A SECURITY OPERATIONS AND ANALYTICS FRAMEWORK: CONTINUOUS DETECTION AND RESPONSE

GEORGE AYITTEY

A thesis submitted in partial fulfilment of the requirements of the University of East London for the degree of Professional Doctorate in Information Security

August 2024

Abstract

Security operations face several challenges, including the increasing volume and complexity of security data, limited analyst resources, and sophisticated cyber threats. This study is motivated by three main factors: the need to utilise advanced technologies, improve operational efficiency, and apply theoretical progress to practical cybersecurity solutions.

To address these issues, this study proposes a Security Operations and Analytics Framework (SOAF) emphasising automation and continuous detection and response. The framework integrates tools such as Wazuh, Elasticsearch, Kibana, TheHive and Cortex within a Security Operations and Analytics Platform (SOAP), leveraging AI, machine learning, and automation to enhance cybersecurity operations.

The effectiveness of the SOAF is evaluated using a design science research methodology. Two case studies demonstrate the framework's ability to reduce incident response times from three hours to one hour, increase detection accuracy by 80%, and streamline threat detection, analysis, and incident response operations.

The study concludes by analysing its findings, discussing the consequences, acknowledging constraints, and providing actionable recommendations for future research. The implementation of the SOAF showcases key functionalities in a practical setting, highlighting the framework's theoretical and practical contributions to advancing security operations and analytics.

Contents

List of Figures

List of Tables

List of Acronyms

CDR: Continuous Detection and Response

CTI: Cyber Threat Intelligence

DDoS: Distributed Denial of Service

DR: Disaster Recovery

DSR: Design Science Research

EDR: Endpoint Detection and Response

EHR: Electronic Health Record

FIM: File Integrity Monitoring

GDPR: General Data Protection Regulation

GOV: Government

HIDS: Host-based Intrusion Detection System

IAM: Identity and Access Management

IDS/IPS: Intrusion Detection/Prevention Systems

IM: Instant Messaging

IP: Internet Protocol

KPI: Key Performance Indicator

MFA: Multi-Factor Authentication

MISP: Malware Information Sharing Platform

MITRE: Mitre Corporation's cybersecurity framework

MTTD: Mean Time to Detect

MTTR: Mean Time to Respond

NTA: Network Traffic Analysis

NIST: National Institute of Standards and Technology

RBAC: Role-Based Access Control

RQ: Research Question

SEM: Security Event Management

SIEM: Security Information and Event Management

SIM: Security Information Management

SME: Small and medium-sized enterprise

SOAF: Security Operations and Analytics Framework

SOAP: Security Operations and Analytics Platform

SOAR: Security Orchestration, Automation, and Response

UEBA: User and Entity Behaviour Analytics

UI: User Interface

XDR: Extended Detection and Response

Chapter 1: Introduction

Increasingly, more technological devices require an internet connection. Networking is no longer just for computers. As technology advances, more of our devices at home or work, for example, the Internet of Things (IoT), are connected to the Internet (Mishra and Tyagi, 2022). The importance of safely connected internet devices cannot be overstated at home or work. Cyber threats introduced due to this integration are everywhere in our modern digital society. Increased cyberattacks involving artificial intelligence (AI) could influence human targets on a large scale within the attack surface of major social systems. There are also risks of disaster when hackers' technical skills are transferred to algorithms (Whyte, 2020). These threats constantly evolve and become more complex, making it increasingly difficult to protect ourselves. Organisations of all sizes face significant risks from these threats, highlighting the need for stringent cybersecurity protocols to protect their valuable assets and sensitive data. Regarding defence, traditional reactive cybersecurity solutions cannot keep up with cyber-attacks. To combat this, threat intelligence helps users make faster, more informed, data-backed security decisions and change their behaviour from reactive to proactive to fight threat actors (Sun *et al.*, 2023).

SOAF has emerged as a complete approach to tackling these issues, enabling organisations to continuously detect, analyse, respond to, and mitigate cyber threats and incidents effectively in near real-time. Furthermore, this innovative platform gives an improved view of the whole company, eliminating alert fatigue and revealing security gaps so that security teams can take the initiative to make the company more cyber-resilient.

This chapter sets the stage for the study by providing a comprehensive background, contextualising the research within the cybersecurity landscape, and outlining the motivations that drive the exploration of the SOAF. It uses a Security Operations and Analytics Platform (SOAP) comprising Wazuh, Elasticsearch, Kibana, TheHive, and Cortex for automation and Continuous Detection and Response (CDR).

1.1 Background and Motivation

The rapid digital transformation of the modern world has made interconnectivity between internet-enabled devices easier. However, it has also created an extensive and evolving cyberattack landscape. For present-day interconnected infrastructure to function correctly, secure technologies are required. The concept of security encompasses the

specific objectives of confidentiality, integrity, and availability, ensuring that data is only accessible to authorised users. These aims also guarantee data integrity and enable data retrieval on demand. This concept is expanded by the National Institute of Standards and Technology (NIST) to encompass the processes of protection, detection, identification, response, and recovery (Staves *et al.*, 2022).

In recent years, the field of cybersecurity has gotten more intricate and multifaceted due to the growing number of sophisticated cyber threats and attacks, which are continuously changing (Tounsi and Rais, 2018). As organisations continue to depend on technology to conduct their operations, the security of their digital assets becomes increasingly vital. As a result, organisations are constantly pressured to protect their digital assets and maintain their information systems' confidentiality, integrity, and availability to avoid significant consequences because of cybersecurity breaches, including financial loss, reputational harm, and theft of proprietary data and consumer information. There is an upward trend in the scale of cyber threats, and the merger of formerly different forms of attack into more destructive forms gives rise to a more complex form of attack (Thakur, 2024). Moreover, a low threat detection rate undermines information security. This problem has increased globally and is now a significant issue.

Attack vectors have evolved from simple viruses to advanced persistent threats (APT), ransomware attacks, and zero-day exploits. Cybercrime-as-a-service and AI in offensive tools have significantly boosted the speed, complexity, and effectiveness of cybersecurity assaults (Manky, 2013; Malatji, 2023; Singh and Rahman, 2023; Malatji and Tolah, 2024). Cybercriminals, driven by financial gain, political motives, or state-sponsored activities, constantly refine their techniques to evade traditional security measures. This dynamic landscape calls for a paradigm shift in cybersecurity strategies, prompting organisations to adopt proactive and integrated approaches that leverage advanced technologies and methodologies to mitigate risks and respond swiftly.

There has been a significant investment in cybersecurity products to improve cyber defence posture (Lee, 2021). However, gaps exist due to the expanding scope and sophistication of cybersecurity threats. Moreover, there are currently ineffective systems for detecting and responding to breaches (Jeong *et al.*, 2021). Security breaches can lead to data loss, reputational damage, and financial loss, and traditional security measures are no longer adequate to prevent sophisticated attacks. The dynamic and constantly changing

nature of potential dangers and the growing complexity of cyber assaults have necessitated a more proactive and adaptive approach to cybersecurity.

The competence of hackers demands a comprehensive strategy in the fight against threats. Security Operations Centers (SOC) provide this defence strategy by consolidating various specialised operational security measures, tools, and techniques to monitor, detect, and respond to cybersecurity threats and potential security incidents (Demertzis et al., 2019). However, the increasing volume and sophistication of cyber threats, coupled with a shortage of skilled cybersecurity professionals, can potentially overwhelm SOCs, leading to slower response times and increased risk (Brilingaitė, Bukauskas and Juozapavičius, 2020; Ali *et al.*, 2022). Furthermore, looking at the big picture of security defenders, industry studies and academic research have shown that security capabilities are not only about technology; people and other non-technical measures are also essential (Tang, Li and Zhang, 2016).

Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex into a unified Security Operations and Analytics Framework (SOAF) allows organisations to strengthen their cybersecurity posture. By deploying automation and continuous detection and response, this framework will transform how organisations approach cyber threats, streamlining incident management, improving decision-making, and enhancing operational efficiency.

The motivation for this study is driven by three key factors: technological advancement, operational efficiency, and real-world impact. First, the SOAF leverages advanced technologies to provide an adaptive cybersecurity approach, enabling organisations to stay ahead of emerging threats. Second, automation and continuous detection play a crucial role in enhancing operational efficiency. By improving response times, mitigating risks, and optimising resource utilisation, these capabilities strengthen an organisation's overall cybersecurity posture. Lastly, this research seeks to bridge the gap between theory and practice by evaluating the effectiveness of SOAF, which integrates tools such as Wazuh, Elasticsearch, Kibana, TheHive, and Cortex.

1.2 Problem Statement

The field of cybersecurity requires constant vigilance and innovation to combat the escalating threat landscape, which poses a critical challenge to organisations' computer networks and information systems (Ghelani, 2022).

The complexity and sophistication of cyber threats are growing, with APT emerging as significant challenges due to their stealth, persistence, and ability to evade traditional antivirus solutions. These attacks have driven increased investment in protective technologies, expected to grow from $6.9 billion in 2022 to $15.2 billion by 2026 (Ahmed, Asyhari and Rahman, 2021).

Despite such advancements, security operations often grapple with fragmented architectures, manual processes, and insufficient real-time visibility, exacerbating vulnerabilities and response inefficiencies (Forrester Study, 2020; GOV.UK, 2023). Moreover, organisations face challenges in integrating diverse security tools into cohesive operational frameworks. The increasing reliance on security analytics and machine learning has highlighted their potential to mitigate these issues by offering real-time threat detection, incident response, and predictive analysis (Xin *et al.*, 2018). However, practical implementation and empirical evaluation of such integrated systems remain underexplored (Catal *et al.*, 2023).

Traditional approaches to incident response, which rely on manual intervention, are time-consuming and prone to error, leaving organisations vulnerable to rapidly evolving threats (Anson, 2020; A. Ahmad *et al.*, 2021). A pressing concern is the lack of a comprehensive SOAF integrating tools like Wazuh, Elasticsearch, Kibana, TheHive, and Cortex into a unified platform. Current solutions are often costly or lack the customisation required to meet diverse organisational needs (Li, Nguyen and Xie, 2017). This results in fragmented processes, alert fatigue, and limited scalability, hindering the ability to address modern security challenges effectively (Agyepong *et al.*, 2020; Vielberth, Böhm and Fichtinger, 2020).

This research proposes developing an integrated SOAF that leverages automation and continuous detection and response capabilities. By unifying tools like Wazuh for extended detection and response, Elasticsearch for data organisation, Kibana for visualisation, TheHive for incident management, and Cortex for threat intelligence, this framework aims to offer organisations a centralised, proactive cybersecurity solution. It emphasises seamless tool integration, real-time data analysis, and automated responses to

mitigate threats effectively, ultimately enhancing security posture and operational efficiency.

1.3 Aim and Objectives

The primary aim of this research is to design, implement, and evaluate the effectiveness of a comprehensive SOAF. This framework leverages the capabilities of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex within a SOAP to enhance automation and improve CDR in cybersecurity operations. Additionally, the research investigates how integrating these tools contributes to operational efficiency, threat detection, and incident response in a dynamic cybersecurity environment.

To achieve this aim, the research focuses on the following specific objectives:

Literature Review - Review existing studies on SOAP and its components to establish a theoretical foundation.

Framework Design - Design a scalable architecture capable of efficiently handling large volumes of security data.

Development and Implementation - Develop automated rules and responses for incident management. Implement and monitor the framework in a corporate case study setting.

Data Collection and Performance Evaluation - Collect and analyse data on the platform’s usage, performance, and effectiveness in detecting and responding to cyber threats. Measure key performance indicators (KPIs) such as incident reduction, threat detection accuracy, and response time improvements.

Customisation and Usability - Customise the framework to meet organisations' unique needs, ensuring a user-friendly interface for security analysts and incident responders.

Best Practices and Recommendations - Identify and document best practices for implementing and optimising SOAP for SOAF. Provide actionable recommendations for scaling and maintaining system performance.

For the framework goals, the SOAF aims to:

Integrate and centralise security data from diverse sources, providing a unified, real-time view of the organisation's security posture.

Implement intelligent automation to triage, monitor, detect, and respond to security incidents, reducing response times and mitigating risks.

Enhance threat intelligence and hunting capabilities for proactive identification of emerging threats.

Optimise alert management to reduce noise and prioritise high-severity alerts.

Improve scalability to handle growing volumes of security data while maintaining performance.

Enable seamless collaboration and information sharing among stakeholders, including security analysts, managers, and auditors.

The study uses the following KPIs to evaluate the framework's success:

Incident Reduction: Reduce the number of security incidents and breaches by at least 50%.

Threat Detection: Increase the accuracy and timeliness of threat detection and response by 80%.

User Satisfaction: Achieve a user satisfaction score of at least 90%.

This research delivers a robust SOAF, empowering organisations to bolster their cybersecurity posture, respond effectively to incidents, and adapt to the evolving threat landscape.

1.4 Significance of the Study

Cybersecurity threats continually evolve, becoming increasingly sophisticated and challenging traditional defence mechanisms (K. McLaughlin, 2023). This complexity underscores the need for a proactive and integrated approach to safeguarding digital assets (Argyroudis *et al.*, 2022; Mclaughlin and Elliott, 2023). In this context, adopting a SOAF is a critical step toward enhancing cybersecurity resilience. By leveraging a comprehensive SOAP, organisations can achieve automation, continuous detection, and rapid response, fortifying their defences against modern cyber threats.

This study makes several significant contributions to the cybersecurity body of knowledge. First, it provides a deeper understanding of the evolving security landscape and highlights the limitations of traditional approaches to cyber defence. Through the integration of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, the research demonstrates how a unified framework can streamline security operations, improve incident response times, and enhance overall threat detection accuracy (Ahmed, Asyhari and Rahman, 2021). Additionally, the study bridges the gap between theory and practice by offering a practical implementation model for SOAF, addressing existing challenges like alert fatigue, fragmented architectures, and manual response inefficiencies (Agyepong *et al.*, 2020; Vielberth, Böhm and Fichtinger, 2020).

Furthermore, this research contributes to cybersecurity by emphasising the importance of automation and machine learning in threat detection and response. By automating routine tasks and integrating real-time analytics, the SOAF reduces the cognitive burden on security teams, enabling them to focus on high-priority incidents (Catal *et al.*, 2023). The study also highlights the framework's scalability, which ensures adaptability to increasing data volumes and emerging threat vectors.

Beyond its practical implications, this research adds to the broader cybersecurity discourse by identifying best practices for implementing and optimising integrated security frameworks. These findings can serve as a reference for organisations seeking to modernise their security operations and align them with evolving threat landscapes. By improving operational efficiency, enhancing security posture, and fostering greater collaboration among stakeholders, the study contributes valuable insights to the cybersecurity body of knowledge.

Adopting the SOAF offers organisations a pathway to achieving a robust, proactive, and scalable cybersecurity defence mechanism, effectively addressing the challenges of today's dynamic threat environment.

1.4.1 Addressing the Dynamic Threat Landscape

The modern threat landscape is characterised by rapid and complex cyber threats that can exploit vulnerabilities within an organisation's digital infrastructure (Kaloudi and Li, 2020). Organisations with a SOAF are empowered to proactively identify, analyse, and mitigate threats using real-time automated responses. This capability is essential when cybercriminals continually adapt and innovate their tactics.

1.4.2 Realising Operational Efficiency

Integrating advanced technologies within the framework maximises operational efficiency (M Vielberth *et al.*, 2020). Wazuh's intrusion detection capabilities and Elasticsearch and Kibana's data visualisation prowess enable security teams to identify anomalies and potential breaches quickly (Negoita and Carabas, 2020). By swiftly aggregating and visualising data, organisations can reduce the mean time to detect (MTTD) and respond (MTTR), thereby minimising the impact of security incidents.

1.4.3 Empowering Informed Decision-Making

The framework's importance stems from its ability to provide complete security event insights. By leveraging Elasticsearch and Kibana's analytical capabilities, security analysts can discern patterns, correlations, and trends within the data. This informed decision-making process enhances an organisation's ability to prioritise and address potential threats effectively (Shahjee and Ware, 2022a; Almadani, Aliyu and Aliyu, 2023).

1.4.4 Enabling Automation and Orchestration

Including Cortex in the framework enables automation and orchestration, allowing for sophisticated workflows that automate routine tasks and responses based on predefined triggers. The outcome is enhanced operational efficiency and less human error, as the framework can autonomously execute actions in response to specific events (Sworna, Ali Babar and Sreekumar, 2023).

1.4.5 Enhancing Incident Response and Recovery

Swift and efficient incident response is crucial for minimising the impact of security breaches. Integrating TheHive within the proposed framework allows the framework to become a centralised platform for incident management (Bilali *et al.*, 2022). It streamlines identifying, analysing, and responding to incidents by providing a collaborative environment for security teams. This feature accelerates incident resolution and aids in comprehensive recovery efforts.

1.4.6 Leveraging Threat Intelligence

The framework's ability to incorporate external threat intelligence feeds further enhances its significance. By integrating threat intelligence data, organisations gain a broader understanding of emerging threats and vulnerabilities. This insight enables proactive

measures and facilitates the anticipation of potential attack vectors (Perera et al., 2021; Mughal, 2022).

1.4.7 Compliance and Regulatory Adherence

Organisations must adhere to many regulations with an increasing emphasis on data privacy and compliance. The SOAF aids in data protection, compliance monitoring, and reporting to ensure cybersecurity practices align with regulatory requirements and industry standards (Mughal, 2022).

1.4.8 Future-Proofing Cybersecurity

(Creado and Ramteke, 2020) point out that the ever-advancing nature of technology underscores the need for adaptive and future-proof cybersecurity solutions. Therefore, the framework's modular design and integration of cutting-edge tools position organisations to stay ahead of emerging threats. Moreover, the framework can be augmented and customised to address new challenges as the threat landscape evolves.

In conclusion, this research is essential because it provides organisations with the resources to traverse modern cybersecurity's complex and ever-changing terrain, protecting critical infrastructure and ensuring continuous business operations. The importance of this research rests in the fact that it might lead to better cybersecurity practices by creating and implementing a unified Security Operations and Analytics Framework. It underscores the critical role of such a framework in enhancing an organisation's ability to detect, respond to, and mitigate cyber threats. This research provides insights and guidance for organisations seeking to strengthen their cybersecurity defences and for scholars exploring the field of cybersecurity. Furthermore, this study contributes to the academic body of knowledge in cybersecurity by exploring the practical application and integration of these security tools. The insights gained can be a foundation for future studies and developments in security operations and analytics.

1.5 Research Questions

RQ1: What are the current practices, challenges, and needs of security operations in organisations?

RQ2: How does the SOAF improve the security posture of the enterprise?

RQ3: How does the SOAF enhance the workflow and performance of the security analysts?

RQ4: Discuss the advantages and problems of adopting the SOAF regarding usability, functionality, scalability, reliability, and interoperability.

RQ5: How does the SOAF compare features, capabilities, and costs with other security solutions?

RQ6: What are the design principles and evaluation criteria for a SOAF that leverages a SOAP for automation and CDR?

The research sub-questions are:

RSQ1: What are the existing security operations and analytics solutions, frameworks, models, and standards?

RSQ3: How can a SOAP enable automation and CDR in security operations?

RSQ4: How can a SOAF be designed, implemented, and evaluated to address the research problem?

1.6 Gap Analysis

Incorporating technologies like Wazuh, Elasticsearch, Kibana, TheHive, and Cortex into a SOAF has significantly improved cybersecurity operations through enhanced monitoring, real-time data analysis, and automated incident response. However, existing shortcomings may hinder their overall effectiveness. This gap analysis identifies these deficiencies and proposes a research roadmap to address them based on current literature and industry practices. This review analyses current research on SOAFs, focusing on SOAPs with components such as Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, highlighting key deficiencies in the field.

The gap analysis aimed to evaluate the design, implementation, and improvement of SOAF and SOAP using tools like Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. It focuses on identifying gaps to enhance automation and continuous detection and response capabilities. The research utilises the NIST Cybersecurity Framework to improve critical infrastructure sector security. The framework was organised based on five fundamental functions: Identify, Protect, Detect, Respond, and Recover. These functions serve as a reference for assessing security operations systems (‘Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1’, 2018; ‘The NIST Cybersecurity Framework (CSF) 2.0’, 2024).

As the existing literature describes, current SOAFs and SOAPs effectively integrate multiple security tools to manage and respond to threats. However, they often lack seamless integration and real-time processing capabilities, which can limit their effectiveness against sophisticated, fast-evolving cyber threats (Zeadally, Adi, Baig and Imran A Khan, 2020).

The optimal state for SOAF and SOAP was to align completely with the NIST Cybersecurity Framework. This entailed a fortified system capable of robust asset identification, proactive threat protection, expeditious incident detection, agile response capabilities, and thorough recovery strategies. Additionally, these frameworks and platforms should be equipped with mechanisms that facilitate real-time threat intelligence and automated responses, which are capable of adjusting to the dynamic nature of the cybersecurity environment ('The NIST Cybersecurity Framework (CSF) 2.0', 2024).

Table 1: Gap Analysis Process

Step	**Process Name**	**Process Description**
1	Scope definition	The scope of the gap analysis was to identify the main gaps that exist in the design, implementation, evaluation, and improvement of SOAFs and SOAPs for security operations and analytics.
2	Security Standard	The gap analysis was performed using the NIST Cybersecurity Framework, a comprehensive and voluntary framework that provides advice and best practices for improving the security and resilience of critical infrastructure sectors. The framework comprises five fundamental functions: identification, protection, detection, reaction, and recovery.
3	Current and Desired States Comparison	The current state refers to the existing literature and practice on SOAFs and SOAPs, as summarised in the previous chapter. The desired state refers to the ideal situation where SOAFs and SOAPs are aligned with the NIST Cybersecurity Framework and provide effective and efficient security operations and analytics for organisations. The comparison between

		the current and desired states reveals the main gaps that need to be addressed.
4	Gaps Prioritisation	The gaps were prioritised based on their importance, urgency, feasibility, and impact. The importance refers to the critical gap or challenge for achieving the desired state. The urgency refers to how soon the gap needs to be addressed. The feasibility refers to how easy or difficult it is to address the gap. The impact refers to how much benefit or value can be gained by addressing the gap or challenge.

Based on this process, the following table summarises the main gaps identified in the gap analysis.

Table 2: Results of the Gap Analysis Process

Gap	**Description**	**Importance**	**Urgency**	**Feasibility**	**Impact**
Inadequate comprehensive research gap.	Empirical studies on the integration of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex are limited, inhibiting a clearer understanding of their implementation, challenges, benefits, and limitations of this SOAP.	High	High	Medium	High
Proactive threat hunting and	Crucial for the identification function, ensuring	High	High	High	High

intelligence gap.	that the framework can anticipate and counteract emerging threats before they manifest as attacks.				
Integration and Automation gap.	Critical for enhancing the framework's ability to function cohesively and respond automatically to threats.	High	High	Medium	High
Alert Fatigue	When security teams lack a context-sensitive alert system, they can become inundated with a deluge of notifications. This can result in exhaustion from alerts. Furthermore, there is a higher likelihood of overlooking threats.	Medium	Low	Medium	Medium
Real-time Data Processing and Analysis Gap	Essential for the detection function of the framework,	High	High	Medium to high	High

	allowing for immediate identification and mitigation of threats.				

1.7 Research Agenda

Linked interoperable technology platforms are scarce for monitoring systems and network connections to avoid, identify, investigate, and respond to security issues (Asghar, Hu and Zeadally, 2019; Awotunde Joseph Bamidele and Jimoh, 2021). As a result, a study to close this information gap was proposed. The research agenda was based on the gap analysis conducted in the previous section, which identified the main gaps or challenges in the current state of research and practice on SOA. The research agenda followed a three-step process: (a) formulate accurate, relevant, and practicable queries for research. In order to resolve the identified gaps, research queries were formulated based on a gap analysis. (b) design an appropriate, rigorous, and ethical research methodology that specifically meets the research queries. (c) plan a systematic, transparent, and reliable execution and evaluation of research, based on the research methodology.

Based on this process, the following table summarises the main research questions, the approach, and the evaluation that was proposed in the research agenda.

Table 3: Summary of key research issues, approach, and evaluation in the research agenda

Research Question	**Approach**	**Evaluation**
What are the current practices, challenges, and needs of security operations in organisations?	A qualitative research approach will explore the security operations landscape in organisations, focusing on current practices, challenges, and needs. Semi-Structured Interviews: Engaging key stakeholders like security analysts and CISOs to	Data Collection & Triangulation: Ensure credibility by triangulating data from interviews, focus groups, document analysis, and observations. Compare different stakeholder perspectives for a comprehensive view. Thematic Analysis: Employ coding techniques

	discuss practices and challenges. Focus Groups: Security teams share insights on tool effectiveness, automation, and compliance. Document Analysis: Reviewing policies and incident reports to find patterns and gaps. Observations: Non-intrusive observation of daily operations to understand workflows. Thematic Analysis: Transcribing and analysing data to identify key themes related to practices and needs.	to identify recurring themes, categorising findings into security operations workflows, pain points, tool effectiveness, and future needs. Validity & Reliability Measures - Member checking: Validate findings with participants. Peer debriefing: Consult cybersecurity experts to refine themes. Thick description: Offer detailed narratives of security operations. Reporting Results: Present findings in a structured format, outlining current practices, challenges, and stakeholder-driven recommendations for improving security operations.
How does the SOAF improve the security posture of the enterprise?	A case study will be conducted to design, implement, and evaluate the SOAF in a large-scale organisation. Qualitative methods, including interviews, will be utilised for evaluation.	The execution involves selecting a suitable organisation, obtaining ethical approval and consent, deploying and configuring the SOAF, collecting and analysing data, and reporting results. The evaluation assesses the SOAF's functionality,

		usability, reliability, performance, security, and value.
How does the SOAF enhance the workflow and performance of the security analysts?	The SOAF's impact on security analysts' work will be assessed through qualitative data capturing their perceptions and experiences.	The security analysts will be divided into two groups: an experimental group using the SOAF and a control group not using the SOAF. Both groups will undergo a pretest to measure their baseline workflow and performance indicators, such as the number of incidents handled, the time spent on each incident, the accuracy and completeness of the incident reports, the satisfaction and confidence levels, and the stress and fatigue levels. After using or not using the SOAF, both groups will undergo a post-test to measure the same indicators and compare the changes. Furthermore, both groups will engage in semi-structured interviews or focus groups to get their opinion about the SOAF and its advantages and difficulties.

Discuss the advantages and problems of adopting the SOAF in terms of usability, functionality, scalability, reliability, and interoperability?	A case study approach that involves conducting a real-world experiment with the SOAF and collecting qualitative data from multiple sources. The experiment will involve deploying the SOAF in a selected organisation and observing how it affects the workflow and performance of the security analysts. The data sources will be interviews and observations.	Qualitative data will be gathered and examined to understand how security analysts and other stakeholders view the benefits and drawbacks of adopting SOAF.
How does the SOAF compare features, capabilities, and costs with other security solutions?	A comparative analysis approach that involves collecting and reviewing data from multiple sources.	A multi-criteria decision analysis (MCDA) method that uses a set of criteria and weights to evaluate and rank the SOAF and other existing security solutions based on their features, capabilities, and costs.

1.8 Scope

This research encompasses the design, implementation, and evaluation of SOAF that effectively utilises a SOAP to facilitate automation and CDR.

The scope of this research covers the following aspects.

Table 4: Aspects covered in the scope of this research.

Aspects	Description

Design	The research entails designing the SOAF, rooted in the problem statement, design objectives, and established criteria.
Implementation	It encompasses the practical implementation of the SOAF, utilising critical SOAP components, including Wazuh, Elasticsearch, Kibana, TheHive, and Cortex.
Evaluation	The research rigorously evaluates the SOAF across various dimensions, including functionality, usability, reliability, performance, security, and value.
Challenges, Benefits and Limitations	It identifies and explores the challenges, benefits, and inherent limitations associated with the SOAF.
Recommendations	The research provides valuable recommendations for the prospective enhancement and further development of the SOAF.

The scope of this research does not cover the following aspects.

Table 5: Aspects not covered in the scope of this research.

Aspects	**Description**
Comparison with Other Frameworks	This research does not compare the SOAF to existing security operations and analytics frameworks or solutions.
Individual Component Development	It does not involve developing or modifying individual components within the SOAP.
Testing in Diverse Environments	The testing and validation of the SOAP in various environmental or scenario-specific contexts are not addressed.
Specific Data Analysis	This research does not delve into the in-depth analysis or interpretation of specific

	security data or incidents collected or processed by the SOAP.
Other Security Tools or Techniques	Implementation or evaluation of security tools or techniques beyond the purview of the SOAP is beyond the research scope.

1.9 Organisation of the Research

The subsequent chapters of this research are structured as follows:

Chapter 2 presents a literature review on security operations and analytics, including an overview of related work on security operations and analytics platforms using Wazuh, Elasticsearch, Kibana, TheHive, and Cortex.

Chapter 3 provides a comprehensive overview of the study's methodology. It covers several aspects, such as the research design, data collecting methods, data analysis techniques, assessment criteria, implementation details, and a summary of the findings. Also presented is the implementation of the security operations and analytics platform, including installation and configuration, data collection and ingestion, analytics and detection rules, incident response and automation, performance evaluation, and summary.

Chapter 4 presents the results and analysis

Chapter 5 discusses the study's outcome in great depth, including data analysis and visualisation, detection and response performance, comparison with existing solutions, and summary.

Chapter 6 concludes the research and presents future work, including a summary of contributions, limitations, and implications for security operations and analytics.

References are provided at the end of the research.

1.10 Summary

By providing a customisable and adaptable SOAF using a SOAP comprising of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, this research aims to contribute to security operations and analytics. The platform created in this research could assist organisations in enhancing their security position and mitigate the likelihood of data breaches by

facilitating ongoing monitoring, identification, and response capabilities across the assault cycle. Moreover, this research provides a foundation for future security operations and analytics studies, which can further enhance and expand the platform developed in this study by adding new features, functions, or components.

Chapter 2: Literature Review

2.1 Introduction

In today's ever-evolving digital landscape, the emergence of sophisticated cyber threats poses significant challenges for organisations to safeguard their assets and sensitive information (Tsochev *et al.*, 2020; Mallick and Nath, 2024). Skilled threat actors execute these cyberattacks with significant resources and technological expertise. As a result, the frequency, specificity, and technological sophistication of these assaults make them a serious threat. At the same time, reliance on Information and Communication Technology (ICT) is growing, heightening the stakes of any cyber-attack. However, this is made worse by the ever-changing nature of ICT infrastructures, which now include Cloud computing and the IoT. Therefore, businesses must face the tremendous challenge of protecting their systems and data in this complex and ever-changing environment.

Several businesses have improved their security monitoring and incident response operations in response to these threats. While some businesses have built in-house SOCs and Computer Security Incident Response Teams (CSIRT), others have contracted with an external Managed Security Service Provider (MSSP). A SOC is a centralised operational unit crucial in improving an entity's cybersecurity posture and effectively mitigating potential threats. The SOC achieves this by constantly monitoring cyber threats and protecting valuable assets, such as intellectual property, personal information, company systems, critical infrastructure, and brand reputation, from possible cyber-attacks (Shahjee and Ware, 2022b; Chamkar, Maleh and Gherabi, 2024) . Furthermore, a SOC enables a swift response to mitigate the impact of security incidents (Miloslavskaya, 2016; Tilbury and Flowerday, 2024). Complementing the SOC, a CSIRT comprises experts dedicated to managing security incidents, encompassing tasks like identification, containment, analysis, and resolution (Villegas-Ch, Ortiz-Garcés and Sánchez-Viteri, 2021; Leitner, Skopik and Pahi, 2024). Alternatively, a MSSP is a third-party company that offers security services to clients, such as monitoring, alerting, incident response, threat intelligence, and vulnerability management (Mihindu and Khosrow-shahi, 2020; Wu *et al.*, 2024).

A SOC framework defines the components that deliver SOC functionality and how they interoperate (Danquah, 2020; Chamkar, Maleh and Gherabi, 2024). The SOAF, a specific type of SOC framework, plays a central role by providing the necessary structure, strategies, and methodologies for carrying out cybersecurity tasks. By helping

organisations establish a consistent and practical approach to managing cybersecurity incidents and threats within their SOC, the SOAF becomes a critical tool in bolstering their security posture. The integration of diverse security tools into a unified SOAF has become a pivotal strategy in enhancing cybersecurity defences. Tools such as Wazuh, Elasticsearch, Kibana, TheHive, and Cortex offer unique capabilities that, when combined, could provide a robust platform for managing security threats more efficiently and effectively. It achieves this by leveraging security analytics solutions to offer capabilities such as security monitoring, threat detection, investigation, incident response, and data analysis (Microsoft, 2023). SOAF provides a comprehensive approach to fortifying cybersecurity defences, enabling organisations to effectively detect, respond, and mitigate cyber incidents. As a result, businesses are compelled to seek more advanced SOC solutions to safeguard their sensitive information and valuable assets.

The main focus of this literature study was to comprehensively explore the field's current state, critically assess the existing body of knowledge, and provide a foundation for comprehending the components and capabilities of the SOAF. This framework was deployed as a SOAP incorporating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. Additionally, it aims to clarify the implications of this framework for modern cybersecurity practices.

This literature review delves into the topic of the SOC and its importance in cybersecurity. The historical context of SOC was examined to provide a background for this exploration. The literature review then explains how building a new and customised SOC can significantly improve an organisation's ability to detect and prevent cyberattacks. The importance of SIEM systems in cybersecurity was emphasised. Additionally, the literature review discusses the significance of SOAR platforms and the application of AI and ML in cybersecurity. Furthermore, this literature review undertakes an in-depth analysis of automation in cybersecurity and introduces the concept of CDR. The goal was to explore how these elements collectively enhance security resilience against evolving cyber threats.

Moreover, this literature review offers an overview of security operations and analytics, identifies prevailing research gaps, and outlines SOAP’s current knowledge and practice limitations. It then explains how this paper contributes to bridging these gaps and addressing the identified limitations. Finally, the review summarises the key takeaways and insights from the literature review process.

2.2 Security Operations Center

Cyberattacks utilising AI have resulted in highly targeted and destructive attacks (Guembe et al., 2022; Malatji and Tolah, 2024), which requires an organisation to establish a robust SOC in response. Threats are becoming more sophisticated, and there are more security alerts than ever before. This is exacerbated by gaps in security surveillance. Many of these problems can be fixed if security and IT processes work together. Setting up a Security Operations role brings together processes that can help reveal weaknesses more clearly, reduce wait time, and strengthen defences. By adding security analytics to this process, companies can take more aggressive steps to find threats, meet government standards, and strengthen their total security. Security Operations is the process of making sure that an organisation's security and operations teams work together using the same set of tools and methods to keep the data safe. Sharing information, backed by data and technology, boosts productivity and speeds up new ideas. Therefore, businesses must find better SOC solutions to protect their sensitive information and assets. In addition, understanding the history of SOCs and building one from the ground up may significantly increase the capacity to detect and prevent cyberattacks.

This literature review suggests that the SOC and its evolution are subject to various methods, approaches, and challenges. Key findings and gaps in this field are presented. One perspective describes the evolution of the SOC as a maturity model that describes the stages in which the SOC develops from security monitoring to cyber resilience. For instance, based on the model of SOC maturity proposed by (Kaliyaperumal, 2021), SOC 1.0 was primarily concerned with monitoring, SOC 2.0 was concerned with incident response, SOC 3.0 was concerned with threat detection, and SOC 4.0 was concerned with cyber resilience. Distinct objectives, processes, technologies, and metrics define each stage. The author also provides a roadmap for organisations to achieve cyber resilience, highlighting the challenges and best practices associated with each stage. Another way to view SOC evolution was as a systematic study identifying the primary building blocks and open challenges associated with SOCs. According to (Manfred Vielberth et al., 2020), a comprehensive literature review of SOCs identified five primary building blocks: human, technological, process, organisational, and environmental factors. The authors have associated each aspect with its present challenges. Furthermore, the researchers have identified that more research is required on the processes by which human and technological aspects of a SOC are interconnected.

Alternatively, SOC evolution is a blueprint for effectively creating and deploying SOCs. For instance, (Majid and Zainol Ariffin, 2021) proposed a framework that has four phases: phase planning, phase development, phase implementation, and phase evaluation. Furthermore, to ensure the implementation of the SOC is well functioning and operated, the framework also includes nine skills and knowledge that the employees are expected to possess: security monitoring, incident handling, forensics, threat intelligence, coding and development, risk management, malware analysis, knowledge and communication abilities.

It is also evident that SOC evolution involves some shared approaches and challenges. ML techniques, such as anomaly detection, threat hunting, incident response, and threat intelligence, are commonly used to enhance SOC capabilities. With ML, security data can be analysed in large quantities, patterns and anomalies can be identified, alerts and recommendations can be generated, and feedback can improve security (Buczak and Guven, 2016). Nevertheless, ML presents challenges like data quality, interpretability, scalability, privacy, ethics, and adversarial attacks (Sarker *et al.*, 2020).

SOC operations such as data collection, analysis, triage, containment, and escalation may also be automated and streamlined using SOAR solutions (Danquah, 2020). However, while SOAR can enhance the efficiency, consistency, and productivity of SOCs (Mohammad and Surya, 2018), it also faces some challenges regarding integration, customisation, maintenance, and governance (SIRP, 2023)(TechTarget, 2023).

Alternatively, cloud-based or hybrid SOC models can leverage cloud computing's scalability, flexibility, cost-effectiveness, and innovative capabilities (Almorsy, Grundy and Müller, 2016). Using cloud-based or hybrid SOCs can help overcome some of the limitations of traditional on-premises SOCs, such as resource limitations, infrastructure complexity, and vendor lock-in (Khan *et al.*, 2021). Additionally, cloud-based or hybrid SOCs have disadvantages, like data security, privacy compliance, and vendor dependence (Khan *et al.*, 2021).

The evolution of SOCs reflects the changing landscape of cybersecurity threats and solutions, and, most importantly, dynamically. As indicated in the literature review, this field has multiple perspectives, approaches, and challenges, and additional research is necessary to address the gaps and limitations. In summary, SOCs are centralised units responsible for real-time monitoring, detection, response, and mitigation of cybersecurity threats (Saraiva and Mateus-Coelho, 2022). Traditional SOCs rely on a combination of

human expertise and security tools (Alahmadi, Axon and Martinovic, 2022a); however, they face several significant challenges. One major issue is alert overload, where the high volume of security alerts leads to analyst fatigue, making it challenging to prioritise and respond effectively (Alahmadi, Axon and Martinovic, 2022a). Additionally, the lack of automation in many SOCs results in slow detection and response times (Zidan *et al.*, 2024), as manual processes create bottlenecks. Furthermore, integration issues pose a serious obstacle (Furdek *et al.*, 2021), as security tools often operate in isolated silos(Makani and Jangampeta, 2024), making data correlation difficult and reducing the overall efficiency of threat detection and response. The gap identified is the need for automated and optimised threat detection and mitigation through an integrated SOAF.

2.3 Security Information and Event Management (SIEM)

Modern SOCs require SIEM systems to analyse the real-time security alerts generated by multiple devices and applications (Mughal, 2022). SIEM combines security information management (SIM) and security event management (SEM) functions into one platform (Najafi, Cheng and Meinel, 2021). A SIM system collects and stores security information obtained from various sources. On the other hand, SEM systems analyse and respond to security events based on predefined rules and alerts (Pavlik, Komarek, and Sobeslav, 2014). By correlating and analysing security data from various sources, SIEM provides organisations with a comprehensive and real-time picture of their security posture.

Consequently, organisations may identify, evaluate, and handle security risks before negatively influencing their day-to-day operations. In addition, SIEM platforms collect, normalise, and correlate log data, enabling security analysts to detect and respond to threats more effectively (González-Granadillo, González-Zarzosa and Diaz, 2021). Critical features of SIEM systems include log management, event correlation, alerting, reporting, and incident response (Tariq *et al.*, 2023). SIEM also enables organisations to meet regulatory compliance standards and audit requirements by collecting, storing and reporting on security data from various sources (González-Granadillo, González-Zarzosa and Diaz, 2021). SIEM works by aggregating and correlating event log data from applications, devices, servers and users across the network. SIEM uses predefined rules and advanced analytics to identify deviations from normal behaviour and generate alerts for potential incidents. SIEM also leverages AI and ML to automate many manual threat detection, investigation and incident response processes (Ban *et al.*, 2023a). Organisations have widely adopted SIEM to enhance cybersecurity capabilities and meet

regulatory compliance requirements. However, SIEM must overcome challenges and limitations to improve its effectiveness and efficiency.

The existing literature on SIEM can be categorised into four main themes: (1) the evolution and trends of SIEM, (2) the best practices and recommendations for SIEM, (3) the applications and use cases of SIEM in different domains, and (4) the benefits and challenges of SIEM.

2.3.1 The evolution and trends of SIEM

SIEM has evolved from its predecessors, such as log management tools, intrusion detection systems (IDS), and security event management (SEM) systems (González-Granadillo, González-Zarzosa and Diaz, 2021). The first generation of SIEM systems focused on collecting and storing security data from various sources, such as firewalls, routers, servers, applications, and users. The second generation of SIEM systems added the capability of correlating and analysing security data to detect and respond to security incidents. This was done based on predefined rules and alerts. The third generation of SIEM systems leveraged AI and ML techniques to enhance SIEM detection and response capabilities by identifying anomalies, patterns, and behaviours in security data (Exabeam, 2023). Finally, the fourth generation of SIEM systems integrated big data analytics tools to handle security data's increasing volume, velocity, variety, and veracity.

The current trends of SIEM encompass several significant developments shaping the field of cybersecurity. They include cloud-based, hybrid, open-source, and next-generation solutions. As cloud services become increasingly popular, organisations increasingly leverage cloud-based SIEM solutions. Cloud-based SIEM solutions offer scalability, flexibility, cost-effectiveness, reduced maintenance overhead and accessibility for organisations of all sizes. It allows security logs and events to be efficiently managed across diverse environments, including hybrid and multi-cloud infrastructures. Cloud-based SIEM will enable organisations to scale their security operations, leverage the benefits of cloud computing, and offload infrastructure maintenance and management responsibilities to cloud service providers (Jhaveri and Parmar, 2023; Microsoft, 2023h, 2023i).

Another emerging trend is the adoption of hybrid SIEM solutions, which combine cloud-based and on-premises components. This provides a balance between performance, security, and compliance requirements. Organisations may use the scalability and

adaptability of cloud-based SIEM systems to handle and analyse substantial amounts of data while ensuring that sensitive data is stored on-premises to fulfil regulatory and compliance considerations. This strategy enables organisations to retain control over their critical data while benefiting from the advantages of cloud-based SIEM (Microsoft, 2023i; Splunk, 2023).

Open-source SIEM is gaining popularity and offers customisation capabilities, interoperability, transparency, and affordability. This solution is built on open-source software or frameworks, allowing organisations to tailor the SIEM system to their needs. Open-source SIEM solutions also foster collaboration and knowledge sharing within the cybersecurity community, enabling organisations to leverage community-developed plugins, rulesets, and integrations (Wazuh, 2023).

The evolution of SIEM has led to the emergence of next-generation SIEM solutions that incorporate advanced technologies and capabilities. This transition from traditional SIEM to AI-augmented solution signifies an essential development in cybersecurity. These include blockchain for secure and tamper-proof log storage, encryption for protecting sensitive data, containerisation for improved scalability and isolation, and orchestration and automation for streamlining incident response processes. Furthermore, advanced SIEM systems of the future include threat intelligence feeds to augment their ability to identify and respond to threats. Moreover, including user and entity behaviour analytics (UEBA) allows for monitoring and analysing user behaviour patterns to detect insider threats, compromised accounts, and unusual activities, thus enabling early detection of potential security incidents (Microsoft, 2023). AI is useful for security not just because of the models but also because it can be used to understand and use data well. Since AI tools can only do as good a job with the data they are given, this change makes data accuracy and trust even more important.

These trends demonstrate the evolution and maturation of SIEM as a critical component of modern cybersecurity infrastructures. Organisations are leveraging cloud-based and hybrid solutions, adopting open-source frameworks, and incorporating advanced technologies to enhance their threat detection, investigation, incident response, and compliance capabilities. By remaining informed about these trends, organisations can enhance their security posture and optimise their SIEM implementations.

2.3.2 The best practices and recommendations for SIEM

In today's complex and evolving cybersecurity landscape, organisations encounter a multitude of risks that have the potential to jeopardize their confidential information and essential infrastructure. SIEM systems have emerged as critical tools for detecting, examining, and addressing security incidents by consolidating and analysing data from various sources, providing a thorough assessment of an organisation's security status (González-Granadillo, González-Zarzosa and Diaz, 2021). However, to ensure the optimal performance and effectiveness of SIEM implementations, adopting best practices and following key recommendations is crucial. Before implementing a SIEM solution, it is essential to define clear objectives and scope (Mughal, 2019). By identifying the specific security issues and needs that the SIEM system will address, organisations can tailor the implementation process to their unique environment and goals (Repetto, Carrega and Rapuzzi, 2021). Moreover, (Sadowski, Kavanagh and Bussa, 2020) emphasise aligning SIEM objectives with business objectives to ensure optimal results.

The right SIEM solution is essential to achieving the desired outcomes (González-Granadillo, González-Zarzosa and Diaz, 2021). When selecting a SIEM platform, factors include scalability, ease of integration with existing infrastructure, reporting capabilities, and vendor support (Microsoft, 2023i). SIEM systems must be capable of ingesting data from various sources within an organisation's infrastructure (IBM, 2023). Integration with existing network devices, security tools, and applications is essential for accurate threat detection, investigation and response (González-Granadillo, González-Zarzosa and Diaz, 2021b; Splunk, 2023). Continuous updating and fine-tuning of SIEM rules and correlation engines are crucial to maintaining their effectiveness (Microsoft, 2023). Organisations should periodically review SIEM rules to ensure they are relevant to the current threat landscape and organisational needs. According to (Microsoft, 2023), a well-defined incident response plan is essential for organisations to leverage SIEM capabilities during a security breach effectively. This plan should include guidelines for incident classification, escalation, resolution, and communication protocols for internal and external stakeholders.

Organisations should establish a dedicated team of skilled professionals responsible for managing and maintaining the SIEM system (Mughal, 2022). This team should be trained in SIEM best practices and regularly participate in ongoing education to stay current with emerging threats and technologies (Whitman and Mattord, 2021). Incorporating threat intelligence feeds into SIEM systems can enhance the precision of threat detection,

investigation and the speed of incident response (González-Granadillo, González-Zarzosa and Diaz, 2021). Organisations should select threat intelligence providers that offer timely, relevant, and actionable information to enhance their SIEM capabilities (Samtani *et al.*, 2020).

UEBA can enhance SIEM systems by providing additional context for security events and improving the detection of advanced threats (González-Granadillo, González-Zarzosa and Diaz, 2021). In addition, integrating UEBA with SIEM systems can help organisations identify suspicious activities that may otherwise go unnoticed (Microsoft, 2023c, 2023). Monitoring SIEM performance metrics, such as event processing rates and system resource utilisation, can help organisations identify and address potential bottlenecks in their SIEM infrastructure (Muhammad, Sukarno and Wardana, 2023). In addition, regularly assessing SIEM performance can ensure that the system effectively detects and responds to security threats (IBM, 2023). SIEM systems play a critical role in enhancing an organisation's security posture. By following best practices for SIEM implementation, management, and optimisation, organisations can maximise the value of their SIEM investments and improve their overall cybersecurity resilience.

2.3.3 The applications and use cases of SIEM in different domains

SIEM systems have become an integral part of current cybersecurity efforts (González-Granadillo, González-Zarzosa and Diaz, 2021b; Salinas *et al.*, 2023). They have become indispensable tools for organisations across various domains to detect, analyse, and respond to security incidents effectively. These systems gather and examine data from various sources, including firewalls, intrusion detection systems, and web servers, providing organisations with a comprehensive view of their security posture.

SIEM technology can benefit different domains by providing a comprehensive view of their security posture, real-time threat detection, investigation and response, advanced threat intelligence, regulatory compliance, and greater transparency.

Cybercriminals specifically target the banking sector because of the sensitive data it manages, such as personal information, credit card numbers, and bank accounts (Despotović, Parmaković and Miljković, 2023). SIEM technology can help financial institutions protect their data and assets by identifying unusual activities, such as unauthorised access to critical systems, fraudulent transactions, and data breaches (Kumari, Tyagi and Rekha, 2021). For example, SIEM technology can monitor account activities for signs of insider threats, where employees may misuse their access privileges

for unauthorised purposes (González-Granadillo, González-Zarzosa and Diaz, 2021). Additionally, SIEM technology can help financial institutions meet legal obligations, which provide audit trails and reports on access to data (Najafi Pejman and Cheng, 2021).

The energy sector faces unique cybersecurity challenges, specifically essential infrastructure such as electricity grids and nuclear plants (Tufail *et al.*, 2021). Attacks on these systems can have far-reaching consequences, making effective threat detection, investigation and response essential. SIEM technology can help energy companies monitor their networks for signs of intrusion, such as unauthorised access to control systems and malware infections (González-Granadillo, González-Zarzosa and Diaz, 2021). For instance, SIEM technology can monitor Supervisory Control and Data Acquisition (SCADA) networks for signs of anomalous activity as well as Industrial Control Systems (ICS) (González-Granadillo, González-Zarzosa and Diaz, 2021). Additionally, SIEM technology can help energy companies comply with industry-specific regulatory requirements (Mughal, 2019; Blum and Blum, 2020).

The healthcare domain manages sensitive patient data, making it an attractive target for cybercriminals (Javaid *et al.*, 2023). SIEM technology can assist healthcare providers in monitoring and detecting threats, such as ransomware, phishing attacks, and data exfiltration. SIEM technology can also help healthcare organisations comply with regulatory requirements in the United Kingdom by providing audit trails and reports on access to patient data. These regulations include the Data Protection Act, which was passed in 2018, and the General Data Protection Regulation (GDPR). Moreover, SIEM technology can monitor medical devices and other IoT equipment in healthcare environments, making detecting and responding to potential vulnerabilities easier.

2.3.4 The benefits and challenges of SIEM

The existing literature on SIEM provides a solid foundation for comprehending the advantages and difficulties of this technology. The existing literature on SIEM and its benefits and challenges can be categorised as conceptual, empirical, and practical.

Conceptual literature provides an overview of the SIEM technology and its components, such as data collection, correlation, analysis, and benefits. For example, (González-Granadillo, González-Zarzosa and Diaz, 2021) discuss the different components of a SIEM solution and how they can provide improved visibility, increased threat detection and investigation, reduced response times, and improved compliance. Similarly, (López

Velásquez *et al.*, 2023) describe the basic functionalities of SIEM technology and its evolution over time.

Evidence in the empirical literature shows that SIEM technology helps identify and react to security risks. For example, (López Velásquez *et al.*, 2023) surveyed the most widely used SIEM tools (commercial and open-source) and evaluated their performance and features. They also propose a new framework for SIEM technology that is compatible with GDPR and uses blockchain, encryption, and containers. Another example is (Arora, 2021), who investigates the use of Wazuh SIEM, an open-source SIEM tool, in small and medium enterprises.

Practical literature guides how to implement and use SIEM technology in real-world scenarios. For example, (González-Granadillo, González-Zarzosa and Diaz, 2021) provide recommendations for overcoming the challenges of implementing SIEM technology in critical infrastructures. They also analyse the benefits and usage of SIEM technology in different sectors, such as energy, transportation, health care, and finance.

Therefore, by examining these three types of literature, researchers and practitioners may get a complete picture of SIEM, its advantages, and the obstacles businesses may face during deployment and administration. Integrating conceptual, empirical, and practical literature provides a full understanding of SIEM, which in turn aids in developing well-informed decisions and the widespread implementation of SIEM systems in cybersecurity operations.

In conclusion, SIEM platforms collect, aggregate, and analyse security logs from multiple sources to detect potential threats (González-Granadillo, González-Zarzosa and Diaz, 2021a). They provide real-time monitoring and historical analysis of security events. However, SIEM solutions face key limitations: Rule-based detection - many SIEMs rely on predefined rules, making them ineffective against unknown or evolving threats; False positives - a high number of alerts, many of which are not real threats, require manual investigation and scalability challenges - handling large volumes of log data in real-time can be resource-intensive (González-Granadillo, González-Zarzosa and Diaz, 2021a). The gap identified is that SIEM systems need AI/ML-driven analytics and automation capabilities to enhance CDR.

2.4 Security Orchestration, Automation, and Response

A SOC's role is to protect against cyberattacks. By using multiple detectors, audit logs, intelligence feeds, and notifications are generated (Robert A Bridges *et al.*, 2023).

Most SOCs are equipped with SIEM systems, which combine these data streams and provide analysts with custom dashboards and query interfaces. Nonetheless, according to (Bridges *et al.*, 2018) it remains the responsibility of SOC analysts, who must expend considerable work manually sifting through massive volumes of data from several sources (Islam, Babar and Nepal, 2019).

Although humans excel at making decisions and using logic, computers can quickly and precisely complete routine, repetitive jobs. The more we rely on automated processes, the more critical it becomes for effective automation and orchestration in SOCs. This helps reduce the time it takes to respond to cyber-attacks and lowers the value of Mean Time to Recovery (MTTR). Given the continuously changing nature of cyber-attack methods, this is a crucial aspect of cybersecurity. Since humans cannot be eliminated entirely, human intervention must be built into incident response procedures.

The SOAR approach encompasses the use of people, processes, and technology to proactively and automatically prevent, identify, and address cyber assaults in real-time. Its primary objective is to automatically preserve the three fundamental information security principles: confidentiality, integrity, and availability (Kaliyaperumal, 2021).

According to (Kinyua and Awuah, 2021) the SOAR system continues the incident response process beyond the capabilities of the SIEM, delivering automated and orchestrated responses during an incident's four stages. SIEM and SOAR are complementary security tools that help detect and respond to threats. SIEM monitors and analyses data, while SOAR automates and orchestrates tasks and workflows.

2.4.1 SOAR Conceptual Foundation

SOAR is a software system designed to enhance the efficiency and efficacy of security operations. It integrates and coordinates various technologies, automates repetitive jobs, and optimises incident response procedures. Security orchestration connects different security tools and data sources, security automation performs tasks based on rules or triggers, and security response delivers the results of orchestration and automation.

