National College of Ireland

Evaluating SIEM Solutions for Small and Medium Enterprises: A metric-based Performance Study

MSc Research Project
MSc Cybersecurity

Parth Madhukar Shinde
Student ID: 23266571

School of Computing
National College of Ireland

Supervisor: Kamil Mahajan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Parth Madhukar Shinde
Student ID:	232666571
Programme:	MSc Cybersecurity **Year:** 2024-2025
Module:	MSc Research Project
Supervisor:	Kamil Mahajan
Submission Due Date:	31st August 2025
Project Title:	Evaluating SIEM Solutions for Small and Medium Enterprises: A metric-based Performance Study
Word Count:	5745 **Page Count:** 19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Parth Madhukar Shinde

Date: 24th August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Evaluating SIEM Solutions for Small and Medium Enterprises: A metric-based Performance Study

Parth Madhukar Shinde

X23266571

Abstract

Small and Medium Enterprises face an increase in cyberattacks due to high reliance on digital technology and limited security infrastructure. Security Information and Event Management tools are essential for real-time detection and response, yet the commercial solutions are unaffordable or complex to setup for SMEs. In this study, we will evaluate four solutions namely – Wazuh, ELK, Huntress and LimaCharlie on Windows and Ubuntu in virtual environment through simulated attack scenarios. Key metrics such as Mean Time to Detect (MTTD), Mean Time to Respond and CPU/memory usage were used for evaluation. The results showed that Wazuh had performed consistently across both operating systems along with a balance of usability and detection capabilities. This research provides SMEs with practical insights in choosing the right SIEM solution based on performance and environment adaptability.

1 Introduction

Cybersecurity is becoming a concern for businesses across all sectors especially the SMEs. With the advancements across digital technologies and increase in IT systems for business operations, the organizations face variety of cyberattack due to increase in their attack surface. Most cyber-attackers target the small and medium businesses as they often lack cybersecurity infrastructure to defend against these attacks("35 Alarming Small Business Cybersecurity Statistics for 2025 | StrongDM," 2025).

SIEM systems act as a backbone for many Security Operations Centre by offering functionalities such as centralized log collection, analysis and real-time monitoring. However, the commercial SIEM solutions are complex to integrate and expensive for the SMEs("Security Monitoring," 2024). Although there are various open-source and affordable solutions present in the market, there is a gap in understanding how they might perform once implemented practically. Existing researches focused more on theoretical feature comparison or tool-specific evaluation of which only few were evaluated on limited parameters in a lab environment. This creates an uncertainty in SMEs for choosing a SIEM solution which supports their environment from detection, usability, compliance and cost perspective.

This research helps us to bridge this gap, as we are conducting a comparative study of four affordable SIEM solutions namely Wazuh, ELK, LimaCharlie and Huntress. These tools will be deployed on Windows and Linux environments, and their performance will be assessed based on few key metrics such as Mean Time to Detect and Mean Time to Respond, ease of deployment and dashboard usability. By using attack scenario simulation such as

EICAR malware test or unauthorized login attempts, this study will give practical insights that SMEs can use to make decision while choosing a SIEM solution.

Research Question : To what extent can affordable and accessible SIEM solutions improve detection and response time for SMEs, while supporting usability across different solutions?

2 Related Work

As the complexity of cyber threats increases, there is need for real-time threat response especially in SME environment. A lot of literature review compares SIEM tools on features, detection capabilities and deployments. However, very limited papers have implemented the tools and tested them. In this section we will segregate these studies and highlight their findings while comparing our approach in the research.

2.1 Comparative Studies of SIEM Solutions:

Comparative analysis was performed on different papers of SIEM tools based on different features. **Jawad et al (Manzoor et al., 2024)** in his paper explored the performance and cost-effectiveness of open-source SIEM tools for SME environment, which highlighted the limitations due to budget constraints and recommended tools like Wazuh. Similarly, **Konstantinos et al ("Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)," 2023)**, presented a comparison of open-source SIEM such as OSSEC, OSSIM, ELK, Apache Metron, SIEMonster, etc based on compatibility, requirements, documentation and licensing and concluded stating that OSSIM was more researched from an open-source perspective.

Maria-Mădalină et al ("A Comparative Study of Intrusion Events in Different SIEM Systems," 2025), compared Wazuh, OSSIM and OSSEC by attempting intrusion attacks such as brute-force, hping3, etc and evaluated the capabilities of the SIEM based on these. They concluded stating Wazuh and OSSIM were better, but could not give a thorough and specific solution. **Dario et al ("(PDF) Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management," 2023)**, stated in their research a comparison of IBM QRadar and Wazuh in terms of detection and usability, but they focused on enterprise-level tools.

These studies were insightful, but lacked a unified, live-testing environment across the tools. Our research addresses the gap by installing and evaluating multiple SIEMs under same conditions and capturing detection capabilities, response metrics and usability of tools.

