MINISTRY OF EDUCATION AND TRAINING

FPT UNIVERSITY

Capstone Project Document

Thesis Title: Developing a SIEM/SOAR Systems with AI Integration to Optimize Operational Costs and Workforce for SME.

Group Member	Phan Gia Huy	DE170108
	Phạm Hưng Thịnh	DE170327
	Phạm Phú Đông	DE170597
	Lê Xuân Mỹ	DE170424
	Trần Lương Thảo Chi	DE170554
Supervisor	Phạm Hồ Trọng Nguyên Nguyễn Văn Điền	
Capstone Project code	IAP491	

- DaNang, 12/2025 -

ABSTRACT

Small and medium-sized enterprises face increasing pressure from sophisticated cyber threats while operating under limited budgets and staffing constraints. Traditional SIEM platforms often rely on static rule sets that generate large volumes of false positives and require continuous manual triage, which overwhelms small security teams. Advanced SOAR solutions can alleviate these burdens but remain financially inaccessible for most SMEs. To address this capability gap, this study develops an AI-enhanced SIEM/SOAR framework built on the open-source Wazuh ecosystem, integrating unsupervised anomaly detection and lightweight automated response to improve both detection quality and operational efficiency.

The proposed architecture incorporates Isolation Forest and Local Outlier Factor to analyze heterogeneous log sources and identify irregular behaviors that traditional rule-based systems frequently miss. The framework further extends incident handling with a simplified SOAR layer that executes automated playbooks and supports analysts through an LLM-assisted investigation workflow. Experiments conducted in a controlled SME-scaled environment demonstrate notable reductions in false positives, improvements in recall for subtle attack patterns such as beaconing and DNS tunneling, and substantial decreases in response time through automated actions. These outcomes confirm that meaningful security enhancements can be achieved without enterprise-grade infrastructure or costly commercial licensing.

The research contributes a practical blueprint for deploying AI-driven detection and automation within resource-constrained environments and provides empirical evidence that open-source SIEM/SOAR platforms, when augmented with lightweight machine learning, can deliver capabilities traditionally reserved for larger organizations. The results highlight a feasible path for SMEs to strengthen cyber resilience, reduce operational workload, and modernize security operations through accessible, cost-effective technologies.

Keywords: SIEM, SOAR, Wazuh, Artificial Intelligence, Rule Optimization, Dashboard Visualization, Security Automation, Small and Medium Enterprises (SMEs), TCO.

ACKNOWLEDGEMENT

We would like to express our deepest gratitude to my supervisors, Pham Ho Trong Nguyen and Nguyen Van Dien, for their invaluable guidance, constructive feedback, and continuous support throughout the process of this thesis. Without his/her encouragement and insightful suggestions, this work would not have been possible.

My sincere thanks also go to the lecturers and staff of FPT University Da Nang, who provided me with essential knowledge, resources, and assistance that greatly contributed to the success of my research.

We are truly grateful to our teammates and friends for their cooperation, encouragement, and for sharing ideas and experiences that enriched the quality of this project.

Finally, we would like to dedicate my heartfelt appreciation to our family, who have always supported us unconditionally with love, patience, and motivation during my academic journey.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

Acronym	Meaning
AI	Artificial Intelligence
TCO	Total Cost of Ownership
FPR	False Positive Rate
SME	Small and Medium-sized Enterprises
IT	Information Technology
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
APT	Advanced Persistent Threats
ML	Machine Learning
SOC	Security Operations Center
MTTR	Mean Time to Respond
MTPD	Mean Time to Prevent/Detect
IF	Isolation Forest
LOF	Local Outlier Factor
HIDS	Host-based Intrusion Detection System
NIDS	Network Intrusion Detection System
FIM	Functional Independence Measure

SPAN	Switched Port Analyzer
EPS	Events per Second
API	Application Programming Interface
ELK	Elasticsearch, Logstash, Kibana
KPI	Key Performance Indicator
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
IP	Internet Protocol
IOC	Indicator of Compromise
AUC-PR	Area Under the Precision-Recall Curve
GDP	Gross Domestic Product
IDS	Intrusion Detection System
GDPR	General Data Protection Regulation

CHAPTER 1
INTRODUCTION

1.1 Background

Cybersecurity has moved beyond a purely technical domain to become a critical field of study and an urgent strategic priority, particularly in the context of cyber threats that are increasing in both scale and sophistication on a global level. The strong and pervasive development of Digital Transformation has integrated nearly every aspect of organizational operations and individual life into the digital environment. This, in turn, means that organizations and individuals are continuously facing evolving cyber threats [1].

While large enterprises receive significant media attention, Small and Medium-sized Enterprises (SMEs) are the backbone of the global economy, especially in developing and emerging nations. In Europe, SMEs account for more than 90% of all enterprises and employ around 60% of the workforce. In the European Union (EU), they make up 99% of all enterprises, and as of 2020, they have generated approximately 85% of new jobs, contributing two-thirds of the total private sector workforce [2]. Due to this vital role, SMEs have become prime targets for cyberattacks, as cybercriminals exploit their weaker defenses and more limited financial resources and staffing compared to large enterprises. SMEs often operate with restricted cybersecurity budgets, small specialized teams, and a lack of advanced technologies, making them the most vulnerable link in the digital supply chain [3]. Consequently, protecting businesses in general, and SMEs in particular, has become a hot topic, and has required cybersecurity professionals and organizations to focus intensively on developing effective countermeasures against today's complex threat landscape.

In response to this demand, the cybersecurity field is undergoing a significant transformation with the application of Artificial Intelligence (AI) and Machine Learning (ML). The integration of AI/ML into security systems like Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) offers a promising way to optimize operational costs and workforce needs [3]. Traditional defenses, which rely on signature-based detection and static rules, are becoming less effective against sophisticated attacks such as ransomware and Advanced Persistent Threats (APTs). The industry is now shifting toward AI/ML to enhance detection and incident response capabilities [4].

A major advantage of AI/ML is their ability to learn and adapt proactively. AI systems can perform real-time analysis of logs and network traffic, learning normal behavior patterns to detect anomalies that may signal attacks without needing predefined signatures. They can also identify zero-day threats through anomaly detection and pattern recognition, a capability traditional signature-based systems lack. Furthermore, AI/ML can automate repetitive tasks like log analysis and vulnerability monitoring, which reduces the workload on security professionals and significantly shortens the Mean Time to Respond (MTTR) to incidents [4]. A study showed that AI/ML models could achieve an impressive 99,6% accuracy in detecting dangerous alerts, greatly reducing false positive APT alarms [5]. By minimizing false alerts, security teams can focus their time on real threats instead of being distracted by numerous benign warnings. This is particularly valuable for SMEs, where limited security personnel must be utilized as efficiently as possible [3].

With the rise of AI, Security Information and Event Management (SIEM) systems have become essential in modern security infrastructures, acting as a central hub for collecting, aggregating, and analyzing logs and security events. Through advanced event correlation, SIEM enables real-time detection of anomalies and potential threats, providing the security team with a holistic view of the organization's security posture. Consequently, SIEM serves as a powerful tool for the Security Operations Center (SOC), allowing organizations to recognize ongoing attacks and generate early warnings before serious consequences occur . Additionally, SIEM's ability to store and analyze historical data is crucial for post-incident forensic investigations and compliance [6].

Complementing SIEM, Security Orchestration, Automation and Response (SOAR) systems enhance operational efficiency by automating incident response processes and executing predefined defensive playbooks. This orchestration and automation reduce MTTR and human error, freeing up security personnel from routine tasks [7]. The synergy between SIEM and SOAR allows organizations to not only detect attacks promptly but also respond rapidly, minimizing damage.

Despite their strategic importance, traditional SIEM/SOAR solutions pose significant challenges for SMEs, explaining why they are slower to bolster their cybersecurity defenses. The financial burden is further increased by pricing models based on data volume or the number of devices. Another major challenge is the expertise gap, SMEs typically lack the skilled personnel needed to manage these complex systems, which require expertise to fine-tune alert rules and process large volumes of data daily. This lack of expertise can lead to alert fatigue from excessive false positives, diminishing the value of the SIEM system. Furthermore, the complexity of integrating SIEM/SOAR into existing, often heterogeneous, IT infrastructures is a significant hurdle. These barriers highlight the urgent need for simplified, cost-effective, and easy-to-operate solutions tailored for smaller enterprises [3].

In conclusion, the convergence of SIEM, SOAR, and AI/ML offers an effective and forward-looking approach to cybersecurity. For SMEs, adopting AI-integrated solutions promises greater effectiveness in threat management and helps them enhance security while optimizing resources. Therefore, enhancing SIEM/SOAR systems with AI is considered a feasible and sustainable strategy for SMEs to fortify their cybersecurity defenses [3].

1.2 Problem Statement

Although Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) systems provide strategic benefits for security management, the deployment and operation of these traditional solutions reveal systemic challenges for Small and Medium-sized Enterprises (SMEs), thereby widening the security gap compared to larger enterprises.

The most prominent challenge for SMEs is the financial barrier. The initial investment and annual licensing costs for commercial SIEM/SOAR solutions often exceed the budget capacity of small businesses. Even when SMEs opt for open-source platforms, the Total Cost of Ownership (TCO) remains significant. TCO encompasses costs for integration, customization, data storage, and continuous operations, leading many SMEs to hesitate before committing to such investments. Recent studies on SMEs clearly highlight that insufficient budgets are the number one barrier when these businesses attempt to upgrade their security operations and adopt advanced tools, particularly in the context of escalating cyber threats and increasingly stringent compliance requirements [3].

Another major challenge is the severe expertise gap. Operating SIEM/SOAR systems effectively requires teams capable of fine-tuning hundreds of alert rules, designing complex correlation scenarios, and processing massive event volumes in real time skills that most SMEs do not possess. Multiple studies emphasize that SMEs face heightened risks while their defensive capacity remains limited. For example, the study *Enhancing Cybersecurity Awareness in Small and Medium Enterprises Through a User-Friendly Risk Assessment Tool* revealed that in Ireland, 67% of SMEs admitted they do not test data backups, and 83% stated they would not know how to respond if a cyber incident occurred [8]. These figures reflect a critical gap in SMEs' protection and incident response capabilities. Similarly, another study published in *Computers & Security* affirmed that the lack of internal cybersecurity expertise is a major obstacle, slowing SMEs' adoption of new technologies and forcing them to rely heavily on default configurations or manual processes, this reduces their ability to fully leverage the benefits of complex tools such as SIEM and SOAR [9].

The inherent limitations of current security tools, particularly traditional SIEM, also pose operational difficulties for SMEs. Alert fatigue and false positives remain severe problems. The massive volume of logs generated by SIEM systems, combined with static rules, often results in overwhelming noise. For a small business with only one or two IT staff, analyzing hundreds of alerts daily is nearly operationally infeasible. This increases the likelihood of missing critical alerts and wastes limited resources [5]. Thereby undermining SIEM's operational effectiveness and leaving SMEs highly vulnerable.

Beyond SIEM, even SOAR systems is expected to automate response exhibit notable shortcomings. In practice, many SOAR platforms operate based on drag-and-drop or no-code playbook builders. While this approach simplifies usage, it is rigid, struggles to capture complex logic, and adapts poorly to new attack techniques. When adversaries shift tactics, playbooks must be updated manually, creating strong dependence on skilled personnel. For SMEs with limited security teams, maintaining playbooks becomes a substantial burden. As a result, many small businesses, despite deploying SOAR, still handle incidents manually because playbooks are outdated or ineffective in fast-changing threat environments. This significantly reduces SOAR's practical value and fosters skepticism regarding the return on investment [10].

Consequently, the cyber readiness gap between large enterprises and SMEs continues to widen. Recent studies published on *ScienceDirect* demonstrate that SMEs are heavily affected by budget constraints, lack of expertise, and hidden costs related to deploying and operating security analytics infrastructures [9]. Due to these barriers cost, workforce, and complexity many SMEs either delay adoption or implement at a limited scale, resulting in benefits that fall short of expectations.

At the same time, the global cybersecurity landscape is becoming increasingly complex with the proliferation of sophisticated attack methods. Threats such as ransomware, supply chain attacks, and Advanced Persistent Threats (APTs) are more common and increasingly capable of bypassing traditional signature-based or static rule-based defenses. Classical security tools like firewalls or antivirus software are no longer sufficient against zero-day attacks and advanced evasion techniques [11]. This underscores the urgent need for a new defensive paradigm one that emphasizes anomaly detection and adaptive response rather than relying solely on known attack patterns.

In this urgent context, the research and practitioner community must develop streamlined, cost-effective, and easy-to-operate solutions tailored for SMEs. A feasible approach is to adopt open-source SIEM/SOAR platforms such as Wazuh, which has been positively evaluated for its flexibility, customizability, and log processing performance in SME environments [12]. However, a clear Research Gap remains: most open-source projects to date have not systematically integrated AI/ML, or such capabilities are only minimally available in free or trial versions [10]. AI/ML is a crucial enabler to address SMEs' core challenges, ranging from reducing false positives to event prioritization and creating dynamic playbooks capable of countering sophisticated threats [5]. Therefore, developing a lightweight, cost-efficient SIEM/SOAR framework integrated with AI/ML algorithms and models on widely adopted open-source platforms is the central focus of our study.

1.3 Research Objective

The Research Objectives of this study are developed upon an in-depth academic analysis of the cybersecurity readiness gap that persists among small and medium-sized enterprises (SMEs), along with the inherent limitations of traditional Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) systems [3]. This gap is not merely a technological disparity but rather the compounded result of financial constraints, shortages in skilled personnel, and increasing compliance pressures [13].

The detailed objectives include:

- Technical Objective (AI/ML Integration): To build and evaluate the performance of an Unsupervised Machine Learning model Isolation Forest (IF) [14] and Local Ouliner Factors [15] for near real-time anomalous alert classification [16], with the goal of significantly reducing the False Positive Rate (FPR) compared to the initial static rule system of Wazuh.

- Architectural Objective (Adaptive SOAR Design): To design and implement an Adaptive Response Automation mechanism (Adaptive SOAR) capable of triggering tiered responses based on the Risk Score calculated by the AI model [7].

- Operational Objective (Performance Evaluation): To evaluate the feasibility and effectiveness of the Framework using core security operational metrics, including Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and False Positive Rate (FPR), within an SME simulated environment.

- Economic Objective (Cost Optimization and Feasibility): Demonstrate measurable reductions in TCO (Licensing Cost, Operating Cost) by leveraging open-source components and automation, achieving the dual goals of zero licensing cost and optimized operational expenditure for SMEs.

- Research Validation Objective (Comparative Evaluation and Reproducibility): Validate the proposed framework through quantitative comparison with traditional configurations, ensuring methodological transparency, reproducibility, and applicability in real-world SME contexts.

The outline model is based on the target to be achieved:

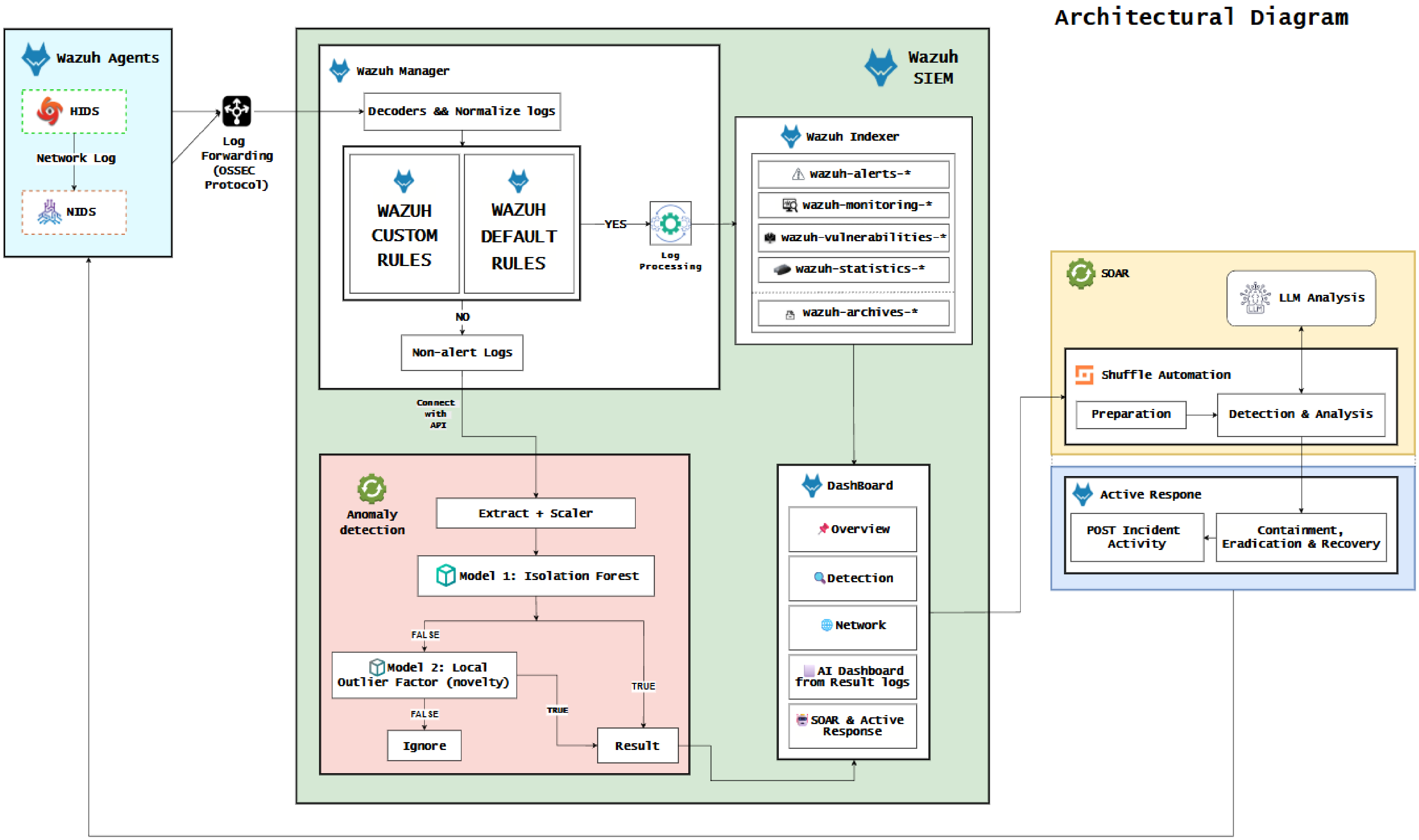


Figure 1.1 The Overall Diagram of Capstone Project

The proposed architecture is designed as a modular framework, leveraging open-source components to ensure both technical efficiency and TCO control [17]. The first component is the Wazuh Agents, deployed across various endpoints including Linux/Windows servers, mail servers, web servers, and database servers. These agents are responsible for collecting operating system logs, application logs, and security events, while also performing File Integrity Monitoring (FIM) [18]. In parallel with this HIDS layer, the architecture integrates Suricata as a virtual machine-based NIDS sensor [3], monitoring traffic in SPAN/mirror mode and recording logs in *eve.json* format. Together, these two sources represent endpoint and network layers, ensuring comprehensive coverage in security event collection.

All logs are forwarded to the Wazuh Manager, where they undergo a structured pipeline: normalization via decoders, matching against predefined rules (signature-based, threshold), correlation with threat intelligence sources for complex pattern detection, classification and prioritization, and alert generation through multiple channels such as dashboards, email, or active response. This central layer unifies data from heterogeneous sources and ensures that all events are processed in a normalized schema.

To prevent bottlenecks and maintain low latency under high-frequency log generation, the architecture employs Filebeat as the intermediary ingestion layer, forwarding all processed logs to the Indexer. In operational settings, Filebeat may be extended with Kafka for horizontal scaling and queue management, thereby ensuring stable Events per Second (EPS) throughput. A distinctive feature of the design is log stream separation: events unmatched by predefined rules are forwarded to the AI/ML module for advanced anomaly analysis, while all logs are still sent to the Indexer for archival and forensic analysis. This parallel approach ensures that no events are discarded while maximizing AI’s utility in handling hard-to-classify logs [14].

The AI module operates as an independent component connected to the SIEM and SOAR framework through lightweight APIs. It performs unsupervised anomaly detection using Isolation Forest (IF) and Local Outlier Factor (LOF) on normalized log data. IF isolates anomalies through random partitioning of features, efficiently detecting global irregularities in high-dimensional event streams. In contrast, LOF evaluates the local density deviation of each point compared to its neighbors, identifying context-specific anomalies in heterogeneous SME logs. Their complementary nature enhances overall detection robustness: IF captures broad deviations while LOF identifies local outliers. The resulting anomaly scores are normalized, combined, and sent back to Wazuh for alert prioritization and automated SOAR response, reducing analyst workload and improving detection of unseen or zero-day threats.

For storage and visualization, the system leverages OpenSearch in place of the original ELK stack. OpenSearch Indexer receives logs from Filebeat and organizes them into multiple index groups: rule-based alerts, unmatched logs, and AI results. The OpenSearch Dashboard (Wazuh Dashboard) provides visual interfaces for analysts, not only displaying alerts along MITRE ATT&CK mappings and operational KPIs such as MTTR/MTPD but also supporting incident response orchestration through SOAR playbooks. Additionally, an independent AI Dashboard (App – Web Views) is integrated to display IF and LOF results separately, enabling comparison between rule-based and AI-based alerts [17]. This separation enhances transparency and explainability, ensuring analysts even non-experts can validate AI outcomes.

At the response layer, SOAR Active Response enables automatic or semi-automatic interventions, such as blocking malicious IPs, isolating compromised endpoints, or activating network-level defenses [19]. Unlike static-rule triggers, these actions are driven by AI-derived risk scores, thereby enabling adaptive, tiered playbooks. For low-risk scores, the system prioritizes enhanced monitoring and logging, for medium-risk cases, the system enriches context by querying external threat intelligence (VirusTotal, WHOIS) before escalating for analyst validation and for high-risk scores, the system enforces strong countermeasures such as endpoint isolation or IOC blocking at the firewall, while opening high-priority incidents with attached forensic evidence. This risk-tiered orchestration overcomes the rigidity of traditional SOAR and prevents the pitfalls of "over-automation" that may disrupt business continuity. Human-in-the-loop safeguards are maintained at intermediate risk thresholds to balance automation speed with operational safety.

The architecture emphasizes measurability and reproducibility. All results are structured into indices to support quantitative evaluation: Detection Rate, False Positive Rate (FPR), AUC-PR for imbalanced datasets, and MTTR for operational responsiveness. These metrics are used to directly compare the performance of "rules-only" versus "rules-plus-AI" configurations. In addition, the study proposes a full TCO model, covering minimum infrastructure costs to sustain target EPS, log lifecycle storage costs, staffing for routine operations and periodic tuning, along with indirect economic gains from reduced false positives and shortened MTTR.

