Hochschule Niederrhein
University of Applied Sciences

January 2025

# OWELK: A Scalable and Cost-Effective Network Security Monitoring Framework for Micro-Enterprises


**Ozan Ayik**
Niederrhein University of Applied Sciences
Matrikelnr.: censored

**Oliver Buchmann**
Niederrhein University of Applied Sciences
Matrikelnr.: censored

**Florian Kohn**
Niederrhein University of Applied Sciences
Matrikelnr.: censored

## Abstract

Micro-enterprises—businesses are vital contributors to the global economy but often lack the resources and expertise to implement robust cybersecurity measures. This vulnerability exposes them to significant cyber threats, leading to potential financial losses and operational disruptions. This paper addresses these challenges by developing a holistic network monitoring approach specifically tailored for micro-enterprises. Utilizing Utility Analysis, we systematically evaluated various network security tools against criteria critical for these businesses—cost-effectiveness, reliability, ease of installation, usability, scalability, and security features. Design Science Research (DSR) provided the methodological framework to design and develop an integrated, practical solution.

The result is OWELK, an open-source, integrated solution comprising OPNsense (firewall and IDS/IPS), Wazuh (security monitoring), Elasticsearch, Logstash, and Kibana. This stack offers comprehensive network security monitoring, intrusion detection and prevention, log management, and data visualization capabilities. By leveraging open-source technologies and strategic configurations, the OWELK stack provides real-time threat detection and comprehensive logging without imposing significant financial or technical burdens.

Our findings demonstrate that OWELK effectively enhances the cybersecurity posture of micro-enterprises, making advanced network security accessible to organizations with limited resources. However, the requirement for basic technical expertise for setup and maintenance may present a barrier, and the specific network configurations used in our implementation could affect generalizability.

Future work should focus on simplifying the deployment process through automation or user-friendly installation tools to reduce technical barriers. Collaborating with managed service providers could offer micro-enterprises access to these solutions without the need for in-house expertise. Conducting studies across diverse micro-enterprise environments would provide deeper insights into the practical applicability and scalability of OWELK.

# Contents

1. Introduction ..... 1
2. Related work ..... 4
3. Fundamentals ..... 6
3.1. Definition and characteristics of micro-enterprises ..... 6
3.2. Security Challenges in Micro-Enterprises ..... 7
3.3. Basics and objectives of network monitoring ..... 8
3.3.1. Security information and event management (SIEM) ..... 9
3.3.2. Intrusion detection/prevention systems (IDS/IPS) ..... 9
3.3.3. Firewall ..... 10
4. Developing a holistic network monitoring strategy for micro-enterprises using Utility Analysis & Design Science Research ..... 11
4.1. Introduction ..... 11
4.2. Context ..... 12
4.3. The Journey ..... 12
4.3.1. Introduction to Design Science Research (DSR) ..... 12
4.3.2. DSR Process ..... 13
4.3.3. Round 1 – Initial Utility Assessment of Network Monitoring Tools for Micro-Enterprise Applications ..... 14
4.3.3.1. Goal Formulation ..... 15
4.3.3.2. Criteria ..... 17
4.3.3.3. Calculation of the average criteria weights ..... 18
4.3.3.4. Calculation of the Utility Score ..... 19
4.3.4. Round 2 – Evaluation of a possible network topology for a micro-enterprise .. 24
4.3.5. Round 3 – Implementing OPNsense, Wazuh, Elastic Search, Logstash & Kibana (OWELK) ..... 26
4.3.5.1. Prerequisites for OWELK ..... 27
4.3.5.2. Network Topology ..... 28
4.3.5.3. Firewall Configuration ..... 29
4.3.5.4. Implementing OWELK – Using our guide ..... 31
4.3.6. Installing Agents ..... 31
4.3.6.1. Recommended Installation Strategy ..... 32
4.3.7. Index Lifecycle Management ..... 32
4.3.7.1. Wazuh Agent ..... 34
4.3.7.2. Elastic Agent ..... 34

4.3.8. Creating Agent Policies ..... 34
4.3.9. Configuring/Loading our alerts ..... 35
4.3.10. Testing OWELK to detect cyber attacks ..... 36
4.3.11. Working with OWELK ..... 38
4.3.12. False Positives ..... 39
4.3.13. Tailored Incident Response and the Role of Standardized Methodologies ..... 40
5. Discussion ..... 41
6. Conclusion ..... 43
7. Attachment A – Installation of OWELK ..... 45
7.1. Preparation ..... 45
7.2. Installation of Wazuh ..... 45
7.3. Cronjobs for log forwarding to Wazuh ..... 46
7.4. Installation of Logstash ..... 46
7.5. Configuration of Logstash ..... 46
7.6. Installation of Elasticsearch and Kibana ..... 47
References ..... 53

# List of Figures

Figure 1: Definition of SMEs by countries [1] ..... 6
Figure 2: DSRM process model by K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee ..... 13
Figure 3: Typical network architecture for small business [3] ..... 25
Figure 4: Example network topology for OWELK implementation ..... 29
Figure 5: Example network topology for OWELK implementation ..... 32
Figure 6: Overview of the Index Lifecycle Policy ..... 33
Figure 7: Overview of agent policies in Kibana ..... 35
Figure 8: Overview of automatically generated alerts in Kibana ..... 36
Figure 9: The scan results of Nessus ..... 37
Figure 10: Running nmap scans on the target system ..... 37
Figure 11: generated alerts by OWELK after running vulnerability scans ..... 38

# List of Tables

Table 1: Related work ..... 4
Table 2: Goal Formulation for Utility Analysis ..... 16
Table 3: Calculation of the average criteria weights ..... 19
Table 4: Number of references in the firewall selection methodology ..... 20
Table 5: Calculation of the utility value for the firewall applications ..... 21
Table 6: Number of references in the SIEM System selection methodology ..... 21
Table 7: Calculation of the utility value for SIEM Systems ..... 22
Table 8: Number of references in the IDS/IPS selection methodology ..... 22
Table 9: Calculation of the utility value for IDS/IPS Systems ..... 23
Table 10: Hardware used for OWELK [4], [5], [6] ..... 27
Table 11: Firewall configuration for OWELK ..... 30

# Listings

Listing 1: Preparation before install ..... 45
Listing 2: Firewall configuration ..... 45
Listing 3: Wazuh installation ..... 45
Listing 4: Cronjobs for log forwarding to Wazuh ..... 46
Listing 5: Installing Logstash ..... 46
Listing 6: Logstash installation ..... 47
Listing 7: Logstash – Entering Elasticsearch username and password ..... 47
Listing 8: Logstash – Entering Elasticsearch username and password follow up ..... 47
Listing 9: Preparation of installing Elasticsearch and Kibana ..... 48
Listing 10: Firewall configuration for Elasticsearch ..... 48
Listing 11: Installation of Elasticsearch and Kibana ..... 48
Listing 12: Starting Elasticsearch for the first time ..... 48
Listing 13: Provision of Certificates ..... 49
Listing 14: Starting Elasticsearch for the first time ..... 49
Listing 15: Providing certificates to Kibana ..... 50
Listing 16: Kibana Keystore ..... 50
Listing 17: Configuration of Kibana ..... 51
Listing 18: Installation of Fleet Servers ..... 51
Listing 19: Installation of Fleet Servers 2 ..... 52
Listing 20: Installation of Fleet Servers 3 ..... 52
Listing 21: Configuration of Kibana ..... 52

# 1. Introduction

Micro-enterprises are a vital part of the global economy, contributing significantly to innovation, employment, and economic diversity. Despite their importance, these small businesses often face significant challenges in managing their information technology (IT) infrastructure, particularly in the area of cybersecurity. The increasing complexity of cyber threats underscores the need for robust network monitoring solutions. However, micro-businesses typically lack the resources and expertise to implement the comprehensive security measures that are standard in larger organizations. As digital transformation accelerates and cyber threats become increasingly sophisticated, micro-enterprises face heightened vulnerabilities that can lead to devastating financial losses, operational disruptions, and reputational damage [7].

The cybersecurity landscape presents unique challenges for micro-enterprises. Limited financial resources hinder their ability to invest in advanced security solutions, while the absence of dedicated IT staff makes the implementation and management of even basic security measures daunting. Moreover, a common misconception among these businesses is the belief that their size renders them insignificant targets for cyberattacks, leading to negligence in adopting necessary precautions. This false sense of security is particularly perilous given reports indicating that a substantial percentage of cyberattacks are directed at small businesses [7].

Holistic network monitoring that integrates multiple security technologies to provide a unified view of network activity is essential to effectively detect and respond to threats. Firewalls, intrusion detection and prevention systems (IDS/IPS), and security information and event management (SIEM) platforms are critical components of such an integrated approach. However, selecting appropriate technologies that are both effective and feasible for micro-enterprises remains a significant challenge due to budget, technical expertise and scalability constraints [7].

This paper focuses on developing a holistic network monitoring approach tailored specifically for micro-enterprises by leveraging Utility Analysis and Design Science Research (DSR). Utility Analysis provides a systematic framework for evaluating and selecting network security tools based on criteria critical to micro-enterprises, such as cost-effectiveness, ease of use, scalability, and security features. DSR offers a methodological approach to design and develop an artifact—in this case, a network monitoring solution—that addresses the identified needs and constraints of micro-enterprises.

The primary objectives of this research are:

- To identify and evaluate network monitoring tools suitable for micro-enterprises using Utility Analysis, ensuring that the selected tools align with the specific requirements and limitations of these organizations.
- To design and develop an integrated network monitoring solution utilizing DSR, resulting in an artifact that enhances the cybersecurity posture of micro-enterprises without imposing significant financial or technical burdens.

By addressing these objectives, this research aims to fill a gap in the cybersecurity space and provide a viable path for micro-enterprises to strengthen their defenses against cyber threats.

The structure of this paper is as follows:

- **Fundamentals**: This section provides a comprehensive overview of micro-enterprises, including their definitions, characteristics, and the unique security challenges they face. It also covers the basics and objectives of network monitoring, Security Information and Event Management (SIEM) systems, Intrusion Detection/Prevention Systems (IDS/IPS), and firewalls, establishing the foundational knowledge necessary for understanding the subsequent sections.

- **Context**: Here, we delve deeper into the specific issues confronting micro-enterprises in the digital age, highlighting the limitations in resources and expertise that hinder their ability to implement effective cybersecurity measures.

- **The Journey**: This chapter outlines the methodology employed in the research. It introduces Design Science Research (DSR) and details the DSR process model used. Through iterative rounds of evaluation and refinement, we describe how Utility Analysis was applied to assess and select suitable network monitoring tools.

- **Implementation of OWELK**: Building upon the findings from the utility analysis, this section discusses the development and deployment of the integrated solution—comprising OPNsense, Wazuh, Elasticsearch, Logstash, and Kibana (collectively referred to as OWELK). It covers the practical aspects of implementing OWELK in a micro-enterprise network topology, including prerequisites, network configuration, and agent deployment.

- **Discussion**: We reflect on the outcomes of the implementation, evaluating the effectiveness of the OWELK stack in enhancing the cybersecurity posture of micro-enterprises. This section also addresses potential limitations and the implications of our findings within the broader context of cybersecurity for small businesses.

- **Conclusion**: The paper concludes by summarizing the key contributions of the research, reaffirming the importance of tailored cybersecurity solutions for micro-enterprises, and suggesting directions for future work to further support these vital components of the global economy.

By integrating Utility Analysis and Design Science Research, this paper contributes to both academic knowledge and practical applications, offering micro-enterprises a feasible and effective strategy to navigate the complex cybersecurity landscape.

## 2. Related work

In order to situate our research within the existing body of knowledge, we conducted a comprehensive analysis of related work in the area of network monitoring solutions for micro-enterprises. Table 1 summarizes the key sources and their contributions, providing insights into previous approaches and highlighting areas that our paper aims to address.

Table 1: Related work

| Nr. | Title | Summary |
|---|---|---|
| 1 | S. Kandpal, S. Bhatt, L. Mohan, A. Patwal, and P. Kumar [8] | Welsh SMEs face complex cybersecurity challenges, including limited resources, high implementation costs, and a lack of awareness around cyber threats. This study investigates how government support could help overcome these barriers, examining perspectives from 34 SMEs. Findings emphasize the need for government interventions such as funding programs, targeted training, and strategic support systems. Recommendations include establishing a managed cybersecurity alert framework, providing financial incentives, and enhancing access to local IT expertise, ultimately aiming to strengthen cybersecurity resilience among Welsh SMEs. |
| 2 | A. Gupta and R. Hammond [9] | This paper examines the security challenges faced by small businesses. Based on a survey of 138 small businesses, the study finds that while many have basic security policies in place, there are significant gaps in their effectiveness. It highlights resource constraints, lack of expertise and limited preventative measures as major barriers, suggesting that small businesses need tailored security strategies to mitigate risk. |
| 3 | A. F. J. A. M. Jawad Manzoor Abdul Waleed [10] | Manzoor et al. investigate open source SIEM tools as cost-effective security solutions for SMEs. The study evaluates the security features and performance of selected SIEM systems, such as Wazuh, OSSIM and Elastic Security, by deploying them in simulated SME network environments. The results show that Wazuh is a strong performer, providing high event processing speed and essential compliance features suitable for the needs of SMBs. |

In developing our holistic network monitoring strategy for micro-enterprises, we closely examined A. F. J. A. M. Jawad Manzoor Abdul Waleed [10] paper, “Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs.” Their work evaluates open-source SIEM solutions—including Wazuh and Elastic Security—highlighting

Wazuh's superior security features and performance in small and medium-sized enterprise contexts. While their analysis provides a solid foundation, focusing on performance metrics in controlled environments, our research advances this by implementing Wazuh and Elastic Stack within live micro-enterprise networks.

# 3. Fundamentals

## 3.1. Definition and characteristics of micro-enterprises

The definition of large, small-to-medium-sized enterprises (SMEs) varies across countries, influenced by their unique industrial and economic frameworks. Key indicators distinguishing micro, small, medium, and large enterprises include revenue, payroll size, total assets, and workforce size. Among these, the number of employees is the most frequently used measure [1]. Figure 1 shows how different countries and regions have varying definitions of SMEs.

| | ***Medium*** | ***Small*** | ***Micro*** |
|---|---|---|---|
| | Up to | Up to | Up to |
| ***USA*** | 500 | 100 | N/A |
| ***China*** | 2000 | 300 | N/A |
| ***EU*** | 250 | 50 | 10 |
| ***Australia*** | 200 | 20 | 5 |
| ***Turkey*** | 250 | 50 | 10 |
| ***UK*** | 249 | 49 | 9 |

Figure 1: Definition of SMEs by countries [1]

In the context of business size categories, large, small-to-medium-sized enterprises (SMEs), and micro-enterprises each display distinct operational and structural characteristics. Large enterprises typically have formalized structures with multiple management layers, extensive formal control systems, and a significant focus on long-term strategic planning and innovation through R&D activities. Their resource capacity allows for continuous training and development programs and robust customer relationships on a broader scale [1, p. 311].