2.2 Tool-Specific Studies:

Wazuh was stated as affordable with rich features present for usage. **Raghda et al (Amami et al., 2024)**, compared the deployment of Wazuh by integrating into security framework for enhancing cyber-defence when evaluating with other solutions due to its reliability, cost-effectiveness, availability and monitoring capabilities. Similarly, **Md Rafiqul**

et al ("(PDF) Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries," 2024), elaborated the deployment of Wazuh in the apparel industry due to its detection capabilities and regulatory compliances, which enhances the reliability.

Răzvan Stoleriu et al (Stoleriu et al., 2021), demonstrated ELK Stack integration with MISP and Virustotal for detecting APT-style attack vectors. This showed how combining threat intel and ML will enhance the anomaly detection through SIEM.

Wararit Hongkamnerd et al (Hongkamnerd et al., 2024), analysed the recovery time for Security Onion. They evaluated the impact of CPU on service start-up time and highlighted that the node's start-up is resource-intensive. This depicted the importance of resource allocation for SIEM performance.

These studies focused on individual tools and specific cases. In contrast, our research compared Wazuh and other tools, which provides a broader view of solutions which helps the SMEs to choose the most suitable solution based on testing and deployment section.

2.3 SIEM Usability and Applicability :

Hassan et al (Mokalled et al., 2019), focused on the applicability of SIEM and the features that the organizations need and how the tools can align with those needs using quantitative and qualitative criteria. Also, **Natalia G. Miloslavskaya ("(PDF) Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers," 2018)**, gave a broader insight into usage of SOC solutions and the architecture of SIEM but lacked in testing and practicality.

Wiame BOUHALI et al (Bouhali et al., 2024), proposed a forensic toolkit to collect the Windows events and forward them to SIEM solution. This shows the integration capabilities of SIEM and speed of investigation to reduce human dependency.

While these researches focus on requirements, our approach is to extend this by validating the usability and deployment complexities through hands-on testing lab across solutions, which makes the evaluation more practical.

2.4 Evolution and Trends in SIEM:

MANFRED VIELBERTH et al (Vielberth et al., 2020), gave a systematic study on SOC and their growing importance and also identified the human, tech and process elements. They focused on the non-technical processes usually ignored which can affect the SOC efficiency.

Shivadutt et al ("(PDF) THE EVOLVING THREAT LANDSCAPE," 2022), in his research discussed how the SIEM solutions evolved from rule based detection to EDR solutions, UEBA and orchestration capabilities which help to tackle the advancing cyber threats, which increased the need for deployment in organizations not as a addition but a requirement. **Aamna et al (Tariq et al., 2022)**, gave a high level overview of SIEM solutions which would help SMEs to consider a solution based on their security requirement.

Similarly **Gustavo et al (González-Granadillo et al., 2021)**, discussed various SIEM solutions but focused on enterprise-level solutions such as Splunk, IBM QRadar, ArcSight, etc based on their features and stated limitation in their usage but through a more theoretical

way rather than practical. Additionally, **Ertugrul et al (Akbas, 2024)**, evaluated Next Generation-SIEM solutions such as ELK, QRadar, Surelog, etc based on their features and focused more from laws and regulations perspective also, which can help SMEs stay compliant with regulations.

These studies were valuable, but did not involve much of tool deployment or performance based measurement. Our research continues this by validating the tools, which is more evident and observable when tested practically.

2.5 Summarization

While the studies reviewed detection capabilities and features of SIEM, few of them gave a methodology for benchmarking the performance. Most of the evaluations lacked some standardization in the environment, which made it difficult to compare the detection efficiency, response time or usability across different solutions. Even though some papers simulated few attack vectors, they focused on some specific tools or incomplete implementations.

This research stands out by deploying and configuring SIEM solutions such as Wazuh, LimaCharlie, Huntress and ELK Stack on Windows and Linux systems. Each of these will be tested using some world scenarios such as EICAR malware file or login failure attempts. By using metrics such as MTTD and MTTR, along with dashboard usability we will compare these solutions for the ease of use. Our approach is more practical in a lab environment which provides the SMEs with insights into SIEM solutions.

3 Research Methodology

In this section we outline the research strategy used for evaluating and comparing the performance, usability and deployment of SIEM solution – Limacharlie, Huntress, Wazuh and ELK Stack for SMEs. With the growing demand for monitoring, especially for the organizations with limited resources, this methodology will be helpful in simulating realistic threat attacks and measure how each solutions performs.

This methodology is built on results and insights gathered from literature review, which highlighted a gap in practical implementation and measuring the effectiveness of the solutions under same conditions. We setup a lab simulation and measured the outcomes on specific metrics.

3.1 Research Approach

This research has a comparative and experimental approach using a lab setup to simulate attacks in a controlled environment. We have used a consistent testing procedure which will be deployed across all SIEM solutions to ensure consistent result such as:

- Requirements of specific SMEs.
- Virtual environment creation.
- Deploying each SIEM with minimum configurations.
- Executing attacks on both Windows and Linux machines.
- Evaluating through quantitative metrics.