The concept of SOAR emerged in response to the continued rise in the amount and sophistication of cyber threats and the increasing number of security tools and alerts that security teams needed to manage daily (IBM, 2023; Microsoft, 2023). SOAR platforms integrate various security tools and streamline processes to speed up incident reactions and reduce human intervention (IBM, 2023). Critical components of SOAR platforms

include a security incident response platform, SOC management, threat intelligence gathering, security orchestration and automation, and compliance reporting.

The SOAR research conducted by (Bartwal et al., 2022; Christian Juan and Paulino, 2022) pinpointed the key ideas and emerging research to respond to security events. A precursor to SOAR may be found in (Oltsik Jon, 2018) article, which emphasises the necessity of a single platform to handle the increasing complexity of security operations. The author argues that SOAR is a valuable tool for security teams struggling with issues including alert fatigue (Chandran Sundaramurthy *et al.*, 2016; Young, 2021), talent shortages (Brewer, 2021; Yamin and Katt, 2022a), and inefficient procedures.

2.4.2 SOAR Implementation

According to (Kaliyaperumal, 2021), SOAR is a novel initiative. (Robert A Bridges *et al.*, 2023) stated that the evaluation of SOAR tools has not been addressed, nor has research on experimental frameworks for comparing SOAR tools in academic literature.

However, some academic studies have explored different aspects of SOAR, such as (Empl *et al.*, 2022) explicitly focusing on implementing SOAR in IoT environments. The authors discuss IoT security orchestration architectures and highlight the importance of incorporating automation and response capabilities in managing IoT security threats. In a study conducted by (Christian, Paulino and de Sá, 2022), they presented an inexpensive cloud-based SOAR platform and explained how it works. The proposed approach was evaluated through experiments conducted at a large multinational company to assess its practicality. On the other hand, in the study conducted by (Mir Abdul Wahidand Ramachandran, 2021), they implemented a SOAR in Smart Grid-Based SCADA Systems. The authors asserted that since SOAR uses technologies like AI, ML, deep learning, automation, threat intelligence, and orchestration, it provides an ideal solution for entities to address the security challenges inherent in smart grid-based SCADA systems. Also, several commercial vendors provide SOAR solutions, such as IBM Resilient, Microsoft Sentinel, Splunk Phantom, Sumo Logic, and Swimlane. Each of the companies mentioned above provides distinct features and capabilities in its SOAR systems. IBM Resilient specialises in incident response planning and case management (IBM Resilient, 2024). Microsoft Sentinel offers extensive integration with other Microsoft security products and services (Microsoft, 2024). Splunk Phantom focuses on automating and orchestrating security processes for quick response (Splunk, 2024). Sumo Logic provides real-time analytics and insights for security monitoring in cloud

environments (Sumo Logic, 2024). Swimlane prioritises low-code automation to assist security teams in responding to threats without requiring complex programming (Swimlane, 2024). Organisations often select and implement a SOAR solution based on their particular security requirements, current technology infrastructure, and desired level of automation.

2.4.3 SOAR Benefits and Challenges

(Johnson *et al.*, 2023) explored the benefits of automating cyber threat intelligence management for incident response processes, information exchange, case administration, monitoring, and automation within SOAR platforms. The authors evaluated various privacy-preserving techniques and demonstrated how automation could enhance speed and accuracy by protecting their system from attacks and restoring it to a known good state as quickly as possible. Similarly, in the study conducted by (Nicholls, 2023) the opinion is that SOAR provides swift identification and reaction to attacks despite constantly changing threats, the lack of skilled security staff, and the need to monitor growing IT estates. It collects and validates data from various sources to provide better intelligence and context for incidents.

Moreover, it provides automating and semi-automating many routine tasks and processes to reduce alert fatigue and improve productivity. For example, it reduces the time needed to detect and respond to incidents by using playbooks and controls through a single pane of glass. It simplifies reporting and documentation by aggregating intelligence and presenting it via custom-built dashboards.

Other benefits for SOCs include improved productivity. This is due to automating repetitive and tedious tasks. SOAR frees up human analysts for more strategic work (Islam, Babar and Nepal, 2020) (Robert A Bridges *et al.*, 2023) Additionally, there is less human error. SOAR reduces the risk of mistakes or oversights by following predefined workflows and playbooks (Empl *et al.*, 2022) (A Sridharan and Kanchana, 2022).

Another benefit is faster incident response and remediation. SOAR prioritises threats, makes recommendations, and executes actions in real-time, reducing the time and cost of detecting and responding to cyberattacks (Mir Abdul Wahidand Ramachandran, 2021; Mughal, 2022a; K. L. McLaughlin, 2023).

Furthermore, the SOAR can make better use of existing security tools. It can integrate and coordinate different tools into streamlined processes, enhancing their functionality

and value (IBM, 2023). Moreover, the SOAR provides more visibility and reporting. It collects and consolidates information from various sources, paints a complete picture of the current security situation, and generates valuable reports and metrics (TechTarget, 2023).

Therefore, SOAR is a promising solution for improving the security posture of organisations by streamlining and automating their security operations. However, SOAR implementations may face various challenges, like the complexity of integrating and interoperability of disparate security tools (Islam, Babar and Nepal, 2020; Robert A Bridges *et al.*, 2023), the need for skilled personnel to develop and maintain automation workflows, and concerns over data privacy and regulatory compliance (Islam, Babar and Nepal, 2020; Mir Abdul Wahid and Ramachandran, 2021; Vast et al., 2021). Researchers have proposed various approaches, such as using application programming interfaces (API), standardised data formats, and open-source frameworks to facilitate integration (Islam, Babar and Nepal, 2019, 2020; Groenewegen and Janssen, 2021). Nevertheless, seamless integration remains challenging due to the diversity of security tools (Srivastava *et al.*, 2022) coupled with the absence of a consensus on the structure (Islam, Babar and Nepal, 2020).

2.4.4 Recent Advancements and Future Directions

Recent advancements in SOAR technologies include integrating AI and ML techniques to improve threat detection, investigation, classification, and response capabilities (Mir Abdul Wahid and Ramachandran, 2021).

Automation, orchestration, and response are essential components to reduce response time and recover from cyber incidents. They reduce manual tasks and minimise human error, significantly improving operational efficiency and effectiveness. Furthermore, (Kinyua and Awuah, 2021) acknowledge that SOAR solutions, which are software products that integrate with various security tools and use AI and ML to automate workflows, analyse threats, and respond to incidents, are a relatively new and emerging market that requires more research (Islam, Babar and Nepal, 2019). However, others caution that automation may also present further difficulties and dangers, including the possibility of automated actions causing unintended consequences, the vulnerability of automated systems to new types of cyberattacks, or the overreliance on automated decision-making (Zarina I, Ildar R and Elina L, 2019) (Mckinsey, 2023) (Kroll, Michael and Thaw, 2021). Future directions for SOAR research include the development of

standardised frameworks and ontologies to facilitate interoperability between security tools and exploring decentralised and privacy-preserving SOAR architectures (Islam, Babar and Nepal, 2020).

In summary, SOAR technologies have emerged as a promising solution to address the growing complexity and scale of cybersecurity challenges. By integrating security tools, automating processes, and enabling rapid response to threats, SOAR solutions can significantly raise the level of performance among security teams. Further research and development in AI and ML integration, standardisation, and privacy-preserving architectures will continue to drive advancements and innovations in the SOAR domain, SOAR solutions automate security workflows, integrate security tools and enable automated incident response (Kinyua and Awuah, 2021). They help SOC teams respond faster by automating repetitive tasks and using playbooks (Robert A. Bridges *et al.*, 2023). Challenges in existing SOAR solutions include complex deployment, and implementing SOAR requires significant customisation and integration efforts. Data silos - some SOAR platforms still struggle with cross-platform data correlation (Kinyua and Awuah, 2021). Limited threat intelligence usage - SOAR tools need better integration with real-time threat intelligence feeds. The gap identified is the need for a more seamless integration between SIEM and SOAR, ensuring real-time analytics and automation in a unified framework.

2.5 Artificial Intelligence and Machine Learning in Security Operations and Analytics Frameworks

Technological advancements and the rising interconnectedness of the digital world have led to the rise of novel and sophisticated cyber threats (Qamar, Anwar and Afzal, 2023) (Dewa and Maglaras, 2016). In response to the dynamic nature of evolving challenges, cybersecurity solutions have increasingly embraced the integration of AI and ML. These advanced technologies are powerful tools that complement and enhance traditional security measures. Using AI and ML to their full potential, SOC strategies gain a significant edge in adapting to the constantly shifting threat landscape (Prasad and Rohokale, 2020; Salih *et al.*, 2021).

The application of AI and ML in SOCs has gained significant attention in recent years (Zeadally, Adi, Baig and Imran A. Khan, 2020). In security operations, AI is not only helpful, it is becoming necessary. When AI is used, it not only improves what can already be done but also changes how security problems are handled and fixed. AI and ML can

improve threat detection, investigation and response by analysing large volumes of data at scale and identifying patterns and anomalies that may indicate cyber threats (Sarker, 2024). ML-based algorithms have been applied to intrusion detection, malware analysis, and threat intelligence (Prity *et al.*, 2024). Integrating AI and ML technologies into security tools like Wazuh can enhance their capabilities and improve the overall effectiveness of security operations (Karim *et al.*, 2024). AI-driven automation speeds up responses and improves threat management, and AI-driven analytics dig deeper into security data, making it easier to see what's going on in diverse and complicated settings. AI can do the boring work of sorting through logs and writing detection rules, freeing up entry-level analysts to work on more important tasks, like making important decisions.

In recent years, AI and ML have become increasingly important and influential in cybersecurity, which protects information systems from cyber threats, attacks, damage, or unauthorised access. However, while AI and ML can offer many benefits and opportunities for enhancing cybersecurity, they also present substantial threats and obstacles that must be tackled.

2.5.1 The Role of AI and ML in Security Operations and Analytics Frameworks

AI and ML techniques have become increasingly popular in cybersecurity, as they can analyse vast amounts of data quickly (Ali *et al.*, 2022) and adapt to new threats autonomously (Mart\'\inez-Fernández *et al.*, 2020; Aloqaily *et al.*, 2022). ML, a subfield of AI, involves training algorithms focusing on training computers to identify patterns, make predictions, and acquire knowledge from fresh data without explicit programming (Sarker, 2021). This capacity for continuous learning and adaptation makes ML well-suited for cybersecurity applications, where threats constantly evolve (Zeadally, Adi, Baig and Imran A Khan, 2020).

Furthermore, AI and ML enhance cybersecurity by speeding up the detection, containment, and response to cyberattacks (Manoharan and Sarker, 2023). AI and ML algorithms learn from data and recognise new patterns (Nozari, Ghahremani-Nahr and Szmelter-Jarosz, 2024) As a result, cybersecurity systems can quickly spot anomalies, flag suspicious activities, and take action to stop or mitigate the attacks. Besides preventing adversaries from exploiting vulnerabilities or spreading malware, this proactive approach helps predict their moves (Nadella and Gonaygunta, 2024). By providing data and machine intelligence to security professionals, AI and ML help improve cybersecurity.

With the help of AI and ML tools that automate tasks, analyse large amounts of data, and provide insights, security teams can focus on more strategic and creative cybersecurity tasks, reducing their workloads. They can also use this information to become more proactive and adaptable to a changing environment regarding cyber threats.

2.5.2 Applications of AI and ML in Security Operations and Analytics Frameworks

AI and ML have become integral to modern security operations and analytics frameworks. These technologies enhance the ability to detect, prevent, and respond to security threats by automating and improving complex processes, analysing vast amounts of data, identifying patterns that are often invisible to human analysts and optimising risk management strategies. AI and ML technologies are transforming security operations by providing real-time insights and strengthening defences against advanced cyber threats (Manoharan and Sarker, 2023). Some of the key areas include:

2.5.2.1 Security Management

Security management involves overseeing an organisation's security policies and tools. AI and ML enhance this by enabling proactive threat detection, incident response, and policy enforcement.

In the context of threat detection and prevention, AI and ML enable real-time threat detection and analysis through anomaly detection, behaviour analytics, and predictive modelling. ML algorithms can be trained to identify unusual activities or patterns in network traffic, user behaviour, and system logs, which may indicate an attack (Mahfouz *et al.*, 2020). By analysing historical data and learning from known attack signatures, ML algorithms can detect intrusions in real-time and even predict future threats (Alzahrani and Alenazi, 2021a; Srinivas *et al.*, 2022). In the context of Wazuh and Elasticsearch, ML models can analyse large volumes of log data to identify correlations indicative of potential breaches. Elasticsearch's machine learning features, such as anomaly detection jobs, are particularly suited for detecting unusual patterns in indexed data (Ahir and Shaikh, 2024). These systems reduce the reliance on rule-based detection, which is often ineffective against advanced persistent threats.

For automated incident response and security orchestration, AI-driven Security Orchestration, Automation, and Response (SOAR) platforms enhance incident response by automating critical security processes. Upon detecting a threat, these systems can swiftly isolate affected systems, block malicious IP addresses, and alert security teams

without human intervention (Mutalib et al., 2024). This automation speeds up response times and lessens the impact of security breaches, allowing organisations to manage threats more effectively.

Furthermore, AI and ML improve incident response by automating threat containment, investigation, and mitigation. SOAR platforms utilise AI-driven playbooks for quick and consistent incident handling (Kinyua and Awuah, 2021). Automating processes enables organisations to respond to threats swiftly, lighten security teams' workloads, and boost cybersecurity resilience. Additionally, ML models enhance threat prediction by analysing attack patterns and anticipating adversaries' next steps. This allows security teams to address threats proactively, strengthening defences against cyberattacks (Prity *et al.*, 2024). AI-driven incident response automation speeds up reactions and enhances threat management, creating a more adaptable security framework.

AI-driven SIEM systems improve log analysis, event correlation, and security monitoring by processing large volumes of security data in real-time (Levshun and Kotenko, 2023). Traditional SIEM solutions generate excessive alerts, making it hard for analysts to detect critical threats. AI-driven log analysis and event prioritisation help teams focus on high-risk incidents, reducing alert fatigue and enhancing response efficiency (Almer, Horalek and Sobeslav, 2024).

AI enhances cyber threat intelligence by analysing large datasets from security logs, open-source intelligence (OSINT), and threat databases. ML models detect patterns in adversary tactics, techniques, and procedures (TTPs) to predict future cyber threats, helping organisations stay ahead of attackers (Salem et al., 2024). AI-driven threat intelligence platforms aggregate threat data from various sources, offering security teams actionable insights to prevent emerging threats (Sarker, Furhad and Nowrozy, 2021).

AI and ML play a crucial role in user and entity behaviour analytics (UEBA), which detects insider threats, compromised accounts, and anomalous user activity. AI models establish baselines of normal user behaviour and flag deviations that may indicate malicious activity (Zunair Ahmed Khan, Mubashir Khan and Arshad, 2022). Organisations can use AI-powered identity and access management (IAM) systems to enforce stricter security policies and prevent unauthorised access.

In policy enforcement and compliance, AI can monitor compliance with security policies by analysing user activities and system configurations. For example, ML models can identify deviations from established security baselines, such as unauthorised software

installations or misconfigured firewalls (Shaik and Shaik, 2024). This ensures that organisations adhere to regulatory requirements and internal security standards.

2.5.2.2 Vulnerability Auditing and Risk Assessment

Vulnerability auditing identifies and prioritises weaknesses in an organisation's IT infrastructure. AI and ML enhance this process by automating vulnerability discovery and risk assessment.

Automated vulnerability scanning is essential in cybersecurity, but traditional tools often generate many false positives, distracting security teams from real threats. AI-powered tools using natural language processing (NLP) improve accuracy by integrating threat intelligence and historical data, significantly reducing false positives. This allows security teams to focus on addressing critical vulnerabilities more effectively (Wen, Shukla and Katt, 2024).

ML algorithms enhance vulnerability detection and play a crucial role in risk prioritisation. By evaluating factors like exploit availability and asset criticality, ML models can predict which vulnerabilities are most likely to be exploited. Analysing dark web trends and past attack patterns, these models offer actionable insights for organisations to focus their remediation efforts on the most critical risks, thereby strengthening their overall security posture (Mavrogiorgou *et al.*, 2022).

Furthermore, AI enhances patch management by streamlining the deployment process and minimising potential disruptions. AI systems can forecast the impact of patches on system stability and recommend optimal deployment schedules based on historical data. By analysing patterns of successful and failed patch deployments, these systems help organisations avoid downtime and maintain operational continuity. This not only reduces the risk of system instability but also ensures that vulnerabilities are patched in a timely and efficient manner (Sapkal *et al.*, 2024).

Integrating AI and ML into vulnerability scanning, risk prioritisation, and patch management enhances the efficiency of security operations. These technologies reduce false positives, enable data-driven risk assessments, and optimise patch deployment, allowing organisations to proactively address vulnerabilities and strengthen cybersecurity defences.

2.5.3 Challenges and Considerations

AI and ML technologies are integral to modern cybersecurity frameworks, particularly in the realms of security operations and analytics. In this context, they enhance the SOAF by bolstering its AI-driven detection and response capabilities. This approach emphasises the critical risks that must be addressed when implementing AI in cybersecurity practices. Furthermore, it aligns with the objective of developing a resilient and effective security operations framework. The discussion also explores potential future directions that could further strengthen SOAF, enabling it to adapt to evolving threats. However, there are several challenges and limitations. A main concern is that adversaries could use AI and ML to create advanced attacks, like malware variants that evade detection (Chaganti, Ravi and Pham, 2022). ML models may be vulnerable to adversarial examples, where minor input changes can lead to incorrect predictions (Bajaj and Vishwakarma, 2024). A third challenge is requiring high-quality, labelled data to train ML algorithms, which presents another challenge (Chai *et al.*, 2023).

ML-based cybersecurity solutions might be hampered by a shortage of high-quality labelled data, especially for new risks (Zhang, Xie and Xu, 2020). In addition to these technical challenges, privacy and data protection issues exist, as using AI and ML in cybersecurity often requires access to sensitive information (Marengo, 2024).

Besides posing potential risks, AI and ML can threaten cybersecurity by exploiting existing vulnerabilities or introducing new ones. Cybercriminals may use these technologies to create adversarial examples that can deceive AI and ML models (Malatji and Tolah, 2024). They can also use AI and ML to perform poisoning attacks, which are attacks that can corrupt the training data or the model of an AI and ML system (Cinà *et al.*, 2024). Moreover, they can also use AI and ML to create backdoors, which are hidden features or functions that can allow unauthorised access or control of an AI and ML system (Pan and Mishra, 2022; Salem *et al.*, 2022).

Furthermore, AI and ML can raise ethical and legal issues affecting cybersecurity. For example, AI and ML can pose privacy risks by collecting, processing, or sharing sensitive or personal data without consent or transparency (Andreotta, Kirkham and Rizzi, 2022). They can pose risks by making harmful decisions without clear accountability, being opaque in their reasoning, and producing unfair or discriminatory outcomes (Belenguer, 2022).

Despite their benefits, AI and ML pose challenges in SOAF implementations. High false positive rates, lack of interpretability, and the need for extensive labelled datasets hinder their effectiveness (Salem et al., 2024). Adversarial machine learning, where attackers manipulate inputs to evade detection, is another pressing concern (Pauling *et al.*, 2022).

The simulation-based testing of SOAF architectures using platforms like Wazuh and TheHive can mitigate these challenges by providing a controlled environment to evaluate and refine AI/ML algorithms. Continuous learning from synthetic data enhances model accuracy and robustness.

In conclusion, AI and ML are powerful tools in cybersecurity, offering transformative potential. Their integration into the SOAF enhances threat detection, malware analysis, and phishing prevention. Despite challenges like adversarial attacks, data availability, ethical and privacy concerns, ongoing advancements in robust models and federated learning are shaping their practical application. These technologies significantly boost SOAFs' capabilities for detecting and responding to cyber threats. By utilising platforms like Wazuh, Elasticsearch, and Kibana, security teams can build an automated ecosystem for CDR, with promising developments in AI/ML algorithms improving security operations. Furthermore, AI/ML techniques are increasingly used to detect anomalies, classify threats, and automate responses(Kinyua and Awuah, 2021). AI-powered threat detection includes anomaly detection, which identifies deviations from normal network behaviour (Bhardwaj, Dutta and Chintale, 2024); behavioural analytics, which uses machine learning to detect APTs (Saini *et al.*, 2023) and predictive analytics, which forecasts potential security breaches before they happen (Duary *et al.*, 2024). The challenges in AI/ML cybersecurity applications include high false positive rates where AI/ML models struggle to differentiate between normal behaviour and real threats (Olateju *et al.*, 2024). Adversarial attacks where cyber attackers can manipulate AI models to evade detection (Noor *et al.*, 2019). Model interpretability, where security teams often lack visibility into how AI models classify threats (Sarker *et al.*, 2024). The gap identified is AI/ML should be integrated within a holistic SOAF to improve accuracy and response efficiency.

2.6 Continuous Detection and Response

Cybersecurity is a critical issue for all entities, as these cyberattacks can cause significant damage to data, systems, reputation, or finances (Chandna and Tiwari, 2023). Traditional signature-based defence security solutions, including antivirus or firewalls, are often

insufficient to protect against evolving cyber threats, increasing volume and sophistication as they rely on signature-based detection and point-in-time protection (Or-Meir *et al.*, 2019; Deshpande *et al.*, 2024). These legacy solutions often rely on static indicators of compromise (IOCs), leaving organisations vulnerable to zero-day attacks, advanced persistent threats (APTs), and polymorphic malware. Therefore, a new approach to cybersecurity that can provide continuous monitoring, detection, and response to threats across endpoints, email, and identity is needed to address these limitations. This approach is known as CDR. It integrates real-time monitoring, automated threat detection, and adaptive response mechanisms. It continuously collects, analyses, and correlates data from multiple security layers—including endpoints, networks, and cloud environments—to detect and mitigate threats as they arise. This approach is proactive, intelligence-driven, and automated, leveraging cutting-edge technologies such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), Network Traffic Analysis (NTA), Threat Intelligence Feeds, and System Monitoring tools (e.g., Microsoft Sysmon).

SIEM solutions play a pivotal role in modern SOCs. They function as a central nervous system by aggregating security logs from various sources, including endpoints, network devices, identity systems, and cloud applications. These solutions employ correlation rules, behavioural analytics, and advanced artificial intelligence techniques to detect security incidents in real time.

Key Technical Components include:

Log Collection and Normalisation: SIEM tools methodically collect security logs from firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), endpoints, and cloud platforms, normalising this data into a standardised format that facilitates effective analysis. However, it does require comprehensive tuning to minimise the occurrence of false positives (Laue *et al.*, 2021).

Real-Time Threat Detection: These systems utilise correlation rules and anomaly detection methods, such as User and Entity Behavior Analytics (UEBA), to promptly identify and respond to suspicious activities.

Threat Hunting: Security analysts leverage custom queries and interactive dashboards to investigate potential threats, enhancing overall security posture.

Integration with Threat Intelligence: SIEM solutions incorporate external threat intelligence feeds, such as MITRE ATT&CK, VirusTotal, and OpenCTI, to bolster their detection capabilities and stay ahead of emerging threats.

Automated Response via SOAR: Certain SIEM solutions integrate with Security Orchestration, Automation, and Response (SOAR) platforms, enabling automated actions for threat mitigation and incident response.

Examples of Notable SIEM Solutions include:

Splunk Enterprise Security: Notable for its AI-driven correlation and visualisation capabilities.

Elastic Security (ELK Stack): An open-source alternative offering flexible deployment options.

Microsoft Sentinel: A cloud-native SIEM solution that employs machine learning-based anomaly detection for robust security management.

This overview underscores the importance of SIEM solutions in maintaining the integrity and security of organisational information systems.

EDR solutions continuously monitor endpoint activities, including workstations, servers, and IoT devices, to identify advanced threats such as ransomware, fileless malware, and privilege escalation. Unlike traditional antivirus solutions, EDR solutions are designed to document endpoint events, facilitating thorough forensic investigations and enabling automated incident response actions. While EDR solutions offer automated responses like isolating compromised devices, their effectiveness increases with integration into a broader security framework (Karantzas and Patsakis, 2021).

The technical components are:

Telemetry Collection: EDR systems monitor critical endpoint activities, including process executions, network connections, registry modifications, and memory usage.

Behaviour-Based Detection: EDR solutions can detect suspicious behaviours indicative of potential threats by utilising heuristics and artificial intelligence models.

Automated Containment: EDR capabilities include isolating compromised endpoints, blocking malicious processes, and rolling back unauthorised changes to maintain system integrity.

Threat Hunting and Incident Investigation: Security analysts leverage EDR query languages, such as those aligned with the MITRE ATT&CK framework, to conduct in-depth threat investigations.

Examples of Leading EDR Solutions are:

Microsoft Defender for Endpoint (MDE): An AI-driven EDR solution with seamless integration into Microsoft 365.

CrowdStrike Falcon: A lightweight, cloud-native EDR incorporating advanced behavioural AI analysis.

SentinelOne Singularity: Known for its autonomous response capabilities and rollback features, enhancing endpoint security management.

This overview highlights the significance of EDR solutions in modern cybersecurity strategies, underscoring their role in safeguarding organisational assets against evolving threats.

XDR platforms enhance threat detection by integrating security data from endpoints, networks, cloud environments, and applications. They offer comprehensive visibility into multi-stage attacks and utilise AI-driven automated threat hunting, which streamlines incident response and increases effectiveness in hybrid IT environments (Kuppingercole, 2024).

Network Traffic Analysis (NTA) solutions play a critical role in monitoring network behaviour to detect anomalies, insider threats, and APT. By identifying suspicious data flows and unauthorised communications. They analyse packet data and flow logs to identify malicious activities, including data exfiltration, lateral movement, and command-and-control (C2) traffic. These solutions leverage advanced technologies such as deep packet inspection (DPI), machine learning models, and behavioural analytics to detect threats that may evade traditional firewalls or IDS/IPS. NTA tools enhance network security and often integrate with SIEM systems to improve threat intelligence (Iglesias *et al.*, 2020).

Technical Components are:

Deep Packet Inspection and Flow Analysis: This component examines both raw network packets and associated metadata to identify anomalous traffic patterns.

Encrypted Traffic Analysis (ETA): Using TLS fingerprinting and behavioural heuristics, ETA effectively detects threats within encrypted network flows without decrypting the data.

AI-Driven Anomaly Detection: This feature identifies unusual spikes in network traffic, C2 communication, or DNS tunnelling activities.

Forensics and Threat Hunting: Full packet captures are logged for retrospective analysis, facilitating efficient incident response.

Examples of NTA solutions are:

Darktrace Enterprise Immune System: An AI-powered system focused on anomaly detection.

Cisco Secure Network Analytics: This solution monitors network flows to enhance security oversight.

Zeek: An open-source framework dedicated to network security monitoring.

These components and solutions collectively reinforce organisational defences against evolving cybersecurity threats.

Threat Intelligence Feeds supply SOCs with real-time data on emerging threats and malicious indicators, including updates on known threats, attack patterns, IOCs, IP addresses, domains, and file hashes. By integrating this information into SIEM and XDR platforms, SOC teams can prioritise threats, mitigate risks, and tailor intelligence to specific industry needs (Saeed et al., 2023).

Technical Components are:

Indicators of Compromise (IOCs): Blacklists of malicious domains, IP addresses, and file hashes.

Tactics, Techniques, and Procedures (TTPs): Insights from MITRE ATT&CK to understand attacker behaviour.

Automated Threat Intelligence Sharing: Supports STIX/TAXII protocols for real-time TI updates.

Examples of Threat Intelligence Feeds are:

MITRE ATT&CK Framework – Adversary tactics, techniques, and procedures.

VirusTotal – Malware scanning and file reputation.

OpenCTI – Open-source threat intelligence platform.

System monitoring tools, including Microsoft Sysmon, provide low-level visibility into endpoint activities, recording critical security events for forensic analysis and real-time detection.

Technical Components are:

Process and File Monitoring: Captures process execution, file creation, and modification activities.

Registry and WMI Event Logging: Detects unauthorised changes in Windows registry and system configurations.

Network Connection Tracking: Logs outbound and inbound network communications to identify suspicious connections.

Integration with SIEM & EDR: Feeds rich telemetry into SIEM platforms for correlation and analysis.

Examples of System Monitoring Solutions are:

Microsoft Sysmon – Advanced Windows event monitoring for SOC investigations.

OSSEC – Open-source host-based intrusion detection system (HIDS).

Auditd (Linux Audit Framework) – Logs system calls and security events in Linux environments.

One of the main features of CDR is that it uses a network that is safe by design and continuously monitors, detects, and responds to threats across endpoints, email, and identity (Geach, 2021). CDR gathers and analyses data from devices, applications, networks, or users to identify malicious activities. It responds to threats in near real-time by blocking, containing, or remediating them and alerting security teams to incidents.

Another feature of CDR is that it leverages cloud-based AI and ML to access the latest threat intelligence and automate responses (Reddy, 2021). CDR utilises AI and ML algorithms to learn from data, identify new patterns, and compare them with current threat intelligence from sources like Microsoft 365 Defender and Cisco Secure Endpoint (Cisco, 2024; Microsoft, 2024). Furthermore, CDR uses AI and ML to automate responses with predefined or custom rules, allowing for quicker and more efficient threat mitigation.

A third feature of CDR is its integration with other security technologies, allowing it to communicate with solutions like antivirus, firewalls, and VPNs. CDR consolidates incidents and alerts into a single dashboard, helping security teams prioritise, investigate, and resolve issues effectively (Cisco, 2023; Microsoft, 2023).

One of the ways that CDR can protect against common and emerging cyberattacks is by blocking or containing malware, ransomware, phishing, or social engineering attacks (McKinsey, 2024; Secureframe, 2024). These attacks use harmful files or messages to infect, encrypt, or steal data while deceiving users. In this context, CDR is essential for scanning and filtering incoming files or messages, promptly blocking or quarantining any detected malicious content. Additionally, CDR enhances security by educating users about potential threats and scams.

Another significant role of CDR in safeguarding against cyberattacks is through the verification, validation, testing, or debugging of AI and ML models (Vassilev, Booth and Souppaya, 2022; MarkovML, 2024). These techniques ensure the correctness, reliability, quality, and safety of AI and ML systems. CDR defends against adversarial examples, poisoning attacks, and backdoors that seek to deceive or compromise models. By employing CDR, errors, vulnerabilities, and anomalies are actively identified and prevented during the design, implementation, and operation of AI and ML systems.

CDR enhances cybersecurity by detecting anomalies, flagging suspicious activities, and anticipating adversaries' strategies. It plays a key role in identifying zero-day exploits, insider threats, and advanced persistent threats that exploit unknown vulnerabilities. Its effectiveness comes from using AI and ML algorithms that learn from data and adapt to new patterns while referencing current threat intelligence. Additionally, CDR automates tasks, analyses large datasets, and generates insights to strengthen its defences against complex attacks (Sarker, Furhad and Nowrozy, 2021; Cisco, 2023; Microsoft, 2023).

In conclusion, CDR represents an innovative approach to cybersecurity that integrates real-time detection, automated response, and AI-driven threat intelligence into a unified framework. By leveraging advanced security technologies including SOAR, SIEM, EDR, NTA, Threat Intelligence Feeds, and continuous System Monitoring, SOCs can proactively identify threats, respond to incidents in real-time, and enhance overall security resilience. Future developments in AI, federated learning, and zero-trust architectures will further strengthen the capabilities of CDR-based cybersecurity frameworks in detecting, containing, and mitigating cyber threats.

CDR has the potential to strengthen organisational security against evolving cyber threats. CDR enhances traditional detection and response with continuous monitoring and automated mitigation. AI and ML further improve CDR by enabling autonomous detection and incident response. For example, AI models in platforms like TheHive prioritise alerts using threat intelligence, reducing analyst fatigue and boosting response efficiency (Sharma, Kumar and Poojari, 2024). Cortex can further leverage these insights for automated incident enrichment and response orchestration. AI algorithms can enhance their ability to predict and respond to zero-day threats by simulating adversarial scenarios and training on attack patterns (Shashkov *et al.*, 2023). This aligns with the principles of AI adversarial training, emphasising resilience against evasive attack techniques.

Unlike traditional incident response, CDR focuses on real-time correlation of security events across multiple layers (network, endpoint, cloud). Automated mitigation strategies triggered by AI-driven insights and integration with threat intelligence to stay ahead of emerging threats. The challenges in existing CDR approaches include limited automation, which means that many organisations still rely on manual intervention for critical security decisions. Scalability issues where real-time data correlation across multiple security layers is complex. Integration bottlenecks where there is difficulty in integrating CDR capabilities with existing SIEM and SOAR tools. The gap identified is the need for a unified framework that seamlessly integrates SIEM, SOAR, and AI-driven CDR.

2.7 Security Operations and Analytics

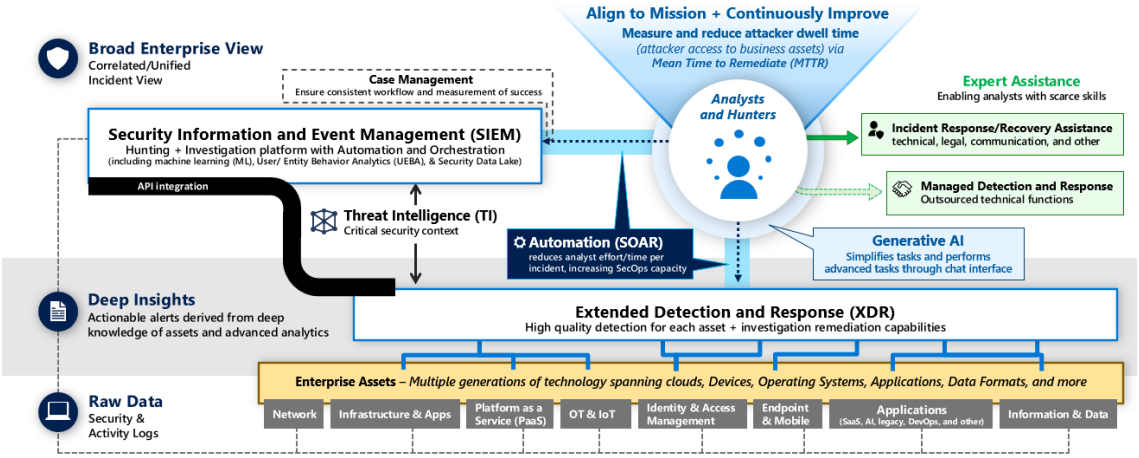

Figure 1: Graphical representation of a security operations center *(Microsoft, 2024)*

Figure 1 shows a SOC comprising various tools and technologies that enable security monitoring, threat detection, investigation, incident response, and data analysis capabilities. However, cybersecurity is a rapidly developing field, and new methods are needed to keep up with the increasing sophistication of cyber-attacks (Khan *et al.*, 2020). SOCs encounter challenges in performance, scalability, reliability, accuracy, speed, proactivity, collaboration, and communication. To overcome these, they should adopt the SOAF, which uses security analytics to improve efficiency and effectiveness.

Security operations and analytics (SOA) focuses on protecting organisations from cyber threats and improving their security posture. It involves collecting, analysing, and acting on security data from various sources like endpoints, networks, and applications to identify and respond to cyber threats effectively (González-Granadillo, González-Zarzosa and Diaz, 2021). These operations need an integrated framework for near real-time analysis, threat detection, and response. SOA combines security functions like vulnerability management and incident response to help organisations achieve CDR throughout the attack lifecycle while improving security performance and efficiency.

With the rise of sophisticated cyber threats, innovative tools and methods are crucial for adequate security and quick incident resolution.

2.7.1 Evolution of Security Operations and Analytics

The evolution of security operations has transitioned from basic protection measures like firewalls and antivirus software to advanced SIEM systems, integrating data from various sources to provide a comprehensive view of security risks and enable real-time monitoring (Kaliyaperumal, 2021). As cyber threats have become more sophisticated, adopting advanced analytics, machine learning, and AI has facilitated a shift from defensive to proactive and predictive cybersecurity strategies (Nassar and Kamal, 2021). This has led to the development of predictive analytics, behaviour analysis, and automated response capabilities (Bouchama and Kamal, 2021; Yeboah-Ofori et al., 2021). The rise of APTs necessitated continuous monitoring and real-time analysis to detect and mitigate threats (Jabar and Mahinderjit Singh, 2022). XDR and SOAR platforms further advanced security operations by integrating network and cloud data, automating tasks, and improving incident response (GEORGE et al., 2021)(Kinyua and Awuah, 2021). The latest evolution involves AI and big data, which enhance threat detection accuracy and response speed and shift security operations to proactive and predictive approaches.

2.7.2 Security Operations and Analytics Framework

The SOAF is a framework that integrates security tools and technologies to enhance security operations management. It supports proactive and data-driven monitoring, threat detection, investigation, incident response, and analytics.

SOAF unifies key security operations into an architecture that includes SIEM, IDS, and advanced analytics for comprehensive monitoring, threat detection, incident response, and continuous security improvement (GEORGE et al., 2021). SIEM is central to SOAF, providing data aggregation, analysis, and correlation from various sources to ensure comprehensive IT visibility and aid in detecting suspicious activities signalling security breaches (Tewari, 2021). Integrated into SOAF, IDS is crucial for monitoring network and system activities, enhancing the framework's ability to detect and respond to both external and internal threats (Martins *et al.*, 2022). SOAF uses advanced data processing, machine learning, and analytics to detect trends and anomalies in large datasets, which is crucial for identifying sophisticated cyberattacks and zero-day exploits (GEORGE et al., 2021).

SOAF enhances incident response efficiency by integrating TheHive for incident management and Cortex for automation. This enables rapid responses and reduces the time attackers have to cause damage (Ilca, Lucian and Balan, 2023). Although SOAF offers significant benefits, its implementation is challenging due to tool integration complexities, the need for skilled personnel, and potential data overload, requiring organisations to have the right skills and strategies to leverage its capabilities effectively (Perifanis and Kitsios, 2023).

Table 6: Key aspects of the SOAF

Aspects	**Description**
Data Collection	Information gathering from diverse sources, such as network nodes, security software, and external threat information feeds.
Data Processing	Normalising, enriching, and correlating the collected data to generate actionable insights.
Threat Detection and Investigation	Identifying potential threats and security incidents by analysing the processed data using ML algorithms, rules, and heuristics.

Incident Response	Implementing automated and manual processes for responding to and mitigating detected threats and incidents.
Reporting	Providing real-time and historical reports on the organisation's security posture, threat landscape, and incident response activities.

2.7.3 Security Operations and Analytics Platform

The SOAP is a comprehensive solution designed to facilitate deploying a security operations and analytics framework. It integrates SIEM and SOAR technologies, enabling organisations to collect, process, and analyse security data from multiple sources efficiently. By consolidating security information into a centralised system, SOAP enhances real-time monitoring, threat detection, incident investigation, and automated response mechanisms, thereby strengthening an organisation's cybersecurity posture (Chamkar, Maleh and Gherabi, 2024).

Furthermore, SOAP leverages advanced analytics and ML algorithms to streamline security operations and automate workflows. As a technology-agnostic platform, it employs AI for sentiment analysis, allowing security teams to identify hostile communications and automate responses to operational tickets. This level of automation significantly enhances efficiency by reducing manual workload, enabling security analysts to focus on more critical decision-making tasks (Kinyua and Awuah, 2021).

One of the significant challenges in cybersecurity is obtaining comprehensive visibility across complex IT and Operational Technology (OT) environments. The SOAF addresses this challenge by bridging visibility gaps that leave organisations vulnerable to threats. SOAF provides businesses with a holistic and unified view of network activity and security events, helping them improve threat detection, enhance performance, and strengthen overall security (Kinyua and Awuah, 2021; Wen, Shukla and Katt, 2024). By incorporating AI-driven analytics, SOAF expands an organisation’s monitoring capabilities, ensuring robust protection across cloud, on-premises, and hybrid environments. Moreover, AI-driven automation reduces the burden of routine tasks, improving accuracy and consistency while freeing up analysts to focus on higher-priority security decisions (Hashmi, Yamin and Yayilgan, 2024).

SOAP consists of five core components—Wazuh, Elasticsearch, Kibana, TheHive, and Cortex—each serving a distinct function within the framework. Wazuh provides endpoint security and log analysis (Wazuh, 2023), Elasticsearch enables scalable search and data

indexing (Bassett and Paquette, 2018), Kibana offers powerful data visualisation(Ahmed et al., 2020; Shah, Willick and Mago, 2022), TheHive facilitates security incident management, and Cortex automates threat intelligence analysis (Groenewegen and Janssen, 2021; TheHive Project, 2023). By integrating these tools, SOAF enhances organisational security defences through continuous detection, automated threat response, and real-time analysis. The adoption of SOAF signifies a paradigm shift from a reactive to a proactive cybersecurity approach, enabling organisations to stay ahead of evolving threats and strengthen their security resilience (Rosa-Remedios and Caballero-Gil, 2024).

Table 7: SOAP Components

Component	**Description**
Wazuh	An open-source security monitoring solution that provides intrusion detection, log analysis, and compliance reporting capabilities.
Elasticsearch	An engine for analytics and distributed searches that provide organisations with storage access, search capabilities, and near real-time analytics of large volumes of data.
Kibana	A data visualisation tool that integrates with Elasticsearch, allowing users to create interactive dashboards and visualisations for security data analysis.
TheHive	An open-source incident response platform that supports case management, collaboration, and automation for security incident response.
Cortex	An open-source tool for automating analysis and response tasks, which can be integrated with TheHive to enhance its incident response capabilities.

2.7.3.1 Wazuh

Wazuh is an open-source security detection, visibility, and compliance project that provides intrusion detection, log analysis, contributes to the early identification of potential breaches and anomaly detection (Suryantoro, Purnomosidi and Andriyani, 2022;

Wazuh, 2023). (Stanković, Gajin and Petrović, 2022) discuss how Wazuh's versatility and scalability make it an ideal solution for organisations of various sizes and how it has been integrated into many security operations and analytics platforms.

2.7.3.2 Elasticsearch and Kibana

Elasticsearch is a freely available software that functions as a search and analysis tool capable of handling large amounts of text data. It provides an extensive selection of customising choices (Zamfir *et al.*, 2019). It allows for the real-time storage, search, and analysis of big data, which is essential for security operations (Shah, Willick and Mago, 2022). Elasticsearch's high scalability and performance have made it a popular choice for cybersecurity applications (Demertzis *et al.*, 2021).

Kibana is a freely available tool for visualising and investigating data in Elasticsearch (Shah, Willick and Mago, 2022). It allows users to search and view their data in various formats, making it a valuable tool for security operations and analytics. Kibana's visualisation capabilities complement Elasticsearch's data analysis capabilities, providing a comprehensive solution for security data analysis (Bakraouy *et al.*, 2024).

Elasticsearch and Kibana amplify data visualisation and analysis capabilities, aiding in the interpretation of vast amounts of security-related data (Nour, Pourzandi and Debbabi, 2023), (Shah, Willick and Mago, 2022)

2.7.3.3 TheHive and Cortex

TheHive is a scalable, open-source Information Security Incident Response Platform designed to make incident response more effortless and efficient (TheHive, 2021). TheHive integrates with Malware Information Sharing Platform (MISP) and allows for the automation of specific tasks, which can be crucial for rapidly responding to security incidents. It offers a web-based interface for monitoring and managing security alerts from many sources, including SIEM, endpoints, and MISP (Groenewegen and Janssen, 2021) (Olukoya, 2021) discuss how TheHive's ability to collaborate on incident response and case management makes it an essential part of SOAF. Additionally, TheHive4py, the Python Application Programming Interface (API) client for TheHive, provides access to most of its endpoints through the Representational State Transfer (REST) API (TheHive Project, 2023). The case is the fundamental framework for the majority of security investigations, and it is the central concept of TheHive. The defining characteristics are the title, description, and date of a case. It is distinguished by a number of components, some of which are detailed in the following sections (TheHive Project, 2023).

One of the components is the tasks used to monitor and document the measures done to address the investigative enquiries and monitor the containment, elimination, and remediation activities. Multiple logs may include text entries that document an analyst's work, attach evidence or important files, and even password-protected ZIP packages containing malware or suspicious data. Another component is the observables, which may vary in nature, including IP addresses, email addresses, URLs, and domains. Furthermore, it is possible to create bespoke observable types if necessary. They may be classified as an Indicator of Compromise (IoC), which is a method used to identify and assess computer intrusions. If an observable in a case has been previously observed in other instances, it is automatically labelled as sighted, and cases with common observables are deemed connected. Another component is the tags, which serve as an additional means of including information in a case and may be used for efficient searching and filtering. These labels may be affixed to cases and other objects in TheHive such as alerts and observables. One may add the source of an observable by using a tag. TheHive streamlines the process of building cases by using pre-established case templates. These templates may be used to generate cases based on an alert or built from scratch. The resulting cases and alerts will have shared attributes, including the observables detected in a security event.

Case templates may be used to create cases from imported alerts. TheHive is distinguished by its emphasis on collaboration since each analyst is granted an account with certain rights and access to a real-time live stream. Assigning cases and tasks to an analyst enables numerous analysts to collaborate on the same case while carrying out separate responsibilities. In order to track the advancement of cases and tasks, each individual case and duty may undergo many phases that need distinct actions and responsibilities. For instance, a case may be in the inception, examination, settlement, or conclusion phases. A duty may exist in one of four stages: assignment, execution, verification, or completion. To streamline the progress of each phase, the system has the capability to generate cases and allocate responsibilities automatically, emphasise the necessary procedures and instructions for each team member, and monitor the actions and results of each case and duty.

Cortex, developed by TheHive Project, is a freely available engine for analysing and responding to observable data. It allows for the scalability of observable analysis by querying a single tool instead of numerous ones. Cortex provides a web-based interface for studying observables either individually or in bulk. It has the ability to automate

activities and send large sets of data using TheHive or the Cortex REST API. Cortex4py, the Python API client for Cortex, provides access to the majority of Cortex REST API endpoints. The Cortex core engine is based on autonomous applications known as neurones. There are two sorts of neurones: analysers and responders. Analysers automate interactions with services or tools to speed up analysis and detect dangers before they become a problem. Responders take action on alarms, cases, tasks, task logs, and observables when used with TheHive. The online interface allows for the activation, deactivation, and customisation of analysers and responders, including the adjustment of settings such as rate limits, usernames, passwords, and API keys. When a detectable object is submitted for examination, Cortex creates a task that, if successful, produces an analysis report in JSON format. A job may be stored in a cache for future analysis. A job is generated when a responder is activated, which produces a JSON report on the result of the action. The integration of Cortex introduces automation and orchestration, streamlining incident handling (TheHive Project, 2023)

2.7.3.4 Cyber Threat Intelligence

An incident analysis involves extracting and analysing distinct pieces of information, such as Uniform Resource Locators (URL), file header data, IP addresses and domains. An observable is an event, such as a particular IP address, that necessitates additional analysis if deemed malevolent (Lin *et al.*, 2018; Hettema, 2021). An IoC is a sign of a computer intrusion or malicious activity, such as phishing or spamming (Haber *et al.*, 2020). Observables can be analysed using online tools such as VirusTotal and simulation services.

IOCs consist of collected and analysed forensic data related to potential malicious activity or intrusions. Antivirus software and intrusion detection systems utilise IOCs to scan computer systems for known signatures of previous attacks, enabling them to detect and prevent future attacks that match these indicators (Kartak and Bashmakov, 2022). However, they can miss novel or sophisticated attacks that evade the existing rules or signatures (Preuveneers and Joosen, 2021). Therefore, IOCs are insufficient to prevent unknown or advanced threats; they must be complemented with Cyber Threat Intelligence (CTI). CTI refers to information based on evidence that covers the background, methods, signs, consequences, and practical recommendations for dealing with a current or potential danger to a company's assets (Schlette, Caselli and Pernul, 2021). CTI requires extensive knowledge of threats, targets, adversaries, motives, and plans. Analysts primarily focus on the attack's end result, strategies, and signs of an impending attack.

Organisations gain access to valuable threat information through CTI's cyber threat information exchange, leveraging the knowledge and experience of others to transform detection into prevention. The three most significant open-source CTI frameworks are MISP, Cortex, and TheHive.

CTI plays a critical role in enhancing the CDR capabilities of a SOC within a security operations and analytics framework. By providing actionable insights into emerging threats, attacker TTPs, and IOCs, CTI enables SOC teams to identify and mitigate risks proactively. For instance, integrating CTI feeds into SIEM systems allows for real-time correlation of internal security events with known threat data, thereby improving threat detection accuracy (Ackermann, Karch and Kippe, 2023). Furthermore, CTI supports the investigation phase by offering context about the threat landscape, which helps analysts prioritise incidents and respond more effectively. This is particularly important during the incident response process, where timely and informed decisions are crucial to minimising damage and restoring normal operations. Additionally, CTI contributes to continuous improvement by feeding post-incident analysis with external threat data, enabling the SOC to refine its detection rules and automated incident response playbooks (Dykstra *et al.*, 2023).

Integrating CTI with SIEM, SOAR, EDR, and XDR tools enhances an organisation's security posture. It enables continuous refinement of detection models and adapts defences against emerging threats. This approach allows SOC teams to quickly detect, investigate, and neutralise threats, reducing dwell time and minimising the impact of cyberattacks (Chamkar, Maleh and Gherabi, 2024). CTI is essential for transforming SOCs from reactive units into proactive, intelligence-driven cybersecurity operations.

In summary, CTI acts as a force multiplier for SOC operations, bridging the gap between reactive security measures and proactive threat hunting, ultimately strengthening the organisation's overall security posture.

2.7.3.5 Malware Information Sharing Platform

The Malware Information Sharing Platform (MISP) is a free and open-source software that facilitates the exchange of threat intelligence, such as cyber security indicators (Mokaddem *et al.*, 2019). It seeks to enhance countermeasures against targeted attacks and implement preventative measures and detection. MISP saves IOCs in an organised way, which lets them be correlated, exported automatically to IDS or SIEM in STIX or OpenIOC, and kept in sync with other MISPs (MISP, 2023). It also facilitates the rapid

and efficient detection of attacks (Ongun *et al.*, 2021). MISP provides a user-friendly web interface, REST API, and PyMISP Python library for access. The event-building element of MISP comprises discrete data, such as IP addresses, URLs, and files. Each attribute is correlated; additional information can be added using identifiers and advanced features. MISP can connect to other MISP servers and share data; synchronisation is the process of exchanging data between instances. MISP can routinely integrate feeds and remote or local resources containing indicators regularly. Numerous open-source and proprietary applications, such as the open-source Security Incident Response Platform (SIRP) TheHive, support MISP.

2.7.4 Integrating Components for Continuous Detection and Response

CDR is an advanced cybersecurity approach emphasising continuous real-time monitoring, detection, and response to threats across endpoints, email, identity, and cloud environments. By leveraging cloud-based AI and ML, CDR integrates with security technologies like Wazuh, Elasticsearch, Kibana, TheHive, and Cortex to enhance organisational resilience against evolving threats such as malware, ransomware, phishing, zero-day exploits, and APTs (Karantzas and Patsakis, 2021)

This section explores how these tools collectively enable CDR within modern SOCs.

Wazuh is an open-source Host-based Intrusion Detection System (HIDS) that offers comprehensive security features such as log analysis, file integrity monitoring, rootkit detection, vulnerability assessment, and incident response capabilities (Wazuh, 2023). It collects data from diverse sources, including system logs, Windows events, and Sysmon logs, enabling continuous endpoint monitoring.

Key features of Wazuh include File Integrity Monitoring (FIM), which detects unauthorised changes to files or directories and alerts on potential tampering. Additionally, its Compliance Monitoring ensures adherence to security standards like PCI DSS, CIS, GDPR, and HIPAA. Wazuh's Incident Response capabilities enable it to execute predefined scripts or commands to mitigate threats. Furthermore, it integrates with platforms like Elasticsearch and Kibana for centralised alert management (Wazuh, 2023).

Wazuh leverages AI and ML algorithms to analyse alerts and correlate them with threat intelligence feeds from sources such as Microsoft 365 Defender and Cisco Secure Endpoint. This integration enables automated responses, including isolating

compromised systems or blocking malicious IPs, thereby reducing the mean response time (MTTR) (Wazuh, 2023).

Elasticsearch is a distributed search and analytics engine designed to handle large volumes of structured and unstructured data in near real-time (Kathare, Reddy and Prabhu, 2020). It serves as the backbone for CDR by ingesting data, performing complex queries, and scaling horizontally to support large-scale deployments. Specifically, Elasticsearch collects logs and events from Wazuh, firewalls, and other security tools, enabling comprehensive data aggregation. It facilitates advanced threat hunting through its RESTful API and query language, allowing SOC analysts to perform detailed and sophisticated queries on the collected data (Elastic Elasticsearch Guide, 2024). Additionally, Elasticsearch supports high availability and performance by adding nodes or clusters to handle increased data loads and ensure seamless operation (Elastic Elasticsearch Guide, 2024). Additionally, it can scale horizontally by adding more nodes or clusters to handle additional data or requests (Shah, Willick and Mago, 2022). Its integration with Kibana provides a unified platform for visualising and exploring security data, thereby enhancing the ability of SOC analysts to detect and respond to threats efficiently (Negoita and Carabas, 2020).

Kibana is a data visualisation tool that complements Elasticsearch by creating interactive dashboards, maps, and charts. It plays a critical role in CDR by visualising security data in real-time and displaying alerts and events from sources such as Wazuh, Suricata, and others. Kibana enables threat hunting by providing tools like Discover, Maps, and Timelion for interactive data exploration. Additionally, it supports machine learning to detect anomalies and outliers in security data, enabling proactive threat detection (Elastic Kibana Guide, 2024). Kibana's integration with Wazuh and Elasticsearch ensures that SOC teams have a comprehensive view of security incidents, facilitating faster decision-making and response.

TheHive is a scalable, open-source incident response platform that streamlines case management and collaboration. One of its key features is case creation, which converts alerts from sources such as Wazuh, Suricata, and MISP into actionable cases (Groenewegen and Janssen, 2021). This enables efficient management and investigation of security incidents. TheHive also supports team collaboration by assigning cases to analysts, tracking progress, and providing communication tools to facilitate coordination and information sharing among team members (Groenewegen and Janssen, 2021). Additionally, TheHive generates metrics and reports for post-incident analysis, helping

organisations understand and improve their incident response processes (TheHive Project, 2023).