SMEs, while still structured, operate with fewer hierarchical layers, often adopting a mix of empowered and controlled supervision. Their strategic focus is typically shorter-term and may be oriented around niche markets. They rely on a blend of formal and informal customer interactions, have moderate access to external networks, and their innovation is often driven by collaborative clusters and industry networking [1, p. 311].

Micro-enterprises, by contrast, are characterized by a highly informal and flexible structure, often limited to a single layer of management with direct control by the owner. Their primary concern is survival rather than long-term strategic planning. Micro-enterprises rarely engage in formal staff development or extensive market innovation due to limited resources. Instead, their innovation is customer-driven, and their networking is minimal, with scarce access to external support or funding opportunities [1, p. 311].

## 3.2. Security Challenges in Micro-Enterprises

Micro-enterprises, small businesses with fewer than ten employees, face unique cybersecurity challenges that arise from their limited resources, technical expertise, and often minimal understanding of digital security practices. Unlike larger organizations, micro-enterprises generally cannot afford dedicated cybersecurity teams or robust technical defenses, making them particularly vulnerable to cyber threats such as phishing, ransomware, and data breaches. Financial constraints further exacerbate these risks, as investing in advanced security tools or cyber insurance often falls outside their budgets. Many cybersecurity decisions in micro-enterprises are made by the business owner, who may lack specialized knowledge, leading to a reliance on basic security measures that may be inadequate for current threat levels. Additionally, micro-enterprises that operate online are exposed to legal risks, including potential non-compliance with data protection regulations and intellectual property violations [7].

In their study, A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi [7] analyze the cyber risks facing SMEs, highlighting the particular vulnerabilities of small e-tailers due to limited resources and dependence on digital infrastructure:

- The most dangerous cyber risks facing small enterprises are those that exploit their limited resources and vulnerabilities in information security. Intellectual property (IP) violations stand out as a critical threat, especially for small enterprises that rely heavily on proprietary products or services. Unauthorized access or theft of IP can have devastating effects, including loss of competitive advantage and severe financial harm, and this risk is given the highest weight (0.597) in cybersecurity assessments for small e-tailers. In addition, small enterprises often struggle with establishing secure online presences, where the lack of trust symbols on their websites—weighted at 0.557 in risk assessments—not only reduces consumer confidence but also increases susceptibility to fraud and phishing attacks. This is particularly dangerous given that consumers are less likely to trust companies that cannot visibly prove their cybersecurity measures, making it easier for attackers to impersonate or breach these enterprises [7, p. 2093].
- Operational risks, such as dependency on third-party payment systems (weighted at 0.367), represent another severe threat. Small enterprises frequently rely on external vendors to handle transactions, exposing them to risks if those vendors are compromised. Similarly, denial-of-service (DoS) attacks, weighted at 0.137, can cripple business operations, as small enterprises typically lack the infrastructure to mitigate such disruptions effectively. Regulatory non-compliance further complicates the cybersecurity landscape; small enterprises

may inadvertently fall short of data protection standards due to a lack of awareness or resources, leading to costly penalties and reputational damage [7, p. 2093].

- Human factors are equally critical, as small enterprises often lack the capacity for extensive cybersecurity training, leaving employees vulnerable to phishing and social engineering attacks. This vulnerability is amplified by limited internal controls and oversight, which can result in accidental data exposure or unauthorized access by current or former employees. Reputation damage due to poor customer service and cybersecurity lapses, weighted at 0.487, further illustrates the impact of operational and service-related risks on consumer perception and business continuity. Given these multifaceted risks, it is essential that small enterprises adopt targeted cybersecurity measures, focusing on critical areas such as IP protection, third-party dependencies, and employee training. Such prioritization is vital to navigate the complex threat landscape with the limited resources available to them [7, p. 2093].

## 3.3. Basics and objectives of network monitoring

Network monitoring is a systematic process central to network management, involving the continuous observation, analysis, and control of network traffic, device behavior, and overall network performance. At its core, network monitoring provides a real-time view of the network's operational status, identifying any discrepancies between the intended and actual network behaviors. By capturing and analyzing metrics such as traffic volume, device health, and user activity, network monitoring equips network operators with the necessary insights to maintain network stability, performance, and security [11], [12].

Network monitoring functions through a range of tools and techniques. It often involves collecting data from various points across the network—such as routers, switches, and end-points—to form a comprehensive model of current network behavior. This data can include packet statistics, CPU loads, link utilization, and latency metrics, each of which contributes to understanding the health of the network. By establishing such a network model, operators can proactively detect issues, optimize network performance, and make informed adjustments to network configurations [11], [12].

Network monitoring methods can be categorized into active and passive approaches. In passive monitoring, data is observed directly from network traffic without introducing any interference, making it a non-intrusive technique. In contrast, active monitoring includes the ability to inject or alter data on the network, allowing for more controlled tests and diagnostics [13], [14].

Several forms of passive monitoring exist, each with unique characteristics and demands. Basic passive monitoring generates minimal data, simplifying manual evaluation. However, when monitoring becomes more detailed and gathers extensive information on network traffic and faults, the sheer volume can make it challenging to isolate critical data from less relevant information. Capturing extensive data also requires advanced technological resources to store and process it efficiently. Consequently, various network monitoring techniques exist, each optimized for specific objectives, environments, and user requirements, balancing trade-offs in data volume, processing demands, and monitoring scope [14].

### 3.3.1. Security information and event management (SIEM)

Security Information and Event Management (SIEM) systems are platforms designed to collect, aggregate, store, and correlate security-related events across IT infrastructures. These systems gather data from multiple network sources, including intrusion detection systems, firewalls, and antivirus applications, to facilitate real-time threat detection and monitoring. The data aggregation and correlation provide security teams with a consolidated view of network activity, which supports efficient incident response and comprehensive security reporting. SIEMs are frequently utilized within Security Operations Centers (SOCs), where they support coordinated responses to security incidents and facilitate ongoing security management [15].

SIEM systems have further integrated advanced data analytics capabilities, enhancing their potential for real-time event analysis and threat detection. In addition to traditional functions like log management and compliance support, current SIEM platforms incorporate automated incident responses, threat prediction models, and enhanced visualization tools [15], [16]. These functionalities allow security teams to monitor potential security issues continuously, implement preventive measures, and streamline incident response processes [15], [16]. As a result, SIEM systems are increasingly utilized in sectors with rigorous security requirements, such as finance, healthcare, and critical infrastructure [15].

### 3.3.2. Intrusion detection/prevention systems (IDS/IPS)

Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) are essential components that bolster network infrastructure security. Positioned immediately behind the firewall, these systems provide additional layers of alerting and defense. The IDS functions as a passive system that monitors, records, and reports potential threats without taking action, whereas the IPS actively examines network traffic and initiates responses as needed. Like the IPS, IDS can log activity; however, it also has the capability to block traffic from malicious sources, discard harmful packets, or reset connections based on specific requirements [17].

For effective threat mitigation, the IPS must operate with near real-time capabilities to address issues promptly while also minimizing false positives within the network [17], [18].

### 3.3.3. Firewall

A Firewall is a fundamental component in the architecture of network security, functioning as a barrier that regulates incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a controlled link between networks of different trust levels, such as the internet and an internal corporate network [19]. By scrutinizing data packets and enforcing access controls, firewalls protect critical network resources from unauthorized access, cyber attacks, and other security threats [20].

From a technical perspective, firewalls operate at various layers of the OSI-model and can be classified into several types:

- Packet-Filtering Firewalls: Operates at the network layer, analyzing packets in isolation based on source and destination IP adresses, ports and protocols. They are efficient but limited in the depth of inspection [20].
- Stateful Inspection Firewalls: Function at the transport layer, maintaining a state table to monitor active connections. They make decisions based on the context of traffic, providing enhanced security over packet-filtering firewalls [21].
- Applications-Level Gateways: Operates at the application layer, intercepting and inspecting entire messages rather than individual packets. They offer detailed control over application-specific protocols but may introduce latency [20].
- Next-Generation Firewalls: Integrate traditional firewall capabilities with advanced features like intrusion prevention systems (IPS), deep packet inspection (DPI), and application-aware filtering. NGFWs address modern security challenges posed by sophisticated threats [22].

# 4. Developing a holistic network monitoring strategy for micro-enterprises using Utility Analysis & Design Science Research

## 4.1. Introduction

Micro-enterprise-businesses with fewer than ten employees are the backbone of many economies worldwide. Despite their significant contributions, these small organizations often lack the resources and expertise to implement robust cybersecurity measures. As cyber threats become increasingly sophisticated, micro-enterprises are disproportionately vulnerable to attacks that can have devastating effects on their operations and reputations [23].

Recent reports highlight a sharp rise in cyberattacks targeting small businesses. According to the European Union Agency for Cybersecurity (ENISA), small and medium-sized enterprises (SMEs) are becoming prime targets due to their limited cybersecurity defenses [24]. Verizon Business [25] further emphasizes that 43% of cyberattacks are aimed at small businesses, underscoring the urgent need for effective security strategies. This vulnerability is exacerbated by common misconceptions within micro-enterprises that their size renders them insignidicant to attackers a perception that leaves them unprotected and highly exposed [26]. Holistic network monitoring is increasingly recognized as an essential protection mechanism for small businesses [27]. By integrating advanced technologies such as firewalls, intrusion detection and prevention systems (IDS/IPS) and security information and event management platforms (SIEM), organizations can achieve comprehensive visibility and real-time threat detection across their networks [28], [29].

Traditional solutions are often associated with high costs and complexity, making them impractical for micro businesses, and comprehensive network monetoring is increasingly recognized as an essential protection mechanism for micro businesses [30].

This research addresses these challanges by proposing a cost-effective and scalable network monitoring solution tailored to the specific needs of microenterprises. Through the use of utility analysis and design science research (DSR), we systematically evaluated a number of open source security tools to find solutions that balance affordability, ease of use and robust security features [31]. This solution aims to provide microenterprises with real-time threat detection and a holistic oversight of their network activity, bridging the gap between their limited resources and the growing need of advanced cybersecurity.

By integrating these methods, we seek to create an artefact that addresses both the technical aspects of network monitoring and the specific needs and constraints of micro-enterprises.

## 4.2. Context

The digital transformation of business processes has made network security a critical concern for organizations of all sizes. Micro-businesses in particular face unique challanges:

- Limited resources: Financial constraints often prevent micro-businesses from investing in advanced cybersecurity solutions [32].
- Lack of expertise: Without dedicates IT staff, implementing and managing security measures becomes a daunting task [32].
- Perception of low risk: Many micro-businesses believe they are too small to be attacked, leading to negligence in adopting necessary security precautions [32].

These factors contribute to higher vulnerability to cyber threats such as phishing attacks, ransomware and data breaches [32]. A successful cyberattack can result in significant financial loss, business disruption and damage to customer trust [33].

Traditional network monitoring solutions are often complex and costly, making them unsuitable for micro-enterprises. There is an urgent need for a tailored approach that considers the benefits and practicality of implementation in these organizations [34].

## 4.3. The Journey

This chapter describes the 'journey' that was taken to obtain the artefact. It describes the methodology of design science research and also the utility analysis process that was used to create the artefact. The process and development of the artefact is presented in this chapter.

### 4.3.1. Introduction to Design Science Research (DSR)

The aim of a DSR research project is to push the boundaries of human and organisational capabilities by designing new and innovative artefacts represented by constructs, models, methods and instances [35, p. 76]. DSR aims to generate knowledge about how things can and should be constructed or arranged, usually through human activity, to achieve a desired set of goals; this is referred to as design knowledge (DK). In the field of information systems (IS), this includes, for example, the knowledge of how to structure and build a database system, how to model business processes, how to align IS with business strategy, how to provide data analytics for effective decision making, and how to use information technology to support sustainable practices [36, p. 1275-1299], [37, p. 337-390]. DSR outcomes have been shown to have significant economic and societal impacts in the information society [38, p. 337-355]. Beyond the field of IS, DSR is a central research paradigm in many other fields, including

engineering, architecture, economics and other disciplines related to information technology, to develop new solutions to relevant design problems [39, p. 2].

### 4.3.2. DSR Process

The process model according to K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee [2] was used for this work. The Design Science Research Methodology (DSRM) is shown in Figure 2. The DSR process comprises six steps: Problem identification and motivation, Defining the goals of a solution, Design and development, Demonstration, Evaluation and Communication, as well as four possible entry points: problem-centred initiation, goal-centred solution, design and development-centred initiation and customer/context-centred initiation. The individual DSR activities are briefly described below.

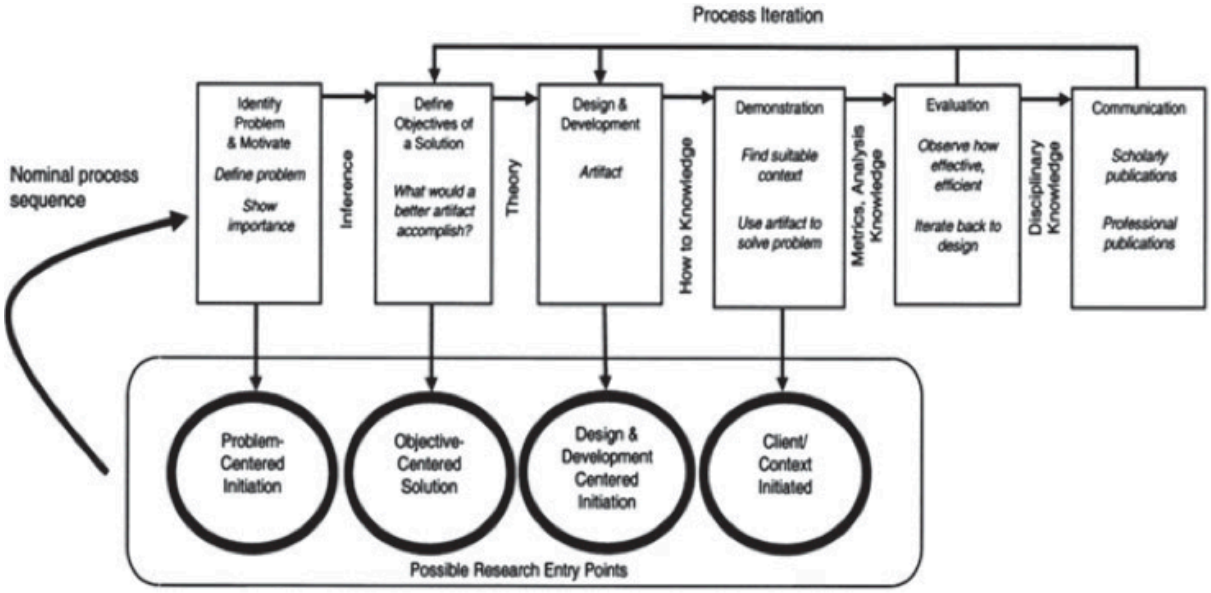


Figure 2: DSRM process model by K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee

**Problem identification and motivation:** This activity defines the specific research problem and justifies the value of a solution. Justifying the value of a solution has two goals: It motivates the researcher and the research public to pursue the solution, and it helps the public appreciate the researcher's understanding of the problem. The resources required for this activity include knowledge of the status of the problem and the importance of its solution.