3.2 Requirement Analysis and System Setup

a) Identifying the requirements of SMEs.

The SMEs have few specific expectation based on their environments("SIEM for Small and Medium-Sized Enterprises," 2024):

- Affordable and low-cost solution.
- Ease of deployment and minimal training.
- Low hardware and resource consumption so that it doesn't affect their systems and processes.
- Effective detection of common threat vectors.
- Alerting and dashboard mechanism.
- Compliant with regulatory frameworks.

b) Virtual Lab environment

We setup a virtual lab using Oracle VirtualBox 7.1.4("Oracle VirtualBox," 2025) on Windows host machine with:

- Intel Core i7 11th Gen,
- 32GB RAM and
- 1TB SSD

The virtual Lab consisted of:

Machine	OS	Resource	Purpose
VM – 1	Windows	2 vCPU RAM : 6144MB Storage: 82GB	Endpoint for SIEM Agent
VM - 2	Ubuntu	2 vCPU RAM : 4096MB Storage: 50GB	Linux Endpoint SIEM agent

Table 1. Virtual Machine Configurations

All the VMs run under **Host-only adapter and NAT** connection

3.3 Tool Selection and Deployment

The SIEM solution selected are few open-source but all do offer commercial licensing if preferred:

Tool	Type	Reason
Wazuh(Wazuh, 2025)	Open-source	Offers customization, lightweight and supports compliance modules.
ELK Stack("Cyber Investigation & Incident Response," 2025)	Open-source and Commercial	Offers EDR solution, automated dashboarding and enhanced log processing

LimaCharlie ("A Public Cloud for SecOps," 2025)	Commercial	Cloud based platform with complete customization available from scratch.
Huntress ("Managed Cybersecurity Platform," n.d.)	Commercial	Managed detection platform with low resource consumption agent.

Table 2. SIEM solutions

All the solutions were deployed using cloud-trial offered by each. Below actions were performed:

- Installed respective agents on Windows and Ubuntu
- Configuring log collection
- Verifying log collection at platform
- Detecting attack vectors.

3.4 Threat Simulations

To evaluate the accuracy and effectiveness of the detection, following attack scenarios were simulated:

Scenario	Description	Purpose
EICAR test file (emmwalsh, 2025)	Malware files for testing AV effectiveness	Checking accuracy and detection capability of EDR
Brute force	Multiple login attempts	Rule-based detection efficiency

Table 3. Attack vectors to be analyzed

3.5 Evaluation Metrics:

Following performance indicators were used for measuring("Top 8 Incident Response Metrics To Know," 2025) :

Metrics	Purpose
Mean Time to Detect – MTTD	Measures the time taken to detect the attack on the platform
Mean time to Respond - MTTR	Measures time taken to respond / resolve
Resource Consumption	Endpoint resource consumed by the agents affecting the machine.

Table 4. Evaluation Metrics

3.6 Data Collection and Analysis

During each attack simulation:

- Logs are being captured using agents installed on endpoints(evdokimov, 2022).
- The alert generation timestamps were noted to check detection time("Considerations for timestamps in centralized logging platforms," 2020).

- Feedback on UI/UX and ease of customization was noted.
- Ease of Deployment was recorded along with resource consumption of deployed agents.

3.7 Validation Strategy

To ensure consistency:

- Each scenario is executed in same identical environment for each SIEM solution using VM snapshots. ("How do I use snapshots effectively in VirtualBox?," 2018)
- Tools are not fine-tuned and tested under minimal configuration and default settings.
- All tools observe and get the same attack to maintain uniformity.
- For commercials solutions like LimaCharlie and Huntress, their trial version were used to have access to complete features.

3.8 Limitation

- The limitation of using commercial tools trial version restricts some integrations.
- Testing is focused on endpoints, complete network detection is out of scope.
- The results of solutions could be utilized for SME environment and may not be completely suitable to scale for enterprise environment due to change in variety of log sources.

4 Design Specification

4.1 Overview

The SIEM solution Wazuh, ELK, Huntress and LimaCharlie were deployed across two operating systems environments, Windows 10 and Ubuntu 22.04, to reflect more diverse environments in SMEs. The configuration of each tool was standardized to ensure a fair and reproducible output. The key design aspects covered includes the system architecture, environment configuration, deployment, integration components, data collection methods and logging.

4.2 Host Environment Configuration

To ensure the consistency across environments, each SIEM solution was deployed and tested in virtual environment configured with below specification:

a) Windows Test Environment:
   - OS: Windows 11
   - CPU: 2 vCPUs
   - RAM: 4GB
   - Disk: 80GB
   - Security settings: Windows Defender and Firewall disabled to accurate decisions.

b) Ubuntu Test Environment:
   - OS: Ubuntu 22.04 LTS
   - CPU: 2 vCPUs
   - RAM: 4GB
   - Disk: 50GB
   - Security Setting: Audit Daemon enabled for logging; UFW disabled

Both systems were configured to simulate to simulate realistic SME environments. Snapshots of the virtual machines were taken to ensure consistency across SIEM solution so that machines can be reverted to original states.