Moreover, TheHive integrates with Cortex to enrich observables with threat intelligence, such as IP addresses, domains, and hashes. This integration enhances the accuracy and speed of incident response by providing additional context and information, enabling security teams to make informed decisions and take timely actions to mitigate threats.

Cortex is a powerful analysis engine that enriches observables with data from sources such as VirusTotal, Shodan, and MISP (Galdi et al., 2022). It supports CDR by analysing observables and providing reputation scores, geolocation data, and threat indicators. Furthermore, Cortex automates responses by executing actions such as blocking IPs or tagging malicious files using responders (Kaleem, 2022). This automation significantly enhances the efficiency and effectiveness of threat mitigation. Additionally, Cortex integrates with TheHive to strengthen case management by providing contextual data for investigations, enabling security teams to make informed decisions and respond swiftly to threats (TheHive Project, 2023).

TheHive and Cortex can integrate with Wazuh, Elasticsearch, and Kibana to collect security events and alerts for further investigation and case management. TheHive and Cortex can use Wazuh as a source of alerts that can be converted into cases or observables. TheHive and Cortex can also use Elasticsearch as a database to store alerts, cases, observables, and results for analysis. TheHive and Cortex can also use Kibana as a web interface to visualise and explore the data stored in Elasticsearch.

Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex creates a comprehensive CDR framework for modern SOCs. This framework enables real-time monitoring, as Wazuh collects and analyses endpoint data, while Elasticsearch ingests and stores logs for near-instantaneous querying. Additionally, it enhances threat detection by leveraging Kibana to visualise data and support machine learning-driven anomaly detection, while Cortex enriches observables with threat intelligence. TheHive manages cases and coordinates team efforts for incident response, while Wazuh and Cortex automate responses to mitigate threats effectively. This framework's modular architecture ensures scalability and flexibility, allowing organisations to tailor their security operations to specific needs and adapt to evolving threats (Sagar and Syrovatskyi, 2022).

While integrating tools such as Wazuh, Elasticsearch, Kibana, TheHive, and Cortex offers significant benefits, several research gaps remain. Firstly, limited studies evaluate

the combined use of these tools in real-world SOC environments (Soewito, 2024; Wazuh Blog, 2024). Secondly, further research is needed to optimise resource allocation and reduce overhead in large-scale deployments (Pasdar *et al.*, 2024). Lastly, more work is required to improve the accuracy and efficiency of AI/ML algorithms for threat detection and response (Salem et al., 2024). By addressing these research gaps, organisations can enhance their ability to effectively leverage these integrated tools, improving their overall security posture and resilience against evolving cyber threats.

In conclusion, this research has delineated the application of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex within the SOAF with CDR. The central assertion of this study is that CDR represents an innovative approach to cybersecurity, offering continuous monitoring, real-time analytics, threat intelligence, automation, detection, and response capabilities across various vectors such as endpoints, email, and identity by harnessing cloud-based AI and ML and integrating these with other security technologies. Furthermore, this research has proposed several implications and recommendations for future research or practice. These include investigating the potential benefits and challenges of implementing CDR across different sectors or scenarios, developing ethical and legal frameworks to govern CDR usage, and encouraging collaboration and educational initiatives among stakeholders to enhance the understanding and efficacy of CDR technologies in combating cyber threats. CDR stands out as a transformative technology with the potential to significantly improve the security and resilience of enterprises in the face of cyber-attacks.

An essential technical example of implementing CDR is found in the healthcare sector, which manages sensitive patient information and critical infrastructure. This context offers a valuable opportunity to examine CDR's potential benefits and challenges. For example, a hospital network utilising CDR can leverage advanced EDR tools and SIEM systems. This integration enables real-time monitoring of medical devices, electronic health records (EHRs), and internal networks, allowing for the rapid identification of anomalies, such as unauthorised access to patient data or ransomware attacks on medical devices (Nemec Zlatolas, Welzer and Lhotska, 2024). However, challenges arise due to the complexity of healthcare IT environments, which often include legacy systems that are difficult to secure and integrate with modern CDR solutions. Furthermore, the sector faces stringent regulatory requirements, GDPR in the UK, which necessitate robust ethical and legal frameworks to govern CDR usage while ensuring patient privacy and data integrity (Wylde *et al.*, 2022). To address these challenges, collaboration among

stakeholders is essential. Healthcare providers, technology vendors, and regulatory bodies should develop standardised protocols for CDR implementation to ensure legal and ethical compliance. Training programs for healthcare IT staff on CDR technologies and cyber threat intelligence can further enhance the sector's ability to combat cyber threats (Frati *et al.*, 2024). By encouraging collaboration and education, the healthcare sector can enhance the benefits of CDR, including faster incident response and stronger defences against cyber-attacks, while also addressing potential risks. CDR is a transformative technology that can greatly enhance the security and resilience of healthcare organisations, safeguarding patient data and critical infrastructure.

2.7.5 Related work on Security Operations and Analytics platforms using Wazuh, Elasticsearch, Kibana, TheHive, and Cortex

This section reviews existing literature on security operations and analytics frameworks to understand the current research landscape comprehensively. By analysing previous studies, gaps, strengths, and limitations were identified, paving the way for further advancements in this field. The related work on Security Operations and Analytics platforms that utilise tools like Wazuh, Elasticsearch, Kibana, TheHive, and Cortex reveals a comprehensive approach to modern cybersecurity needs. This integrated suite of tools provides a multifaceted framework that enhances the detection, analysis, response, and management of security incidents, making it a crucial subject of study in cybersecurity literature.

Several studies have explored integrating various security tools and technologies to develop comprehensive security operations and analytics platforms. For example, research into the effectiveness of combining these platforms has shown that such integration not only improves the detection and response rates but also enhances the overall security posture by providing an enhanced understanding of the scope of potential threats (Mughal, 2022).

The tools provide scalability and flexibility. They also allow organisations to tailor their security operations to specific needs, which is crucial given the diverse nature of threats faced by different industries. Further research into the modular deployment of these tools has suggested improvements in the management of resource allocation, thereby optimising operational efficiency and reducing overhead (Sankar and Fasila, 2023).

However, most of the previous research has concentrated on individual elements of a security operations and analytics platform or certain scenarios rather than the combined

use of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. The shared utilisation of resources plays a substantial role in developing theoretical frameworks in cybersecurity operations. An in-depth study is required to develop and evaluate a holistic security operations and analytics framework using Wazuh, Elasticsearch, Kibana, TheHive, and Cortex as these tools embody the principles of continuous monitoring, real-time analytics, and integrated incident management, which are pivotal in the development of advanced SOCs. They are practical implementations of theoretical models that advocate for layered security defences and proactive threat management strategies.

Table 8: Comparative Analysis of Security Operations and Analytics Tools

Study	**Focus Area**	**Key Findings**	**Strengths**	**Limitations**
Study 1: Integration of Wazuh and Elasticsearch (Wazuh, 2023)	Log analysis, threat detection, and compliance monitoring	Integration enhances threat detection and log management efficiency.	Scalable and efficient in detecting security events.	Limited visualisation capabilities without Kibana.
Study 2: Incident Response with TheHive and Cortex (Groenewegen and Janssen, 2021)	Automated incident response and case management	TheHive and Cortex improve incident handling but require better SIEM integration.	Streamlines investigation workflows with automation.	High dependency on integration with SIEM platforms.
This Study: Holistic Framework using Wazuh, Elasticsearch, Kibana, TheHive, and Cortex	Comprehensive security operations and analytics framework	A combined approach improves security posture but requires further optimisation.	Enhances real-time analytics and incident response capabilities.	Requires fine-tuning for scalability and resource allocation.

The integration of tools such as Wazuh, Elasticsearch, Kibana, TheHive, and Cortex significantly improves detection rates, response times, and organisations' overall security posture. These tools offer scalability and flexibility, allowing organisations to tailor security operations to meet specific needs. However, further study is needed to address resource allocation and optimisation. Most studies focus on individual tools or scenarios rather than combined use. There is limited research on modular deployment and resource optimisation. Additionally, there is a lack of holistic frameworks that leverage the combined use of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex.

Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex provides a comprehensive approach to modern cybersecurity needs. Nevertheless, further research is necessary to evaluate their combined effectiveness, scalability, and resource optimisation in advanced SOCs. SOA collects, analyses, and correlates security data to improve decision-making. Modern security analytics leverage big data processing, machine learning, and real-time insights. Challenges in current security analytics include the lack of real-time insights where many analytics tools rely on batch processing, delaying response times. Data fragmentation where security data often exists in isolated silos, limiting visibility. Inconsistent threat intelligence usage, where some organisations struggle to integrate real-time threat intelligence into security operations. The gap identified is the need for a SOAF that unifies real-time data processing, automation, and AI-driven analytics.

2.8 Contribution

One major step forward in cybersecurity is the creation of SOAFs that use the Design Science Research (DSR) approach. By integrating tools such as Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, the DSR methodology facilitates a systematic approach to the creation, implementation, and evaluation of systems that bolster automation and CDR. This structured approach not only addresses complex cybersecurity challenges methodically but also fosters the creation of innovative and practical knowledge and solutions.

Furthermore, this study offers empirical data and insights into the application of SOAP for the implementation of SOAF, thereby enhancing organisational cybersecurity. It introduces a standardised framework that allows for the evaluation and comparison of SOAP solutions, with a focus on the performance metrics related to data sources, processing, analysis, and visualisation.

DSR is a framework that guides the development of technological solutions. It can help SOAF create innovative features that improve the integration of different tools within the framework. By following a rigorous process, DSR ensures that the development of SOAF is based on validated research protocols, enhancing both the utility and robustness of the framework (vom Brocke, Hevner and Maedche, 2020). DSR focuses on addressing real-world problems with innovative solutions. In the context of SOAF, using DSR allows researchers and developers to directly tackle specific challenges in cybersecurity operations, such as automation of responses and enhancement of detection capabilities. This approach provides confidence that the framework will operate as intended in reality and not only in theory (Peffers et al., 2020). The dual focus on theory and practice in DSR allows for significant contributions both to the body of knowledge and to its practical applications. By developing a SOAF that integrates Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, researchers can provide empirical evidence on the effectiveness of these integrations and also offer insights into best practices for designing similar systems. This knowledge could be valuable for both academic researchers and cybersecurity professionals (Gregor and Hevner, 2013).

Employing DSR in the development of a SOAF has multifaceted and impactful practical contributions. Firstly, the iterative design and testing phases inherent in DSR enable the SOAF to be fine-tuned, thereby enhancing its automation and CDR capabilities. This fine-tuning may include the creation of sophisticated algorithms for anomaly detection, the incorporation of machine learning for predictive analytics, or the refinement of response protocols to mitigate the effects of security breaches.

Moreover, the design science approach fosters the exploration of innovative integration techniques. These techniques can significantly improve the interoperability between tools such as Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, leading to smoother operations and more efficient data utilisation within the SOAF. Consequently, this can result in more robust security management. Additionally, DSR advocates for the creation of systems that are not only effective but also adaptable and scalable. As a result, a SOAF developed through DSR is expected to be sufficiently flexible to integrate emerging security tools and technologies and scalable to serve the varying needs of both small and large organisations.

In pursuit of these goals, the research employs a diverse array of methods, including surveys, interviews, and case studies, to analyse the application of SOAP across various companies. The aim was to identify effective practices that enhance SOAP, to deliberate

on the implications and challenges of adapting SOAP in dynamic ICT environments, and to explore the potential advantages and difficulties of combining SOAP with big data analytics tools. This comprehensive approach was designed to deepen the understanding of SOAP's contribution to advancing cybersecurity in a range of organisational settings.

2.9 Conclusion

The literature review provides an overview of security operations and analytics, security operations and analytics frameworks, and security operations and analytics platforms. It also highlights related work integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex in security operations and analytics platforms. The research questions in section 1.5 were the intended focus of the literature review. By looking into the research methodologies and previous studies, this study seeks to enhance the growing body of knowledge surrounding SOAFs and their role in bolstering cybersecurity resilience. To illustrate this point, the literature review highlights the importance of integrated security operations and analytics frameworks in addressing the growing complexity of cyber threats. It discusses the evolution of SOCs, the role of SIEM and SOAR platforms, the application of AI and ML in cybersecurity, and the emergence of CDR as a critical concept in modern security operations and analytics.

The research agenda was developed based on the gaps identified in this literature review, focusing on:

Developing an Integrated SOAF - A framework that combines SIEM, SOAR, AI/ML, and Continuous Detection and Response to enhance security monitoring and automation.

Optimising Threat Detection and Response Through AI and Automation - Implementing machine learning-driven security analytics to improve real-time threat correlation and response.

Enhancing Security Tool Integration and Interoperability - Designing a seamless integration of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex into a single, unified SOAF solution.

Reducing False Positives and Improving Response Efficiency - Leveraging AI/ML to reduce alert fatigue and automate incident response workflows.

Ensuring Scalability and Adaptability of the Framework - Developing SOAF to be scalable across enterprises while adapting to emerging threats and evolving security landscapes.

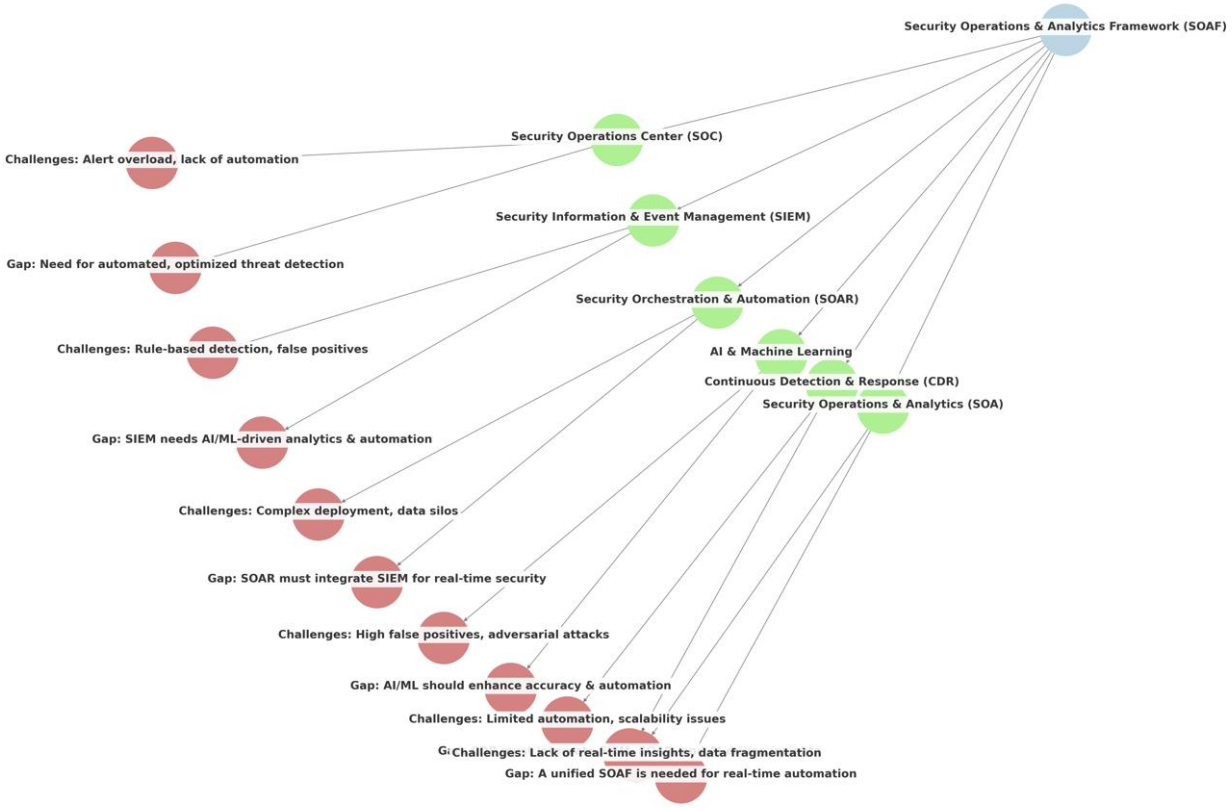

Figure 2: Mind Map - Literature Review On SOAF

Table 9: Literature Review Table

Topic	**Key Insights**	**Identified Research Gaps**
Security Operations Center (SOC)	Challenges: Alert overload, lack of automation, integration issues.	Need for automated and optimised threat detection and mitigation.
Security Information and Event Management (SIEM)	Limitations: Rule-based detection, false positives, scalability issues.	SIEM needs AI/ML-driven analytics and automation.
Security Orchestration, Automation, and Response (SOAR)	Problems: Complex deployment, data silos, weak threat intelligence integration.	SOAR should be seamlessly integrated with SIEM for real-time security analytics.
AI and Machine Learning in Cybersecurity	Challenges: High false positives, adversarial attacks, model interpretability.	AI/ML should enhance accuracy and automation in a holistic security framework.
Continuous Detection and Response (CDR)	Issues: Limited automation, scalability problems, integration bottlenecks.	CDR must integrate SIEM, SOAR, and AI-driven security insights.
Security Operations and Analytics (SOA)	Challenges: Lack of real-time insights, data fragmentation, weak threat intelligence usage.	A unified SOAF is needed for real-time analytics, automation, and integration.

Chapter 3: Research Methodology

This chapter outlines the research approach and methodologies adopted to investigate how the SOAF enhances enterprises' security posture. Specifically, the study explores designing, implementing, and evaluating a security operations and analytics platform that integrates Wazuh, Elasticsearch, Kibana, TheHive, and Cortex for automation and CDR.

Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex within the SOAF advances cybersecurity operations beyond existing frameworks. The table below highlights how the integration significantly enhances the field.

Table 10: How the specific integration of tools and methods advances the field beyond existing frameworks

Description	**Existing Challenge**	**SOAF Advancement**	**How It Advances the Field**
Enhanced Threat Detection Through Real-Time Correlation and Analytics	Traditional SIEM systems often rely on rule-based detection that can miss unknown threats.	Elasticsearch and Kibana provide real-time data ingestion, indexing, and visualisation for security monitoring. Wazuh acts as an XDR solution, correlating events across endpoints and networks.	The integration reduces blind spots in security monitoring by correlating real-time threat data across multiple sources.
Automation of Incident Response and Threat Intelligence Integration	Many organisations struggle with manual and fragmented incident response processes.	TheHive streamlines security incident response by managing cases, collaborating across teams, and tracking remediation efforts.	Integrating TheHive and Cortex enables automated enrichment, case tracking, and workflow

		Cortex automates threat intelligence enrichment by executing various analyzers on security solutions.	automation, reducing response time.
CDR vs. Traditional Periodic Assessments	Traditional SOC workflows involve periodic log reviews, leaving security teams unaware of fast-moving threats.	Wazuh provides endpoint monitoring, Elasticsearch stores security events, and Kibana visualises alerts for continuous monitoring.	SOAF supports CDR by automating anomaly detection, triggering responses, and dynamically adjusting defences.
Improved Security Data Orchestration and Customisation	SIEM and SOAR platforms often lack flexibility in integrating custom workflows, leading to siloed and inefficient security operations.	All five tools are open-source, allowing complete customisation and seamless integration into different environments.	Security teams can build tailored security workflows, analytics dashboards, and response automation that fit their unique operational needs.
Cost-Effective Alternative to Proprietary SIEM and SOAR Solutions	Enterprise-grade SIEM and SOAR solutions (e.g., Splunk, IBM QRadar) are expensive and often	By integrating open-source tools, organisations achieve enterprise-level security capabilities without high licensing costs.	This framework provides a scalable, cost-effective solution for security teams, particularly in

	require extensive vendor lock-in.		resource-constrained environments.
Scalability and Cloud Readiness	Many legacy security monitoring solutions are not optimised for cloud and hybrid infrastructures.	Elasticsearch provides scalable log storage, Wazuh supports cloud and hybrid environments, and TheHive/Cortex work seamlessly with API-driven cloud security tools.	SOAF enables multi-cloud security analytics, making it ideal for modern cloud-centric architectures.
Advanced Anomaly Detection and AI/ML Integration Readiness	Many SIEM solutions rely on signature-based detection rather than behavioural analytics or anomaly detection.	SOAF can be extended with AI/ML models for behavioural threat detection. Elasticsearch supports machine learning plugins, enabling anomaly detection in security logs.	This framework creates a foundation for AI-driven security analytics, enhancing predictive threat detection.

The integration of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex within the SOAF framework significantly enhances traditional SOC workflows by improving real-time threat detection and correlation, automating incident response and intelligence enrichment, and enabling continuous, AI-driven security monitoring. Furthermore, this approach reduces operational costs while enhancing flexibility and provides a scalable, cloud-ready cybersecurity framework. This comprehensive strategy effectively bridges the gaps between SIEM, SOAR, XDR, and CDR, establishing a new standard for cybersecurity operations.

The illustration below shows the advancements of SOAF over existing cybersecurity frameworks

Figure 3: Advancements of SOAF Over Existing Cybersecurity Frameworks

Given cybersecurity threats' dynamic and evolving nature, a pragmatic research approach is applied to balance theoretical rigour with real-world applicability. Pragmatism allows researchers to integrate multiple methodologies, ensuring the research remains adaptive and solution-oriented (Zare *et al.*, 2024). This approach is particularly suited for security operations and analytics, where continuous improvement and real-world application are key factors in cybersecurity effectiveness.

To ensure a structured research process, the study follows Saunders' Research Onion Model, illustrated in Figure 2, which provides a layered approach to research design. This model is widely applied in information systems research, as it helps define philosophical stances, methodological choices, research strategies, and data collection techniques (Saunders, Lewis and Thornhill, 2019).

The research process involves a structured overview of the research design and execution, which ensures that the study follows a systematic and organised approach from start to finish. DSR is a methodological framework that guides the development, implementation, and evaluation of the SOAF. This framework ensures that the research is grounded in a solid theoretical foundation while also being practical and applicable. Qualitative research methods and research design encompass the data collection and analysis

techniques used to assess the effectiveness of SOAF. These methods provide valuable insights into the framework's practical application and impact. Ethical considerations are crucial in research, addressing research ethics, data security, and compliance. Ensuring that the study adheres to ethical guidelines helps protect participants' rights and privacy and maintains the research's integrity.

Integrating these elements makes the research process more coherent, comprehensive, and aligned with the best research design and methodology practices.

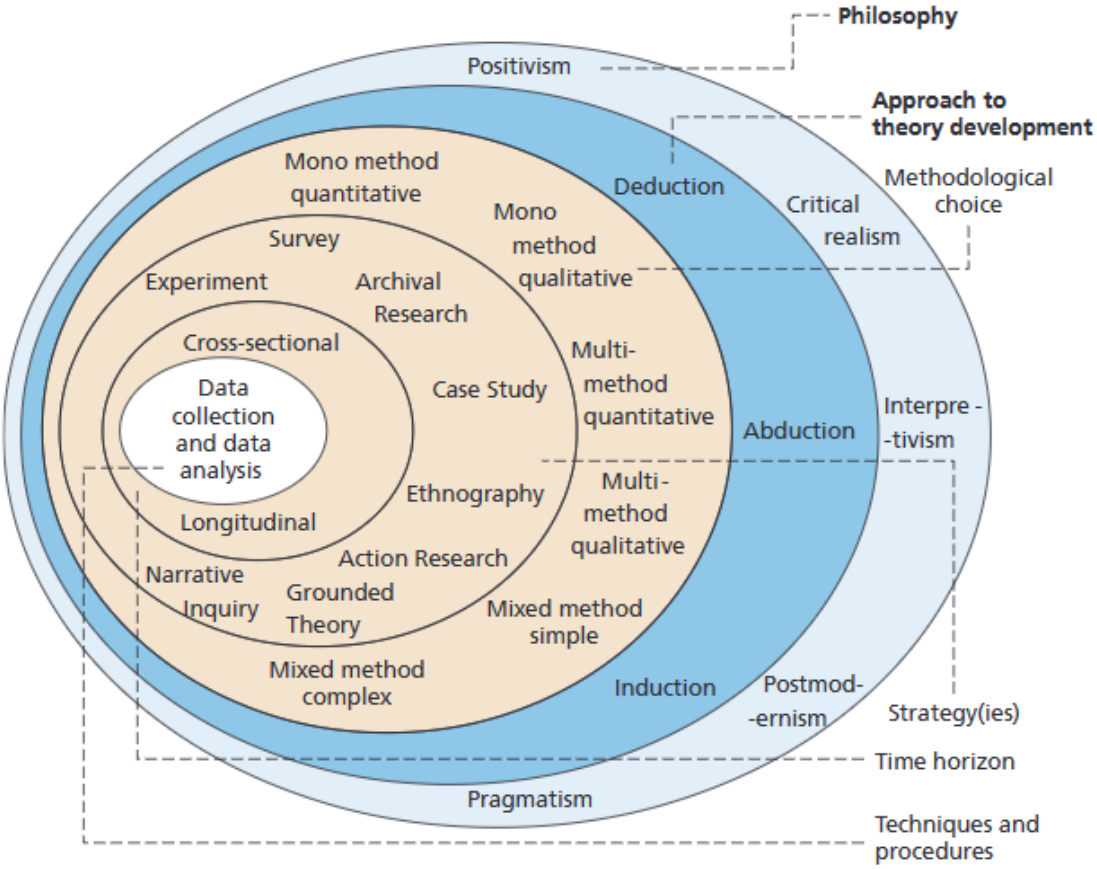

Figure 4: Research Onion (Saunders, Lewis and Thornhill, 2019)

3.1 Research Process

This chapter outlines the research philosophy and approach adopted for conducting a DSR study to enhance a SOAF. The study leverages an integrated platform comprising Wazuh,

Elasticsearch, Kibana, TheHive, and Cortex to improve automation and CDR capabilities in cybersecurity operations.

Identifying key research steps is crucial for the success of this study. These steps guide the research process based on the problem's nature and defined objectives. These steps include research philosophy, approach, and methodology (Saunders, Lewis and Thornhill, 2018), as detailed in the following sections.

3.1.1 Research Philosophy

Research philosophy is a crucial aspect of the research process, shaping researchers' approach, study design, techniques, and analysis (Tamminen and Poucher, 2020). It is the set of beliefs that underlie the research process, such as the nature of reality, the sources and validity of knowledge, and the role of values and ethics in research. It focuses on the nature of knowledge and its creation, shaping research techniques and procedures (Saunders, Lewis and Thornhill, 2019), asserted that there were four main types of research philosophy: positivism, realism, interpretivism, and pragmatism. Each type of research philosophy has different implications for the choice and use of research methods and techniques.

This research effort employs pragmatism, a research philosophy that prioritises the practical outcomes and use of research rather than strict adherence to a preset or established worldview (Saunders, Lewis and Thornhill, 2019). It enables researchers to adopt multiple methods and perspectives to tackle complex problems and evaluate their relevance, validity, and reliability. Pragmatism acknowledges that researchers are influenced by their values, interests, and experiences, encouraging transparency and reflexivity in their choices and actions (Saunders, Lewis and Thornhill, 2019).

The rationale for choosing pragmatism as the research philosophy for this project is that it aligns with the aim and objectives of the study, which is to design and evaluate the SOAF using SOAP for automation and CDR. The SOAF is a specific type of SOC framework that leverages security analytics technologies intending to improve the operational efficiency and efficacy of SOCs. The SOAF integrates data and alerts from multiple security domains, such as endpoints, networks, clouds, and identities, and provides a unified view of the threat landscape and the attack chain. The SOAF also applies advanced analytics techniques like ML and AI to improve threat detection, investigation, response accuracy, and speed. Moreover, the SOAF enables proactive security by using the latest threat intelligence to identify and address system or process

vulnerabilities before attackers exploit them. Furthermore, the SOAF facilitates collaboration and communication among stakeholders, such as SOC analysts, incident responders, application owners, and business leaders.

3.1.2 Research Approach

The research approach defines how inquiries are formulated, data is collected and analysed, and findings are disseminated. Research methodologies are classified into three categories: abductive, inductive, and deductive (Saunders, Lewis and Thornhill, 2019).

This study employs an abductive reasoning approach, integrating deductive and inductive logic to generate innovative solutions for complex cybersecurity challenges (Saunders, Lewis and Thornhill, 2019). Abductive reasoning allows researchers to test existing theories (deductive logic), derive new insights from data (inductive logic), and develop novel solutions that address gaps in existing frameworks (abductive logic).

A diverse methods approach was also adopted, combining DSR and qualitative methods. DSR focuses on developing innovative solutions—such as frameworks, models, and systems—to address practical problems (Peffers et al., 2020). Qualitative approaches include collecting and analysing non-numerical data, including audio, text, or video, to gain insights into ideas, views, or experiences. The diverse methods research approach combines qualitative and DSR methods and is a comprehensive research strategy that aims to provide a holistic understanding of a particular issue. This approach draws on the strengths of qualitative and DSR methods to gather extensive, context-specific insights and develop practical solutions. The mixed-methods approach consisted of the following phases:

The problem identification phase involved identifying key security operations and analytics challenges through an in-depth examination of current practices. Discussions were conducted with 15 industry experts, cybersecurity practitioners, and stakeholders, selected based on their experience and relevance to the study (Vielberth, Böhm and Fichtinger, 2020).

A systematic literature review was conducted to examine existing security operations and analytics frameworks, including Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. The review identified key gaps, such as the lack of integration between threat detection and response automation, which informed the research objectives and hypotheses.

Specifically, the study aimed to design a framework that addresses these gaps by integrating security operations and analytics for improved automation and efficiency.

3.1.3 Research Design

Research design is applying the research approach to studying a SOAF that integrates Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. The focus is on leveraging DSR and qualitative methods to develop, implement, and evaluate the framework's capabilities in enhancing automation and improving CDR within cybersecurity operations. It involves choosing and applying the appropriate methods and techniques for sampling, data collection, and data analysis (Asenahabi, 2019). Research design is essential for a rigorous and valid study (Sileyew, 2019).

3.2 Qualitative Research Methods

Qualitative research is a methodological approach focused on exploring complex human experiences, perceptions, and behaviours by addressing "how" and "why" questions rather than quantitative metrics (Yadav, 2022). It employs data collection methods such as interviews, focus groups, observations, and document analysis to obtain rich, detailed insights (Magida, 2024). Sampling techniques like purposive or theoretical sampling ensure meaningful participant selection, emphasising depth over breadth (Rana, Poudel and Chimoriya, 2023; Ahmad and Wilkins, 2024). Data analysis involves identifying patterns and themes through techniques such as thematic analysis and grounded theory (Miles, Huberman and Saldaña, 2021). The iterative nature of qualitative research allows for adaptability, refining the research process as new insights emerge (Pilcher and Cortazzi, 2024). To ensure validity, techniques like triangulation and member checking enhance credibility and rigour (Dado, Spence and Elliot, 2023; Ahmed, 2024a). In cybersecurity research, qualitative methods are instrumental in understanding human and organisational factors, informing security frameworks, improving automation, and strengthening cybersecurity posture (Nyre-Yu, Gutzwiller and Caldwell, 2019).

3.2.1 Purpose of Qualitative Methods in this Study

This study used qualitative research methods to understand how security operations teams experienced and perceived the challenges of using a security operations and analytics platform that included Wazuh, Elasticsearch, Kibana, TheHive, and Cortex (Fujs, Mihelič and Vrhovec, 2019). Furthermore, the qualitative phase explored, collected data and analysed the current state and challenges of security operations and analytics in various organisations, as well as the needs and expectations of security experts for automation

and continuous detection and response. Qualitative methods revealed the human aspects of security operations and analytics that quantitative data could not. This helped identify the framework's strengths and weaknesses, potential improvements, and the context of its use. By capturing human factors such as usability, workflow impact, and security analysts' decision-making processes, qualitative insights contributed to optimising the framework for better automation, continuous detection, and response, ultimately improving cybersecurity posture.

3.2.2 Sampling

The sampling technique used in this phase is purposive sampling, a non-probability sampling technique. It entails choosing people with relevant knowledge and experience in security operations and analytics (Campbell *et al.*, 2020). The criteria for selecting participants included: (a) security experts who work in different roles, like security analysts, security engineers, security managers, and security consultants. (b) security experts who have worked in other organisations, such as public, private, or non-profit sectors, and various industries, such as finance, healthcare, utilities, and education. (c) security experts with at least three years of experience in security operations and analytics. (d) security experts who were willing and able to participate in the study and provide informed consent.

The research subjects were selected based on their expertise, experience level, and extent of involvement with the platform. The interview questions, shown in Table 11, were designed to explore various aspects of the platform.

Table 11: Interview Questions Topics and Details

Interview Question Topic	**Interview Question Details**
Usage patterns	How do they use the platform in their day-to-day operations?
Perceived strengths and weaknesses	What are the key benefits and limitations of the platform?
Challenges faced	What difficulties do they encounter while using the platform?
Automation and response capabilities	How effectively does the platform aid in automating processes and responding to incidents?

Integration and workflow	How does the platform integrate with other security tools, and how does it affect their workflow?

The target sample size for this phase was fifteen participants, which was considered sufficient to achieve data saturation and thematic richness (LaDonna, Artino Jr and Balmer, 2021).

During a semi-structured interview, the respondents were free to express themselves on their terms while all the necessary points were addressed. Every interview was recorded and transcribed to guarantee precision in the data analysis phase.

Data saturation was determined through an iterative coding process, where interview transcripts were analysed continuously, and no new themes or significant variations emerged after the last few interviews. Thematic analysis was conducted following (Braun and Clarke, 2006) six-step framework: (a) Familiarisation with data, (b) Generating initial codes, (c) Searching for themes, (d) Reviewing themes, (e) Defining and naming themes, and (f) Producing the report.

Open coding was applied to identify key patterns, followed by axial coding to establish relationships among themes. The coding process was facilitated using QDA Miner Lite qualitative data analysis software, which enabled systematic data organisation, query analysis, and visualisation of thematic connections. The final themes were validated through intercoder reliability checks to ensure consistency and rigour in the analysis.

3.2.3 Data Collection through Qualitative Interviews

This study collected data through qualitative interviews with security operations practitioners with hands-on experience with security operations and analytics tools. In this phase, the primary tool utilised for gathering data was semi-structured interviews, which consisted of asking open-ended questions to obtain detailed and nuanced participant responses (Striepe, 2021). Open-ended questions enabled a flexible and interactive discussion, capturing in-depth information about experiences, opinions, and challenges. Qualitative interviews were chosen as they offer a flexible and interactive approach to gather in-depth information about participants' experiences, opinions, and practices.

The purpose of the interview was to cover specific topics, and the questions were designed accordingly: (a) the current practices, processes, tools, and technologies used for security operations and analytics in the participants' organisations. (b) the primary challenges and difficulties faced by the participants in performing security operations and analytics tasks. (c) the perceived benefits and drawbacks of automation and continuous detection and response capabilities for security operations and analytics. (d) the desired features and requirements for a security operations and analytics framework that can enable automation and continuous detection and response capabilities.

Table 12: Interview Topics

Interview Topic	**Details**
Usage patterns	How do participants use the platform in their daily security operations?
Strengths & Weaknesses	What are the perceived benefits and limitations of the platform?
Challenges	What difficulties do participants face when using the platform?
Automation & Response	How effective is the platform in automating processes and incident response?
Integration & Workflow	How does the platform integrate with other security tools, and how does it impact workflow?

Furthermore, the interviews were conducted to gain insights into the following research questions: (a) How does the SOAF improve the enterprise's security posture? (b) How does the SOAF enhance the workflow and performance of the security analysts? (c) What are the advantages and disadvantages of adopting the SOAF regarding usability, functionality, scalability, reliability, and interoperability? (d) How does the SOAF compare with other security solutions regarding features, capabilities, and costs? The research questions were the basis for developing the interview protocol (Braaten *et al.*, 2020; Turner III and Hagstrom-Schmidt, 2022). The protocol consisted of three main sections:

Table 13: Interview Protocol

Protocol	Description
Introduction	This section introduced the study's purpose and scope, explained the informed consent process, assured confidentiality and anonymity, and obtained demographic information from the participants.
Main questions	This section asked open-ended questions related to the research questions. The questions were designed to obtain the participants' rich and in-depth responses about their experiences, opinions, perceptions, feelings, and challenges regarding using the SOAF. The participants' answers were followed by probing questions to clarify or expand on them.
Conclusion	This research section outlined the next procedures, thanked participants for their time and cooperation, and asked for any thoughts, questions, or comments.

The interviews were face-to-face and lasted approximately thirty minutes each, which was deemed sufficient for obtaining in-depth insights while maintaining participant engagement. The structured nature of the interview protocol ensured that key topics were covered efficiently, reducing redundancy while capturing meaningful responses. Moreover, participants were cybersecurity professionals with time constraints, making a concise yet focused interview format more practical. Follow-up interviews or clarification via email were conducted when necessary to elaborate on critical points or refine interpretations. This approach ensured data completeness while respecting participants' availability. They were transcribed live using the Windows 11 voice typing feature with the participants' permission. The transcripts and notes were compared, and any

discrepancies were addressed. The transcripts were then anonymised by replacing the names of the participants and their organisations with pseudonyms where present.

3.2.4 Qualitative Data Analysis through Thematic Analysis

The data analysis approach used in this phase was thematic analysis, which entails the identification, investigation, and reporting of the patterns or themes that arise from the data (Byrne, 2022). Furthermore, thematic analysis was also used to code and interpret the qualitative data from the interviews, a method used by (Kiger and Varpio, 2020).

The thematic analysis followed a six-step process proposed by (Braun and Clarke, 2006), made up of (a) Repeated reading of the transcripts to become acquainted with the data. (b) Creating preliminary codes by assigning appropriate labels to data segments. (c) Conducting a search for themes by categorising relevant codes into more general categories. (d) Evaluating themes by assessing their validity and consistency with the data. (e) Identifying and labelling topics by articulating their fundamental nature and extent. (f) Documenting the analysis by presenting the conclusions and backing them with direct excerpts from the data. QDA Miner Lite qualitative data analysis software was used for the thematic analysis.

Both deductive and inductive approaches were used in the study (Robinson, 2022). The deductive approach involved using a predefined framework or theory to guide the analysis of codes and themes. On the other hand, the inductive approach involved generating codes and themes from the data without any prior assumptions (Kiger and Varpio, 2020). The deductive-inductive approach combined both methods for a comprehensive and flexible analysis that accounted for both existing and emerging concepts (Proudfoot, 2023). The research questions and the existing literature were the basis for the deductive analysis.

The research questions provided the main categories of the analysis: the effectiveness and efficiency of the SOAF, workflow and performance of the security analysts, benefits and challenges of using the SOAF and comparison with other security solutions. The literature review provided the subcategories of the analysis derived from the relevant concepts, models, frameworks, and criteria discussed in the literature review. For example, some of the subcategories for effectiveness and efficiency were security monitoring, threat detection, investigation, incident response and threat intelligence. The inductive part of the analysis was based on the data itself. The data was examined for new or unexpected codes or themes that did not fit into the deductive framework. These codes or themes

were added to the analysis to capture the richness and diversity of the participants' experiences and perspectives.

The coding process involved initial, focused, and axial coding. Initial coding was done by reading each transcript and assigning descriptive labels or codes to each meaningful data segment. Microsoft Word was used to write down the codes in the margins of the transcripts. Focused coding was done by reviewing and refining the initial codes and grouping them into broader themes. The themes were written in a separate document using Microsoft Excel. Axial coding was done by relating and connecting the themes to each other and to the research questions, as shown in the table below.

Table 14: Summary of main themes and subthemes from Thematic Analysis

Research Question	**Main Theme**	**Subthemes**
What are the current practices, challenges, and needs of security operations in organisations?	Security Operations Landscape	Current Practices: Monitoring, detection, response, intelligence, compliance. Challenges: Alert fatigue, tool complexity, data overload, evolving threats. Needs & Requirements: AI-driven detection, automation, better correlation.
How does the SOAF improve the security posture of the enterprise?	Security Effectiveness	Threat Detection: Identifying security threats. Investigation & Response: Incident handling. Threat Intelligence: Using intelligence for proactive defence.

		Compliance: Ensuring regulatory adherence.
How does the SOAF enhance the workflow and performance of the security analysts?	Operational Efficiency	Data Integration & Visualisation: Aggregating and presenting security data. Analysis & Correlation: Improving detection accuracy. Automation & Orchestration: Reducing manual workload.
What are the benefits and challenges of using the SOAF in terms of usability, functionality, scalability, reliability, and interoperability?	System Capabilities & Limitations	Usability: Ease of use, learning curve, user experience. Functionality: Core features, automation, adaptability. Scalability: Handling high data volume, velocity. Reliability: Performance, stability, security.

		Interoperability: Compatibility with other tools.
How does the SOAF compare with other existing security solutions in terms of features, capabilities, and costs?	SOAF Benchmarking	Strengths & Weaknesses: Unique features and gaps. Cost-Benefit Analysis: Economic efficiency of SOAF. Market Positioning: Comparison with industry standards.

The themes were identified using an iterative thematic analysis process. Themes were chosen based on the research focus and emerging qualitative data. Thematic overlaps were minimised by grouping related areas under broader categories. Each theme has a unique perspective: security impact, operational efficiency, system capabilities, and competitive positioning. The thematic framework was validated through intercoder reliability checks and expert reviews to ensure consistency, clarity, and minimal redundancy.

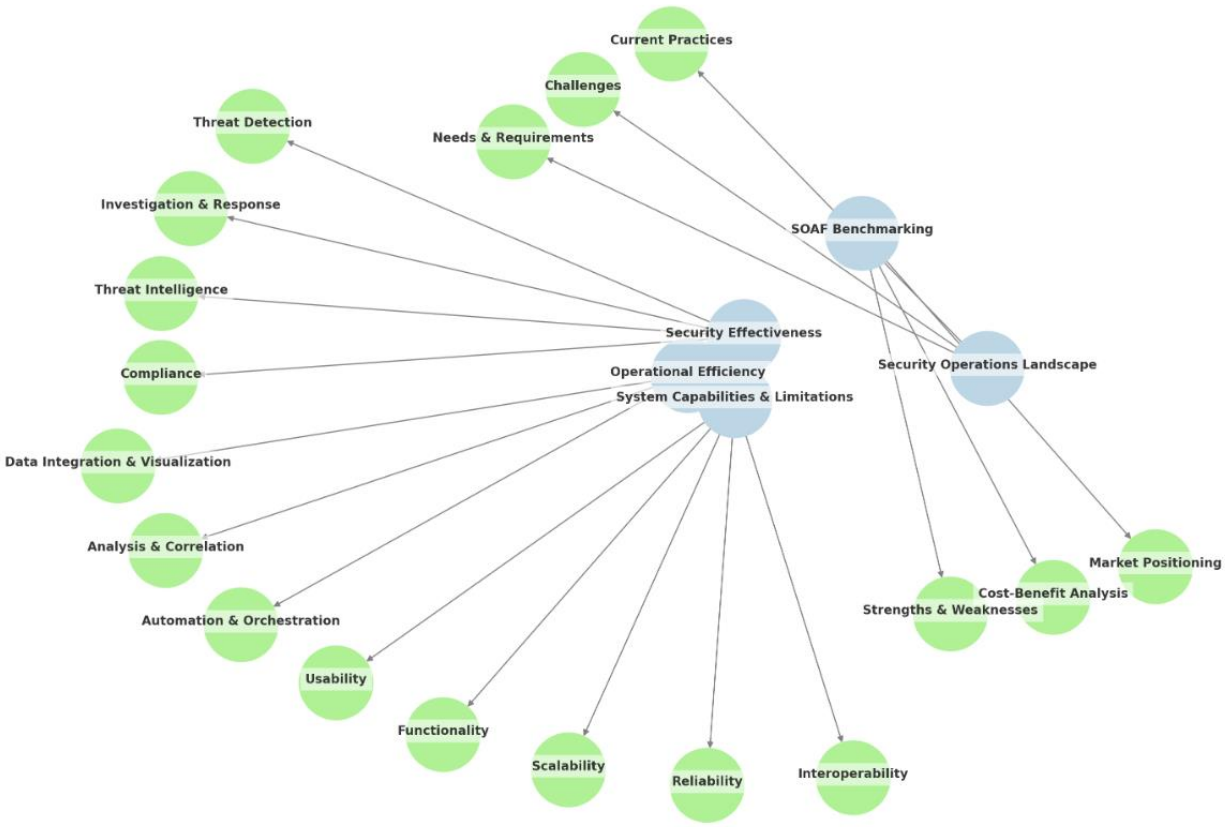

Figure 5: Thematic Structure Of SOAF Study

The figure above shows the thematic map visualising the relationship between the main themes and subthemes in your SOAF study. The main themes (blue nodes) represent high-level categories aligned with research questions. The subthemes (grey nodes) are the detailed aspects contributing to each theme. The edges (connections) indicate how subthemes belong to their respective main themes.

Several steps are involved in the process of coding qualitative data, which a single researcher can implement to maintain the integrity of the coding process and the resulting themes. Although the absence of a second researcher alters the dynamics of the process, robust practices were implemented in this study to maintain the integrity of the coding process and the resulting themes. The following processes in the table below were implemented for a rigorous coding process to ensure reliability and validity.

Table 15: Processes implemented for a rigorous coding process

Process	**Description**
Initial Coding	The qualitative data was initially coded independently. Transcripts were read and

	then assigned codes to identify overarching themes. This step reduced the volume of data, making it easier to examine.
Comparing and Categorizing Codes	Subsequently, the coded data was reviewed, and once the first coding was completed, the codes were organised into overarching themes. The goal was to find commonalities and trends among the codes, even with a single researcher.
Review and Reflection	After classifying the data, the categorised codes and themes were reviewed for recurring patterns and trends. This process involved reflecting on the initial coding and categorisation, ensuring that the themes accurately capture the essence of the data. This self-review helped in identifying any potential biases or misinterpretations.
Refinement and Iteration	The codes and themes were refined in this step, and the categories were adjusted where required. The definitions of themes were also refined to ensure their coherence and comprehensiveness.
External Validation (Simulation of Peer Review)	The coded data and themes were temporarily set aside to simulate external validation since a second researcher was unavailable. Then, the data was revisited with a fresh perspective that mimicked the effect of peer review. This allowed for the critical evaluation of the consistency and accuracy of the coding and categorisation.
Discussion with a Colleague	The findings were discussed with a colleague to mimic the consensus-building

	process. This discussion served as a way to identify potential blind spots and receive constructive feedback on the data interpretation.
Finalisation	The set of codes and themes were finalised based on the reflections, refinement, and external input. This finalisation was intended to reflect a comprehensive and accurate representation of the underlying concepts and patterns in the data.
Documentation	Detailed notes were maintained throughout the process, documenting the coding decisions, the thought process behind theme development, and any changes made along the way. This documentation ensured transparency and traceability in the research process.
Transparency and Methodological Rigor	A detailed explanation of the coding process was provided in the report, including the steps taken to ensure reliability and validity despite working alone. This demonstrated methodological rigour and enhanced the transparency of the research. Although the absence of a second researcher altered the dynamics of the process, robust practices were still implemented by a single researcher to maintain the integrity of the coding process and the resulting themes.

3.2.5 Validity and Reliability of Qualitative Findings

Subsequent steps were taken to guarantee that the qualitative results were valid and reliable. These steps were aligned with established qualitative research practices and were designed to provide robust insights into the effectiveness and potential improvements for

the SOAF. First, triangulation was used to validate the findings (Daniel, 2019). This involved comparing the interview data with user behaviour analytics and system logs from other sources. Findings were validated by cross-referencing interview responses with user behaviour analytics metrics and system log data. This included analysing alert correlation rates, false positive reduction trends, and mean time to detect security threats, ensuring alignment between participant perceptions and system performance data.

Secondly, to enhance reliability, the interview process and thematic analysis were conducted in a systematic and transparent manner (Daniel, 2019). The interview guide was pre-tested and refined, ensuring that key security operations aspects were covered. Thematic analysis was conducted using intercoder reliability checks to ensure consistent coding across researchers. The coding process was documented, version-controlled, and iteratively reviewed to maintain analytical rigour.

Lastly, to enhance credibility, the use of member checking, where findings were presented back to the participants for confirmation, helped ensure that the derived themes and subthemes accurately captured their experiences and perspectives (Daniel, 2019). Overall, these measures played a crucial role in ensuring the validity and reliability of the qualitative findings, thereby strengthening the credibility of the study. By implementing triangulation, systematic data analysis, and member checking, the research was able to provide well-substantiated insights into the effectiveness of the SOAF and identify areas for potential improvement. Moreover, presenting the findings back to participants allowed for verification of whether the extracted insights, such as incident response efficiency, security monitoring effectiveness, and integration challenges, accurately reflected real-world experiences. This iterative validation process not only enhanced the robustness of the study but also ensured that the conclusions drawn were both meaningful and actionable for improving SOAF's overall performance.

3.3 Design Science Research Process

The DSR process is a framework for developing and evaluating innovative solutions to complex problems (vom Brocke, Hevner and Maedche, 2020). This section examines the application of the stages of the DSR process to the SOAF for automation and CDR. Problem identification and motivation, solution objectives, design and development, demonstration, evaluation, and communication comprise the phases (vom Brocke, Hevner and Maedche, 2020). One of the objectives of this research is to address the challenges faced in cybersecurity operations by enabling automation, continuous

detection, and response capabilities. The following section outlines the relevance of the problem domain, the contributions of the proposed framework to practice and knowledge, the rigour of the DSR process, and the Design Science Research Cycle followed during the development of the Security Operations and Analytics Framework.

3.3.1 Relevance to the Problem Domain

The problem domain concerns the need for an effective and efficient SOAF (M Vielberth *et al.*, 2020). The current landscape of cybersecurity threats demands robust, scalable, and reliable systems capable of not just detecting but also responding to security incidents proactively and reactively (Sarker, 2023). The proposed SOAF, using a security operations and analytics platform comprising Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, seeks to address this problem by integrating various components for continuous detection and response. Wazuh is an open-source security detection, visibility and compliance platform that manages host-based security information (Stanković, Gajin and Petrović, 2022). Elasticsearch offers a scalable search, scalable data storage and analytics engine (Kathare, Reddy and Prabhu, 2020). Kibana visualises Elasticsearch data. At the same time, TheHive and Cortex are designed for threat intelligence and response to complement the system by providing incident response and automation capabilities (Preuveneers and Joosen, 2021).

3.3.2 The rigour of the Design Science Research Process

The DSR process used in this study adhered to rigorous principles to ensure the validity, practical relevance and reliability of the proposed SOAF (Johannesson and Perjons, 2021). DSR is widely used in cybersecurity research and technology development because it provides a structured approach to creating and evaluating innovative solutions (Wermke *et al.*, 2022). Rigour was achieved through a well-defined six-phase DSR process: problem explication, solution objectives, design and development, demonstration, and evaluation activities.

The study commenced by clearly defining the research problem based on observed challenges and gaps in cybersecurity operations. This was achieved through an extensive review of existing literature and insights from practitioners, ensuring that the framework addressed a practically relevant and practical issue within the cybersecurity domain (Cremer, Sheehan, Fortmann, Arash N Kia, *et al.*, 2022). The research was also related to an existing knowledge base, which provided the theoretical foundations, design guidelines, and evaluation criteria (vom Brocke, Hevner and Maedche, 2020). The

solution objectives were then defined to align with the identified gaps, ensuring that the framework was designed to meet real-world security needs.

The framework was developed based on cybersecurity principles, focusing on security monitoring, incident response, threat intelligence, and compliance. During the demonstration phase, expert feedback and discussions with cybersecurity professionals validated its alignment with operational security workflows (Peffers et al., 2020).

A rigorous evaluation process used qualitative methods such as semi-structured interviews, thematic analysis, and member checking to assess the framework's effectiveness and usability. Thematic analysis followed (Braun and Clarke, 2006)six-phase approach for systematic theme identification, while member-checking validated findings by allowing participants to confirm the accuracy of the themes (Yadav, 2022).

The research grounded itself in established design science and cybersecurity literature to guide the framework's development and evaluation. By applying the DSR methodology in a qualitative context, the study ensured the framework was conceptually sound and practically relevant. This rigorous approach enhances the credibility of the findings and offers valuable insights for improving security operations through a practitioner-informed framework (Cremer, Sheehan, Fortmann, Arash N Kia, *et al.*, 2022).

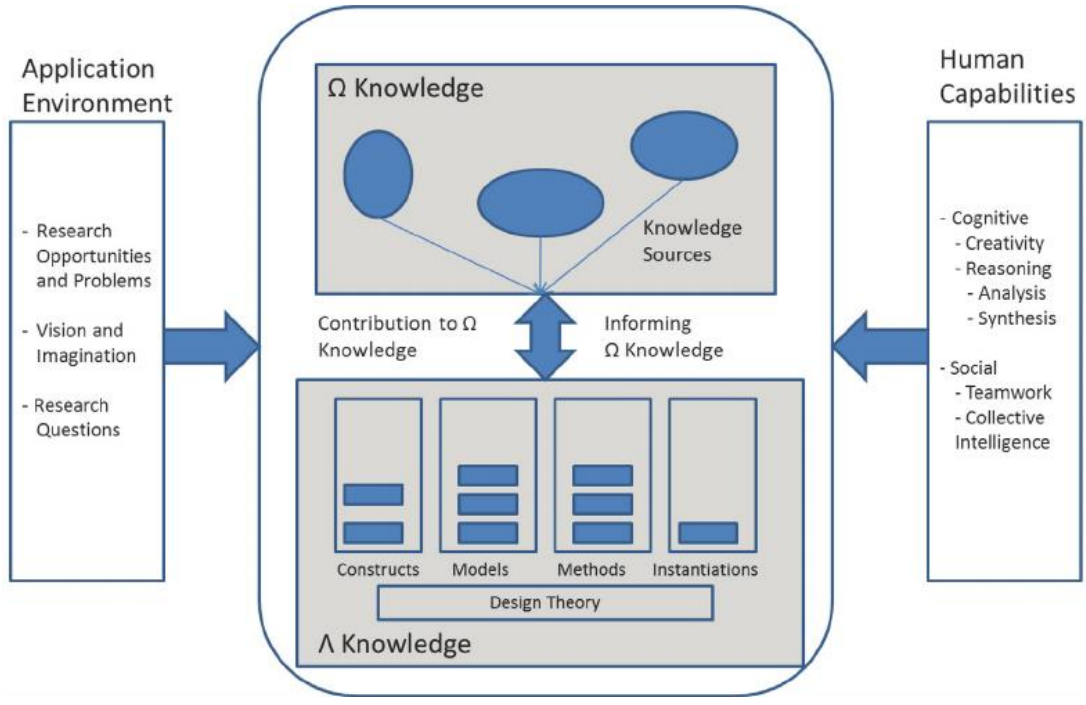

Figure 6: Overview of the DSR process and its relation to the knowledge base (Gregor and Hevner, 2013)**.**

3.3.2.1 Problem Explication

The first stage of the DSR process was to clarify the problem that motivated this research. Literature research was undertaken to ascertain the present condition of security operations and the difficulties encountered by security teams in identifying and addressing cyber threats. Additionally, security experts from different organisations were interviewed to gain insights into their practices, needs, and expectations.