**Defining the goals of a solution:** The goals of a solution can be derived from the problem definition and the knowledge of what is possible and feasible. The goals can be quantitative, e.g. in terms of the conditions under which a desirable solution would be better than the current one, or qualitative, e.g. a description of how a new artefact should support solutions

to previously unaddressed problems. The goals should be rationally derived from the problem specification.

**Design and development:** An artefact is created. Conceptually, a DSR artefact can be any designed object with a research contribution embedded in its design. This activity involves defining the desired functionality and architecture of the artefact and then creating the artefact itself.

**Demonstration:** This activity demonstrates the use of the artefact to solve one or more instances of the problem. This may include use in experiments, simulations, case studies, proofs or other appropriate activities.

**Evaluation:** Evaluation measures how well the artefact supports the solution to the problem. This activity compares the objectives of a solution with the actual observed results of using the artefact in context. Depending on the nature of the problem domain and the artefact, evaluation can take many forms. At the end of this activity, researchers can decide whether to return to the third step to improve the effectiveness of the artefact, or to continue with communication and leave further improvement to later projects

**Communication:** Here, all aspects of the problem and the developed artefact are communicated to the relevant stakeholders. Depending on the research objective and target group, e.g. experts from the field, suitable forms of communication are used.

#### 4.3.3. Round 1 – Initial Utility Assessment of Network Monitoring Tools for Micro-Enterprise Applications

**Problem:** Micro-enterprises face significant challenges in identifying and implementing suitable network monitoring solutions due to limited budgets, minimal technical expertise, and specific operational needs. Unlike larger organizations, which have access to advanced resources and dedicated IT staff, micro-enterprises often operate with constrained resources, making it difficult to adopt complex and costly cybersecurity tools [30].

This limitation creates a high-risk environment as micro-enterprises become attractive targets for cyber threats, yet lack adequate defences. The selection process is further complicated by the need to balance several factors - cost, reliability, ease of installation, usability, scalability and security features - to find solutions that can provide effective protection without exceeding their operational capabilities. [30].

**Solution:** In the realm of decision-making for network monitoring, a utility analysis provides a robust framework for evaluating and selecting optimal solutions. This structured approach is

designed to assess multiple decision criteria objectively, balancing quantitative and qualitative factors to derive a comprehensive score that reflects the utility of each alternative. Utility analysis, a form of scoring and evaluation tool, is widely regarded in management as a "Swiss Army knife" due to its flexibility and applicability across various complex decision scenarios [40].

The J. B. Kühnapfel [40] method allows network monitoring requirements to be broken down into manageable criteria, ensuring that each aspect - from technical compatibility to cost-effectiveness - is systematically evaluated. By weighting these criteria according to their relevance, this analysis provides a transparent and repeatable basis for decision making, minimising subjective bias and increasing clarity of decision.

The utility analysis process for network monitoring begins by defining the objective, ensuring clarity in the decision problem. Alternatives are then identified, followed by determining relevant evaluation criteria. Each criterion is weighted to reflect its importance, and scoring scales are developed for consistent evaluations. The alternatives are scored based on these criteria, and weighted scores are calculated to obtain a utility score for each option. Sensitivity analysis may be performed to test the robustness of results, and finally, all findings are documented to support transparency in the decision-making process [40].

#### 4.3.3.1. Goal Formulation

To select the most suitable network monitoring tools for micro-enterprises, it is essential to establish clear and specific goals that directly address the unique challenges these organizations face. The goal formulation serves as a foundation for the utility analysis, guiding the evaluation process to ensure that the selected tools align with the strategic needs and operational constraints of micro-enterprises.

Table 2 outlines the formulated goals, categorized into four key areas: Selection Objectives, Performance Evaluation, Implementation Impact, and Strategic Alignment. Each goal is linked to the relevant evaluation criteria, providing a structured framework for the utility analysis.

Table 2: Goal Formulation for Utility Analysis

| **Goal Category** | **Specific Goal** | **Related Evaluation Criteria** | **Expected Outcome** |
|---|---|---|---|
| Selection Objectives | Identify network monitoring tools that offer the highest utility for micro-enterprises by balancing cost, functionality, and ease of use. | Cost, Usability, Ease of Installation | Selection of tools that are affordable, user-friendly, and easy to implement without extensive technical expertise. |
| Performance Evaluation | Assess the reliability and effectiveness of different network monitoring tools in threat detection and response within a micro-enterprise context. | Reliability, Security Features | Identification of tools that provide robust security capabilities and consistent performance in detecting and mitigating threats relevant to micro-enterprises. |
| Implementation Impact | Evaluate how the implementation of selected monitoring tools improves the security posture and operational performance of micro-enterprise networks over time. | Scalability, Usability, Resource Utilization | Understanding of the tools' impact on network performance, scalability to meet future needs, and efficient use of limited resources. |
| Strategic Alignment | Determine which network monitoring tools support long-term sustainability and align with the strategic objectives of micro-enterprises, including adaptability to evolving threats and integration with existing systems and workflows. | Scalability, Integration Capabilities, Usability | Selection of tools that are future-proof, adaptable, and enhance overall business resilience by aligning with long-term strategic goals. |

**Selection Objectives:** The primary aim under Selection Objectives is to find network monitoring tools that offer the highest utility for micro-enterprises by effectively balancing cost, functionality, and ease of use. Given the limited financial and technical resources of micro-enterprises, it is crucial to select tools that are affordable, user-friendly, and straightforward to implement without requiring extensive technical expertise. This ensures that the solutions are accessible and practical for organizations with constrained budgets and limited IT staff.

**Performance Evaluation:** Under Performance Evaluation, the goal is to assess the reliability and effectiveness of different network monitoring tools in threat detection and response within the specific context of micro-enterprises. This involves evaluating the tools' capabilities in providing robust security features and consistent performance in identifying and mitigating threats that are relevant to small businesses. Reliable and effective tools are essential to protect

micro-enterprises from cyber-attacks that could have significant operational and financial impacts.

**Implementation Impact:** The Implementation Impact category focuses on evaluating how the selected monitoring tools will improve the security posture and operational performance of micro-enterprise networks over time. This includes assessing the scalability of the tools to meet future needs, their usability in daily operations, and their efficient utilization of limited resources. Understanding the impact on network performance and resource utilization helps ensure that the tools will not overburden the organization's infrastructure and will remain effective as the business grows.

**Strategic Alignment:** The goal under Strategic Alignment is to determine which network monitoring tools support long-term sustainability and align with the strategic objectives of micro-enterprises. This involves selecting tools that are adaptable to evolving threats, integrate seamlessly with existing systems and workflows, and enhance overall business resilience. By aligning the tools with the organization's long-term goals, micro-enterprises can ensure that their investment in network monitoring contributes to sustained cybersecurity and operational effectiveness.

**Integration into the Utility Analysis:** By establishing these specific goals and linking them directly to the relevant evaluation criteria, we created a structured framework for our utility analysis. Each network monitoring tool under consideration was evaluated against these criteria, with the goals guiding the assessment to ensure that the selected solutions meet the unique needs of micro-enterprises. This approach enabled us to systematically compare alternatives and make informed decisions based on how well each tool aligns with the established goals.

#### 4.3.3.2. Criteria

The next phase in the utility analysis process involves defining the evaluation criteria, which serve as the measurable standards against which network monitoring tools are assessed. In this context, establishing appropriate criteria is essential to ensure that each tool is evaluated comprehensively and objectively, addressing both technical and operational aspects that are critical for micro-enterprises.

Criteria selection should align with the primary goals of affordability, reliability, and ease of implementation, as well as address additional factors that support effective network monitoring:

**Cost:** This criterion evaluates both initial and ongoing expenses, such as licensing, setup, and maintenance costs, essential for micro-enterprises operating with limited budgets.

**Reliability:** Reliability involves assessing the tool's effectiveness in continuous monitoring, uptime, and resilience to network failures or overloads. High reliability ensures stable network operations with minimal interruptions.

**Ease of Installation and Implementation:** This criterion considers the technical complexity involved in deploying the tool, including required expertise, setup time, and integration with existing systems, which is crucial for micro-enterprises lacking extensive IT support.

**Usability:** Usability assesses how intuitive and accessible the tool's interface is, allowing non-expert users to monitor network activities effectively. A clear, user-friendly user interface is vital for daily operations.

**Scalability:** Although micro-enterprises may have limited needs initially, scalability evaluates the tool's capacity to expand as the business grows, ensuring long-term utility without requiring costly upgrades.

**Security Features:** This criterion examines the tool's ability to detect, prevent, and respond to security threats, such as its intrusion detection capabilities, data encryption options, and response time to incidents.

These criteria provide a structured framework to quantify each tool's alignment with the needs of micro-enterprises, allowing for a consistent, objective comparison. Selecting well-defined criteria also ensures transparency, helping stakeholders understand the basis of the evaluation and the specific strengths and limitations of each tool within a real-world context.

#### 4.3.3.3. Calculation of the average criteria weights

Following the establishment of evaluation criteria, the next phase involved a systematic weighting process to assign relative importance to each criterion, ensuring a total of 100%. Table 3 illustrates the calculated average weights assigned to each evaluation criterion based on individual assessments by Ayik, Buchmann, and Kohn. Each evaluator assigned percentage weights to the six criteria (see Section 4.3.3.2) — Cost, Reliability, Ease of Installation and Implementation, Usability, Scalability, and Security Features — reflecting the perceived importance of each factor in selecting network security solutions for micro-enterprises. The individual weights were averaged and rounded to form the final weighting scheme used in the utility score calculation.

Table 3: Calculation of the average criteria weights

| **Criteria** | **Ayik (%)** | **Buchmann (%)** | **Kohn (%)** | **Ø Weights (rounded) (%)** |
|---|---|---|---|---|
| Cost | 25 | 30 | 35 | 30 |
| Reliability | 15 | 10 | 10 | 11,5 |
| Ease of Installation and Implementation | 15 | 15 | 15 | 15 |
| Usablity | 20 | 25 | 20 | 22 |
| Scalability | 15 | 10 | 5 | 10 |
| Security Features | 10 | 10 | 15 | 11,5 |
| **Sum** | **100** | **100** | **100** | **100,00** |

The analysis reveals a consensus on the high importance of Cost, which received the highest average weight (30%), highlighting its critical role for budget-conscious micro-enterprises. Usability was also weighted significantly (22%), underlining the necessity for user-friendly solutions that are manageable without extensive IT expertise. Moderate emphasis was placed on Ease of Installation and Implementation (15%), signaling a preference for solutions that are easy to deploy, while Reliability and Security Features each received an average weight of 11.5%, reflecting their value but slightly lower priority. Scalability, with the lowest weight (10%), indicates a relatively lesser focus on this criterion, likely due to the limited growth requirements typical of micro-enterprises.

#### 4.3.3.4. Calculation of the Utility Score

This chapter introduces the methodology for calculating the utility score, which aids in selecting the most suitable network security solutions for micro-enterprises. The evaluation follows criteria defined in previous chapters, focusing on affordability, reliability, ease of deployment, usability, scalability, and comprehensive security features. The Evaluation has a score range from 0-10 (10 is the best score). The scoring was done in the team collectivly.

##### 4.3.3.4.1. Selection Methodology

To identify potential solutions in each category—firewalls, SIEM systems, and IDS/IPS —- we conducted a systematic search using popular search engines (Google and Bing) with relevant search terms in both English and German. This approach ensured a comprehensive collection of data from a wide range of sources.

We compiled lists of vendors based on the frequency of mentions across various websites, allowing us to rank them according to popularity and common recommendations. Focusing

on the top ten vendors in each category, we evaluated their offerings against our established criteria to assess their suitability for micro-enterprises.

#### 4.3.3.4.2. Firewall Selection Methodology

From our search results, we identified the top ten firewall vendors based on the number of references (see Table 4). We evaluated these vendors against our criteria, emphasizing factors crucial for micro-enterprises such as affordability, ease of use, and compatibility with future SIEM integration.

Table 4: Number of references in the firewall selection methodology

| Manufacturer | Number of references |
|---|---|
| Fortinet | 13 |
| Sophos | 13 |
| Cisco | 12 |
| Check Point | 11 |
| SonicWall | 11 |
| WatchGuard | 11 |
| Palo Alto | 10 |
| netgate | 8 |
| Barracuda | 5 |
| Juniper Networks | 5 |

Our assessment led us to select three firewalls—OPNsense, FortiGate, and Sophos—as the most promising candidates. These products met our objectives by offering a balance of cost-effectiveness, robust security features, and user-friendly interfaces suitable for organizations with limited technical expertise.

The utility scores for these firewalls are presented in Table 5.

Table 5: Calculation of the utility value for the firewall applications

| **Criteria** | **Weights (%)** | **OPNsense** | | **FortiGate** | | **Sophos** | |
|---|---|---|---|---|---|---|---|
| | | Evaluation | Score | Evaluation | Score | Evaluation | Score |
| Cost | 30 | 10 | 3 | 5 | 1.5 | 5 | 1,5 |
| Reliability | 11.5 | 8 | 0,92 | 9 | 1,035 | 9 | 1,035 |
| Ease of Installation | 15 | 7 | 1,05 | 9 | 1,35 | 8 | 1,2 |
| Usability | 22 | 10 | 2,2 | 8 | 1,76 | 8 | 1,76 |
| Scalability | 10 | 8 | 0,8 | 7 | 0.7 | 7 | 0,7 |
| Security Features | 11,5 | 8 | 0,92 | 9 | 1,035 | 9 | 1,035 |
| **Sum** | **100,00** | 50 | **8,89** | 47 | **7,38** | 46 | **7,23** |

OPNsense scored the highest utility value (8.89) due to its zero licensing costs, ease of use, and comprehensive features, making it ideal for micro-enterprises with limited budgets and technical expertise.

#### 4.3.3.4.3. SIEM System Selection Methodology

Applying the same methodology, we identified the top SIEM vendors (see Table 6) and evaluated them against our criteria tailored for micro-enterprises. Key considerations included affordability, scalability, and essential security functionalities.