Overall, these objectives form a logical trajectory: from foundational architecture to intelligent analysis, from adaptive automation to quantitative and economic evaluation, culminating in a ready-to-use prototype. The novelty lies not merely in "adding AI to SIEM," but in strategically combining two lightweight ML models IF and Local Outliner Factor into the Wazuh-SOAR pipeline, tailored for SMEs' resource-constrained environments, and embedding this intelligence into adaptive SOAR orchestration. This holistic integration is designed to directly address three structural bottlenecks faced by SMEs: cost, expertise, and operational noise. Should the research hypotheses hold namely, significantly reduced FPR without recall degradation, substantially shorter MTTR, stable EPS within SME resource limits, and demonstrably lower TCO compared to commercial systems then the proposed framework will not only serve as a technical proof-of-concept but also as a sustainable security operations model. Ultimately, this defines the true benchmark for SME-ready cybersecurity: not absolute optimization across all metrics, but the optimal balance between protection, operability, and cost.

Finally, the study explicitly defines its scope and limitations to maintain scientific integrity. The entire system will be implemented and evaluated in a controlled laboratory environment, where attack scenarios and logs are simulated based on public benchmark datasets. Results will then be compared with performance indicators published in prior peer-reviewed studies on both commercial and open-source SIEM/SOAR systems, providing an objective reference baseline.

This comparative approach allows the study to demonstrate feasibility and potential improvements even without direct SME deployment.

Mitigation strategies are also incorporated to balance automation speed with business safety. Specifically, in automated response scenarios, decision points with potential for operational disruption will always operate under semi-automatic approval, requiring human validation. This ensures that the benefits of reduced response time are not achieved at the expense of business continuity. For reproducibility, all configurations, hyperparameters, and quantitative results (including metrics and performance graphs) will be published alongside research artifacts, enabling independent organizations or researchers to verify outcomes within their own environments.

By maintaining equilibrium between technical ambition and methodological discipline, between academic goals and practical applicability, this Research Objectives section underscores the rigor of the study while laying a foundation for a solution genuinely aimed at closing the cybersecurity gap for SMEs a sector where the demand for protection is urgent, yet resources remain perpetually scarce.

1.4 Significance of the Study

This research carries critical, multidimensional significance, aiming to transcend laboratory boundaries and address both operational realities and broader socio-economic policy implications. The core value of the study lies in its ability to bridge the gap between advanced cybersecurity solutions traditionally accessible only to large enterprises and the operational capacities of small and medium-sized enterprises (SMEs), which dominate in number yet remain the most vulnerable segment within the digital ecosystem.

1.4.1 Practical Significance – Enhancing Cybersecurity Capabilities and Optimizing Costs for SMEs

From a practical perspective, the study offers a feasible and financially sustainable solution for SMEs, a sector particularly exposed to cyberattacks due to constraints in both financial and human resources [9].

a. Optimizing Total Cost of Ownership (TCO) and Addressing the Cost Barrier

The foremost practical contribution is the reduction of Total Cost of Ownership (TCO) in a comprehensive manner. By integrating lightweight AI/ML models into open-source SIEM/SOAR platforms such as Wazuh, SMEs can eliminate upfront licensing costs, which constitute the primary barrier preventing many SMEs from upgrading their cybersecurity posture [9]. However, the value of this research extends beyond license reduction. Through a carefully engineered modular architecture and SME-ready deployment documentation, the study also significantly mitigates the hidden costs of integration, maintenance, and operation that frequently cause open-source TCO to escalate. Consequently, the research demonstrates that advanced cybersecurity can become economically sustainable for small enterprises.

b. Improving Operational Efficiency and Reducing Workforce Burden

The proposed system directly addresses the persistent issues of alert fatigue and the high False Positive Rate (FPR). Given the overwhelming volume of logs and alerts, SMEs' limited IT staff often expend substantial time on false positives instead of focusing on real threats. By reducing false positives through AI-driven anomaly detection, the system alleviates the burden on security teams, enabling faster and more effective responses [5]. Furthermore, by lowering Mean Time to Respond (MTTR) through SOAR-driven automation the solution reduces financial and reputational damages in the aftermath of incidents [7].

c. Balancing Automation with Business Safety

The introduction of a risk-tiered response model ensures that SMEs are not compelled to respond to every alert at the highest severity level. Instead, responses are calibrated based on contextual severity and reliability, thus overcoming the rigidity of many current SOAR implementations [10]. This approach balances automation with operational continuity, preventing unnecessary business disruptions (e.g., isolating a critical server prematurely) while ensuring timely protection. As a result, the model reinforces business leaders' trust in automated solutions.

1.4.2. Technological Significance and Solution Innovation

The research micro-engineers the integration of advanced technologies, showcasing the transformative potential of AI/ML in reimagining traditional security tools.

a. Innovation in AI/ML Application for Resource-Constrained Environments

The study introduces a noteworthy innovation: embedding lightweight AI models Isolation Forest (IF) and Local Outliner Factor directly into the SIEM/SOAR pipeline. A major barrier in applying AI to cybersecurity is the high computational demand of most ML algorithms [11]. Unlike traditional machine learning algorithms that require high computational resources, IF and LOF operate with near-linear complexity and perform effectively on imbalanced, unlabeled security data. IF detects global anomalies across multiple correlated features, while LOF identifies local deviations based on neighborhood density. Their complementary behavior enables a detection system that is both accurate and resource-efficient, aligning with the goal of optimizing cost and workforce for SMEs.

b. Developing Adaptive SOAR Playbooks Driven by Risk and Context

The study further innovates by designing adaptive SOAR playbooks guided by AI-generated risk scores. This allows the response path to dynamically adjust to varying levels of severity and reliability, thereby overcoming the inflexibility of static SOAR playbooks [10]. Recent research, although not SME-focused, supports the potential of context-aware, data-driven playbooks to enhance SOAR efficiency and adaptability [7]. In addition, by adopting a modular and open-source architecture, this framework remains extensible, allowing the substitution or augmentation of AI modules, thereby ensuring long-term adaptability to an evolving threat landscape.

1.4.3. Academic Significance and Contribution to the Research Community

a. Closing the Research Gap on AI Integration for SMEs

Academically, this study addresses a critical research gap: sự thiếu vắng các công trình tích hợp AI/ML trong SIEM/SOAR dành cho SMEs [11]. the scarcity of works that integrate AI/ML into SIEM/SOAR frameworks designed specifically for SMEs. Existing research on AI-driven SIEM/SOAR largely focuses on large enterprises or controlled environments, neglecting the practical constraints of SMEs in terms of cost, workforce, and infrastructure [3]. By leveraging lightweight machine learning and open-source platforms, this work contributes to a new theoretical foundation for "AI-driven security at scale in resource-constrained environments" [5].

b. Providing Empirical Data and Reference Models

The experimental outcomes of this study will offer quantitative benchmarks (e.g., FPR, MTTR, EPS, TCO) that enrich the research community with practical and measurable evidence. This not only supports the development of new theoretical models but also enables refinements of existing approaches based on empirical validation of economic and technical feasibility. Furthermore, the proposed architecture (Wazuh with IF and LOF Adaptive SOAR) can serve as a reference model for future research and deployment, particularly in sectors such as education, healthcare, and non-profits, where resources are equally constrained. By publishing detailed configurations, parameters, and datasets, this study promotes reproducibility and benchmarking across diverse environments.

1.4.4. Societal and Macro-Economic Significance

a. Strengthening the Economic Backbone and Reducing Systemic Risk

SMEs represent the backbone of national economies, contributing significantly to GDP and employment [2]. Enhancing SME cybersecurity not only protects sensitive data and preserves corporate reputation but also ensures long-term business sustainability. On a systemic level, bolstering SME defenses mitigates risks across supply chains, as cybercriminals frequently exploit smaller vendors as stepping stones to larger targets ("exploiting the weakest link"). Protecting SMEs therefore helps safeguard broader national digital value chains.

b. Supporting National Policy Development

At the national and regional levels, the proposed model can inform policy frameworks aimed at incentivizing SME cybersecurity adoption. Governments and regulators may leverage such cost-effective approaches as instruments for bolstering small enterprise participation in national cybersecurity strategies, promoting compliance without imposing excessive financial strain. Ultimately, the societal impact of this research lies in advancing digital resilience and sustainable development: by securing SMEs, fostering innovation, and curbing cybercrime risks, the study aligns with the broader vision of digital transformation pursued by many nations.

1.5 Scope and Limitations

This section clearly defines the boundaries of the study, ensuring academic focus and transparency regarding the results obtained. Establishing a well-delimited scope is necessary to concentrate resources on the core objective: delivering a cost-effective and operationally simple cybersecurity solution for small and medium-sized enterprises (SMEs), while acknowledging the technical and practical limitations inherent to an academic project.

1.5.1. Research Scope

This research focuses on the design, implementation, and evaluation of an AI-integrated SIEM/SOAR framework built on the open-source Wazuh platform. The scope is strategically defined to optimize for SMEs, which are typically constrained by financial resources, staffing, and technical capacity [9].

a. Depth of Technology Integration and Event Coverage

The technological scope is broadened to ensure event coverage at both endpoint and network layers – an essential requirement for a comprehensive security system.

Collection and Monitoring Layer. Wazuh Agents (HIDS) are employed to collect operating system logs (Windows/Linux), application logs, and security events on servers and endpoints. In parallel, Suricata (NIDS/IDS) is used to monitor and analyze network traffic, adding protocol-level threat detection capabilities [3]. The HIDS–NIDS combination enables detection of anomalous insider activities as well as externally originating attack patterns.

Analysis Layer. This is the core innovation. Collected logs are delivered to the Wazuh Manager and then processed along two parallel paths: a traditional rule-based path (Wazuh Decoders and Rules) and an AI path for anomaly analysis [17]. This bifurcation preserves detection of known attack patterns (rule-based) while adding the ability to surface novel and complex threats (AI-based).

Lightweight AI Module. The AI scope is intentionally limited to two unsupervised algorithms Isolation Forest (IF) and Local Outliner Factor (LOF). This choice is guided by computational efficiency and robustness on anomalous, heterogeneous log data characteristic of SME environments [14]. The AI module performs anomaly detection and assigns risk scores to events, which serve as core inputs for the response layer.

b. Response and Evaluation Layer

The scope includes translating analytics into actions and quantifying operational effectiveness:

Visualization and Automated Response. OpenSearch Dashboard is used to visualize logs against the MITRE ATT&CK framework, display AI-derived risk scores, and manage key operational metrics such as FPR and MTTR [17]. In parallel, SOAR Active Response (via Wazuh's active response or a lightweight open-source SOAR integration) is triggered through adaptive playbooks. Response actions are bound to core measures: endpoint isolation, malicious IP blocking, and elevated monitoring [7].

Experimental Evaluation. The evaluation scope is quantitative testing within a controlled laboratory environment. Test data are generated from public benchmark datasets and simulated attack scenarios to ensure reproducibility and comparability. Quantitative metrics include False Positive Rate (FPR), Recall, Mean Time to Respond (MTTR), and a quantitative Total Cost of Ownership (TCO) model to demonstrate economic feasibility [3].

Intended Application. The scope targets SMEs with high security needs but limited budgets, exemplified by retail, education, healthcare, and IT services where protection of personally identifiable information (PII) and privacy is paramount [20].

1.5.2. Research Limitations

a. Limitations of the Test Environment and Generalizability

The principal limitation is the laboratory-based test environment. The system is deployed in a tightly controlled setting with fixed resources and simulated data. Consequently, the reported outcomes (FPR, MTTR, TCO) reflect technical and operational feasibility under idealized conditions and may not fully capture the variability, heterogeneity, and complexity of real-world enterprise infrastructures [9]. Unanticipated user behavior, sporadic network misconfigurations, and traffic spikes common in SME environments may adversely affect FPR and MTTR. Therefore, the generalizability of the results requires validation through future field studies.

b. Constraints in AI Technology and Data Sources

The study acknowledges constraints in algorithmic choice. Only two unsupervised algorithms (IF and LOF) are used due to their lightweight nature, resource efficiency, and suitability for unlabeled data [14], [15]. More advanced methods (e.g., deep learning or supervised models) may achieve higher classification performance and lower FPR but are excluded given strict computational limits and the overarching goal of cost efficiency for SMEs. Incorporating deep models could significantly increase TCO, running counter to the study's primary objective. Similarly, logs and attack scenarios are derived from public benchmarks and simulations, which may not fully reflect the diversity, heterogeneity, and noise of production SME data, potentially reducing performance upon real-world deployment.

c. Limitations in Automation and Scalability

Although the study aims to minimize manual intervention, it explicitly recognizes human dependency. Certain critical response actions (e.g., isolating production systems, shutting down core business services) require human approval to preserve business safety and avoid unnecessary disruption [3]. Full end-to-end automation is therefore not achieved. Regarding scalability, the prototype targets SME-scale deployments (with EPS below specific thresholds). Applying the architecture at larger scales (e.g., enterprise groups, complex multi-cloud settings) may require substantial redesign (e.g., larger OpenSearch clusters, re-architected data pipelines), beyond the time and resource constraints of this study.

d. Limitations in Compliance Depth and Legal Considerations

This work is an engineering-oriented study and does not delve into detailed regulatory compliance (e.g., GDPR, HIPAA, ISO 27001). While the solution can support log auditing and incident response requirements, attaining full compliance certification is a multifaceted process involving organizational and legal procedures that fall outside the core scope of this research.

In summary, the study emphasizes developing a simple, cost-efficient, and operable AI-integrated SIEM/SOAR framework for SMEs, with the objective of demonstrating technical and economic feasibility under controlled conditions. The current results are limited to laboratory proof-of-feasibility. Future work should extend to real-world SME environments, incorporate more diverse datasets, experiment with advanced AI models, and conduct comprehensive assessments of compliance implications and scalability.

1.6 Project Management Plan

This Project Management Plan (PMP) is essential for establishing the foundational structure, guiding principles, and control mechanisms required for the successful execution of the research project, “Developing a SIEM/SOAR Systems with AI Integration to Optimize Operational Costs and Workforce for SME”. Given the project’s complex nature, integrating advanced AI with an open-source security platform, a meticulous approach is necessary. This plan is designed to coordinate all activities, ensuring that the research progresses smoothly, adheres strictly to the projected timeline, remains within the defined resource and time budget, and, critically, achieves all stated technical and operational objectives. The project execution is systematically organized into four major phases, providing a clear roadmap from conceptualization to final evaluation.

1.6.1 Project Management Objectives and Scope

The overarching objective of this PMP is to guarantee the timely delivery of the proposed AI-enhanced security solution, transforming the research framework into a validated.

a. Scope Definition

The primary and non-negotiable deliverable is a fully functional AI-Enhanced SIEM/SOAR Framework. This framework is specifically built upon the open-source Wazuh platform and is tailored to the resource constraints of Small and Medium-sized Enterprises (SMEs). The technical scope emphasizes two critical outcomes: the systematic False Positive Rate (FPR) reduction through AI-driven anomaly detection, and the development of reliable automated threat response (SOAR) playbooks. The scope excludes full-scale production deployment but includes deployment in a robust simulated environment.

b. Time Management

Successful time management dictates that all four research phases, as meticulously detailed in the Work Breakdown Structure (WBS), must be completed accurately according to the projected timelines. This involves rigorous monitoring of milestones, proactive identification of dependencies between the development and testing tasks, and swift mitigation of any delays to prevent scope creep or schedule slippage.

c. Resource Optimization

This objective focuses on the efficient allocation and utilization of all project assets, including personnel, computational power for the AI training, and specialized technical tools. The goal is to minimize the resource burden, particularly on the technical team, by implementing clear task partitioning and delegation, thereby reducing time spent on repetitive data preparation and system maintenance tasks.

d. Quality Assurance

Ensuring quality is crucial to validating the feasibility of the proposed system. This requires the prototype to achieve high performance and reliability within the simulated experimental environment. Key quality metrics include the effectiveness of the AI model in detecting anomalies, as well as the execution accuracy and stability of SOAR playbooks triggered after alert quality enhancement. The system must meet predefined technical thresholds aimed at improving False Positive Rate (FPR) and Mean Time to Respond (MTTR) compared to the baseline configuration.

1.6.2 Work Breakdown Structure (WBS) in Detail

The project is logically divided into Four Major Phases, each serving as a critical milestone that must be successfully completed before proceeding to the next.

a. Phase 1: Research & Platform Setup

Objective: Understand Wazuh architecture and establish a stable baseline SIEM environment.

Key Tasks:
- Research SIEM fundamentals and Wazuh components (Manager, Indexer, Dashboard).
- Install and configure Wazuh Server (Manager, Indexer, Dashboard) for basic log ingestion.
- Customize dashboards and create initial log filtering rules to reduce noise.
- Write Chapter 1 (Introduction) and Chapter 2 (Literature Review).

Deliverables: Installed Wazuh SIEM environment, customized dashboards, and literature review report.

b. Phase 2: Data Acquisition & Testing Environment

Objective: Build a simulated SME network and collect labeled log data for AI training.

Key Tasks:
- Deploy Wazuh Agents on simulated SME hosts (Suricata, Windows, Linux, Web/DB).
- Generate attack scenarios (Brute Force, SQL Injection, SSH Failures, Malware).
- Verify and label logs as *Normal* or *Anomaly*.
- Write Chapter 3 (Methodology) detailing architecture and data collection.

Deliverables: Functional testbed environment and labeled dataset for AI model training.

c. Phase 3: AI/ML Integration & SOAR Automation

Objective: Integrate AI/ML models to reduce FPR and enable adaptive SOAR automation.

Key Tasks:
- Research and select lightweight anomaly detection models (Isolation Forest, Local Outliner Factor).
- Preprocess, normalize, and train AI models to classify alerts.
- Integrate AI into Wazuh alert flow and connect with SOAR tool (Shuffle).
- Write Chapter 4 (Experimental and Results) describing AI workflow and playbook logic.

Deliverables: Trained AI model, integrated SIEM/SOAR system, and automated SOAR playbooks.

d. Phase 4: Testing, Validation & Documentation

Objective: Evaluate system performance and finalize project documentation.

Key Tasks:
- Conduct stress tests and simulate attacks to assess system stability and scalability.
- Validate AI and SOAR performance using FPR, FNR, Accuracy, and MTTR metrics.
- Containerize the system with Docker for deployment readiness.
- Finalize thesis report, test case documentation, installation guide, and demo video.

Deliverables: Dockerized AI-enhanced SIEM/SOAR system, final thesis report, test case report, and demo video.

1.6.3 Risk Management

The project faces several potential risks that require proactive mitigation strategies:

Risk	**Severity**	**Mitigation Plan**
Complex AI Integration	High	Select low computational complexity AI algorithms (IF and LOF). Focus on using standard Python libraries for simplified integration rather than developing custom algorithms.
High Alert Fatigue Persistence	High	Post-Phase 3, implement an iterative Fine-tuning Loop for the AI model and Wazuh correlation rules to systematically eliminate persistent false or noisy alerts.
Lack of Realistic Attack Data	Medium	Intensify simulated attack scenarios in Phase 2, utilizing traffic generators and known attack samples to ensure a diverse and representative dataset for AI training.

Scope Creep	Low	Strictly adhere to the technical objectives defined in the scope, avoiding the expansion into related technologies not directly relevant to the core SIEM/SOAR and AI integration.

Table 1.1 Project Risk Management Matrix

1.6.4 Communication and Reporting Management

a. Reporting Frequency

Weekly check-in meetings are mandatory to review progress, address technical challenges, and adjust task assignments as needed.

b. Tools

Utilization of project management tools (drive or the provided WBS spreadsheet) to maintain transparency regarding task status, ownership, and deadlines.

c. Escalation (ES) Protocol

Any technical issue that cannot be resolved internally by the group within 24 hours must be formally escalated to the Supervisor for guidance and direction.

1.7 Thesis Structure

Chapter 1 – Introduction

The introductory chapter establishes the foundation of the thesis, setting the research context and rationale. It begins with the Background, analyzing the increasing complexity and frequency of cyber threats, with a particular emphasis on the vulnerability of Small and Medium-sized Enterprises (SMEs) due to financial constraints and the shortage of specialized human resources. It then presents the Problem Statement, clearly identifying the existing gap in both academic literature and commercial solutions: the absence of an AI-integrated SIEM/SOAR model built on open-source platforms that is both cost-effective and easy to operate for SMEs. Based on this, the Research Objectives are articulated in detail and quantitatively defined, covering goals related to system architecture design, AI model development (IF and LOF), adaptive automated response, and economic evaluation (TCO). Finally, the chapter highlights the Significance of the study for both the academic community and industry, defines the Scope and Limitations, and provides an Overview of the Thesis Structure.

Chapter 2 – Literature Review

The literature review chapter builds the theoretical foundation and contextualizes the research within the current academic landscape. It systematically evaluates prior work in three major areas. First, it examines the Theoretical Foundations of SIEM and SOAR, analyzing their evolution, identifying the core limitations of traditional SIEM solutions (e.g., alert fatigue and high false positive rates), and assessing the potential of SOAR automation. Second, it explores Open-source Platforms, with a focus on Wazuh (SIEM/HIDS), assessing its existing capabilities, community support, and prior studies that leveraged Wazuh as an extensible foundation. Third and most critically, it reviews AI/ML Integration in Cybersecurity, analyzing existing methods applied to intrusion and anomaly detection, with particular attention to unsupervised models such as Isolation Forest and Local Outliner Factor. It further explains why these models are better suited to SME-specific data characteristics compared to resource-intensive deep learning approaches. The chapter concludes by reaffirming the Research Gap, thereby demonstrating the novelty and necessity of this study in delivering a cost-effective AI-integrated solution for SMEs.

Chapter 3 – Methodology

This chapter details the research methodology, ensuring transparency, reproducibility, and reliability of the experimental results. It begins with the Research Design, describing the chosen approach (e.g., applied experimental research) and the execution process. It then elaborates on the Proposed System Architecture, outlining the modular structure, API interfaces between the Wazuh Manager and the AI/ML module, and the schema definition for log normalization and real-time processing. Next, it specifies the Data Sources and Experimental Scenarios, including publicly available benchmark datasets and simulated attack scenarios based on the MITRE ATT&CK framework to test detection capabilities. The chapter then describes the AI Model Development Process, from preprocessing and feature selection to training and hyperparameter tuning for Isolation Forest and Local Outliner Factor. Finally, it defines the Evaluation Framework, listing quantitative performance metrics such as FPR, Recall, MTTR, and TCO, and explains how data will be collected and analyzed to address Research Objective 4.