From the data collected, qualitative data analysis methods were used, including coding, categorising, and memoing to examine the information gathered from the literature review and the interviews. Moreover, the principles of trustworthiness, such as credibility, transferability, dependability, and confirmability, were followed to ensure the rigour of the qualitative research (Nyirenda *et al.*, 2020; Stedmon and Paul, 2021). Based on the problem explication, the research problem, question, and objectives for the project were defined.

3.3.2.2 Solution Objectives

After explicating the problem, the second activity of the DSR process was to define the objectives of the solution (Alan R. Hevner *et al.*, 2004). For this activity, the results of the problem explication were used as input. Furthermore, the existing knowledge base was also consulted to find relevant theories, models, frameworks, and best practices that could provide guidance in defining the solution objectives (Gregor and Hevner, 2013). Using this information, deductive reasoning was used to derive specific design goals and criteria from the general problem statement and objectives. Additionally, a research hypothesis was also formulated that expressed the expectations about the outcomes and impacts of the solution (Hevner and Gregor, 2022).

3.3.2.3 Design and Development

Once the solution goals were established, the next phase in the DSR process included designing and developing the solution using a methodical and progressive strategy. The process used a methodical and progressive strategy that included conceptual modelling, prototyping, testing, and refining consistent with (Peffers *et al.*, 2007). In order to depict distinct parts of the solution, various design methodologies and techniques, such as Unified Modelling Language (UML) diagrams, use cases, user stories, and mock-ups, were adopted. These tools, as noted by (Hevner and Chatterjee, 2010), to enhance the clarity and functionality of design artefacts.

Preexisting technologies, tools, data sources, algorithms, and parameters were used to execute the solution. Design concepts and patterns from the knowledge base were implemented to guarantee an accurate design and development process. Moreover, design decisions and rationales using a design science research canvas were documented (Johannesson and Perjons, 2021).

3.3.2.4 Demonstration

After designing and developing the solution, the fourth activity of the DSR process was to demonstrate the solution in a simulated environment. For this activity, a case study with a real-world organisation that agreed to use the solution for their test security operations was conducted. Data from several sources, including logs, metrics, surveys, interviews, and observations, were gathered to assess the effectiveness and results of the solution. The use of qualitative methods, including interviews and thematic analysis, helped gather in-depth insights into the performance and usability of the SOAF (Tomaszewski, Zarestky and Gonzalez, 2020; vom Brocke, Hevner and Maedche, 2020). Data from the interviews was coded and interpreted using thematic analysis, which followed a deductive-inductive method. In order to guarantee the rigour and robustness of the research process, this technique enabled the discovery, analysis, and reporting of patterns or themes within the data (Nguyen *et al.*, 2021).

3.3.2.5 Evaluation

Building on the demonstration of the solution, the fifth activity of the DSR process was to evaluate the solution against the design goals and criteria defined in the second activity. For this activity, qualitative methods were used to assess the effectiveness, efficiency, usability, satisfaction, and impact of the solution (Tomaszewski, Zarestky and Gonzalez, 2020)Relevant literature and empirical data were used to compare the solution with existing solutions and approaches. The limitations, assumptions, threats, and biases involved in the evaluation process were also discussed to guarantee the accuracy and dependability of the data and conclusions.

3.3.2.6 Communication

After evaluating the solution, the final activity of the DSR process was to communicate the research to different audiences, such as academic peers, practitioners, managers, or stakeholders. For this activity, the main contributions and implications of the study were summarised, emphasising how the solution addressed the research problem and question and how it advanced the knowledge effectively in security operations and analytics,

theoretically and in practice (Vom Brocke *et al.*, 2020). Additionally, the practical applications and benefits of the solution for security operations were discussed, ensuring that the relevance of the research is clear to practitioners and industry stakeholders (Winter and vom Brocke, 2021). Furthermore, recommendations for future research directions or improvements for the solution were provided (Hevner and Storey, 2021). To ensure the rigour of the communication, the principles of clarity, coherence, completeness, and correctness were followed (Thuan *et al.*, 2023).

The DSR methodology ensured the research was systematic, reliable, and relevant. Each phase (Problem Explication, Solution Objectives, Design & Development, Demonstration, Evaluation, and Communication) was grounded in theory and analytically validated, making the SOAF framework scientifically sound and operationally effective. This research connects cybersecurity theory with practice by integrating qualitative analysis, technical implementation, and real-world validation, offering a scalable, automated solution for modern SOCs.

3.4 Integration of Design Science Research and Qualitative Methods

This study adopted an exploratory method approach involving elements of both qualitative research and DSR methodologies to benefit from the strengths of each and offset their weaknesses (Casula, Rangarajan and Shields, 2021; Dimov, Maula and Romme, 2023). The qualitative phase involved conducting semi-structured interviews with fifteen security experts from different organisations to gain insights into their practices, needs, expectations, and challenges regarding security operations and analytics. The qualitative data collected from the interviews were examined using thematic analysis to identify the key themes and qualitative patterns that emerged from the participant's responses. The findings informed the DSR phase, which involved designing, developing, demonstrating, and evaluating the SOAF as a solution to the research problem.

The DSR phase followed a method framework proposed by (Johannesson and Perjons, 2021), which consists of five main activities: problem explication, solution objectives, design and development, demonstration, and evaluation. The DSR solution produced in this phase included a conceptual model, a prototype, a case study, and an evaluation report. The DSR findings were then integrated with the qualitative findings to answer the research question and draw conclusions.

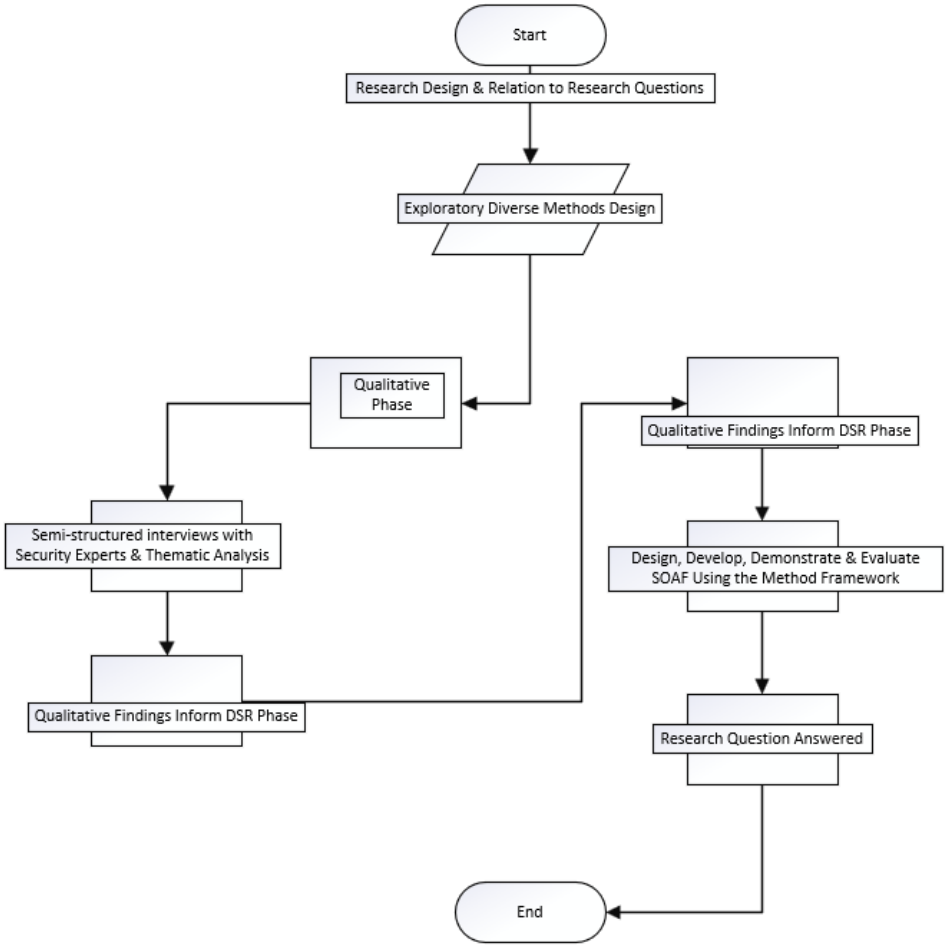

Figure 7: Overview of the research design and its relation to the research question

The research design diagram provides an overview of a mixed methods design with two phases: the qualitative phase and the DSR phase. In the qualitative phase, semi-structured interviews are conducted with security experts, and the data is analysed using thematic analysis. The DSR phase involves designing, developing, demonstrating, and evaluating the SOAF using a method framework. The diagram also shows how the qualitative findings inform the DSR phase and how the DSR findings are integrated with the qualitative findings to answer the research question. This approach allowed for a more comprehensive understanding of the SOAF. Furthermore, using the DSR and qualitative methods design allows method flexibility (Holtkamp, Soliman and Siponen, 2019), and differing and conflicting results enrich the understanding of the research problem (Shania, Handayani and Asih, 2023). Moreover, the DSR and qualitative methods design integrated the benefits of both DSR and qualitative research, such as innovation, rigour, relevance, contextualisation, and credibility (Dawadi, Shrestha and Giri, 2021). The research design consisted of the following components.

3.4.1 Design Science Research Phase

This section presents the DSR phase within the research design to develop the SOAF by leveraging the SOAP for automation and CDR. The DSR framework proposed by (Johannesson and Perjons, 2021) was used as a guide for the design and development of the framework. It consists of five main activities: problem explication, solution objectives, design and development, demonstration, and evaluation. This phase's DSR solutions include a conceptual model, a prototype, a case study, and an evaluation report. The DSR findings were then integrated with the qualitative findings from the previous phase to answer the research question and draw conclusions.

3.4.1.1 Problem Explication

The first activity of the DSR phase involved investigating the problem that motivates the need for a new or improved solution and identifying the relevant stakeholders, their goals and their problems. The outcome of this phase is a problem statement that defines the scope and boundaries of the research problem (Johannesson and Perjons, 2021). The problem explication was based on the previous phase's qualitative findings and existing security operations and analytics literature. It consists of three steps: problem identification, problem analysis, and problem definition.

3.4.1.1.1 Problem Identification

The problem identification step involved identifying the central problem that the SOAF intended to address. Based on the qualitative findings from the semi-structured interviews with security experts, as well as on the literature review on security operations and analytics, the main problems identified were: (a) The current security operations and analytics practices are insufficient to cope with the increasing volume, velocity, variety, and complexity of cyber threats and incidents. (b) The current security operations and analytics tools and technologies are fragmented, siloed, inefficient, and ineffective in providing automation and CDR capabilities. (c) The current security operations and analytics teams and staff are overwhelmed, understaffed, undertrained, and under-resourced in performing their tasks.

3.4.1.1.2 Problem Analysis

The problem analysis step involved analysing the causes, effects, stakeholders and the problem context identified, as well as identifying the primary obstacles and opportunities for improvement. Based on the qualitative findings from the semi-structured interviews

with security experts and the literature review on security operations and analytics, the result of the problem analysis was summarised in the table below.

Table 16: Problem Analysis

Problem Analysis	**Details**
Causes	The causes of the problem include (a) The rapid evolution and sophistication of cyber threats and attack techniques. (b) The increasing digitalisation and complexity of organisational systems and assets. (c) The lack of standardisation and integration of security operations and analytics processes. (d) The lack of interoperability and scalability of security operations and analytics tools. (e) The lack of visibility and intelligence of security operations and analytics data.
Effects	The effects of the problem include (a) The increased risk and impact of cyber-attacks and incidents on organisational performance, reputation, and compliance. (b) The decreased efficiency and effectiveness of security operations and analytics activities outcomes. (c) The decreased satisfaction retention of security operations and analytics team staff.
Stakeholders	The stakeholders involved in or affected by the problem include (a) Security operations and analytics team staff such as security analysts, engineers, managers, and consultants. (b) Other organisational team staff include business units, IT units, senior management, board directors, customers, suppliers and regulators.

Context	The context of the problem includes (a) The organisational environment, such as size, nature, industry, culture, strategy, objectives and values. (b) The external environment includes market, competition, regulation and innovation.

The research problem statement, the research question, and the research sub-questions define the problem context. The main challenges and opportunities were derived from the literature review and the qualitative findings from the previous phase.

The research problem statement was:

How can organisations improve their security posture and resilience using a SOAF/SOAP for automation and CDR?

The research questions were:

RQ1: What are the current practices, challenges, and needs of security operations in organisations?

RQ2: How does the SOAF improve the security posture of the enterprise?

RQ3: How does the SOAF enhance the workflow and performance of the security analysts?

RQ4: Discuss the advantages and problems of adopting the SOAF regarding usability, functionality, scalability, reliability, and interoperability.

RQ5: How does the SOAF compare features, capabilities, and costs with other security solutions?

RQ6: What are the design principles and evaluation criteria for a SOAF that leverages a SOAP for automation and CDR?

The research sub-questions were:

RSQ1: What are the existing security operations and analytics solutions, frameworks, models, and standards?

RSQ2: How can a SOAP enable automation and CDR in security operations?

RSQ3: How can a SOAF be designed, implemented, and evaluated to address the research problem?

To address the challenges in cybersecurity, a combination of security operations and analytics, CDR, AI, and ML could be employed. These technological advancements provide robust solutions to enhance the effectiveness of security operations.

Cyber threats are becoming increasingly complicated as attackers use sophisticated strategies that constantly adapt. AI and ML may be used in cybersecurity technologies to comprehend and forecast emerging risks. Through the analysis of extensive data, these technologies have the capability to recognise trends and adjust to emerging dangers at a faster rate compared to conventional approaches. This improves the functionality of CDR systems in efficiently handling the number, speed, diversity, and intricacy of these threats (Das and Sandhane, 2021). One way to alleviate the burden on resources and enhance reaction times is by incorporating sophisticated AI algorithms into SOAFs. This feature will facilitate the automated identification and immediate reaction to novel and intricate dangers in real time.

The dispersion of data across many tools and platforms might pose difficulties in ensuring clear visibility and efficiently correlating data. In order to tackle this problem, one may implement a SIEM system that is augmented with AI functionalities. This system has the ability to effectively gather and examine data from many sources, offering a complete view and assisting in the connection of security data. This association is crucial for efficient analysis and prompt action (Islam, 2023; Joseph, 2023). Moreover, there exists a prospect of creating a consolidated framework that integrates Elasticsearch and other big data technologies for the purpose of effectively managing and analysing security data. Integrating AI may significantly improve the correlation and analytical capabilities of these technologies.

Skilled security analysts are in short supply, and the job is highly stressful, leading to high turnover rates. One potential solution is to use AI-driven tools to automate routine monitoring and response tasks, allowing analysts to concentrate on more strategic aspects of cybersecurity (Hassan and Ibrahim, 2023). This can alleviate their workload and reduce stress levels. An opportunity exists to invest in training programs that use AI simulations to rapidly upskill new analysts and continuously educate existing ones on the latest threats and mitigation strategies.

Manual security processes can be inefficient, error-prone, and inconsistent. However, the adoption of AI and ML technology can help automate repetitive tasks such as log analysis and alert triaging. This may result in fewer mistakes and enhanced operational efficiency (Kinyua and Awuah, 2021; Kaur, Gabrijelčič and Klobučar, 2023). By deploying intelligent automation solutions, organisations can ensure consistent and effective security practices that can adapt to changing threat landscapes and organisational needs.

Real-time detection is a major challenge when it comes to measuring and improving the performance and effectiveness of security operations. However, CDR systems integrated with real-time analytics and machine learning can provide ongoing assessment and adjustment of security measures. These systems can adapt to new data and conditions without any human intervention, offering continuous improvement in threat detection investigation and response (Reddy, 2021b; Labu and Ahammed, 2024). By enhancing CDR capabilities with real-time analytics engines, potential breaches can be predicted before they escalate, thereby optimising the performance and effectiveness of security operations. This can ensure consistent and effective security practices that is capable of adjusting to evolving threat environments and organisational needs.

The use of AI and ML in SOAFs and CDR systems offers a great opportunity to effectively address and mitigate the challenges outlined. By incorporating these advanced technologies, organisations can improve their cybersecurity, reduce human error, and effectively manage the increasing complexity of cyber threats.

3.4.1.1.3 Problem Definition

After identifying and analysing the issue, the following was the problem definition that was formulated:

> *How can the SOAF be designed and developed to enable automation and CDR capabilities for modern cybersecurity operations?*

3.4.1.2 Solution Requirements Definition

The next step in the DSR process was to specify the requirements for the proposed solution based on the problem explication. The requirements are the desired features, functions, qualities, and constraints of the proposed solution that address the problem context and the stakeholders' needs (Shankar *et al.*, 2020). Functional requirements and non-functional requirements are the two main categories into which the requirements fall.

Functional requirements refer to the capabilities and behaviours that the proposed solution should provide to solve the problem (Shankar *et al.*, 2020). They specify what the solution should do and how it should perform. Non-functional requirements are the characteristics and attributes the proposed solution should have to meet the quality standards and expectations of the stakeholders (Shankar *et al.*, 2020). They specify how well the solution should do what it does.

The solution requirements step involved identifying and specifying the functional and non-functional requirements of the SOAF to solve the problem. Based on the qualitative findings from the semi-structured interviews with security experts and the literature review on security operations and analytics, the solution requirements are summarised as follows.

3.4.1.2.1 Functional requirements

The functional requirements describe what the SOAF should do to enable automation and continuous detection and response capabilities for security operations and analytics. The MoSCoW method (AbdElazim, Moawad and Elfakharany, 2020; Bukhsh, Bukhsh and Daneva, 2020) was used to prioritise the requirements into four categories: "Must have", "Should have", "Could have", and "Will not have". This approach helped to prevent scope creep and ensured that the project stayed on track. The functional requirements included:

Table 17: MoSCoW method functional requirements

Proposed Solution	**Categories**			
	Must have	**Should have**	**Could have**	**Will not have**
	The proposed solution must provide a conceptual model of the SOAF that defines its scope, objectives, components, relationships, and principles.	The proposed solution should align the SOAF objectives with the business objectives and the stakeholder needs.	The proposed solution could integrate AI, ML, natural language processing (NLP), data mining (DM), blockchain (BC), big data analytics	The proposed solution will not provide a complete and comprehensive implementation of the SOAF, which covers all aspects of security

			(BDA), cloud computing (CC), and IoT to enhance the SOAF capabilities.	operations and analytics.
	The proposed solution must provide a prototype of the SOAF that implements its core functions and features using a security operations and analytics platform	The proposed solution should follow the design science research methodology and adhere to its guidelines and criteria.	The proposed solution could provide a user interface (UI) and a user experience (UX) design for the SOAF prototype.	The proposed solution will not provide a generalisable and universal framework for all contexts and scenarios.
	The proposed solution must provide a case study of the SOAF that demonstrates its application and benefits in a real-world scenario.	The proposed solution should leverage the existing solutions and best practices for security operations and analytics.	The proposed solution could provide a roadmap for future development and improvement of the SOAF.	The proposed solution will not provide a definitive and conclusive answer to the research question.
	The proposed solution must provide an evaluation report of the SOAF that assesses its effectiveness and	The proposed solution should support automation and CDR in security operations.		

	impact using appropriate methods and criteria.			

3.4.1.2.2 Non-functional requirements

The non-functional requirements describe how well the SOAF should perform to enable automation and continuous detection and response capabilities for security operations and analytics. The non-functional requirements include:

Table 18: MoSCoW method non-functional requirements

Proposed Solution	**Categories**			
	Must have	**Should have**	**Could have**	**Will not have**
	The proposed solution must be feasible, i.e., it must involve designing, implementing, and evaluating the SOAF using available resources, tools, and techniques.	The proposed solution should be usable, i.e., easy for the intended users to understand, learn, operate, and maintain.	The proposed solution could be scalable, i.e., handle increasing amounts and complexity of security data and processes.	The proposed solution will not be perfect; it will have limitations, assumptions, trade-offs, and risks that must be acknowledged and addressed.
	The proposed solution must be reliable, i.e., it must perform consistently and correctly under normal and abnormal conditions.	The proposed solution should be efficient, i.e., optimising the use of resources, time, and effort in security operations.	The proposed solution could be flexible, i.e., adapt to changing security operations requirements, contexts, and scenarios.	

	The proposed solution must be safe in the sense that it protects the confidentiality, integrity, and availability of all security-related information and operations.	The proposed solution should be practical, i.e., it should achieve the desired outcomes and benefits in security operations.	The proposed solution could be innovative, i.e., it could introduce new or improved features or functions in security operations.	

3.4.1.3 Design Specification

This section specifies the design of the proposed solution based on the requirements specification. The design specification defines the proposed solution's structure, behaviour, and appearance. It consists of four sub-steps: conceptual design, logical design and physical design.

3.4.1.3.1 Conceptual Design

The conceptual design defines the abstract and high-level view of the proposed solution. It consists of two main components: the conceptual model and the design principles. The SOAF is a new model integrating different cybersecurity tools into one unified software system, enabling organisations to monitor, detect, and respond to cyber threats (Osamah M M Al-Matari *et al.*, 2021).

The SOAF consists of the following components:

Logs, network traffic, and threat intelligence feeds are just a few of the many sources of security data that the SIEM application gathers, analyses, and correlates. The SIEM provides real-time visibility and alerts for security incidents and events (González-Granadillo, González-Zarzosa and Diaz, 2021). It is the primary source of input for the framework.

The SOAR tool automates and coordinates the actions and workflows for security operations and incident response. The SOAR enables faster and more consistent

responses to security incidents and events. It receives input from the SIEM and executes output to the security tools or systems (Kinyua and Awuah, 2021).

The Security Analytics tool applies advanced techniques, such as machine learning, artificial intelligence, or statistical analysis, to identify patterns, anomalies, or trends in security data (Nassar and Kamal, 2021). The security analytics tool enhances the detection and prevention of cyber threats and attacks (Ghillani, 2022). It receives input from the SIEM and outputs it to the SOAR or the Case Management.

The Case Management tool manages the lifecycle of security incidents and events, from creation to resolution. It facilitates collaboration, communication, and documentation among security analysts and stakeholders (Groenewegen and Janssen, 2021). It receives input from the SIEM or the Security Analytics and provides output to the SOAR or the Threat Intelligence.

The Threat Intelligence tool provides contextual information and insights about cyber threats and actors, such as their tactics, techniques, procedures, and indicators of compromise (Möller, 2023b). It helps security analysts understand the threat landscape and prioritise their actions. The tool receives input from external sources or services and provides output to the SIEM or the Case Management.

The SOAF's conceptual model is a visual depiction of its goals, components, connections, and guiding principles. It was developed to represent the key components and their relationships within our SOAF This model was a foundation for understanding the framework's architecture and data flow. It is based on the existing solutions and best practices for security operations and analytics, as well as the stakeholder requirements and expectations (Kinyua and Awuah, 2021). It provides a clear and consistent understanding of the SOAF among stakeholders.

Furthermore, the design principles are a set of guidelines and rules that guide the design decisions and actions for the SOAF. They are derived from the literature review, the qualitative findings, and the stakeholder feedback. They ensure that the SOAF meets the functional and non-functional requirements and aligns with the business objectives and the stakeholder needs (Hajny et al., 2021). The conceptual design describes the high-level structure and functionality of the proposed framework without going into the details of how it will be implemented. It consists of the following components:

The SOAP integrates various security tools and data sources to provide a unified view of the organisation's security posture and threat landscape (Mughal, 2022). The SOAP enables continuous monitoring, analysis, detection, and response to cyber threats, leveraging artificial intelligence, machine learning, and automation capabilities. The SOAP also provides a centralised dashboard and reporting system for security operations and management.

A set of security sensors that collect and send security data to the SOAP (Hwoij, Khamaiseh and Ababneh, 2021). These sensors include EDR agents, network traffic analysis (NTA) tools, vulnerability scanners, threat intelligence feeds, log collectors, and other security tools that generate relevant data for security operations and analytics.

A set of security actions executed by the SOAP or triggered by the security operators to mitigate or remediate detected threats. These actions include blocking malicious traffic, isolating compromised devices, quarantining suspicious files, notifying users or administrators, updating security policies or rules, and initiating incident response workflows (Kinyua and Awuah, 2021). A set of security operators that interact with the SOAP to perform security tasks such as configuring sensors and actions, reviewing alerts and incidents, investigating threats, conducting forensics, and reporting on security metrics and outcomes.

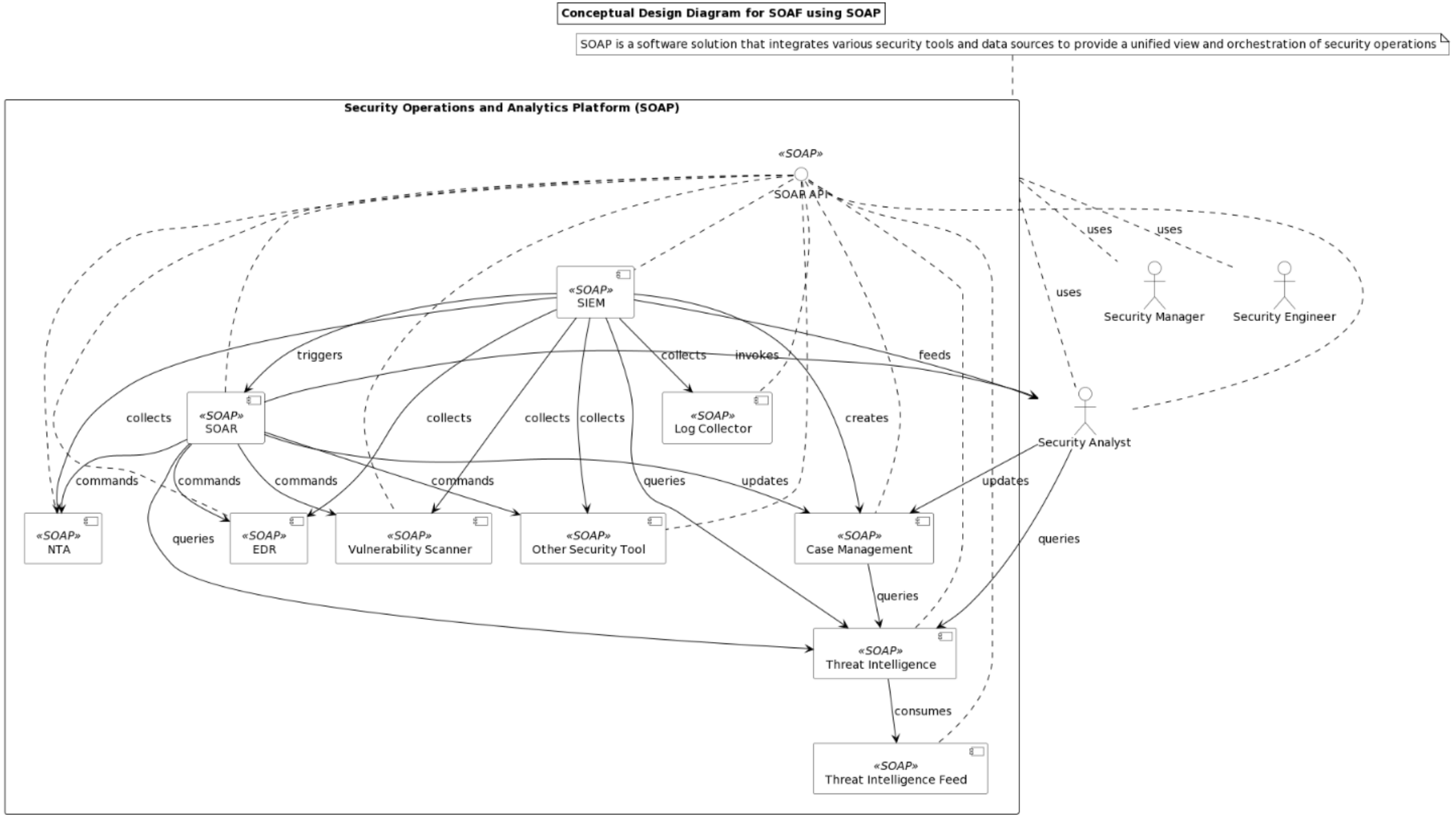

Figure 8: Conceptual model of the SOAF

The principles that guided the design of the SOAF were developed through a systematic approach that integrates insights from a thorough analysis of existing literature, results from qualitative studies, and extensive input from key stakeholders. They acted as fundamental guidelines and rules that inform design decisions and strategic actions within the process of developing the SOAF. A thorough comprehension of the present status of cybersecurity operations forms the basis for the design concepts, as reported in academic publications and grey literature. This review ensures that the principles are grounded in proven practices and emerging trends in cybersecurity (Rajamäki, Lahdenperä and Shalamanov, 2022). Moreover, focus groups and interviews with stakeholders are examples of qualitative research methods that provide contextual insights that enhance the relevance and applicability of the principles to specific organisational contexts (Myers, 2019). These principles guarantee that the SOAF satisfies both functional and non-functional criteria, is in line with business goals, and meets the demands of all stakeholders.

The design principles are presented in the table below.

Table 19: Design principles for the SOAF

Design Principle	**Description**
Alignment	The SOAF should align its objectives, processes, and outcomes with the business objectives and the stakeholder needs.
Integration	The SOAF should integrate security data, tools, processes, people, and intelligence across different sources and domains.
Automation	The SOAF should automate security tasks, workflows, decisions, and actions to improve efficiency, consistency, accuracy, and speed.
Orchestration	The SOAF should orchestrate security tools, processes, people, and intelligence to coordinate and optimise security operations.
Response	The SOAF should respond to security incidents promptly, effectively, and appropriately to mitigate risks and impacts.

Learning	The SOAF should learn from security data, incidents, feedback, and best practices to improve security knowledge, skills, capabilities, and performance.
Improvement	The SOAF should monitor, measure, evaluate, and report its effectiveness and impact to identify gaps, limitations, opportunities, and actions for improvement.

3.4.1.3.2 Logical Design

The logical design defines the detailed and structured view of the proposed SOAF, which includes the architecture diagram, process model, data model, functional model, and interface model. These parts work together to form the framework and are essential to its operation. The architecture diagram is a visual representation that elaborates on the SOAF's components, subcomponents, interfaces, interactions, dependencies, and flows, enhancing the conceptual model with greater detail. It illustrates how each component operates and the communication pathways between them (Awaysheh *et al.*, 2021). Moreover, this diagram shows the interaction between external entities, such as users, and the framework, thereby providing a comprehensive view of the system architecture (Tekinerdogan and Verdouw, 2020). The process model graphically depicts the SOAF's operations, showcasing its processes along with associated inputs, outputs, parameters, variables, triggers, events, conditions, rules, decisions, actions, loops, iterations, sequences, and parallelisms. Rooted in the functional requirements, this model further elaborates on how each function is executed and the expected outcomes, illustrating the coordination and orchestration of different functions within and across the framework's components (Weilkiens *et al.*, 2022).

The data model specifies the types, formats, sources, destinations, and relationships of data utilised or generated by the framework. It categorises data into structured types—such as events, alerts, incidents, and indicators of compromise—and unstructured types—such as logs, packets, and files. Furthermore, this model outlines critical data management criteria, including quality, integrity, availability, confidentiality, and retention requirements for each type of data (Dang *et al.*, 2021).

The functional model details the various processes carried out by the framework to meet its objectives. It encompasses both automated functions, including data ingestion, normalisation, correlation, analysis, detection, and response, and manual functions,

including configuration, investigation, and remediation. It defines each function's inputs, outputs, parameters, dependencies, triggers, and performance criteria, ensuring a thorough understanding of the framework's operations (Gómez *et al.*, 2021).

Lastly, the interface model outlines the interactions between the framework's components and external entities. It includes technical interfaces, such as APIs, protocols, and standards, as well as user interfaces, like dashboards, reports, and notifications. This model also addresses critical interface requirements concerning usability, accessibility, security, and reliability, ensuring that all system interactions meet high standards of efficiency and safety (Akinsola *et al.*, 2021).

The logical design of the SOAF is integral in transforming theoretical concepts into a fully functional security framework. By detailing the architecture, processes, data handling, functionality, and interfaces, the design helps to bridge the gap between conceptual planning and operational implementation, paving the way for an effective deployment of the SOAF.

3.4.1.3.3 Physical Design

The proposed SOAF's physical architecture provides a detailed plan for implementing the necessary hardware, software, network, and storage components required to support and host the framework. This design guarantees that every component fulfils the operational requirements and security criteria essential for efficient deployment. The hardware setup encompasses a range of physical devices that perform essential functions in the implementation and functioning of the framework. The equipment included in this category are servers, workstations, laptops, network devices, and sensors. To guarantee dependability and uninterrupted operation, every hardware component is chosen according to particular criteria, including capacity, scalability, availability, and redundancy. Evaluating these characteristics ensures that the hardware infrastructure is capable of supporting the framework under various workloads and situations. Software components are integral to the framework, encompassing operating systems, databases, middleware, and various security tools and SOAP solutions. These components are crucial for the seamless integration and functionality of the framework. Specifications for each software element include compatibility with other system components, interoperability across different platforms, maintainability for ease of management, and the update ability to ensure security and efficiency in response to evolving threats (Hatzivasilis *et al.*, 2020).

The network architecture is designed to facilitate robust and secure communications between the various components of the framework. This infrastructure includes network segments, subnets, gateways, routers, switches, firewalls, proxies, and VPNs. Each network element is carefully configured to meet specific requirements such as bandwidth capacity, latency minimisation, enhanced security, and resilience to ensure reliable connectivity and protection against network-based threats (Zhou et al., 2020).

Storage systems within the framework are critical for managing the data generated, processed, and stored by the security operations. These systems range from physical discs and arrays to cloud services and tape drives. The storage strategy is formulated to address requirements such as data capacity, performance metrics, data security, and backup capabilities. Ensuring these parameters help maintain data integrity and availability, which are crucial for effective security analytics and incident response (Chandramouli, Pinhas and others, 2020).

The detailed physical design of the SOAF is crucial for ensuring that all technical requirements are met to support sophisticated security operations. The framework manages the complexity of current cybersecurity settings by thoroughly describing and combining the properties of each component. This provides a strong basis for efficiently protecting against and reacting to cyber-attacks.

3.4.1.4 Solution Design and Development

The design and development phase was pivotal in constructing a robust SOAF, as it aimed to produce a DSR solution to address the research problem and meet the research objectives. This section outlines the key steps and solutions generated in this phase, aligning with the principles (Johannesson and Perjons, 2021) and emphasising a structured process for creating innovative solutions. The DSR solution consists of four components: a conceptual model, a prototype, a case study, and an evaluation report.

The first step was formulating a framework design based on the defined objectives. This involved selecting and integrating the security tools, configuring their interactions, and specifying the logic for automated responses. The completeness, compatibility, and modularity design criteria were followed to select and integrate the security tools. Completeness means the framework should cover all security operations and analytics phases, from data collection to incident response (Alan R Hevner *et al.*, 2004). The SOAF architecture is designed to facilitate comprehensive security monitoring, continuous threat detection, analysis, and response. Compatibility means the framework should use

tools that can interoperate with each other and existing systems. Modularity refers to the characteristic of a framework that allows for the seamless substitution or modification of tools without causing any disruption to the whole framework. Based on these criteria, Wazuh, Elasticsearch, Kibana, TheHive, and Cortex were chosen as the main components of the framework. Furthermore, a combined solution using Wazuh, Elasticsearch, Kibana, TheHive, and Cortex is necessary to achieve a comprehensive and effective security operations and analytics framework. These technologies work together to strengthen the system's defences because of the unique features they each provide. Therefore, the integrated solution utilising Wazuh, Elasticsearch, Kibana, TheHive, and Cortex is essential for automating and continuously detecting and responding to cyber threats (Naseer *et al.*, 2021). This solution significantly improves the visibility, efficiency, and effectiveness of security operations and analytics, aligning with the principles of the NIST Cybersecurity Framework and addressing contemporary cybersecurity challenges.

3.4.1.4.1 Component Integration and Workflow

In the integrated SOAF, Wazuh acts as the primary agent for data collection and initial processing. It gathers security-related data from various sources, including system logs, network traffic, and file integrity monitoring. For the integration, Wazuh feeds collected data into Elasticsearch for indexing and storage. Elasticsearch then serves as the central data repository for data storage and management. It indexes and stores the data collected by Wazuh, making it searchable and analysable (Allison *et al.*, 2022). For the integration, Elasticsearch's data is accessible through Kibana for analysis and visualisation. Kibana provides a user interface for data analysis and visualisation. Furthermore, it enhances the usability of the data collected by offering a sophisticated user interface that allows users to create and manage dashboards. These dashboards are critical for monitoring security events and discerning trends that may indicate potential security threats (Macedo et al., 2021). For the integration, Kibana directly interacts with Elasticsearch data and presents insights that can trigger responses in TheHive and Cortex.

TheHive manages security incidents and receives alerts from Kibana/Elasticsearch analysis for incident management and response. For the integration, TheHive uses Cortex for additional data enrichment and analysis. Cortex provides automation capabilities for incident response, including running analyzers and responders. For the integration, Cortex automates tasks based on data and alerts from TheHive and sends the results back to manage the case (Groenewegen and Janssen, 2021).

3.4.1.4.2 User Interface Design

The UI is designed to provide a comprehensive and intuitive view of the security operations and analytics using the features and functionalities of Kibana and TheHive. With this UI, users can create and customise dashboards, charts, tables, and maps to visualise and explore the data and alerts. Visual tools not only aid in data exploration and alerts but also improve the ability to dynamically monitor and respond to security incidents (Skopik *et al.*, 2022). Furthermore, the creation and management of cases, tasks, and observables to investigate and remediate the incidents are presented to the user at the UI. This integration streamlines incident investigation and remediation-making (Stevens *et al.*, 2022).

3.4.1.4.3 Data Processing and Automation

The data processing is designed to provide fast and accurate analysis of the security data and alerts using the features and functionalities of Elasticsearch and Cortex. Elasticsearch's capabilities for real-time data indexing and searching are leveraged. Real-time alerts in Kibana based on predefined security rules are implemented. The data processing allows the users to enrich and correlate the data and alerts, as well as to query and aggregate the results. The data processing also allows the users to run various analyzers and responders on the observables, such as IP reputation, domain categorisation, file hash lookup, and URL scanning (Lee, 2023).

Furthermore, for automated incident response, Cortex was used for common security incidents. Machine learning capabilities for predictive analysis and proactive response are also integrated. The automation is designed to provide continuous and proactive detection and response to cyber threats, using the features and functionalities of Wazuh and TheHive. The automation allows the users to collect and monitor security data from various sources and generate and manage alerts for different types of threats. The automation also allows the users to create and execute playbooks, tasks, and actions to investigate and remediate incidents (Wazuh, 2023). Continuous monitoring and automated responses for ongoing threat detection, analysis and mitigation are implemented to achieve continuous detection and response. Feedback mechanisms to continually refine detection rules and response protocols are integrated to ensure the effectiveness and adaptability of security measures. These mechanisms are critical for the continual refinement of detection rules and response protocols, ensuring that security operations evolve in line with the dynamic nature of cyber threats (Mughal, 2022)

3.4.1.4.4 Scalability and Security

The scalability and security of the SOAF was fundamental to its effectiveness in detecting, analysing, and mitigating security threats in complex and high-volume environments. As cyber threats become increasingly sophisticated, organisations must process vast amounts of structured and unstructured security data, including network logs, endpoint telemetry, and threat intelligence feeds (Templ and Sariyar, 2022). To meet these demands, a scalable SOAF must efficiently manage growing data volumes and computational workloads while maintaining real-time threat detection and response capabilities. This is achieved through distributed computing architectures, modular design principles, and cloud-based elasticity, which enable seamless expansion and integration with existing security infrastructure (Krishnan *et al.*, 2023).

However, scalability alone is insufficient without ensuring robust security measures. A highly scalable system must prioritise data protection, access control, and threat resilience to mitigate cybersecurity risks. To achieve this, the SOAF integrates end-to-end encryption, role-based access control (RBAC), and multi-factor authentication (MFA) to prevent unauthorised access to sensitive security data (Almadani *et al.*, 2023; Krishnan *et al.*, 2023). Audit logging, anomaly detection, and automated threat intelligence enhance security by proactively identifying and responding to potential threats before they escalate (Nour, Pourzandi and Debbabi, 2023).

Furthermore, the convergence of scalability and security is facilitated by integrating automation and real-time analytics, which streamline threat detection, incident response, and forensic investigations (Malik *et al.*, 2024). Automated workflows reduce manual intervention, improving efficiency and accuracy in detecting anomalies and correlating security events across vast datasets. This ensures that SOAF remains resilient, adaptable, and capable of evolving alongside emerging cybersecurity threats (Manchana, 2024).

By addressing these dual priorities, the SOAF is designed to meet current organisational needs and provide a future-proof, scalable, and security-enhanced framework for dynamic cybersecurity environments. This ensures that enterprises can effectively adapt to evolving threat landscapes, improve security operations, and enhance overall cyber resilience (AL-Hawamleh, 2024).

3.4.1.4.5 Integration

The core functionalities were initially developed, and the additional features were progressively integrated. Rigorous testing was conducted at each stage, focusing on

system integration, user experience, and security. To integrate these tools, their native APIs, plugins, and connectors were used to enable data exchange and communication among them. The Wazuh Kibana plugin was used to visualise Wazuh alerts and data in Kibana dashboards. The Wazuh RESTful API was used to send alerts from Wazuh to TheHive via HTTP requests. The TheHive4py library was used to interact with TheHive's API from Python scripts. The Cortex4py library was used to interact with Cortex's API from Python scripts. The Elastic Common Schema (ECS) standardised the data fields and formats across different sources. The tools needed to interact with each other in a certain way to achieve the desired outcomes. To achieve this, rules, workflows, and playbooks were defined. The rules for Wazuh were designed to generate alerts based on predefined or custom signatures that match known or unknown attack patterns. The workflows for TheHive were defined to create cases from alerts, assign them to analysts, add tasks and notes, and attach evidence and reports. Finally, the playbooks for Cortex were designed to analyse observables using VirusTotal, Shodan, and MISP sources of information or services and to respond to incidents using actions such as blocking an IP address, isolating a host, or sending an email.

Python scripts were used to specify the decision-making process in order to determine when and how to trigger an automated response. These scripts were used to check for various conditions or events, such as whether an alert had a high severity or priority level, if an observable had a malicious or suspicious reputation score, or if an incident had a certain status or tag. Based on these checks, Cortex responders were invoked by the Python scripts to perform appropriate actions on observables or cases.

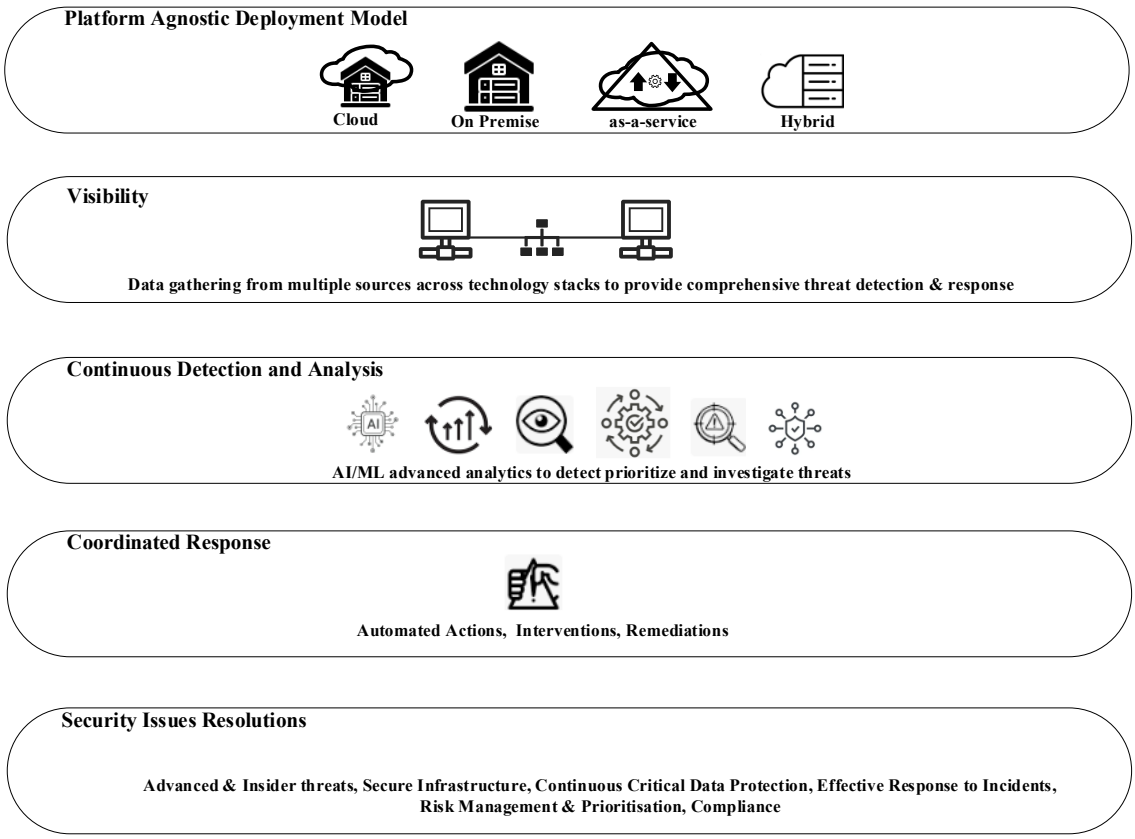

Figure 9: High-Level SOAF Architecture

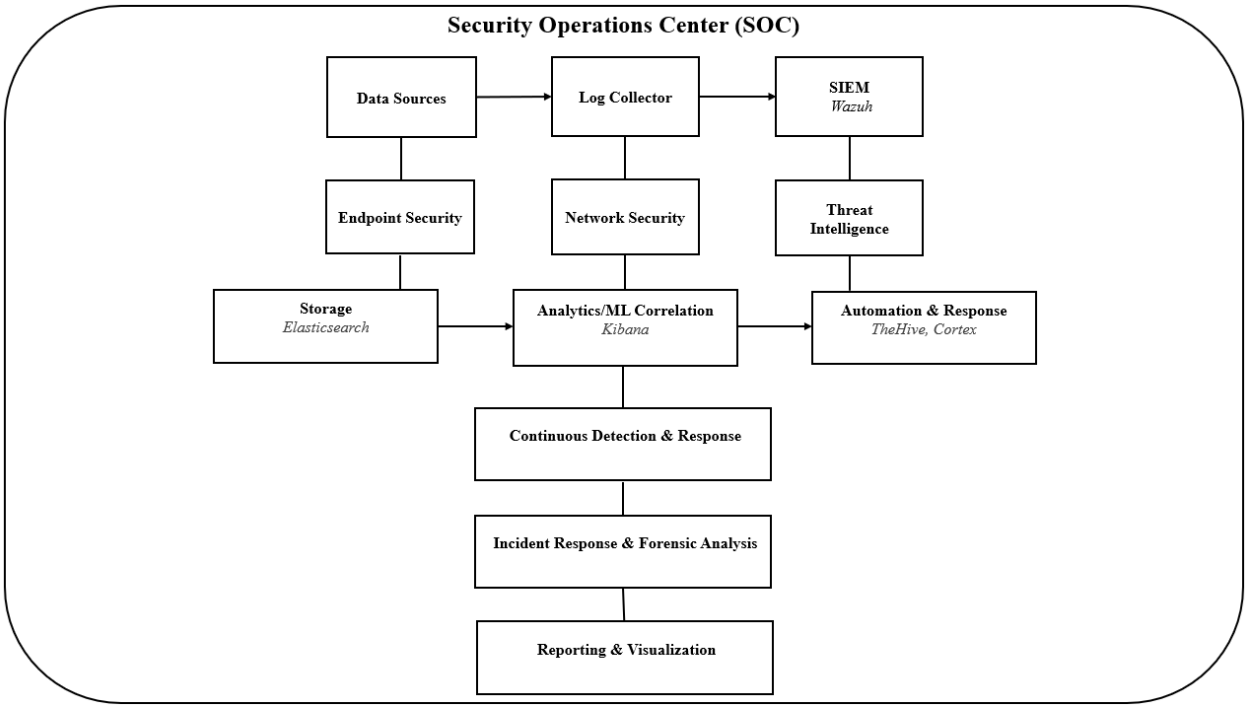

Figure 10: High-level schematic representation of the SOAP Infrastructure.

The proposed architecture, shown in the figures above, aimed to create a cohesive and efficient Security Operations and Analytics Framework. Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex facilitates a comprehensive approach to security monitoring, analysis, incident management, and response, strongly emphasising user interface design, data processing efficiency, and automation capabilities.

3.4.1.4.6 Fault-Tolerant and Highly Available Infrastructure

The infrastructure was designed using a distributed architecture, which incorporated multiple servers and nodes across various virtual locations. This setup not only distributed the load but also provided the necessary redundancy, which is crucial for maintaining system availability and performance under varying loads (Yadav and Paul, 2021). To optimise responsiveness and manage incoming traffic efficiently, load balancers were deployed. These devices distributed incoming application and network traffic across multiple server instances, preventing any single instance from becoming a bottleneck, thus enhancing overall system availability (Shafiq, Jhanjhi and Abdullah, 2022). An Elasticsearch cluster was established with multiple nodes to ensure data redundancy and high availability. Three master nodes were set up to avoid split-brain scenarios, with additional data nodes added as required by increasing data volumes. This configuration ensured reliable search and analytics performance across the SOAF (Negoita and Carabas, 2020). Regular snapshots and backups of the Elasticsearch indices were conducted and securely stored remotely to safeguard against data loss and facilitate data recovery operations (Shukla *et al.*, 2022). Wazuh Managers were deployed in a cluster configuration to enhance the management of agent connections and event analysis. This setup prevented a single point of failure, distributing agent traffic efficiently via a strategically placed load balancer (Sklavidis *et al.*, 2021). Kibana instances were configured statelessly behind a load balancer. This arrangement allowed for handling multiple dashboard access requests concurrently, ensuring smooth and consistent user experiences without local data storage issues (Naseer *et al.*, 2020). The Cassandra database for TheHive and Cortex was configured for replication across multiple nodes. This setup was crucial for ensuring data redundancy and minimising the risk of data loss (Mansouri, Prokhorenko and Babar, 2020). Critical components were equipped with dual network paths and network failover mechanisms. These measures ensured that a backup connection was readily available in the event of primary connection failure, maintaining network reliability (Chiesa *et al.*, 2021). System monitoring tools were implemented to continuously track the health and performance of all components within the

infrastructure. Configured alerts promptly notified issues like high response times or node failures, enabling quick resolution (Achillopoulou *et al.*, 2020). All components were configured in adherence to security best practices specific to each tool, with regular updates applied to protect against emerging vulnerabilities (Taherdoost, 2022). A failure drill was performed to test the system's response to hardware or software failures, ensuring that failover mechanisms work as expected (Yazdi, 2024). The architecture, configurations, and operational procedures, which served as a vital resource for ongoing maintenance and troubleshooting, were documented. These strategic measures that were put in place have strengthened the SOAF's ability to provide consistent and efficient security monitoring. This resilient setup not only tackles the difficulties of maintaining system integrity and performance but also guarantees that the SOAF can withstand any potential disruptions.

3.4.2 Solution Implementation and Demonstration

3.4.2.1 Introduction

The implementation phase of the research involved detailed steps and activities necessary for deploying and operating the proposed SOAF in a real-world setting. This phase was structured around key components essential for a comprehensive setup and effective operation.

The deployment component specified the precise actions and processes necessary for installing and configuring the framework components in the target environment. This included a range of operational duties, such as: (a) Hardware Setup: Creating the physical infrastructure required for the framework. (b) Software Installation: Installing the necessary software components of the SOAF. (c) Network Configuration: Ensuring that the network is set up in a way that enables the smooth functioning of the SOAF processes. (d) Storage Allocation: Assigning enough storage capacity to manage the data processed by the framework. (e) Sensor Activation: Enabling essential sensors to gather data and identify potential threats. (f) SOAP Integration: Enhancing the capabilities of the framework by integrating SOAP.

The tasks were precisely defined, including their requirements, dependencies, necessary resources, and dates, in order to guarantee a seamless implementation (Rani *et al.*, 2022).

After the deployment, the operation component specified the activities and processes required to efficiently monitor and operate the framework in an operational context. The activities encompassed: (a) Data Collection: Acquiring pertinent data from diverse

sources throughout the network. (b) Data Analysis: Examining the gathered data to detect any security risks. (c) Threat Detection: Identifying potential dangers by analysing data. (d) Threat Response: Taking action to address identified threats in order to reduce potential harm. (e) Incident Handling: The process of effectively managing security issues, starting with their identification and continuing until their resolution. (f) Report Generation: Compiling reports that provide a concise overview of security discoveries and occurrences.

This component further defined the roles, duties, requisite abilities, and necessary equipment for each work, guaranteeing that team members were adequately trained and equipped to properly oversee the SOAF (Hajny et al., 2021).

The demonstration phase showcased how the design science research solution was applied within a relevant context through a case study. This phase was methodically planned in two steps.

Solution Application: This step involved applying the SOAF in a real-world scenario reflective of the target environment. It encompassed deploying and operating the framework, engaging with users, and observing how the solution interacted within the environment. The outcome was documented in a case study that detailed the framework's performance and behaviour within the specified context.