Test scenario included user login failures, file integrity violation, simulated malware execution (Eicar test file) and system configuration changes

4.3 Architecture Design and Overview

The architecture for this research represents a scalable deployment of SIEM solutions for SME environments. The architecture has been split into Frontend and Backend components to ensure a separation between systems generating and collecting logs along with the infrastructure for ingestion, parsing, storage and analysis.

a) Frontend Components(communications@manageengine.com, 2024)

The frontend architecture represents:

- Log sources:
  - ✓ Windows
  - ✓ Ubuntu

- SIEM agents:

  SIEM agents are installed on log sources to collect and forward systems, user activity and security related logs to the backend. These agents help to provide additional capabilities such as FIM, real-time alerting and policy enforcements, For tools that support agentless collection, logs are forwarded using other mechanism such as syslog.

- Log monitoring, visualization and Alerting

  Once the logs are processed and alerts are generated by the backend, they are then sent back to the frontend monitoring. These dashboards provide real-time alerts, metrics and visualization for security analysts.

- Action Execution:

  In real SOC environments, the actions taken to the alerts are often triggered manually or automatically by agents, For testing, the logging was used to calculate MTTD.

b) Backend Components:

- Log Ingestion Module

These components receive logs forwarded by agents and handle the routing and parsing.

- ✓ Log Forwarder is responsible for receiving the logs data stream
- ✓ API Gateway is used by cloud solutions like Huntress or LimaCharlie securing the Telementry ingestion on HTTPS.

- Cloud Based or Local Storage and Indexing:
  - ✓ The logs are parsed, enriched and stored. These storages support structured queries for searching an correlation, enabling thorough investigation.
  - ✓ The ingested logs are parsed using predefined or custom rules.

c) Log Forwarding

- Event generated: A simulated attack occurs on machine.
- Agent collection: Agents collect the log
- Log Forwarding: The log is sent to the backend ingestion.
- Parsing and Detection: The backend system applies parsing and checks or anomalous signs in logs for alerting.
- Alert Generation: If an anomalous activity is detected, an alert is generated and stored. This alert is forwarded to dashboard for monitoring and response.
- Response: The security personnel or tools respond to the alert according to the playbooks.

d) Architecture Flexibility and Adaptability:

The modularity of the architecture allows easy replacement or evaluation of different SIEM solutions under similar test conditions. The separation of frontend and backend components enables testing of tools such as Huntress, which offer limited functionality but reply on their intelligence.

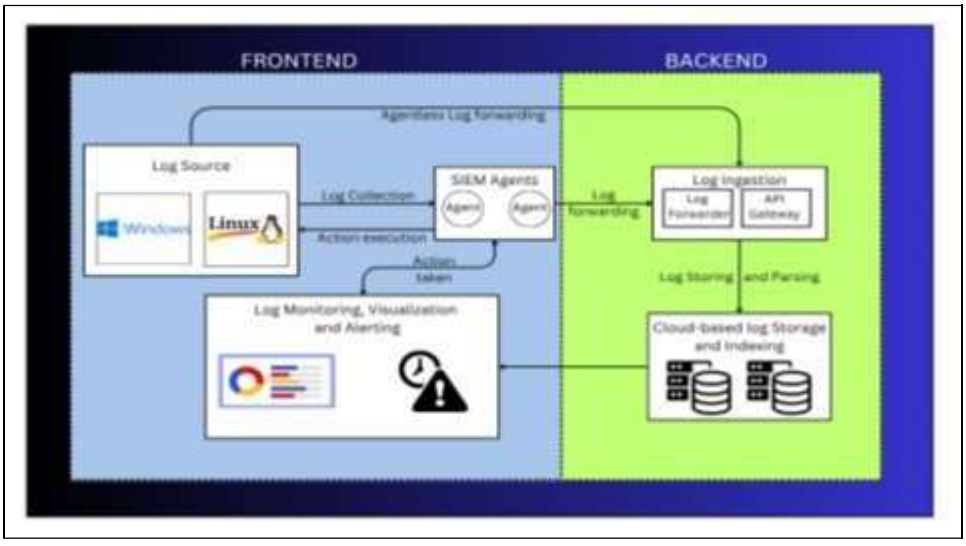

Figure 1. Architecture Diagram

4.4 Tool Specific Deployment

a) Wazuh(Wazuh, 2025)

Wazuh was installed on an offline instance comprising of following components:

- Wazuh Manager: For processing data, correlation rules and generating alerts
- Wazuh Agents: Installed on Windows and Ubuntu clients for collecting logs and perform file integrity checks.
- Wazuh Indexer: Used for storing and indexing security data.
- Wazuh Dashboard: Used for visualizing alerts and system data.