Chapter 4 – Experimental and Results

This chapter provides the empirical evidence of the study, detailing the process of transforming the proposed architecture into a working prototype and presenting the quantitative evaluation results. It begins with the Prototype Implementation, including the configuration of open-source components (Wazuh, Suricata, OpenSearch) and the development of the AI/ML module (using Python/Scikit-learn) along with their integration mechanisms. It then describes the Controlled Lab Environment Setup, simulating an SME network and generating both normal and malicious traffic. The core of this chapter lies in the Experimental Results, including tables and visualizations showing the performance of the AI models analyzing FPR and Recall of IF and LOF against Wazuh's traditional rule-based detection. It also reports quantitative results on Operational Performance, including MTTR before and after deploying adaptive SOAR, as well as EPS stability under varying loads. The chapter concludes with a TCO Analysis, demonstrating the economic benefits of the open-source AI-integrated solution compared to commercial alternatives.

Chapter 5 – Discussion

The discussion chapter provides a deeper analysis of the experimental results within the broader academic and practical context. It begins with the Interpretation of Findings, examining the significance of the results (e.g., why FPR dropped significantly, or why IF outperformed LOF in certain scenarios). It then conducts a Comparison with Prior Studies, contrasting the detection performance of the proposed system with related AI-SIEM research, highlighting its advantages in cost-effectiveness and computational efficiency. The chapter also evaluates the Strengths and Weaknesses of the Proposed Architecture, acknowledging the limitations identified in Chapter 1, particularly regarding the generalizability of lab-based results to real-world SME environments. Finally, it discusses the Practical Implications for SMEs, analyzing how the results can be translated into tangible business benefits, and proposes an Improved Security Operations Model tailored to small enterprises.

Chapter 6 – Conclusion and Future Work

The final chapter synthesizes the entire research process and outlines future directions. It begins with a Summary of Key Contributions, reaffirming that the thesis has achieved its stated research objectives, particularly by demonstrating the feasibility of a cost-effective AI-integrated SIEM/SOAR solution for SMEs. It then revisits the Research Limitations, drawing on insights from the experimental findings in Chapter 4. Most importantly, it presents the Future Work, suggesting potential areas for extension, including testing in real-world SME environments, experimenting with more advanced AI techniques (e.g., lightweight deep learning, federated learning), incorporating compliance standards, and developing simplified user interfaces for non-expert operators. The chapter closes by emphasizing the long-term significance of this research in advancing sustainable cybersecurity for SMEs, positioning the proposed framework as both academically rigorous and practically impactful.

CHAPTER 2
LITERATURE REVIEW

2.1 Review of Previous Studies

2.1.1 Analysis of Commercial SIEM Solutions

Commercial SIEM solutions such as Microsoft Sentinel, Splunk, QRadar, Google Security Operations, AlienVault USM and Graylog Security are well known for their superior performance and scalability, but they come with extremely high costs, making them unsuitable for SMEs.

Total Cost of Ownership (TCO): The overall cost of commercial tools is significantly high, including expensive licensing fees, hardware costs, and specialized personnel expenses. For example, the three-year TCO for solutions such as LogRhythm or SolarWinds LEM has been reported at around $50.000, whereas enterprise-grade systems like AlienVault USM, IBM QRadar, and HP ArcSight can start from $250.000, Splunk is typically among the highest in terms of license costs [3]. Licensing and ongoing maintenance fees create a financial barrier that is insurmountable for organizations with limited budgets.

Human Resource Requirements: Commercial systems demand substantial specialized manpower, including security experts, system engineers, and SOC analysts, along with significant training costs. Dependence on highly skilled personnel and additional operational overhead represent key limitations, particularly when SMEs face a shortage of cybersecurity professionals.

Limitations for SMEs: While these tools provide strong performance and advanced functionalities (e.g., extensive reporting, robust vendor support), their excessive costs and customization complexity make them entirely unsuitable for SMEs.

2.1.2 Summary Table of Commecial SIEM/Security Solutions

Table 2.1 Summary Comparison of Commecial SIEM/Security Solutions

Platform	Pricing model	AI	Overview
Microsoft Sentinel	Pay-as-you-go & Commitment Tier by $/GB (Microsoft Sentinel packages overview article says: ~$5,22/GB PAYG, ~$342,52/day for 100GB/d tier) [21].	Cloud-native SIEM (2019) + Security Copilot (GenAI) for investigation/summary support [21].	Strong in AI/automation & M365 ecosystem, cost depends on ingest, optimized by commitment & data filtering.
Splunk (Enterprise Security + SOAR)	Not publicly available. Workload Pricing (pay per computer/storage instead of GB/day). 2/2025 guidelines give estimates per plan/use case. See how to purchase and use Splunk plans [22].	Very "mature" ~2003, AI Assistant for Security announced/preview 2024–2025 11/6/2024, preview security assistant: Aug 2024 [23].	Analytical power & app ecosystem but "opaque" cost, easy to increase if volume/compute is not controlled.
Rapid7 InsightIDR + InsightConnect (SOAR)	InsightIDR: official site is currently offering pricing from $5,89/asset/month (Dection and Response) [24].	The platform has been developed since 2010, has automation and ML/UEBA and many other notable features [25]. The InsightConnect product is SOAR.	Accessible for SMEs per "per-asset", but total cost depends on asset min & add-ons.

Google Security Operations (Chronicle + SOAR)	“Package + ingestion-based”, no public pricing, just “Contact sales for pricing” [26], there is a service “Chronicle SecOps” in the UK service catalog priced at £2.000 a terabyte a year [27].	Chronicle (Google Cloud's new generation SIEM) was born later (2018+) but AI Gemini for SecOps is deeply integrated (Google brings the new generation AI model embedded into SecOps, helping to analyze, detect, and respond to incidents more intelligently) [28].	Strong in scale & AI, for small SMEs it can be a bit too much if ingestion is large, cost is usually contract based [26].
Securonix	Move to GB/Day & tier from 4/2025 [29] (simplify/reduce complexity), specific prices as per quote	UEBA long-standing (2008+) [30]. There are many mentions of Securonix pricing by GB/Day to simplify & reduce complexity, but no specific source has mentioned “SIEM cost optimization” as a long-term strategy with specific values.	Reasonable if prioritizing UEBA & ingestion/retention reduction strategy, still need POC to lock in costs.
Graylog Security (SIEM)	Starting ~$18.000/year (Graylog Security), Enterprise ~$15.000/year [31]	Released after Splunk/QRadar, special in UEBA/anomaly detection + AI reporting [32]. The Investigations feature includes an AI-powered reporting function that analyzes submitted events and logs to generate a detailed report that highlights key findings and recommends defensive actions. Requirements: Investigation must have at least 3 logs, Graylog environment must have public internet access to use	Suitable for SMEs: transparent costs, lighter operations, basic AI features.

		the AI service [33]	

2.1.3 Analysis of Open-source SIEM Solutions

Open-source solutions, by eliminating software licensing costs, represent a more feasible option for SMEs, but they also pose challenges in terms of manpower and scalability.

a. Wazuh

Wazuh is considered one of the most robust open-source platforms, functioning both as a SIEM and a Host-based Intrusion Detection System (HIDS).

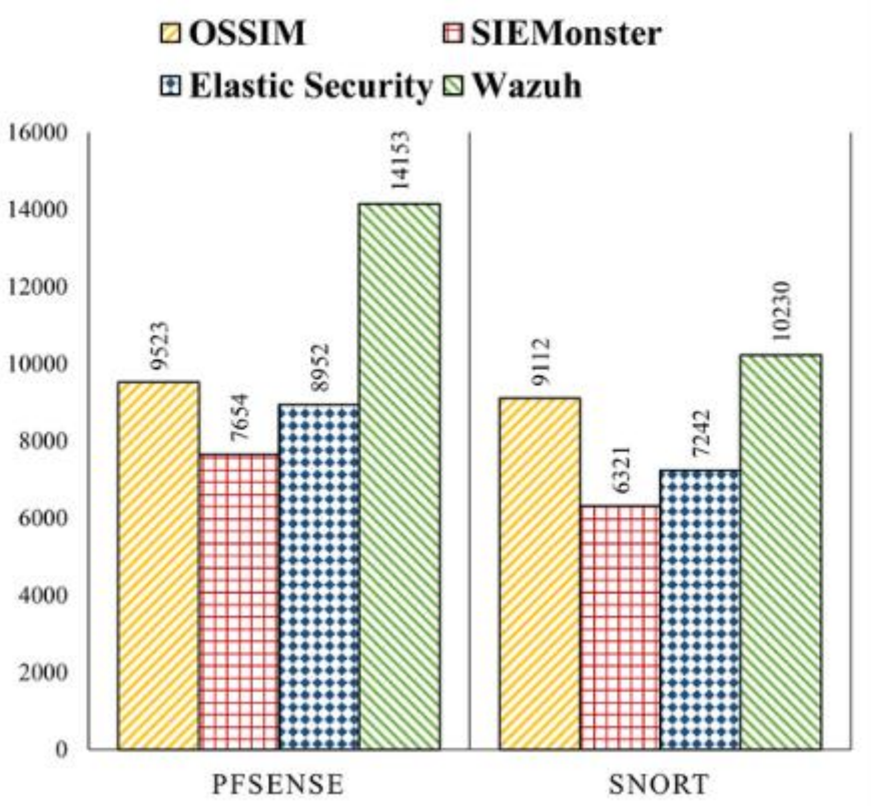


Figure 2.1 EPS of Open-source SIEM solutions [3]

Cost and TCO: Open-source solutions such as Wazuh do not require software license fees. The main costs arise from infrastructure (storage, servers) and human resources required for configuration and operation.

Performance and Scalability: Manzoor et al. evaluated Wazuh as the open-source solution with the highest EPS (Events Per Second) among those studied (including OSSIM, SIEMonster, and Elastic Security) [3].

Strengths: Wazuh stands out for its high openness, superior customizability, and efficiency in SME environments.

Limitations: Despite its robustness, Wazuh requires specialized expertise in SIEM, log analysis, and system administration (particularly integration with the ELK stack) to maximize its potential. Maintenance and infrastructure configuration costs may rise significantly as data volume grows.

b. Elastic Stack/Elastic Security

Elastic Stack (formerly ELK Stack) is another popular option, particularly strong in visualization and search capabilities.

Performance: Vazão et al. evaluated Elastic Stack in a GDPR-compliant environment, showing acceptable log processing performance, including throughput measurements.

Strengths: Elastic Stack tightly integrates search and visualization tools (Kibana, Logstash), offering high flexibility.

Limitations: As data volumes increase, storage and hardware costs can become substantial. Moreover, optimization requires expertise in complex data processing and system configuration.

c. OSSIM/AlienVault USM Open-source (OSSIM)

OSSIM is another open-source solution, serving as the predecessor to AlienVault USM.

Performance: According to Manzoor, OSSIM demonstrates lower log-handling performance compared to Wazuh and Elastic, particularly under heavy log loads.

Limitations: OSSIM's scalability, performance, and customizability are more restricted compared to Wazuh or Elastic. It may experience significant slowdowns if server resources are insufficient.

d. SIEMonster

SIEMonster is another open-source SIEM platform that has been evaluated.

Performance: Manzoor reported that SIEMonster has lower EPS performance than Wazuh when handling large log volumes and suffers from scalability constraints.

Limitations: Its configuration and operation are more complex compared to OSSIM and Wazuh, and its community support and documentation may be weaker for large-scale deployments.

2.1.4 Summary Table of SIEM/Security Solutions

Table 2.2 Summary Comparison of Open-Source SIEM/Security Solutions

Platform	**Operating Cost / License & TCO**	**Human Resource Requirements**	**Performance / EPS / Log Processing Capability / Scalability**	**Key Strengths**	**Main Limitations**
Elastic Stack / Elastic Security	Open-source tools do not require original software license fees, however, infrastructure costs (servers, storage, processing) can become significant when handling large log volumes [34].	Log analysts and specialists are required for configuring Elasticsearch, Kibana, and Logstash, as well as for handling complex data processing [35].	The Vazão study evaluated log-processing capabilities in a GDPR-compliant environment, including throughput measurements, showing that the Elastic Stack delivers acceptable performance under stringent conditions [36] .	Strongly integrated with search, analysis, and rapid data visualization, offering high flexibility.	As data volume increases, storage and hardware costs rise, and expertise in Elastic optimization becomes necessary.
Wazuh [20]	Open-source solutions do not require license fees, the costs primarily stem from infrastructure	Specialized personnel with expertise in SIEM, log parsing, configuration, and system administration	It was evaluated as having the highest EPS among open-source tools in the individual study by Manzoor et al [3].	High openness, strong customizability, effective operation in SME environments,	Skilled personnel are required, and maintenance and infrastructure configuration costs (log storage, security, backup,

	and human resources [37].	(particularly ELK stack in cases of integration) are required to fully utilize the system [38]. This need is implicitly highlighted in many studies addressing the “lack of expertise” challenge.		and superior performance compared to other open-source tools.	etc.) may increase as the system scales, official support and documentation may also be less comprehensive compared to commercial solutions.
OSSIM / AlienVault OSSIM [3]	Open-source and free from software license fees, with operating costs dependent on infrastructure and personnel.	Requires skills in log correlation, rule configuration, and sensor integration.	According to Manzoor’s study, OSSIM’s processing capacity and performance are lower than Wazuh in terms of EPS, particularly under heavy log loads.	Suitable for SMEs seeking a simple SIEM system with community support.	Performance, scalability, and customizability are limited compared to Wazuh or Elastic, and it may exhibit slowdowns if server configuration and resources are insufficient.
SIEMontster [3]	Open-source tool, software licensing is not a major cost factor, with operating expenses primarily driven	Requires engineers with expertise in deploying distributed systems for scalability and managing multiple components.	According to Manzoor, SIEMonster demonstrates lower EPS performance compared to Wazuh under high log volumes, with	Provides a user interface and some extended features, serving as an alternative to OSSIM or Wazuh.	Configuration and operation are more complex, documentation and community support may be weaker than in larger projects, personnel costs can

	by hardware and personnel.		scalability constraints.		be high if optimal performance is desired.

Notes / Explanations:

Manzoor et al. (2024) – *Evaluating Security and Performance of Open-Source SIEM Solutions for SMEs* is a key reference, as it provides a detailed comparison of open-source tools (Wazuh, OSSIM, SIEMonster, Elastic Security) against commercial solutions, with particular focus on EPS and total cost of ownership (TCO).

Regarding human resource requirements, several studies and analyses (e.g., Manzoor et al., 2024) emphasize that SMEs often lack cybersecurity expertise and have limited staff, which poses challenges in deployment and configuration [3].

2.1.5 Summary And Research Gap

a. Analysis of the Performance - Cost Paradox

Paradox 1: High performance comes with unacceptable cost. Leading commercial SIEM solutions such as QRadar, ArcSight, and Splunk deliver superior performance in terms of Event Processing Capacity (EPS) and scalability for large-scale systems. However, these platforms demand an enormous Total Cost of Ownership (TCO), encompassing expensive software licensing, continuous support fees, and, most critically, the cost of highly skilled personnel. This creates an insurmountable financial barrier, rendering such systems economically infeasible for SMEs.

Paradox 2: Low cost comes with human resource burden. Conversely, open-source solutions such as Wazuh, Elastic Stack, OSSIM, and SIEMonster eliminate licensing fees, significantly reducing the initial TCO. Nonetheless, in order to fully operate and leverage the potential of these tools – particularly Wazuh, which has been evaluated as having the highest EPS among open-source platforms – organizations still require staff with specialized expertise in SIEM, log configuration, and system integration. SMEs, which are already constrained both in workforce size and technical expertise, therefore struggle to adopt these solutions effectively.

b. The Burden of Traditional SIEM and the Challenge of Human Effort

The most critical challenge, present in both commercial and open-source SIEM, lies in the quality of alerts. Traditional rule-based SIEM systems tend to generate a large number of false positives (False Positive Rate – FPR), a phenomenon commonly referred to as Alert Fatigue.

This exacerbates the shortage of skilled professionals within SMEs. Their limited IT staff must devote a disproportionate amount of time and effort to filtering out false alerts, wasting scarce resources and risking the oversight of genuine threats. As a result, even when SIEM solutions are deployed, operational costs and human effort remain unsustainably high.

c. Identification of the Research Gap

From the above analysis, a clear research gap emerges: the lack of a SIEM/SOAR solution that is both cost-efficient and operationally lightweight, specifically optimized for SMEs.

Lack of Integrated Models: To date, no study has systematically developed an integrated model that combines a robust open-source SIEM platform (such as Wazuh) with lightweight unsupervised machine learning algorithms such as Isolation Forest (IF) or Local Outliner Factor (LOF) to address the unique challenges of anomalous logs and false positives in SMEs.

Lack of Adaptive SOAR: Existing studies rarely propose adaptive automation mechanisms (Adaptive SOAR) driven directly by AI-derived risk analysis, which would enable SMEs to execute tiered, flexible responses while minimizing the risk of business disruption.

This research is therefore designed to fill that gap by demonstrating that augmenting Wazuh with AI/ML is not merely a technical enhancement, but an economically and operationally sustainable solution. The aim is to build a system capable of significantly reducing false positives (FPR) while automating incident response to lower Mean Time to Respond (MTTR), thereby fundamentally alleviating the operational and financial burdens of cybersecurity for SMEs.

d. Evaluation of Wazuh's current capabilities and strategic advantages

The strategic choice of Wazuh as the foundational platform for this research is predicated on its status as a leading Open-Source SIEM/XDR solution, primarily due to its superior EPS throughput and robust customizability. However, a critical analysis of the current market and technological landscape reveals three key areas where Wazuh must be augmented to compete effectively with advanced commercial platforms and, more importantly, to serve the unique needs of SMEs.

Firstly, in terms of Artificial Intelligence (AI), Wazuh currently lacks a native Generative AI (GenAI) assistant, a feature already integrated by major competitors such as Microsoft Sentinel, Splunk, and Google Chronicle. This deficiency creates a significant research gap and a strategic opportunity to develop a proprietary AI Enhancement Layer. This layer will not aim to build a large language model (LLM) from scratch, but rather to integrate on-demand LLM APIs to perform crucial operational tasks. These tasks include summarizing complex security alerts, generating triage recommendations, enabling natural language rule generation (simplifying configuration for non-specialists), and performing auto-enrichment (e.g., querying VirusTotal/WHOIS) to provide context before automated response, and suggesting adaptive SOAR playbooks. If competitors sell "integrated GenAI," this research delivers "intelligent, cost-optimized operational efficiency."

Secondly, concerning Total Cost of Ownership (TCO), Wazuh holds an undeniable competitive advantage. The Wazuh OSS model incurs nearly $0 license costs (only infrastructure and operation costs), while the Wazuh Cloud service remains highly competitive. This significant cost margin, which stands in stark contrast to the GB-ingest pricing models of solutions like Sentinel and Elastic or the expensive enterprise packages of Splunk and Google, provides the financial flexibility to invest strategically in the lightweight AI layer. The variable cost structure of on-demand LLM APIs, coupled with minimal additional deployment costs for dashboard enhancements, ensures that the proposed solution remains far more affordable than the licensing and ingestion fees of its commercial counterparts, directly addressing the SME's core requirement for optimized TCO.

Finally, regarding Novelty and Contribution, while Wazuh is mature in the traditional SIEM/XDR space, the true innovation lies entirely in the design and implementation of the AI augmentation. The research's distinct contribution will be demonstrated by providing quantifiable evidence of improvement against pre-integration metrics. Specifically, proving a significant reduction in Mean Time to Respond (MTTR), a tangible decrease in analyst hours (human effort) due to lower False Positive Rates (FPR) generated by the IF and LOF models, and an overall reduction in alert noise will validate the framework's effectiveness. This ability to demonstrate quantifiable improvements over a pure Wazuh deployment establishes a novel, high-impact reference model for cost-effective, AI-driven security operations.

2.2 Summary of the Literature Review

The comprehensive review of prior research and existing technological solutions has illuminated several key findings that establish the urgency of this study, simultaneously exposing a persistent dual paradox within the cybersecurity landscape, particularly as it pertains to Small and Medium-sized Enterprises (SMEs).

The evolution of Security Information and Event Management (SIEM) systems and Security Orchestration, Automation, and Response (SOAR) platforms marks significant progress in centralizing defensive capabilities. However, a formidable financial barrier remains firmly in place. Leading commercial SIEM solutions such as Splunk, QRadar, and ArcSight stand out for their high Event Per Second (EPS) throughput and superior scalability, effectively serving the needs of large corporations. Yet, their enormous Total Cost of Ownership (TCO) which encompasses expensive software licensing fees, continuous support costs, and crucially, the high operational cost associated with requiring highly skilled and specialized personnel renders them economically unfeasible for SMEs. This significant cost discrepancy is clearly demonstrated by TCO estimates: three-year TCO for enterprise-grade solutions like QRadar or ArcSight can ascend to hundreds of thousands of dollars, while even lower-tier SIEM solutions start around $50.000. This unassailable financial hurdle, repeatedly highlighted in academic literature and industry reports, is the primary reason why SMEs hesitate to invest in advanced security measures, thereby cementing their position as the weakest link in the digital supply chain.

Secondly, in response to this cost barrier, open-source solutions like Wazuh, Elastic Stack, OSSIM, and SIEMonster have emerged as more cost-effective alternatives by eliminating software licensing fees. Among these, Wazuh is highly regarded for its superior EPS and strong customizability, while Elastic excels in data visualization and searching capabilities. Specifically, research by Manzoor et al. confirms that Wazuh possesses the highest EPS among open-source counterparts, attesting to its efficient log processing capabilities. However, the literature review uncovers a different kind of burden: these platforms necessitate specialized personnel proficient in SIEM administration, log analysis, and complex system integration to operate them effectively. Studies on staffing requirements indicate that SMEs frequently lack cybersecurity expertise and have limited IT teams, which severely hinders their ability to fully leverage the systems' functionalities (e.g., the intricate configuration of the ELK Stack accompanying Wazuh). Furthermore, as data volume increases, storage costs and optimization efforts become substantial challenges, threatening the system's long-term sustainability unless continuously managed by skilled personnel. This dynamic effectively shifts the burden from a financial cost to a human resource strain, a resource SMEs critically lack.

Thirdly, a pervasive and chronic issue across both commercial and open-source SIEM deployments is alert fatigue. Rule-based SIEM systems typically generate a very high False Positive Rate (FPR). This systemic issue within Security Operations Center (SOC) activities compels the limited IT staff of an SME to dedicate a disproportionate amount of time and effort to manually sifting through false alerts, thus wasting precious resources and increasing the risk of missing genuine, critical incidents amidst the high volume of noise.