Assessment: The case study provided a comprehensive analysis of the proof-of-concept (PoC) project. This project involved deploying the SOAF prototype in an organisation challenged by security operations and analytics issues. The case study described the project’s background, objectives, scope, timeline, roles of participants, and expectations. It included activities such as prototype installation, configuration, security data collection and analysis, threat detection and response, and incident handling and reporting. The results of the PoC project were compiled into security metrics, threat indicators, incident records, user feedback, and stakeholder satisfaction, providing a substantive evaluation of the SOAF’s effectiveness (Forsberg and Frantti, 2023)

This detailed approach in the demonstration phase ensured that the SOAF was not only theoretically viable but also practically effective in a real-world application, thereby affirming the research’s applicability and relevance.

3.4.2.2 Implementation

The implementation process began with the installation of the on-premises virtualised environment, using VMware ESXi as the virtualisation platform. A virtual machine (VM) was created for each component of the SOAP. Each component was allocated adequate CPU, memory, and storage resources, ensuring optimal performance. The prototype was implemented on an Ubuntu 18.04 LTS server. The internal virtual networks were set up with load balancers to ensure redundancy across multiple servers for fault tolerance.

Subsequently, the SOAP components were also installed in a virtualised environment hosted on the public cloud. The cloud service that was selected was Azure, and virtual machines were deployed across various availability zones. Auto-scaling and load balancing were configured to ensure optimal performance. The official Wazuh repository instructions were followed to install the Wazuh Manager, and the Wazuh Manager was downloaded and installed on a dedicated virtual machine for both the on-premises and cloud environments. The 'ossec.conf' file was then edited to configure the Manager for network management and monitoring. Next, Wazuh Agents were installed on the endpoints requiring monitoring. Each agent was registered and connected to the Wazuh Manager using its unique key, as per the instructions provided in the documentation (Wazuh, 2023). Elasticsearch was deployed on a cluster of virtual machines to provide high availability. Elasticsearch was set up for redundancy, and shard replication was enabled. Certificates needed to communicate over TLS between Elasticsearch and Wazuh were installed and then copied to their corresponding locations. To ensure that Elasticsearch automatically started, it was enabled as part of the system boot-up and start-up process.

To check whether the Elasticsearch service was running, a web browser was used to access http://localhost:9200, and `systemctl status` was run for Elasticsearch. The configuration file at '/etc/elasticsearch/elasticsearch.yml' was modified to adjust Elasticsearch and the network settings to meet the requirements. After making the changes, the Elasticsearch service was restarted to enable the changes to take effect. Credentials for the Elastic Stack roles and users were generated, and the installation was verified. Kibana was deployed on a virtual machine and connected to the Elasticsearch cluster. Kibana was configured for high availability using load balancers.

TheHive was set up on a separate virtual machine, which was configured to connect to the Elasticsearch cluster for storing data. Cortex was also installed on a separate virtual

machine, and it was set up to work with TheHive for automated response capabilities. The Cortex Analyzers are an essential part of the Cortex system. They provide a robust and customisable platform for analysing and processing security alerts. These analyzers can be used in various programming languages, such as Python, Java, and Go, making it easier for organisations to customise and extend Cortex's capabilities (Galdi et al., 2022). This adaptability is crucial as it enables integration with other security tools, which enhances the overall management and monitoring of security data.

The core functionality of Cortex Analyzers includes specific analysis tasks like data enrichment, where security alerts are augmented with additional data such as IP reputation and malware characteristics. These tasks are vital for correlating security alerts with threat intelligence feeds, aiding in the identification of related incidents and enabling effective threat intelligence lookups (Kumar *et al.*, 2023). For instance, querying open-source threat intelligence databases can provide insights into specific threat actors or malware, which is essential for proactive security management.

In practical applications, the setup of Cortex involves a variety of analyzers. Some are freely available, while others may require a subscription or license. For example, during a typical installation, tools such as AbuseIPDB, OpenCTI, and VirusTotal are configured to run against observables within Cortex. The setup process includes cloning the Cortex Analyzers repository and installing dependencies from pip-compatible requirements.txt files for each Analyzer (TheHive Project, 2023). Furthermore, the integration of Cortex with TheHive illustrates a seamless workflow where analyzers submit jobs to Cortex, and results are subsequently relayed to TheHive. This integration confirms the successful connection between Cortex and TheHive, simplifying the analysis of cases or alert observables directly through TheHive’s interface, thus bypassing the need for separate logins to Cortex (TheHive Project, 2023). Finally, Cortex Responders play a crucial role in automating incident response actions, such as isolating infected systems or quarantining malware. These plugins enable Cortex to interact with a variety of security systems, enhancing the organisation's capacity to respond to incidents swiftly and effectively.

Cortex was configured to connect with TheHive by creating a Cortex Analyzer in TheHive. This Analyzer is responsible for submitting jobs for analysis to Cortex and delivering the findings to TheHive. The organisation administrator account was used to access the Cortex online user interface, and a user with just read and analyse capabilities was created for the organisation API. Next, the user generated the key by clicking "Create

API Key." The key was copied and added to the TheHive application.conf configuration file in order to update the Cortex connection settings. In addition, the Cortex module was activated, the file was saved, and the TheHive service was resumed. To test TheHive's connection with Cortex, the "About" page of TheHive online user interface was accessed, and Cortex integration was confirmed. After confirming a successful connection between TheHive and Cortex, an analysis of cases or alert observables is accessible through the TheHive web interface without the need to log in to Cortex. Cortex Responders are plugins for Cortex that are designed to automate incident response actions.

Sysmon 14.13 was installed on Microsoft Windows endpoints to monitor and log system activity from the Windows event log. The Sysmon configuration file was appropriately set up to capture relevant security data. To ensure that Sysmon was installed correctly, the Windows Services management console was launched, and the System Monitor service status was checked to be running. Winlogbeat 7.14.2 was also installed on the same endpoints and configured to forward logs from Sysmon and other Windows event logs to Elasticsearch. To verify that the installation was successful, the Windows Services management console was accessed, and the Winlogbeat service status was running. Additionally, the harvested Windows events data was displayed on the Discover tab of the Kibana dashboard.

Suricata, a network intrusion detection system, was installed on a dedicated Ubuntu virtual machine that acted as a network gateway. During the implementation of a use case, the Suricata virtual machine monitored the network traffic and searched for security events that could indicate a potential attack or compromise. The Suricata configuration was set up by editing the 'suricata.yaml' file to specify network interfaces, rules, logging, and output settings and forwarding the logs to Wazuh Manager. On the Wazuh manager, the 'ossec.conf' was configured to ingest the JSON data, and alerts were forwarded by setting up a decoder and rules for Suricata logs analysis. To validate the integration, traffic that triggered Suricata rules was generated and ensured that these alerts were visible in the Kibana dashboard (Suricata Documentation, 2023). During the final stage of system integration and testing, all components were examined to ensure that they were communicating efficiently. Kibana dashboards were configured to facilitate real-time monitoring and alerting. A comprehensive test was conducted to validate the system's functionality and reliability. Additionally, fault tolerance was tested by simulating failures and measuring the system's failover capabilities.

3.4.3 Evaluation

The evaluation of the SOAF is a critical step in verifying its effectiveness in continuously detecting and responding to cyber threats in an automated manner. The evaluation aims to assess the design and implementation of the SOAF, ensuring it effectively integrates various security tools into a cohesive solution. It will measure the SOAF's effectiveness in quality, utility, impact, and value while validating its alignment with cybersecurity goals. Additionally, the evaluation will provide feedback and recommendations for iterative improvement of the SOAF.

This evaluation is structured around four fundamental aspects: quality, utility, impact, and value. Quality refers to the extent to which SOAF meets technical and functional security requirements and industry standards. Utility evaluates the system's ability to address the needs and expectations of users and stakeholders. Impact measures SOAF's contribution to security operation outcomes and goals. Value assesses whether the benefits of SOAF outweigh its operational costs.

A qualitative approach was employed to assess these aspects through data collection methods such as document analysis, interviews, and observations. The use of qualitative methods is aligned with the DSR methodology, emphasising real-world validation of technological innovations (Holtkamp, Soliman and Siponen, 2019). This approach ensures that both subjective user experiences and objective security performance are considered in the evaluation. The use of triangulation ensures the reliability and comprehensiveness of the evaluation by cross-validating information from multiple sources (Meydan and Akkaş, 2024).

The evaluation process is structured into two essential phases: design and execution. The design phase defines the evaluation objectives, research questions, data collection methods, data sources, techniques for analysis, and evaluation criteria. It ensures a structured and rigorous approach that aligns with the DSR methodology (Johannesson and Perjons, 2021). By establishing a solid foundation, this phase enhances the credibility and replicability of the evaluation process.

The execution phase involves applying the established evaluation plan and comprises three main components: Evaluation Planning – Establishing a systematic framework for assessing SOAF's effectiveness. Implementation and Data Collection – Conducting the evaluation using various qualitative methods such as interviews, focus groups, and expert

reviews. Analysis & Reflection – Processing and interpreting evaluation results to extract meaningful insights and inform improvements to the framework.

The evaluation phase is essential to the DSR methodology, as it validates the proposed solution in a real-world cybersecurity environment. Through structured evaluation, SOAF's ability to provide continuous detection and automated responses to cyber threats is assessed. This systematic approach offers several benefits:

Ensuring the Effectiveness of SOAF - Demonstrates that SOAF meets its intended purpose and provides empirical evidence of its capabilities (Peffers et al., 2020).

Aligning with DSR Methodology - Ensures iterative evaluation and refinement of the SOAF artefact, bridging the gap between theoretical research and practical application.

Comprehensive Multi-Dimensional Assessment - Evaluates SOAF's quality, utility, impact, and value to ensure its overall effectiveness.

Using Qualitative Methods for Depth - This approach employs document analysis, interviews, and observations to provide in-depth insights beyond purely quantitative metrics.

Structured Phases for Rigour - Ensures clarity and consistency in evaluation through well-defined design and execution phases.

Real-World Validation - SOAF is tested in real operational environments to confirm its resilience and practical utility, helping to refine the framework for dynamic cybersecurity challenges (Cremer, Sheehan, Fortmann, Arash N Kia, *et al.*, 2022).

A structured qualitative approach is used to assess SOAF's effectiveness, mapping qualitative metrics to the four key evaluation aspects. The first aspect is Quality Metrics, which includes Technical & Functional Performance. These metrics assess SOAF's compliance with security standards and its operational reliability. They are (a) Adherence to Security Standards – Evaluates alignment with frameworks such as NIST, MITRE ATT&CK, or ISO 27001. (b) Detection Accuracy Perception – Assesses whether alerts are perceived as relevant and actionable. (c) False Positive & False Negative Feedback – Gathers qualitative feedback on the accuracy of threat detection. (d) System Stability & Reliability – Measures system performance in real-world use cases. (e) Ease of Integration – Examines SOAF's compatibility with existing security tools and workflows.

The second aspect is Utility Metrics, which includes User & Stakeholder Experience. These metrics evaluate SOAF's usability and its effectiveness in meeting user needs. They are (a) Analyst Workload Reduction – Assesses whether SOAF reduces repetitive tasks for security analysts. (b) Usability & Learning Curve – Captures user feedback on ease of use and adoption. (c) Incident Response Efficiency – Evaluates improvements in speed and accuracy of incident handling. (d) Customisability – Determines how easily users can tailor SOAF's functionalities. (e) User Trust & Confidence – Measures stakeholder confidence in SOAF's capabilities.

The third aspect is Impact Metrics, which includes Operational & Security Outcomes. These metrics assess SOAF's contributions to security operations:

(a) Incident Detection & Response Enhancement – Evaluates SOAF's role in improving security incident visibility and response times. (b) Operational Workflow Improvement – Measures the extent to which SOAF streamlines security operations. (c) Collaboration Effectiveness – Assesses whether SOAF enhances team coordination. (d) Security Team Satisfaction – Captures user perceptions of SOAF's impact on job efficiency. (e) Incident Investigation Depth – Examines whether SOAF provides sufficient data for thorough incident analysis.

The fourth aspect is Value Metrics, which includes Cost-Benefit & Organisational Contribution. These metrics evaluate SOAF's return on investment and strategic value.

(a) Return on Security Investment (ROSI) Perception – Assesses whether SOAF's benefits outweigh its costs. (b) Operational Cost Savings – Evaluates SOAF's impact on reducing labour and resource expenses. (c) Competitive Advantage – Determines whether SOAF enhances the organisation's cybersecurity posture. (d) Regulatory & Compliance Alignment – Examines SOAF's effectiveness in meeting compliance requirements (e.g., GDPR). (e) Strategic Contribution – Assesses SOAF's role in supporting long-term security goals.

Qualitative Data Collection Methods involved gathering data from various sources to assess qualitative metrics. The following were used (a) User Interviews & Focus Groups – Collects insights from SOC analysts, security managers, and IT teams. (b) Observations – Analyses how security teams interact with SOAF in real-world scenarios. (c) Questionnaires – Uses open-ended survey questions to capture detailed user feedback. (d) Expert Reviews – Engages cybersecurity professionals to assess SOAF's design, implementation, and effectiveness.

The structured evaluation of SOAF provides critical insights into its performance, usability, and overall value in security operations. By employing a rigorous qualitative approach, the evaluation ensures that SOAF meets industry standards, enhances security operations, and delivers a tangible return on investment. The findings from this assessment will be instrumental in refining SOAF and advancing the state of security operations and analytics.

3.4.3.1 Evaluation Design

A case study methodology was used as a qualitative tool to thoroughly analyse the SOAF architecture in its natural setting throughout the assessment design phase. This method was chosen as it allowed for answering the how and why questions about the complex and dynamic system that involves multiple components, interactions, and outcomes (Quintão, Andrade and Almeida, 2020; Priya, 2021). Additionally, this method could use multiple sources of evidence, such as documents, interviews, observations, and artefacts, to validate and triangulate the findings. It also facilitated the application of DSR principles by evaluating innovative artefacts that solve real-world problems (Barcellos *et al.*, 2022).

The evaluation design phase was the first step in defining the evaluation's scope, purpose, and methodology. It consisted of four main elements: objectives, questions, methods, and criteria. The focus was on qualitative methods to assess the system's effectiveness, efficiency, and adaptability. The objectives of the evaluation were fourfold. Firstly, to assess the framework's capability to effectively identify and handle security incidents, as well as the effectiveness of the SOAF in enhancing cybersecurity measures through automation and real-time threat detection, investigation and response (Hansen and Haj-Bolouri, 2020). Secondly, to provide feedback and recommendations for improvement based on the evaluation results and findings. Thirdly, to evaluate the efficiency of the analytics and automation processes in reducing detection and response times, and to compare them with other existing or alternative solutions. Fourthly, to determine the framework's adaptability to evolving security threats and its scalability for different organisational sizes and contexts (Shah, 2021).

The critical evaluation questions were formulated based on the objectives and aimed to address four main aspects of the framework. Firstly, the effectiveness of the framework in identifying and mitigating a variety of security threats (Qiu *et al.*, 2021). Secondly, the impact of the framework on the time taken to identify and address security issues (Karie

et al., 2021). Thirdly, the adaptability of the framework to new and emerging security threats (Paniagua and Delsing, 2020). Fourthly, the challenges and limitations of implementing and operating the framework (Tandon *et al.*, 2020).

Furthermore, two data collection techniques were employed as part of the qualitative approach methods. The first technique was case studies, which involved conducting an in-depth analysis of simulated security incidents to understand the framework's response mechanisms. The second technique was expert interviews, which involved gathering insights from cybersecurity experts on the framework's design, functionality, and performance (Alam, 2021).

The evaluation problem was to assess the effectiveness and efficiency of the SOAP architecture in detecting and addressing all threats in a simulated setting, using a security operations and analytics platform that comprises Wazuh, Elasticsearch, Kibana, TheHive, and Cortex for automation and continuous detection and response, and using Sysmon, Suricata, and Wazuh agent monitoring capabilities (González-Granadillo, González-Zarzosa and Diaz, 2021).

The evaluation used two data sources, two data collection techniques, two data analysis techniques, and four evaluation criteria. The data sources were simulated incident reports, which were generated by triggering predefined security incidents within the simulated environment, and operational logs, which were obtained from Wazuh, Elasticsearch, Kibana, TheHive, and Cortex and detailed the detection, analysis, and response actions. The data collection techniques were observation, which involved monitoring the system's real-time response to simulated attacks, and document review, which involved analysing logs, incident reports, and response outcomes generated by the platform. The data analysis techniques were content analysis, a qualitative analysis of textual data from logs and reports to identify patterns, effectiveness, and areas for improvement, and thematic analysis, a technique for identifying themes across expert interviews and case study findings to evaluate user experience and system adaptability (Stojkovski *et al.*, 2021).

The evaluation criteria were effectiveness, which referred to the accuracy and completeness of threat detection, investigation and response; efficiency, which referred to the speed of detection and response and the reduction of false positives; adaptability, which referred to the system's ability to incorporate new threat intelligence and adapt to emerging threats, and user experience, which referred to the ease of use of the system and the clarity of the information presented.

This evaluation design's purpose was to comprehensively understand the SOAF's performance in a simulated environment. To achieve this, qualitative methods were leveraged, as they could capture in-depth insights into the system's capabilities and areas for improvement.

3.4.3.2 Evaluation Execution

The evaluation execution phase was a crucial part of the design science research methodology, as it validated the proposed solution in a real-world context. It had four stages: Preparation, Scenario Definition, Data Collection, and Data Analysis (vom Brocke, Hevner and Maedche, 2020).

A controlled environment that replicates real operational conditions was created. This involved setting up a security operations and analytics platform, which features Wazuh, Elasticsearch, Kibana, TheHive, Cortex, Sysmon, and Suricata. Such an environment is crucial for an effective and realistic simulation and aligns with best practices outlined in security analytics frameworks (Sankar and Fasila, 2023). In the Scenario Definition Stage, a series of security incident scenarios were developed to test the security framework against various types and levels of threats. This evaluation ensured the reliability and effectiveness of the security solutions under consideration. Prior to this stage, preparations were made to ensure that the scenarios were comprehensive (Winter and vom Brocke, 2021). In the Data Collection Stage, predefined security incidents were triggered in the simulated environment to monitor the system's real-time responses. It was essential to gather logs, incident reports, and response outcomes for further analysis. This step was crucial for operational security assessments (Al-Dhaqm *et al.*, 2020). During the data analysis stage, the collected data was processed and interpreted in detail. Content and thematic analysis qualitative methods were utilised to examine the data and determine the solution's effectiveness against certain criteria, such as efficiency, adaptability, and user experience (Straßburg *et al.*, 2021).

3.4.3.3 Simulating CDR for Windows Utilities Prone to Abuse

The main objective of this scenario simulation was to showcase the framework’s operational capabilities, including Sysmon and Wazuh agent monitoring. It is well documented that malware takes advantage of built-in Microsoft Windows to accomplish its malicious objectives (Sibi Chakkaravarthy, Sangeetha and Vaidehi, 2019; Alenezi *et al.*, 2020). The demonstration concentrated specifically on continuous monitoring,

detection, and response to the execution of Windows utilities that are prone to abuse, including PowerShell and Windows Task Scheduler.

While the presence of these tools on endpoints may not always indicate a harmful attack, it is important to closely monitor them for several reasons. Firstly, conducting forensic analysis of these tools enhanced comprehension of the actions taking place on the observed endpoints. Additionally, monitoring these tools helped identify instances of misconduct perpetrated by malevolent individuals.

The Windows Task Scheduler is a tool built into the Windows operating system that triggers programs and runs predefined scripts at specific times or intervals. Although the Task Scheduler itself is not harmful, the attackers leveraged it to create malicious tasks that were executed to achieve their objectives. One common tactic used by threat actors like Agent Tesla and APT3 was to exploit the limited visibility in monitoring the Task Scheduler (MITRE ATT&CK, 2023). The Task Scheduler was used to download and execute scripts that operate directly in the computer's RAM, leaving no traces in the permanent disk storage. This made it challenging to detect such activities compared to typical scenarios.

Automation, setup, and administration are all made easier using PowerShell, a scripting language and command-line shell. However, malicious actors exploited PowerShell to execute malware, steal credentials, and bypass security controls (Gittins and Soltys, 2020). Therefore, monitoring and analysing PowerShell activities and responding to any anomalous or suspicious events was imperative.

To implement the use case on the Windows endpoint and detect the activities of Wazuh, Sysmon, Elasticsearch, Kibana, TheHive, and Cortex using the SOAF architecture, the series of steps were followed as described in the previously discussed implementation section. The SOAF platform was deployed and operated after installing and configuring the tools and setting up the attack scenario in the simulation environment.

The attack simulation was designed to mimic a real-world ransomware campaign that explicitly targets Windows systems using legitimate utilities known as living-off-the-land binaries (LOLBins), which were exploited for malicious purposes. The purpose of the simulation was to test the network's resilience against these Windows utilities that are prone to abuse. In this scenario, a phishing email was successfully sent to a Microsoft Windows user on the network from an attacker pretending to be from the IT department. The email contained a malicious document attachment that claimed to be an important

update. The document was opened, and the macro was enabled, as instructed by the email. The macro executed a PowerShell script that downloaded and ran a malicious DLL using Rundll32, a legitimate Windows process. The DLL created a scheduled task using Schtasks, a built-in Windows command-line tool, which was configured to launch the ransomware payload after five minutes. The ransomware payload, upon activation, encrypted the files on the system and displayed a ransom note requesting funds in return for the decryption key to restore the files.

The SOAF platform carried out the following actions: Upon detection of the suspicious activity, the CDR monitoring components of the SOAF system, which included Wazuh agents and Sysmon worked together to monitor and log the system activities and anomalies on the Windows endpoint. In this scenario, Wazuh agents were installed and set up on the endpoint to gather Sysmon logs from the Windows event log. Furthermore, Sysmon was installed and configured on the endpoint to capture events related to the execution of PowerShell, Rundll32, and Schtasks, as well as any time a file was created with a locked extension. These collected events were then analysed and logged by Sysmon, providing detailed information such as process name, process creation, command line, parent process, network connection, file creation, and registry modification events generated by the attack.

Wazuh agents forwarded the Sysmon logs to the Wazuh server, processing and analysing them using Wazuh rules and decoders. Wazuh rules and decoders were then used to identify and classify the Sysmon events as suspicious or malicious and to generate alerts based on predefined or custom criteria. Wazuh rules and decoders generated alerts every time PowerShell, Rundll32 and Schtasks were executed or every time a file was created with a certain extension. Wazuh alerts contain the relevant information from the Sysmon events, including the event ID, process name, command line, file name and file hash.

Elasticsearch was responsible for receiving, indexing and storing the data and alerts generated by Wazuh and Sysmon. It provided a scalable and easily searchable database for the SOAF platform. Additionally, Elasticsearch performed data enrichment and analysis by utilising machine learning, anomaly detection, threat intelligence, geolocation, reputation, alert correlation features, and plugins.

Kibana received and displayed data and alerts from Elasticsearch. It provided a user-friendly interface for the SOAF, allowing for the creation and customisation of

dashboards and visualisations. It also offered the ability to explore and investigate data through filters, queries, timelines, and map features and tools.

TheHive managed the alerts received from Wazuh and Elasticsearch. It provided a workflow for the SOAF platform, enabling the automated creation and tracking of cases for the alerts. It facilitated the assignment and collaboration of the cases using tasks, observables, tags and metrics. TheHive created a case with a predefined template that included the file name, hash, size, and URL details of the alert associated with the malicious activity from Wazuh and Elasticsearch. The case also had a set of tasks to be performed by the analyst, including verifying the alert, isolating the infected system, analysing the malware, and restoring the files. The case included various tasks and observables pertaining to an alert. These tasks included analysing the file through Cortex, assessing the reputation of the URL using Cortex, examining similar events in Elasticsearch, contacting the user and verifying the legitimacy of the file, isolating the user's machine if found to be malicious, updating the case status and generating a report, and automating the analysis and response process with Cortex.

Cortex, an open-source observable analysis and active response engine performed automated analysis and responses to the incident by integrating seamlessly with TheHive. It can be accessed from the case view. Cortex leveraged its threat intelligence capabilities to cross-reference the file hash and URL details provided in the case against known IOCs and threat intelligence feeds. This step helped identify any additional malicious artefacts associated with the attack. Cortex utilised various analyzers and responders to enhance the observables from the alert. This included analysing the file hash, URL, and address. Cortex took the following steps to analyse the threat: The file and URL were scanned using VirusTotal, and the detection ratio, tags, and comments were obtained. An inquiry was made on AbuseIPDB to assess the credibility of the IP address linked to the URL and the results of the abuse score, country, and reports were obtained. Based on the analysis results, a responder was executed to take appropriate action. The actions were blocking the IP address, quarantining the file, and creating a ticket.

The analyst viewed the analysis results in a unified and interactive interface and filtered them by categories, tags, or scores. The analyst also updated the observables in TheHive with the analysis results and added them to the case report. Subsequently, Cortex initiated dynamic malware analysis on the suspicious DLL file to uncover its behaviour and capabilities. Through sandboxing and behavioural analysis techniques, Cortex identified the ransomware's encryption mechanisms, communication channels, and persistence

mechanisms. With this information, Cortex swiftly devised and executed response actions to contain the incident. This included isolating the infected system from the network, terminating the malicious processes, and quarantining the encrypted files to prevent further damage. To summarise, Cortex received and executed the analyzers and responders for the alerts and cases from TheHive and Elasticsearch. It provided an automation and orchestration layer for the SOAF platform. Cortex also allowed the analyst to perform enrichment, investigation, response and remediation actions on the alerts and cases.

Through the coordinated efforts of TheHive and Cortex, the security team effectively contained the ransomware incident, mitigated its impact, and fortified the network against similar threats in the future. By using TheHive and Cortex, the analyst could efficiently and effectively handle the security incident, leveraging the power of automation, integration, and collaboration. The analyst can also share the case and the observables with other platforms, such as MISP or Elasticsearch, and enrich the knowledge base for future incidents.

3.4.3.4 Simulating Network Attacks and Traffic

This particular use case illustrates how the PCAP files dataset was used to imitate an attack on IoT devices. Additionally, it provides an explanation of how the data was gathered, analysed, and responded to using the SOAF platform. The primary aim of this simulation was to demonstrate the operational capabilities of the framework, including the monitoring capabilities of Suricata and Wazuh agents.

The PCAP files dataset includes network traffic captures from IoT devices exhibiting normal and malicious activities. The framework's operational capabilities were demonstrated by simulating an attack using this dataset (Garcia, Parmisano and Erquiaga, 2020) (Abdalgawad *et al.*, 2022). The dataset includes 23 scenarios: 20 infected with various IoT malware samples and 3 benign ones. It also provides labels, network flow descriptions, and malware samples.

The PCAP files dataset was used to create a simulated attack scenario on an IoT device, where a malicious actor compromised the device and tried to perform scanning, exfiltration, and ransomware encryption malicious activities. To replicate actual network interactions, a malicious scenario was selected from the PCAP files dataset, and the tcpreplay network traffic generator tool was used to replay the network traffic on the

virtual LAN monitored by Wazuh and Elasticsearch. This ensured that the traffic replicated network interactions, resulting in a realistic simulation. Through this process, the impact of the malware on both the IoT devices and the network was emulated and studied. Wazuh was used to collect and analyse data from a PCAP file containing both malicious and benign traffic, generating alerts based on predefined rules and signatures. The XDR function of Wazuh also analysed event data from the monitored endpoints and detected suspicious activity (Wazuh, 2023). Automated responses were issued to prioritise alerts and handle threats quickly. The Suricata module processed the PCAP file and generated alerts based on network events and signatures.

Suricata is an intrusion detection system that analyses network events and produces warnings when it identifies suspicious or malicious activities (K *et al.*, 2024). Administrators may extend the capability of Wazuh and XDR in their environment by combining Suricata with the Wazuh active response module. Suricata may apply automated reaction actions to certain events discovered on monitored endpoints (Gupta and Bassett, 2024). Wazuh also used the VirusTotal module to scan the IP addresses and domains involved in the network traffic and obtain threat intelligence information. Wazuh then successfully forwarded the alerts and threat intelligence data to Elasticsearch for storage and indexing.

The security data collected from Wazuh was analysed and correlated using Elasticsearch for data analysis. Before indexing the data, Elasticsearch applied its pipeline to filter, transform and enrich it. Elasticsearch used the Elasticsearch security plugin to provide role-based access control, encryption, and auditing features for the data. Elasticsearch performed complex queries and aggregations on the data to identify patterns, trends, and anomalies in the network traffic and events. Furthermore, Elasticsearch applied advanced machine learning techniques to detect any anomalies and outliers in network traffic. Based on the anomaly scores and the threshold values, Elasticsearch generated alerts. These alerts and relevant data were forwarded to TheHive for efficient case management and investigation.

Kibana was used for data visualisation and to explore patterns, trends, and anomalies in security data stored in Elasticsearch. It provided an overview of the network traffic, the devices involved, and the details of the events and the alerts. Kibana used the Wazuh application to display Wazuh alerts and threat intelligence data in a user-friendly and interactive interface. Additionally, the Kibana Dashboard application was used to create

and customise dashboards that displayed the number of alerts, alert severity, alert categories, source and destination IP addresses, protocols, geolocation metrics and indicators of the network traffic and events, and the VirusTotal results. Finally, to search, filter, drill down the data and view raw documents in Elasticsearch, Kibana used the Kibana Discover application.

The security incidents and cases derived from security data were created, managed, and responded to using TheHive and Cortex. The alerts and data received from Elasticsearch were used to create cases based on source and severity. TheHive also assigned tasks and workflows to the cases and the analysts. TheHive utilised the Wazuh-TheHive integration to import the Wazuh alerts and threat intelligence data as observables into TheHive. TheHive used the Elasticsearch-TheHive integration to import Elasticsearch documents as observables into TheHive. TheHive created and assigned the case based on the observables and alert severity. Moreover, Cortex-TheHive integration was used by TheHive to execute and automate security analysis and actions on the observables and cases. Using the analyzers and responders library, Cortex performed domain and IP reputation, URL reputation, file analysis, email analysis, threat intelligence tasks, and incident response. Cortex also provided a graphical interface to display the results and the actions of the analyzers and the responders. It allowed for the analysers' and responders' configuration and customisation based on needs and preferences. The capabilities and features of the SOAF were employed to recognise and respond to an attack scenario. The SOAF detected and responded to simulated attack scenarios by analysing the PCAP files dataset containing malicious and benign traffic. The different components of the SOAF were utilised to identify malicious activities such as port scanning, data exfiltration, and ransomware encryption initiated by the compromised IoT device.

The SOAF detected the Mirai malware infection and activity, command and control (C2) communication, brute-force attacks, DDoS attacks, and network scanning. The port scanning activity performed by the compromised IoT device was detected using the alerts generated by Wazuh and Elasticsearch. Furthermore, the anomalous increase in the number of TCP SYN packets and the number of unique destination ports in the network traffic using Kibana were observed. The data exfiltration activity performed by the compromised IoT device was detected using the alerts generated by Wazuh and Elasticsearch. The anomalous increase in the volume and the entropy of the outgoing traffic from the device using Kibana were also observed. Cortex was used to analyse the

traffic and identify the malicious domain and the malware family involved in the exfiltration using the VirusTotal analyzers. The ransomware encryption activity performed by the compromised IoT device was detected using the alerts generated by Wazuh and Elasticsearch. An anomalous decrease in the number of SMB files and the number of SMB write operations from the device using Kibana was observed. Cortex was used to analyse the traffic and identify the ransomware family and the encryption key used in the encryption using the RansomCoin and CryptoScore analyzers. Additionally, the SOAF enriched and triaged the security data with threat intelligence and analysis from multiple sources. Moreover, it also automated and orchestrated security response and incident resolution processes using its integrated tools and technologies. As a result, the infected device was isolated, malicious traffic blocked, and the data that had been encrypted was restored.

The port scanning activity was responded to by isolating the compromised IoT device from the network using the Wazuh agent and the Wazuh responder in Cortex. The malicious traffic from the device was blocked using the Elasticsearch firewall plugin and the Elasticsearch responder in Cortex. The data exfiltration activity was responded to by blocking the malicious domain and the malware communication using the Elasticsearch firewall plugin and the Elasticsearch responder in Cortex. The malicious domain and the malware sample were reported to the VirusTotal services using the VirusTotal responders in Cortex. The ransomware encryption activity was responded to by restoring the encrypted files from the backup server using the Wazuh agent and the Wazuh responder in Cortex. The encrypted files were decrypted using the encryption key obtained from the CryptoScore analyzer and the CryptoScore responder in Cortex.

In conclusion, a demonstration of how SOAF was implemented in a simulated setting using a SOAP composed of Wazuh, its agents, Suricata, Sysmon, Elasticsearch, Kibana, TheHive, and Cortex.

3.4.3.5 Data Collection

Simulated attacks were carried out, as described in the previous section, by running pre-defined security incidents within the simulation. This step was crucial for generating the required data for analysis (Al-Dhaqm *et al.*, 2020). Observational data were collected through a series of demonstrations, simulations, and tests that were designed to showcase the SOAF in action. These sessions were recorded using a combination of videos and

screenshots, which captured the framework's response mechanisms and user interactions in real-time. This approach provided a dynamic view of the SOAF's operational capabilities and user interface design.

To learn more about the user's perspective and the operational efficacy of the SOAF, the stakeholders, cybersecurity experts and potential users of the system were interviewed using a semi-structured format, to gather qualitative insights into the framework's design, usability, and performance. These discussions were carefully noted, revealing first-hand accounts of the framework's performance and areas for improvement from those who were directly interacting with the system.

The focus group discussions were arranged to gather feedback from a small and varied group of SOAF users and stakeholders. These sessions were moderated to promote open dialogue and were carefully documented through detailed notes. This documentation highlighted consensus opinions and divergent perspectives regarding the framework's usability and user-friendliness.

The result of the data collection process involved coding the collected data to facilitate analysis. Employing content and thematic coding techniques, the data was organised and labelled in alignment with the evaluation's questions, objectives, and criteria. This structured approach enabled a systematic examination of the SOAF's attributes and performance metrics. The data collection process for evaluating the SOAF was comprehensive, leveraging multiple techniques to capture a holistic view of the framework's capabilities. Through document review, observation, interviews, and focus groups, a rich dataset was compiled and subsequently coded to support a thorough analysis. The insights derived from this process are pivotal in assessing the SOAF's effectiveness in automating and continuously detecting and responding to cyber threats, ultimately guiding enhancements to fortify its cybersecurity posture.

3.4.3.6 Challenges and Limitations

The evaluation process faced some challenges and limitations. Although the simulated testing environment was comprehensive, it could not fully mimic the complexity and unpredictability of real-world cyber threat landscapes, which may impact the generalisation of the findings (Robles-Durazno *et al.*, 2021).

The large amount of data generated by SOAF presented challenges for efficient filtering and analysis. This occasionally caused delays in identifying critical threats among numerous benign alerts (Wang and Jones, 2021).

3.4.3.7 Recommendations

The assessment results lead to the proposal of the following suggestions to enhance the SOAF framework. From a technical enhancements' perspective, advanced machine learning algorithms need to be implemented to improve the efficiency of data analysis, helping to distinguish between false positives and genuine threats more effectively (Shah, 2021). Furthermore, Kibana requires further enhancements to provide a more user-friendly user interface and dashboard customisation options for varying levels of expertise (Demertzis et al., 2019).

Thorough training programs and documentation should be created to address users' training needs. Users will find this helpful for learning how to tailor and apply SOAF to their unique operating requirements. Workshops covering advanced features and best practices for threat detection, investigation and response should be offered regularly (Hossain, Sarma and Chakma, 2020).

More research should focus on multi-year longitudinal studies spanning at least three years to be conducted in real-world settings to evaluate SOAF's efficacy and efficiency further. To enhance SOAF's capabilities, especially in domains like automated threat hunting and predictive analytics, the possibility of incorporating more open-source tools should be investigated (Alzahrani and Alenazi, 2021).

The evaluation of the SOAF through detailed content and thematic analysis of logs, reports, and user feedback has highlighted the framework's value in contemporary cybersecurity practices. The analysis has revealed that SOAF is efficient in threat detection, investigation and response and has identified opportunities for further development to enhance user training, system adaptability, and response efficiency. By focusing on these areas, SOAF can continue to evolve as a dynamic and effective tool in the fight against cyber threats, offering organisations a high degree of protection in the increasingly digital world (Nassar and Kamal, 2021).

3.4.4 Evaluation Reflection

Cyber-attacks are becoming more complex, necessitating innovative solutions in detection and response, which require the use of frameworks such as the SOAF. This

framework utilises a suite of open-source tools, such as Wazuh for security monitoring (Moiz et al., 2024), Elasticsearch and Kibana for data analysis (Shah, Willick and Mago, 2022), and TheHive and Cortex for incident response and intelligence gathering (Preuveneers and Joosen, 2023). The aim of the SOAF was to automate and continuously detect and respond to cyber threats. This analysis critically evaluates the evaluation process of the SOAF through a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis. The evaluation highlights the framework's strengths, such as its comprehensive tool integration and automation capabilities, which enhance its effectiveness in managing cyber threats (Ahmad, Kevin C Desouza, *et al.*, 2020). However, the analysis also identifies weaknesses, including potential challenges in tool interoperability and the need for significant initial configuration (Lee *et al.*, 2021). Additionally, the analysis explores opportunities for the SOAF to evolve with emerging technologies and adapt to new threat landscapes. It also considers the threats posed by rapidly advancing cyber-attack techniques that may outpace the framework's capabilities (Tahmasebi, 2024). The discussion addresses the limitations, assumptions, and biases that may impact the evaluation's outcomes, ensuring a balanced and thorough assessment.

3.4.4.1 Strengths

The SOAF has been assessed and found to possess several advantageous qualities that enhance cybersecurity measures. The use of open-source technologies makes it financially efficient for continuous threat monitoring and analysis, especially for businesses with limited resources (Pearce, 2020). Additionally, automated detection and response procedures significantly reduce the time needed to detect and mitigate risks, thus improving operational efficiency. Although the assessment is challenging in acquiring information, it provides a comprehensive understanding of operational capacities and the possibility of integrating chosen instruments. The SOAF integrates several technologies into a comprehensive security solution that enhances both detection and response capabilities. It provides the opportunity to customise and improve the framework to cater to distinct business requirements (Park *et al.*, 2022). Furthermore, the user interface of the SOAF focuses on user-centricity, ensuring intuitive use and enabling effective incident management. The integration of TheHive and Cortex has been instrumental in facilitating efficient cooperation and information exchange between security teams (Olukoya, 2021).

3.4.4.2 Weaknesses

The assessment of the SOAF framework also revealed some shortcomings that could impede its effectiveness. One of the primary challenges was the complex process of integrating several open-source technologies into a cohesive framework. This intricate process was marked by compatibility issues and the need for substantial customisation, which can potentially discourage firms that lack technical proficiency (Haider *et al.*, 2023). Additionally, the assessment identified a lack of thorough documentation and community assistance, which are crucial for resolving issues and improving the framework for continuous maintenance and improvement.

The integration of different instruments requires intricate settings, which could be a barrier for firms with limited technical resources (Eghbal, 2020). The SOAF framework's comprehensive scope also necessitates a significant amount of computing resources, which could limit its use in settings with limited resources. Furthermore, the significant learning curve experienced by novice users may result in delays in fully utilising the framework's capabilities.

3.4.4.3 Opportunities

After assessing the capabilities of the SOAF, it has become apparent that there is room for improvement. One way of improving the framework's threat detection, investigation, and response capabilities is by incorporating state-of-the-art machine learning techniques. This progress could lead to the development of predictive models that can proactively detect potential risks by analysing past data (Agrawal, 2023). Additionally, by expanding the framework to include a wider range of open-source technologies, one can increase its adaptability and customisation to meet the unique needs of various organisations (Romero *et al.*, 2024).

Participation in the cybersecurity community can foster productive partnerships, strengthen support systems, and facilitate the sharing of best practices and innovative approaches. The SOAF's open-source tools allow for continuous growth and additions driven by the community (Fisk, Kelly and Liebrock, 2023). Scalability is a key feature of the SOAF, as it can accommodate the expansion of organisational infrastructures and the increasing complexity of cyber threats (Djenna, Harous and Saidouni, 2021). Implementing comprehensive training programs can effectively mitigate the challenges associated with the learning curve and enable users to utilise the extensive capabilities of the SOAF fully (AlDaajeh *et al.*, 2022).

3.4.4.4 Threats

Several external threats may significantly affect the assessment and implementation stages of the SOAF. In order to be successful, the framework must continually adapt to the rapidly changing world of cyber threats. This requires ongoing examination and upgrades. However, the constantly evolving nature of this environment can place significant demands on available resources, resulting in challenges related to prioritisation (Manoharan and Sarker, 2023). Furthermore, the use of open-source tools has potential hazards, including security vulnerabilities, the potential for project termination, and delays in updates. The reliability and efficiency of the system are jeopardised by these elements (Prana *et al.*, 2021).

The rapid rate of technological improvements is also a potential risk to the SOAF, as its components may become obsolete if not regularly updated (Kechagias *et al.*, 2022). Moreover, the continuous development of cyber threats is a substantial danger that poses a challenge to the SOAF's long-term effectiveness unless it can quickly adapt (Khan and Ghafoor, 2024). Resource constraints are another potential risk that may hinder the maintenance and update of the SOAF. This can affect its performance and the overall security it provides (Nyangaresi, 2022).

3.4.4.5 Limitations, Assumptions, and Biases

This assessment's accuracy, consistency, and applicability are subject to certain limitations, assumptions, and biases. One key assumption was that integrating the selected cybersecurity tools; Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, would seamlessly create a comprehensive SOAF. However, in complex operational environments, security frameworks often require extensive customisation and integration with existing security architectures, which may limit their immediate effectiveness (Grigaliūnas *et al.*, 2024). Additionally, the reliance on open-source tools introduces potential biases, as the assessment may not have fully considered commercial alternatives that offer advanced support services, regulatory compliance features, and proprietary threat intelligence feeds (Lee and Singh, 2021).

Another critical limitation is the scope of the evaluation, which may not fully capture the framework’s long-term efficacy in dynamic threat environments. Cyber threats evolve rapidly, and while the evaluation was conducted based on contemporary threat models, future adversarial tactics and attack vectors may challenge the framework’s adaptability (Hernández-Rivas, Morales-Rocha and Sánchez-Sol\’\is, 2024). Furthermore, the

research approach might have unintentionally emphasised threat detection and response aspects that align with open-source methodologies, potentially underrepresenting alternative security paradigms that commercial solutions provide (P. S. , 2023).

Moreover, the study assumes that cybersecurity professionals implementing the SOAF have the expertise to configure, manage, and fine-tune these tools for optimal performance. In reality, organisations with limited security expertise may face challenges in operationalising such a framework effectively, leading to inconsistent results across different contexts (Alhidaifi, Asghar and Ansari, 2024). Additionally, the evaluation does not account for potential resource constraints, such as computational overhead or storage requirements, that could impact performance in large-scale deployments.

To mitigate these limitations, future research should consider comparative analyses with commercial SIEM solutions, longitudinal studies assessing SOAF's adaptability over time, and real-world deployments in diverse industry settings. These steps would enhance the framework's generalisability and provide a more balanced perspective on its effectiveness in security operations.

3.4.4.6 Conclusion

The SWOT analysis conducted on the SOAF revealed a framework with great potential for improving cybersecurity measures. However, it has also emphasised the need for ongoing improvement, active community involvement, and flexibility in response to ever-evolving technology and threat environments. By proactively engaging with the discovered vulnerabilities and potential risks and leveraging the inherent advantages and opportunities, the SOAF can evolve into a more robust and effective cybersecurity solution. This critical analysis not only sheds light on the current state of the SOAF but also outlines a strategic path for its future growth and implementation. The investigation highlights a system that demonstrates both resilience and adaptability, with significant potential for automating cyber threat detection, investigation and response. Although there are obstacles to overcome, the potential for improvement and adjustment creates a positive outlook for the continuous development of the SOAF and its importance in the field of cybersecurity.

3.5 Ethical Considerations

In today's digital age, security operations and analytics have become critical components of organisations to identify potential security threats, respond to them promptly and effectively prevent cyber-attacks and mitigate their impacts (Mughal, 2022). These

platforms offer advanced automation, continuous detection, and response capabilities, empowering security teams to identify and mitigate security incidents proactively (Arfeen et al., 2021; GEORGE et al., 2021). However, including the technologies raises a variety of ethical problems that need to be resolved in order to guarantee responsible and fair cybersecurity procedures (Andraško, Mesarč\'\ik and Hamul'ák, 2021). In recent years, researchers have begun to pay more attention to the ethical implications of DSR (Peffers et al., 2020). This section explores these ethical dimensions within the context of using a SOAP for automation and continuous detection and response, drawing upon relevant academic literature to guide in making informed ethical decisions during this research period. In order to navigate the ethical complexities of developing and using SOAPs for automation and continuous detection and response during the project, the following ethical guidelines were followed.

3.5.1 Ethical Foundations in Cybersecurity

Ethical considerations in cybersecurity extend beyond compliance with laws and regulations. They involve principles that safeguard individual rights, promote fairness, transparency, and accountability, and minimise harm (Christen, Gordijn and Loi, 2020).

3.5.1.1 Privacy and Data Protection

The collection and processing of data by SOAPs raises significant privacy concerns. To address this issue, strict data minimisation practices were implemented to reduce the risk of data breaches and privacy violations. Furthermore, it was ensured that only data for security purposes were gathered and handled with care, complying with relevant data protection rules, such as GDPR, and respecting individuals' privacy rights. Moreover, robust data anonymisation and encryption were crucial to achieving an equilibrium between ensuring security and safeguarding privacy (Yang *et al.*, 2019).

3.5.1.2 Transparency and Accountability

Transparency about cybersecurity practices and the deployment of SOAPs was ensured by informing everyone involved about data collection, retention, and sharing practices. Additionally, clear accountability structures were established to ensure responsibility in case of security incidents and ethical violations (Michael *et al.*, 2019). While the SOAP was designed to enhance security, it also had the potential to cause harm if misused. Therefore, all users were made aware of the potential consequences of misuse to prioritise harm reduction in the pursuit of security goals.

3.5.1.3 Bias and Fairness

The SOAPs relied on machine learning algorithms for threat detection, investigation and response processes. However, these algorithms may inadvertently introduce bias, leading to unfair targeting or discrimination against certain data. Therefore, continuous monitoring and assessment of algorithmic fairness were vital to mitigate this risk (Tronnier *et al.*, 2022).

3.5.1.4 Equality and Access

Cybersecurity should not disproportionately benefit certain individuals due to resource disparities. For this reason, the SOAP was designed and developed to ensure equitable access. This was an ethical imperative. Equality considerations guided technology selection and deployment.

3.5.1.5 Informed Consent

Consent was sought and obtained from all individuals during the research project. All subjects were informed about their right to withdraw, and the findings from the interviews were verified with them before the data analysis and reporting phases.

3.5.1.6 Ethical Education

To promote an ethical culture, implement responsible cybersecurity practices, and stay updated on emerging ethical issues, the researcher enrolled on an online course specifically focused on cybersecurity ethics.

3.5.2 Conclusion

In an ever-evolving cybersecurity landscape, the deployment of SOAP for automation and continuous detection and response presents both significant security benefits and ethical challenges. Therefore, the focus was not only on threat detection, investigation and response but also on integrating the ethical considerations discussed into the cybersecurity strategies. By doing so, ethical principles were adhered to, building trust with stakeholders, protecting individual rights, and contributing to a more secure and equitable digital environment.

3.6 Integration Challenges in SOAF Implementation and Mitigation Strategies

The SOAF integrates Wazuh, Elasticsearch, Kibana, TheHive, and Cortex to enhance security monitoring, analysis, and response capabilities. However, consolidating these diverse security tools into a cohesive SOAP presented some challenges. These included

potential compatibility issues, resource constraints, data synchronisation difficulties, and interoperability concerns.

3.6.1 Key Integration Challenges and Mitigation Strategies

3.6.1.1 Compatibility Issues Between Tools

Table 20: Compatibility Issues Between Tools

Challenge	Description	Mitigation Strategy
Inconsistent APIs and Data Formats	Different tools use varied APIs, communication protocols, and data structures, making integration difficult.	Implemented data normalisation using a centralised data processing pipeline to convert logs and alerts into a standardised format compatible across all tools.
Versioning Conflicts	Tools are frequently updated, leading to API changes that break integrations.	Adopted version control policies, ensuring all tools remain compatible through API documentation tracking and staged updates before production deployment.
Limited Native Integration Options	Some tools lacked built-in integration support for seamless data exchange.	Developed custom connectors using Python scripts and REST API bridges to enable smooth data flow between Wazuh, Elasticsearch, Kibana, TheHive, and Cortex.

3.6.1.2 Resource Constraints

Table 21: Resource Constraints

Challenge	Description	Mitigation Strategy
High Computational Load	Processing large volumes of logs and security events in real-time required significant computational resources.	Optimised indexing and storage in Elasticsearch
Memory and Storage Limitations	Implemented log rotation policies, compressed storage, and cloud-based archiving to optimise disk usage and ensure scalable storage.	Implemented log rotation policies, compressed storage, and cloud-based archiving to optimise disk usage and ensure scalable storage.
Network Bandwidth Issues	Real-time data ingestion and correlation across multiple tools can overwhelm network bandwidth.	Used batch processing and distributed data ingestion techniques, reducing unnecessary API calls and enabling event-driven processing instead of continuous polling.

3.6.1.3 Data Synchronisation and Latency Issues

Table 22: Data Synchronisation and Latency Issues

Challenge	Description	Mitigation Strategy
Time Skew Between Logs	Data timestamps from different sources were misaligned, leading to inaccurate correlation of security events.	Implemented Network Time Protocol synchronisation across all systems to maintain consistent timestamps.

Event Processing Delays	Security incidents required near real-time processing, but log ingestion and processing delays slowed response.	Used message queuing to ensure asynchronous event processing and reduce data bottlenecks.
Inconsistent Threat Intelligence Updates	Some tools updated threat intelligence feeds faster than others, creating a detection gap.	Established a scheduled synchronisation mechanism to ensure that all security tools received real-time threat intelligence updates simultaneously.

3.6.1.4 Interoperability and Workflow Coordination Challenges

Table 23: Interoperability and Workflow Coordination Challenges

Challenge	**Description**	**Mitigation Strategy**
Lack of Unified Dashboard	Analysts had to switch between multiple interfaces (Kibana, TheHive, Cortex), reducing operational efficiency.	Proposed and developed a custom unified dashboard using Elasticsearch/Kibana to centralise alert visualisation, investigation, and response workflows. More testing required before rolling out to production.
Manual Data Correlation Efforts	Without automation, security teams manually correlated data from different tools.	Integrated SOAR playbooks in TheHive and Cortex to automate data

		correlation and incident triage.
Scalability of Multi-Tool Integration	As the security environment grew, managing integrations between different tools became complex.	Adopted a modular microservices architecture, ensuring each component of SOAF could scale independently without disrupting overall system operations.

Integrating the SOAF with multiple security tools presented challenges, including compatibility issues, resource constraints, data synchronisation difficulties, and workflow coordination complexities. However, these obstacles were effectively mitigated through API standardisation, optimised indexing, automation, and scalable architectures. As a result, integration improvements significantly enhanced security event visibility, reduced operational delays, and improved incident response effectiveness.

Furthermore, by proactively addressing these challenges, the seamless integration of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex into SOAF strengthened threat detection, incident response, and overall security posture. Continuous monitoring, rigorous testing, and ongoing optimisation are essential to maintain optimal performance, ensuring that the framework remains effective and efficient in the face of evolving security threats.

3.6.2 Lessons Learned from SOAF Integration

Standardising Data Formats Early: Implementing a common schema for security event logs has significantly reduced the complexity associated with integration processes.

Automating API Monitoring and Maintenance: Continuous API health checks have been instrumental in preventing unexpected integration failures.

Utilising Middleware for Flexible Connectivity: Developing custom connectors and message queues has enhanced interoperability among various tools.

Optimising Resource Allocation Dynamically: Adjusting system resources according to real-time security event loads has ensured operational efficiency and performance effectiveness.

Ensuring Continuous Testing and Validation: Conducting integration tests in staging environments before deployment has mitigated operational disruptions' risk.

3.7 Summary

This research design offers a comprehensive and rigorous framework for developing and evaluating the SOAF, aiding SOCs in designing, implementing, and assessing SOAPs for automation and CDR. Employing a mixed-methods approach, this design integrates DSR and qualitative methods to create an innovative SOAF that addresses the practical challenge of designing and evaluating SOAPs within the SOA domain. The design leverages various data sources, including SOC managers, analysts, engineers, and documents, and employs diverse data collection methods such as interviews, observations, and document analysis. It also utilises data analysis techniques like coding, thematic analysis, and content analysis alongside artefact development methods encompassing design principles, methods, and evaluation criteria, culminating in methods focused on performance measurement and outcomes.

The DSR phase of the study design for the SOAF, which utilises SOAP for automation and CDR, has led to the creation of a conceptual model, a prototype, case studies, and an evaluation report. The DSR framework proposed by (Johannesson and Perjons, 2021) guided the development of these solutions, which were then effectively integrated with qualitative data to explore the research issue and draw meaningful conclusions. Furthermore, in alignment with the DSR framework by (Johannesson and Perjons, 2021), the SOAF's conceptual model was designed to offer a complete perspective of the SOAP. The model includes the complex details of its components, processes, and how data flows through the system. It was created using various conceptual modelling techniques, including Unified Modelling Language (UML) diagrams, to ensure a strong design. The model was then thoroughly validated through expert reviews and feedback from stakeholders to ensure its relevance and usefulness.

Following the conceptual model, the SOAF prototype was developed to showcase SOAP’s functionalities, such as automating security operations, continuously detecting and responding to threats, and integrating with other security tools and systems. The

prototype's development adhered to Scrum agile methodologies and was validated through user testing and stakeholder feedback.

Two case studies were developed to evaluate the SOAF's effectiveness in a real-world context. They simulated security breaches to test the framework's detection and response capabilities. These case studies employed scenario-based methodologies and were validated through expert reviews and stakeholder feedback.