Integration :

- Agents were connected over TCP / UDP port.
- Windows Event logs and Linux syslogs were collected via native modules.

b) ELK Stack("Cyber Investigation & Incident Response," 2025)

The ELK solution was hosted on GCP cloud. The stack is configured with:

- Agent: Installed on Windows and Ubuntu endpoint for forwarding logs.
- Logstash: For log enrichment
- Elasticsearch: For indexing and storing the logs
- Kibana: For dashboarding and visualization

Integration:

- EDR was integrated with standard agent for deep log collection.
- Kibana dashboards were generated for the agents once installed.

c) Huntress("Managed Cybersecurity Platform," 2025)

Huntress is a cloud based MDR solution. Agents were configured only on Windows as it doesn't support Linux.

- Installed Huntress agent on Windows.
- Alerts analysed for failed login and logs found for eicar file.
- Leveraged built-in EDR capability.
- Integrates with local Antivirus solution on endpoints.

d) LimaCharlie: ("A Public Cloud for SecOps," 2025)

LimaCharlie offers detection as code with custom detection logic and integration.

- Agents were deployed on Windows and Linux endpoints.
- Output logs were collected and analysed in UI
- No dashboards were provided for enhanced analysis.

4.5 Attack Simulation

To measure detection and response capabilities, common attack vector scenario was simulated:

- The EICAR file was downloaded and executed in OS environments(emmwalsh, 2025).
- The SIEM were evaluated and based on time taken to log the data from time of download of file on OS was noted.
- This allowed the evaluation of file integrity, log monitoring and real-time malware detection functionalities.

4.6 Evaluation Metrics:

The following evaluation metrics were used to analyse the SIEM solutions: ("SIEM Evaluation Checklist" 2025)

- Mean Time to Detect (MTTD): Time taken between attack initiation and alert
- Mean Time to Respond(MTTR): Time between alert detection and mitigation response.
- CPU/Memory Usage: System overhead caused by agents being installed.
- Agent Size on Disk: Impact on system resources.

The design ensures standardized testing across all tools and provides real-time insights into performance and usability. The selected SIEM tools represent a range of solutions from open-source to cloud based commercial SIEM solutions. By simulating realistic attacks and measuring key performance indicators, the architecture helped to produce meaningful results that SMEs can use to select a suitable SIEM solution for their environments.

5 Implementation

5.1 Environment Setup

The environment setup consisted of 2 virtual machines namely Windows and Ubuntu. Snapshots for both had been taken on a fresh stage to revert after every tool was tested. This helped to maintain consistency when testing for different solutions. Having both Windows and Ubuntu helped to maintain cross-platform diversity when testing tools to imitate an SME environment.

Parameter	Windows System	Ubuntu System
OS Version	Windows 11 Pro	Ubuntu 22.04 LTS
RAM	4 GB	4 GB
CPU	2 vCPU	2 vCPU
Disk	80 GB SSD	60 GB SSD
Network Adapter	NAT-Enabled, Host-enabled Adapter	NAT-Enabled, Host-enabled Adapter

Table 5. Virtual machine configurations

All systems were time-synchronized using NTP for precise logging timestamps of detection and response timestamps.

5.2 Deployment Overview

a) Wazuh
- Windows: Agent was installed that integrated to collect logs and check for FIM.
- Ubuntu: Agent configured for audit logs and kernel-level events.
- Wazuh Manager: Used for analysis and log monitoring being collected on local instance.

b) ELK Stack
- Windows: Fleet agent was installed, which enables remote control of the agent to add modules such as EDR.
- Ubuntu: Fleet agent was used to fetch logs from log directory and function as EDR agent.
- Pipeline: Logs forwarded directly to cloud instance of ELK, parsed and indexed in Elasticsearch.

c) Huntress
- Windows: Agent installed to monitor suspicious behaviour and uses local AV to act as EDR.
- Ubuntu: Not supported.
- Detection: Alerts are visible on the dashboard.

d) LimaCharlie
- Windows and Ubuntu: Agent installed collects logs with a tag to segregate among the systems.
- Detection rules need to be configured manually using YARA or Sigma-like logic set.
- No native dashboard support, but telemetry data being captured in real-time.

5.3 Testing Methodology

a) Step 1: Deployment
- Install and configured the SIEM solutions agents on both Windows and Ubuntu as suited.
- Enabled all modules as required and supported.

b) Step 2: Simulation of attacks
- EICAR test file: Download and execute the eicar file meant to test the effectiveness of AV and EDR solutions without harming the systems.
- Login Attempt Simulation: Simulated brute force login attempts (only tested for huntress due to limitation on other platforms)

c) Step 3: Log and Alert Monitoring
- Time taken from event occurrence to alert observation was recorded as MTTD.

- Time taken from alert generation to observable mitigation action was noted as MTTR.

d) Step 4: Resource Usage
   - Amount of resources consumed such as RAM, memory usage and size on disk to ensure it is suitable for environments and does not hamper existing processes.