Fourthly, while SOAR platforms are expected to mitigate the human workload through response automation, the literature reveals that many current solutions still rely on static and rigid playbooks. These playbooks struggle to adapt to the dynamic nature of modern threats like Advanced Persistent Threats (APTs) or zero-day exploits. The absence of a risk-tiered adaptive response mechanism, where the mitigation action is dynamically adjusted based on the alert's actual severity and context, severely limits SOAR's practical value in SME environments. For smaller businesses, flexibility and minimizing unnecessary human intervention are critical to ensuring business continuity.

The integration of Artificial Intelligence and Machine Learning (AI/ML) into cybersecurity has demonstrated significant potential, particularly in anomaly detection and risk scoring to enhance alert quality. Models like Isolation Forest (IF) and Local Outliner Factor (LOF) are considered suitable for SME environments due to their lightweight nature, computational efficiency, and proven ability to handle unlabeled, imbalanced log data, a hallmark of small business environments. However, the majority of AI/ML research in cybersecurity focuses on large enterprises or controlled laboratory settings with abundant resources, paying insufficient attention to the stringent constraints of cost, personnel, and operational feasibility faced by SMEs.

In summary, the literature review emphatically highlights a profound paradox: commercial solutions offer high performance but are economically unattainable, while open-source solutions mitigate costs but place an unsustainable burden on the SME's limited human resources and operational optimization capabilities. Neither category has effectively solved the pervasive problem of false alerts nor provided an adequate adaptive response mechanism. The Research Gap is thus clearly identified: there is a distinct lack of an AI-integrated SIEM/SOAR model explicitly designed and optimized for SMEs that simultaneously ensures cost-effectiveness and reduces the operational burden through the integration of lightweight AI/ML models to reduce false positives, while enabling contextual, automated responses to enhance the system's sustainability. Bridging this gap by building a solution based on the Wazuh platform is the core motivation and primary contribution of the proposed research.

2.3 Contribution of Research

This research is expected to deliver significant and highly applicable value, directly addressing systemic challenges prevalent in the cybersecurity domain, particularly those impacting Small and Medium-sized Enterprises (SMEs). The contributions of this study are categorized into three main facets: Technical and Technological Contributions, Academic Contributions, and Economic and Operational Contributions.

2.3.1 Technical and Technological Contributions

The core technical contribution of this research lies in the construction and validation of a novel integrated architecture, meticulously optimized to leverage open-source technologies for maximal effect in resource-constrained environments.

The study pioneers the Development of a Lightweight AI/ML Integration Architecture by designing a modular, low-latency security event processing pipeline specifically for SMEs. The key breakthrough is the seamless integration of two computationally efficient Unsupervised Machine Learning models (Isolation Forest - IF and Local Outliner Factor - LOF) into the Wazuh-SIEM platform. This amalgamation creates a dual-mechanism for anomaly detection, capitalizing on the resource efficiency of IF and the interpretability of LOF, making it perfectly suited for environments limited by hardware resources and lacking labeled security data. This combined approach is set up to fundamentally resolve the issue of high False Positive Rates (FPR) often plaguing traditional rule-based systems.

Furthermore, the research contributes by formulating an Adaptive SOAR Playbook Design based on Context. The study develops Adaptive SOAR playbooks that move beyond rigid, static rules. Instead, they are dynamically governed by a risk score and threat classification derived directly from the AI module. This Graduated Response model is a significant technical improvement, enabling the system to automate response actions in a way that is both flexible and safer, thus avoiding unnecessary disruption to business operations while drastically reducing the Mean Time to Respond (MTTR) to genuine threats.

2.3.2 Academic Contributions

This research is positioned to fill a noticeable gap in the existing academic literature and provide valuable new empirical data.

The study addresses the significant Research Gap in Applying AI to SMEs by being one of the few works to simultaneously tackle the issues of low TCO, human resource constraints, and detection efficacy through the integration of AI into an open-source platform. While the majority of AI/ML research in cybersecurity focuses on large enterprises, this work provides the foundational theoretical and empirical basis for the field of "AI-driven security for resource-constrained environments."

Moreover, the research is dedicated to Providing a Reference Model and Quantitative Data. The study will publish a Reproducible Prototype, accompanied by detailed documentation and deployment scripts. Crucially, the research contributes quantitative performance data on the system, including essential metrics such as FPR, Recall, MTTR, and a comprehensive TCO analysis comparing the AI-integrated open-source solution against commercial alternatives. This data provides a crucial reference architecture and a new benchmark set for subsequent research into open-source SIEM/SOAR implementations.

2.3.3 Economic and Operational Contributions

The most impactful contribution of this research is the delivery of a sustainable and financially viable security solution for SMEs.

The study champions a Low-TCO and Economically Sustainable Solution. By utilizing an open-source platform (eliminating licensing costs) and leveraging automation (reducing personnel costs), the research demonstrates that high-level cybersecurity is achievable with optimized TCO. The construction of a quantified TCO model will provide empirical evidence of economic sustainability, giving SMEs a solid foundation for investing in advanced cybersecurity measures rather than being constrained by expensive commercial solutions.

Finally, the research directly contributes to Improving Human Effort and Operational Feasibility for the resource-limited IT teams in SMEs. By significantly reducing the burden of Alert Fatigue (via reduced FPR) and accelerating the speed of response (via reduced MTTR), the system enables personnel to focus on strategic tasks and real threats, instead of being bogged down in manual alert triage. This not only optimizes cost but fundamentally enhances the quality of defense for SMEs, solidifying their security posture within the digital supply chain.

CHAPTER 3
METHODOLOGY

3.1 Research Design

3.1.1 Type of Research

This study applies a mixed method experimental design to develop and evaluate an integrated SIEM and SOAR system enhanced with artificial intelligence. The main goal is to determine how AI based anomaly detection and automated response can reduce operational costs and manpower requirements for small and medium enterprises (SMEs) without sacrificing detection accuracy or response speed [10].

The experiment is implemented in a controlled virtual laboratory using open source components including Wazuh as the SIEM, Suricata for network intrusion detection, Filebeat for log collection, and Shuffle for automated response. Two unsupervised learning algorithms, Isolation Forest (IF) and Local Outlier Factor (LOF), are integrated to assist the SIEM in detecting abnormal events more efficiently and with fewer false alerts, thereby reducing analyst workload and incident triage time.
This research is primarily classified as Applied Research combined with a robust Experimental Design.

Quantitative evaluation focuses on detection performance and response efficiency through metrics such as FPR, Recall, AUC PR, MTTD, and MTTR. Qualitative observations assess configuration effort, maintenance complexity, and time savings to estimate the potential cost reduction and labor optimization achieved through AI integration [3].

Both configurations are compared under identical conditions to ensure fair evaluation: the baseline configuration with rule based detection and manual response, and the proposed configuration with AI supported detection and automated response. This design ensures objective measurement of technical improvements together with tangible impacts on operational costs and workforce efficiency.

3.1.2 Research Approach

The research follows an applied and comparative approach, combining both quantitative measurement and qualitative assessment to determine how AI integration in SIEM and SOAR systems can improve detection efficiency while lowering operational cost and workforce demand.

Quantitatively, the study designs two configurations under identical network and data conditions. The baseline system represents a conventional Wazuh deployment relying solely on signature and rule matching. The proposed system integrates AI models (Isolation Forest and Local Outlier Factor) to generate dynamic anomaly scores and trigger automated SOAR playbooks through Shuffle. Key performance metrics such as False Positive Rate, Recall, AUC PR, Mean Time To Detect, and Mean Time To Responses are collected to measure improvement in accuracy and response speed.

Qualitatively, the study observes installation time, configuration complexity, and the number of analyst interventions required during incident handling. These data are used to estimate labor reduction, time savings, and cost efficiency derived from AI driven automation. This dual approach ensures that the evaluation covers both technical and organizational perspectives relevant to SMEs.

By combining measurable performance gains with qualitative insights on resource optimization, the research approach demonstrates not only the technical viability but also the economic and workforce impact of AI integrated security operations in SMEs.

3.1.3 Overall Research Framework

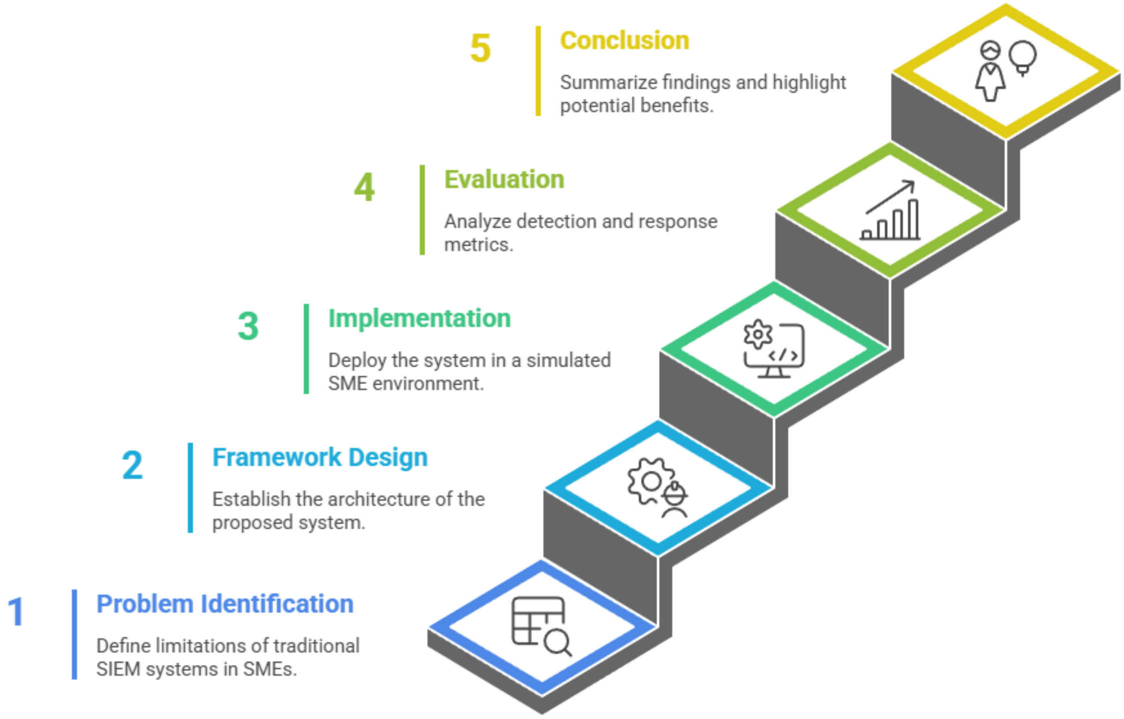

5
Conclusion
Summarize findings and highlight potential benefits.
4
Evaluation
Analyze detection and response metrics.
3
Implementation
Deploy the system in a simulated SME environment.
2
Framework Design
Establish the architecture of the proposed system.
1
Problem Identification
Define limitations of traditional SIEM systems in SMEs.

Figure 3.1 Research Framework for AI-Intergrated SIEM.

The overall research framework of this study illustrates the sequential process from identifying the problem to concluding the evaluation results.

Figure 3.1 illustrates the overall research framework connecting the five main stages of the study: Problem Identification, Framework Design, Implementation, Evaluation, and Conclusion which together form the methodological foundation of this research.

In the **Problem Identification** stage, the research defines existing limitations of traditional SIEM systems in SMEs, such as high manual workload, alert fatigue, and the difficulty of maintaining cost efficiency with limited staff.

The **Framework Design** stage establishes the architecture of the proposed system, integrating open source tools including Wazuh, Suricata, Filebeat, and Shuffle with AI based anomaly detection models (Isolation Forest and Local Outlier Factor). This stage aims to enhance detection accuracy and enable automated response actions to reduce analyst workload.

During the **Implementation** stage, the system is deployed in a controlled virtual laboratory that simulates a realistic SME environment. The integration between SIEM, SOAR, and AI modules is tested through simulated attack scenarios, with detailed log data collection for later analysis.

The **Evaluation** stage involves quantitative analysis of detection and response metrics such as FPR, Recall, MTTD, and MTTR, as well as qualitative assessment of configuration effort, maintenance time, and cost savings. The objective is to verify how AI integration contributes to measurable reductions in operational cost and manpower requirements.

Finally, the **Conclusion** stage summarizes the findings, compares both configurations, and highlights the potential of AI integrated SIEM and SOAR systems to deliver sustainable security management for SMEs with reduced cost and workforce pressure.

3.1.4 Experimental Environment

The experimental environment was designed to simulate a small and medium-sized enterprise (SME) network, providing a realistic testbed for deploying, training, and evaluating the proposed AI-integrated SIEM/SOAR framework. The objective of this environment is to replicate real-world operating conditions while maintaining controlled and measurable parameters to assess the performance of the system under both normal and attack scenarios.

The experimental environment was designed with five core components, working together to simulate a complete security monitoring, detection, and response process for a SME.

- Wazuh Server (Manager, Indexer, Dashboard): Responsible for centralized log collection, correlation, and visualization from various sources, including Windows, Linux, Web Server, Database Server endpoints and Email Server.

- Suricata Network Intrusion Detection System (NIDS): Monitors all network traffic and exports logs in eve.json format, which are then compared with Wazuh data to generate alerts when suspicious or abnormal activities are detected [39].

- Filebeat: Functions as a log forwarder, continuously transmitting log data from Wazuh Agents and Suricata to both the Wazuh Manager and OpenSearch, ensuring reliable and lossless data flow [40].

- AI Algorithm: Performs anomaly detection using two complementary algorithms: Isolation Forest (IF) [41] and Local Outlier Factor (LOF) [42]. These algorithms calculate a dynamic risk score for each malicious event. IF isolates outliers through random partitioning of the feature space, effectively detecting rare and irregular events. In contrast, LOF enhances this by evaluating the local density deviation of each data point relative to its neighbors, allowing the model to detect subtle or localized anomalies.

- SOAR Module (Shuffle): This component is responsible for automating incident response workflows based on the type and severity of detected attacks. Depending on the assessed risk level, it can automatically block malicious IP addresses, isolate compromised hosts, quarantine suspicious files, or send real-time alerts via Slack or Email to the security operations team. The

SOAR playbooks are designed with an adaptive, multi-layered structure, enabling flexible and context-aware responses while maintaining human oversight (human-in-the-loop) for critical actions to ensure safety, accuracy, and prevention of false or excessive reactions in real-world deployments [7].

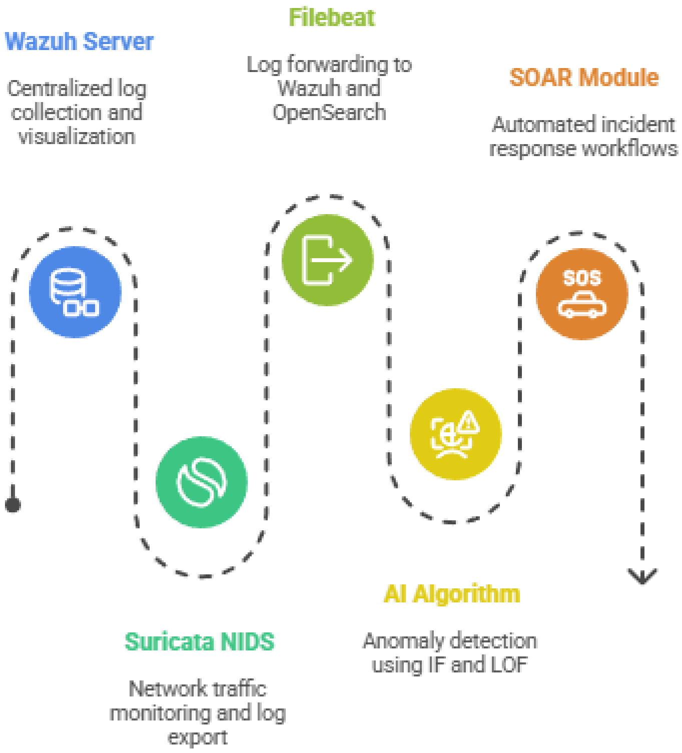

Wazuh Server
Centralized log collection and visualization
Filebeat
Log forwarding to Wazuh and OpenSearch
SOAR Module
Automated incident response workflows
SOS
Suricata NIDS
Network traffic monitoring and log export
AI Algorithm
Anomaly detection using IF and LOF

Figure 3.2 Security System Workflow.

The system is deployed on a virtualized infrastructure using VMware Workstation, consisting of multiple virtual machines representing different endpoint types: Windows Server, Linux Server, Web Server (DVWA), Database Server, Email Server. These virtual machines are connected within a single virtual network segment, where Suricata acts as a network gateway to monitor and analyze all traffic. The Wazuh Manager and OpenSearch Stack run on a dedicated Linux virtual machine (8 GB RAM, 2 vCPUs), while the AI module operates in a Python environment using libraries such as Scikit-learn, Pandas, and NumPy [43].

To evaluate the system's detection and response capabilities, we utilize both normal activity logs and simulated attack data, including scenarios commonly encountered at the Network or DNS layers. Additionally, public benchmark datasets, such as CTU-13 [44] and CIC-Bell-DNS-EXF-2021 [45], are integrated to enhance data diversity and model generalization.

This experimental configuration allows the research team to measure key performance indicators (KPIs): FPR, MTTR, and TCO, while providing a controlled yet realistic testing environment that validates the system's scalability, automation, and practical suitability for cybersecurity operations within SME environments.

3.2 Data Collection Methods

3.2.1 Data Sources

The data collection process in this research was designed to ensure that both system logs and network traffic are accurately captured, processed, and transformed into a structured dataset suitable for training and evaluating the AI-integrated SIEM/SOAR system. Data were obtained from three main sources: Wazuh Agents, Suricata NIDS, and public benchmark datasets.

Wazuh Agent Logs: Wazuh Agents deployed on Windows, Linux, Web, Database, and Email servers continuously collect and forward security events to the Wazuh Manager. The collected logs include system activity, authentication events, file integrity changes, and policy violations. This data represents host-based intrusion detection (HIDS) and reflects endpoint behaviors under both normal and attack conditions [46].

Suricata Network Traffic: The Suricata NIDS captures and analyzes live network packets, exporting the results into an eve.json file. Each record contains fields such as source/destination IPs, ports, protocols. This dataset is essential for detecting network and DNS-level attacks [39].

Public Benchmark Datasets: To enhance dataset diversity and reliability, labeled public datasets such as CTU-13 [44] and CIC-Bell-DNS-EXF-2021 [45] were incorporated . These benchmark datasets strengthen the generalization capability of the AI model, enabling it to detect previously unseen or zero-day attack patterns [4].

a. Data Collection Pipeline

Pipeline Overview:

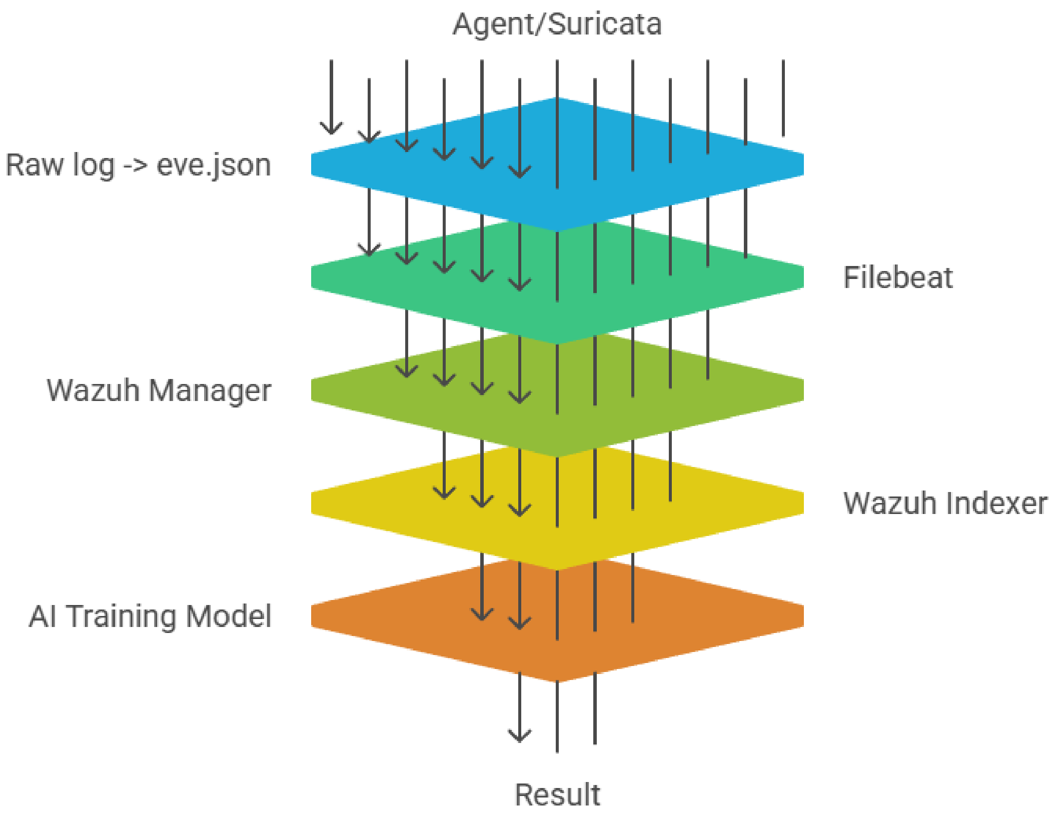


Figure 3.3 Data Processing Funnel..

All logs collected by Wazuh Agents and Suricata were forwarded via Filebeat, acting as a centralized log shipper. Filebeat transmitted the data to the Wazuh Manager, which in turn forwarded the processed events to OpenSearch for storage, indexing, and subsequent AI-model training [47]. During ingestion, custom filter and normalization rules were applied to drop redundant or irrelevant events to minimize alert fatigue and focus on security-relevant events. The data collection spanned continuously the entire project period, with logging triggered by simulated attacks across all configured endpoints. After collection, the dataset was partitioned into training and testing sets to enable quantitative evaluation of the model's generalization performance

b. Normalization Process

Before model training, all datasets were standardized and preprocessed to maintain consistency across heterogeneous sources. Since the public datasets used in this study [44], [45] were already validated and normalized by trusted organizations, additional preprocessing was primarily applied to the real collected logs. The purpose of this step was to enrich the dataset with features that Wazuh could directly capture or derive from existing attributes related to specific attack behaviors [5].

All fields were converted into numeric representations to ensure compatibility with machine learning algorithms. Categorical variables such as event type, DNS query type, and severity level were encoded numerically. Subsequently, all numeric features were scaled using the RobustScaler method to reduce the influence of outliers and stabilize model convergence [48].