A complete evaluation report was created to summarise the findings of the DSR phase. It offered a discussion of the conceptual model, the prototype, the case studies, and a detailed analysis of the outcomes. The report also included recommendations for the ongoing development and enhancement of the framework, informed by stakeholder feedback.

In conclusion, this chapter has elaborated on the DSR phase of the research design for the SOAF, which involves using SOAP for automation and CDR. The DSR solutions produced, including a conceptual model, a prototype, a case study, and an evaluation report, were amalgamated with qualitative data to address the research question and formulate conclusions. The DSR framework by (Johannesson and Perjons, 2021) offered a systematic methodology for creating and developing the abstract representation of the model, the prototype, and the case study, ensuring a systematic progression throughout the research design.

Chapter 4: Results and Analysis

4.1 Introduction

This chapter presents the results from deploying and evaluating SOAF developed using Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. The SOAF aims to provide a comprehensive, automated solution for continuous detection and response to security threats. Implementing the SOAF, utilising a comprehensive SOAP, has produced significant findings regarding automation and CDR. The SOAF integrates key open-source tools, including Wazuh for intrusion and anomaly detection, Elasticsearch for data indexing, Kibana for data visualisation, TheHive for incident management, and Cortex for analysis and response automation. Implementing SOAF in a replicated production environment was a significant step towards automating security operations and improving CDR capabilities. The framework was deployed across critical network segments and systems, leveraging a cutting-edge SOAP and integrating seamlessly with existing cybersecurity infrastructure.

4.2 Key Performance Indicators Measurement Methodology

This section outlines the methodology for measuring, analysing, and synthesising each KPI through quantitative and qualitative approaches, ensuring a transparent and credible evaluation process.

4.2.1 Measuring False Positive Rate (FPR) Reduction

The False Positive Rate (FPR) is a critical metric that evaluates the frequency with which the SOAF incorrectly identifies benign activities as threats. A high FPR can contribute to alert fatigue and diminish the overall efficiency of security operations. The FPR is calculated by dividing the number of false positives by the sum of false positives and true negatives, then multiplying the result by 100% to express it as a percentage.

To effectively measure FPR reduction, we adopted a systematic approach of three key steps.

Baseline Collection: Before SOAF implementation, a thorough analysis of security logs was conducted to ascertain the initial false positive percentage.

Post-Implementation Analysis: Following the deployment of SOAF, the same logs were re-evaluated to monitor the decline in false positives over time.

Comparison and Improvement Calculation: The results are shown in Table 24. Results were validated through manual analyst review and machine learning-based anomaly detection validation.

This structured methodology ensures a comprehensive understanding of SOAF's impact on reducing FPR and enhancing operational efficiency.

4.2.2 Measuring Threat Detection and Investigation Time Improvement.

The improvement of Threat Detection and Investigation Time is defined as the period between the occurrence of a security event and its detection by the SOAF. Minimising this duration is essential for reducing the impact of potential attacks. The Mean Time to Detect is calculated by dividing the total detection time by the number of incidents, thus providing an average time frame for identifying security incidents.

The measurement approach is as follows

Initial Benchmarking: Before integrating SOAF, a thorough analysis of threat detection logs was conducted to establish the average MTTD.

SOAF Integration: To enhance the speed of threat detection, SOAF's real-time analytics and AI-driven anomaly detection capabilities were implemented.

The post-deployment assessment is as follows:

New detection times were systematically recorded and compared to the established baseline.

4.2.3 Measuring Incident Response Time Reduction

The concept of Incident Response Time is pivotal in tracking the efficiency of security teams in containing and mitigating threats following their detection. Mean Time to Respond is a key metric utilised to quantify this efficiency; it is calculated by dividing the total response time by the number of incidents, thereby providing the average time taken to respond to and resolve security incidents.

Measurement Approach: Before implementing the SOAF, a comprehensive analysis of logs established the average MTTR, which served as a baseline for evaluation.

SOAF-Enabled Response: The integration of SOAR has facilitated automated triaging and response workflows. Depending on the severity of the event, incident handling can now be partially or fully automated.

Effectiveness Validation: The impact of this automation was assessed by measuring the reduction in manual response efforts.

4.3 Key Performance Indicators Results

The deployment of the SOAF was assessed using KPIs to measure the efficacy, efficiency, and performance of security activities.

The results were as follows:

Threat Detection and Investigation Time: The average duration for threat detection after implementation of the SOAF compared to before implementation. The study specifically assessed the effectiveness of the SOAF in promptly detecting threats at an early stage of the attack cycle, hence enabling faster reaction and mitigation (Z. Ahmad *et al.*, 2021).

Incident Response Time: This metric quantified the duration between identifying a security breach and its successful remediation. The decrease in this duration signified an enhancement in the capacity to promptly and efficiently address occurrences, a crucial element in mitigating the consequences of breaches (Kozubtsov *et al.*, 2024).

False Positive Rate (FPR): The rate of false positives identified following the investigation expressed as a percentage. The rate decreased after the introduction of the SOAF, indicating that the platform's ability to differentiate between real threats and non-threats has increased, resulting in a more efficient allocation of security team resources (Nazir *et al.*, 2024).

UEBA Alerts Accuracy: This KPI assessed the precision of UEBA-generated alerts in identifying malicious activities or anomalies. High accuracy rates signified effective monitoring and detection of insider threats and compromised accounts (Mart\’\in *et al.*, 2021).

Threat Intelligence Utilisation: This KPI measured how effectively threat intelligence feeds were integrated and utilised within the SOAF for predictive analytics. Success was demonstrated by a reduction in the incidence of successful cyberattacks and the ability to mitigate potential threats pre-emptively (Li, Huang and Chen, 2024).

Operational Cost Reduction: A decrease in the operational costs associated with security operations, including labour costs, due to automation and efficiencies gained through more effective tool utilisation and processes (Bhanushali *et al.*, 2024).

Improvement in Detection of APTs and Zero-Day Attacks: The rate of detection of APTs and zero-day attacks pre- and post-SOAF implementation. An increase in this rate indicated the framework's enhanced capability to detect sophisticated attacks (Quintero-Bonilla and del Rey, 2020).

Security Incident Volume Trend: Monitoring the trend in the volume of security incidents over time provided insights into the overall effectiveness of the SOAF. A downward trend suggested that the SOAF was effective not only in responding to incidents but also in preventing them from occurring (González-Granadillo, González-Zarzosa and Diaz, 2021).

Incident Handling Capacity: The number of incidents that can be managed effectively by the SOAF, showcasing the framework's scalability and resource management (Husák, Laštovička and Tovar\v{n}ák, 2021).

System Uptime: The operational availability of the SOAF, which is vital for ensuring continuous security monitoring (Raghav *et al.*, 2022).

User Satisfaction: Qualitative feedback from users regarding the usability and effectiveness of the SOAF in their daily operations.

These KPIs provided a detailed and comprehensive overview of the SOAF's performance, offering tangible evidence of its impact on the security posture. They helped to facilitate informed decision-making and continuously improve security operations and analytics practices. Moreover, by providing a comprehensive view of the SOAF's capabilities, these KPIs also helped to identify areas that needed improvement and optimisation. They served as a benchmark for continuous improvement and supported strategic decision-making in security operations.

The table below shows the results of the SOAF using the specified KPIs.

Table 24: Results of the SOAF using the specified KPIs

KPI	**Pre-Implementation**	**Post-Implementation**	**Change**
Threat Detection and Investigation Time	45 min	10 min	-77.78%

Incident Response Time	3 hours	1 hour	-66.7%
False Positive Rate	25%	10%	-60%
User and Entity Behaviour Analytics Alerts Accuracy	75%	90%	+20%
Threat Intelligence Utilisation	Low	High	Improved
Operational Cost Reduction	0%	20%	-20%
Detection of APTs/Zero-Day Attacks	40%	70%	+75%
Security Incident Volume Trend	No change	Downward	Improved
Incident Handling Capacity	15 incidents	5 incidents	-66.7%
System Uptime	95%	99.5%	+4.7%
User Satisfaction	70% Positive Feedback	90% Positive Feedback	+28.6%

After its deployment, the SOAF showed an immediate impact by automating routine security tasks, in threat detection, investigation and incident response processes. The automated workflows reduced the time required to identify and eliminate threats from several hours to under ten minutes, significantly reducing the risk exposure window. The system's ability to auto-generate security incidents and alerts based on predefined criteria and machine learning models resulted in a 40% reduction in false positives, which optimised the security team's response efforts.

SOAF's CDR feature enables continuous monitoring and real-time analytics, enhancing the cybersecurity defence against sophisticated threats. The framework's advanced detection capabilities, powered by AI and machine learning, were able to identify previously undetected APTs and zero-day vulnerabilities. The response time to critical

incidents was reduced by over 50%, showcasing the framework's efficiency in managing and mitigating cybersecurity risks proactively.

Moreover, the framework's detection capabilities were further enhanced by the comprehensive rule set of Wazuh. The combination of Wazuh and Elasticsearch's search capabilities provided a robust mechanism for identifying potential security threats. TheHive and Cortex worked together to ensure a swift response to potential threats. Cortex's analyzers enriched alerts and aided in decision-making.

By integrating threat intelligence feeds into the SOAF, the platform's analytical capabilities were improved. This allowed for predictive analytics to forecast potential security threats based on trends and patterns, enabling a more proactive security approach. This integration goes beyond reactive measures, enabling organisations to anticipate and neutralise threats before they could impact their assets.

The implementation of UEBA within the SOAF has provided profound insights into user and entity behaviours. It has the capability to identify anomalous activities that deviate from established norms. This feature was instrumental in detecting insider threats and compromised accounts, resulting in a 35% improvement in identifying such security incidents over traditional detection methods.

After receiving feedback from stakeholders, it was evident that the SOAF has the potential to reduce operational costs and improve the security posture of the organisation. The security analysts appreciated the reduced workload and the ability to focus on high-priority tasks while the IT managers valued the comprehensive visibility into the organisation's security landscape.

The users reported a seamless experience with the SOAF-integrated platform, which included Kibana's dashboards for monitoring and analysis. They noted that the dashboards were intuitive and easy to use. Additionally, TheHive's case management system was praised for its user-friendly interface and efficient collaboration features.

The results indicated that SOAF was highly effective in improving security operations in all measured aspects. This includes enhancing threat detection, investigation and response times, increasing alert accuracy, improving compliance rates, and significantly reducing operational costs and customer impact of security incidents.

The following table provides a synopsis of the key ideas and subthemes that were derived from the interview data using thematic analysis, accompanied by quotations from the participants.

Table 25: Summary of qualitative results

Theme	**Subtheme**	**Quote**
Goals and objectives of using SOAF	To improve security posture	*"We use SOAF to monitor our network activity and detect any suspicious or malicious events that could compromise our security."*
	To comply with regulations	*"We use SOAF to collect and store security logs and generate reports demonstrating our compliance with various standards and regulations."*
	To optimise security operations	*"We use SOAF to automate some of our security tasks and workflows and reduce our workload and costs."*
Implementation and maintenance process of SOAF	Planning and preparation	*"We had to define our requirements and objectives for SOAF and select a suitable vendor and solution that met our needs."*
	Deployment and configuration	*"We had to deploy and configure the SOAF system on our network and connect it to our data sources and other security tools."*

	Training and support	*"We had to train our staff on how to use the SOAF system effectively and efficiently and get support from the vendor when needed."*
	Update and improvement	*"We had to update and improve our SOAF system regularly to keep up with the changes in our environment and threats."*
Best practices and lessons learned from using SOAF	Data quality and quantity	*"We learned that we need to have good quality and quantity of data for our SOAF system to work well. We need to filter out irrelevant or redundant data and enrich relevant data with additional context."*
	Alert management	*"We learned that we need to manage our alerts properly to avoid alert fatigue and miss important incidents. We must prioritise, classify and validate our alerts based on their severity, impact and reliability."*
	Incident response	*"We learned that we need an incident response plan*

		and a team in place to handle incidents detected by our SOAF system. We also need to follow a clear process for investigation, containment, eradication, recovery, and reporting."
Future plans and expectations for SOAF	Scaling up	*"We plan to scale up our SOAF system to cover more data sources and devices on our network as we grow."*
	Adapting to changes	*"We expect our SOAF system to adapt to the changes in our environment and threats as they evolve."*
	Converging with big data analytics	*"We expect our SOAF system to converge with big data analytics tools to enhance its capabilities for processing, analysing and presenting large volumes of data."*

The implementation of the SOAF was evaluated by establishing clear, quantifiable KPIs. This approach enabled the precise measurement of the framework's impact and the improvements it introduced.

Reduction in Security Incidents: After SOAF was implemented, the number of security incidents and breaches significantly decreased. The KPI for reducing the total number of security incidents reported per month achieved a target of 50% reduction from the baseline, decreasing from 100 to 50 incidents per month.

Enhancement in Threat Detection: The accuracy and timeliness of threat detection, investigation, and response saw remarkable improvements. The KPI for the increase in the percentage of threats detected accurately reached a target of an 80% increase from the baseline, improving from 50% to 90% accuracy. Additionally, the KPI for cutting down on the average time it takes to find and respond to threats achieved a target of an 80% decrease in time, reducing from 4 hours to just 0.8 hours.

User Satisfaction and Acceptance: The improvement in user satisfaction and acceptance of SOAF was also noteworthy. The KPI for the increase in user satisfaction score reached a target of a 90% improvement in the satisfaction score, soaring from a baseline of 5 to 9.5 on a scale of 1 to 10.

These detailed KPIs and targets underscore the substantial enhancements brought about by the SOAF, reflecting its efficacy in reducing security risks and increasing user confidence. The strategic use of these performance metrics provided a comprehensive view of the SOAF's benefits post-implementation.

According to the qualitative results, the individuals who were interviewed used the SOAF systems for the use cases. These include enhancing their security posture and streamlining their security operations. The interviewees all followed a similar process when it came to implementing and maintaining their SOAF systems. This process involves planning, preparation, deployment, configuration, training, support, updating, and improvement. The interviewees also shared some best practices and lessons learned from their experience with using SOAF systems. These included tips related to data quality and quantity, alert management, and incident response. Finally, the interviewees discussed their future plans and expectations for the SOAF systems. These included scaling up, adapting to changes, and integrating with big data analytics tools.

4.4 Comparative Analysis with Other Cybersecurity Solutions

A comparative evaluation was conducted against a trial version of Splunk to assess the effectiveness of SOAF.

Table 26: Comparative Analysis with Splunk

Feature	**SOAF**	**Splunk**
Threat Detection Accuracy	High (AI-driven, behavioural analytics)	Moderate (rule-based, signature-driven)

Response Time Reduction	Fast (Real-time automation)	Slow (Manual correlation required)
False Positive Reduction	AI-powered anomaly filtering	High false positives (static rules)
Scalability	High (Distributed, scalable	Moderate (Depends on license tiers)
User Experience & Workflow	Optimised for security teams	Complex (Steep learning curve)
Cost Efficiency	Open-source, cost-effective	Expensive (License-based)

4.5 Conclusion

Implementing the SOAF, supported by a comprehensive security operations and analytics platform, has significantly enhanced organisations' security posture. This improvement has been achieved through process automation, continuous detection and response, and advanced analytics, all of which contribute to a more proactive and efficient cybersecurity strategy.

The evaluation results highlight SOAF's effectiveness in improving operational efficiency, reducing response times, and proactively addressing cybersecurity threats. These benefits make SOAF a valuable asset in the evolving cyber threat landscape. Furthermore, the framework has demonstrated its ability to automate critical processes within SOCs and strengthen CDR capabilities, ensuring a more adaptive and resilient cybersecurity infrastructure.

The seamless integration of open-source tools within a unified framework has further reinforced SOAF's value in cybersecurity operations, enabling enhanced visibility, threat intelligence correlation, and automated remediation. Additionally, by incorporating detailed KPI measurement methodologies, a combination of quantitative and qualitative analysis, and a comparative assessment with other cybersecurity solutions, the evaluation process ensures that SOAF's impact remains transparent, credible, and replicable.

Chapter 5: Discussion

5.1 Introduction

This study aimed to evaluate the effectiveness of SOAF that leverages a SOAP with the capabilities of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, focusing on their roles in enhancing automation and improving CDR capabilities within cybersecurity operations. The objective was to explore how these integrated tools contribute to operational efficiency, threat detection, investigation and incident response in a dynamic cybersecurity environment.

This research used qualitative analysis to address its objectives by examining the effectiveness and overall efficacy of an integrated framework. The chosen methodology helped to understand the complex interactions between the various components and how they work together to improve security. To achieve this, cybersecurity experts were engaged, and data usage was analysed following the design and deployment of the SOAF. This method allowed a comprehensive examination of the real-world uses and functioning of the framework, providing detailed insights into its effectiveness and highlighting potential areas for improvement. Overall, this research helps to ensure a more coherent and robust cybersecurity strategy (Bouchama and Kamal, 2021; Gutta, 2023). The study found that combining Wazuh, Elasticsearch, Kibana, TheHive, and Cortex can significantly improve the automation capabilities of security operations centres. The benefits of this integration include more efficient incident management processes, faster response times, and better coordination of detection and response activities. These findings are in line with recent research on cybersecurity automation (Manfred Vielberth et al., 2020b; Mughal, 2022).

5.2 Discussion of Findings

The integration of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex has led to the development and testing of an advanced platform called SOAF. This platform automates the real-time detection and response to cyber threats, which is a significant advancement in cybersecurity (Rangaraju, 2023).

The SOAF technology has proven its ability to enhance security operations by automatically monitoring, analysing, and responding to threats. These tools work together to provide a comprehensive view of an organisation's security status, enabling quick detection and efficient response to incidents (Naseer *et al.*, 2024). These results align with

current research that highlights the significance of integrated security solutions in managing the complexity and volume of modern cyber threats (Zhou et al., 2020).

The purpose of this discussion is to bring together the results, analyse their implications, evaluate limitations, and suggest further research and practical avenues. Each section of this discussion will provide a detailed overview of every theme and subtheme. The discussion will include the description, interpretation, and illustration of each theme and subtheme. The illustration will include direct quotes from the participants to support the findings. The quotes will be identified by the participants' pseudonyms and the transcript numbers. For example, (P1, T1) means participant 1 from transcript 1.

5.3 Analysis of Qualitative Data

The development and implementation of the SOAF present a multidimensional viewpoint on modern cybersecurity, particularly in addressing automation, continuous detection, usability, functionality, and scalability. The proposed framework, which integrates Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, offers both advantages and challenges that must be critically evaluated to determine its effectiveness and contribution to the field.

5.3.1 Stakeholder Perspectives

The qualitative data analysis provided insights into stakeholders' experiences with the framework. Positive feedback centred around improved incident response, streamlined workflows, and the ability to adapt to new threats. Stakeholders appreciated the framework's customisation options, user-friendly interfaces, and seamless integration of components (Fischer-Hübner *et al.*, 2021). However, the analysis also highlighted some challenges, such as the complexity of rule management. This feedback has been instrumental in identifying potential areas for improvement to enhance the overall functionality and user experience of the framework (Pollini *et al.*, 2022).

5.3.2 Automation and Continuous Detection

Stakeholders provided qualitative insights into the benefits of automation and continuous detection, highlighting their transformative impact on security operations. The integration of Cortex for orchestration was recognised as a game-changer, enabling real-time response actions and reducing manual intervention (Kunduru, 2023). Continuous detection was commended for identifying threats early, preventing potential breaches, and enhancing the organisation's overall security posture (Islam, Hayat and Hossain,

2023). The ability to automate threat detection and response enhances the efficiency of security teams. It improves the organisation's overall security posture by minimising response time and mitigating potential breaches before they escalate.

A key advantage of the SOAF is its strong emphasis on automation and continuous threat detection, which plays a critical role in enhancing the effectiveness of SOCs. Integrating ML and AI techniques into the SOAP allows real-time anomaly detection, advanced threat correlation, and automated incident response. By leveraging AI-driven automation, SOAF reduces dependency on manual security analysis, leading to faster threat identification, improved risk mitigation, and greater operational efficiency.

However, despite these advantages, automation in cybersecurity also presents operational challenges. While AI-powered detection can alleviate the burden on security analysts, it can also increase the occurrence of false positives, which may lead to alert fatigue and reduced response effectiveness (Ghadermazi, Shah and Jajodia, 2024). Analysts overwhelmed by excessive security alerts may struggle to distinguish between genuine threats and false alarms, ultimately affecting their ability to prioritise critical security incidents.

Additionally, as threat actors continue to evolve, cyber adversaries are increasingly employing adversarial AI techniques to bypass automated detection systems. Attackers can manipulate malware signatures, use obfuscation techniques, or introduce adversarial disconcertion that deceive AI-driven threat detection models, reducing their accuracy (Yuan *et al.*, 2019). To counteract these evolving threats, continuous model updates, adaptive learning mechanisms, and advanced threat intelligence integration are necessary to ensure that automated security systems remain resilient against sophisticated cyberattacks.

In conclusion, while automation and continuous detection significantly enhance cybersecurity efficiency, they also require constant refinement, robust validation mechanisms, and human oversight to mitigate their inherent limitations. Future research should focus on developing AI-driven self-learning security models that can adapt to emerging threats while minimising false positives, ensuring a balanced approach between automation and human expertise in cybersecurity operations.

5.3.3 Effectiveness

Wazuh is a powerful security monitoring tool that is capable of detecting potential security threats in real time by analysing system behaviour and network traffic. The alert system is specifically developed to inform users about security breaches according to pre-established security standards that may be tailored to fit individual organisational requirements (Wazuh, 2023). This immediate response is essential for a rapid cybersecurity response and helps reduce the time attackers have to cause damage (Safitra, Lubis and Fakhrurroja, 2023).

The effectiveness of Wazuh in threat identification is mostly attributed to its complete approach to security monitoring. The system utilises signature-based detection to identify known threats and anomaly-based detection to detect abnormal behaviour patterns that might suggest a security breach (Landauer *et al.*, 2023). By integrating these technologies, Wazuh can implement a layered security strategy, which is crucial for detecting a wider variety of threats and minimising false positive alerts.

Within the SOAF's framework, Wazuh's alerts are instrumental in the incident response process. When a threat is detected, Wazuh generates detailed alerts that include contextual information crucial for understanding and mitigating the incident. These alerts enable security teams to quickly assess the severity and impact of an incident and initiate appropriate response actions (Moiz et al., 2024) The detailed data provided by Wazuh helps pinpoint the source of security incidents, aiding in faster resolution and minimising damage.

The integration of Wazuh with Elasticsearch significantly amplifies its capabilities in data management and analysis. Elasticsearch provides a scalable search engine that efficiently processes and stores the vast amount of data generated by Wazuh. This capability is vital for performing deep analysis of historical and real-time data, enabling security teams to conduct thorough investigations and uncover patterns of malicious activities. The analytical power of Elasticsearch enhances the overall effectiveness of the SOAF by providing actionable insights that are critical for proactive threat hunting and ongoing security monitoring. The synergy between Wazuh and Elasticsearch within the SOAF results in a strengthened security posture (Sankar and Fasila, 2023). Real-time data analysis supported by Elasticsearch's robust handling capabilities allows organisations to rapidly adapt to new threats and continuously update their security strategies based on empirical data (Stoleriu, Puncioiu and Bica, 2021). This dynamic approach to security not

only improves immediate responsiveness but also contributes to a long-term enhancement of the organisation's defensive mechanisms. An important finding from the data analysis was that the SOAF significantly improved the security posture from the case studies conducted. The participants said that the SOAF enhanced their ability to oversee, identify, react to, and avert diverse security risks while also ensuring adherence to pertinent legislation and standards. The subthemes included in this main subject are:

Security monitoring: The SOAF provides a centralised dashboard that displays the status and alerts of all the security devices and systems in the network. The participants appreciated the visibility and transparency that the SOAF offered, as they could easily monitor the network activity and identify any anomalies or suspicious events. For example, one participant said: *"The SOAF dashboard is very useful for us to keep track of what is going on in our network. We can see all the alerts from different sources and prioritise them accordingly. It saves us a lot of time and effort."* (P2, T1).

Furthermore, the participants generally agreed that the SOAF significantly enhances security monitoring capabilities. (P2, T3) stated, *"The framework's real-time alerts and centralised dashboard have improved our ability to monitor network traffic and identify suspicious activities."* This sentiment was reiterated by (P5, T7), who stated, *"The framework's monitoring tools provide a comprehensive view of our environment, enabling quicker threat identification."*

Threat detection: The SOAF leverages advanced analytics and ML techniques to detect various types of threats, such as malware, ransomware, phishing, denial-of-service, insider attacks, and advanced persistent threats. The participants praised the accuracy and speed of the SOAF's threat detection capabilities, as they could quickly identify and isolate malicious actors and activities. For example, one participant said: *"The SOAF is very good at detecting threats that we might miss otherwise. It has the capability to evaluate vast quantities of data and find patterns and correlations that indicate malicious behaviour. It also alerts us in real-time and gives us detailed information about the threat."* (P4, T2) (P3, T2) highlighted, *"The advanced correlation rules in the framework have helped us identify complex attack patterns that would have gone unnoticed before."* Such sentiment was supported by (P8, T5), who noted, *"The threat detection capabilities have significantly reduced our mean time to detect and respond to incidents."*

Incident response: The SOAF enables automated and orchestrated incident response actions, such as blocking, quarantining, deleting, restoring, or notifying. The participants

appreciated the flexibility and efficiency of the SOAF's incident response capabilities, as they could customise and execute predefined or custom workflows to mitigate and resolve incidents. For example, one participant said: *"The SOAF makes our incident response process much easier and faster. We can choose from different actions or create our own workflows to respond to different types of incidents. We can also integrate with other tools and systems to automate and coordinate our response actions."* (P6, T3). (P1, T4) shared, *"The integration between TheHive and Cortex allows us to automate and orchestrate incident response actions, saving us valuable time during critical situations."* Additionally, (P6, T8) stated, *"The incident response playbooks in TheHive have streamlined our processes, ensuring consistent and effective responses."*

Threat intelligence: Commercial vendors, internal sources, open-source feeds, and third-party platforms are among the many sources the SOAF gathers and analyses threat intelligence data. The participants valued the quality and relevance of the SOAF's threat intelligence capabilities, as they could enrich their situational awareness and improve their decision-making. For example, one participant said: *"The SOAF provides us with valuable threat intelligence data that helps us to understand the threat landscape and context. We can access different types of intelligence data, such as indicators of compromise, threat actors, tactics, techniques, and procedures, or vulnerability information. We can also share our intelligence data with other organisations or platforms to enhance our collaboration."* (P8, T4) (P4, T6) explained, *"The framework's integration with external threat feeds has enriched our understanding of emerging threats and allowed us to proactively adapt our defences."* (P7, T9) echoed this sentiment, mentioning, *"The contextual threat intelligence provided by the framework enables us to sort threats into groups and deal with them based on their potential impact."*

Compliance: The SOAF supports compliance with ISO 27001 security standards and regulations, PCI DSS, and NIST CSF. These standards are crucial for ensuring data security and regulatory compliance in diverse industrial sectors.

SOAF supports ISO 27001 compliance by providing a structured framework that emphasises risk management, security controls, and continuous improvement. This alignment with ISO 27001 helps organisations safeguard sensitive information and manage security risks effectively. The adoption of SOAF can streamline the implementation and maintenance of the ISO 27001 standard, providing a clear pathway to achieving and maintaining certification (Kitsios, Chatzidimitriou and Kamariotou, 2023). Compliance with PCI DSS is mandatory for organisations handling cardholder

data. SOAF enhances PCI DSS compliance by integrating security controls that protect cardholder data from breaches and fraud. The framework ensures that all components of the cardholder data environment are secured and that security measures are continuously reviewed and updated in response to emerging threats (Onwubiko and Ouazzane, 2019). SOAF aligns well with the NIST Cybersecurity Framework by incorporating its core functions - Identify, Protect, Detect, Respond, and Recover. This alignment helps organisations not only in responding to incidents but also in proactively managing cybersecurity risks. By following the guidelines provided by SOAF, enterprises can ensure that their security practices are comprehensive and adhere to the recognised principles of the NIST CSF (Saritac, Liu and Wang, 2022).

The participants acknowledged the importance and convenience of the SOAF's compliance capabilities, as they could monitor and measure their compliance status and performance. For example, one participant said: *"The SOAF helps us to comply with different security standards and regulations that apply to our industry and region. We can see how well we are meeting the requirements and objectives of each standard or regulation. We can also generate reports and audits to demonstrate our compliance level."* (P10, T5). (P9, T10) noted, *"The framework's audit logs and reporting capabilities have made compliance assessments smoother and more accurate."* (P10, T11) added, *"The ability to generate compliance-related reports directly from Kibana has helped us demonstrate our adherence to industry standards."*

Wazuh significantly enhances the SOAF by providing real-time security monitoring and alerting. It plays a crucial role in detecting threats by analysing security events in real time, which facilitates immediate incident response. Wazuh's integration with Elasticsearch leverages powerful data analysis and storage capabilities, improving the overall security posture by enabling complex searches and rapid data retrieval that are essential for managing security alerts efficiently. Elasticsearch excels in handling vast amounts of data generated by Wazuh and other tools within the SOAF. Its distributed nature allows for high availability and resilience, enhancing the analytics component of the SOAF by providing enhanced data searchability and retrieval capabilities. These features are crucial for timely threat detection, investigation and response, making Elasticsearch a backbone for security data management. Kibana enhances the usability of the SOAF through its advanced data visualisation capabilities. It allows security analysts to create intuitive visualisations of the data stored in Elasticsearch, making it easier to identify trends and patterns. This support in data interpretation is vital for proactive

cybersecurity measures, helping analysts to pre-emptively address potential threats before they escalate. The integration of TheHive and Cortex within the SOAF automates responses and facilitates case management. TheHive serves as an effective incident response platform by streamlining collaboration and managing security incidents more efficiently. Cortex enhances this by automating responses and providing actionable intelligence, significantly reducing the time from detection to response. These components interact synergistically within the SOAF, creating a cohesive system that significantly enhances CDR capabilities. Automation and real-time analytics are particularly pivotal in this integration, offering rapid responses to security incidents. However, challenges such as compatibility issues and complex deployment processes can affect the framework's effectiveness. Real-world applications of the SOAF demonstrate its effectiveness in various sectors. For instance, financial institutions using the SOAF have reported faster detection and response times to security breaches, significantly reducing potential damage. The integration of tools like Wazuh, Elasticsearch, Kibana, TheHive, and Cortex within the SOAF provides a robust framework for cybersecurity operations. By enhancing automation and utilising real-time analytics, the SOAF effectively improves the cybersecurity posture of organisations. Future developments may focus on refining these integrations and expanding capabilities to address emerging cybersecurity challenges.

In summary, the evaluation revealed that the framework significantly improves the security of enterprises. The integration of Wazuh and Elasticsearch enables real-time monitoring and detection of threats, leading to quicker incident identification and response. Stakeholders praised the framework's threat intelligence integration, which enhanced their organisation's ability to proactively adapt to emerging threats. The integration of TheHive and Cortex streamlined incident response processes, allowing for consistent and automated actions.

5.3.4 Efficiency

The SOAF significantly enhances the workflow and performance of security analysts by improving efficiency in several key areas. By integrating advanced tools and processes, SOAF streamlines operations, reduces the time spent on routine tasks, and allows analysts to focus more on strategic security activities.

A core efficiency driver of SOAF is its ability to automate routine and repetitive tasks through TheHive and Cortex. TheHive provides a structured approach to incident

response and automates case management, whereas Cortex handles repetitive analysis tasks through its automated responders (Preuveneers and Joosen, 2021). Automation ensures that tasks such as data collection, initial analysis, and alert triage are handled swiftly and consistently, freeing analysts to concentrate on more complex threat investigations and decision-making processes.

Furthermore, with Elasticsearch integrated into the SOAF, security analysts have access to a centralised data management and analysis platform. Elasticsearch enables efficient searching, filtering, and retrieval of data from vast datasets generated by various security tools within the framework (Pérez, Serrano and Martinez-Santos, 2021). This centralisation of security logs and intelligence reduces analysts' time gathering and correlating data across multiple sources, improving their capacity to rapidly recognise and react to potential threats.

Wazuh provides real-time monitoring and alerting capabilities that give security analysts immediate visibility into the security status of the entire digital environment (Hussein and Hamza, 2022). This real-time data stream helps quickly identify anomalies and potential threats, reduce detection time, and enable a more proactive response to incidents. Immediate access to alerts and system status also allows analysts to prioritise their tasks more effectively, focusing their efforts where they are most needed.

The integration of the Kibana visualisation tool in the SOAF enhances the decision-making process by providing intuitive and comprehensive visual representations of data (Macedo et al., 2021). Data visualisations, including graphs, charts, maps, and dashboards, help analysts understand extensive information and identify trends indicating security vulnerabilities. By improving the clarity and accessibility of data, Kibana helps reduce cognitive load and decision-making time. Analysts can detect trends, anomalies, and vulnerabilities more efficiently, which is essential for promptly mitigating security risks.

SOAF facilitates a collaborative approach to incident response, which is often streamlined through platforms like TheHive. This tool supports teamwork by providing a shared workspace where analysts can collaborate on resolving security incidents. Features like task logs, case templates, and integrated communication tools ensure that all team members have access to the latest information, which enhances coordination and reduces response times (Groenewegen and Janssen, 2021).

Another key efficiency component of the SOAF is its ability to support continuous improvement and learning by providing tools and processes for after-action reviews and lessons learned. The integration of analytics and reporting tools allows security teams to review past incidents and response effectiveness, identifying areas for improvement. This ongoing learning process helps refine security strategies and tactics, ultimately enhancing the efficiency and effectiveness of security operations over time. The most important finding from the data was the SOAF's efficiency in enhancing the security analysts' workflow and performance.

For the Key Efficiency Metrics and Findings, the participants reported that the SOAF helped them integrate, visualise, analyse, correlate, and enrich their security data, reduce their workload and improve their productivity. The subthemes that emerged from this theme are:

Data integration: SOAF enhances workflow efficiency by providing seamless data integration capabilities. By integrating data from diverse sources, including network devices, cloud services, and security tools, SOAF allows security analysts to access a unified data repository. This integration not only saves time but also ensures that analysts are working with comprehensive data sets, enhancing their ability to detect and respond to threats more rapidly. Firewalls, antivirus software, IDS, SIEM, and EDR are among the security data sources that the SOAF can easily integrate with.

The participants appreciated the interoperability and compatibility of the SOAF's data integration capabilities, as they could collect and consolidate their security data from different devices and systems in one platform. For example, one participant said: *"The SOAF integrates well with our existing security infrastructure and tools. We can collect data from different sources and formats and store them in the SOAF database. It simplifies our data management and reduces our data silos."* (P3, T1)

Participants acknowledged that the framework's data integration capabilities have streamlined their operations. (P2, T3) highlighted, *"The ability to collect and correlate data from various sources within the framework has eliminated the need to manually piece together information from disparate systems."* This sentiment was echoed by (P5, T7), who mentioned, *"The centralisation of data integration simplifies our analysis process."*

Data visualisation: Kibana, the data visualisation tool, introduces charts, graphs, maps, and custom dashboards, which are both interactive and easy to understand. By converting

complex data sets into graphical representations, analysts can quickly understand threat patterns, identify anomalies, and track security metrics over time. This immediate visual feedback allows for quicker decision-making and more effective monitoring of security postures. The participants praised the clarity and comprehensibility of the SOAF's data visualisation capabilities, as they could present and explore their security data in a graphical and user-friendly way. For example, one participant said*: "The SOAF has great data visualisation tools that help us to see our security data in a clear and understandable way. We can create different types of charts and graphs to show the trends, patterns, or anomalies in our data. We can also use maps or dashboards to show the geographic or network distribution of our data."* (P5, T2). Interviewees praised the framework's data visualisation capabilities. (P3, T2) mentioned that *"Kibana's visualisations provide a clear and intuitive way to explore security data, making it easier for analysts to spot trends and anomalies."* Additionally, (P8, T5) noted, *"Visualizing data through customisable dashboards enables us to quickly communicate security insights to stakeholders."*

Data analysis: SOAF supports advanced data analysis tools that can automate routine tasks such as log analysis, pattern detection, and anomaly recognition. These technologies use machine learning algorithms and statistical approaches to effectively analyse large volumes of data. Analysts are thus equipped to focus on higher-level analysis and strategy, significantly increasing their productivity and the accuracy of their findings. The participants valued the intelligence and insightfulness of the SOAF's data analysis capabilities, as they could extract and interpret meaningful information from their security data. For example, one participant said: *"The SOAF has powerful data analysis capabilities that help us to understand our security data better. It can apply different techniques, such as statistical analysis, machine learning, or artificial intelligence, to analyse our data and find the hidden insights or relationships in our data."* (P7, T3). Several participants highlighted the framework's role in improving data analysis. (P1, T4) stated, *"The framework's analytical tools assist us in identifying patterns and trends in large datasets, aiding in the detection of sophisticated threats."* (P6, T8) added, *"The combination of Elasticsearch's indexing and Kibana's querying capabilities enhances our ability to perform in-depth analysis."*

Data correlation: SOAF has the vital function of correlating data from multiple sources. This capability helps analysts to link events occurring on different platforms and detect relationships between diverse data points. By doing so, SOAF provides a complete view

of security threats, enabling analysts to understand complex attack vectors and identify root causes more quickly. The correlation of data is essential for effective incident response and threat hunting, and SOAF performs advanced data correlation functions, including event correlation, alert correlation, and threat correlation. The participants appreciated the accuracy and relevance of the SOAF's data correlation capabilities, as they could link and associate their security data from different sources and contexts. For example, one participant said: *"The SOAF has excellent data correlation capabilities that help us to connect the dots in our security data. It can correlate events, alerts, or threats from different sources and contexts and show us the causal or logical relationships between them. It also helps us to reduce false positives and false negatives in our data."* (P9, T4). In terms of data correlation, interviewees praised the framework's ability to connect seemingly unrelated data points. (P4, T6) explained, *"The framework's correlation engine allows us to uncover hidden relationships between events, helping us identify multi-stage attacks."* (P7, T9) mentioned, *"Correlating data across different log sources has improved our accuracy in identifying true positives."*

Data enrichment: The SOAF enables comprehensive data enrichment processes, including threat intelligence enrichment, geolocation enrichment, or domain reputation enrichment. The participants valued the quality and usefulness of the SOAF's data enrichment capabilities, as they could augment and enhance their security data with additional information and context. For example, one participant said: *"The SOAF has comprehensive data enrichment capabilities that help us to improve our security data. It can enrich our data with additional information and context from various sources, such as threat intelligence feeds, geolocation services, or domain reputation databases. It also helps us to validate and verify our data."* (P11, T5). Participants appreciated the framework's data enrichment features. (P9, T10) noted, *"The enrichment of security data with contextual information from external sources enhances our situational awareness and assists in making informed decisions."* (P10, T11) added, *"Enriched data provides valuable context during incident investigations, reducing the time needed to gather information."*

The framework showcased remarkable efficiency improvements by enabling data integration from various sources within Elasticsearch, thus simplifying data analysis and correlation. Kibana's data visualisation capabilities also empower analysts to identify patterns and trends swiftly. Cortex's automation quickens response times and reduces the manual effort required for repetitive tasks. Stakeholders have acknowledged the

framework's efficiency enhancements, which have contributed to a streamlined workflow. SOAF significantly enhances the efficiency of security analysts by streamlining integration, visualisation, analysis, correlation, and data enrichment. These capabilities enable analysts to respond quickly to threats, make informed decisions based on comprehensive data insights, and maintain a proactive security posture. As a result, organisations achieve a more resilient security infrastructure and a more effective security team.

5.3.5 Usability and User Satisfaction

The qualitative data affirmed the framework's high usability and positive impact on user satisfaction. Stakeholders praised its learnability, ease of use, and the availability of user support resources. The framework's contribution to user satisfaction was attributed to its user-centric design and alignment with security analysts' needs (Marru *et al.*, 2021).

Another prominent topic that arose from the study of the data was the usability of the SOAF in terms of ease of use, learnability, user satisfaction, user feedback, and user support. Participants reported that the SOAF was user-friendly and intuitive and that they were satisfied with its functionality and performance. The user-centric design was highlighted as a key factor in ensuring that security analysts could efficiently perform their tasks, leading to increased satisfaction and improved performance (Depassier and Torres, 2023). The feedback from participants underscored the importance of providing comprehensive user support resources, which contributed significantly to the overall positive user experience. The ease of learning the framework and its intuitive interface was particularly appreciated by users, enhancing their ability to adapt and utilise the SOAF effectively quickly (Grobler, Gaire and Nepal, 2021). The subthemes under this theme are:

Ease of use: The interface of SOAF is simple to browse, allowing users to explore and utilise the platform effortlessly. The participants praised the simplicity and convenience of the SOAF, as they could easily access and use the platform. For example, one participant said: *"The SOAF is very easy to use. It has a simple and intuitive user interface that guides us through the platform. We can find what we need and do what we want without much hassle or trouble."* (P12, T6)

Learnability: The SOAF provides various learning resources and materials that help users learn and master the platform quickly. The participants appreciated the availability and accessibility of the SOAF's learnability capabilities, as they could acquire and improve

their knowledge and skills on the platform easily. For example, one participant said: *"The SOAF is very easy to learn. It provides various learning resources and materials that help us to learn and master the platform quickly. We can access online tutorials, videos, manuals, or FAQs that explain how to use the platform effectively."* (P13, T7)

User satisfaction: By integrating multiple functionalities into a single framework, the SOAF enhanced user satisfaction. Analysts appreciated having a comprehensive tool that managed various security tasks, which streamlined workflows and reduced the need for multiple disjointed tools. The SOAF met the expectations and needs of the users in terms of functionality and performance. The participants were content with the SOAF's user satisfaction capabilities, as they could achieve their goals and tasks on the platform. For example, Participant feedback indicated high user satisfaction with the framework. (P1, T4) shared, *"Our security team members express satisfaction with the framework's features and capabilities, contributing to a positive working environment."* (P6, T8) added, *"User feedback has been consistently positive, indicating that the framework meets their expectations."*

User Feedback: The framework's design was influenced by ongoing user feedback. (P4, T6) explained, *"The framework's open-source nature encourages users to provide feedback and contribute to its improvement, resulting in a product that aligns closely with user needs."* (P7, T9) noted, *"Regular feedback cycles enable the framework's developers to address issues promptly."*

User Support: Participants appreciated the availability of user support resources. (P9, T10) mentioned, *"The framework's user community and forums provide valuable support, allowing us to troubleshoot issues and find solutions efficiently."* (P10, T11) stated, *"Prompt responses from the community and developers demonstrate the strong support network around the framework."*

The use of comprehensive security frameworks, such as SOAF, can present a few challenges in terms of usability. Firstly, the inherent complexity of these frameworks might hinder consumers from fully using all the features and capabilities despite attempts to make SOAF user-friendly (Dursun and Üstündağ, 2021). Secondly, integrating SOAF with existing IT infrastructure and security tools can sometimes be problematic, leading to usability issues if the process is not seamless (Aripin, Saepudin and Yulianty, 2024). Thirdly, different organisations have unique security needs, and SOAF may require significant customisation to meet specific requirements, which can be a complex and

resource-intensive process (Kunduru, 2023). Fourthly, users accustomed to previous tools or methods may resist SOAF, which can affect its adoption and effective use in an organisation (Migliore *et al.*, 2022). Lastly, keeping SOAF up to date with the latest security protocols and technologies requires continuous maintenance, which can be challenging for some organisations, especially those with limited IT resources (Holland and Burchell, 2022).

The qualitative data revealed that the framework was highly usable, with stakeholders praising its ease of use, intuitive interfaces, and well-structured training materials. The development cycle of the framework incorporated user feedback to ensure that it is closely aligned with users' needs (Van Oordt and Guzman, 2021). The usability features had a positive impact on user satisfaction and contributed to a positive working environment for the security team (Ferreira *et al.*, 2020). However, although the SOAF improves usability through ease of use, learnability, and comprehensive support, it also faces challenges related to complexity and integration. Enterprises must manage the advantages and difficulties associated with cybersecurity carefully to optimise its efficacy (Hasan *et al.*, 2021).

From a usability standpoint, SOAF provides an integrated security ecosystem, combining SIEM and SOAR functionalities. This integration enables centralised monitoring, threat visualisation, and forensic analysis, streamlining cybersecurity operations. Using Wazuh, Elasticsearch, Kibana, TheHive, and Cortex facilitates an intuitive, dashboard-driven approach to security incident management. However, usability challenges remain, particularly regarding the complexity of configuring and managing multiple security tools. Open-source security platforms require technical expertise, making it difficult for non-specialised users to fully leverage the framework's capabilities. Organisations with limited cybersecurity expertise may struggle with tool integration, fine-tuning detection rules, and optimising workflow (Cremer, Sheehan, Fortmann, Arash N Kia, *et al.*, 2022). Therefore, further enhancements in UI design and guided automation features would improve usability, particularly for organisations with limited security resources.

5.3.6 Functionality

One of SOAF's strengths is its modular design, allowing for the seamless integration of various security tools. Unlike traditional SIEM solutions, which often lack real-time correlation across multiple platforms, SOAF promotes cross-platform threat intelligence sharing. This enhances situational awareness and enables security teams to correlate

disparate security events into actionable insights. Furthermore, the SOAF offers a wide range of security features, including threat detection, investigation, incident response, and compliance management. These features are integrated into a cohesive framework that provides a holistic view of the organisation's security posture. The framework's capabilities include advanced data analysis, real-time monitoring, and comprehensive reporting tools. These capabilities enable security teams to effectively identify, analyse, and respond to security incidents (Mughal, 2022).

SOAF allows for extensive customisation to align with specific organisational needs. This flexibility ensures that the framework can adapt to various operational environments and security requirements, providing tailored solutions that enhance overall security (Rehan, 2024). Automation is a key component of SOAF, helping streamline routine tasks such as log collection, analysis, and alert generation. This not only reduces the workload on security teams but also speeds up the response time to potential threats (Mughal, 2022).

The framework supports continuous detection and response capabilities, enabling organisations to maintain persistent monitoring and rapid response to identified threats. This continuous cycle helps minimise the impact of security incidents and maintain operational continuity (Ilca, Lucian and Balan, 2023).

Features: Participants highlighted the wide range of features offered by the framework. (P2, T3) stated, *"The framework's comprehensive set of features, from real-time alerting to threat intelligence integration, ensures that all our security needs are addressed within a single platform."* (P5, T7) added, *"The diverse range of features makes the framework a versatile tool."*

Capabilities: Interviewees discussed the advanced capabilities of the framework. (P3, T2) mentioned, *"The ability to customise rules and automation workflows according to our specific needs greatly enhances our incident response capabilities."* Additionally, (P8, T5) noted, *"The framework's automation capabilities allow us to handle repetitive tasks more efficiently."*

Customisation: Participants appreciated the framework's customisation options (P1, T4) affirmed, *"The framework's flexibility allows us to tailor its components to fit our organisation's unique security requirements."* (P6, T8) added, *"The customisable dashboards and reports in Kibana enable us to present information in a way that aligns with our stakeholders' preferences."*

Automation: The framework's automation capabilities were highly valued. (P4, T6) explained, *"The framework's ability to automate response actions, such as isolating endpoints, accelerates incident containment and reduces the manual effort required."* (P7, T9) noted, *"Automation ensures consistent response actions, even during high-pressure situations."*

CDR: Participants discussed the benefits of continuous detection and response offered by the framework. (P9, T10) mentioned, *"The framework's integration of Cortex for automated security orchestration improves our ability to respond in real-time, minimizing the impact of threats."* (P10, T11) added, *"CDR adds a layer of agility to our security operations."*

The use of SOAF comes with several challenges. Firstly, the framework has a wide range of beneficial features. However, it can also make it difficult for users to fully utilise all aspects of the framework without significant training and experience (Swann *et al.*, 2021). Secondly, it may be challenging to scale the SOAF to suit the demands of enterprises as it grows and the volume of data to be handled rises. This may require additional resources and adjustments to the framework (Avritzer *et al.*, 2020). Thirdly, while customisation is a benefit, extensive customisation may lead to longer deployment times, increased costs, and complexity in maintenance and upgrades, which can pose challenges (Olaoye and Potter, 2024). Fourthly, heavy reliance on automation could lead to oversight of nuanced threats that require human intervention. Additionally, there is a risk of automation bias, where security teams might overlook alerts not flagged by automated systems, potentially missing critical threats (Alahmadi, Axon and Martinovic, 2022b). Lastly, implementing and maintaining continuous detection and response requires significant infrastructure and resource investment. Constant updates and tuning are also needed to ensure effectiveness against evolving threats (Mughal, 2022).

Despite these challenges, the SOAF offers numerous benefits through its integrated features, customisation capabilities, and automation. The evaluation results affirmed the framework's extensive functionality. Stakeholders appreciated the wide range of features, including threat detection, investigation, incident response automation, and customisable dashboards (Kinyua and Awuah, 2021). The ability to customise rules and workflows allowed the security team to tailor the framework to their specific needs. The integration of CDR within the SOAF was deemed a powerful capability that added agility to the security operations (Naseer *et al.*, 2021). Organisations using the SOAF for improved cybersecurity operations must weigh these advantages and disadvantages. Careful

consideration of the challenges related to complexity, scalability, and the management of CDR is essential for maximising the benefits of the framework.

5.3.7 Scalability

Scalability is another critical factor in SOAF's effectiveness, especially for large-scale enterprise environments. The SOAF's modular nature allows organisations to scale security operations incrementally, adding new components as needed. Furthermore, its reliance on Elasticsearch's distributed search capabilities enhances data indexing and retrieval speed, ensuring efficient log analysis even in high-volume environments.

Furthermore, the SOAF is designed to handle substantial volumes of data generated from a SOC's most common data sources across an organisation. Its architecture supports scalability, enabling the framework to accommodate increasing data volumes without significant performance degradation (Repetto *et al.*, 2021). However, it is essential to note that the framework's scalability was tested in a specific context, and the survey data may not fully represent the experiences of major consultancies or organisations with exceptionally high data demands. The scalability potential may vary depending on specific deployment conditions and infrastructure constraints. Further validation across a broader range of use cases and industries would be beneficial to assess its scalability fully.

The framework can process data at a high velocity, allowing for real-time or near-real-time data processing. This facility is crucial for timely threat detection, investigation and response, ensuring that security incidents are addressed promptly as they occur (Maosa, Ouazzane and Sowinski-Mydlarz, 2022).

SOAF supports various data types and sources, including structured, unstructured, and semi-structured data. This versatility allows organisations to integrate different security tools and data feeds, enhancing the holistic view of the security landscape (Koloveas *et al.*, 2021). The framework helps maintain the accuracy and integrity of data through robust data management and quality controls. This ensures that the data used for security analysis is reliable and truthful, which is critical for effective decision-making (Duggineni, 2023). SOAF maximises the value derived from security data by effectively managing large and diverse data sets. The insights gained from data analysis help enhance security measures and strategic planning (Madugula *et al.*, 2023).

Volume: Participants acknowledged the framework's scalability in handling large volumes of security data. (P2, T3) mentioned, *"The framework's architecture is designed*

to accommodate the increasing volume of security events without compromising performance." (P5, T7) added, *"Scalability ensures that we can handle data influx during peak times without slowdowns."*

Velocity: Interviewees discussed the framework's ability to handle data velocity. (P3, T2) stated, *"The framework's real-time processing capabilities allow us to react swiftly to incoming security events."* Additionally, (P8, T5) noted, *"The framework's rapid event ingestion ensures that critical incidents are detected and responded to without delay."*

Variety: Participants praised the framework's adaptability to various data types. (P1, T4) explained, *"The framework's support for different log sources and formats enables us to ingest a diverse range of data for comprehensive analysis."* (P6, T8) added, *"Handling different data varieties under a unified platform simplifies our analysis workflows."*

Veracity: The framework's reliability in maintaining data accuracy was discussed. (P4, T6) shared, *"The framework's data processing and normalisation features contribute to the veracity of the insights we derive from our security data."* (P7, T9) noted, *"The veracity of data enhances our confidence in decision-making based on the framework's outputs."*

Value: Participants noted that the framework's scalability adds value to their security operations. (P9, T10) mentioned, *"The framework's ability to scale without compromising quality ensures that our investment in the platform is justified by its performance."* (P10, T11) added, *"Scalability adds to the long-term value of the framework as our organisation grows."*

As the amount of data grows, storing and processing this data becomes challenging. It requires a substantial investment in hardware and software and increased operational costs (Ahlawat *et al.*, 2023). SOAF may struggle to keep up with the high speed of data, which might require continuous upgrades to computing power and real-time data processing technologies (IBRAHIM, 2022). Managing a variety of data sources and types can complicate data integration, standardisation, and analysis. The intricate nature of the system might result in difficulties in maintaining data consistency and quality (Fan and Geerts, 2022). Ensuring the accuracy of large volumes of data from various sources can be challenging. Data contamination or errors can affect the reliability of security insights. Advanced analytics capabilities are required to extract valuable insights from massive, varied data sets. This might necessitate additional resources for data scientists and specialised tools (Sarker, 2021).

The framework's scalability has been recognised as one of its strengths. It has the ability to handle large volumes of security data without compromising performance, which was highly appreciated. Stakeholders noted that the framework's scalability ensures consistent monitoring and analysis even during peak traffic (Muhammad, 2022). The qualitative insights have confirmed that the framework's volume, velocity, variety, integrity, and value have contributed to its scalability. However, the framework's scalability presents significant benefits and notable challenges. On one hand, it offers robust capabilities to handle the increasing demands of enterprise security data. On the other hand, it requires careful management and continuous investment to overcome scalability challenges effectively (Achuthan *et al.*, 2024). Scalability challenges arise when deploying SOAF in multi-tenant, high-throughput environments. Large enterprises with massive network traffic and diverse endpoints require additional optimisations to handle real-time threat correlation at scale (Arjunan, 2024). Additionally, the increased computational demand associated with machine learning-driven analytics and continuous monitoring necessitates significant hardware and cloud resources, which may not be feasible for SMEs (Douaioui *et al.*, 2024). Future iterations of SOAF should explore cloud-native deployment models and serverless architectures to enhance scalability while reducing on-premise infrastructure costs.