Table 6: Number of references in the SIEM System selection methodology

| **Manufacturer** | **Number of references** |
|---|---|
| Splunk | 8 |
| IBM Security QRadar | 7 |
| Elastic Security | 6 |
| Exabeam | 6 |
| LogRhythm | 5 |
| Microsoft Sentinel | 4 |
| Securonix | 4 |
| Rapid7 | 4 |
| Logpoint | 3 |
| SolarWinds | 3 |

Our evaluation highlighted Elastic Security as the leading SIEM solution, alongside Splunk and IBM QRadar. Elastic Security stood out due to its open-source nature, cost-effectiveness, and strong performance in usability and scalability—attributes that align well with the needs of micro-enterprises.

The utility scores for these SIEM systems are detailed in Table 7.

Table 7: Calculation of the utility value for SIEM Systems

| **Criteria** | **Weights (%)** | **Splunk** | | **IBM QRadar** | | **Elastic Security** | |
|---|---|---|---|---|---|---|---|
| | | Evaluation | Score | Evaluation | Score | Evaluation | Score |
| Cost | 30 | 4 | 1,2 | 5 | 1,5 | 8 | 2,4 |
| Reliability | 11,5 | 9 | 1,035 | 9 | 1,035 | 8 | 0,92 |
| Ease of Installation | 15 | 8 | 1.2 | 7 | 1,05 | 6 | 0,9 |
| Usability | 22 | 8 | 1,76 | 8 | 1,76 | 10 | 2,2 |
| Scalability | 10 | 9 | 0,9 | 9 | 0,9 | 9 | 0,9 |
| Security Features | 11,5 | 10 | 1,15 | 9 | 1,035 | 8 | 0,92 |
| **Sum** | **100,00** | 48 | **7,245** | 47 | **7,38** | 49 | **8,24** |

Elastic Security achieved the highest utility value (8.24) owing to its cost-effectiveness and strong usability, despite a slightly more complex installation process.

#### 4.3.3.4.4. IDS/IPS

Using the same approach, we identified the top IDS/IPS vendors (see Table 9) and assessed them based on factors critical for micro-enterprises.

Table 8: Number of references in the IDS/IPS selection methodology

| **Manufacturer** | **Number of references** |
|---|---|
| Snort | 9 |
| Cisco | 9 |
| Trend Micro | 7 |
| Check Point | 7 |
| Suricata | 7 |
| Trellix | 6 |
| Security Onion | 6 |
| Palo Alto Networks | 5 |
| ossec | 5 |
| Zscaler | 4 |

Our analysis led us to focus on OPNsense, Snort, and Palo Alto Networks as the top candidates. OPNsense emerged as a particularly attractive option due to its integration capabilities and cost advantages, providing both firewall and IDS/IPS functionalities within a single open-source platform.

The utility scores for these IDS/IPS solutions are shown in Table 9.

Table 9: Calculation of the utility value for IDS/IPS Systems

| **Criteria** | **Weights (%)** | **OPNsense** | | **Snort** | | **Palo Alto** | |
|---|---|---|---|---|---|---|---|
| | | Evaluation | Score | Evaluation | Score | Evaluation | Score |
| Cost | 30 | 8 | 2,4 | 10 | 3 | 4 | 1,2 |
| Reliability | 11.5 | 7 | 0,805 | 7 | 0,805 | 9 | 1,035 |
| Ease of Installation | 15 | 10 | 1,5 | 7 | 1,05 | 8 | 1,2 |
| Usability | 22 | 9 | 1,98 | 6 | 1,32 | 8 | 1,76 |
| Scalability | 10 | 9 | 0,9 | 9 | 0,9 | 9 | 0,9 |
| Security Features | 11,5 | 8 | 0,92 | 8 | 0,92 | 9 | 1,035 |
| **Sum** | **100,00** | 51 | **8,505** | 47 | **7,995** | 47 | **7,13** |

OPNsense again scored the highest utility value (8.505), offering integrated IDS/IPS capabilities without additional cost and with high usability, making it an optimal choice for micro-enterprises.

#### 4.3.3.4.5. Conclusion

Following a comprehensive assessment of a range of tools against our established criteria, we have identified the following technologies as the most suitable for implementation, based on their performance in the utility assessment.

- The Elastic Stack was selected as the SIEM system.
- Additionally, OPNsense was selected as the firewall and IDS/IPS solution.

The scoring methodology, described in the preceding sections, enabled an objective evaluation of each tool in accordance with essential criteria for micro-businesses, including cost, usability, scalability, and integration capabilities. This approach ensured that the selected tools were the optimal fit for the needs of micro-enterprises.

An important factor in our decision-making process was the need to avoid increasing costs for small businesses. Proprietary ecosystems often come with high acquisition and licensing costs, as well as subscription fees that can be prohibitive for micro-businesses. By choosing open source and non-proprietary tools, we minimized these financial burdens and ensured that the solution was cost-effective, sustainable, and easy to maintain. This allows for easy integration with other technologies without vendor lock-in, ensuring the solution remains adaptable and independent.

Moreover, the issue of data ownership was a significant consideration. The selected tools ensure that data remains within the organization's control, preventing its outsourcing or storage of third-party vendors.

Another crucial requirement was scalability, as the selected solution must be capable of accommodating growth. The Elastic Stack is renowned for its scalability, enabling organizations to augment their security information and event management (SIEM) capabilities in accordance with their evolving requirements. Additionally, the selected tools are highly integrated, facilitating straightforward connection of supplementary security technologies to the Elastic Stack SIEM for comprehensive network monitoring.

During our evaluation, we discovered that OPNsense, initially chosen solely as a firewall, also includes an integrated IDS/IPS system. This unexpected feature led us to incorporate OPNsense in our IDS/IPS evaluation as well, and ultimately, we selected it to serve both functions. This dual-purpose use of OPNsense allowed us to open an additional slot for a complementary technology that would integrate seamlessly with our chosen solutions.

Following additional research, we identified Wazuh as a compatible option. OPNsense includes a "Wazuh Agent" package, designed for Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR), which can integrate effectively with Elastic Stack and OPNsense. Given its compatibility and added functionality, we selected Wazuh to round out our technology set.

By combining Elastic Stack, OPNsense, and Wazuh, we have developed a flexible and scalable set of tools, which we refer to as OWELK. The following chapter will evaluate a potential network topology in a micro-enterprise setting, with a particular emphasis on how this framework can be adapted to align with the specific requirements of small businesses.

#### 4.3.4. Round 2 – Evaluation of a possible network topology for a micro-enterprise

A typical network architecture for small businesses is designed to ensure secure, reliable, and efficient connectivity, balancing cost-effectiveness with essential network functionalities. Such an architecture often includes the following key components [3]:

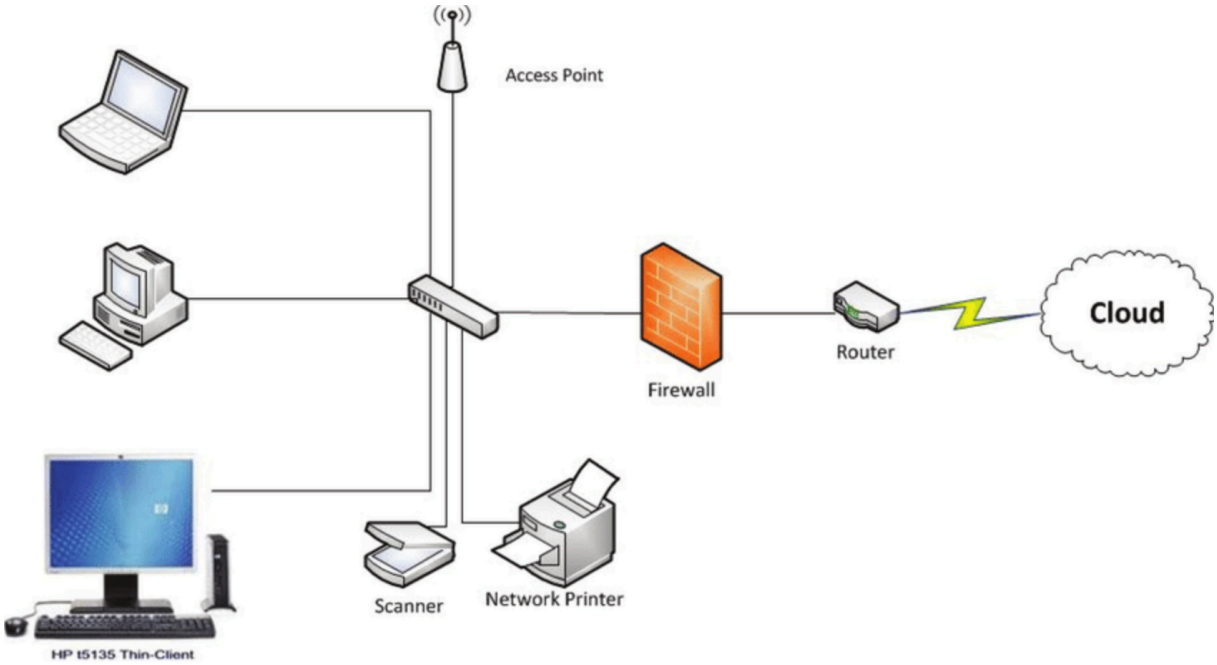


Figure 3: Typical network architecture for small business [3]

**Access Point**: An access point provides wireless connectivity for mobile devices, enhancing flexibility and mobility for employees within the business premises. By supporting Wi-Fi-enabled devices, it allows seamless access to the network, which is crucial for businesses that rely on mobile communication and workstations.

**Firewall**: Positioned between the internal network and the router, a firewall acts as a primary defense mechanism against unauthorized access and cyber threats. It filters incoming and outgoing traffic, ensuring that only legitimate data passes through, thus protecting sensitive business information and reducing the risk of cyber-attacks. A firewall is essential for any small business that handles customer data, financial information, or proprietary information.

**Router**: The router connects the internal network to external networks, such as the internet. It enables internet access for all devices on the network and may include basic security features, network management options, and even virtual private network (VPN) capabilities. By routing data efficiently, it ensures stable internet connectivity, which is critical for cloud services, communication, and daily operations.

**Network Printer and Scanner**: Centralized network printers and scanners allow multiple users to share resources, reducing the need for individual devices for each workstation. This setup is cost-effective and practical, as it consolidates office functions into shared devices that can be accessed by anyone on the network, promoting efficient document handling and resource sharing.

**Thin Clients or PC Workstations**: Thin clients or traditional PCs serve as user access points within the network. Thin clients are particularly beneficial in a small business setting, as they are cost-effective and rely on a central server for processing power, reducing the need for high-specification computers. This approach centralizes computing power and enables easier management and maintenance, making it ideal for businesses with limited IT resources.

**Cloud Integration**: Many small businesses incorporate cloud-based services for data storage, application hosting, and remote access. By leveraging cloud services, businesses can reduce the need for on-premises hardware, minimize costs, and enhance scalability. Cloud integration also facilitates remote access, allowing employees to connect securely to the network from various locations, which is especially beneficial for businesses with remote work or off-site requirements.

In this architecture, all components are interconnected, with the firewall and router providing security and internet access, respectively, while access points, printers, and workstations ensure internal connectivity and resource sharing. This setup supports both wired and wireless connections, accommodating a variety of devices and usage scenarios commonly found in small business environments. The structure is designed to be scalable and adaptable, allowing the network to grow as the business expands [3].

#### 4.3.5. Round 3 – Implementing OPNsense, Wazuh, Elastic Search, Logstash & Kibana (OWELK)

OWELK is a comprehensive open source solution for holistic network security monitoring and log management. It integrates several powerful technologies into a SIEM system. The components are:

- Opnsense: An open source firewall and routing platform that provides security features such as intrusion detection and prevention, traffic shaping, and VPN functionality [41].
- Wazuh: An open source security monitoring platform primarily used for intrusion detection, log analysis and integrity monitoring [42].
- Elasticsearch: A distributed search and analytics engine used to store and search large volumes of log data [43].
- Logstash: A data processing pipeline that ingests, transforms, and passes logs to Elasticsearch [44].
- Kibana: A data visualization and exploration tool used to analyze and visualize data stored in Elasticsearch [45].

Together, these technologies provide a framework for detecting and responding to security incidents, collecting and analyzing logs, and visualizing network activity in real time.

Before implementing OWELK as a comprehensive monitoring solution, certain requirements must be met to ensure a smooth and functional setup. This section outlines the basic requirements.

#### 4.3.5.1. Prerequisites for OWELK

A basic IT network is required to set up OWELK. At a minimum, this includes an Internet-connected router that allows devices and servers to connect to the network and communicate with each other. OWELK requires dedicated hardware on which the technologies can operate effectively. At least two servers are needed for Elasticsearch and Wazuh (see Table 10).

The exact method for installing and deploying these technologies is also adaptable to the needs of the organization. A bare-metal installation is not required; OWELK can run in a virtualized environment using platforms such as Proxmox or VMware, provided sufficient resources are allocated [46]. For guidance on recommended resources, organizations should consult the official documentation for each technology. For reference, below is a table detailing the hardware we used in our setup (see Table 10).

Table 10: Hardware used for OWELK [4], [5], [6]

| **Technology** | **CPU** | **RAM** | **Storage** | **OS** |
|---|---|---|---|---|
| Wazuh and Logstash | 4 | 8GB | 256GB | Debian |
| Elasticsearch and Kibana | 6 | 16GB | 512GB | Debian |
| OPNsense | 4 | 8GB | 128GB | FreeBSD |

However, it is important to note that the hardware requirements for OWELK are dynamic and will vary significantly depending on several factors, including [4], [5], [6]]:

- The number of agents being monitored.
- The volume of logs collected and analysed.
- The length of time logs are stored.

As such, this table serves only as an example configuration used in this reference implementation. For production environments, organizations should carefully evaluate their own specific needs and consult the official documentation for each technology (OPNsense, Wazuh, Elasticsearch) to determine the optimal hardware requirements tailored to their use case [4], [5], [6].

#### 4.3.5.2. Network Topology

Each organization's network infrastructure is unique, reflecting its specific operational needs, resources, and security requirements. Therefore, it is important to understand that while this guide provides a reference implementation, the actual network configuration and topology must be tailored to each organization's environment. This section outlines the basic network infrastructure concepts relevant to the OWELK implementation. A sample network topology is shown in Figure 4 for reference.

It is important to note that depending on the specific network topology in use, the installation steps may need to be adjusted. For example, differences in IP address allocation and subnet configuration will require changes to the setup of various components such as the firewall (Opnsense), IDS/IPS (Wazuh), and log forwarding mechanisms (Logstash). These changes must be accounted for during the configuration phase to ensure that all systems are properly integrated and functioning within the network.

For detailed implementation instructions, including configuration examples and specific installation steps, please refer to our GitHub repository [47]. The repository contains comprehensive documentation in both English and German that provides step-by-step instructions for setting up and connecting the OWELK components in a Debian-based Linux environment. You will find configuration files, bash scripts, and examples that can be used as a reference for your implementation [47].