The fully preprocessed data were then utilized for feature engineering and the training of two unsupervised anomaly detection models: Isolation Forest (IF) and Local Outlier Factor (LOF) [49]. The anomaly scores generated by these models were reintegrated into the SIEM workflow, allowing Wazuh to prioritize high-risk alerts and enabling the Shuffle SOAR system to execute automated response actions based on risk levels [7].

c. Summary

This data collection process ensures that both host-based and network-based events are comprehensively captured and transformed into a machine-learning-ready format. The resulting dataset provides a robust foundation for developing an accurate, interpretable, and adaptive anomaly detection model, ultimately enhancing the intelligence and automation of the AI-driven SIEM/SOAR framework.

3.2.2 Data Asquisition and Preparation

The data collection method is designed to ensure that both host-based and network-based security events are continuously gathered, processed, and transformed into structured data for AI model training and evaluation. The process is currently being conducted within a controlled virtual laboratory simulating a small and medium-sized enterprise (SME) network.

a. Data Collection Workflow

Logs from Wazuh Agents (deployed on Windows, Linux, Web, Database, and Email servers) and Suricata NIDS are automatically collected and forwarded through Filebeat to the Wazuh Manager, where they are parsed, normalized, and indexed into OpenSearch for analysis [47].

The AI module processes the indexed data, applies anomaly detection algorithms (Isolation Forest and Local Outlier Factor), and generates risk scores for each event. These scores are then forwarded to the SOAR platform (Shuffle) [7], which triggers automated playbooks such as IP blocking, host isolation, or alert notifications. Logs generated during these automated responses are also recorded to evaluate the system's reaction time and automation reliability.

b. Attack Simulation

To ensure realistic and representative datasets, multiple attack scenarios were simulated within the controlled laboratory environment. These simulations were designed to replicate common threat patterns typically faced by small and medium enterprises, while providing diverse input for model training and evaluation [50].

The first category involved Malware Beaconing [44] and DNS Tunneling [45], which emulate covert data exfiltration and periodic command and control communications.

The second group included SQL injection and cross site scripting (XSS) attacks launched from Kali Linux hosts, targeting the web server to trigger correlated alerts across both Suricata and Wazuh [51].

Another scenario simulated SSH brute force attacks, where repeated failed login attempts were generated from distributed source addresses to test authentication anomaly detection [52].

Each event produced during these simulations was processed through Wazuh decoders, correlated with Suricata network alerts, and stored in OpenSearch with synchronized timestamps. Ground truth labels identifying normal and attack traffic were preserved to compute performance metrics such as precision, recall, and false positive rate. The structured execution of these attack scenarios allows precise evaluation of how AI augmentation improves detection accuracy and reduces operational latency, contributing to overall cost and manpower optimization in security operations [4].

c. Log Filtering and Preprocessing

Custom filtering rules are applied to maintain dataset quality and minimize alert fatigue [5]. Redundant or non-security events are excluded. The retained logs represent meaningful security events relevant to intrusion detection and anomaly detection tasks. In addition, correlated events sharing identical timestamps, IPs ,or rule IDs are grouped to create temporal patterns that can improve AI feature learning and behavior analysis [53].

d. Integration with SOAR

During data collection, the SOAR system (Shuffle) remains integrated into the pipeline to capture real-time feedback from automated responses. For example, when the AI model flags a suspicious connection, the SOAR playbook automatically executes mitigation actions and records metadata such as execution time, alert category, and resolution status [7]. These response logs serve as an additional dataset to evaluate the Mean Time to Respond (MTTR) metric and to verify that automation workflows are functioning correctly [54].

e. Ongoing Collection and Storage

Data were continuously collected throughout the experimental phase under controlled conditions. Logging covered multiple operational states including normal system behavior, background network noise, and simulated cyberattacks. All collected events were automatically validated, stored, and indexed within OpenSearch, forming the basis for subsequent AI training and evaluation [55]. The dataset partitioning strategy was applied chronologically to preserve temporal consistency and to ensure fair performance assessment of both anomaly detection and automated SOAR response workflows [7].

3.2.3 Data Collection Duration and Scope

The data collection process was conducted continuously throughout the project implementation period within a controlled virtualized laboratory that replicates the operational characteristics of a small and medium sized enterprise (SME) [11]. The test environment consists of multiple interconnected virtual machines representing essential components of an enterprise infrastructure, including Windows Server, Linux Server, Web Application Server, Database Server, and Email Server.

During this period, all system components including the Wazuh Manager, Suricata NIDS, Filebeat, OpenSearch Stack, and the AI module were configured to operate continuously to ensure uninterrupted collection of both normal activity logs and simulated attack logs [47].

Periodic execution of attack scenarios generated diverse data samples that reflect realistic cybersecurity conditions typically encountered by SMEs [44], [45].

The dataset primarily includes security relevant logs that directly support anomaly detection and automated response objectives. Routine operational records such as maintenance logs, service startup events, and heartbeat messages were excluded during preprocessing to reduce noise and preserve data quality.

Although the data collection took place in a simulated environment, the network topology, log flow, and attack behaviors were carefully designed to mirror real world SME infrastructures. This approach ensures that the resulting dataset is representative, reproducible, and suitable for evaluating the performance, accuracy, and scalability of the proposed AI integrated SIEM and SOAR framework under SME scale operational conditions.

3.2.4 Data Normalization

Since the benchmark datasets used in this research (such as CTU-13 [44] and CIC-Bell-DNS-EXF-2021 [45]) were already preprocessed, normalized, and labeled by their original authors, no major normalization steps were required. The datasets were verified to ensure numerical consistency, valid labels, and the absence of missing or duplicate records.

For integration purposes, minor adjustments were made to align the benchmark data with the field structure used in the experimental logs collected from Wazuh and Suricata. This included renaming certain fields (e.g., “Source IP” to “src_ip”, “Destination Port” to “dest_port”) and verifying timestamp formats [56], [57].

A validation step was also conducted to confirm that all numeric features were within expected ranges and that class labels were properly balanced for anomaly detection (Normal vs Anomalous) [58]. After validation, the dataset was confirmed to be ready for training and evaluating the IF and LOF algorithms.

This process ensured compatibility between the benchmark datasets and the lab-generated logs, enabling consistent and reliable AI model training.

3.3 Sampling and Data Analysis Techniques

This section describes the procedures for sampling, preprocessing, model selection, and evaluation used in analyzing the collected dataset. The goal is to ensure that the AI models can detect anomalies efficiently and that the results are validated through measurable metrics.

3.3.1 Sampling

The dataset used in this study consists of both real collected logs from Wazuh and Suricata, as well as public benchmark datasets, specifically CTU-13 [44] and CIC-Bell-DNS-EXF-2021 [45]. The CTU-13 dataset contains thirteen botnet attack scenarios with a very high level of noise, where legitimate traffic accounts for only about five percent of all logs. All irrelevant or noisy records were filtered out, retaining only normal logs for model training. In contrast, the

CIC-Bell-DNS-EXF-2021 dataset is pre-labeled, focusing on DNS data exfiltration behavior, and was used as a reference for model evaluation.

To ensure statistical validity and avoid data bias, a stratified sampling method was applied to maintain the ratio between normal and anomalous events. The final combined dataset was then divided into two subsets: the training set, consisting mainly of normal samples for model fitting and parameter tuning, and the testing set, which includes both normal and attack logs for performance evaluation [57].

This partitioning strategy preserves class balance and temporal continuity between datasets, ensuring that the anomaly detection model is evaluated in a fair, accurate, and reproducible manner.

3.3.2 Preprocessing

Before model training, all log data collected from Wazuh, Suricata, and public datasets were preprocessed to ensure consistency, quality, and model readiness. This stage aimed to remove redundant or noisy events, unify heterogeneous data structures, and generate suitable input features for machine learning models while maintaining high computational efficiency for real-time operation.

Two main categories of network behavior were the focus of processing: DNS tunneling and Beaconing. Each category's features were extracted based on well-established theoretical and empirical foundations from previous studies.

For **Beaconing**, flow-level features [44] were extracted, including: flow_start, flow_duration, flow_bytes_per_s, flow_pkts_per_s, down_up_ratio, average_packet_size, time_diff, time_diff_std, repetition_rate.

For **DNS tunneling**, feature extraction followed the field structure of the CIC-Bell-DNS-EXF-2021 dataset [45], including: subdomain_length, upper, lower, numeric, entropy, special, labels, labels_max, labels_average, longest_word, len, subdomain.
These features reflect the semantic and entropy characteristics of DNS queries, allowing the detection of hidden data exfiltration channels embedded in domain names.

Among them, three features: time_diff, time_diff_std, and repetition_rate were newly proposed and computed based on aggregated data from Wazuh and Suricata:

- The **time_diff** feature represents the time interval between consecutive flows with the same source, describing the communication periodicity of the host. Previous studies have demonstrated that inter-arrival time (IAT) at the flow level is a standard indicator for network traffic classification. In the context of Wazuh, where packet-level IAT is unavailable, using flow-level time_diff is fully justified and scientifically grounded [59], [60].

- The **time_diff_std** feature denotes the standard deviation of time_diff, quantifying the stability of communication periodicity. The study *Traffic Classification – Packet-, Flow-, and Application-based Approaches* confirms that the distribution and variance of IAT serve as reliable indicators of connection stability, providing a solid theoretical foundation for this feature [61].

- Similarly, repetition_rate expresses the ratio of repeating delta intervals within a flow. When most deltas are nearly equal, the traffic exhibits regular repetition, a typical characteristic of beaconing. This finding aligns with the basis presented in *Packet Inter arrival Time Distribution in Academic Computer Network* [62], which shows that small deviations between time deltas reflect automated and periodic communication activity, such as command and control (C2) connections.

All features were numerically encoded and normalized using the RobustScaler method to minimize the influence of outliers, ensuring that extreme flow values do not distort anomaly detection models [48]. The preprocessed dataset was then used to train two unsupervised models, Isolation Forest (IF) [41] and Local Outlier Factor (LOF) [42]. The anomaly scores generated by these models were reintegrated into the SIEM pipeline, allowing the system to prioritize high risk alerts and trigger automated SOAR (Shuffle) response actions based on dynamic risk scoring [20].

This preprocessing and feature extraction workflow ensures that the AI integrated SIEM and SOAR system can operate effectively in SME environments, maintaining high detection accuracy while reducing operational costs and workforce requirements in real world deployment.

Before model training, all log data collected from Wazuh, Suricata, and public datasets were preprocessed to ensure data consistency and quality. The preprocessing pipeline was designed to eliminate redundant messages, unify data formats, and prepare standardized inputs for machine learning models while ensuring model efficiency and operational performance.

3.3.3 AI Algorithm Used

This research integrates two unsupervised machine learning algorithms, Isolation Forest (IF) and Local Outlier Factor (LOF), to detect anomalous patterns in both network and host level logs. The combination of these algorithms enables the system to capture both global and local anomaly structures, improving detection accuracy and interpretability.

a. Isolation Forest (IF)

The Isolation Forest algorithm isolates anomalies through recursive random partitioning of the feature space [63]. Since anomalous data points are fewer and behave differently from normal observations, they can be isolated with fewer random splits. Isolation Forest operates in near-linear time, with linear training complexity and low memory overhead, making it suitable for large and high-dimensional datasets. Previous studies have demonstrated IF’s robustness in industrial and cybersecurity contexts, especially in detecting abnormal authentication patterns, file system modifications, and network traffic anomalies [49], [64].

b. Local Outlier Factor (LOF)

The Local Outlier Factor algorithm identifies anomalies by comparing the local density of each data point with that of its neighboring points. A sample is considered anomalous if its density is significantly lower than the densities of its neighbors, indicating a local deviation from normal behavior [15]. LOF is highly effective for detecting context dependent or subtle anomalies such as slow rate beaconing, DNS tunneling, or lateral movement patterns that may not appear abnormal in a global context [45]. While LOF has a higher computational cost compared to IF, it complements the Isolation Forest by focusing on the local density relationships within the dataset, enhancing the overall sensitivity of the anomaly detection system [65].

By combining Isolation Forest for global detection and Local Outlier Factor for local contextual analysis, the system achieves a balanced detection mechanism that is both computationally efficient and context aware. This hybrid approach enables the AI integrated SIEM SOAR framework to reduce false positives while maintaining real time detection capabilities suitable for small and medium sized enterprise environments.

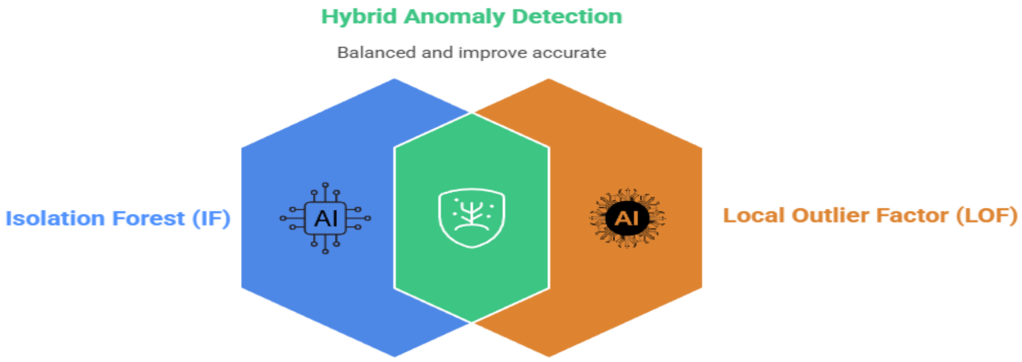


Figure 3.4 Hybrid Anomaly Detection for Enhanced Accuracy.

3.3.4 Evaluation Metrics

The evaluation metrics are designed to assess both the technical performance and operational efficiency of the proposed AI-enhanced SIEM/SOAR framework.

While the technical metrics (e.g., FPR, Recall, Precision, AUC-PR) focus on the detection capability and accuracy of the anomaly detection models, the operational metrics (e.g., MTTR, EPS stability, and TCO) measure the system's responsiveness, scalability, and cost-effectiveness when deployed in a real-world SME environment.

These metrics collectively ensure that the system is not only capable of accurate detection but also practical, efficient, and economically viable for organizations with limited cybersecurity resources.

Table 3.1 Definitions of Detection and Operational Metrics.

Metric	Description
False Positive Rate (FPR)	FP / (FP + TN). Represents the proportion of benign events incorrectly flagged as malicious [66].
Recall (Detection Rate)	TP / (TP + FN). Measures the proportion of true attacks successfully detected [66].

Precision & AUC-PR (F1)	TP / (TP + FP) and 2PR / P + R. Balance between correct detections and false positives under imbalanced datasets. The Area Under Precision-Recall Curve (AUC-PR) provides robustness evaluation [66].
MTTD / MTTR	Mean Time to Respond / Detect. Calculated based on timestamps from detection to response execution [54].
EPS Stability	Measures the number of events processed per second by the SIEM under continuous load [3].
TCO Analysis	Includes licensing and operational cost.

By combining these metrics, the evaluation framework provides a multi-dimensional understanding of both detection performance and operational practicality. This allows the research to demonstrate not only how accurate the AI-enhanced SIEM/SOAR is, but also how well it performs within the financial and resource constraints of SMEs [67], [68].

3.3.5 Analysis Method

This section explains in detail how we analyze and evaluate the effectiveness of the proposed AI-enhanced SIEM/SOAR model. The analysis is based on two main comparison aspects: Technical Evaluation (performance comparison) and Economic Analysis (TCO comparison).

The goal is to ensure objective results and demonstrate that the proposed system can significantly reduce operational costs for small and medium-sized enterprises (SMEs).

a. Technical Performance Comparison and Evaluation

The evaluation framework compares two configurations: Wazuh using only its default detection rules (Baseline Configuration) and Wazuh combined with AI (Isolation Forest and Local Outlier Factor) and the adaptive SOAR platform Shuffle (Proposed Configuration).

Each configuration is tested across multiple simulated attack scenarios and repeated several times to minimize statistical variance. Paired statistical tests are applied to verify the significance of improvements in FPR and Recall.

The results are illustrated through charts, including anomaly detection plots and cost performance comparison graphs. This multi-layer validation approach ensures both technical reliability and economic feasibility within small and medium-sized enterprise (SME) environments.

Baseline Configuration:
This is the standard Wazuh deployment that relies entirely on its built-in detection rules. All incident responses are handled manually by analysts without any support from AI or SOAR components, and it serves as the reference point for comparison.

Proposed Configuration:
This is an enhanced version of Wazuh integrated with an AI module (Isolation Forest and Local

Outlier Factor) and a SOAR module (Shuffle platform). In this configuration, the system automatically calculates a risk score for each alert, triggers automated response playbooks, and supports semi-automated workflows to reduce analyst workload and shorten response time.

b. Experiment Process and Data Collection

All experiments were conducted under controlled lab conditions. Both configurations were tested using the same log and network traffic dataset collected from the simulated SME environment.

The dataset contains both normal activity and real attack scenarios such as DNS tunneling, malware beaconing, brute-force attacks, and data exfiltration [44][45].

To prepare the data for AI training, attack events were labeled as "Anomaly", while normal activities were labeled as "Normal" based on known timestamps.

Each attack scenario was repeated multi-times to minimize random errors and ensure consistency in results.

c. Quantitative and Statistical Analysis

Quantitative analysis was performed using the main performance metrics: False Positive Rate (FPR), Recall, Precision, Mean Time to Respond (MTTR), Events Per Second (EPS), and Total Cost of Ownership (TCO) [54].

SOAR Evaluation: The MTTR metric was measured from the exact time an alert was generated until the automated or semi-automated SOAR action was completed.

Statistical analysis was performed to compare the average values of FPR and Recall between the two configurations, assessing the level of improvement achieved by the proposed model. All calculations and images will be clearly presented, ensuring that the results are reproducible and objectively verifiable.

This ensures that the observed improvements are statistically significant and not due to random variation [69].

Null Hypothesis (**H_0**): There is no significant difference in performance between the two configurations.
Alternative Hypothesis (**H_a**): The proposed configuration shows significant improvement.

d. Economic Comparison (TCO Evaluation)

The Total Cost of Ownership (TCO) analysis compares both configurations internally and against other popular open-source SIEM/SOAR solutions (e.g., ELK Stack, OSSEC, OSSIM/AlienVault OSSIM, SIEMonster).

The economic comparison covers the following cost categories:

- **License Cost:** Includes licensing (if applicable), cloud or hardware requirements.

- **Operational Cost (OpEx):** Covers maintenance, updates, and staff time for manual alert handling.

Through this analysis, the research aims to demonstrate that integrating AI and SOAR not only improves technical efficiency (higher precision, lower FPR, shorter MTTR) [66] but also achieves better cost optimization compared to other open-source alternatives [3].

This makes the proposed solution highly practical and affordable for SMEs with limited cybersecurity budgets [70].

3.4 Limitations of the Methodology

3.4.1 Experimental Enviroment Limitations

The experimental setup was implemented in a controlled and virtualized laboratory environment to ensure consistency and safety during testing. Although this approach allows for repeatable experiments and controlled attack simulations, it also introduces certain limitations when compared to a real-world SME infrastructure.

First, the lab environment does not fully replicate the network scale, traffic diversity, and endpoint heterogeneity typically found in production systems. The number of endpoints, users, and concurrent sessions is limited, which may result in lower log volume and fewer complex correlations than those seen in a real organization [71].

Second, system resources such as CPU, memory, and network bandwidth are constrained by the virtualization platform [71]. These factors can influence the Events Per Second (EPS) rate and might not reflect the scalability behavior of a full-scale deployment.

Third, attack simulations, although realistic (e.g., DNS tunneling, brute-force, malware beaconing), are still controlled scenarios. They do not fully capture unpredictable attack patterns or zero-day exploits that occur in live enterprise environments.

Finally, the integration between Wazuh, Suricata, and SOAR (Shuffle) was tested on isolated virtual machines, meaning inter-system latency and real-time response performance may differ when deployed in distributed or cloud-based infrastructures

Despite these limitations, the virtual lab provides a reliable foundation for proof-of-concept validation. The results obtained are sufficient to demonstrate the technical feasibility, operational reliability, and potential scalability of the proposed AI-enhanced SIEM/SOAR framework for SMEs.

3.4.2 Limitations of studying hidden cost components

One of the major challenges in evaluating the Total Cost of Ownership (TCO) for cybersecurity systems such as SIEM and SOAR is identifying and accurately estimating the hidden cost factors [70]. While direct costs such as hardware, software licenses can be clearly estimated, many indirect or “soft” costs are difficult to measure and compare objectively.

The hidden cost factors include:

- Labor cost: The time security specialists spend handling false alerts, updating rules, and maintaining the system is often not recorded in detail.

- Training and knowledge maintenance cost: Continuous training is needed to keep up with new threats or system changes, which leads to varying costs among organizations.

- Productivity loss due to alert fatigue: When the number of alerts becomes too high, employees lose focus and response times increase, reducing operational efficiencythis impact is rarely measured.

- Maintenance and integration cost: Open-source systems often require ongoing customization and integration with other tools, which adds many unrecorded work hours.

According to LOGPOINT Blog [72], since most small and medium-sized enterprises (SMEs) do not keep detailed accounting data for their operational activities, this study estimates hidden costs using two complementary approaches. For public cost components such as license fees, the research examines the pricing mechanisms of different SIEM platforms, which may follow either a “pay-as-you-go” model (charging based on actual usage) or a fixed-capacity subscription model for a period of 6 to 12 months or longer.

From this, two key data points are collected:

- The pricing model and unit cost of each SIEM platform.

- The average daily log volume or Events Per Second (EPS) generated by a typical SME. The estimated average cost is then calculated by multiplying the unit price by the average daily log volume and converting it into a monthly or yearly cost.

For indirect costs such as training, maintenance, and system integration, direct quantitative data is often unavailable. Therefore, the study applies a case study synthesis approach by reviewing technical documents, research reports, and real-world discussions from trusted cybersecurity forums that address SIEM or SOAR operational costs in SMEs. This serves as an alternative to traditional direct measurement methods.

Using these two approaches, the TCO analysis maintains a reasonable basis for comparison between the baseline configuration and the proposed configuration. However, it should be noted that this method cannot fully capture every indirect cost that may occur in a real enterprise environment. It only provides a relative and verifiable estimation based on public data and credible references.

3.4.3 AI Model Limitations

Although integrating AI significantly improves detection accuracy and automation within the SIEM/SOAR system, the two anomaly detection algorithms used: Isolation Forest (IF) [73] and Local Outlier Factor (LOF) [42] still exhibit several inherent limitations at the algorithmic, data, and operational levels. These limitations must be clearly identified to design appropriate risk control mechanisms and ensure sustainable model performance in real-world environments.

a. Unsupervised nature and hidden label risks

Both algorithms are unsupervised learning models that rely entirely on training from existing datasets that have already been labeled and prepared for learning. When the models are deployed in real environments, behavioral patterns can change due to business shifts, system policy updates, or seasonal variations. As a result, the model's understanding of what constitutes an "anomaly" may gradually drift away from its original intent [74].