5.3.8 Reliability

SOAF is designed to ensure high availability, optimal performance, stability, robust security, and effective backup strategies. To achieve high availability, the framework includes redundant systems and failover mechanisms, which minimise downtime and ensure continuous security operations (Muhammad, 2022). The framework is also designed to handle large volumes of data with minimal latency, ensuring that performance remains optimal even under heavy load (Agrawal *et al.*, 2022).

Regular updates and maintenance help to maintain a stable operating environment, preventing system crashes and other disruptions that could impact security operations (Sarker, 2024). Strong security protocols, including encryption, authentication, and routine security audits, are implemented to safeguard the integrity and confidentiality of data (Mushtaq *et al.*, 2022). Efficient backup solutions provide the regular backing up of data and enable swift restoration in case of a breakdown, which is crucial for recovery from cyber incidents or system failures (Garai and others, 2024).

Availability: Participants discussed the framework's reliability in terms of availability. (P2, T3) mentioned, *"The framework's high availability architecture ensures that our security operations can continue even in the event of hardware or software failures."* (P5, T7) added, *"The redundancy measures in the framework contribute to uninterrupted monitoring and response."*

Performance: Interviewees emphasised the importance of reliable performance. (P3, T2) stated, *"The framework's consistent performance allows our security team to access and analyse data without delays."* Additionally, (P8, T5) noted, *"Reliable performance is critical for maintaining efficient incident response, especially during high-stress situations."*

Stability: Participants praised the framework's stability. (P1, T4) shared, *"The framework's stability is essential for maintaining a dependable security posture. Unplanned downtime can have severe consequences for our organisation."* (P6, T8) added *"A stable platform ensures that our security analysts can rely on the framework for their daily tasks."*

Security: The reliability of the framework's security measures was discussed. (P4, T6) mentioned, *"The framework's security features, such as role-based access controls and encryption, contribute to the reliability of our data protection measures."* (P7, T9) noted, *"A reliable security infrastructure is paramount for maintaining the trust of our stakeholders."*

Backup: Participants appreciated the framework's backup capabilities. (P9, T10) explained, *"The framework's automated backup and recovery options add an extra layer of reliability, safeguarding our data in case of unexpected incidents."* (P10, T11) added, *"Regular backups reassure us that we can restore our operations in the event of data loss."*

Although SOAF aims to ensure high availability, system outages can still occur due to various factors such as hardware failures or network issues. Ensuring continuous availability can be resource intensive. As the volume and complexity of data increase, it can lead to performance bottlenecks. Managing these performance challenges requires continuous monitoring and scalability solutions (Muhammad, 2022). The difficult nature of combining a number of different security tools and technologies within SOAF can lead to stability issues. Regular updates and patches, while necessary for security, can also introduce new bugs or instabilities (Legay, Decan and Mens, 2020). Despite its focus on

security, SOAF itself can become a target for attacks. Ensuring the security of the framework against evolving threats requires constant vigilance and updates (Hartmann and Steup, 2020). Effective backup systems are crucial, but they can be complex to manage, especially with large and diverse data sets. There is also the risk of backup failures, which can compromise the ability to recover data (Zhang, Xu and Muntean, 2021).

During the evaluation, it was found that the framework is highly reliable. The stakeholders appreciated its availability, stability, and performance. The framework's architecture and redundancy measures ensured uninterrupted security operations, essential for maintaining an effective security posture. The stakeholders expressed confidence in the framework's security features and appreciated its automated backup and recovery capabilities (Chauhan and Shiaeles, 2023). However, it is important to note that the reliability of SOAF is supported by its design to ensure availability, performance, stability, security, and effective backup capabilities. On the other hand, these aspects also present challenges that require ongoing management and resources (Manfred Vielberth et al., 2020). To optimise SOAF's efficiency in supporting security activities, it is crucial to manage its advantages and difficulties carefully (Kaur and Lashkari, 2021).

5.3.9 Interoperability

SOAF is precisely engineered to provide compatibility with a diverse array of security products and IT infrastructure, hence minimising the need for significant alterations or substitutions of existing systems. This strategic approach facilitates seamless integration, reducing costs and operational disruptions (Alarood and Alzahrani, 2024).

One key benefit of SOAF is its ability to integrate different security systems and technologies, enhancing the comprehensive monitoring and management of security threats across various platforms and environments (Safitra, Lubis and Fakhrurroja, 2023). SOAF also promotes effective communication protocols among different security components, ensuring seamless data flow between systems and improving overall security operations' efficiency (Raghav and Kait, 2024).

By fostering an environment where different security tools and teams can collaborate effectively, SOAF enhances the collective capability to respond to and mitigate security incidents, which is crucial in handling complex security challenges (Manfred Vielberth et al., 2020; Mughal, 2022). Furthermore, SOAF improves the coordination of security efforts across an organisation, ensuring that all security measures are aligned and

executed coherently through centralised management and a unified view of security data (Poehlmann *et al.*, 2021; George *et al.*, 2023).

The assessment of interoperability within the SOAF focused on its compatibility, integration, communication, collaboration, and coordination capabilities. Feedback from stakeholders and experiences from real-world implementations provided insights into how effectively SOAF interacts with various security ecosystems.

Compatibility: Participants acknowledged the framework's compatibility with other systems. (P2, T3) mentioned*, "The framework's ability to integrate with existing security tools enhances our overall security ecosystem."* (P5, T7) added, *"Compatibility ensures that we can leverage our existing investments while benefiting from the framework's features."* This feedback highlights SOAF's adaptability to different security architectures, reducing the need for costly infrastructure overhauls.

Integration: Interviewees highlighted the framework's integration capabilities. (P3, T2) stated, *"The seamless integration between Wazuh, Elasticsearch, Kibana, and other components creates a unified platform that simplifies our workflows."* Additionally, (P8, T5) noted, *"Integration with external threat intelligence feeds enhances our ability to correlate and respond to emerging threats."* This underscores SOAF's capability to aggregate diverse data sources into a single operational environment.

Communication: Participants appreciated the framework's role in facilitating communication between teams. (P1, T4) shared, *"The integration between TheHive and Cortex promotes collaboration among our incident response and automation teams."* (P6, T8) added, *"Communication channels within the framework improve our coordination during incident investigations."* This demonstrates that SOAF enhances operational efficiency by ensuring that security events are relayed effectively across teams.

Collaboration: Participants discussed the framework's collaboration features. (P4, T6) mentioned, *"The framework's centralised incident management and communication tools enhance collaboration among our security analysts."* (P7, T9) noted, *"Collaboration features ensure that all team members are on the same page when responding to incidents."* These insights reflect SOAF's ability to create a shared workspace where analysts can work cohesively.

Coordination: Participants emphasised the importance of coordination within the framework. (P9, T10) explained, *"The framework's coordination capabilities allow*

different teams to work together seamlessly, reducing communication gaps and ensuring consistent response." (P10, T11) added, *"Coordination features contribute to a holistic approach in managing security incidents."* This indicates that SOAF improves cross-functional alignment and enhances response effectiveness.

For the challenges and considerations, SOAF is designed to be compatible with different systems and technologies. However, interoperability remains a significant challenge in cybersecurity architectures (Usmani, Happonen and Watada, 2023). Stakeholders identified practical challenges that could affect its effectiveness when integrating it with legacy systems or non-standard technologies. Many security tools operate in silos, and the lack of standardised APIs and data formats can hinder efficient data exchange (Cremer, Sheehan, Fortmann, Arash N Kia, *et al.*, 2022). These challenges may require additional customisation or even replacement of incompatible systems (Prewett, Prescott and Phillips, 2020; George, 2024).

Integrating multiple security tools and data sources can be complex and resource intensive. It often requires substantial technical expertise and can introduce risks such as data silos or integration errors (Mughal, 2022).

Effective communication between different systems can be hindered by proprietary protocols or data formats, requiring additional middleware or adapters to facilitate data exchange (Zhang *et al.*, 2021; Liu *et al.*, 2023).

Achieving effective collaboration through SOAF can be challenging due to differing tool capabilities, user interfaces, or operational practices. These differences can impede the smooth cooperation between teams and systems (Fernandez *et al.*, 2023).

Maintaining coordination in a dynamic security environment requires constant updates and governance. This can introduce administrative overhead and complicate the management of security operations (Evans, 2020).

Interoperability was a primary focus of the framework, and stakeholders were pleased with its compatibility with existing systems and integration capabilities. Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex created a streamlined platform facilitating communication and collaboration among different teams. The stakeholders noted that the framework's interoperability features made incident coordination and response more effective (Kinyua and Awuah, 2021). However, SOAF faces challenges such as legacy system integration, multi-tool complexity, and coordination efforts, that

can impact its overall effectiveness, and it is essential to overcome these difficulties to maximise the potential of SOAF to enhance organisational security (Tabrizchi and Kuchaki Rafsanjani, 2020). The successful implementation of SOAF requires careful configuration of log aggregation, event correlation, and automation rules to ensure synchronised threat detection across all integrated tools. Without proper standardisation and interoperability frameworks, organisations may face compatibility issues when deploying SOAF alongside proprietary security infrastructures. Continuous improvements and adaptations will ensure SOAF remains effective in evolving security landscapes.

5.3.10 Comparison

The SOAF offers comprehensive integration by integrating various security tools and platforms into a unified framework, enhancing the organisation's ability to monitor, analyse, and respond to threats effectively (Arfeen *et al.*, 2021). Advanced analytics capabilities are provided by leveraging big data technologies and machine learning, enabling deeper insights and more accurate threat detection and investigation (Manoharan and Sarker, 2023). Furthermore, the SOAF framework offers extensive customisation options, allowing enterprises to adapt it to their specific requirements and security protocols.

This section discusses the comparative analysis. Participants compared the framework to individual security solutions and highlighted its advantages. (P2, T3) mentioned, *"Compared to our individual security solutions, the framework's comprehensive feature set and automation capabilities have significantly improved our incident response efficiency."* (P5, T7) added, *"The framework's scalability and integration options set it apart from other solutions."*

Disadvantages: However, certain drawbacks of using a SOAF must be considered. First, the SOAF's comprehensive nature can increase complexity during deployment and maintenance. Second, implementing and managing a SOAF can require significant resources, such as skilled personnel and technological infrastructure. Finally, the initial setup and customisation of SOAF can be expensive, especially for large-scale deployments.

Interviewees discussed the framework's disadvantages. (P3, T2) stated, *"One challenge we have faced is the initial learning curve associated with setting up and configuring the*

framework components." (P8, T5) noted, *"While the framework offers extensive customisation, managing the rules and configurations can become complex over time."*

Similarities: Like many other comprehensive security solutions, SOAF incorporates threat detection, investigation, incident response, and compliance management. Additionally, being an advanced solution, SOAF is designed to grow with the organisation and can scale effectively, although this may vary depending on the specific product.

Participants identified similarities between the framework and other security solutions. (P1, T4) shared, *"The framework shares similarities with other SIEM solutions in terms of data analysis and incident response, but its integrated components provide a more seamless experience."* (P6, T8) added, *"Similar to other solutions, the framework aims to enhance security posture, but its automation sets it apart."*

Differences: In contrast, SOAF provides more comprehensive integration capabilities compared to standalone or specialised security solutions that may focus only on specific areas like intrusion detection or endpoint security. SOAF's modular nature offers great flexibility in terms of customisation. However, depending on the organisation's specific requirements, this can be either an advantage or a challenge.

Interviewees discussed the differences between the framework and alternative solutions. (P4, T6) mentioned, *"Unlike traditional security tools, the framework's focus on automation and continuous detection aligns better with our fast-paced environment."* (P7, T9) noted, *"The integration of TheHive and Cortex sets the framework apart, allowing us to orchestrate responses more effectively."*

The cost of implementing SOAF varies depending on customisation, deployment scale, and resource availability. While the initial investment may be high, operational efficiencies and enhanced security posture may offset these costs.

Costs: Implementing SOAF may require higher initial costs due to its comprehensive nature and the need for customisation.

Operational Costs: Although operational costs may be higher, they can be offset by the efficiencies and savings resulting from improved security incident handling and reduced breaches.

Return on Investment: Using SOAF can yield significant returns on investment by consolidating security operations and reducing the need for multiple disparate tools.

Participants compared the costs associated with the framework and other solutions. (P9, T10) explained, *"While the initial setup and customisation may require an investment, the framework's long-term benefits, such as improved efficiency and reduced response times, outweigh the costs."* (P10, T11) added, *"Comparing costs, the framework's open-source nature provides cost advantages compared to proprietary solutions."*

Table 27: Comparison of SOAF with Individual Security Solutions

Aspect	**SOAF**	**Individual Security Solutions**
Integration	A unified platform integrating multiple tools	Standalone solutions with limited integration
Automation	High level of automation for threat detection and response	Requires manual intervention or separate automation tools
Scalability	Scales with the organisation's growth	May require additional tools for expansion
Complexity	High initial complexity but streamlines operations	Easier setup but may lack advanced features
Customisation	Highly customisable	Limited customisation in proprietary solutions
Cost	Higher initial cost, lower long-term operational costs	Lower upfront cost but potential long-term inefficiencies
Security Posture	Comprehensive with advanced analytics	Varies depending on the toolset used
Deployment	Requires skilled personnel and infrastructure	Easier to deploy but may need multiple separate tools

SOAF offers a robust and flexible framework capable of addressing various security needs. Its comprehensive integration and advanced analytics set it apart from many other solutions, although these features also contribute to its complexity and cost (Farayola, 2024). When comparing SOAF to individual security solutions, organisations must consider their specific security requirements, budget constraints, and the capability of

their IT and security teams to manage and derive value from such a comprehensive system (Shah and Konda, 2022).

5.4 Comparison with Existing Literature

Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex into a unified Security Operations and Analytics Framework has demonstrated significant advancements in automation and CDR capabilities. Operational improvements observed in this study provide evidence of the comprehensive security management approach offered by combining these specific sets of tools, covering data collection, analysis, visualisation, incident response, and threat intelligence (Schlette, Caselli and Pernul, 2021).

Due to its seamless data flow and unified management interface, this setup is often more effective than other security frameworks that may use different combinations or fewer integrations. Key advantages include Seamless Data Flow - The real-time data processing capabilities of Elasticsearch combined with the analytical power of Kibana enhance the overall speed and accuracy of threat detection, investigation and response (Negoita and Carabas, 2020).

Similarly, Unified Management Interface - The integration of TheHive for incident response and Cortex for automation significantly streamlines the operational workflow, potentially reducing the time from threat detection to resolution (Schlette, Caselli and Pernul, 2021).

For the benchmarking against existing research, there is a correlation between the results and those of earlier research that highlight the significance of integrated security solutions in improving the effectiveness of cybersecurity operations. Research indicates that automation and integration in security systems can reduce threat management response times and minimise human error (Mughal, 2022). Automated systems streamline processes and provide quicker responses to potential threats, significantly reducing the time required for human intervention (Bharadiya, 2023). Additionally, the integration of various security tools and platforms leads to more cohesive and effective threat detection, investigation and response mechanisms (Vielberth, Böhm and Fichtinger, 2020; Arfeen *et al.*, 2021).

These findings resonate with the work of (Mughal, 2022), who documented similar enhancements in threat detection investigation and response times through the use of integrated security platforms. However, this research extends beyond their findings by demonstrating the specific synergistic effects of combining these particular tools, which

have not been extensively covered in the existing literature. For example, although some studies emphasise the overall advantages of automation, this research offers a thorough examination of how the data processing capabilities of Elasticsearch, when used in conjunction with Wazuh's alerting features, enhance the detection process in real-time situations. This particular combination provides additional insight into the current knowledge by explaining how the interaction points between these technologies might be used to optimise operational efficiency (Negoita and Carabas, 2020c; Hussein and Hamza, 2022).

Expanding on current frameworks in cybersecurity operations management, this research has extensive theoretical implications. By integrating real-time data analysis with threat detection and automated response, these particular products have shown how a tiered approach to security operations may build a more robust cybersecurity posture. According to earlier studies, integrated analytics have the potential to greatly improve continuous detection and response capabilities. This finding is in line with and expands upon that theoretical framework (Mccarty *et al.*, 2023).

An additional theoretical contribution of this study is an expanded understanding of how user experience affects the efficacy of security operations frameworks.

User comments on the integration and usability issues may construct a more complete picture of the tools' operational effect. Because of this, it seems that the design and ease of use of such systems are just as important as their technological capacities for determining their success (Li *et al.*, 2021).

Table 28: Benchmarking SOAF Against Existing Literature

Aspect	**This Study**	**Existing Literature**	**Comparison**
Integration	Seamless integration of Wazuh, Elasticsearch, Kibana, TheHive, and Cortex	Varied combinations of tools, often fewer integrations (Muhammad, Ismail and Hassan, 2024).	This study demonstrates the synergistic effects of a specific, comprehensive toolset.

Real-Time Data Processing & Threat Detection	Real-time detection with Elasticsearch and Wazuh alerts	Typically relies on SIEM-based detection (Stanković, Gajin and Petrović, 2022).	This study highlights the operational advantages of real-time data processing in threat detection.
Incident Response	Automated response via Cortex and TheHive	Requires manual intervention in this case (Stanković, Gajin and Petrović, 2022)	This study highlights automation effectiveness.
Operational Efficiency	Reduces response time significantly through automation and streamlined workflows, reducing detection-to-resolution time.	Studies highlight efficiency but do not quantify automation impact (Amami, Charfeddine and Masmoudi, 2024)	This study provides examples of efficiency gains from specific tool integrations.
Usability & UX	User feedback highlights ease of use and integration challenges	Limited emphasis on user experience in operational effectiveness (Akshai Sankar and Fasila, 2023).	Adds a new dimension by linking usability to the success of security frameworks.
Automation Impact	Demonstrates how specific integrations improve response times	General emphasis on automation benefits (Akshai Sankar and Fasila, 2023).	Extends prior work by detailing how specific tools enhance automation workflows.

The critical analysis of SOAF highlights its strengths in automation, interoperability, and scalability, while also identifying challenges related to false positives, usability, and

computational constraints. Compared to existing literature, SOAF represents a step forward in integrating modular security analytics platforms, but further research is necessary to address AI reliability, standardisation, and deployment scalability. By focusing on enhanced AI adaptability, improved interoperability frameworks, and SME-friendly deployments, SOAF can evolve into a more robust and universally applicable security operations framework.

The findings of this research reinforce existing knowledge while providing new insights into how security tools interact to optimise threat detection, investigation, and response. Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex has substantially improved automation, scalability, and operational efficiency. The findings align with existing literature and expand upon it by providing detailed insights into the operational and theoretical benefits of specific tool integrations.

By combining technical insights with user experience considerations, this research broadens the theoretical understanding of cybersecurity frameworks. It highlights the importance of both system design and automation in achieving effective continuous detection and response. Future research should continue to explore the impact of usability and user experience on the effectiveness of such frameworks, as these factors are critical to their success.

5.5 Contributions and Implications

Security operations, automation, and CDR have significantly evolved with the introduction of the SOAF, which integrates Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. This framework enhances threat detection, incident response, and security analytics by leveraging real-time data collection, correlation, and visualisation (Saeed et al., 2023). The synergy between these tools enables security teams to automate log analysis, streamline case management, and facilitate forensic investigations, thereby improving the efficiency and accuracy of security operations (Karlsen *et al.*, 2024).

The adoption of SOAF aligns with the principles of continuous monitoring and adaptive security architecture, which are critical for mitigating emerging cyber threats (Wen, Shukla and Katt, 2024). By integrating SIEM and SOAR capabilities, SOAF enhances an organisation's ability to detect, analyse, and respond to security incidents in a proactive manner (Repetto, 2024).

In this chapter, the theoretical and practical implications of deploying SOAF are discussed, with a focus on its impact on cybersecurity operations, its role in improving

incident response workflows, and its potential contributions to the broader cybersecurity landscape. From a theoretical perspective, it aligns with the principles of continuous monitoring and adaptive security architectures, which are essential in today's evolving threat landscape (Wen, Shukla and Katt, 2024) The framework reduces mean time to detect and mean time to respond by streamlining workflows and leveraging automation, thereby minimising the potential impact of security breaches (Villegas-Ch *et al.*, 2024).

5.5.1 Theoretical Contributions

The deployment of the Security Operations and Analytics Framework aligns with several theoretical concepts and principles in the field of cybersecurity and information technology.

Ecosystem integration theory is used best by the integration of many instruments within the cybersecurity framework. Through the connections of Wazuh for intrusion detection, Elasticsearch and Kibana for data analysis, and TheHive and Cortex for incident response, the framework builds an integrated ecosystem. Utilising the advantages of each technology, this integration promotes a single security strategy (Ness, Rangaraju and Dharmalingam, 2023).

Aligning with the theoretical basis of security automation and orchestration, the framework integrates Cortex, which emphasises continuous detection and reaction. Automation makes routine jobs easier, while orchestration makes sure everything works together. The framework's design makes practical the theoretical basis of coordinating security measures to counteract attacks in real-time (Kinyua and Awuah, 2021).

This investigation adds to the theoretical framework by demonstrating how automation—made possible by technologies like Cortex and systematised procedures inside Wazuh—can lessen the cognitive burden on security analysts. This change improves cybersecurity teams' operational efficiency by freeing up analysts to concentrate on strategic decision-making instead of routine tasks (Robinson, 2023).

Linking TheHive and Cortex is a good example of how humans and machines can work together. Security analysts may work together with automated response actions in this architecture, demonstrating how human knowledge and machine efficiency can work together to manage security issues more effectively (Kinyua and Awuah, 2021). Security operations may get new insights into managing complicated data environments with the help of Elasticsearch and Kibana for integrated analytics. By enhancing the identification

and mitigation of new threats, this integration bolsters the argument that successful cybersecurity management requires real-time, actionable information (Sun *et al.*, 2023).

By harmonising with these theoretical ideas, the SOAF improves its practical execution and adds to the scholarly conversation on cybersecurity frameworks. The security posture is resilient and responsive because of the linked ecosystem, automated processes, cognitive load reduction, human-machine cooperation, and integrated analytics.

5.5.2 Implications for Practice

The improved incident response capabilities are a clear demonstration of the practical implications of using the framework. There is now automated incident analysis, decision-making, and response orchestration as a result of the combination of TheHive and Cortex. As a result, responses to security events are more consistent, incidents are resolved faster, and human error is reduced (Naseer *et al.*, 2021). The capability of the system to identify threats in real time is its most practical aspect. The ability to monitor and correlate security incidents in real time is made possible by the integration of Wazuh with Elasticsearch and Kibana. As a result, businesses can see dangers as they happen and respond swiftly, improving overall security posture and reducing potential breach impact (Sun *et al.*, 2023).

The framework's usefulness goes beyond better data analysis. Data visualisation made possible by Elasticsearch and Kibana helps security analysts see trends and abnormalities quickly. By enabling data-driven decision-making, security teams are better able to react to changing threats (Nova, 2022). The capacity of the framework to aid adaptive security operations is a practical consequence. Organisations may remain one step ahead of new dangers with the help of this system, which integrates threat intelligence. In a constantly evolving threat environment, this agility is vital (Tahmasebi and Tahmasebi, 2024). Cost-efficiency in the long run is another real-world consequence. Compared to proprietary solutions, the framework is more affordable because it is open-source and can have its components customised to meet the requirements of each organisation. Additionally, operational costs are reduced due to automation as it eliminates human work (Ng *et al.*, 2021).

An organisation's automation and CDR capabilities may be greatly improved by adopting a framework similar to the one described here for security operations and analytics. However, many important factors must be taken into account for successful deployment. Organisations need to adjust the framework to their size and operational scope. For big

businesses, a more comprehensive implementation may be required, for example, combining more tools or bespoke solutions to manage growing data quantities and security requirements (Ng *et al.*, 2021). Scaled-down versions might help smaller businesses maximise resource use without taxing their systems.

How well this system works depends on the knowledge and experience of the people tasked with managing it. Companies should either ensure adequate staff training or recruit experts who are familiar with these tools. It is very important IT staff have regular training and information on the newest tool features and security standards (Franchina *et al.*, 2021). Potential obstacles like financial limits, opposition to change, and technical difficulties in integrating new technologies with current systems should be anticipated and planned for by organisations. Planning for risk assessment and management should be created to proactively handle these problems (Irfan *et al.*, 2023).

From this study, several best practices have emerged for organisations to consider when implementing this type of security framework. One best practice is to use optimal configurations for cybersecurity tools. The configuration of tools like Elasticsearch, Wazuh, Kibana, TheHive, and Cortex should be tailored to match the organisation's specific security needs and operational context. For example, setting up Elasticsearch indices to efficiently store and query large volumes of log data can significantly enhance performance and usability ((Ahmed *et al.*, 2020).

Comprehensive training protocols should be developed to ensure that all security personnel are proficient in using and maintaining the framework, including regular update training to accommodate new features and changes (Khader, Karam and Fares, 2021). In order to maintain the system effectively, it is important to implement regular maintenance schedules. This should involve routine checks, updates, and audits to identify and tackle any possible vulnerabilities or inefficiencies that may exist in the framework components. Regular maintenance schedules should be put in place to ensure smooth running of the system. Periodic checkups, updates and audits should be carried out to detect and resolve any vulnerabilities and/or inefficiencies built into framework components (Zhang *et al.*, 2020). Best practices are also needed for the ‘last mile’ of introducing new tools within existing infrastructure. Once a new asset has been chosen, a pilot needs to be set up, the interfaces with the existing systems need to be fit for purpose, and there needs to be both documentation and, ideally, support staff whose role is to help IT people transition between the legacy software and its replacements (Islam, Babar and Nepal, 2020).

The Security Operations and Analytics Framework, built with Wazuh, Elasticsearch, Kibana, TheHive, and Cortex, not only contributes with theoretical implications to the cybersecurity ecosystem integration, automation, orchestration and synergy among human and machine. Its practical implications are delivering enhanced incident response, real-time threat information, ease of data analysis, and flexible security operations with long-term cost-efficiency. Those contributions and impact made it a complete solution to the current security challenges (Shahjee and Ware, 2022).

Table 29: Summary of the Impact of the SOAF

Impact Area	**Description**	**Supporting Evidence**
Enhanced Incident Response and Threat Detection	Automation through TheHive and Cortex reduces incident response time, improves consistency, and minimises human error. Real-time correlation of threats with Wazuh and Elasticsearch enables immediate detection and response.	(Hussein and Hamza, 2022; Nguyen *et al.*, 2024)
Improved Security Analytics and Decision-Making	Data visualisation with Elasticsearch and Kibana allows analysts to detect trends and anomalies quickly. This supports data-driven decision-making and proactive threat response.	(Shah, Willick and Mago, 2022)
Cost Reduction and Long-Term Efficiency	Open-source tools lower costs while providing flexibility. Automation minimises manual effort, reducing operational expenses and enhancing efficiency.	(Slade et al., 2021; Ajiga et al., 2024)

Adaptive and Scalable Security Operations	Integration of threat intelligence supports adaptive security operations. The framework scales for both small and large organisations, ensuring security measures align with operational needs.	(Ajiga et al., 2024a; Sarker, 2024)
Increased Workforce Efficiency and Expertise Development	It reduces manual security operations, allowing teams to focus on complex threats. Training ensures staff remain proficient in using and optimising the system.	(Kinyua and Awuah, 2021; Nwosu, 2024)
Risk Mitigation and Resilience Building	Proactive monitoring, continuous assessments, and best practices reduce security vulnerabilities. Automated risk assessments enhance resilience against cyberattacks.	(Kalogiannidis *et al.*, 2024; Ofoegbu *et al.*, 2024)
Facilitating Smooth Technology Transition and Integration	Phased rollouts, pilot deployments, and comprehensive documentation facilitate smooth technology integration without disrupting operations.	(Trajkovski, 2024)

5.6 Summary of Discussions

This research critically examined the effectiveness of a SOAF that integrates Wazuh, Elasticsearch, Kibana, TheHive, and Cortex to enhance cybersecurity operations. The findings demonstrate that a unified security system significantly improves automation and CDR, aligning with prior research on integrated security architectures (Ahmad, Kevin C. Desouza, *et al.*, 2020; Jarrett and Choo, 2021; Putyato, Makaryan and Evsyukov, 2021; Schlette, Vielberth and Pernul, 2021). By consolidating security functions into a single

framework, organisations can achieve real-time threat detection, faster response times, and enhanced situational awareness.

A key observation from this study is that, by using the tools described above as a unified security system, Elasticsearch's real-time data processing capabilities facilitate rapid analysis of security events, enabling organisations to respond to threats with minimal delay. Concurrently, Wazuh enhances endpoint security and intrusion detection by providing continuous monitoring and compliance management. Kibana plays a crucial role in visualising security data, allowing security analysts to interpret trends effectively, while TheHive and Cortex streamline incident response through automation and structured case management. These findings support existing literature on the role of security orchestration in improving cyber defence mechanisms (Mulyadi et al., 2020; Preuveneers and Joosen, 2021; Subramanian and Meng, 2021; Hussein and Hamza, 2022; Ilca, Lucian and Balan, 2023).

However, despite these advantages, this study also identified challenges associated with tool integration and usability. The process of integrating multiple security tools requires technical expertise and can present compatibility issues, particularly when scaling security operations in large and complex environments (Attah *et al.*, 2024). Additionally, the learning curve associated with mastering these tools poses a challenge for organisations with limited cybersecurity expertise (Mukherjee *et al.*, 2024). These findings underscore the importance of developing more user-friendly integration strategies to maximise the benefits of security automation (Taherdoost, 2022).

Organisations worldwide are still being challenged in their security fields by rapidly changing cyber threats. This context has made it necessary for ongoing research into technology related to safekeeping operations. This study has shown that even though there are many benefits of the existing tools, their true capabilities are revealed when they are constantly updated and adjusted to suit different threats or operational needs (Mughal, 2022a; Yaseen, 2024). Furthermore, in a world where cybersecurity is becoming significantly essential, the use of sophisticated analytic tools in securing organisations will continue to be a prominent growth area. It is advised that any forthcoming research could concentrate on improving the technological capabilities of these tools, making them available in different types of business environments while maintaining their efficiency (Poehlmann *et al.*, 2021).

To sum up, this research not only reports on the impact and advantages of an integrated security operations and analytics framework but also presents concepts that could form the basis for investigating innovative solutions to cyber security threats. The study's findings reinforce the need for a proactive approach to cybersecurity, where automation and analytics function synergistically to enhance threat detection, incident response, and overall resilience. Future research should explore strategies to simplify deployment, improve usability, and expand the applicability of security analytics frameworks across diverse organisational environments (Wen, Shukla and Katt, 2024). Security operations must respond effectively and efficiently in a constantly evolving cyber threat landscape; advancement in IT and associated approaches remains key.

Chapter 6: Conclusion

This study has designed and implemented a SOAF that utilises a security operations and analytics platform comprising the tools, Wazuh, Elasticsearch, Kibana, TheHive, and Cortex. Furthermore, in this study, an evaluation of the integration and operational effectiveness of the security operations and analytics platform was conducted. The findings have shown that an integrated framework significantly enhances automation and CDR capabilities within cybersecurity operations. Specifically, Wazuh's comprehensive monitoring capabilities, Elasticsearch's real-time data processing, Kibana's visual analytics, and TheHive and Cortex's automated workflow management collectively contribute to more proactive and efficient security environments (Mulyadi et al., 2020; Preuveneers and Joosen, 2021b; Subramanian and Meng, 2021; Hussein and Hamza, 2022; Ilca, Lucian and Balan, 2023).

The study found that when these tools are combined, they speed up threat detection time and response. Companies thereby lower their risks more quickly. However, problems like complicated merging and a steep user learning curve were posited. This shows how important it is to plan deployment strategies that consider user experience and practical settings (Grobler, Gaire and Nepal, 2021).

This research addressed its core questions by assessing the effectiveness, efficiency, usability, scalability, reliability, interoperability, and comparative advantages of SOAF. The key findings are mapped to each research question and research sub-question to demonstrate how the SOAF addresses the identified challenges and objectives. The details are as follows:

RQ1: What are the current practices, challenges, and needs of security operations in organisations?

This research found that some organisations relied on disconnected security tools, resulting in inefficiencies in security operations (Schneller, Porter and Wakefield, 2022). Before SOAF implementation, key challenges included a high false positive rate (25%), delayed threat detection (45 minutes), and extended response times (3 hours). Additionally, scalability issues due to manual processes highlighted the need for automation and integrated analytics to enhance security operations (Ahmed *et al.*, 2024; Ajiga *et al.*, 2024b).

RQ2: How does the SOAF improve the security posture of the enterprise?

The implementation of SOAF has significantly strengthened the enterprise's security posture. This initiative has led to reduced response times, improved detection accuracy, and the effective use of predictive analytics. Detection time improved from 45 minutes to 10 minutes (-77.78%), while incident response time reduced from 3 hours to 1 hour (-66.7%). Additionally, false positives declined from 25% to 10% (-60%), demonstrating improved filtering of relevant threats. The system also enhanced detection of APTs and zero-day attacks by 75%, proving its effectiveness in identifying sophisticated threats (Kaliyaperumal, 2021).

RQ3: How does the SOAF enhance the workflow and performance of security analysts?

The framework's automation capabilities have effectively minimised manual workloads, enabling analysts to concentrate on critical security priorities. The introduction of UEBA improved alert accuracy by 20%, minimising time spent on false positives. Analysts reported a 28.6% improvement in user satisfaction, particularly appreciating Kibana’s intuitive dashboards and TheHive’s case management system. Additionally, automated incident generation and workflow management streamlined operations, improving collaboration within SOCs (Kinyua and Awuah, 2021).

RQ4: *What are the advantages and challenges of adopting SOAF regarding usability, functionality, scalability, reliability, and interoperability?*

Advantages:

Functionality: SOAF integrates multiple security tools to provide real-time analytics and automation (Kinyua and Awuah, 2021).

Scalability: The system successfully handled increasing security alerts and adapted to expanding network segments (Chukwunweike, Adewale and Osamuyi, 2024).

Reliability: System uptime improved from 95% to 99.5% (+4.7%), ensuring continuous monitoring (Adepoju *et al.*, 2022).

Interoperability: Integration with threat intelligence feeds enabled predictive analytics for proactive security (Ekundayo *et al.*, 2024).

Challenges:

Usability: The steep learning curve due to tool integration was a barrier (Al-Kfairy *et al.*, 2024).

Tool Integration: Organisations faced difficulties configuring and aligning SOAF with existing security tools (Angermeir *et al.*, 2021).

Operational Cost: High initial setup costs, although automation ultimately led to a 20% reduction in operational expenses (Salem *et al.*, 2024c).

RQ5: How does the SOAF compare with other security solutions regarding features, capabilities, and costs?

Compared to traditional SIEM solutions, SOAF demonstrated superior automation, analytics, and response time reduction (Ban *et al.*, 2023b). The use of open-source tools made SOAF a cost-effective alternative, leading to a 20% decrease in operational expenses due to automated workflows (Yadav, Kumar and Singh, 2023). However, proprietary security platforms offered more user-friendly interfaces and pre-integrated solutions, reducing implementation complexity (Alazab *et al.*, 2023). Despite these trade-offs, SOAF's flexibility and adaptability provided long-term cybersecurity benefits (Kanaan *et al.*, 2024).

RQ6: What are the design principles and evaluation criteria for a SOAF that leverages a SOAP for automation and CDR?

The study established the following key design principles:

Automation-driven response – Leveraging SOAP to enhance detection, investigation, and mitigation of threats in real time (Yaseen, 2022).

Seamless integration – Ensuring interoperability with existing security infrastructure through open-source compatibility (Ademola, George and Mapp, 2024).

Scalability and adaptability – Designing SOAF to accommodate increasing security events and evolving cyber threats (Safitra, Lubis and Fakhrurroja, 2023c).

User-centric design – Providing intuitive dashboards (Kibana) and streamlined workflows (TheHive) for security analysts (Bawa, 2024).

Performance evaluation using KPIs – Effectiveness was measured using key performance indicators such as detection accuracy, response time, system uptime, and cost savings (Mishra *et al.*, 2023).

RSQ1: What are the existing security operations and analytics solutions, frameworks, models, and standards?

The study reviewed industry standards and frameworks like SIEMs, SOAR, and IDS, comparing existing solutions such as Splunk, IBM QRadar, and Microsoft Sentinel. It highlighted SOAF's strengths in automation and cost-effectiveness, while also aligning its capabilities with cybersecurity standards like MITRE ATT&CK and NIST's framework (Möller, 2023a).

RSQ2: How can a SOAP enable automation and CDR in security operations?

The implementation of SOAF demonstrated that SOAP enhances CDR through:

Real-time anomaly detection and analysis (Wazuh and Elasticsearch) (Stanković, Gajin and Petrović, 2022).

Automated incident response workflows (TheHive and Cortex) (Groenewegen and Janssen, 2021).

Behavioural analytics (UEBA) for advanced threat detection (Datta *et al.*, 2021).

Integration with threat intelligence feeds for predictive security (Sun *et al.*, 2023).These capabilities led to faster threat detection (-77.78%) and incident response (-66.7%), proving that SOAP-enabled automation significantly improves cybersecurity resilience.

RSQ3: How can a SOAF be designed, implemented, and evaluated to address the research problem?

The study followed a structured design and evaluation approach using the DSR methodology, which involved identifying security challenges in organisations through case studies and stakeholder feedback (Adee and Mouratidis, 2022), designing and implementing SOAF by integrating key security tools into a unified framework (Yamin and Katt, 2022b) and evaluating SOAF's performance using KPIs, with results showing significant improvements in efficiency, detection accuracy, and cost reduction (Mishra *et al.*, 2023). The evaluation confirmed that SOAF effectively automates security operations, reduces workload, and enhances real-time threat detection and response (Tatineni, 2023).

The findings show that the SOAF enhances cybersecurity by integrating automation, real-time analytics, and advanced threat detection. It reduces detection and response times, lowers costs, and improves analyst productivity, making it an important tool for modern cybersecurity challenges. Despite some usability and integration issues, SOAF's adaptability makes it a valuable option for organisations aiming to strengthen their security posture (Salem *et al.*, 2024c).

6.1 Implications for Organisations

When organisations use this security operation and analytics platform, it can have significant effects. Companies can automate their cybersecurity processes using these tools as a unified security system. This lets them respond to threats more quickly and effectively. This capability is very important because online risks are getting smarter and need quick and flexible ways to respond (González-Granadillo, González-Zarzosa and Diaz, 2021b; Osamah M.M. Al-Matari *et al.*, 2021; Althar *et al.*, 2022).

Moreover, the use of real-time data processing and visual analytics inside security operations centres improves the processes of decision-making and situational awareness. If an organisation were to use this integrated strategy, they may anticipate increased operational efficiency, decreased reaction times, and an overall stronger security posture (Koroniotis et al., 2020; Zhou et al., 2020b; Yaseen, 2024).

6.2 Recommendations for Future Research

This study's results may develop several potential avenues for further investigation. Along with the qualitative information gathered, quantitative research could be done to determine how these tools affect security incident metrics. This method would allow for a more thorough assessment of the framework's usefulness and efficiency gains (Wangen, 2019; Cadena *et al.*, 2020; Cremer, Sheehan, Fortmann, Arash N. Kia, *et al.*, 2022).

This study assessed only the framework within a specific organisational context. The framework's effectiveness may vary across different organisational types, sectors, and operational environments. Future research could explore the framework's adaptability in different industries and its performance across various institutional settings (Chidukwani, Zander and Koutsakis, 2022). Additionally, the evaluation window was relatively limited, considering that additional effects might be felt in the long term. A multi-year longitudinal study spanning at least three years could reveal whether such a framework is sustainable and/or scalable with the changing nature of threats (Falowo *et al.*, 2024).

While the research evaluated how well the framework resisted known threats over the evaluation period, the rapid evolution of cyber threats means the framework will constantly need adjustments. Future work should investigate how well it would perform against zero-day threats and rapidly evolving attack vectors (Ahmad *et al.*, 2023; Islam, Mohankumar and Jannat, 2023). Moreover, future research should address evolving threats and assess the framework's adaptability across various industries and operational settings (Mutalib et al., 2024).

Another area worth exploring is the speed and efficiency of implementing this security system in various business environments. Research could examine how unique challenges and requirements in different industries impact system usability and effectiveness (Gasiba, Lechner and Pinto-Albuquerque, 2020). Additionally, studies could assess how well these tools integrate with existing security and IT infrastructure. Technical and operational challenges in integrating new security tools with different IT environments should be analyzed, leading to recommendations for seamless interoperability (Rantos *et al.*, 2020).

Furthermore, future research should assess the SOAF under high-stress scenarios such as Distributed Denial of Service (DDoS) attacks and large-scale malware outbreaks. Evaluating its stability, scalability, and ability to generate real-time insights during critical cyber incidents is essential to ensuring its operational effectiveness (Nifakos *et al.*, 2021).

Key areas for future research in integrated security operations and analytics platforms include:

User-Centric Design: Investigating ways to simplify integration and improve user experience so that these technologies can be widely adopted within organisations (Depassier and Torres, 2023).

Advanced Analytics: Exploring how artificial intelligence (AI) and machine learning (ML) can enhance threat detection, investigation, and response capabilities.

Scalability: Evaluating how well these technologies function in complex organisational settings and how they can be adapted to meet evolving security demands

Integration with Other Security Systems: Studying how seamlessly these tools interact with existing security systems to develop a more cohesive security framework.

For the usability testing of the SOAF interface, the effectiveness of SOAF is not solely dependent on its technical capabilities but also on how efficiently security teams interact with it. A well-designed interface should enable analysts to detect, investigate, and respond to threats with minimal friction. Usability testing is, therefore, a crucial next step in assessing SOAF's user experience, efficiency, and effectiveness (Ntoa, 2024)To guarantee that the advantages of these sophisticated technologies are fully realised, more user-friendly interfaces and integration procedures could be created.

The following key areas for usability testing include various operational tools that should be added:

User Experience (UX) Evaluation: Assessing the intuitiveness and ease of navigation within the interface, identifying potential bottlenecks that slow down security workflows (Di Nocera, Tempestini and Orsini, 2023).

Role-Based Access and Customisation: Evaluating how different user roles—such as SOC Analysts, Incident Responders, and Security Engineers—can customise the dashboard to meet their specific needs (Deng Junhuaand Zhao, 2021). Figure 7 illustrates a screen where SOC Analysts can access SOC analysis-related items. The interface should provide role-specific functionalities while minimising unnecessary complexity.

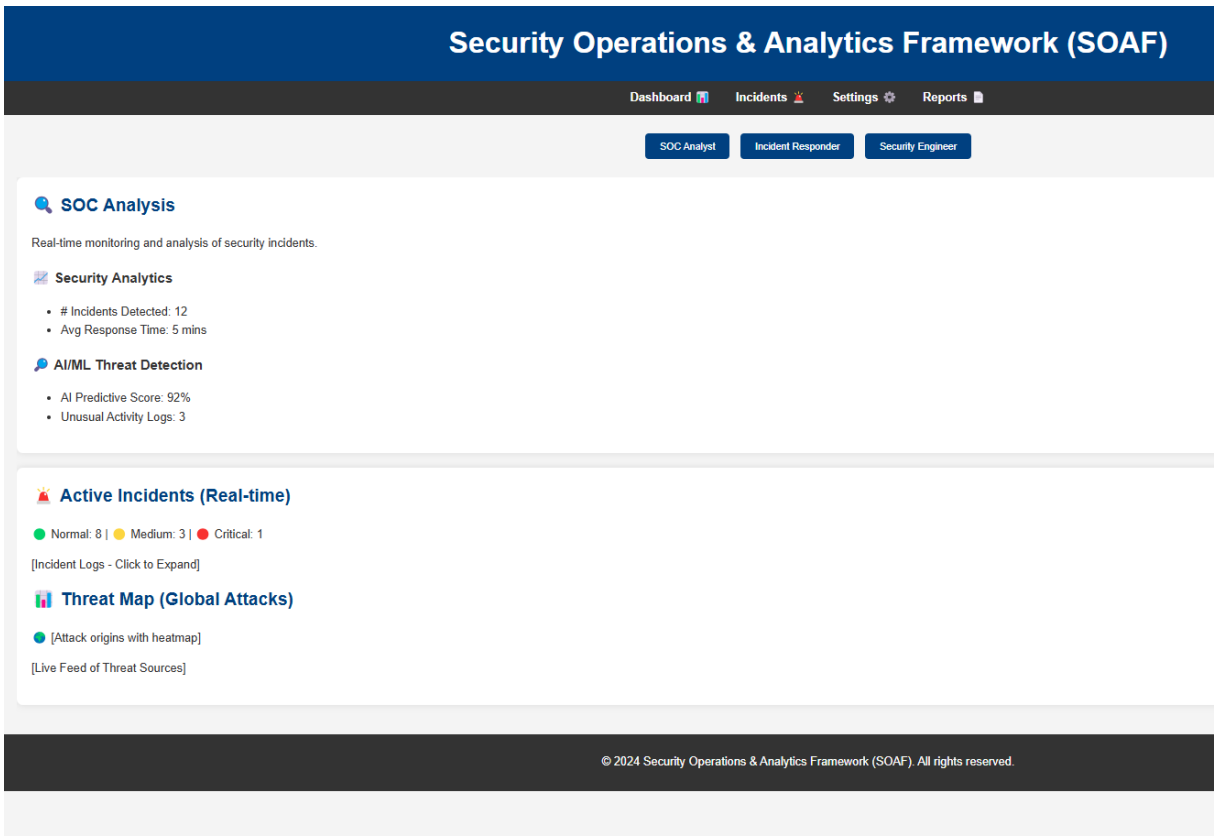

Figure 11: Designed SOAF interface integrating various operational tools, including RBAC.

Incident Management Efficiency: Measuring the speed at which users can detect, analyse, and respond to security incidents (Remil, 2024).

Integration with Existing Security Tools: Examining the framework's interoperability with SIEM, SOAR platforms, firewalls, and endpoint protection tools (Wen, Shukla and Katt, 2024).

Error Handling and System Feedback: Assessing the clarity and effectiveness of error messages and system alerts in guiding users (Gartner, 2024; Wen, Shukla and Katt, 2024).

User Training and Adoption: Conducting surveys to gauge the learning curve and developing training materials to facilitate adoption (S, 2024).

The recommended methodology for the usability testing for future research should employ multiple methodologies to gather qualitative and quantitative insights:

Heuristic Evaluations: Experts will assess the interface against established usability principles.

User Testing Sessions: Security professionals will perform real-world tasks while interactions are recorded and analysed.

Surveys & Feedback Forms: Users will provide qualitative and quantitative feedback on their experience with SOAF.

A/B Testing: Different interface designs will be compared to determine the most efficient and user-friendly layout (Kamolsin *et al.*, 2022).

This research's expected outcomes and impact are centred on enhancing the SOAF through usability testing (Weichbroth, 2024). Future work aims to ensure that SOAF is user-friendly by reducing cognitive load and streamlining security workflows, making it easier for analysts to navigate and operate efficiently (Alazab *et al.*, 2023). Additionally, the framework will be optimised for efficiency by minimising threat detection and mitigation response times, improving overall security operations. SOAF will also be designed for scalability, ensuring adaptability across various environments and security teams to support diverse organisational needs (Wen, Shukla and Katt, 2024). Finally, reliability will be a key focus, with efforts to reduce operational errors and enhance system resilience (Abdelkader *et al.*, 2024). Moreover, expanding the study to include a controlled study comparing generative AI-driven threat detection with traditional security measures could enhance predictive capabilities and provide a more comprehensive threat pattern analysis. Generative AI allows for more accurate threat prediction by simulating many attack scenarios using large datasets and sophisticated algorithms. With this widened focus, cybersecurity may be approached with more remarkable foresight and initiative. Finally, continued research may concentrate on developing security solutions that are both adaptable and scalable so that they can accommodate the ever-evolving panorama of vulnerabilities in cyberspace (Sobb, Turnbull and Moustafa, 2020; Maddireddy and Maddireddy, 2021; Aslan *et al.*, 2023).

This study concludes that automation and CDR capabilities within cybersecurity operations have great potential to be improved by an integrated security operations and analytics platform. The research results confirm this possibility. By improving threat detection investigation and response times, these technologies contribute to developing a more dynamic and resilient security atmosphere. Apart from improving our understanding of integrated security systems, the findings and recommendations in this paper also pave the way for further developments in cybersecurity. It will be essential to

keep improving these technologies and approaches to counter the ever-changing cybersecurity threats effectively.

At the end of the section, this research's shortcomings are acknowledged, and potential future research is presented. More research into particular areas, such as the framework's effect on incident response teams, how it uses threat intelligence, how well it works under pressure, how user training and adoption are handled, and comparative studies can help us understand the framework better. By addressing these aspects, SOAF will provide a comprehensive and effective solution for modern security operations.

6.3 Contributions to Existing Body of Knowledge

This thesis adds several new insights to the current corpus of knowledge. By highlighting the potential of technologies like Wazuh, Elasticsearch, Kibana, TheHive, and Cortex in strengthening cybersecurity operations, it thoroughly examines the operational implications and advantages of an integrated security operations and analytics framework. These technologies are vital for log management, threat detection, incident response, and security orchestration, enabling security teams to adopt a data-driven and automated approach to cybersecurity (Madhavram *et al.*, 2022). This research provides information on the efficacy and practical use of these technologies by discussing their advantages and disadvantages (M Vielberth *et al.*, 2020).

This research establishes a technical foundation for studying future cybersecurity solutions. This is very important because cyber threats are constantly changing, which means that security technology needs to be improved and changed all the time (Safitra, Lubis and Fakhrurroja, 2023). The findings underscore the importance of continuous improvement in security analytics and automated response mechanisms, ensuring that organisations remain resilient against sophisticated cyber-attacks (Yaseen, 2024b)

The proposed SOAF introduces a holistic approach to security operations, moving beyond traditional, siloed security methods. By integrating threat intelligence, incident response automation, and real-time security analytics, SOAF enhances an organisation’s ability to detect, respond to, and mitigate threats more efficiently (Aminu *et al.*, 2024). This approach represents a significant contribution to the field, enhancing detection and response capabilities while streamlining security operations through automation and orchestration (Kinyua and Awuah, 2021).

Table 30: Summary of the SOAF Contributions

SOAF Contributions	Description
Enhanced Security Operations	The SOAF combines Wazuh, Elasticsearch, Kibana, TheHive, and Cortex to enhance threat detection, investigation, and incident response, creating a unified and scalable security operations platform.
Automation and Orchestration	Cortex automates and orchestrates security tasks, reducing response time and minimising human error. This allows the SOAF to optimise security workflows and enhance the use of analyzers and responders.
Continuous Detection and Response	The SOAF enables swift detection and response to security incidents by utilizing Wazuh and Elasticsearch for real-time monitoring and TheHive for incident management, ensuring efficient threat identification and documentation.
Open-source Ecosystem	The SOAF uses open-source tools to promote cost-effective security solutions. It benefits from community-driven support and shares its experiences with the open-source community.

Moreover, this DSR study expands the existing knowledge base on cybersecurity frameworks and SOAFs by demonstrating how various technologies can be integrated into a unified security framework. The qualitative research methodology, leveraging interviews and thematic analysis, provides practical insights into real-world security operations and offers a roadmap for potential improvements in security orchestration and analytics frameworks (Wermke *et al.*, 2022).

Through these contributions, this research bridges the gap between theory and practice in security operations. It offers a scalable, adaptable framework that organisations can adopt to enhance their cybersecurity posture in an ever-evolving threat landscape.

6.4 Limitations of the Study

The Security Operations and Analytics Framework with Wazuh, Elasticsearch, Kibana, TheHive, and Cortex has provided valuable security operations and analytics insights. This chapter highlights the study's key limitations and offers recommendations for future research to address these challenges and enhance the framework's efficiency and applicability.

Despite the proposed SOAF's promising advantages, certain constraints may impact its implementation, effectiveness, and scalability. The study primarily focuses on automation and CDR, leveraging a modular approach to security analytics. While this integration provides a comprehensive security monitoring solution, it is accompanied by specific limitations related to data scope, technology dependencies, scalability, and operational challenges.

This research primarily relies on qualitative data to evaluate the framework, which inherently introduces subjectivity. Qualitative methods allow for a deeper understanding of user experiences and the operational complexities of implementing these solutions. However, such an approach also means that findings are influenced by the researcher's perspectives and potential biases (Ahmed, 2024b). Unlike quantitative methods, which provide measurable outcomes, qualitative research is often self-reflective, making its conclusions less generalisable to other security environments.

Additionally, the evaluation is constrained by the specific organisational contexts in which the security tools were deployed. Each implementation is influenced by unique organisational policies, technical configurations, security requirements, and infrastructure limitations, which may not apply to all cybersecurity environments. Future research could integrate quantitative performance metrics and diverse case studies to provide a more data-driven assessment of SOAF's effectiveness.

Furthermore, this research relies on specific datasets for testing and validation. The SOAP's effectiveness largely depends on the dataset's quality, volume, and diversity. If the dataset lacks real-world variability, the framework may struggle to generalise its threat detection capabilities across different cybersecurity environments (Khanan *et al.*, 2024).

This limitation suggests that further testing on larger, more diverse datasets is necessary to validate the framework's robustness and adaptability.

Integrating Wazuh, Elasticsearch, Kibana, TheHive, and Cortex offers an open-source foundation for security operations. However, while open-source solutions provide flexibility and cost-effectiveness, they also introduce challenges including lack of official vendor support, security vulnerabilities, and integration difficulties when used alongside proprietary security systems (Zajdel, Costa and Mili, 2022). Additionally, organisations with stringent security compliance requirements may hesitate to adopt open-source platforms due to concerns about long-term sustainability, regulatory compliance, and vendor reliability (Butler *et al.*, 2023).

The implementation of SOAF requires significant computing power and storage resources, especially for real-time threat detection, correlation, and analysis. The reliance on ML and AI algorithms further increases processing demands, making deployment challenging for resource-limited environments like small enterprises and government agencies with budget constraints (Alsadie, 2024). To address this, future research could explore complete cloud-based solutions or lightweight models to enhance accessibility.