In this implementation of OWELK, the following setup was utilized as shown in Figure 4:

- Elasticsearch and Kibana were deployed on a Debian server with the IP address 192.168.100.10.
- Wazuh and Logstash were installed on an Ubuntu server with the IP address 192.168.100.11.
- Opnsense was configured as the firewall, assigned the IP address 192.168.100.1 on its internal LAN interface.
- The Wazuh agent was installed on the end devices (e.g., laptops).
- The Elastic Agent was deployed on the servers.

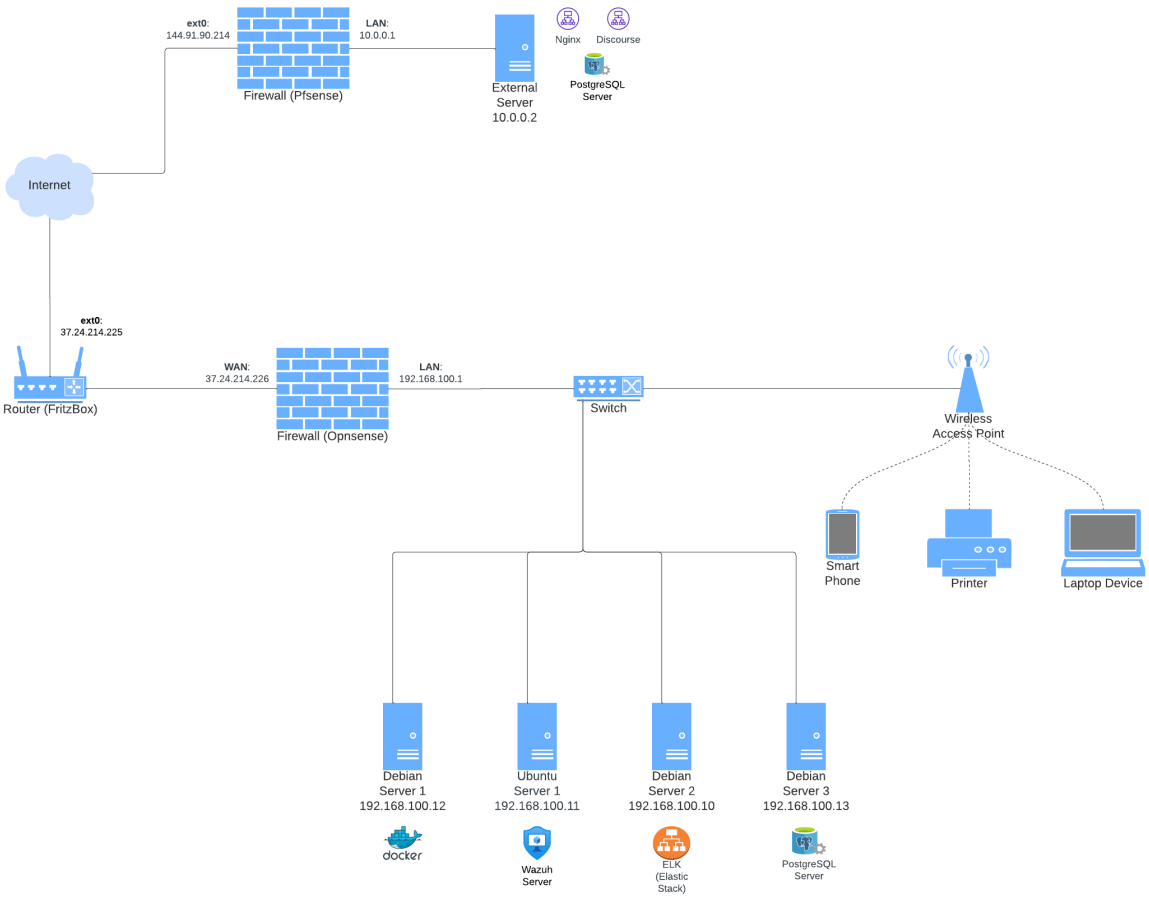


Figure 4: Example network topology for OWELK implementation

#### 4.3.5.3. Firewall Configuration

In order for the OWELK components to work properly, certain network ports must be opened on the firewall. These ports are essential to enable communication between the various systems involved in the implementation, such as log forwarding, event correlation and dashboard access.

Table 11 provides an overview of the ports that need to be opened for each of the OWELK technologies. This configuration is for guidance only and applies to our reference implementation.

Table 11: Firewall configuration for OWELK

| Technology | Port | Location | Description |
|---|---|---|---|
| Wazuh | 1514/TCP | On the server where wazuh is running | This port is used to connect agents to wazuh. The port should be accessible to the devices you want to monitor. |
| Wazuh | 1515/TCP | On the server where wazuh is running | This port is used to register agents to wazuh. The port should be accessible to the devices you want to monitor. |
| Wazuh | 9200/TCP | On the server where wazuh is running | Used for the log-forwarding with logstash. |
| Wazuh | 55000/TCP | On the server where wazuh is running | Used for the log-forwarding with logstash. |
| Elasticsearch | 9200/TCP | On the server where elasticsearch is running | Used to collect logs from various sources. |
| Kibana | 5601/TCP | On the server where kibana is running | This is used to access the Kibana dashboard. |
| Fleet Server | 8220/TCP | On the server where the fleet server is running | Used to connect agents to the Fleet Server. |

However, it is important to note that firewall requirements can vary significantly depending on the organization's specific network infrastructure. Additional firewall rules or settings may be required depending on the organization's internal architecture, security policies or network topology. For example:

- Organizations with segmented network zones may need to configure inter-zone traffic rules to allow communication between OWELK components located in different segments.
- If additional security devices such as VPNs or external monitoring tools are in place, further adjustments to firewall settings may be required to ensure that all traffic is routed securely.
- Special attention should also be paid to external access controls to ensure that only authorized users can access critical OWELK components such as the Kibana dashboard or Opnsense management interface.

For organizations planning to implement OWELK, it is critical to evaluate existing network infrastructure and firewall policies to ensure seamless integration with OWELK components. As part of this process, we recommend that users thoroughly review their network security

architecture and consult the official documentation for each technology to identify any additional firewall rules that may be required [48], [49].

#### 4.3.5.4. Implementing OWELK – Using our guide

To facilitate the implementation of OWELK, we have created a comprehensive guide that is available on GitHub [47] and is also included in Section 7. This guide provides detailed, step-by-step instructions that allow users to set up and configure each OWELK component in their own network environment. While this paper provides insight into our methodology and approach, following the GitHub guide is sufficient to implement OWELK.

Key features of the guide include:

- Bilingual documentation: The GitHub repository contains instructions in both English and German, ensuring accessibility to a wider audience.
- Sample configuration files: To aid in the setup process, we provide sample configuration files from our reference implementation. These files serve as templates and illustrate the settings used in our specific setup.
- Reference, not blueprint: It is important to treat the guide as a reference, not a one-to-one copy. Each network environment is unique, with specific needs and configurations. Therefore, adjustments will likely be necessary to adapt the guide to your organization's infrastructure and needs.
- Prerequisite Knowledge: A basic understanding of IT concepts and familiarity with Linux is required to effectively implement OWELK. Familiarity with network management and security tools is also beneficial.

### 4.3.6. Installing Agents

Once OWELK has been successfully deployed, the next step is to install agents on the systems to be monitored. Agents are lightweight software components that reside on endpoint devices and servers and are responsible for collecting logs, system metrics, and security-related events. They play an essential role in transmitting this data back to centralized servers for analysis, enabling comprehensive network monitoring and threat detection.

In our implementation, we focused on two primary agents:

1. Wazuh agent
2. Elastic Agent

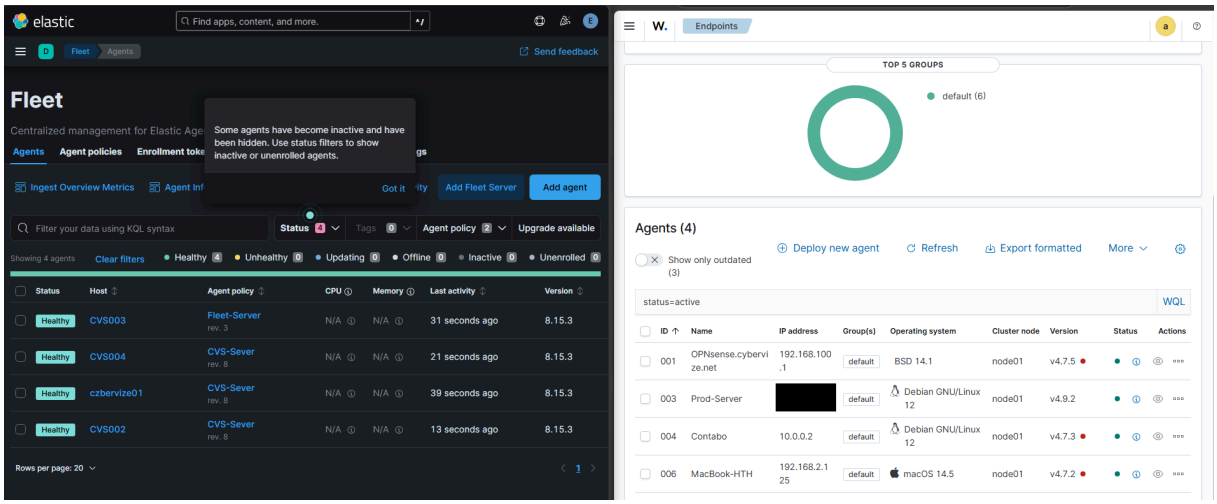


Figure 5: Example network topology for OWELK implementation

These agents are designed to collect detailed information from their host systems and pass it to either the Wazuh server or the Elastic Stack's Fleet Server, an extension of Elasticsearch that manages agent connections and data ingestion.

#### 4.3.6.1. Recommended Installation Strategy

To optimize performance and resource utilization while ensuring maximum coverage of network resources, we recommend the following installation approach:

- Wazuh Agent on endpoints: Install the Wazuh Agent on endpoints such as desktops, laptops, and other user-operated systems.
- Elastic Agent on servers: Deploy the Elastic Agent on server machines that host applications, databases, or other critical services.

This strategy leverages the strengths of each agent type and tailors its capabilities to meet the specific needs of different categories of systems on the network.

### 4.3.7. Index Lifecycle Management

Effective data retention strategies are critical to maintaining the performance and stability of the Elasticsearch cluster within the Elastic Stack. Without proper management, the continuous accumulation of indexed logs can quickly consume available disk space, resulting in system slowdowns or outages. To address this issue, it is important to configure the Index Lifecycle Management (ILM) policy appropriately.

In our implementation, we made specific adjustments to the ILM policy to ensure sustainable operation:

- **Retention Period:** We configured Elasticsearch to retain logs for a maximum of 130 days.

- **Size Threshold:** We set a size limit where if the total indexed logs exceed 20 GB, the oldest data will be deleted to free up space.

This dual condition ensures that the system retains sufficient historical data for analysis and compliance purposes while preventing storage resources from being exhausted. Figure Figure 6 illustrates the ILM policy configuration used in our setup. It is important to note that these parameters are not fixed and should be tailored to an organization's specific needs and resource capabilities. Organizations with greater storage capacity or different data retention requirements may opt for longer retention periods or higher size thresholds. For detailed instructions on how to configure the ILM policy, please visit our GitHub repository [47].

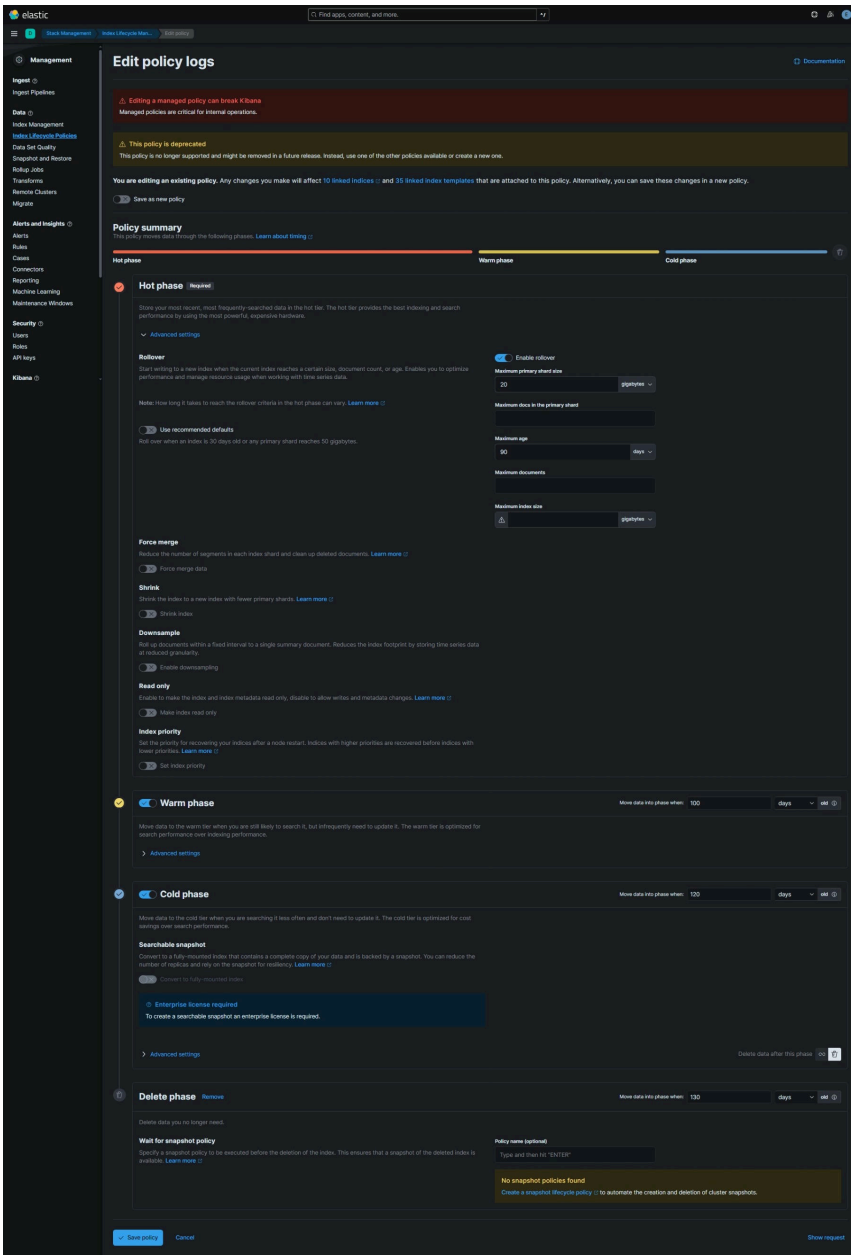


Figure 6: Overview of the Index Lifecycle Policy

#### 4.3.7.1. Wazuh Agent

The Wazuh Agent is a lightweight component that requires minimal system resources, making it ideal for endpoints that have limited processing power or are sensitive to performance impact. Despite its low overhead, the Wazuh Agent provides robust security features, including

- **Vulnerability detection**: Scans the system for known vulnerabilities using up-to-date vulnerability databases.
- **Configuration Assessment**: Evaluates system configurations against security best practices and compliance standards.
- **Security event monitoring**: Detects suspicious activity and anomalies using rules based on the MITRE ATT&CK Framework, a globally accessible knowledge base of adversary tactics and techniques.