Consequently, legitimate but rare or newly emerging activities may be incorrectly flagged as anomalies, especially in dynamic enterprise networks. This issue becomes more severe when the background data contain a high level of noise or when historical data do not accurately represent the current operational context [14].

To mitigate this problem, several strategies were applied. Anomaly thresholds were defined for each data source and event type instead of using a single global threshold. Additionally, pre-labeled and numerically standardized datasets verified by domain experts during operation and testing were incorporated to support regular fine-tuning of the model.

b. Limited interpretability and implications for SOAR

While IF provides relative anomaly scores and LOF computes local density deviations, neither identifies root causes, feature importance, nor the specific attack category associated with an anomaly. In a SOAR context, this limitation can lead to inappropriate automated responses if no review mechanism is in place [7]. Beyond transparency during incident investigation, interpretability is also crucial for optimizing thresholds, refining playbooks, and improving operator training.

c. Explainability limitations

The explainability of both algorithms remains limited, as they essentially behave like "black boxes." Analysts often cannot understand precisely why a particular event was flagged as anomalous. Although IF [73] offers a relative anomaly score and LOF [42] indicates local density deviation, neither provides clear reasoning or links to specific attack patterns. This makes it difficult to justify or audit SOAR's automated actions, especially in cases requiring traceability or post-incident review.

d. Sensitivity to feature selection and preprocessing

Finally, both algorithms are highly sensitive to feature selection and normalization. If input data are not consistently processed or contain redundant features, the model's precision may degrade significantly [41], [42]. Furthermore, LOF tends to suffer performance loss on high-dimensional datasets, where the cost of neighbor searches increases, causing latency and potential instability under heavy event throughput.

e. Summary

The limitations above do not reduce the value of IF and LOF in the SME context. Instead, they help define the operational boundaries and the conditions required for safe and efficient deployment. With careful tuning of anomaly thresholds according to specific contexts, continuous monitoring of data quality, retraining strategies to manage concept drift, and the inclusion of human oversight for high-risk SOAR actions, IF and LOF remain highly suitable choices thanks to their strong performance, low computational requirements, and simple implementation.

In future work, the framework could be improved by adding lightweight explainability layers to enhance transparency, adopting semi-supervised learning to make use of partially labeled operational data, or integrating large language models (LLMs) as intelligent assistants for threat hunting. This approach would build on the strengths of the Wazuh baseline, allowing analysts to conduct faster investigations and reduce their workload during incident response.

3.4.4 Data Limitations

Although the data collection process was designed carefully, several limitations remain. Most data were gathered from a controlled virtual lab that simulated SME networks, which cannot fully capture the complexity and unpredictability of real enterprise environments [71]. The simulated attacks covered common threats but not advanced or multi-stage attacks. Public benchmark datasets like CTU-13 [44] and CIC-Bell-DNS-EXF-2021 [45] added diversity but differed from real network data in structure and labeling. Furthermore, no real user data were included due to privacy concerns, limiting behavioral realism [75]. Overall, the dataset provides a solid base for evaluation but lacks the scale and variability of real-world conditions, suggesting future work should expand data sources and apply augmentation or transfer learning to improve adaptability.

CHAPTER 4
EXPERIMENTAL AND RESULTS

4.1 Introduction

This chapter presents a comprehensive experimental evaluation of the proposed AI-enhanced SIEM/SOAR framework, designed to improve detection accuracy, reduce false positives, and lower operational workload for small and medium-sized enterprises (SMEs). The experiments were conducted in a controlled laboratory environment that emulates realistic SME operating conditions, including constrained hardware capacity, moderate log volumes, diverse cyberattack scenarios, and limited security personnel. The primary objective is to determine whether lightweight unsupervised machine learning models, specifically Isolation Forest (IF) and Local Outlier Factor (LOF), can enhance the baseline detection capabilities of Wazuh while remaining computationally efficient and financially viable for SME deployment.

The evaluation explores five key dimensions:

1. Dataset generation and preprocessing.
2. Benchmarking AI-driven anomaly detection performance.
3. False positive reduction and alert quality improvement.
4. Operational efficiency gains, especially TCO and MTTR reduction.
5. System-level implications and comparative analysis with existing literature.

Beyond quantitative metrics, this chapter also highlights qualitative observations regarding system behavior, analyst workload, and overall feasibility of deploying the AI-enhanced SIEM/SOAR architecture within SME environments. These insights contribute to validating the practicality and operational relevance of the proposed approach, reinforcing findings in contemporary research on AI-assisted security operations centers.

4.2 Presentation of Data

4.2.1 Dataset Composition

The experimental dataset was constructed with an average of approximately *~**14.000.000 logs*** collected from four endpoints over a period of ***27 to 30 days.*** This collection process was designed to simulate the log distribution typically observed in small and medium sized enterprise environments. The dataset is organized into three groups that include normal operational logs representing legitimate system and user behavior, simulated attack logs generated from controlled ATT&CK based scenarios, and hybrid or noise inducing events that capture ambiguous situations that often lead to false positives in real world systems. The combination of these three groups creates a diverse and realistic log environment that allows for a comprehensive evaluation of detection accuracy, the ability to identify abnormal behavior, and the resilience of the system against false positives.

a. Normal Operational Logs

This category contains approximately average ***~428.300 logs per day*** representing legitimate day-to-day system and network activities within a typical SME environment. These logs include:

- Windows Event Logs (authentication records, process creation, security policy updates)
- Linux system logs (system calls, file operations, service start/stop events)
- Web server access logs (HTTP requests, status codes, request paths)
- Database audit logs (query execution, user session events)

These events form the baseline behavioral profile of the environment. They serve as the reference distribution from which the anomaly detection models attempt to distinguish abnormal or malicious patterns.

b. Simulated Cyberattack Logs

The second category consists of approximately average ***~49.000 logs per day*** generated from controlled attack scenarios executed in the experimental testbed. These simulations replicate high-impact adversarial behaviors mapped to the MITRE ATT&CK framework, including:

- Brute-force authentication attempts
- Network reconnaissance and port scanning (e.g., masscan, Nmap scans)
- Lateral movement patterns (abnormal SSH usage, PsExec executions)
- File modification bursts indicative of ransomware behavior
- Unauthorized privilege escalation attempts
- Command-and-control (C2) beaconing and periodic outbound callbacks

These logs represent the malicious ground-truth samples used to assess recall, precision, and anomaly detection performance.

c. Hybrid and Noise-Inducing Events

This category contains approximately average ***~7.700 logs per day*** that exhibit mixed or ambiguous characteristics neither fully benign nor overtly malicious. Hybrid examples include:

- Legitimate administrator activities resembling lateral movement
- Irregular but non-malicious network bursts
- Application errors misclassified as potential policy violations
- User behaviors that deviate from baseline but do not constitute attacks

These events introduce realistic noise into the dataset and help evaluate the system’s robustness against false positives.

All logs were collected using Wazuh agents deployed on Windows and Linux endpoints, Suricata NIDS sensors producing **eve.json** network telemetry, and additional application-level services. After collection, events were normalized via Wazuh decoders and indexed into OpenSearch before being forwarded to the AI anomaly detection engine. The final dataset structure aligns closely with empirical studies on enterprise log distributions and adheres to established methodologies for evaluating unsupervised anomaly detection systems.

4.2.2 Attack Scenarios

Number of logs generated from each attack scenario:

Table 4.1 Summary of Simulated Attack Dataset

Attack Type	**Description**	**Number of Logs**	**Number of Alerts**
DNS Tunneling	Long DNS queries	~7.500	~1.300
SSH Brute Force	High-rate failed logins	~12.500	~2.600
SQLi, XSS, SSRF	DVWA exploitation	~4.000	~900
Beaconing	Periodic C2-like patterns	~6.100	~850
Port Scanning	Nmap scans	~8.800	~1.200
File Integrity Tampering	Change sensitive system files	~10.100	~2.500
Total		***~49.000***	***~9.350 (19,082%)***

4.2.3 Data Preprocessing and Feature Engineering

The preprocessing stage was designed to ensure the consistency, reliability, and suitability of the collected logs for the unsupervised anomaly detection task. All events originating from multiple heterogeneous sources were transformed into a unified representation through a processing pipeline that includes normalization, feature encoding, and vector preparation. This pipeline ensures that the final dataset can be effectively processed by the Isolation Forest and Local Outlier Factor models without losing contextual meaning or incurring unnecessary computational overhead.

During feature construction, we focused on two representative attack types within the system: DNS Tunneling and Malware Beaconing, as these attacks are notoriously difficult to detect using traditional rule-based mechanisms and align well with anomaly-based detection approaches. The extracted feature sets are summarized as follows:

DNS Tunneling: subdomain_length, upper, lower, numeric, entropy, special, labels, labels_max, labels_average, longest_word, len, subdomain.

Beaconing: flow_start, flow_duration, flow_bytes_per_s, flow_pkts_per_s, down_up_ratio, average_packet_size, time_diff, time_diff_std, repetition_rate.

4.3 Analysis of Results

This section presents the quantitative evaluation of the anomaly detection module and analyzes how the combined Isolation Forest (IF) and Local Outlier Factor (LOF) model improves the system’s ability to identify abnormal behaviors across multiple attack scenarios. Since the native Wazuh ruleset does not perform statistical anomaly detection, the comparison focuses exclusively on model-level performance: Isolation Forest alone versus the hybrid IF + LOF ensemble. The evaluation metrics include Recall, Precision , and F1-score.

4.3.1 Scenario-Based Detection Results

a. Anomaly-based Detection Scenarios (IF vs IF + LOF)

Two representative attack classes were selected for detailed analysis: DNS Tunneling and Beaconing, both of which traditionally exhibit subtle patterns that challenge rule-based detection. Tables 4.2 and 4.3 below summarize the precision, recall, and F1-score for each configuration.

Table 4.2 DNS Tunneling detection Metrics Comparison (IF vs. IF + LOF).

Metric	Isolation Forest (IF)	IF + LOF (Refine)	Improvement
Precision	95,88%	95,98%	0,1%
Recall	92,70%	94,95%	2,25%
F1	94,26%	95,46%	1,2%

- Precision remains nearly unchanged, indicating that the inclusion of LOF does not increase false positives or misclassification of benign DNS queries.
- Recall shows a **2,25%** improvement, demonstrating that LOF significantly enhances the system’s ability to identify high-entropy, obfuscated DNS traffic commonly used in tunneling.
- The F1-score increase reflects more balanced, reliable detection.

Table 4.3 Beaconing detection Metrics Comparison (IF vs. IF + LOF).

Metric	Isolation Forest (IF)	IF + LOF (Refine)	Improvement
Precision	89,9%	89.7%	-0,2%
Recall	53,5%	80,4%	26,9%
F1	67,1%	84,8%	17,7%

- Precision remains stable, confirming that LOF does not introduce additional noise into the detection pipeline.

- Recall improves by **26,9%**, indicating that the ensemble better captures the periodic, low-volume communication patterns typical of C2 beaconing.
- The F1-score again shows substantial improvement, confirming the ensemble's ability to detect low-and-slow behaviors that IF alone struggles with.

Summary:

Across both attack categories, the combined IF + LOF model demonstrates clear and consistent improvements in recall and F1-score. The ensemble exploits the complementary strengths of the two algorithms: IF excels at identifying global anomalies, and combining with LOF captures subtle local deviations in behavioral density.

By integrating both, the system achieves more robust anomaly detection without compromising precision. This validates the suitability of the IF + LOF ensemble as an effective unsupervised approach for detecting complex and evasive threats in SME environments.

b. Rule-Based Detection Scenarios (AI-assisted)

For the remaining attack categories such as SSH Brute Force, SQL Injection (SQLi), Cross-Site Scripting (XSS), Server-Side Request Forgery (SSRF), Port Scanning, and others, the primary detection mechanism is handled through Wazuh's rule-based engine in combination with custom correlation rules developed during the experiment. These signatures form the core detection logic for high-confidence, pattern-based attacks where rule-based strategies remain highly effective.

In these scenarios, the role of the AI module is fundamentally different from its direct detection function in DNS Tunneling and Beaconing. After incoming logs are processed by Wazuh's rule engine, any events that do not match existing signatures but still exhibit irregularities are isolated and passed into the anomaly detection pipeline. The AI module then evaluates these events and assigns anomaly scores to support triage and prioritization. This process provides several operational benefits:

- Reduction of low-severity false positives and background noise, thereby lowering analyst workload in SOC environments.
- Assignment of anomaly scores to highlight potentially important deviations, enabling analysts to quickly identify high-priority events.
- Improved situational awareness by clustering related log events and revealing behavioral patterns that may not be obvious from signature-based alerts alone.
- Elimination of redundant or duplicate alerts, optimizing the alert stream and preventing alert fatigue.

Clarification: In these scenarios, the AI model does not directly improve rule-based Recall. Detection is still driven by Wazuh's built-in signatures and custom rule enhancements. The contribution of AI lies in reducing false positives, assisting in alert prioritization, and enhancing classification efficiency not in increasing the raw detection rate of rule-based attack types.

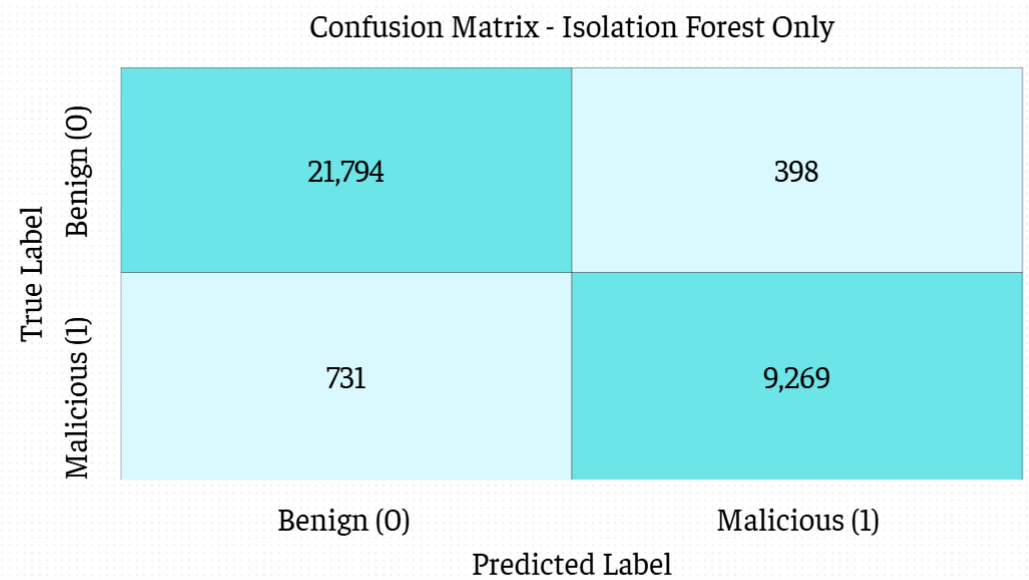
4.3.2 Classification Performance (Confusion Matrix)

a. Isolation Forest Only

Figure 4.1 illustrates the confusion matrix of the baseline Isolation Forest model. The results indicate that the model performs well in handling benign traffic, achieving **21,794 True Negatives**, while generating only **398 False Positives**, corresponding to a low false alarm rate (**FPR ≈ 1.79%**).

Nevertheless, the model exhibits a noticeable limitation in detecting malicious activities. Specifically, **731 False Negatives** are observed, indicating that a portion of attack events are misclassified as normal traffic, resulting in a **False Negative Rate (FNR)** of approximately **7.31%**. Although the model achieves a relatively high **Recall of 92.69%**, these results suggest that Isolation Forest may still overlook certain attack behaviors with subtle or low-intensity characteristics.

This behavior highlights an inherent limitation of one-class anomaly detection approaches, which are effective at identifying significant deviations but tend to struggle with low-frequency beaconing, mild probing activities, or low-volume DNS tunneling, where deviations from normal behavior are less pronounced.



Confusion Matrix - Isolation Forest Only

True Label \ Predicted Label	Benign (0)	Malicious (1)
Benign (0)	21,794	398
Malicious (1)	731	9,269

Figure 4.1 Confusion Matrix - Isolation Forest Only

Performance metric calculations for Isolation Forest:

- $\text{Precision} = \frac{TP}{TP+FP} = \frac{9.269}{9.269+398} = 0{,}9588 \approx 95{,}88\%$
- $\text{Recall} = \frac{TP}{TP+FN} = \frac{9.269}{9.269+\ 731} = 0{,}9269 \approx 92{,}69\%$
- $\text{F1} = \frac{2PR}{P+R} = \frac{2 * 0{,}9588 * 0{,}9269}{0{,}9588+0{,}9269} = 0{,}9426 \approx 94{,}26\%$
- $\text{FPR} = \frac{FP}{FP+TN} = \frac{398}{398+21.794} = 0{,}0179 \ \approx 1{,}79\%$

- FNR $= \dfrac{FN}{FN + TP} = \dfrac{731}{731 + 9.269} = 0{,}0731 \approx 7{,}31\%$

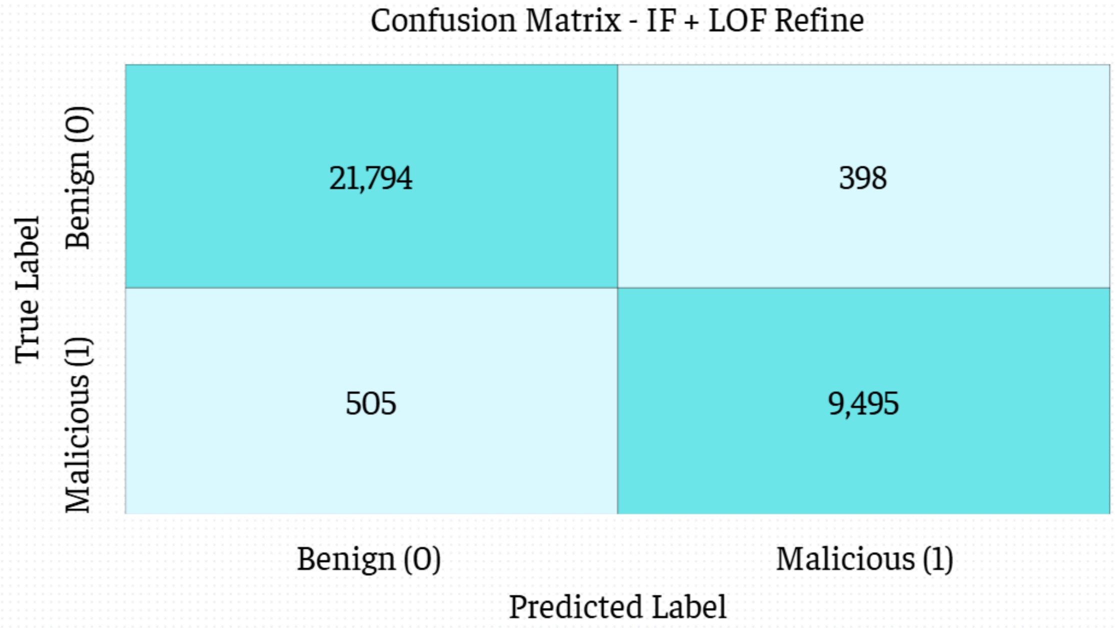
b. Isolation Forest + Local Outlier Factor Refine

Figure 4.2 presents the confusion matrix of the Isolation Forest combined with Local Outlier Factor (IF + LOF) model. Compared to the baseline configuration, the enhanced model demonstrates a clear improvement in detecting malicious activities.

Specifically, the number of **True Positives** increases to **9,495**, while **False Negatives** are reduced to **505**, resulting in a **False Negative Rate (FNR)** of approximately **5.05%**. This reduction indicates that the LOF refinement effectively enhances the model's sensitivity to subtle anomalous behaviors.

Notably, the number of **False Positives** remains unchanged at **398**, keeping the **False Positive Rate low (≈ 1.79%)**. As a result, the model achieves **Precision ≈ 95.98%**, **Recall ≈ 94.95%**, and an **F1−score ≈ 95.46%**, reflecting a well-balanced detection performance.

These results highlight the effectiveness of integrating LOF as a refinement step for Isolation Forest, particularly in identifying non-signature-based attacks such as low-frequency beaconing and low-volume DNS tunneling.



Confusion Matrix - IF + LOF Refine

True Label \ Predicted Label	Benign (0)	Malicious (1)
Benign (0)	21,794	398
Malicious (1)	505	9,495

Figure 4.2 Confusion Matrix - IF + LOF Refine

Performance metric calculations for Isolation Forest + Local Oulier Factor Refine:

- Precision $= \dfrac{TP}{TP + FP} = \dfrac{9.495}{9.495 + 398} = 0{,}9598 \approx 95{,}98\%$
- Recall $= \dfrac{TP}{TP + FN} = \dfrac{9.495}{9.495 + 505} = 0{,}9495 \approx 94{,}95\%$

- F1 = $\frac{2PR}{P+R} = \frac{2 * 0{,}9598 * 0{,}9495}{0{,}9598 + 0{,}9495} = 0{,}9546 \approx 95{,}46\%$
- FPR = $\frac{FP}{FP+TN} = \frac{398}{398 + 21.794} = 0{,}0179 \ \approx 1{,}79\%$
- FNR = $\frac{FN}{FN+TP} = \frac{505}{505 + 9.495} = 0{,}0505 \ \approx 5{,}05\%$

Summary:

Overall, the results from the confusion matrix demonstrate that adding LOF as a refinement step significantly enhances anomaly-classification accuracy. The combined model is able to identify a wider range of attack behaviors although precision decreases slightly, the reduction is negligible. Importantly, the AI model maintains stable performance on benign traffic, making it more suitable for SME environments where high sensitivity to emerging threats is essential.

4.3.3 Operational Benefits with SOAR Integration

Beyond improving the accuracy of anomaly detection, another important objective of the proposed architecture is to enhance operational efficiency during incident handling. The integration of Shuffle SOAR and LLM introduces multiple layers of automation that reduce analyst workload, standardize investigation procedures, and significantly improve the responsiveness of the overall system.

a. Automated Response and MTTR Reduction

Shuffle SOAR executes a series of automated response playbooks, including:

- Blocking malicious IP addresses
- Isolating suspicious endpoints
- Quarantining or removing malicious files
- Disabling unauthorized user accounts
- Sending incident notification emails to SOC team

With these automated workflows, MTTR is substantially reduced across the system, particularly since the baseline Wazuh configuration does not include any SOAR capabilities. Response actions no longer rely solely on manual analyst intervention or specialized expertise. This is especially beneficial for SMEs that lack a dedicated or continuously available SOC team.