To test the real-time detection and response capability, the EICAR test file was used as test case across all tools. It simulated a malware scenario without harming the entire systems. Additionally we used, unauthorized login attempts were simulated only for Huntress, which offers dedicated behavioural detection features for this scenario.
Definitions:

- Actions taken The time when the EICAR file was executed or login attempt triggered.
- Mean Time to Detect (MTTD): Time from file logging to detection on dashboard.
- Mean Time to Respond (MTTR): Time from detection to mitigation of attack.

5.4 Summary

Each SIEM solution was tested in identical environments to ensure consistent evaluation. Despite functioning on same basis, there were significant differences noted in terms of:

- Detection speed
- Response time
- System usage
- Platform compatibility

Testing was conducted on practical metrics and is not opinion-based, which ensures objectivity in measuring detection and response efficiency.

6 Evaluation

6.1 Overview

The purpose is to evaluate the effectiveness and efficiency of each SIEM solution on real-world simulations. The primary concepts of evaluation were(“Optimizing SIEM Performance with Key Security Metrics - SearchInform,” 2025):

a) Detection and Response Metrics:
   - MTTD: Time taken by SIEM solution to detect incident once occurred.
   - MTTR: Time taken to investigate or mitigate the incident as a response action.

b) Resource Utilization:
   - CPU Usage
   - Memory Usage
   - Agent Size on Disk

These metrics helps us to objectively assess each tool's performance, responsiveness and impact on system which become critical factors for SMEs to select a SIEM solution.

6.2 Evaluation

a) MTTD and MTTR Evaluation

Tool	OS	Test Type	Action Time	MTTD Time	MTTD (sec)	MTTR Time	MTTR (sec)
Wazuh	Windows	EICAR	12-07-2025 16:58	16:58:07	4	17:01:00	177
	Ubuntu		12-07-2025 19:27	19:27:39	1	19:29:00	82
ELK	Windows	EICAR	09-07-2025 19:12	19:13:41	46	19:14:50	115
	Ubuntu		09-07-2025 20:10	20:11:43	54	20:12:33	104
Huntress	Windows	EICAR	13-07-2025 12:53	12:56:58	219	12:58:35	337
	Windows	Login Attempt	13-07-2025 13:00	13:06:41	361	13:08:41	481
LimaCharlie	Windows	EICAR	09-07-2025 15:39	15:41:28	122	15:43:05	97
	Ubuntu		09-07-2025 17:42	17:43:05	10	17:44:15	70

Table 6. Metrics Analysed from testing

Key Observation:

- Lowest MTTD: Wazuh on Ubuntu
- Fastest MTTR: Limacharlie on Ubuntu
- Huntress had a significant delay to display logs on the portal though they were received.
- LimaCharlie had a instantaneous detection in Ubuntu but relied on user verification MTTR.

b) Resource Utilization

Tool	OS	CPU Usage	Memory Usage	Agent Size on Disk
Wazuh	Windows	8%	14.2 MB	55.2 MB
	Ubuntu	0.50%	62.7 MB	26 MB
ELK	Windows	6%	450 MB	661 MB
	Ubuntu	0.50%	315 MB	830 MB
Huntress	Windows	10%	24 MB	34.2 MB
	Ubuntu	Not Supported		
LimaCharlie	Windows	3%	1.5 MB	1.8 MB
	Ubuntu	2%	1.2 MB	1.6 MB

Table 7. Resource Utilization metrics

Key Observation:

- LimaCharlie was **most lightweight**, as it requires complete customization and doesn't work as an EDR.
- ELK agent had highest memory and disk usage, as it function like complete EDR agent, but still can be a challenge for smaller infrastructures.
- Wazuh had a good balance between performance and resource usage.

6.3 Discussion and Key Observation

a) Analysis of Findings

- Wazuh consistently demonstrated faster detection time and effective response times. Combined with its lightweight agent and lower resource usage, Wazuh emerged as a balanced, high-performing solution which can be very suitable for the SMEs having limited infrastructure.
- ELK, though had a feature-rich and customizable solution, it had higher resource consumption and few delays in MTTR / MTTR due to it layered architecture. It will be better suited for organization with significant system resources and technical expertise.
- Huntress offered automated response through its MDR, and also integrates itself with local Antivirus solution but had some delayed detection and no Linux support. Still, it remained a good contender for MSPs or small Windows based environments having required minimal setup.
- LimaCharlie, though was extremely lightweight and efficient, it required good amount of familiarity with the infrastructure-as-code and scripting. It showed good performance on Ubuntu but was slower on Windows. However, lack of GUI and dashboarding acted as a barrier for less technical users or smaller teams.

b) Limitations

- Time constraints: Due to time constraints, only limited attack scenarios such as EICAR malware was tested with brute force. Broad attack vectors such as privilege escalation or lateral movement along network was not conducted.
- Resource Limitation: The evaluation was performed on home lab with limited system resources which had affected the scalability or simultaneous testing.
- Platform Limitation: Huntress did not offer Linux support and LimaCharlie required subscription for advanced features for extended telemetry data.
- Manual Response Limitation: For tools which did not support automated response, some manual steps had to be taken for analysing MTTR.
- Licensing Restriction: Some features in tools like LimaCharlie were locked due to trials being used. This affected the evaluation to some extent.