By deploying the Wazuh Agent on endpoints, organizations can gain valuable insight into potential security issues at the user level, where threats such as malware infections and unauthorized access attempts are prevalent.

#### 4.3.7.2. Elastic Agent

The Elastic Agent is a more comprehensive tool that offers a wide range of capabilities and integrations, making it well-suited for server environments that require detailed monitoring and analysis. Key features of the Elastic Agent include

- **Integration with multiple technologies**: Supports integrations with various services and applications such as Nginx, Apache, MySQL, and many others.
- **Unified data collection**: Collects logs, metrics, and security data in a standardized format for easier analysis and visualization.
- **Scalability**: Designed to handle the higher data throughput typically associated with servers, ensuring reliable performance even under heavy load.

Deploying the Elastic Agent on servers enables in-depth monitoring of critical infrastructure components to proactively identify performance issues, security threats, and compliance violations.

### 4.3.8. Creating Agent Policies

With the agents installed on the designated systems, the next step is to create agent policies within Elasticsearch Figure 7. Agent policies define the specific configurations and integrations that the agents will use to collect, process, and deliver data from the monitored endpoints to the Elastic Stack. Elastic Stack offers a comprehensive set of integrations that make it easy

to collect logs, metrics, and security events from a variety of sources and technologies. These integrations include, but are not limited to:

- **Nginx Integration**: For collecting logs and metrics from Nginx web servers.
- **Elastic Defend**: To protect systems from security threats.
- **System Metrics Collection**: For gathering essential operating system metrics such as CPU usage, memory utilization, disk I/O, and network statistics.

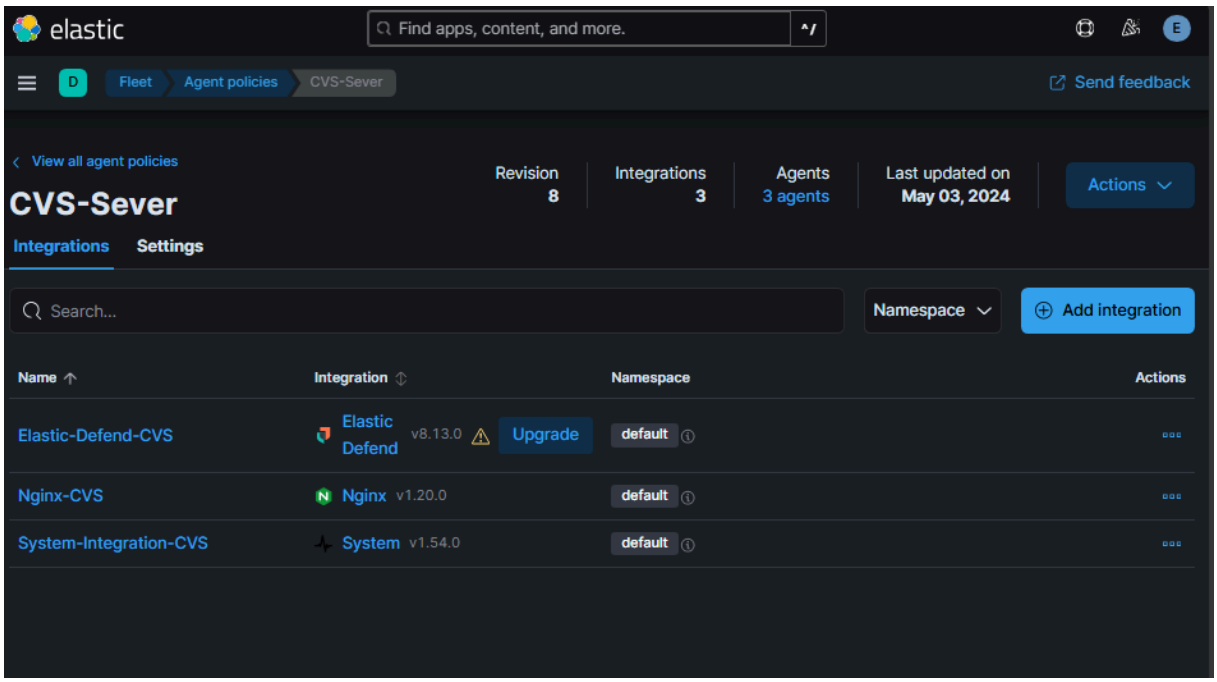


Figure 7: Overview of agent policies in Kibana

### 4.3.9. Configuring/Loading our alerts

An integral part of enhancing the threat detection capabilities within our OWELK stack is the use of pre-defined alert rules. These rules are available in our GitHub repository and are documented in a single NDJSON (Newline Delimited JSON) file for ease of import and management [47].

Our alert rules are based on the MITRE ATT&CK framework, which provides a comprehensive taxonomy of adversary tactics and techniques. Using this framework, the ruleset is designed to effectively query the Wazuh alert logs and filter for specific MITRE incidents. This approach enables the system to detect sophisticated threats by identifying patterns consistent with known attack methods. Users can easily load these predefined alerts into the Elastic Stack via the Kibana dashboard (see Figure 8). Detailed instructions for this process are available in our GitHub repository. After loading the alerts, the Elastic Stack automatically generates alerts in the alert dashboard whenever matching events are detected. This automation facilitates

proactive monitoring and allows users to respond to potential security incidents directly in Kibana. In addition, users have the flexibility to create custom alerts tailored to their specific security needs. Kibana's intuitive interface supports the creation of new alert rules, allowing organizations to address unique threats relevant to their environment. For guidance on creating custom alerts, users are encouraged to consult the official Kibana documentation, which provides comprehensive instructions and best practices.

By integrating our pre-defined alerts and leveraging Kibana's alerting capabilities, organizations can significantly enhance their network monitoring strategy. This approach ensures timely detection and response to security events and strengthens the overall cybersecurity posture.

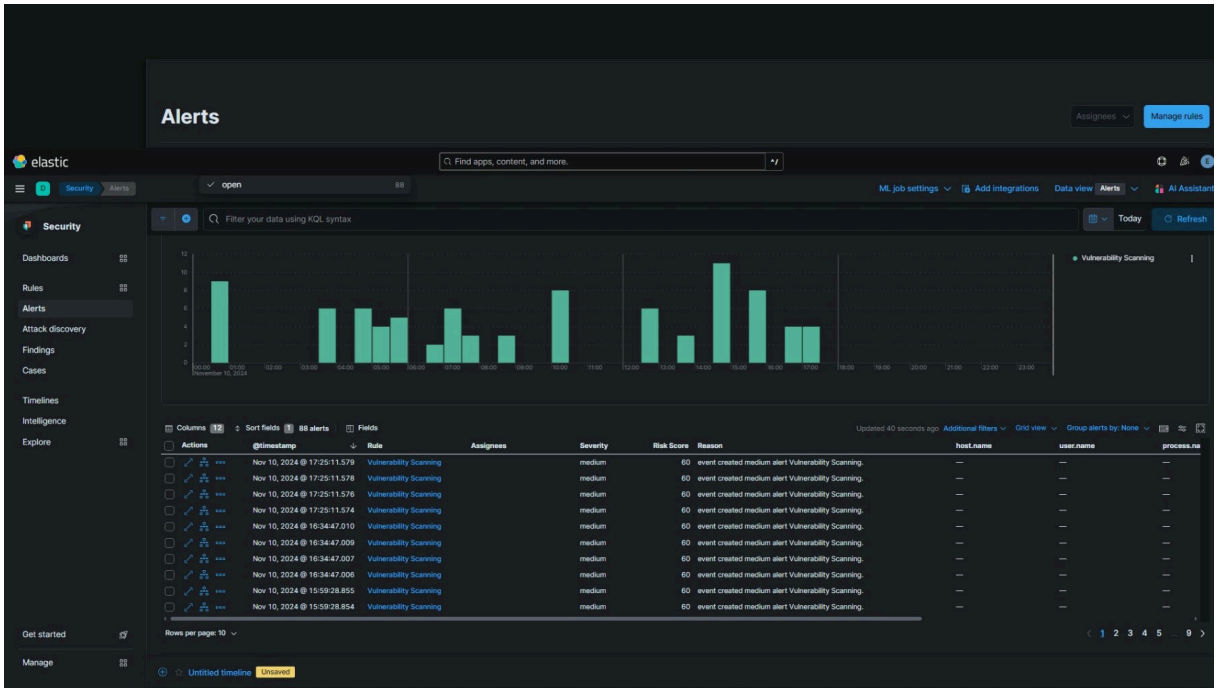


Figure 8: Overview of automatically generated alerts in Kibana

### 4.3.10. Testing OWELK to detect cyber attacks

To validate the effectiveness of the OWELK stack in detecting cyber attacks, we conducted a series of tests using popular network scanning tools such as Nessus and Nmap. These tools simulate common attack vectors by scanning networks and systems for vulnerabilities, providing a realistic assessment of OWELK's monitoring capabilities.

We installed a local Nessus Docker image and performed a vulnerability scan in our test environment (see Figure 9). Figure 11 illustrates the scan process and the alerts generated by OWELK in response. The system successfully detected the Nessus scan and automatically

generated alerts that were visible in the alert dashboard. This demonstrates OWELK's ability to detect and report on activity that indicates potential security threats.

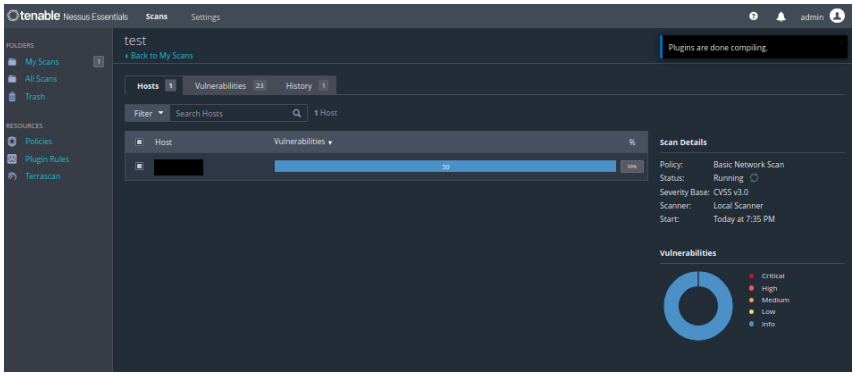


Figure 9: The scan results of Nessus

In addition to Nessus, we ran Nmap scans against the monitored system (see Figure 10). Nmap is widely used for network discovery and security auditing.

```
ocean@oPC:~$ sudo nmap -sS --top-ports 100 [redacted]
[sudo] Passwort für ocean:
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-13 18:55 CET
Nmap scan report for ns3238897.ip-[redacted] ([redacted])
Host is up (0.022s latency).
Not shown: 94 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
3000/tcp open   ppp
5060/tcp closed sip
8000/tcp open   http-alt

Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds
ocean@oPC:~$ sudo nmap -sV -p22,80,443,3000,5060,8000 [redacted]
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-13 18:55 CET
Nmap scan report for ns3238897.ip-[redacted] ([redacted])
Host is up (0.021s latency).

PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp   open   http     nginx 1.22.1
443/tcp  open   ssl/http nginx 1.22.1
3000/tcp open   http     Node.js Express framework
5060/tcp closed sip
8000/tcp open   http     nginx
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
ocean@oPC:~$ _
```

Figure 10: Running nmap scans on the target system

To further evaluate OWELK's performance in a real-world scenario, we installed a Wazuh agent on an Internet-facing Nginx web server. The system automatically generated alerts in response to external scanning attempts and potential intrusion activity. This indicates that OWELK can effectively monitor and detect security threats in a production environment and provide timely alerts for incident response.

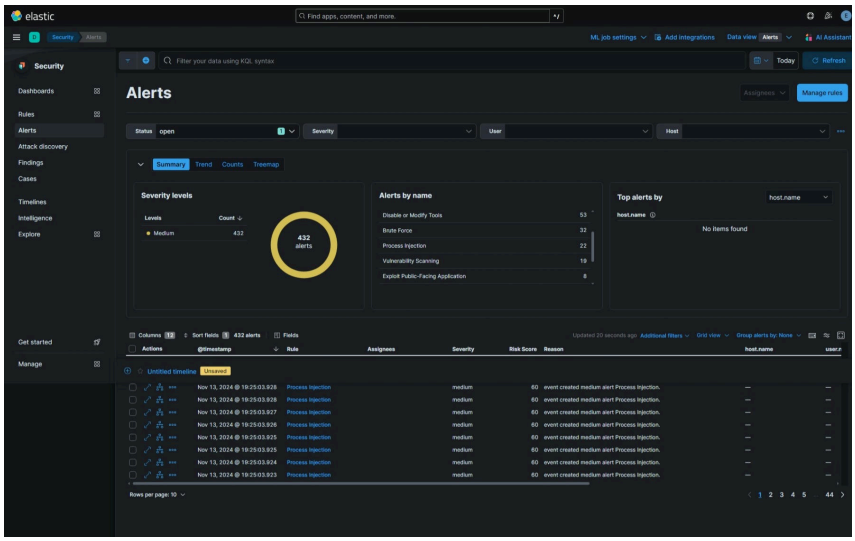


Figure 11: generated alerts by OWELK after running vulnerability scans

These tests confirm OWELK's ability to detect and alert on suspicious activity associated with common cyber attack methodologies. By identifying these threats early, organizations can take proactive steps to mitigate risk and improve their overall security posture. The successful detection of both simulated and real-world attacks underscores OWELK's effectiveness as a holistic network monitoring solution suitable for micro-enterprises.

### 4.3.11. Working with OWELK

After deploying OWELK and configuring the necessary agents and policies using our guide, users can leverage its capabilities to effectively monitor and secure their network infrastructure. The platform offers several key features:

- **Alert Dashboard with predefined rule sets**: The Alert Dashboard is the central interface for security monitoring. It uses our predefined rule sets to detect potential threats and anomalies in real time using the MITRE ATT%CK Framework. Users can respond to alerts directly in the dashboard, enabling rapid incident response and remediation.
- **Resource Monitoring with Kibana Dashboards**: OWELK integrates with Kibana to provide comprehensive dashboards for monitoring system resources. Administrators can track metrics such as CPU usage, memory usage, disk I/O, and network traffic to facilitate performance optimization and capacity planning.
- **Event Dashboard Overview**: The Event Dashboard provides a holistic view of all connected agents and the security events they report. This feature allows users to monitor the operational status of agents, review security events, and identify patterns or trends that may indicate underlying issues.