Because existing literature does not provide a standardized percentage quantifying MTTR reduction achieved through SOAR, we do not specify an absolute numerical value. Nevertheless, our experimental environment clearly indicates that SOAR accelerates the incident-handling lifecycle while maintaining the practical effectiveness of the SIEM system.

b. Enhanced Incident Analysis via LLM (Qwen)

Shuffle also integrates a Large Language Model (LLM-Qwen) which acts as an analytical assistant to improve threat-hunting capabilities through:

- Natural-language interpretation of alerts
- Analysis and recommendation of defensive actions based on MITRE techniques
- Incident context summarization
- Recommendations for subsequent investigation steps

Such capabilities are absent in both Wazuh Community Edition, which rely exclusively on traditional rule-based SIEM mechanisms. The addition of LLM support strengthens analytical depth and reduces the expertise required to perform effective investigation in SME environments, though it does not reduce infrastructure resource requirements unless the LLM is hosted externally.

c. Standardization and Optimization of SOC Workflows

SOAR ensures that incident-response procedures are executed consistently and automatically according to SOC best practices. Specifically:

- Alerts are prioritized based on anomaly scores
- Alerts are enriched with metadata and contextual information
- Response steps are executed in a predefined workflow, such as:

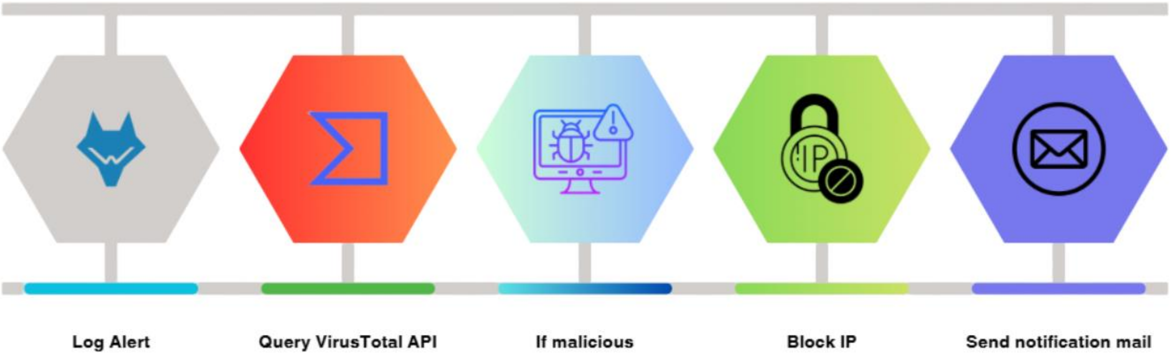


Figure 4.3 Improved Wazuh workflow.

This standardization improves operational efficiency, minimizes human error, and ensures consistent incident-response quality throughout system operation.

d. Summary

SOAR transforms the system from a traditional alert-driven SIEM into a fully automated incident-response platform. It reduces MTTR, enhances analytical depth, and enables LLM-assisted threat hunting, even in scenarios where AI does not directly improve the Recall of rule-based detections. These operational benefits demonstrate the practicality and value of combining rule-based mechanisms, anomaly-based models, and orchestration layers within SME security environments.

Table 4.4 SOAR Comparison Between Baseline Wazuh and the Improved System.

Operational Aspect	Wazuh Baseline	Improved Wazuh (Proposed System)

Response Time	Manual response, dependent on analyst experience, easily delayed	Automated playbooks
Email Alerting	Unsupported	Supported
Threat Hunting (LLM)	Community edition (free) does not support LLM	LLM-assisted investigation
Scalability	Difficult to scale due to high alert volume	High scalability thanks to automation and LLM-assisted analysis
Triage & Alert Prioritization	No prioritization high-severity alerts.	AI anomaly label, SOAR prioritizes high-severity alerts
MTTR	High, due to manual investigation and step-by-step handling	Significantly reduced MTTR through automated workflows and real-time response actions

4.3.4 System-Level Performance Metrics

a. Log Processing Throughput

Across the 27–30 days of experimentation, the system collected approximately ***14.000.000 log events***, resulting in an average throughput of:

$$\boldsymbol{EPS} = \frac{\mathit{14.000.000}\ logs}{\mathit{27} - \mathit{30}\ days} \approx \mathit{5{,}401} - \mathit{6{,}012}\ \textbf{\textit{(events/second)}}$$

The obtained EPS value is reasonable, as the entire experiment was conducted in a controlled testbed environment with a limited number of endpoints and without continuous real-world user activity. Consequently, the measured EPS reflects the workload of the experimental setup but remains considerably lower than that of many production SME environments, where log volume is typically higher and fluctuates significantly depending on working hours, system usage, and user behavior. Therefore, the reported EPS should be regarded as an indicator of the system's processing capability under controlled conditions, rather than a representation of the full operational spectrum of SMEs.

Nonetheless, the results provide several important confirmations:

- The log collection architecture processed the entire dataset without bottlenecks.

- The anomaly-scoring pipeline operated smoothly without introducing noticeable latency.

- The SOAR workflows remained stable even during simulated attack phases.

To compensate for the lack of continuous user activity during dataset collection, we additionally conducted a series of stress tests with gradually increasing durations from 5 to 30 minutes to evaluate the system's load tolerance. The results show an average throughput of approximately ***3.500 - 3.800 EPS***, with a slight increase across iterations, a common warm-up effect in ingestion pipelines as internal buffers and processing components reach optimal operating states. Importantly, no log loss, queue saturation, or performance degradation was observed, indicating that the system remains stable even under elevated load.

Although this EPS level is not intended to generalize to all SMEs, the achieved throughput demonstrates processing capabilities consistent with the workloads commonly found in many small and medium-sized enterprises with typical infrastructure sizes (from a few dozen to roughly one hundred endpoints). Based on the measured throughput and characteristic EPS ranges for different endpoint types, the system is estimated to support approximately 150 - 200 endpoints under similar configurations. This estimate serves as a technical reference rather than an absolute upper bound, yet it effectively illustrates the scalability and practical applicability of the proposed architecture within the scope of this study.

Overall, the throughput and stress-test results show that the system remains stable under both experimental and elevated loads while preserving a lightweight and cost-efficient architecture, key characteristics for successful deployment in SME environments.

b. CPU usage

- The SIEM operated on: **2 CPUs** and **8 GB RAM.**
- The SOAR on **2 CPUs** and **8 GB RAM**.
- The AI module on **2 CPUs** and **6 GB RAM**.

c. Memory usage

- The SIEM required approximately **100 GB** of storage.
- The SOAR used around **40 GB** of storage.

4.3.5 Operational and Economic Metrics

To evaluate operational practicality, we compare the baseline Wazuh deployment with the improved architecture (Wazuh + AI + SOAR + LLM). This assessment considers workforce, complexity, and cost implications. Since the proposed system relies exclusively on open-source components, no licensing fees are introduced.

Table 4.5 Comparison of Cost and Workforce Requirements

Cost/Workforce Category	Baseline Wazuh	Improved Wazuh (Proposed System)	Reduction
License & Subscription	$0 (open-source)	$0 (open-source)	No change (0%)
Deploy System Cost	571$ - 923$ - 1467$ / month	650$ - 1030$ - 1550$ / month	Trade-off with main workflow
Workforce Load	High, manual triage and manual incident response	SOAR (Shuffle) response	Significant reduction in human workload
High-skill Analyst	Requires senior SOC	Many tasks automated,	Reduced skill

Requirement	analysts to triage & respond manually	LLM assists junior analysts	dependency
Incident Handling Cost	Higher, due to longer MTTR and manual steps	Lower, playbooks reduce incident dwell time	Reduced cost per incident
MTTR (Qualitative)	High, sequential manual handling	Substantially reduced, automated workflows	Faster containment
Time per Investigation	Long, analysts must read raw logs	Shortened, LLM summarizes, explains anomalies	Reduced analysis time
Scalability	Limited by human capacity	Scales better with automation & LLM support	Improved scalability
Total Cost of Ownership (TCO)	Higher (workforce-driven)	Lower (automation-driven)	Overall TCO reduction

The improvements reveal that the proposed system does not aim to reduce monetary licensing costs since Wazuh is already free, but instead targets workforce cost, operational efficiency, and analyst time, which are the largest expenses for SMEs.

- Automation reduces analyst hours, decreasing operational cost
- LLM reduces the skill barrier, lowering training and hiring requirements
- Noise reduction and prioritization reduce analyst fatigue
- Lower MTTR reduces financial impact of incidents
- Overall TCO decreases despite a slight increase in compute usage

These benefits demonstrate that the proposed system is not only technically effective, but economically suitable for SMEs with limited cybersecurity budgets.

4.4 Interpretation of Results

The experimental results demonstrate that the proposed AI integrated SIEM SOAR architecture yields clear improvements in both detection quality and operational efficiency. This architecture is particularly suitable for the limited conditions of SMEs.

Firstly the Isolation Forest IF and Local Outlier Factor LOF models primarily improve Recall for anomalous attacks. These include DNS Tunneling and Beaconing where signature based detection does not fully cover the behavior. For rule based attacks AI does not directly enhance Recall but still contributes to reducing the operational False Positive Rate FPR and mitigating noise. It achieves this through alert prioritization and anomaly scoring.

SOAR plays a critical layer in the architecture due to its ability to automate responses to eliminate manual operations and to standardize SOC processes. This enables the system to react faster and reduces reliance on highly skilled SOC personnel. Concurrently this automation has significantly reduced the Mean Time to Respond MTTR. It has also helped ease the burden on analysts by decreasing the number of alerts requiring manual handling.

Furthermore the integration of a Large Language Model LLM within the workflow enhances the quality of investigation. The LLM provides alert explanations and suggests next steps follow the MITRE guildline thereby greatly reducing the analytical load.

Overall these results prove that the combined architecture of rule based anomaly based detection and SOAR is not only technically effective but also cost appropriate and easy to deploy. It is especially suitable for SMEs a group typically lacking the resources dedicated SOC staff and budget to operate large scale commercial SIEM systems.

4.5 Comparison with Literature

4.5.1. Alignment with Existing Literature & Modern Requirements

Previous studies have extensively shown that anomaly detection models, such as Isolation Forest and Local Outlier Factor, are highly effective in identifying non-linear and unpredictable behaviors, particularly in the context of low-and-slow attacks or anomalous DNS patterns. Our findings are entirely consistent with this established literature, as the combined IF + LOF models exhibited superior capability in DNS Tunneling and Beaconing scenarios.

Concurrently, modern industry documentation and Security Operations Center (SOC) reports emphasize that traditional rule-based SIEM systems reveal significant limitations when confronting novel attack variations and complex network traffic. This aligns precisely with our experimental results: while rule-based detection remains essential, its lack of adaptability necessitates the integration of anomaly detection as an undeniable evolution in the field.

Furthermore, current SOC standards prioritize SOAR as a mandatory component for reducing the Mean Time to Respond (MTTR) and standardizing incident response workflows. Our system exhibits behavior that is fully compatible with these recommendations, showcasing SOAR's pivotal role in automation and incident orchestration.

4.5.2. Improvements Over Previous Studies

Unlike the majority of existing research, which focuses narrowly on detection accuracy on standardized datasets such as CIC-Bell-DNS-EXF-2021 or CTU-13, our study significantly extends its scope to the operational aspect, a factor largely neglected by prior works. Specifically:

- We evaluate a comprehensive set of operational metrics including noise and FPR reduction, triage efficiency, and MTTR. These are key performance indicators that directly impact the practical viability of a SIEM/SOAR system within an enterprise environment.

- While SIEM with ML research predominantly concentrates on data modeling, our study innovatively integrates SOAR and LLM components that are almost entirely absent in current open-source security systems.

- Most previous studies do not address the operational feasibility for SMEs. Conversely, our system was constructed and rigorously evaluated in a simulated real-world SME environment, characterized by low log ingestion volume, limited personnel, and modest infrastructure.

- We propose a novel multi-layered architecture (Rule-based + Anomaly-based + SOAR + LLM), whereas prevailing research typically focuses on optimizing a single component.

In summary, our system not only validates the results established by prior research but also broadens the scope, incorporating robust operational mechanisms and practical application that demonstrate its real-world applicability and cost-effectiveness.

4.5.3. Impact and Contribution to the Research Landscape

The findings of this study provide three significant contributions to the fields of SIEM/SOAR and Machine Learning in cybersecurity:

- **Practical Contribution:** We introduce a complete, efficient, and low-cost SIEM/SOAR and AI-Integrated architecture tailored specifically for the Small and Medium-sized Enterprise (SME) segment. This segment is often underserved in both academic research and the commercial market, providing a highly viable solution where resource constraints are paramount.

- **Methodological Contribution:** This research demonstrates that operational efficiency (including reduced Mean Time to Respond (MTTR), decreased alert volume, alert prioritization, and LLM-assisted analyst support) is as critical as, if not more important than, pure detection accuracy. This represents a crucial dimension that the majority of prior academic works have largely overlooked.

- **Academic Contribution:** The integration of a Large Language Model (LLM) into the incident investigation workflow opens a renewed, cutting-edge research avenue, particularly within open-source security systems. To our knowledge, no existing work has comprehensively combined SIEM + ML Anomaly Detection + SOAR + LLM in a single framework like this study.

Overall, driven by these factors, the proposed architecture not only reinforces established arguments found in the specialized literature but also serves as a forward-looking experiment. It thus contributes significantly to broadening the research scope on SOC automation and AI-assisted incident response.

4.6 Implications of the Results

The experimental results provide several important implications regarding the technical effectiveness, operational value, and economic feasibility of the proposed AI-integrated SIEM/SOAR system for small and medium-sized enterprises (SMEs).

First, the introduction of a new workflow designed to reduce the False Positive Rate (FPR) demonstrates that combining rule-based detection in Wazuh with the unsupervised learning models Isolation Forest and Local Outlier Factor can effectively address one of the most critical limitations of traditional SIEM systems, namely alert fatigue. A reduction in FPR leads directly to a decrease in the volume of manual alert triage, thereby lowering the risk of analyst overload and improving the overall reliability of the detection pipeline. This capability is especially valuable for SMEs, where security resources are typically limited.

Furthermore, the consistent improvement in Recall, Precision, and F1-score indicates that the system becomes more sensitive to malicious behaviors without being influenced by background noise. This demonstrates that integrating AI with rule-based detection is not only feasible but also enhances the overall detection quality. In the context of rapid AI advancements during 2024 - 2025, integrating AI into the SIEM infrastructure of SMEs has become highly realistic and serves as an additional defensive layer capable of identifying emerging or previously unseen attacks.

In addition, the integration of SOAR through the Shuffle platform, combined with the Qwen language model, significantly reduces Mean Time to Respond (MTTR). This finding confirms that automation can effectively narrow the gap between detection and response, which has long been a challenge for smaller organizations. Automated actions, synchronized playbooks, and cross-system orchestration allow SMEs to achieve response speeds approaching those of professional security operations centers, even in the absence of a continuously staffed team.

From a performance perspective, the system maintains stable event-processing throughput (EPS) and resource utilization even with the addition of AI and SOAR components. Although there is a modest increase in hardware requirements to ensure smooth operation of the AI module, this increase is offset by the reduction in storage overhead resulting from fewer false alerts. This outcome supports the feasibility of deploying the system on the existing commodity infrastructure typically available in SMEs without causing performance degradation.

From an economic standpoint, the combined improvements in FPR, Recall, and MTTR contribute to optimizing the total cost of ownership (TCO). A reduction in false positives lowers the workload placed on staff. Faster response times help minimize potential damage from attacks. Automation eliminates repetitive manual tasks, improving overall operational efficiency. Collectively, these advantages render the solution capable of delivering enterprise-level security outcomes while remaining financially suitable for SMEs.

Overall, the results confirm that the proposed AI-integrated SIEM/SOAR system is not only technically effective but also operationally and economically appropriate for SMEs. The system helps narrow the security resource gap between smaller companies and larger organizations equipped with professional security operations centers.

CHAPTER 5
DISCUSSION

5.1 Restate the Research Problem or Objectives

Small and medium-sized enterprises (SMEs) increasingly face significant cybersecurity challenges as modern attacks become more frequent and sophisticated, while their available financial and human resources remain limited. Traditional SIEM systems rely primarily on static rule-based detection, which tends to generate a large number of false positives and requires continuous manual triage. This results in operational inefficiencies, analyst overload, and reduced reliability in identifying true security incidents. Additionally, commercial SOAR platforms are often cost-prohibitive for SMEs, preventing them from implementing automated response workflows that could substantially reduce incident handling time.

This research was conducted to address these limitations by proposing and evaluating an integrated SIEM/SOAR framework enhanced with unsupervised machine learning and open-source automation. The primary objectives were to reduce the False Positive Rate through AI-driven anomaly detection, improve detection quality by combining rule-based and behavioral analysis, and decrease Mean Time to Respond through automated playbooks. The study also aimed to assess the operational feasibility and economic suitability of such a system when deployed in typical SME environments.

5.2 Summarize Key Findings

The experimental evaluation process clarified several important findings, thereby confirming the effectiveness of the proposed AI-integrated SIEM/SOAR system.

Firstly, the combination of unsupervised learning models with rule-based detection mechanisms significantly reduced the False Positive Rate (FPR). This created a more reliable alerting pipeline and substantially mitigated the manual processing workload for operational personnel.

Secondly, the system achieved higher Recall, Precision, and F1 scores across the majority of attack scenarios. This indicates that the AI module not only enhances the ability to identify true threats but also maintains stability against noise within the logging environment. These results simultaneously validate the value of integrating rule-based detection with methods for anomalous behavior analysis.

Furthermore, the integration of SOAR automation capabilities coupled with the assistance of a Large Language Model (LLM) led to a significant reduction in the Mean Time to Respond (MTTR). Automated playbooks and the coordinated capabilities among multiple system components distinctly improved the speed and consistency of the entire incident handling process, thereby addressing a critical operational limitation often encountered by SMEs.

Finally, the overall system performance, including the stability of the Events Per Second (EPS) processing rate, remained consistent throughout the testing environment. Although resource utilization increased due to the addition of the AI and SOAR components, this increase was not overly substantial and was offset by the ability to optimize the volume of logs requiring storage for analysis. This demonstrates that the system architecture is entirely feasible for deployment on common SME infrastructure without demanding specialized hardware.

5.3 Discussion in Broader Context

The findings of this research contribute meaningful insight when placed within the broader academic and industrial context. Prior studies have repeatedly emphasized the weaknesses of free or rule based SIEM systems, particularly their inability to adapt to evolving attack patterns and their tendency to produce overwhelming numbers of false positives. While several works have explored the use of anomaly detection models such as Isolation Forest and Local Outlier Factor, they often evaluated these techniques in isolated experimental settings without embedding them into a functional SIEM and SOAR ecosystem. The present study advances the field by demonstrating how these models can be integrated into a real operational pipeline and how their combined strengths enhance detection performance more effectively than using either approach individually.

The results also reinforce a broader trend in the cybersecurity research community that highlights the growing importance of behavioral analysis as a complement to classical signature based methods. Through the combined use of artificial intelligence and traditional rule based detection, the system demonstrates a more comprehensive ability to cover a wide spectrum of attack types. This aligns with modern SOC practices, in which layered detection mechanisms are increasingly considered essential for defending against subtle or previously unseen threats. The experiment confirms that artificial intelligence does not replace signature based detection but rather enhances it, and that this synergy is particularly beneficial in environments where resources and staffing are limited.

Beyond detection accuracy, the integration of automation and large language model assistance reflects a shift in how smaller organizations can approach security operations. Automation has historically been associated with enterprise scale SOCs, yet the findings show that substantial operational improvements can be achieved even with open source and lightweight SOAR tools. This carries practical significance because it suggests that SMEs, which traditionally lack mature security teams, can still adopt advanced operational workflows that were once considered accessible only to large organizations.

Finally, the study illustrates that useful artificial intelligence enabled security enhancements do not necessarily require extensive computational infrastructure. The system's stable EPS processing rate, along with its ability to maintain effectiveness under typical SME resource constraints, demonstrates that meaningful improvements in detection and response can be achieved without enterprise grade hardware. This contributes to an increasingly important discussion on how to democratize security technologies so that smaller organizations can better defend themselves against modern threats.

5.4 Limitations of the Study

Although the proposed AI-enhanced SIEM/SOAR framework demonstrates encouraging results, several limitations should be acknowledged to ensure a balanced evaluation. These limitations also provide direction for future development.

First, the dataset was collected entirely within a laboratory environment. Even though multiple attacks were simulated, the traffic did not fully reflect the diversity, noise, and irregular behavior of real enterprise networks. As a result, the detection performance observed in this study may not generalize perfectly to production deployments.

Second, the artificial intelligence component was limited to two unsupervised learning algorithms, Isolation Forest and Local Outlier Factor. While these models are effective for rare-event and anomaly detection, they do not capture complex temporal correlations or multi-stage attack sequences. The study did not explore hyperparameter optimization or compare performance with more advanced methods such as recurrent models or deep autoencoders, which could potentially yield richer behavioral insights.

Third, the SOAR implementation used an open-source platform with only essential automation features. Without advanced orchestration, large-scale incident correlation, or integrated threat intelligence, the playbooks were restricted to a small set of controlled scenarios and may require refinement for real SOC operations.

Fourth, the experiments were executed on modest virtual machines representing the hardware constraints of typical SMEs. While this supports the feasibility of deployment in resource-limited environments, the system was not stress-tested under high-throughput conditions such as event rates exceeding several thousand EPS. It also did not evaluate performance in distributed sensor deployments. Therefore, the scalability and long-term stability of the AI and SOAR components under heavier operational loads remain unverified.

Finally, the economic evaluation focused primarily on observable operational gains such as reduced false positives and shortened response time. A complete cost analysis was not performed, and factors such as long-term maintenance, integration overhead, staff training requirements, and potential hidden costs were not included. This limits the completeness of the cost-effectiveness assessment, especially for SMEs with diverse financial constraints.

In summary, these limitations do not diminish the contributions of the study but highlight areas where expanded datasets, advanced modeling approaches, real-world validation, and broader economic analysis would strengthen the robustness and applicability of the proposed framework.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 Conclusion

This study demonstrates that meaningful advancements in cybersecurity are achievable even within the financial and operational constraints of small and medium-sized enterprises. By integrating unsupervised machine learning with an open-source SIEM and a lightweight SOAR platform, the research shows that high-quality detection and automated response capabilities once reserved for large and well-funded organizations can now be delivered using accessible and cost-efficient technologies. The resulting system not only improves detection accuracy but also elevates the entire security workflow toward a more proactive, behavior-driven, and automation-assisted model.

