IBM Innovation Center for Education

PHEMESOFT Software That Matters
TRUSTED DELIVERY PARTNER for IBM ICE

YENEPOYA
(Deemed To Be University)

RABBI ZIDNI 'ILMA
YENEPOYA
(DEEMED TO BE UNIVERSITY)

SIEM FOR SMALL BUSINESS

PROJECT SYNOPSIS

IMPLEMENTING SIEM FOR SMALL BUSINESSES

BACHELOR OF COMPUTER APPLICATION
IoT,Ethical Hacking and CyberSecurity

SUBMITTED BY:

Shivani TV - 22BCIECS114
Vismaya CT – 22BCIECS122
Mubeena R - 22BCIECS075
Fathima- 22BCIECS032

GUIDED BY :
Mr.Sashank

TABLE OF CONTENTS

INTRODUCTION

Small businesses face increasing cyber threats without the resources or infrastructure to implement advanced cybersecurity solutions. Security Information and Event Management (SIEM) systems can bridge this gap by offering centralized visibility into system logs, real-time alerts, and compliance support. However, enterprise SIEMs are often costly and complex.

This project focuses on implementing a lightweight, cost-effective, and open-source SIEM system using **Wazuh** and the **ELK Stack (Elasticsearch, Logstash, Kibana)**. The system is tailored to the scale and needs of small businesses, ensuring they gain the capability to detect intrusions, monitor logs, and comply with regulations—without high overhead costs.

Falling under the domain of **Cybersecurity Infrastructure and Threat Monitoring**, this project blends practical deployment strategies with core SOC (Security Operations Center) functionalities, aiming to empower small enterprises with enterprise-grade monitoring tools.

LITERATURE SURVEY

Cybersecurity in small-scale businesses is an often overlooked area despite being one of the most vulnerable sectors to cyber threats. Research indicates that over 60% of small businesses experience cyberattacks annually, yet only a fraction invest in advanced security infrastructure. This gap is primarily due to budget constraints, limited IT personnel, and lack of awareness about cybersecurity best practices.

Several studies and industry reports suggest that Security Information and Event Management (SIEM) systems can significantly improve an organization's ability to detect, analyze, and respond to threats in real-time. However, commercial SIEM platforms such as Splunk, IBM QRadar, and ArcSight are cost-prohibitive and complex, making them unsuitable for small organizations.

As an alternative, open-source solutions like Wazuh, OSSIM (by AlienVault), and Snort have gained attention. Wazuh, an advanced fork of OSSEC, is a free, open-source SIEM tool that integrates seamlessly with the ELK stack (Elasticsearch, Logstash, Kibana). It provides capabilities such as log analysis, intrusion detection, vulnerability detection, and compliance monitoring.

The literature also underscores the importance of log centralization and automated alerting as key benefits of SIEM. Centralizing logs from multiple sources ensures better visibility and quicker detection of anomalies. Automated alerting reduces the need for constant manual monitoring, allowing small teams to act on incidents quickly.

However, many papers also highlight challenges:

- Complex initial setup and maintenance
- Steep learning curve for non-experts
- Potential performance issues on limited hardware
- Need for fine-tuning rules to avoid false positives
-

Despite these challenges, the adoption of open-source SIEM tools has been rising in academic and SME environments due to their cost-effectiveness, customizability, and community support.

This project leverages findings from prior work to implement a simplified, pre-configured SIEM deployment suitable for small business environments. By addressing installation complexity and focusing on essential use cases like intrusion alerts, file integrity monitoring, and basic log analysis, the proposed solution aims to offer a practical and replicable framework for SMEs.

METHODOLOGY / PLANNING OF WORK

Phase 1: Requirement Gathering
Identify the security needs, infrastructure layout, and typical threats faced by small businesses to define scope and key log sources.

Phase 2: Tool Selection
Select open-source tools such as **Wazuh** for SIEM capabilities and the **ELK Stack** (Elasticsearch, Logstash, Kibana) for data visualization and log management.

Phase 3: Environment Setup
Create a virtual test environment using VirtualBox to simulate a small business network with clients and servers.

Phase 4: SIEM Deployment
Install and configure Wazuh Manager and Agents, Filebeat, Elasticsearch, Logstash, and Kibana to enable end-to-end log collection and analysis.

Phase 5: Log Aggregation & Rule Setup
Integrate log sources and define detection rules for events like failed logins, malware activity, and unauthorized access.

Phase 6: Testing & Simulation
Conduct simulated attacks to test detection accuracy and alert generation. Fine-tune rules to minimize false positives.

Phase 7: Evaluation
Assess system performance, alert accuracy, usability, and suitability for non-technical users in a small business setting.

Phase 8: Documentation
Prepare a user-friendly deployment and configuration guide, ensuring ease of adoption and maintenance by small business administrators.

FACILITIES REQUIRED

Software Requirements:

Component	Purpose
Wazuh & Wazuh Agents	SIEM core for event collection and detection
ELK Stack	Log storage, parsing, and dashboard visualization
VirtualBox/VMware	Environment simulation
Ubuntu Server	OS for SIEM infrastructure

Hardware Requirements:

Hardware	Description
Host Machine	PC with minimum 8GB RAM, 100GB disk space
Internet Connection	Required for updates, repositories, and threat feeds

REFERENCE

1. Wazuh Documentation - https://documentation.wazuh.com/
2. Elastic Stack Docs - https://www.elastic.co/guide/
3. OSSIM - AlienVault Open Source SIEM
4. “SIEM Architecture and Applications” – SANS Institute
5. MITRE ATT&CK Framework – https://attack.mitre.org/
6. Snort IDS - https://www.snort.org/
7. NIST Cybersecurity Framework – https://www.nist.gov/cyberframework