Beyond these core functionalities, OWELK encompasses a wide range of advanced features that, while beyond the scope of this paper, significantly enhance its utility:

- **Log Analysis**: Enables in-depth examination of logs for troubleshooting, auditing, and forensic investigations.
- **Configuration Management with Wazuh SCA Module**: Assesses system configurations against established security benchmarks and compliance standards to ensure adherence to best practices.
- **Vulnerability Assessment using the Wazuh Vulnerability Module**: Utilizes Wazuh's vulnerability module to detect and report known vulnerabilities across the network, aiding in proactive risk management.
- **Custom Agent Policies**: Supports the creation of tailored agent policies for different system groups, such as Docker containers, AWS instances, and web servers, to meet specific monitoring needs.
- **Integration of Additional Technologies**: OWELK's flexible architecture allows for the integration of other technologies, including additional IDS/IPS systems, NAS devices, firewalls, and more, enhancing its scalability and adaptability.

Organizations interested in exploring these advanced capabilities are encouraged to consult the official documentation for Wazuh and the Elastic Stack.

#### 4.3.12. False Positives

In our approach to developing a holistic network monitoring strategy for micro-enterprises, we recognize the importance of addressing false positives (FPs) within monitoring systems. However, given the diversity in network configurations and resource constraints specific to micro-enterprises, handling FPs with a one-size-fits-all solution is impractical. Each micro-enterprise operates within unique constraints—its network components, IT infrastructure, and user behaviors vary significantly, all of which influence how FPs are generated and managed.

B. A. Alahmadi, L. Axon, and I. Martinovic [50] paper on FPs provides valuable context here. Their analysis underscores how frequent FPs can overwhelm monitoring efforts, reduce trust in alerts, and potentially lead to the oversight of real threats. For micro-enterprises, which often lack dedicated IT security teams, the burden of managing FPs can be especially taxing. While larger organizations may have resources to fine-tune their systems and regularly adjust thresholds, micro-enterprises may not have this flexibility.

Our paper thus includes insights from B. A. Alahmadi, L. Axon, and I. Martinovic [50] to highlight the broader implications of FP management, reinforcing the importance of selecting

adaptable tools that can help alleviate FP issues by aligning with each enterprise's specific network and operational setup. This adaptability is central to our strategy, as it allows micro-enterprises to optimize their network monitoring without requiring complex FP handling mechanisms that may not be feasible given their resource limitations.

#### 4.3.13. Tailored Incident Response and the Role of Standardized Methodologies

Effective incident response is vital in mitigating the impact of cybersecurity incidents and ensuring rapid recovery. However, each organization's approach to incident response is unique, shaped by its specific operational environment, technology, and regulatory landscape. This chapter explores the importance of tailoring incident response to organizational needs and highlights the benefits of incorporating structured methodologies, particularly from Bundesamt für Sicherheit in der Informationstechnik [51]. Although incident response is not the core focus of this paper – which centers on network monitoring – understanding a standardized process can provide micro-businesses with valuable insights on how to build and implement such procedures effectively.

In our research, we focus on network monitoring strategies for micro-businesses, recognizing the importance of affordability, ease of use, and scalability. However, we include a reference to the BSI's DER.2.1 guidelines to offer an example of how an incident response process could be structured and implemented, especially relevant for micro-businesses with limited resources [51]. The BSI framework provides a structured, repeatable process adaptable to organizations of varying sizes, ensuring that even small enterprises can establish a foundational incident response approach.

BSI's standardized methodology offers benefits like defined processes, clear role assignments, and incident classification guidelines that can help micro-businesses streamline their response approach. This framework's emphasis on documentation, continuous improvement, and maintaining forensic evidence can support smaller businesses in legal compliance and resilience. Even though a detailed implementation of incident response is outside the scope of this paper, understanding the BSI framework offers valuable context for micro-businesses seeking to establish comprehensive security practices alongside network monitoring.

Integrating a structured approach like the BSI framework with tailored, business-specific insights helps ensure a balanced and effective incident response strategy. While the primary focus here remains on network monitoring, this reference to BSI standards encourages micro-businesses to consider structured incident response as part of a broader cybersecurity posture, enhancing resilience and enabling a coordinated, resource-appropriate response to incidents.

# 5. Discussion

The primary objective of this paper was to develop a holistic network monitoring strategy tailored specifically for micro-enterprises by leveraging Design Science Research (DSR) and Utility Analysis. By systematically evaluating open-source network security tools against criteria critical for micro-enterprises — such as cost, reliability, ease of installation, usability, scalability, and security features — we identified a cost-effective and scalable solution termed OWELK. OWELK integrates OPNsense as the firewall and IDS/IPS solution, the Elastic Stack as the SIEM system, and Wazuh for enhanced security monitoring.

Our findings highlight that cost and usability are paramount for micro-enterprises, receiving the highest weights in our utility analysis. The selection of open-source platforms like OPNsense and the Elastic Stack aligns with these priorities, offering functionalities without the financial burden of licensing fees. The implementation of OWELK demonstrated its effectiveness in enhancing the cybersecurity posture of micro-enterprises by providing real-time threat detection, comprehensive logging, and intuitive data visualization. Deploying agents on endpoints and servers facilitated detailed network monitoring, while configuring Index Lifecycle Management ensured sustainable operation by managing data retention and preventing resource exhaustion.

OWELK offers a viable path for implementing robust network monitoring without incurring prohibitive costs or requiring extensive technical expertise, thus addressing a critical gap in the cybersecurity landscape for small businesses. Our tests have shown that OWELK is able to detect potential cyber attacks and security incidents.

However, several limitations must be acknowledged. The generalizability of our findings is constrained by the specific network environment and configurations used in our implementation. Micro-enterprises vary widely in their network architectures, and our reference setup may not reflect all operational scenarios. While we minimized hardware requirements, deploying OWELK still necessitates a baseline level of computing resources, which may be challenging for organizations with extremely constrained resources. Additionally, the setup and maintenance of OWELK demand a certain level of technical expertise that may not be readily available in all micro-enterprises. The management of false positives in network monitoring remains a challenge that we did not extensively address, potentially impacting operational efficiency. Human factors, such as limited cybersecurity awareness and training, could also affect the effectiveness of the implemented solution.

Future research should aim to address these limitations by exploring methods to simplify the deployment and management of OWELK, such as automation scripts, containerization using technologies such as Docker and Kubernetes, or the development of user-friendly installation wizards to reduce the technical burden. Improving incident management capabilities within OWELK, possibly by incorporating standardized methodologies tailored to the needs of microenterprises, would improve their ability to respond effectively to security incidents. In addition, addressing the challenge of managing false positives through adaptive algorithms or machine learning techniques could improve operational efficiency by reducing unnecessary alerts. Studies evaluating the effectiveness of OWELK in various real-world environments would provide deeper insights into its practical applicability and scalability.

In this context, this paper demonstrates that a carefully selected and integrated set of open source tools can provide micro-enterprises with a network monitoring strategy. By tailoring the solution to their specific needs and constraints – particularly in terms of cost and usability – we provide a viable and cost-effective way for these organisations to improve their cybersecurity resilience in an increasingly risky digital landscape. OWELK enables micro businesses to detect cyber threats.

# 6. Conclusion

This paper successfully developed a holistic network monitoring strategy tailored for micro-enterprises by utilizing Utility Analysis and Design Science Research (DSR). Recognizing that micro-enterprises—businesses with fewer than ten employees—are integral to global economies yet often lack the resources and expertise to implement robust cybersecurity measures, we aimed to address their unique challenges.

By examining the characteristics and security challenges specific to micro-enterprises, we underscored the necessity for affordable, scalable, and user-friendly network security solutions. Micro-enterprises face heightened vulnerabilities due to limited resources, lack of technical expertise, and minimal understanding of digital security practices. Traditional security systems are often complex and costly, rendering them unsuitable for these organizations. Our approach addressed this gap by employing utility analysis to evaluate various network monitoring tools against criteria critical for micro-enterprises—cost, reliability, ease of installation, usability, scalability, and security features.

The application of DSR provided a structured methodology to design and develop an artifact that meets the specific needs of micro-enterprises. Through iterative rounds of evaluation and refinement, we identified and integrated open-source tools—OPNsense, Wazuh, Elasticsearch, Logstash, and Kibana—forming the OWELK stack. This integrated solution offers comprehensive network security monitoring, intrusion detection and prevention, log management, and data visualization capabilities. It aligns with the basics and objectives of network monitoring by providing real-time insights into network operations, enabling proactive threat detection and system optimization.

Our implementation demonstrated that OWELK effectively enhances the cybersecurity posture of micro-enterprises. By deploying agents on endpoints and servers, we facilitated detailed monitoring across the network, capturing metrics and security events. The use of open-source technologies minimized costs without compromising functionality or scalability —a critical consideration given the financial constraints highlighted in our fundamentals. Additionally, configuring Index Lifecycle Management ensured sustainable operation by effectively managing data retention and resource utilization.

This paper can help improve the cybersecurity posture of micro-enterprises that are committed to strengthening their cybersecurity defences. It fills a critical gap in the cybersecurity landscape for micro businesses, providing a solution that is not only technically sound, but also accessible and manageable for organizations with limited resources.

However, we acknowledge certain limitations. The generalizability of our findings may be constrained by the specific network environments and configurations used in our implementation. While we minimized hardware requirements, micro-enterprises with extremely limited resources might still face challenges in deploying the OWELK stack. The setup and maintenance of such a system require a basic level of technical expertise, which may not be readily available in all micro-enterprises. Furthermore, human factors such as limited cybersecurity training and awareness, as discussed in our fundamentals, could affect the effectiveness of the implemented solution.

In this paper, we demonstrate that a carefully selected and integrated set of open source tools can provide micro-enterprises with a network monitoring strategy. By addressing the unique challenges that micro-enterprises face - limited resources, lack of technical expertise, and heightened vulnerability to cyber threats - and leveraging utility analysis and design science research, we provide a viable solution for improving their cybersecurity resilience. The OWELK stack is a step toward empowering micro-enterprises to protect themselves in an increasingly complex digital landscape. By helping these organizations implement effective network monitoring and security measures, we aim to enhance the cybersecurity of individual microenterprises and support the resilience of this important business sector.

# 7. Attachment A – Installation of OWELK

## 7.1. Preparation

- First, the system is updated and prepared for Docker operation:
- The following file is edited first: ‘nano /etc/sysctl.conf’
- Then the following is added: vm.max_map_count=262144
- The file is saved and closed. The following commands are executed:

```bash
apt update; sudo apt upgrade -y
apt install docker
apt install docker-compose
systemctl start docker
```

Listing 1: Preparation before install

Then the firewall is configured:

```bash
apt install ufw
ufw enable
ufw allow 1514
ufw allow 1515
ufw allow 1515
ufw allow 9200
ufw allow 55000
```

Listing 2: Firewall configuration

## 7.2. Installation of Wazuh

Now we install Wazuh:

```bash
cd /opt/
git clone https://github.com/wazuh/wazuh-docker.git -b v4.9.1
cd wazuh-docker/single-node/
docker-compose -f generate-indexer-certs.yml run --rm generator
docker-compose up -d
```

Listing 3: Wazuh installation

## 7.3. Cronjobs for log forwarding to Wazuh

```Bash
apt install cron
systemctl enable cron
systemctl start cron
cd /root/
mkdir logs
```

Listing 4: Cronjobs for log forwarding to Wazuh

- Enter the following command: crontab -e
- Add the following to crontab: */5 * * * * docker cp single-node_wazuh.manager_1:/var/ossec/logs/alerts/alerts.json /root/logs/
- Then: systemctl restart cron

## 7.4. Installation of Logstash

```Bash
cd /etc/
mkdir /etc/sysconfig
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic-keyring.gpg
sudo apt-get install apt-transport-https
echo "deb [signed-by=/usr/share/keyrings/elastic-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list
sudo apt-get update && sudo apt-get install logstash
cd /etc/logstash/
mkdir certs
```

Listing 5: Installing Logstash

## 7.5. Configuration of Logstash

- Now we copy the Elasticsearch CA to the following directory and set the following permissions: chmod -R 755 CA.crt and change the permissions: chown logstash:logstash CA.crt (and the directory where the file is located chown logstash:logstash /etc/logstash/certs).
- Then run the following commands:

```
sudo /usr/share/logstash/bin/logstash-plugin install logstash-output-elasticsearch
sudo chmod -R 755 /etc/logstash/certs/elastic-ca.crt
sudo mkdir /etc/logstash/templates
sudo curl -o /etc/logstash/templates/wazuh.json https://packages.wazuh.com/integrations/elastic/4.x-8.x/dashboards/wz-es-4.x-8.x-template.json
echo 'LOGSTASH_KEYSTORE_PASS="k3txcvSJGNsdjfkn#asd#"' | sudo tee /etc/sysconfig/logstash
export LOGSTASH_KEYSTORE_PASS=k3txcvSJGNsdjfkn#asd#
sudo chown root /etc/sysconfig/logstash
sudo chmod 600 /etc/sysconfig/logstash
sudo systemctl start logstash
```

Listing 6: Logstash installation

In the next step, we enter the elasticsearch username and password:

```
sudo -E /usr/share/logstash/bin/logstash-keystore --path.settings /etc/logstash create
sudo -E /usr/share/logstash/bin/logstash-keystore --path.settings /etc/logstash add ELASTICSEARCH_USERNAME
sudo -E /usr/share/logstash/bin/logstash-keystore --path.settings /etc/logstash add ELASTICSEARCH_PASSWORD
```

Listing 7: Logstash – Entering Elasticsearch username and password

Then we continue with the following commands:

```
sudo touch /etc/logstash/conf.d/wazuh-elasticsearch.conf
sudo systemctl stop logstash
sudo systemctl enable logstash.service
sudo systemctl start logstash.service
```

Listing 8: Logstash – Entering Elasticsearch username and password follow up

## 7.6. Installation of Elasticsearch and Kibana

First, we need to prepare the system for the Elastic Stack:

```bash
sudo apt update; sudo apt upgrade -y
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
sudo apt-get install apt-transport-https
sudo apt install unzip
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
```

Listing 9: Preparation of installing Elasticsearch and Kibana

Now we will open the necessary ports on the server that are required for the Elastic Stack to function correctly:

```bash
ufw enable
ufw allow 9200
ufw allow 5601
ufw allow 8220
```

Listing 10: Firewall configuration for Elasticsearch

Now we install both elasticsearch and kibana

IMPORTANT: Once elasticsearch is installed, the terminal will display the login data for the elasticsearch user. Save it!

```bash
sudo apt-get update && sudo apt-get install elasticsearch
sudo apt-get update && sudo apt-get install kibana
```