7 Conclusion and Future Work

In this study, our primary objective was to deploy and evaluate four SIEM solutions namely Wazuh, ELK, Huntress and LimaCharlie, to assess their capability in real-world SME environments. The research question focused on identifying which of these tools offered most effective and resource efficient detection and response capabilities across Windows and Linux system, based on metrics such as Mean Time to Detect and Mean Time to Respond.

The lab setup included live simulation of common attacks, mainly the EICAR malware file and unauthorized login attempts, which was followed by data collection on detection time, response duration and resource consumption. The methodology focused on practical,

lab-based implementation under standard conditions to ensure consistency in comparative analysis.

The results indicated that Wazuh demonstrated, the most balanced performance with low resource consumption, faster MTTD and MTTR and compatibility across different operating systems. Though ELK has rich log analytics and visualization capabilities, it comparatively consumes higher resources and higher subscription prices makes it significantly less suitable for smaller enterprises. Huntress had strong detection capabilities but lacked Linux support which are crucial in IT environments, along with delayed response. LimaCharlie was lightest in terms of resource consumption and had quick detection for Linux but has a very steep learning curve with no dashboarding support which makes it difficult for adoption for non-expert teams.

These findings will provide practical insights for SMEs, which struggle to select and effective and cost-efficient SIEM solution. Our approach stood out from prior work as we emphasized on real-time detection and deployment of the tools, rather than theoretical comparisons.

However, we faced certain limitations. The testing environment was restricted to local virtual machines, which could not show the scalability requirement for enterprises. Time constraints limited scope to mainly one attack vector, whereas SIEM can be expected to observe a broader range of attack types. Additionally, limited access to tools due to subscription and use of free trials, affected use advanced features being supported.

For future work, several directions can be considered:

- Extended Attack Vector: Incorporating wider attack vectors using MITRE ATT&CK for testing threat detection capabilities.
- Cloud-based detection: Integrating agents on cloud based environments to test the quality and effectiveness of detection.
- Integration Testing: Combining SIEM with external log sources such as firewall, email and other services to check the compatibility and event collection.
- Automation Enhancements: Exploring the integration of SOAR for automated incident response for reducing manual effort by using Shuffle, TheHive, etc. (“What Is SOAR?,” 2024)
- Long-term monitoring: Running tests to evaluate the stability and log management capabilities of solutions for retention.
- Alert accuracy: Quantifying detection precisions when considering use of wider attack vectors.

To conclude, the research successfully demonstrated that Wazuh offered most effective and balanced SIEM solution for SMEs among the tested tools. Though some limitations exist, the study added substantial value to the existing research. Future enhancements, can help refine the research and expand the analysis to more complex and enterprise-level environments.

8 References

35 Alarming Small Business Cybersecurity Statistics for 2025 | StrongDM [WWW Document], n.d. URL https://www.strongdm.com/blog/small-business-cyber-security- statistics (accessed 8.3.25).

A Comparative Study of Intrusion Events in Different SIEM Systems [WWW Document], n.d. URL https://ieeexplore.ieee.org/abstract/document/10883178?casa_token=gjt1UNBKyI4AAAAA:u-d8O9l6fzFFy2vQJxUKPb7i5Yr6fKgyZYQaDzwscbJANdDq7UcUmSwFRMYXjChnVjllgyzuDtby1E8 (accessed 8.3.25).

A Public Cloud for SecOps [WWW Document], n.d. URL https://limacharlie.io (accessed 8.3.25).

Akbas, E., 2025. Assessing the Frontiers of SIEM Technology: A Rigorous Evaluation and Validation of Innovative Features in SIEM Solutions, in: Proceeding of the 2024 6th International Conference on Information Technology and Computer Communications, ITCC '24. Association for Computing Machinery, New York, NY, USA, pp. 21–29. https://doi.org/10.1145/3704391.3704395

Amami, R., Charfeddine, M., Masmoudi, S., 2024. Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense, in: 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT). Presented at the 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT), pp. 1–7. https://doi.org/10.1109/CoDIT62066.2024.10708476

Bouhali, W., Belmekki, E., Bellafkih, M., 2024. Advanced Techniques for Security Incident Analysis, in: 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM). Presented at the 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 1–6. https://doi.org/10.1109/WINCOM62286.2024.10654882

communications@manageengine.com, M., n.d. ManageEngine Log360 [WWW Document]. ManageEngine Log360. URL https://www.manageengine.com/log-management/ (accessed 8.3.25).

Considerations for timestamps in centralized logging platforms [WWW Document], 2020. . Elastic Blog. URL https://www.elastic.co/blog/considerations-for-timestamps-in-centralized-logging-platforms (accessed 8.3.25).