Beyond its technical achievements, the project offers two significant contributions. From a practical standpoint, it provides SMEs with a clear path to reduce alert fatigue, enhance their ability to recognize modern attack patterns, and respond to incidents with greater consistency all without requiring enterprise-grade infrastructure or a large SOC team. From an academic perspective, the results strengthen the evidence that unsupervised anomaly detection can effectively complement traditional signature-based methods, and that open-source SOAR platforms, when integrated strategically, can deliver real and measurable operational value.

Ultimately, this work illustrates a broader and more compelling message: advanced cybersecurity does not have to be exclusive. With thoughtful system design and the strategic use of artificial intelligence, even small organizations can close the capability gap between themselves and large enterprises. The proposed framework marks a step toward democratizing security technology and shows that accessible, low-cost, and open-source solutions can play a transformative role in protecting SMEs against the evolving threat landscape.

6.2 Future Work

Although the proposed system demonstrates strong potential, several ambitious directions can significantly extend its capabilities and position it as a next-generation security platform for SMEs and beyond. A major future direction is the development of advanced AI architectures that move beyond traditional anomaly detection. This includes exploring deep neural networks, graph-based threat detection, transformer-driven models capable of understanding long-term temporal dependencies, and adaptive learning pipelines that continuously retrain themselves from live traffic. Such advancements could allow the system to detect multi-stage, stealthy, or previously unseen attacks at a level comparable to enterprise-grade security solutions.

Another important direction is expanding the SOAR component into a fully autonomous security layer. This can include the ability to dynamically generate response playbooks using large language models, autonomous decision-making engines that select optimal remediation paths, and cross-environment orchestration that spans cloud, on-premise, and hybrid infrastructures. Ultimately, this would push the system toward a self-defending architecture, reducing human involvement to high-level validation rather than routine incident handling.

Future work should also evaluate the system on large-scale and highly diverse datasets collected from real production networks across different industries. Stress-testing the AI and SOAR modules under extreme EPS conditions, distributed deployments, and long-running operational environments would provide insight into their scalability and reliability. Such evaluations would be essential if the system is to evolve into a deployable solution for organizations with tens of thousands of daily events.

Economic analysis could also be broadened by constructing a predictive cost-benefit model that incorporates not only operational savings but also potential risk reduction, avoided breach costs, and long-term return on investment. This would offer SMEs a clearer path toward adopting AI-driven security systems and quantifying their strategic impact.

Ultimately, future work should aim higher: transforming the proposed architecture into a fully adaptive, intelligent, and autonomous security ecosystem capable of learning from its environment, scaling to enterprise workloads, and minimizing human intervention. Achieving these goals would move the system beyond a practical SME-friendly solution and toward a blueprint for the next era of AI-driven cybersecurity platforms.

REFERENCES

[1] Wasyihun Sema Admass a , Yirga Yayeh Munaye b , and Abebe Abeshu Diro c, "Cyber security: State of the art, challenges and future directions" Volume 2, 2024.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S2772918423000188

[2] Ş. C. Gherghina, M. A. Botezatu, A. Hosszu, and L. N. Simionescu, "Small and Medium-Sized Enterprises (SMEs): The Engine of Economic Growth through Investments and Innovation," *Sustainability*, vol. 12, no. 1, p. 347, 2020.
[Online] Available: https://www.mdpi.com/2071-1050/12/1/347

[3] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PLOS ONE*, vol. 19, no. 3, p. e0301183, 2024.
[Online] Available:
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0301183

[4] N. Mohamed, "Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms," Knowl. Inf. Syst., 2025.
[Online] Available: https://link.springer.com/article/10.1007/s10115-025-02429-y

[5] G. Ali, S. Shah, and M. ELAffendi, "Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection," Results Eng., vol. 25, p. 104078, Mar. 2025.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S2590123025001665

[6] A. R. Muhammad, P. Sukarno, and A. A. Wardana, "Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning," *Procedia Comput. Sci.*, vol. 217, pp. 1406–1415, 2022.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S1877050922024243

[7] R. A. Bridges et al., "Testing SOAR tools in use," Comput. Secur., vol. 129, p. 103201, Jun. 2023.
[Online] Available:
https://www.sciencedirect.com/science/article/abs/pii/S0167404823001116

[8] M. Curtin, B. Sheehan, M. Gruben, G. O'Carroll, and H. Murray, "Enhancing Cybersecurity Awareness in Small and Medium Enterprises Through a User-Friendly Risk Assessment Tool," *2025 IEEE 10th European Symposium on Computer and Communications Security*, 2025.
[Online] Available: https://ieeexplore.ieee.org/document/11129403
[9] A. Chidukwani, S. Zander, and P. Koutsakis, "Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications," Comput. Secur., vol. 145, p. 104026, Oct. 2024.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S0167404824003316

[10] I. Ismail, R. Kurnia, Z. A. Brata, G. A. Nelistiani, S. Heo, and H. Kim, "Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence," *Information*, vol. 16, no. 5, p. 365, 2025.
[Online] Available: https://www.mdpi.com/2078-2489/16/5/365

[11] S. A. Alansary *et al.*, "Emerging AI threats in cybercrime: a review of zero-day attacks via machine, deep, and federated learning," Knowl. Inf. Syst., 2025.
[Online] Available: https://link.springer.com/article/10.1007/s10115-025-02556-6

[12] Wazuh Inc., "Wazuh Documentation Index (Current Version)," 2025.
[Online]. Available: https://documentation.wazuh.com/current/index.html

[13] Z. Halim *et al.*, "An effective genetic algorithm-based feature selection method for intrusion detection systems," *Comput. Secur.,* vol. 110, p. 102448, Nov. 2021
[Online] Available:
https://www.sciencedirect.com/science/article/abs/pii/S0167404821002728

[14] E. F. Agyemang, "Anomaly detection using unsupervised machine learning algorithms: A simulation study," *Sci. Afr.,* vol. 26, p. e02386, Dec. 2024.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S2468227624003284

[15] O. Alghushairy *et al.*, "A Review of Local Outlier Factor Algorithms for Outlier Detection in Big Data Streams," *Big Data Cogn. Comput.,* vol. 5, no. 1, p. 1, Dec. 2020.
[Online] Available: https://www.mdpi.com/2504-2289/5/1/1

[16] A. Techaviseschai *et al.*, "A Real-Time Semi-Supervised Log Anomaly Detection Framework for ALICE O2 Facilities," *Appl. Sci.,* vol. 15, no. 11, p. 5901, May 2025.
[Online] Available: https://www.mdpi.com/2076-3417/15/11/5901

[17] Wazuh, "White Paper: How Wazuh delivers enterprise-level security for free," 2024.
[Online] Available: https://wazuh.com/resources/white-paper/

[18] Wazuh, "Architecture Overview," 2024.
[Online] Available: https://documentation.wazuh.com/current/getting-started/architecture.html

[19] Y. Cao *et al.*, "Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges," *Mach. Intell. Res.*, vol. 21, no. 2, pp. 294–317, 2024.
[Online] Available: https://link.springer.com/content/pdf/10.1007/s11633-023-1456-2.pdf

[20] S. Waelchli and Y. Walter, "Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study," Comput. Secur., vol. 148, p. 104137, Jan. 2025.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S0167404824004425

[21] M. Kibalna, "Microsoft Sentinel: Pricing and Key Features in 2025," UnderDefense Cybersecurity, Feb. 2025.
[Online] Available: https://underdefense.com/industry-pricings/microsoft-sentinel-pricing/

[22] Splunk LLC, "Pricing | Splunk," 2025.
[Online] Available: https://www.splunk.com/en_us/resources/splunk-pricing-options.html

[23] R. Whiting, ".conf24: Splunk Introduces Advanced AI Enhancements for Observability, Security and IT Service Intelligence," CRN, Jun. 2024.
[Online] Available: https://www.splunk.com/en_us/newsroom/press-releases/2024/conf24-splunk-introduces-advanced-ai-enhancements-for-observability-security-and-it-service-intelligence.html

[24] Rapid7, “Rapid7 Product Pricing,” 2025.
[Online] Available: https://www.rapid7.com/pricing/

[25] Rapid7, “Incident Command: AI Powered Next-Gen SIEM | Rapid7,” 2025.
[Online] Available: https://www.rapid7.com/products/siem/

[26] Google Cloud, “Google Security Operations | Google Cloud,” 2025.
[Online] Available: https://cloud.google.com/security/products/security-operations

[27] SEP2 LIMITED, “Google Chronicle SecOps - Digital Marketplace,” 2025.
[Online] Available: https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/886272716164548

[28] Google Cloud, "AI for Security Overview," 2025.
[Online] Available: https://cloud.google.com/security/ai

[29] Securonix, “Introducing Simplified Security: Securonix Unveils New Pricing and Tiered Packaging,” *Securonix Blog, 2025.*
[Online] Available: https://www.securonix.com/blog/introducing-simplified-security-securonix-unveils-new-pricing-and-tiered-packaging/

[30] Securonix, "Why I Joined Securonix," 2025.
[Online] Available: https://www.securonix.com/blog/why-i-joined-securonix/

[31] Graylog, "Pricing Plans Overview," 2024.
[Online] Available: https://graylog.org/pricing/

[32] Graylog, "Anomaly Detection Capabilities," 2024.
[Online] Available: https://graylog.org/feature/anomaly-detection/

[33] Graylog Docs, "Investigations in Graylog," 2024.
[Online] Available:
https://go2docs.graylog.org/current/what_more_can_graylog_do_for_me/investigations.htm

[34] Elastic, “Elastic Cloud Hosted pricing,” *Elastic,* 2025.
[Online] Available: https://www.elastic.co/pricing/cloud-hosted

[35] Elastic, “AI-driven SIEM that is open source and affordable” *Elastic,* 2025.
[Online] Available: https://www.elastic.co/security/siem

[36] A. P. Vazão, L. Santos, R. L. C. Costa, and C. Rabadão, “Implementing and evaluating a GDPR-compliant open-source SIEM solution,” *J. Inf. Secur. Appl.*, vol. 75, 103509, Jun. 2023.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S2214212623000935

[37] TrustRadius, "Wazuh Pricing Information," 2024.
[Online] Available: https://www.trustradius.com/products/wazuh/pricing

[38] Wazuh, "Leveraging Artificial Intelligence for Threat Hunting in Wazuh," 2024.
[Online] Available: https://wazuh.com/blog/leveraging-artificial-intelligence-for-threat-hunting-in-wazuh/

[39] G. R. Andreica, I. A. Ivanciu, D. Zinca, and V. Dobrota, “Integration of the Suricata Intrusion Detection System and of the Wazuh Security Information and Event Management for

Real-Time Denial-Of-Service and Data Tampering Detection and Alerting,” *ACTA TECHNICA NAPOCENSIS Electronics and Telecommunications*, vol. 64, no. 2, pp. 1–8, 2024.
[Online] Available: https://users.utcluj.ro/~atn/papers/ATN_2_2024_1.pdf

[40] Elastic, “Filebeat: Lightweight shipper for logs,” Elastic, 2025.
[Online] Available: https://www.elastic.co/beats/filebeat

[41] L. Galka and P. Karczmarek, “Minimal spanning tree-based isolation forest with anomaly score function built on the basis of fuzzy rules,” *Appl. Soft Comput.*, vol. 148, 110935, Nov. 2023.
[Online] Available:
https://www.sciencedirect.com/science/article/abs/pii/S1568494623009535

[42] M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, “LOF: Identifying Density-Based Local Outliers,” in *Proc. 2000 ACM SIGMOD Int. Conf. on Management of Data (SIGMOD '00)*, Dallas, TX, USA, 2000
[Online] Available: https://dl.acm.org/doi/pdf/10.1145/335191.335388

[43] S. Raschka, J. Patterson, and C. Nolet, “Machine Learning in Python: Main Developments and Technology Trends in Data Science, Machine Learning, and Artificial Intelligence,” *Information*, vol. 11, no. 4, 193, Apr. 2020
[Online] Available: https://www.mdpi.com/2078-2489/11/4/193

[44] Stratosphere IPS, "CTU-13 Malware Dataset," 2024.
[Online] Available: https://www.stratosphereips.org/datasets-ctu13

[45] S. Mahdavifar *et al.*, “CIC-Bell-DNS-EXF-2021 dataset,” Canadian Institute for Cybersecurity, Univ. of New Brunswick, Fredericton, NB, Canada, 2021.
[Online] Available: https://www.unb.ca/cic/datasets/dns-exf-2021.html

[46] A. Brooks, "Deep Dive into Wazuh: The Heartbeat of Security Onions," June. 2024.
[Online] Available: https://helmsmaninfosec.com/blog/deep-dive-into-wazuh-the-heartbeat-of-security-onions-host-based-intrusion-detection/

[47] Wazuh Inc., “OpenSearch integration,” *Wazuh documentation*, version 4.14.
[Online] Available: https://documentation.wazuh.com/current/integrations-guide/opensearch/index.html

[48] M. Markatou, J. L. Horowitz, and R. V. Lenth, “Robust scale estimation based on the the empirical characteristic function,” *Stat. Probab. Lett.*, vol. 25, no. 2, pp. 185-192, Nov. 1995.
[Online] Available: https://www.sciencedirect.com/science/article/pii/016771529400221S

[49] Á. Michelena *et al.*, “Comparative analysis of unsupervised anomaly detection techniques for heat detection in dairy cattle,” *Neurocomputing*, vol. 618, Art. no. 129088, Feb. 2025.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S0925231224018599

[50] C. R. Junior, I. Becker, and S. Johnson, “Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity,” *arXiv e-print,* arXiv:2309.17186, 2023.
[Online] Available: https://arxiv.org/pdf/2309.17186

[51] R. Raouf, A. K. Jumaa, and A. F. Fadhil, “Real Time Intrusion Detection System Based on Web Log File Analysis,” *Kurdistan J. Appl. Res.*, vol. 10, no. 1, pp. 35–49, Feb. 2025.

[Online] Available:
https://www.researchgate.net/publication/389699158_Real_Time_Intrusion_Detection_System_Based_on_Web_Log_File_Analysis

[52] Wazuh, Inc., "Proof of Concept guide: Detecting a brute-force attack," *Wazuh Documentation, v4.14.*
[Online] Available: https://documentation.wazuh.com/current/proof-of-concept-guide/detect-brute-force-attack.html

[53] M. Sheeraz *et al.*, "Revolutionizing SIEM Security: An Innovative Correlation Engine Design for Multi-Layered Attack Detection," *Sensors*, vol. 24, no. 15, Art. no. 4901, Jul. 2024.
[Online] Available: https://www.mdpi.com/1424-8220/24/15/4901

[54] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "A systematic method for measuring the performance of a cyber security operations centre analyst," *Computers & Security*, vol. 124, p. 102959, Jan. 2023. doi: 10.1016/j.cose.2022.102959.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S0167404822003510

[55] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in *International Conference on Information Systems Security and Privacy,* 2018.
[Online] Available: https://www.semanticscholar.org/paper/Toward-Generating-a-New-Intrusion-Detection-Dataset-Sharafaldin-Lashkari/a27089efabc5f4abd5ddf2be2a409bff41f31199

[56] Y. Zhang and Z. Wang, "Feature Engineering and Model Optimization Based Classification Method for Network Intrusion Detection," *Appl. Sci. 2023,* vol. 13, no. 16, Art. no. 9363, Aug. 2023.
[Online] Available: https://www.mdpi.com/2076-3417/13/16/9363

[57] R. Magán-Carrión *et al.*, "Towards a Reliable Comparison and Evaluation of Network Intrusion Detection Systems Based on Machine Learning Approaches," *Appl. Sci. 2020,* vol. 10, no. 5, Art. no. 1775.
[Online] Available: https://www.mdpi.com/2076-3417/10/5/1775

[58] J. Hussain and S. Lalmuanawma, "Feature Analysis, Evaluation and Comparisons of Classification Algorithms Based on Noisy Intrusion Dataset," *Procedia Comput. Sci.,* vol. 92, pp. 188–198, 2016.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S1877050916315927

[59] M. A. Talib *et al.*, "APT beaconing detection: A systematic review," *Comput. Secur.,* vol. 122, Art. no. 102875, Nov. 2022.
[Online] Available:
https://www.sciencedirect.com/science/article/abs/pii/S0167404822002693

[60] R. Kovar and D. Gunter, "Traditional and Advanced Techniques for Network Beaconing Detection," Software Engineering Institute (SEI), Carnegie Mellon University, Technical Report, 2022.
[Online] Available: https://www.sei.cmu.edu/documents/60/2022_500_001_875351.pdf

[61] S. Adibi, "Traffic Classification - Packet-, Flow-, and Application-based Approaches," Int. J. Adv. Comput. Sci. Appl. (IJACSA), vol. 1, no. 1, 2010, pp. 6–12.

[Online] Available:
https://pdfs.semanticscholar.org/92dd/c0a1792567a26d70e1f17cec94c773656b0c.pdf

[62] E. Garsva, N. Paulauskas, G. Grazulevicius, and L. Gulbinovic, “Packet Inter-arrival Time Distribution in Academic Computer Network,” *Elektronika Ir Elektrotechnika,* vol. 20, no. 3, pp. 87–90, 2014.
[Online] Available:
https://pdfs.semanticscholar.org/d9ea/27c072b0c28df6e993bede0d9e2f1e85668e.pdf

[63] M. Chater, A. Borgi, M. T. Slama, K. S. Gandoura, and M. I. Landoulsi, “Fuzzy Isolation Forest for Anomaly Detection,” *Procedia Comput. Sci.,* vol. 207, pp. 916–925, 2022, doi: 10.1016/j.procs.2022.09.147.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S1877050922010298

[64] R. C. Ripan, I. H. Sarker, M. M. Anwar, M. H. Furhad, F. Rahat, M. M. Hoque and M. Sarfraz, “An Isolation Forest Learning Based Outlier Detection Approach for Effectively Classifying Cyber Anomalies,” *arXiv e-print,* Art. no. arXiv:2101.03141, Dec. 9, 2020.
[Online] Available: https://arxiv.org/pdf/2101.03141

[65] L. Bai, J. Wang and Y. Zhou, “Outlier Detection and Explanation Method Based on FOLOF Algorithm,” *Entropy 2025,* vol. 27, no. 6, Art. no. 582, May 2025.
[Online]. Available: https://www.mdpi.com/1099-4300/27/6/582

[66] S. Sorbo and M. Ruocco, “Navigating the metric maze: a taxonomy of evaluation metrics for anomaly detection in time series,” *Data Min. Knowl. Discov.,* vol. 38, pp. 1027–1068, Nov. 2023.
[Online] Available: https://link.springer.com/article/10.1007/s10618-023-00988-8

[67] M. Jedliński and M. Sowa, “The Impact of Using the Total Cost of Ownership (TCO) Account for a Reusable Wooden Flat Pallet in Its Operational Phase on Respecting the Principles of Sustainable Development,” *Resources 2021,* vol. 10, no. 11, Art. no. 116, Nov. 2021, doi: 10.3390/resources10110116.
[Online] Available: https://www.mdpi.com/2079-9276/10/11/116

[68] G.-Y. Kim, S.-M. Lim and I.-C. Euom, “A Study on Performance Metrics for Anomaly Detection Based on Industrial Control System Operation Data,” *Electronics 2022,* vol. 11, no. 8, Art. no. 1213, Apr. 2022, doi: 10.3390/electronics11081213.
[Online] Available: https://www.mdpi.com/2079-9292/11/8/1213

[69] J. Demšar, “Statistical Comparisons of Classifiers over Multiple Data Sets,” *J. Mach. Learn. Res.,* vol. 7, pp. 1–30, Jan. 2006.
[Online] Available: https://www.jmlr.org/papers/volume7/demsar06a/demsar06a.pdf

[70] G. Giray and E. Tüzün, “A Systematic Mapping Study on the Current Status of Total Cost of Ownership for Information Systems,” *Bilişim Teknolojileri Dergisi,* vol. 11, no. 2, pp. 131–145, Apr. 2018, doi: 10.17671/gazibtd.327544.
[Online] Available:
https://www.researchgate.net/publication/323369458_A_Systematic_Mapping_Study_on_the_Current_Status_of_Total_Cost_of_Ownership_for_Information_Systems

[71] A. E. Pena-Molina and M. M. Larrondo-Petrie, “Safety and Security Considerations for Online Laboratory Management Systems,” *J. Cybersecur. Priv.,* vol. 5, no. 2, Art. no. 24, May 2025, doi: 10.3390/jcp5020024.
[Online] Available: https://www.mdpi.com/2624-800X/5/2/24

[72] Logpoint, “The ultimate SIEM pricing guide,” *Logpoint Blog,* Nov. 24, 2023.
[Online] Available: https://logpoint.com/en/blog/the-ultimate-siem-pricing-guide

[73] F. T. Liu, K. M. Ting and Z.-H. Zhou, “Isolation Forest,” in *Proc. Int. Conf. Data Mining (ICDM)*, 2008, pp. 413–422.
[Online] Available: https://www.lamda.nju.edu.cn/publication/icdm08b.pdf

[74] M. A. Shyaa *et al.*, “Enhanced Intrusion Detection with Data Stream Classification and Concept Drift Guided by the Incremental Learning Genetic Programming Combiner,” *Sensors,* vol. 23, no. 7, Art. no. 3736, Apr. 2023, doi: 10.3390/s23073736.
[Online] Available: https://www.mdpi.com/1424-8220/23/7/3736

[75] K. Macnish and J. van der Ham, “Ethics in cybersecurity research and practice,” Technology in Society, vol. 63, p. 101382, Nov. 2020. doi: 10.1016/j.techsoc.2020.101382.
[Online] Available: https://www.sciencedirect.com/science/article/pii/S0160791X19306840

CLARIFICATION

During the development of this project, the system was designed to be optimized for small and medium-sized enterprises and was evaluated using a dataset that combined real logs with a larger portion of simulated attack logs. The AI models were applied with the goal of performing lightweight anomaly detection that fits the hardware limitations commonly found in SME environments. The MTTR and TCO results were measured in a controlled test environment, which means that these values may change when the system is deployed in real-world settings. The SOAR playbooks were created based on common incident scenarios and can be expanded to support more complex situations.

Throughout the report-writing process, the team used AI (ChatGPT, Gemini, Claude, Perplexity) only as a support tool for analyzing arguments, checking logical consistency, and proposing initial content structures. All technical content, system analysis, experimental results, and evaluation metrics were produced directly by the team based on the actual implementation work. The team did not rely on AI to write the report in order to avoid any inaccuracies or deviations from the original research direction and to ensure both technical accuracy and academic integrity. AI served only as a reference and support tool and did not replace the research process carried out by the team.