Listing 11: Installation of Elasticsearch and Kibana

- Now we need to configure Elasticsearch
- The Elasticsearch configuration files are located at /etc/elasticsearch/
- We need to configure the following file: elasticsearch.yml
- Add the following fields to the configuration file (IMPORTANT: replace the IP address with the server's IP address):

```yaml
cluster.name: ELK
network.host: 192.168.100.10
http.port: 9200
```

Listing 12: Starting Elasticsearch for the first time

- After we have made the changes and saved the file, we start elasticsearch: sudo systemctl start elasticsearch.
- Check the availability of elasticsearch at: https://192.168.100.10:9200 (replace this with the server's IP address)
- Ignore the warning and continue
- Enter the elastic user data (it was automatically generated earlier. See step 4)
- Stop Elasticsearch: sudo systemctl stop elasticsearch
- Now we will install the SSL certificates so that the connection to our Elastic instance is encrypted.
- Install the certificates:

```Bash
cd /etc/elasticsearch/certs/
/usr/share/elasticsearch/bin/elasticsearch-certutil ca --pem --out /etc/elasticsearch/certs/ca.zip
unzip ca.zip
/usr/share/elasticsearch/bin/elasticsearch-certutil cert --out /etc/elasticsearch/certs/elastic.zip --name elastic --ca-cert /etc/elasticsearch/certs/ca/ca.crt --ca-key /etc/elasticsearch/certs/ca/ca.key --ip 192.168.100.10 --pem
cd /etc/elasticsearch/certs/
unzip elastic.zip
chown -R elasticsearch:elasticsearch .
sudo systemctl daemon-reload
```

Listing 13: Provision of Certificates

Open the elasticsearch.yml again and add the following fields:

```YAML
certificate: /etc/elasticsearch/certs/elastic/elastic.crt
key: /etc/elasticsearch/certs/elastic/elastic.key
certificate_authorities: /etc/elasticsearch/certs/ca/ca.crt
```

Listing 14: Starting Elasticsearch for the first time

- After we have made the changes and saved the file, we start elasticsearch: sudo systemctl start elasticsearch

- Access elasticsearch via the browser: https://192.168.100.10:9200 (replace with the server's IP address)
- And check the SSL certificate. It should now be provided.
- Now that elasticsearch is running, let's repeat this process for kibana.
- First, stop elasticsearch: sudo systemctl stop elasticsearch
- Then run the following commands (replace the IP with the server's IP):

```
cd /etc/kibana
mkdir certs/
cd certs/
mkdir elastic
/usr/share/elasticsearch/bin/elasticsearch-certutil cert --out /etc/kibana/certs/kibana.zip --name kibana --ca-cert /etc/elasticsearch/certs/ca/ca.crt --ca-key /etc/elasticsearch/certs/ca/ca.key --ip 192.168.100.10 --pem
unzip kibana.zip
cp /etc/elasticsearch/certs/ca/* /etc/kibana/certs/elastic/
cd /etc/elasticsearch/
chown -R elasticsearch:elasticsearch .
cd /etc/kibana/
chown -R kibana:kibana ./
```

Bash

Listing 15: Providing certificates to Kibana

Now we will create the Kibana keystore for secure authentication between elasticsearch and Kibana (SAVE THE TOKEN):

```
/usr/share/elasticsearch/bin/elasticsearch-service-tokens create elastic/kibana kibana_token
cd /etc/elasticsearch/
chown -R elasticsearch:elasticsearch service_tokens

/usr/share/kibana/bin/kibana-keystore add elasticsearch.serviceAccountToken
cd /etc/kibana/
chown -R kibana:kibana ./
```

Bash

Listing 16: Kibana Keystore

```yaml
server.port: 5601
server.host: "0.0.0.0"
server.publicBaseUrl: "https://192.168.100.10:5601"

server.ssl.enabled: true
server.ssl.certificateAuthorities: ["/etc/kibana/certs/elastic/ca.crt"]
server.ssl.certificate: /etc/kibana/certs/kibana/kibana.crt
server.ssl.key: /etc/kibana/certs/kibana/kibana.key
elasticsearch.hosts: ["https://192.168.100.10:9200"]

elasticsearch.ssl.certificateAuthorities: [ "/etc/kibana/certs/elastic/ca.crt" ]
elasticsearch.ssl.verificationMode: full
```

Listing 17: Configuration of Kibana

- Start elasticsearch: sudo systemctl start elasticsearch
- Start kibana: sudo systemctl start kibana

First, we need to create new SSL certificates for the fleet server:

```bash
cd /etc/
mkdir certs/
cd certs/
mkdir elastic/
cp /etc/elasticsearch/certs/ca/ca.crt elastic/
/usr/share/elasticsearch/bin/elasticsearch-certutil cert --out /etc/certs/fleet.zip --name fleet --ca-cert /etc/elasticsearch/certs/ca/ca.crt --ca-key /etc/elasticsearch/certs/ca/ca.key --ip 192.168.100.10 --pem
cd /etc/certs/
unzip fleet.zip
```

Listing 18: Installation of Fleet Servers

1. Then we perform the following steps:
2. Go to the Kibana Dashboard -> Open Menu -> Fleet -> Settings -> Outputs -> Edit
3. Change Hosts: https://192.168.100.10:9200
4. Advanced YAML Configuration: ssl.certificate_authorities: [“/etc/certs/elastic/ca.crt”]
5. Save and apply settings
6. Go to Agents
7. Click on Add Fleet Server -> Advanced -> Create policy -> Production -> Name: fleet -> URL: https://192.168.100.10:8220 -> Add host -> Generate Service Token

8. We then get a command and we save it
9. We then execute the following commands:

```bash
cd /root/
touch install.sh
chmod 755 install.sh
```

Listing 19: Installation of Fleet Servers 2

We open this new file with nano install.sh and copy the installation command:

```bash
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.3-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.15.3-linux-x86_64.tar.gz
cd elastic-agent-8.15.3-linux-x86_64
sudo ./elastic-agent install --url=https://192.168.100.10:8220 \
  --fleet-server-es=https://192.168.100.10:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3MjkzMjU4NDM3NTk6S1k3TTg2U2tUNzJ6 \
  --fleet-server-policy=fleet-server-policy \
  --certificate-authorities=/etc/certs/elastic/ca.crt \
  --fleet-server-es-ca=/etc/certs/elastic/ca.crt \
  --fleet-server-cert=/etc/certs/fleet/fleet.crt \
  --fleet-server-cert-key=/etc/certs/fleet/fleet.key \
  --fleet-server-port=8220
```

Listing 20: Installation of Fleet Servers 3

- Now we will install the Kibana encryption keys: /usr/share/kibana/bin/kibana-encryption-keys
- We receive an output in the terminal
- We add these keys to the file kibana.yml:

```yaml
xpack.encryptedSavedObjects.encryptionKey: 26b693e4a6bde560069207dabe49a865
xpack.reporting.encryptionKey: 409f2b25ec999c70dcc64a441a1436ec
xpack.security.encryptionKey: 0784cd5158afe89ec71e684972625062
```

Listing 21: Configuration of Kibana

- Then we start Kibana: systemctl restart kibana
- Both Elasticsearch and Kibana are now ready for use. The installation is complete.

# References


[1] G. G. Inan and U. S. Bititci, "Understanding organizational capabilities and dynamic capabilities in the context of micro enterprises: a research agenda," *Procedia-Social and Behavioral Sciences*, vol. 210, pp. 310–319, 2015.

[2] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

[3] S. A. Aljawarneh, "Cloud Security Engineering: Avoiding Security Threats the Right Way," *Int. J. Cloud Appl. Comput.*, vol. 1, no. 2, pp. 64–70, 2011, doi: 10.4018/IJCAC.2011040105.

[4] Wazuh Inc., "Quickstart · Wazuh documentation," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://documentation.wazuh.com/current/quickstart.html

[5] OPNsense, "Hardware sizing & setup — OPNsense documentation," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://docs.opnsense.org/manual/hardware.html

[6] Elasticsearch B.V., "Hardware prerequisites | Elastic Cloud Enterprise Reference [3.7] | Elastic," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://www.elastic.co/guide/en/cloud-enterprise/current/ece-hardware-prereq.html

[7] A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi, "Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors," *Risk Analysis*, vol. 43, no. 10, pp. 2082–2098, 2023.

[8] S. Kandpal, S. Bhatt, L. Mohan, A. Patwal, and P. Kumar, "Cyber Security Implementation Issues in Small to Medium-sized Enterprises (SMEs) and their Potential Solutions: A Comprehensive Analysis," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, pp. 1–5. doi: 10.1109/ICCCNT56998.2023.10307363.

[9] A. Gupta and R. Hammond, "Information systems security issues and decisions for small businesses: An empirical examination," *Inf. Manag. Comput. Security*, vol. 13, pp. 297–310, 2005, doi: 10.1108/09685220510614425.

[10] A. F. J. A. M. Jawad Manzoor Abdul Waleed, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," 2024, doi: https://doi.org/10.1371/journal.pone.0301183.

[11] S. Lee, K. Levanti, and H. S. Kim, "Network monitoring: Present and future," *Computer Networks*, vol. 65, pp. 84–98, 2014.

[12] VMware, "What Is Network Monitoring?." Accessed: Nov. 05, 2024. [Online]. Available: https://www.vmware.com/topics/network-monitoring

[13] L. Cottrell, "Passive vs. active monitoring," *Retrieved June*, vol. 20, p. 2014, 2001.

[14] J. Svoboda, I. Ghafir, V. Prenosil, and others, "Network monitoring approaches: An overview," *Int J Adv Comput Netw Secur*, vol. 5, no. 2, pp. 88–93, 2015.

[15] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, 2021.

[16] J. Pavlik, A. Komarek, and V. Sobeslav, "Security information and event management in the cloud computing infrastructure," in *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*, 2014, pp. 209–214.

[17] A. Sawant, "A comparative study of different intrusion prevention systems," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1–5.

[18] K. SCARFONE, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST special publication*, 2007.

[19] W. R. Cheswick, *Firewalls And Internet Security: Repelling The Wily Hacker, 2/E*. Pearson Education India, 2003.

[20] W. Stallings and L. Brown, *Computer security: principles and practice*. Pearson, 2015.

[21] X. Li, Z.-Z. Ji, and M.-Z. Hu, "Stateful Inspection firewall session table processing," in *International Conference on Information Technology: Coding and Computing (ITCC'05)-Volume II*, 2005, pp. 615–620.

[22] K. Neupane, R. Haddad, and L. Chen, "Next generation firewall for network security: a survey," in *SoutheastCon 2018*, 2018, pp. 1–6.

[23] O. Mukhoryanova, L. Kuleshova, N. Rusakova, and O. Mirgorodskaya, "Sustainability of micro-enterprises in the digital economy," in *E3S Web of Conferences*, 2021, p. 6008.

[24] E. European Union Agency for Cybersecurity, *CYBERSECURITY FOR SMES*. 2021.

[25] Verizon Business, *2021 Data Breach Investigations Report*. 2021.

[26] C. R. Junior, I. Becker, and S. Johnson, "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity." [Online]. Available: https://arxiv.org/abs/2309.17186

[27] R. Bejtlich, *The practice of network security monitoring: understanding incident detection and response*. No Starch Press, 2013.

[28] K. SCARFONE, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST special publication*, 2007.

[29] P. Stephenson, J. Killmeyer, J. S. Tiller, and B. Rothke, *Information security architecture: an integrated approach to security in the organization*. Auerbach Publications, 2006.

[30] M. Mkansi, "E-business adoption costs and strategies for retail micro businesses," *Electronic Commerce Research*, vol. 22, no. 4, pp. 1153–1193, 2022.

[31] J. O. De Sordi, *Design science research methodology: theory development from artifacts*. Springer Nature, 2021.

[32] A. Cartwright, E. Cartwright, and E. S. Edun, "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," *Computers & Security*, vol. 131, p. 103288, 2023.

[33] Sophos, "The State of Ransomware 2023," 2023. [Online]. Available: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

[34] T. Chimucheka and F. Mandipaka, "Challenges faced by small, medium and micro enterprises in the Nkonkobe Municipality," *The international business & economics research journal (Online)*, vol. 14, no. 2, p. 309, 2015.

[35] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS quarterly*, pp. 75–105, 2004.

[36] S. Seidel, J. Recker, and J. Vom Brocke, "Sensemaking and sustainable practicing: Functional affordances of information systems in green transformations," *MIS quarterly*, pp. 1275–1299, 2013.

[37] J. Becker, J. Vom Brocke, M. Heddier, and S. Seidel, "In search of information systems (grand) challenges: A community of inquirers perspective," *Business & Information Systems Engineering*, vol. 57, pp. 377–390, 2015.

[38] S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact," *MIS quarterly*, pp. 337–355, 2013.

[39] J. Vom Brocke, A. Hevner, and A. Maedche, "Introduction to design science research," *Design science research. Cases*, pp. 1–13, 2020.

[40] J. B. Kühnapfel, "Scoring und Nutzwertanalysen," *Ein Leitfaden für die Praxis. Wiesbaden et al: Springer Gabler*, 2021.

[41] OPNsense, "OPNsense - a true open source firewall and more," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://opnsense.org/

[42] Wazuh Inc., "Wazuh Open Source XDR," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://wazuh.com/

[43] Elasticsearch B.V., "Elasticsearch: The Official Distributed Search & Analytics Engine | Elastic," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://www.elastic.co/elasticsearch

[44] Elasticsearch B.V., "Logstash: Collect, Parse, Transform Logs | Elastic," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://www.elastic.co/logstash

[45] Elasticsearch B.V., "Kibana: Explore, Visualize, Discover Data | Elastic," 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://www.elastic.co/kibana

[46] Wazuh Inc., "Wazuh - Installation Alternatives." Accessed: Nov. 09, 2024. [Online]. Available: https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

[47] O. Ayik, O. Buchmann, and F. Kohn, “University research project - OWELK (Opnsense, Wazuh, Elasticsearch, Logstash, Kibana),” 2024. Accessed: Nov. 09, 2024. [Online]. Available: https://github.com/cryptocean22/research-project

[48] Wazuh Inc., “Architecture - Getting started with Wazuh · Wazuh documentation,” 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://documentation.wazuh.com/current/getting-started/architecture.html

[49] Elasticsearch B.V., “Installing the Elastic Stack | Elastic Installation and Upgrade Guide [8.15] | Elastic,” 2024, Accessed: Nov. 05, 2024. [Online]. Available: https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html

[50] B. A. Alahmadi, L. Axon, and I. Martinovic, “99% false positives: A qualitative study of {SOC} analysts' perspectives on security alarms”, in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 2783–2800.

[51] Bundesamt für Sicherheit in der Informationstechnik, “DER.2.1 Behandlung von Sicherheitsvorfällen.” Accessed: Nov. 09, 2024. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2023.pdf?__blob=publicationFile&v=3