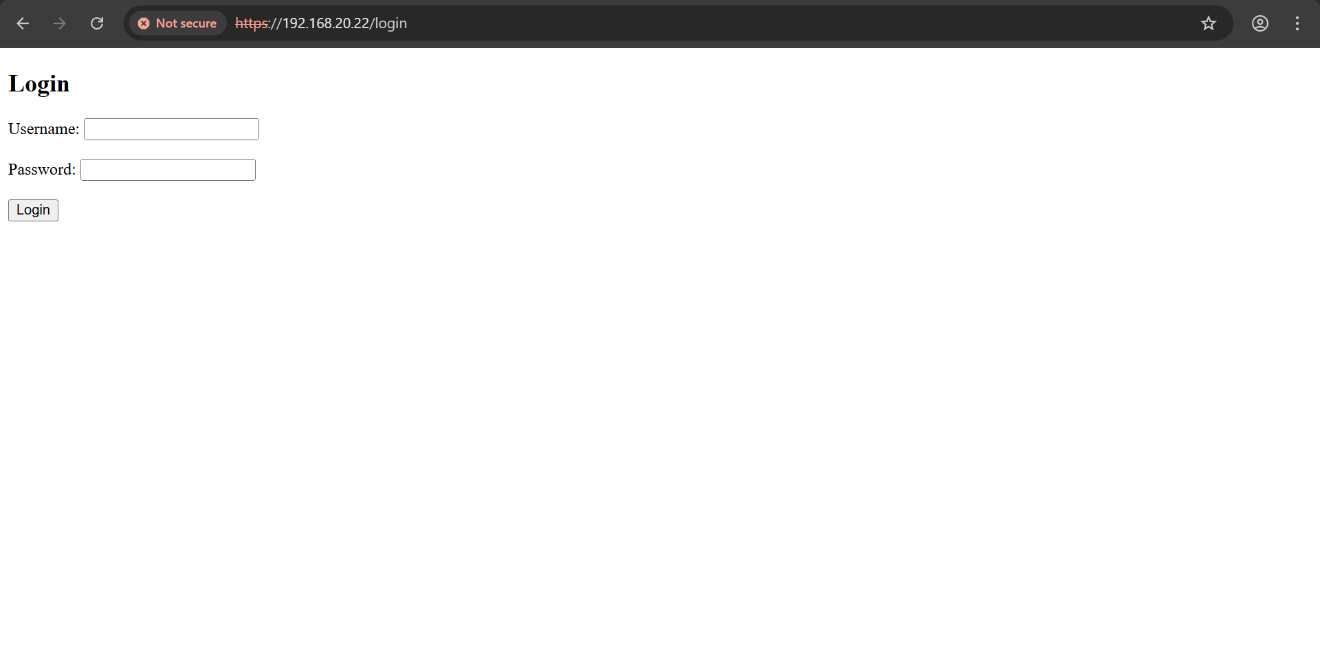
### Alerting: Can be paired with alerting tools like ElastAlert or Kibana Alerting to send notifications when predefined conditions are met.

# 4. Project Output

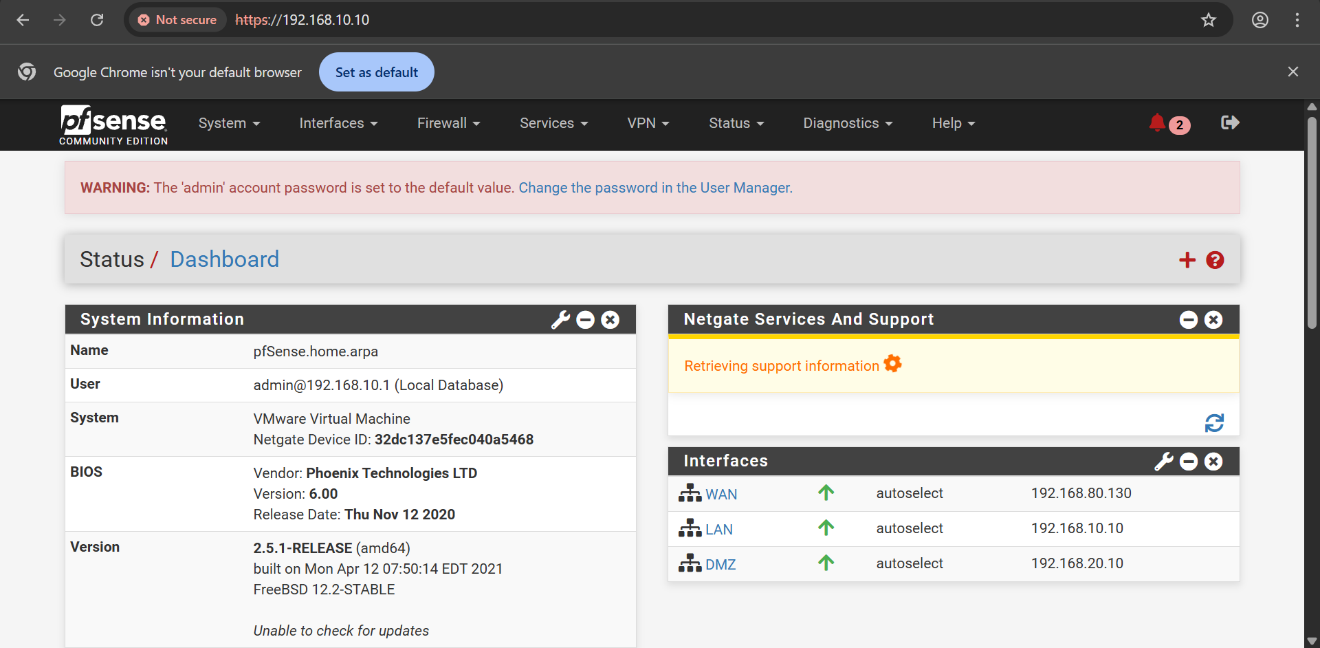
## Kibana Dashboard



## Webhosting using docker swarm



## PfSense



# 5. CONCLUSION

**5.1 Conclusion**  
Hence, we have successfully designed and implemented an Integrated Security and Monitoring System using open-source technologies such as pfSense, Wazuh, ELK Stack, and Docker Swarm. The system ensures a segmented, secure, and continuously monitored IT infrastructure capable of detecting and responding to threats in real time.

**5.2 Future Scope**The current implementation has been designed for small to medium-scale environments, but its modular and scalable architecture allows it to be adapted for larger enterprises. In the future, additional features such as automated incident response, integration with cloud-based security services, and AI-driven threat analysis can be incorporated to further strengthen security..

# REFERENCES

**Paper 1:** – A Qualitative Study of DevOps Usage in Practice  
**Author:** Floris Erich, C. Amrit & M. Daneva

**Paper 2:** – DevOps, A New Approach To Cloud Development & Testing  
**Author:** Dhaya Sindhu Battina

**Paper 3:** – Review Paper on Snort and Reviewing Its Applications in Different Fields  
**Author:** Harpreet Sandhu, Manpreet Kaur