Cyber Investigation & Incident Response [WWW Document], n.d. . Elastic. URL https://www.elastic.co/security/investigation-response (accessed 8.3.25a).

Cyber Investigation & Incident Response [WWW Document], n.d. . Elastic. URL https://www.elastic.co/security/investigation-response (accessed 8.3.25b).

emmwalsh, n.d. Antivirus detection test for verifying device's onboarding and reporting services - Microsoft Defender for Endpoint [WWW Document]. URL https://learn.microsoft.com/en-us/defender-endpoint/validate-antimalware (accessed 8.3.25).

evdokimov, eugene, 2022. What Is a Log Agent and Why It Matters, Plus Examples. Coralogix. URL https://coralogix.com/blog/benefits-logging-agents/ (accessed 8.3.25).

González-Granadillo, G., González-Zarzosa, S., Diaz, R., 2021. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 21, 4759. https://doi.org/10.3390/s21144759

Hongkamnerd, W., Tangtrongpairoj, W., Watanapongse, P., Sanguanpong, S., 2024. Effects of SIEM Recovery Time: Case Study on Security Onion, in: 2024 21st International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). Presented at the 2024 21st International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp. 1–6. https://doi.org/10.1109/ECTI-CON60892.2024.10594988

How do I use snapshots effectively in VirtualBox? [WWW Document], n.d. URL https://backup.education/showthread.php?tid=3195 (accessed 8.3.25).

Managed Cybersecurity Platform [WWW Document], n.d. . Huntress. URL https://www.huntress.com/ (accessed 8.3.25).

Manzoor, J., Waleed, A., Jamali, A.F., Masood, A., 2024. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. PLOS ONE 19, e0301183. https://doi.org/10.1371/journal.pone.0301183

Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., Zunino, R., 2019. The Applicability of a SIEM Solution: Requirements and Evaluation, in: 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). Presented at the 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 132–137. https://doi.org/10.1109/WETICE.2019.00036

Optimizing SIEM Performance with Key Security Metrics - SearchInform [WWW Document], n.d. URL https://searchinform.com/articles/cybersecurity/measures/siem/management/metrics/ (accessed 8.3.25).

Oracle VirtualBox [WWW Document], n.d. URL https://www.virtualbox.org/ (accessed 8.3.25).

(PDF) Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers, n.d. . ResearchGate. https://doi.org/10.1007/978-3-319-63940-6_40

(PDF) Comparative Analysis of IBM Qradar and Wazuh for Security Information and Event Management, 2025. , in: ResearchGate. https://doi.org/10.2507/34th.daaam.proceedings.014

(PDF) THE EVOLVING THREAT LANDSCAPE: HOW SIEM CAN ADAPT TO EMERGING ATTACK TECHNIQUES, n.d. . ResearchGate.

(PDF) Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries, n.d. . ResearchGate. https://doi.org/10.26776/ijemm.09.04.2020.02

Security Monitoring [WWW Document], n.d. . Splunk. URL https://www.splunk.com/en_us/solutions/security-monitoring.html (accessed 8.3.25).

SIEM Evaluation Checklist 2025: Choose the Best SIEM Tool, n.d. . SentinelOne. URL https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-evaluation-checklist/ (accessed 8.3.25).

SIEM for Small and Medium-Sized Enterprises: What You Need to Know [WWW Document], n.d. URL https://www.linkedin.com/pulse/siem-small-medium-sized- enterprises-what-you-need-know-abhijith-soman-fdwfc (accessed 8.3.25).

Stoleriu, R., Puncioiu, A., Bica, I., 2021. Cyber Attacks Detection Using Open Source ELK Stack, in: 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI). Presented at the 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–6. https://doi.org/10.1109/ECAI52376.2021.9515120

Tariq, A., Manzoor, J., Aziz, M.A., Tariq, Z.U.A., Masood, A., 2022. Open source SIEM solutions for an enterprise. Information and Computer Security 31, 88–107. https://doi.org/10.1108/ICS-09-2021-0146

Top 8 Incident Response Metrics To Know [WWW Document], n.d. . Splunk. URL https://www.splunk.com/en_us/blog/learn/incident-response-metrics.html (accessed 8.3.25).

Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G., 2020. Security Operations Center: A Systematic Study and Open Challenges. IEEE Access 8, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514

View of Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs) [WWW Document], n.d. URL http://ijcs.net/ijcs/index.php/ijcs/article/view/3182/118 (accessed 8.3.25).

Wazuh, n.d. Wazuh - Open Source XDR. Open Source SIEM. [WWW Document]. Wazuh. URL https://wazuh.com/ (accessed 8.3.25a).

Wazuh, n.d. Architecture - Getting started with Wazuh · Wazuh documentation [WWW Document]. URL https://documentation.wazuh.com/current/getting-started/architecture.html (accessed 8.3.25b).

What Is SOAR? Technology and Solutions | Microsoft Security [WWW Document], n.d. URL https://www.microsoft.com/en-ie/security/business/security-101/what-is-soar (accessed 8.3.25).