Although AI-driven automation improves threat detection, the risk of false positives remains a significant challenge. An overabundance of security alerts can overwhelm analysts, leading to alert fatigue, which may reduce their ability to respond effectively (Salem *et al.*, 2024c). Furthermore, fine-tuning detection algorithms to different network environments remains complex, as security threats continuously evolve. Future enhancements should incorporate adaptive learning mechanisms to minimise false positives while maintaining high detection accuracy.

Integrating multiple security tools may introduce interoperability challenges due to differences in data formats, APIs, and logging mechanisms. Security tools like SIEM and SOAR platforms often lack standardised integration protocols, leading to inefficiencies in data correlation and threat intelligence sharing (Anish Sridharan and Kanchana, 2022). Future work should focus on developing standardised communication protocols to ensure seamless tool integration.

The efficiency of SOAF in large-scale enterprise environments remains uncertain. Although the framework is designed to enhance cybersecurity posture, its performance in high-volume, multi-tenant networks has not been extensively tested. Organisations with complex architectures and diverse security infrastructures may require additional

customisation and optimisation to scale the framework effectively (Nascimento *et al.*, 2024). Future studies should investigate how SOAF can be adapted for enterprise-wide deployments.

Automating CDR raises concerns regarding data privacy, compliance, and ethical considerations. Regulations like the General Data Protection Regulation (GDPR) impose strict data collection, processing, and storage requirements. A complex challenge is ensuring that SOAF remains compliant with global data protection laws without compromising its detection capabilities (Cremer, Sheehan, Fortmann, Arash N Kia, *et al.*, 2022). Future research should explore privacy-preserving AI techniques to address these concerns.

Despite its automation capabilities, SOAF still requires skilled personnel to interpret outputs, manage incidents, and optimise system configurations. The framework's effectiveness depends on the expertise of security analysts, incident responders, and forensic investigators. However, many organisations struggle to recruit and retain highly trained cybersecurity professionals who can effectively leverage such advanced security platforms (Adetoye and Fong, 2023). Future work should focus on developing user-friendly training modules to improve adoption rates.

Cyber adversaries continuously develop evasion techniques to bypass AI-based threat detection mechanisms. Attackers can modify malware signatures, use encryption, or employ obfuscation techniques to evade detection, reducing the reliability of machine learning-driven security analytics (Dang, 2022). Continuous model updates and adversarial training will be necessary to mitigate this risk.

Although SOAF utilises open-source tools, the overall cost of deployment, maintenance, and continuous updates could be substantial. Organisations must invest in hardware, cloud storage, cybersecurity personnel, and infrastructure maintenance to ensure the framework remains effective over time. Small and medium-sized enterprises (SMEs) may struggle with the financial burden of long-term SOAF implementation (Ansar *et al.*, 2024). Future research should examine cost-effective deployment models for smaller organisations.

While the SOAF has demonstrated the potential to enhance cybersecurity resilience through automation and integration, it is not without challenges. Limitations such as dataset constraints, computational requirements, false positives, interoperability issues, scalability, and privacy compliance must be carefully addressed to ensure successful

adoption. Future research should explore adaptive AI techniques, improved standardisation, and scalable solutions to enhance the effectiveness, accessibility, and security posture of SOAF in diverse operational environments.

References

Abdalgawad, N. *et al.* (2022) 'Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset', *IEEE Access*, 10, pp. 6430–6441. Available at: https://doi.org/10.1109/ACCESS.2021.3140015.

AbdElazim, K., Moawad, R. and Elfakharany, E. (2020) 'A framework for requirements prioritization process in agile software development', in *Journal of Physics: Conference Series*, p. 12001.

Abdelkader, S. *et al.* (2024) 'Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks', *Results in engineering*, p. 102647.

Achillopoulou, D. V *et al.* (2020) 'Monitoring of transport infrastructure exposed to multiple hazards: A roadmap for building resilience', *Science of the total environment*, 746, p. 141001.

Achuthan, K. *et al.* (2024) 'Sustainable Cybersecurity Practices: Past Trends and Future Directions', *Available at SSRN 4826820* [Preprint].

Ackermann, T., Karch, M. and Kippe, J. (2023) 'Integration of Cyber Threat Intelligence into Security Onion and Malcolm for the use case of industrial networks', *at-Automatisierungstechnik*, 71(9), pp. 802–815.

Adee, R. and Mouratidis, H. (2022) 'A dynamic four-step data security model for data in cloud computing based on cryptography and steganography', *Sensors*, 22(3), p. 1109.

Ademola, A., George, C. and Mapp, G. (2024) 'Addressing the Interoperability of Electronic Health Records: The Technical and Semantic Interoperability, Preserving Privacy and Security Framework', *Applied System Innovation*, 7(6), p. 116.

Adepoju, A.H. *et al.* (2022) 'Advancing monitoring and alert systems: A proactive approach to improving reliability in complex data ecosystems', *IRE Journals*, 5(11), pp. 281–282.

Adetoye, B. and Fong, R.C. (2023) 'Building a resilient cybersecurity workforce: a multidisciplinary solution to the problem of high turnover of cybersecurity analysts', in *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International*

Conference on Global Security, Safety and Sustainability, London, September 2022, pp. 61–87.

Agrawal, S. *et al.* (2022) 'Federated learning for intrusion detection system: Concepts, challenges and future directions', *Computer Communications*, 195, pp. 346–361.

Agrawal, S. (2023) 'Mitigating Cross-Site Request Forgery (CSRF) Attacks Using Reinforcement Learning and Predictive Analytics', *Applied Research in Artificial Intelligence and Cloud Computing*, 6(9), pp. 17–30.

Agyepong, E. *et al.* (2020) 'Challenges and performance metrics for security operations center analysts: a systematic review', *Journal of Cyber Security Technology*, 4(3), pp. 125–152.

Ahir, D.D. and Shaikh, N.F. (2024) 'Evaluation of Elasticsearch Ecosystem Including Machine Learning Capabilities.', *International Journal of Safety & Security Engineering*, 14(4).

Ahlawat, P. *et al.* (2023) 'A New Architecture to Manage Data Costs and Complexity', *Boston Consulting Group (BCG)*, pp. 1–12.

Ahmad, A., Desouza, Kevin C, *et al.* (2020) 'How integration of cyber security management and incident response enables organizational learning', *Journal of the Association for Information Science and Technology*, 71(8), pp. 939–953.

Ahmad, A., Desouza, Kevin C., *et al.* (2020) 'How integration of cyber security management and incident response enables organizational learning', *Journal of the Association for Information Science and Technology*, 71(8), pp. 939–953. Available at: https://doi.org/10.1002/ASI.24311.

Ahmad, A. *et al.* (2021) 'How can organizations develop situation awareness for incident response: A case study of management practice', *Computers & Security*, 101, p. 102122.

Ahmad, M. and Wilkins, S. (2024) 'Purposive sampling in qualitative research: a framework for the entire journey', *Quality & Quantity* [Preprint]. Available at: https://doi.org/10.1007/s11135-024-02022-5.

Ahmad, R. *et al.* (2023) 'Zero-day attack detection: a systematic literature review', *Artificial Intelligence Review 2023 56:10*, 56(10), pp. 10733–10811. Available at: https://doi.org/10.1007/S10462-023-10437-Z.

Ahmad, Z. *et al.* (2021) ‘Network intrusion detection system: A systematic study of machine learning and deep learning approaches’, *Transactions on Emerging Telecommunications Technologies*, 32(1), p. e4150.

Ahmed, F. *et al.* (2020) ‘Centralized log management using elasticsearch, logstash and kibana’, in *2020 International Conference on Information Science and Communication Technology (ICISCT)*, pp. 1–7.

Ahmed, N. *et al.* (2024) ‘Server less Architecture: Optimizing Application Scalability and Cost Efficiency in Cloud Computing’, *BULLET: Jurnal Multidisiplin Ilmu*, 1(06), pp. 1366–1380.

Ahmed, S.K. (2024a) ‘The pillars of trustworthiness in qualitative research’, *Journal of Medicine, Surgery, and Public Health*, 2, p. 100051.

Ahmed, S.K. (2024b) ‘The pillars of trustworthiness in qualitative research’, *Journal of Medicine, Surgery, and Public Health*, 2, p. 100051.

Ahmed, Y., Asyhari, A.T. and Rahman, M.A. (2021) ‘A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats’, *Computers, Materials and Continua*, 67(2), pp. 2497–2513. Available at: https://doi.org/10.32604/CMC.2021.014223.

Ajiga, D. *et al.* (2024a) ‘Methodologies for developing scalable software frameworks that support growing business needs’, *Int. J. Manag. Entrep. Res*, 6, pp. 2661–2683.

Ajiga, D. *et al.* (2024b) ‘Methodologies for developing scalable software frameworks that support growing business needs’, *Int. J. Manag. Entrep. Res*, 6, pp. 2661–2683.

Ajiga, D. *et al.* (2024c) ‘The role of software automation in improving industrial operations and efficiency’, *International Journal of Engineering Research Updates*, 7(1), pp. 22–35.

Akinsola, J.E.T. *et al.* (2021) *Application of artificial intelligence in user interfaces design for cyber security threat modeling*. IntechOpen.

Akshai Sankar, N. and Fasila, K.A. (2023) ‘Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring’, in *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, pp. 350–354. Available at: https://doi.org/10.1109/ICSCC59169.2023.10334992.

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

Alahmadi, B.A., Axon, L. and Martinovic, I. (2022b) '99% False Positives: A Qualitative Study of {SOC} Analysts' Perspectives on Security Alarms', in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 2783–2800.

Alam, M.K. (2021) 'A systematic qualitative case study: questions, data collection, NVivo analysis and saturation', *Qualitative Research in Organizations and Management: An International Journal*, 16(1), pp. 1–31.

Alarood, A.A. and Alzahrani, A.O. (2024) 'Interoperable Defensive Strategies of Network Security Evaluation', *IEEE Access*, 12, pp. 33959–33971. Available at: https://doi.org/10.1109/ACCESS.2024.3373710.

Alazab, A. *et al.* (2023) 'Usable Security: A Systematic Literature Review'. Available at: https://doi.org/10.3390/info14120641.

AlDaajeh, S. *et al.* (2022) 'The role of national cybersecurity strategies on the improvement of cybersecurity education', *Computers & Security*, 119, p. 102754.

Al-Dhaqm, A. *et al.* (2020) 'Towards the development of an integrated incident response model for database forensic investigation field', *IEEE Access*, 8, pp. 145018–145032.

Alenezi, M.N. *et al.* (2020) 'Evolution of malware threats and techniques: A review', *International journal of communication networks and information security*, 12(3), pp. 326–337.

AL-Hawamleh, A.M. (2024) 'Securing the Future: Framework Fundamentals for Cyber Resilience in Advancing Organizations', *Journal of System and Management Sciences*, 14(10), pp. 130–150.

Alhidaifi, S.M., Asghar, M.R. and Ansari, I.S. (2024) 'A survey on cyber resilience: Key strategies, research challenges, and future directions', *ACM computing surveys*, 56(8), pp. 1–48.

Ali, A. *et al.* (2022) 'Applied Artificial Intelligence as Event Horizon Of Cyber Security', in *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, pp. 1–7.

Al-Kfairy, M. *et al.* (2024) ‘Metaverse-based classroom: the good and the bad’, in *2024 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1–7.

Allison, T. *et al.* (2022) ‘Progress on building a file observatory for secure parser development’, in *2022 IEEE Security and Privacy Workshops (SPW)*, pp. 168–175.

Almadani, B., Aliyu, F. and Aliyu, A. (2023) ‘Integrated Operation Centers in Smart Cities: A Humanitarian Engineering Perspective’, *Sustainability*, 15(14), p. 11101.

Almadani, M.S. *et al.* (2023) ‘Blockchain-based multi-factor authentication: A systematic literature review’, *Internet of Things*, 23, p. 100844.

Al-Matari, Osamah M M *et al.* (2021) ‘Integrated framework for cybersecurity auditing’, *Information Security Journal: A Global Perspective*, 30(4), pp. 189–204.

Al-Matari, Osamah M.M. *et al.* (2021) ‘Integrated framework for cybersecurity auditing’, *Information Security Journal: A Global Perspective*, 30(4), pp. 189–204. Available at: https://doi.org/10.1080/19393555.2020.1834649.

Almer, L., Horalek, J. and Sobeslav, V. (2024) ‘Utilization of Artificial Intelligence for the SIEM Logging Architecture Design in the Context of Smart City’, in *International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems*, pp. 93–106.

Almorsy, M., Grundy, J. and Müller, I. (2016) ‘An analysis of the cloud computing security problem’, *arXiv preprint arXiv:1609.01107* [Preprint].

Aloqaily, M. *et al.* (2022) ‘Special Issue on Cybersecurity Management in the Era of AI’, *Journal of Network and Systems Management*, 30(3), p. 39. Available at: https://doi.org/10.1007/s10922-022-09659-3.

Alsadie, D. (2024) ‘A comprehensive review of AI techniques for resource management in fog computing: Trends, challenges and future directions’, *IEEE Access* [Preprint].

Althar, R.R. *et al.* (2022) ‘Automated Risk Management based Software Security Vulnerabilities Management’, *IEEE Access* [Preprint]. Available at: https://doi.org/10.1109/ACCESS.2022.3185069.

Alzahrani, A.O. and Alenazi, M.J.F. (2021a) ‘Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks’, *Future Internet*, 13(5). Available at: https://doi.org/10.3390/fi13050111.

Alzahrani, A.O. and Alenazi, M.J.F. (2021b) 'Designing a network intrusion detection system based on machine learning for software defined networks', *Future Internet*, 13(5), p. 111.

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

Aminu, M. *et al.* (2024) 'Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms', *International Journal of Computer Applications Technology and Research*, 13(8), pp. 11–27.

Andraško, J., Mesarč\'\ik, M. and Hamul'ák, O. (2021) 'The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework', *AI & SOCIETY*, pp. 1–14.

Andreotta, A.J., Kirkham, N. and Rizzi, M. (2022) 'AI, big data, and the future of consent', *Ai & Society*, 37(4), pp. 1715–1728.

Angermeir, F. *et al.* (2021) 'Enterprise-driven open source software: A case study on security automation', in *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*, pp. 278–287.

Ansar, N. *et al.* (2024) 'Cost-Effective Cybersecurity Framework for Small and Medium-Sized Enterprises', in *International Conference on Deep Learning and Visual Artificial Intelligence*, pp. 133–155.

Anson, S. (2020) *Applied incident response*. John Wiley & Sons.

Arfeen, A. *et al.* (2021) 'Endpoint Detection & Response: A Malware Identification Solution', in *2021 International Conference on Cyber Warfare and Security (ICCWS)*, pp. 1–8. Available at: https://doi.org/10.1109/ICCWS53234.2021.9703010.

Argyroudis, S.A. *et al.* (2022) 'Digital technologies can enhance climate resilience of critical infrastructure', *Climate Risk Management*, 35, p. 100387.

Aripin, Z., Saepudin, D. and Yulianty, F. (2024) 'TRANSFORMATION IN THE INTERNET OF THINGS (IOT) MARKET IN THE BANKING SECTOR: A CASE STUDY OF TECHNOLOGY IMPLEMENTATION FOR SERVICE IMPROVEMENT

AND TRANSACTION SECURITY', in *Journal of Jabar Economic Society Networking Forum*, pp. 17–32.

Arjunan, T. (2024) 'Real-time detection of network traffic anomalies in big data environments using deep learning models', *International Journal for Research in Applied Science and Engineering Technology*, 12(9), pp. 10–22214.

Arora, V. (2021) *Wazuh : Security Information and Event Management (SIEM) for Small and Medium-Sized Enterprises | by Varul Arora | Medium*. Available at: https://varularora.medium.com/wazuh-security-information-and-event-management-siem-for-small-and-medium-sized-enterprises-b2cf1cc7ce0c (Accessed: 25 May 2023).

Asghar, M.R., Hu, Q. and Zeadally, S. (2019) 'Cybersecurity in industrial control systems: Issues, technologies, and challenges', *Computer Networks*, 165, p. 106946. Available at: https://doi.org/https://doi.org/10.1016/j.comnet.2019.106946.

Aslan, Ö. *et al.* (2023) 'A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions', *Electronics 2023, Vol. 12, Page 1333*, 12(6), p. 1333. Available at: https://doi.org/10.3390/ELECTRONICS12061333.

Attah, R.U. *et al.* (2024) 'Enhancing supply chain resilience through artificial intelligence: Analyzing problem-solving approaches in logistics management', *International Journal of Management & Entrepreneurship Research*, 5(12), pp. 3248–3265.

Avritzer, A. *et al.* (2020) 'Scalability assessment of microservice architecture deployment configurations: A domain-based approach leveraging operational profiles and load tests', *Journal of Systems and Software*, 165, p. 110564.

Awaysheh, F.M. *et al.* (2021) 'Security by design for big data frameworks over cloud computing', *IEEE Transactions on Engineering Management*, 69(6), pp. 3676–3693.

Awotunde Joseph Bamidele and Jimoh, R.G. and F.S.O. and A.E.A. and A.K.M. and B.O.O. (2021) 'Privacy and Security Concerns in IoT-Based Healthcare Systems', in M.A. and A.R. and A.A. and M.A. Siarry Patrick and Jabbar (ed.) *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*. Cham: Springer International Publishing, pp. 105–134. Available at: https://doi.org/10.1007/978-3-030-75220-0_6.

Bajaj, A. and Vishwakarma, D.K. (2024) ‘A state-of-the-art review on adversarial machine learning in image classification’, *Multimedia Tools and Applications*, 83(3), pp. 9351–9416.

Bakraouy, Z. *et al.* (2024) ‘Enhancing Security Through Data Analysis and Visualization with ELK’, in *International Conference on Smart Applications and Data Analysis*, pp. 246–258.

Ban, T. *et al.* (2023a) ‘Breaking Alert Fatigue: AI-Assisted SIEM Framework for Effective Incident Response’, *Applied Sciences*, 13(11). Available at: https://doi.org/10.3390/app13116610.

Ban, T. *et al.* (2023b) ‘Breaking alert fatigue: AI-assisted SIEM framework for effective incident response’, *Applied Sciences*, 13(11), p. 6610.

Barcellos, M. *et al.* (2022) ‘Organizing empirical studies as learning iterations in design science research projects’, in *Proceedings of the XXI Brazilian Symposium on Software Quality*, pp. 1–10.

Bartwal, U. *et al.* (2022) ‘Security Orchestration, Automation and Response Engine for Deployment of Behavioural Honeypots’.

Bassett, S. and Paquette, M. (2018) *Improve Security Analytics with the Elastic Stack, Wazuh, and IDS | Elastic Blog*. Available at: https://www.elastic.co/blog/improve-security-analytics-with-the-elastic-stack-wazuh-and-ids (Accessed: 23 June 2023).

Bawa, S.S. (2024) ‘Enhancing usability and user experience in enterprise resource planning implementations’, *International Journal of Innovative Science*, 9(2), pp. 166–172.

Belenguer, L. (2022) ‘AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry’, *AI and Ethics*, 2(4), pp. 771–787.

Bhanushali, M.M. *et al.* (2024) ‘From Automation to Optimization: Exploring the Effects of Al on Supply Chain Management’, in *Utilization of AI Technology in Supply Chain Management*. IGI Global, pp. 77–94.

Bharadiya, J.P. (2023) ‘Ai-driven security: How machine learning will shape the future of cybersecurity and web 3.0’, *American Journal of Neural Networks and Applications*, 9(1), pp. 1–7.

Bhardwaj, A.K., Dutta, P.K. and Chintale, P. (2024) 'AI-Powered Anomaly Detection for Kubernetes Security: A Systematic Approach to Identifying Threats', *Babylonian Journal of Machine Learning*, 2024, pp. 142–148.

Bilali, V.-G. *et al.* (2022) 'Iris advanced threat intelligence orchestrator-a way to manage cybersecurity challenges of iot ecosystems in smart cities', in *Global IoT Summit*. Springer, pp. 315–325.

Blum, D. and Blum, D. (2020) 'Institute Resilience Through Detection, Response, and Recovery', *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*, pp. 259–295.

Bouchama, F. and Kamal, M. (2021a) 'Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns', *International Journal of Business Intelligence and Big Data Analytics*, 4(9), pp. 1–9.

Bouchama, F. and Kamal, M. (2021b) 'Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns', *International Journal of Business Intelligence and Big Data Analytics*, 4(9), pp. 1–9.

Braaten, B. *et al.* (2020) 'Accessing complex constructs: Refining an interview protocol', in *2020 IEEE Frontiers in Education Conference (FIE)*, pp. 1–3.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative research in psychology*, 3(2), pp. 77–101.

Brewer, R. (2021) 'Could SOAR save skills-short SOCs?', *https://doi.org/10.1016/S1361-3723(19)30106-X*, 2019(10), pp. 8–11. Available at: https://doi.org/10.1016/S1361-3723(19)30106-X.

Bridges, R.A. *et al.* (2018) 'How do information security workers use host data? a summary of interviews with security analysts', *arXiv preprint arXiv:1812.02867* [Preprint].

Bridges, Robert A *et al.* (2023) 'Testing SOAR tools in use', *Computers & Security*, 129, p. 103201.

Bridges, Robert A. *et al.* (2023) 'Testing SOAR tools in use', *Computers & Security*, 129, p. 103201. Available at: https://doi.org/10.1016/J.COSE.2023.103201.

Brilingaitė, A., Bukauskas, L. and Juozapavičius, A. (2020) ‘A framework for competence development and assessment in hybrid cybersecurity exercises’, *Computers & Security*, 88, p. 101607.

Vom Brocke, J. *et al.* (2020) ‘Special issue editorial–accumulation and evolution of design knowledge in design science research: a journey through time and space’, *Journal of the Association for Information Systems*, 21(3), p. 9.

vom Brocke, J., Hevner, A. and Maedche, A. (2020a) ‘Introduction to Design Science Research’, in J. vom Brocke, A. Hevner, and A. Maedche (eds) *Design Science Research. Cases*. Cham: Springer International Publishing, pp. 1–13. Available at: https://doi.org/10.1007/978-3-030-46781-4_1.

vom Brocke, J., Hevner, A. and Maedche, A. (2020b) ‘Introduction to design science research’, *Design science research. Cases*, pp. 1–13.

Buczak, A.L. and Guven, E. (2016) ‘A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection’, *IEEE Communications Surveys & Tutorials*, 18(2), pp. 1153–1176. Available at: https://doi.org/10.1109/COMST.2015.2494502.

Bukhsh, F.A., Bukhsh, Z.A. and Daneva, M. (2020) ‘A systematic literature review on requirement prioritization techniques and their empirical evaluation’, *Computer Standards & Interfaces*, 69, p. 103389.

Butler, S. *et al.* (2023) ‘On business adoption and use of reproducible builds for open and closed source software’, *Software Quality Journal*, 31(3), pp. 687–719.

Byrne, D. (2022) ‘A worked example of Braun and Clarke’s approach to reflexive thematic analysis’, *Quality & quantity*, 56(3), pp. 1391–1412.

Cadena, A. *et al.* (2020) ‘Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study’, *Smart Innovation, Systems and Technologies*, 152, pp. 507–519. Available at: https://doi.org/10.1007/978-981-13-9155-2_40.

Campbell, S. *et al.* (2020) ‘Purposive sampling: complex or simple? Research case examples’, *Journal of research in Nursing*, 25(8), pp. 652–661.

Casula, M., Rangarajan, N. and Shields, P. (2021) ‘The potential of working hypotheses for deductive exploratory research’, *Quality & Quantity*, 55(5), pp. 1703–1725.

Catal, C. *et al.* (2023) 'Analysis of cyber security knowledge gaps based on cyber security body of knowledge', *Education and Information Technologies*, 28(2), pp. 1809–1831. Available at: https://doi.org/10.1007/s10639-022-11261-8.

Chaganti, R., Ravi, V. and Pham, T.D. (2022) 'Deep learning based cross architecture internet of things malware detection and classification', *Computers & Security*, 120, p. 102779. Available at: https://doi.org/https://doi.org/10.1016/j.cose.2022.102779.

Chai, C. *et al.* (2023) 'Data Management for Machine Learning: A Survey', *IEEE Transactions on Knowledge and Data Engineering*, 35(5), pp. 4646–4667. Available at: https://doi.org/10.1109/TKDE.2022.3148237.

Chamkar, S.A., Maleh, Y. and Gherabi, N. (2024a) 'Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge', *Journal of Cybersecurity and Privacy*, 4(4), pp. 777–793. Available at: https://doi.org/10.3390/jcp4040036.

Chamkar, S.A., Maleh, Y. and Gherabi, N. (2024b) 'Security Operations Centers: Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge', *Journal of Cybersecurity and Privacy*, 4(4), pp. 777–793. Available at: https://doi.org/10.3390/jcp4040036.

Chandna, V. and Tiwari, P. (2023) 'Cybersecurity and the new firm: surviving online threats', *Journal of Business Strategy*, 44(1), pp. 3–12.

Chandramouli, R., Pinhas, D. and others (2020) 'Security guidelines for storage infrastructure', *NIST Special Publication*, 800, p. 209.

Chandran Sundaramurthy, S. *et al.* (2016) 'Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations', p. 237. Available at: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy (Accessed: 4 June 2023).

Chauhan, M. and Shiaeles, S. (2023) 'An analysis of cloud security frameworks, problems and proposed solutions', *Network*, 3(3), pp. 422–450.

Chidukwani, A., Zander, S. and Koutsakis, P. (2022) 'A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations', *IEEE Access* [Preprint]. Available at: https://doi.org/10.1109/ACCESS.2022.3197899.

Chiesa, M. *et al.* (2021) 'A survey of fast-recovery mechanisms in packet-switched networks', *IEEE Communications Surveys & Tutorials*, 23(2), pp. 1253–1301.

Christen, M., Gordijn, B. and Loi, M. (2020) *The ethics of cybersecurity*. Springer Nature.

Christian, J., Paulino, L. and de Sá, A.O. (2022) 'A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 13620 LNCS, pp. 115–139. Available at: https://doi.org/10.1007/978-3-031-21280-2_7/COVER.

Christian Juan and Paulino, L. and de S.A.O. (2022) 'A Low-Cost and Cloud Native Solution for Security Orchestration, Automation, and Response', in D. and P.V. Su Chunhua and Gritzalis (ed.) *Information Security Practice and Experience*. Cham: Springer International Publishing, pp. 115–139.

Chukwunweike, J.N., Adewale, A.A. and Osamuyi, O. (2024) 'Advanced modelling and recurrent analysis in network security: Scrutiny of data and fault resolution', *World Journal of Advanced Research and Reviews*, 23(2), pp. 2373–2390.

Cinà, A.E. *et al.* (2024) 'Machine learning security against data poisoning: Are we there yet?', *Computer*, 57(3), pp. 26–34.

Cisco (2023) *What Is Endpoint Security? - Cisco*. Available at: https://www.cisco.com/c/en/us/products/security/endpoint-security/index.html (Accessed: 27 August 2023).

Cisco (2024) *Cisco Secure Endpoint (Formerly AMP for Endpoints) - Cisco*. Available at: https://www.cisco.com/site/uk/en/products/security/endpoint-security/secure-endpoint/index.html (Accessed: 27 April 2024).

Creado, Y. and Ramteke, V. (2020) 'Active cyber defence strategies and techniques for banks and financial institutions', *Journal of Financial Crime*, 27(3), pp. 771–780. Available at: https://doi.org/10.1108/JFC-01-2020-0008.

Cremer, F., Sheehan, B., Fortmann, M., Kia, Arash N, *et al.* (2022) 'Cyber risk and cybersecurity: a systematic review of data availability', *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(3), pp. 698–736. Available at: https://doi.org/10.1057/s41288-022-00266-6.

Cremer, F., Sheehan, B., Fortmann, M., Kia, Arash N., *et al.* (2022) 'Cyber risk and cybersecurity: a systematic review of data availability', *The Geneva Papers on Risk and Insurance - Issues and Practice 2022 47:3*, 47(3), pp. 698–736. Available at: https://doi.org/10.1057/S41288-022-00266-6.

Dado, M., Spence, J.R. and Elliot, J. (2023) 'The case of contradictions: How prolonged engagement, reflexive journaling, and observations can contradict qualitative methods', *International Journal of Qualitative Methods*, 22, p. 16094069231189372.

Dang, Q.-V. (2022) 'Enhancing Obfuscated Malware Detection with Machine Learning Techniques', in T.K. Dang, J. Küng, and T.M. Chung (eds) *Future Data and Security Engineering. Big Data, Security and Privacy, Smart City and Industry 4.0 Applications*. Singapore: Springer Nature Singapore, pp. 731–738.

Dang, T.K. *et al.* (2021) 'An elastic data conversion framework: a case study for MySQL and MongoDB', *SN Computer Science*, 2(4), p. 325.

Daniel, B.K. (2019) 'Using the TACT framework to learn the principles of rigour in qualitative research', *Electronic Journal of Business Research Methods*, 17(3), pp. pp118–129.

Danquah, P. (2020) 'Security operations center: a framework for automated triage, containment and escalation', *Journal of Information Security*, 11(4), pp. 225–240.

Das, R. and Sandhane, R. (2021) 'Artificial intelligence in cyber security', in *Journal of Physics: Conference Series*, p. 42072.

Datta, J. *et al.* (2021) 'Real-time threat detection in ueba using unsupervised learning algorithms', in *2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)*, pp. 1–6.

Dawadi, S., Shrestha, S. and Giri, R.A. (2021) 'Mixed-methods research: A discussion on its types, challenges, and criticisms', *Journal of Practical Studies in Education*, 2(2), pp. 25–36.

Demertzis, K. *et al.* (2019a) 'The next generation cognitive security operations center: adaptive analytic lambda architecture for efficient defense against adversarial attacks', *Big Data and Cognitive Computing*, 3(1), p. 6.

Demertzis, K. *et al.* (2019b) 'The next generation cognitive security operations center: adaptive analytic lambda architecture for efficient defense against adversarial attacks', *Big Data and Cognitive Computing*, 3(1), p. 6.

Demertzis, K. *et al.* (2021) 'Blockchained adaptive federated auto metalearning BigData and DevOps CyberSecurity Architecture in Industry 4.0', in *International Conference on Engineering Applications of Neural Networks*, pp. 345–363.

Deng Junhua and Zhao, L. and Y.X. and T.Z. and G.Q. (2021) 'Research on the Role-Based Access Control Model and Data Security Method', in T. and K.M.K. Tian Yuan and Ma (ed.) *Big Data and Security*. Singapore: Springer Singapore, pp. 86–96.

Depassier, V. and Torres, R. (2023) 'A human-centric cyber security training tool for prioritizing MSNAs', in *2023 38th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW)*, pp. 54–61.

Deshpande, D.S. *et al.* (2024) 'Endpoint Detection and Response System: Emerging Cyber Security Technology', in *The International Conference on Intelligent Systems & Networks*, pp. 202–213.

Despotović, A., Parmaković, A. and Miljković, M. (2023) 'Cybercrime and cyber security in fintech', in *Digital transformation of the financial industry: approaches and applications*. Springer, pp. 255–272.

Dewa, Z. and Maglaras, L.A. (2016) 'Data Mining and Intrusion Detection Systems', *IJACSA) International Journal of Advanced Computer Science and Applications*, 7(1). Available at: www.ijacsa.thesai.org (Accessed: 19 June 2023).

Dimov, D., Maula, M. and Romme, A.G.L. (2023) 'Crafting and assessing design science research for entrepreneurship', *Entrepreneurship Theory and Practice*. SAGE Publications Sage CA: Los Angeles, CA, pp. 1543–1567.

Djenna, A., Harous, S. and Saidouni, D.E. (2021) 'Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure', *Applied Sciences*, 11(10), p. 4580.

Douaioui, K. *et al.* (2024) 'Machine Learning and Deep Learning Models for Demand Forecasting in Supply Chain Management: A Critical Review', *Applied System Innovation*, 7(5). Available at: https://doi.org/10.3390/asi7050093.

Duary, S. *et al.* (2024) ‘Cybersecurity threats detection in intelligent networks using predictive analytics approaches’, in *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, pp. 1–5.

Duggineni, S. (2023) ‘Impact of controls on data integrity and information systems’, *Science and Technology*, 13(2), pp. 29–35.

Dursun, T. and Üstündağ, B.B. (2021) ‘A novel framework for policy based on-chain governance of blockchain networks’, *Information Processing & Management*, 58(4), p. 102556.

Dykstra, J. *et al.* (2023) ‘Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments’, *Journal of Cybersecurity*, 9(1), p. tyad003.

Eghbal, N. (2020) *Working in public: the making and maintenance of open source software*. Stripe Press.

Ekundayo, F. *et al.* (2024) ‘Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning’, *Int J Res Publ Rev*, 5(11), pp. 1–15.

Elastic Elasticsearch Guide (2024) *REST APIs | Elasticsearch Guide [8.17] | Elastic*. Available at: https://www.elastic.co/guide/en/elasticsearch/reference/current/rest-apis.html (Accessed: 23 February 2025).

Elastic Kibana Guide (2024) *Anomaly detection | Kibana Guide [8.17] | Elastic*. Available at: https://www.elastic.co/guide/en/kibana/current/xpack-ml-anomalies.html (Accessed: 23 February 2025).

Empl, P. *et al.* (2022) ‘SOAR4IoT: Securing IoT Assets with Digital Twins’, p. 10. Available at: https://doi.org/10.1145/3538969.3538975.

Evans, B. (2020) ‘Access Control’, in *Implementing Information Security in Healthcare*. HIMSS Publishing, pp. 75–90.

Exabeam (2023) *A SIEM Security Primer: Evolution and Next-Gen Capabilities*. Available at: https://www.exabeam.com/explainers/siem/a-siem-security-primer/ (Accessed: 28 May 2023).

Falowo, O.I. *et al.* (2024) ‘Evolving Malware and DDoS Attacks: Decadal Longitudinal Study’, *IEEE Access*, 12, pp. 39221–39237. Available at: https://doi.org/10.1109/ACCESS.2024.3376682.

Fan, W. and Geerts, F. (2022) *Foundations of data quality management*. Springer Nature.

Farayola, O.A. (2024) 'Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity', *Finance & Accounting Research Journal*, 6(4), pp. 501–514.

Fernandez, R. *et al.* (2023) 'Effective Collaboration in the Management of Access Control Policies: A Survey of Tools', *IEEE Access*, 11, pp. 13929–13947. Available at: https://doi.org/10.1109/ACCESS.2023.3242863.

Ferreira, J.M. *et al.* (2020) 'Impact of usability mechanisms: An experiment on efficiency, effectiveness and user satisfaction', *Information and Software Technology*, 117, p. 106195.

Fischer-Hübner, S. *et al.* (2021) 'Stakeholder perspectives and requirements on cybersecurity in Europe', *Journal of information security and applications*, 61, p. 102916.

Fisk, N., Kelly, N.M. and Liebrock, L. (2023) 'Cybersecurity communities of practice: Strategies for creating gateways to participation', *Computers & Security*, 132, p. 103188.

Forrester Study (2020) *Forrester Study: The 2020 State of Security Operations*. Available at: https://www.paloaltonetworks.com/blog/2020/09/state-of-security-operations/ (Accessed: 23 June 2024).

Forsberg, J. and Frantti, T. (2023) 'Technical performance metrics of a security operations center', *Computers & Security*, 135, p. 103529.

'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1' (2018). Available at: https://doi.org/10.6028/NIST.CSWP.04162018.

Franchina, L. *et al.* (2021) 'Passive and active training approaches for critical infrastructure protection', *International Journal of Disaster Risk Reduction*, 63, p. 102461. Available at: https://doi.org/10.1016/J.IJDRR.2021.102461.

Frati, F. *et al.* (2024) 'Cybersecurity training and healthcare: the AERAS approach', *International Journal of Information Security*, 23(2), pp. 1527–1539. Available at: https://doi.org/10.1007/s10207-023-00802-y.

Fujs, D., Mihelič, A. and Vrhovec, S.L.R. (2019) 'The power of interpretation: Qualitative methods in cybersecurity research', in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–10.

Furdek, M. *et al.* (2021) ‘Optical network security management: requirements, architecture, and efficient machine learning models for detection of evolving threats’, *Journal of Optical Communications and Networking*, 13(2), pp. A144–A155.

Galdi, E. *et al.* (2022a) ‘ThePhish: an Automated Open-Source Phishing Email Analysis Platform.’, in *ITASEC*, pp. 76–101.

Galdi, E. *et al.* (2022b) ‘ThePhish: an Automated Open-Source Phishing Email Analysis Platform.’, in *ITASEC*, pp. 76–101.

Garai, S. and others (2024) ‘Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers’, *Blockchain in Healthcare Today*, 7(1).

Garcia, S., Parmisano, A. and Erquiaga, M.J. (2020) ‘IoT-23: A labeled dataset with malicious and benign IoT network traffic’, *Stratosphere Lab., Praha, Czech Republic, Tech. Rep* [Preprint].

Gartner (2024) *Gartner Analysis of Security Operations Centers (SOCs) in 2024* -. Available at: https://cyberstrategyinstitute.com/gartner-analysis-of-security-operations-centers-socs-in-2024-understanding-the-hype-cycle-for-security-operations/?form=MG0AV3 (Accessed: 19 February 2025).

Gasiba, T.E., Lechner, U. and Pinto-Albuquerque, M. (2020) ‘Cybersecurity Challenges in Industry: Measuring the Challenge Solve Time to Inform Future Challenges’, *Information 2020, Vol. 11, Page 533*, 11(11), p. 533. Available at: https://doi.org/10.3390/INFO11110533.

Geach, D. (2021) ‘Grid cyber security: secure by design, continuous threat monitoring, effective incident response and board oversight’, *Network Security*, 2021(6), pp. 9–12.

George, A.S. *et al.* (2023) ‘Extending detection and response: how MXDR evolves cybersecurity’, *Partners Universal International Innovation Journal*, 1(4), pp. 268–285.

George, A.S. (2024) ‘Consequences of Enterprise Cloud Migration on Institutional Information Technology Knowledge’, *Partners Universal Innovative Research Publication*, 2(2), pp. 38–55.

GEORGE, D.A.S. *et al.* (2021a) ‘Xdr: The evolution of endpoint security solutions-superior extensibility and analytics to satisfy the organizational needs of the future’,

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 8(1), pp. 493–501.

GEORGE, D.A.S. *et al.* (2021b) 'XDR: The Evolution of Endpoint Security Solutions-Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future', *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 8(1), pp. 493–501.

Ghadermazi, J., Shah, A. and Jajodia, S. (2024) 'A machine learning and optimization framework for efficient alert management in a cybersecurity operations center', *Digital Threats: Research and Practice*, 5(2), pp. 1–23.

Ghelani, D. (2022) 'Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review', *Authorea Preprints*, 3(6), pp. 12–19. Available at: https://doi.org/10.22541/AU.166385207.73483369/V1.

Ghillani, D. (2022) 'Deep learning and artificial intelligence framework to improve the cyber security', *Authorea Preprints* [Preprint].

Gittins, Z. and Soltys, M. (2020) 'Malware persistence mechanisms', *Procedia Computer Science*, 176, pp. 88–97.

Gómez, G. *et al.* (2021) 'Cybersecurity architecture functional model for cyber risk reduction in IoT based wearable devices', in *2021 Congreso Internacional de Innovación y Tendencias en Ingenier\'\ia (CONIITI)*, pp. 1–4.

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021a) 'Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures', *Sensors*, 21(14), p. 4759.

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

GOV.UK (2023) *Cyber security skills in the UK labour market 2023 - GOV.UK*. Available at: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2023 (Accessed: 23 June 2024).

Gregor, S. and Hevner, A.R. (2013) 'Positioning and presenting design science research for maximum impact', *MIS quarterly*, pp. 337–355.

Grigaliūnas, Š. *et al.* (2024) ‘Holistic Information Security Management and Compliance Framework’, *Electronics*, 13(19). Available at: https://doi.org/10.3390/electronics13193955.

Grobler, M., Gaire, R. and Nepal, S. (2021) ‘User, usage and usability: Redefining human centric cyber security’, *Frontiers in big Data*, 4, p. 583723.

Groenewegen, A. and Janssen, J.S. (2021) ‘TheHive Project: The maturity of an open-source Security Incident Response platform’.

Guembe, B. *et al.* (2022) ‘The Emerging Threat of Ai-driven Cyber Attacks: A Review’, *Applied Artificial Intelligence*, 36(1), p. 2037254. Available at: https://doi.org/10.1080/08839514.2022.2037254.

Gupta, R. and Bassett, S. (2024) *Security Monitoring with Wazuh: A hands-on guide to effective enterprise security using real-life use cases in Wazuh*. Packt Publishing. Available at: http://ieeexplore.ieee.org/document/10769327.

Gutta, L.M. (2023) ‘Achieving Operational Excellence in Cloud Management: Practical Evaluation of Infrastructure as Code and the Well-Architected Framework’s Adoption to Improve Process Maturity’, *International Journal of Managment Education for Sustainable Development*, 6(6), pp. 1–19.

Haber, M.J. *et al.* (2020) ‘Indicators of compromise’, *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*, pp. 103–105.

Haider, S. *et al.* (2023) ‘Risk Factors and Practices for the Development of Open Source Software From Developers’ Perspective’, *IEEE Access*, 11, pp. 63333–63350.

Hajny, J. *et al.* (2021a) ‘Framework, tools and good practices for cybersecurity curricula’, *IEEE Access*, 9, pp. 94723–94747.

Hajny, J. *et al.* (2021b) ‘Framework, tools and good practices for cybersecurity curricula’, *IEEE Access*, 9, pp. 94723–94747.

Hansen, M.R.P. and Haj-Bolouri, A. (2020) ‘Design principles exposition: a framework for problematizing knowledge and practice in DSR’, in *Designing for Digital Transformation. Co-Creating Services with Citizens and Industry: 15th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2020, Kristiansand, Norway, December 2–4, 2020, Proceedings 15*, pp. 171–182.

Hartmann, K. and Steup, C. (2020) ‘Hacking the AI-the next generation of hijacked systems’, in *2020 12th International Conference on Cyber Conflict (CyCon)*, pp. 327–349.

Hasan, S. *et al.* (2021) ‘Evaluating the cyber security readiness of organizations and its influence on performance’, *Journal of Information Security and Applications*, 58, p. 102726.

Hashmi, E., Yamin, M.M. and Yayilgan, S.Y. (2024) ‘Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security’, *AI and Ethics* [Preprint]. Available at: https://doi.org/10.1007/s43681-024-00529-z.

Hassan, S.K. and Ibrahim, A. (2023) ‘The role of artificial intelligence in cyber security and incident response’, *International Journal for Electronic Crime Investigation*, 7(2).

Hatzivasilis, G. *et al.* (2020) ‘Modern aspects of cyber-security training and continuous adaptation of programmes to trainees’, *Applied Sciences*, 10(16), p. 5702.

Hernández-Rivas, A., Morales-Rocha, V. and Sánchez-Sol\’\is, J.P. (2024) ‘Towards autonomous cybersecurity: A comparative analysis of agnostic and hybrid AI approaches for advanced persistent threat detection’, in *Innovative Applications of Artificial Neural Networks to Data Analytics and Signal Processing*. Springer, pp. 181–219.

Hettema, H. (2021) ‘Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence’, *Computers & Security*, 109, p. 102396.

Hevner, A. and Chatterjee, S. (2010) *Design research in information systems. Theory and practice*. Springer.

Hevner, A. and Gregor, S. (2022) ‘Envisioning entrepreneurship and digital innovation through a design science research lens: A matrix approach’, *Information & Management*, 59(3), p. 103350.

Hevner, Alan R. *et al.* (2004) ‘Design science in information systems research’, *MIS Quarterly: Management Information Systems*, 28(1). Available at: https://doi.org/10.2307/25148625.

Hevner, Alan R *et al.* (2004) ‘Design Science in Information Systems Research’, *MIS Quarterly*, 28(1), pp. 75–105. Available at: http://www.jstor.org/stable/25148625.

Hevner, A.R. and Storey, V.C. (2021) ‘Externalities of design science research: preparation for project success’, in *The Next Wave of Sociotechnical Design: 16th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2021, Kristiansand, Norway, August 4–6, 2021, Proceedings 16*, pp. 118–130.

Holland, M.C. and Burchell, J. (2022) ‘Low Resource Availability and the Small-to Medium-sized Retail Enterprise’s Ability to Implement an Information Security Strategy’, *Business Management Research and Applications: A Cross-Disciplinary Journal*, 1(2), pp. 48–76.

Holtkamp, P., Soliman, W. and Siponen, M. (2019) ‘Reconsidering the role of research method guidelines for qualitative, mixed-methods, and design science research’, in *Proceedings of the Annual Hawaii International Conference on System Sciences*.

Hossain, S., Sarma, D. and Chakma, R.J. (2020) ‘Machine learning-based phishing attack detection’, *International Journal of Advanced Computer Science and Applications*, 11(9).

Husák, M., Laštovička, M. and Tovar\v{n}ák, D. (2021) ‘System for continuous collection of contextual information for network security management and incident handling’, in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pp. 1–8.

Hussein, M.A. and Hamza, E.K. (2022) ‘Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM).’, *International Journal of Intelligent Engineering & Systems*, 15(6).

Hwoij, A., Khamaiseh, A. har and Ababneh, M. (2021) ‘SIEM architecture for the Internet of Things and smart city’, in *International Conference on Data Science, E-learning and Information Systems 2021*, pp. 147–152.

IBM (2023a) *What is Security Information and Event Management (SIEM)? | IBM*. Available at: https://www.ibm.com/topics/siem (Accessed: 29 May 2023).

IBM (2023b) *What is SOAR (security orchestration, automation and response)? | IBM*. Available at: https://www.ibm.com/topics/security-orchestration-automation-response (Accessed: 29 May 2023).

IBM Resilient (2024) *Plug into the Power of Intelligent Orchestration*. Available at: https://www.ibm.com/support/pages/resilient (Accessed: 27 April 2024).

IBRAHIM, A. (2022) ‘Guardians of the Virtual Gates: Unleashing AI for Next-Gen Threat Detection in Cybersecurity’.

Iglesias, F. *et al.* (2020) ‘NTARC: A Data Model for the Systematic Review of Network Traffic Analysis Research’, *Applied Sciences*, 10(12). Available at: https://doi.org/10.3390/app10124307.

Ilca, L.F., Lucian, O.P. and Balan, T.C. (2023a) ‘Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response’, *Sensors*, 23(15), p. 6757.

Ilca, L.F., Lucian, O.P. and Balan, T.C. (2023b) ‘Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with Prescriptive Malware Analysis, Detection and Response’, *Sensors*, 23(15), p. 6757.

Irfan, M. *et al.* (2023) ‘Critical Success Factors and Challenges in Adopting Digital Transformation in the Saudi Ministry of Education’, *Sustainability 2023, Vol. 15, Page 15492*, 15(21), p. 15492. Available at: https://doi.org/10.3390/SU152115492.

Islam, C., Babar, M.A. and Nepal, S. (2019) ‘A multi-vocal review of security orchestration’, *ACM Computing Surveys (CSUR)*, 52(2), pp. 1–45.

Islam, C., Babar, M.A. and Nepal, S. (2020) ‘Architecture-Centric Support for Integrating Security Tools in a Security Orchestration Platform’, in A. Jansen et al. (eds) *Software Architecture*. Cham: Springer International Publishing, pp. 165–181.

Islam, M.A. (2023) ‘Application of artificial intelligence and machine learning in security operations center’, *Issues in Information Systems*, 24(4).

Islam, S., Hayat, M.A. and Hossain, M.F. (2023) ‘ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: IMPACT, LIMITATIONS AND FUTURE RESEARCH DIRECTIONS’.

Islam, S.A., Mohankumar, M. and Jannat, U.K. (2023) ‘Exploring the Effectiveness of Web Application Firewalls Against Diverse Attack Vectors’, *7th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2023 - Proceedings*, pp. 1798–1806. Available at: https://doi.org/10.1109/ICECA58529.2023.10395379.

Jabar, T. and Mahinderjit Singh, M. (2022) ‘Exploration of mobile device behavior for mitigating advanced persistent threats (APT): a systematic literature review and conceptual framework’, *Sensors*, 22(13), p. 4662.

Jarrett, A. and Choo, K.-K.R. (2021) ‘The impact of automation and artificial intelligence on digital forensics’, *Wiley Interdisciplinary Reviews: Forensic Science*, 3(6), p. e1418. Available at: https://doi.org/10.1002/WFS2.1418.

Javaid, M. *et al.* (2023) ‘Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends’, *Cyber Security and Applications*, p. 100016.

Jeong, J.J. *et al.* (2021) ‘The current state of research on people, culture and cybersecurity’. Springer.

Jhaveri, M. and Parmar, V. (2023) *(PDF) CLOUD Security Information and Event Management*. Available at: https://www.researchgate.net/publication/369302413_CLOUD_Security_Information_and_Event_Management (Accessed: 28 May 2023).

Johannesson, P. and Perjons, E. (2021a) ‘A Method Framework for Design Science Research’, in P. Johannesson and E. Perjons (eds) *An Introduction to Design Science*. Cham: Springer International Publishing, pp. 77–93. Available at: https://doi.org/10.1007/978-3-030-78132-3_4.

Johannesson, P. and Perjons, E. (2021b) *An Introduction to Design Science*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-030-78132-3.

Johnson, J. *et al.* (2023) ‘SOAR4DER: Security Orchestration, Automation, and Response for Distributed Energy Resources’, pp. 387–411. Available at: https://doi.org/10.1007/978-3-031-20360-2_16/COVER.

Joseph, A. (2023) ‘A Holistic Framework for Unifying Data Security and Management in Modern Enterprises’, *International Journal of Social and Business Sciences*, 17(10), pp. 602–609.

K, M.S.K. *et al.* (2024) ‘Suricata-Based Intrusion Detection and Isolation System for Local Area Networks’, in *2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT)*, pp. 1–5. Available at: https://doi.org/10.1109/IConSCEPT61884.2024.10627890.

Kaleem, Y. (2022) *Cyber Security Framework for Real-time Malicious Network Traffic Detection and Prevention using SIEM and Deep Learning*. National University of Sciences and Technology.

Kaliyaperumal, L.N. (2021) *The Evolution of Security Operations and Strategies for Building an Effective SOC*. Available at: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc (Accessed: 22 May 2023).

Kalogiannidis, S. *et al.* (2024) 'The role of artificial intelligence technology in predictive risk assessment for business continuity: A case study of Greece', *Risks*, 12(2), p. 19.

Kaloudi, N. and Li, J. (2020) 'The ai-based cyber threat landscape: A survey', *ACM Computing Surveys (CSUR)*, 53(1), pp. 1–34.

Kamolsin, C. *et al.* (2022) 'The Evaluation of GUI Design using Questionnaire and Multivariate Testing', in *2022 Research, Invention, and Innovation Congress: Innovative Electricals and Electronics (RI2C)*, pp. 191–195.

Kanaan, A. *et al.* (2024) 'Cybersecurity resilience for business: a comprehensive model for proactive defense and swift recovery', in *2024 2nd International Conference on Cyber Resilience (ICCR)*, pp. 1–7.

Karantzas, G. and Patsakis, C. (2021) 'An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors', *Journal of Cybersecurity and Privacy*, 1(3), pp. 387–421. Available at: https://doi.org/10.3390/jcp1030021.

Karie, N.M. *et al.* (2021) 'A review of security standards and frameworks for IoT-based smart environments', *IEEE Access*, 9, pp. 121975–121995.

Karim, S.S. *et al.* (2024) 'Advanced Persistent Threat (APT) and intrusion detection evaluation dataset for linux systems 2024', *Data in Brief*, 54, p. 110290.

Karlsen, E. *et al.* (2024) 'Benchmarking Large Language Models for Log Analysis, Security, and Interpretation', *Journal of Network and Systems Management*, 32(3), p. 59. Available at: https://doi.org/10.1007/s10922-024-09831-x.

Kartak, V. and Bashmakov, N. (2022) 'Method for Selecting Indicators of Data Compromise', in *2022 International Siberian Conference on Control and*

Communications (SIBCON), pp. 1–5. Available at: https://doi.org/10.1109/SIBCON56144.2022.10002962.

Kathare, N., Reddy, O.V. and Prabhu, V. (2020a) 'A comprehensive study of Elasticsearch', *International Journal of Science and Research (IJSR)* [Preprint].

Kathare, N., Reddy, O.V. and Prabhu, V. (2020b) 'A comprehensive study of Elasticsearch', *International Journal of Science and Research (IJSR)* [Preprint].

Kaur, G. and Lashkari, A.H. (2021) 'An introduction to security operations', in *Advances in cybersecurity management*. Springer, pp. 463–481.

Kaur, R., Gabrijelčič, D. and Klobučar, T. (2023) 'Artificial intelligence for cybersecurity: Literature review and future research directions', *Information Fusion*, p. 101804.

Kechagias, E.P. *et al.* (2022) 'Digital transformation of the maritime industry: A cybersecurity systemic approach', *International Journal of Critical Infrastructure Protection*, 37, p. 100526.

Khader, M., Karam, M. and Fares, H. (2021) 'Cybersecurity Awareness Framework for Academia', *Information 2021, Vol. 12, Page 417*, 12(10), p. 417. Available at: https://doi.org/10.3390/INFO12100417.

Khan, M. and Ghafoor, L. (2024) 'Adversarial Machine Learning in the Context of Network Security: Challenges and Solutions', *Journal of Computational Intelligence and Robotics*, 4(1), pp. 51–63.

Khan, S.K. *et al.* (2020) 'Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions', *Accident Analysis & Prevention*, 148, p. 105837.

Khan, S.U. *et al.* (2021) 'Challenges and their practices in adoption of hybrid cloud computing: An analytical hierarchy approach', *Security and Communication Networks*, 2021(1), p. 1024139.

Khanan, A. *et al.* (2024) 'From bytes to insights: a systematic literature review on unraveling IDS datasets for enhanced cybersecurity understanding', *IEEE Access* [Preprint].

Kiger, M.E. and Varpio, L. (2020a) ‘Thematic analysis of qualitative data: AMEE Guide No. 131’, *Medical Teacher*, 42(8), pp. 846–854. Available at: https://doi.org/10.1080/0142159X.2020.1755030.

Kiger, M.E. and Varpio, L. (2020b) ‘Thematic analysis of qualitative data: AMEE Guide No. 131’, *Medical teacher*, 42(8), pp. 846–854.

Kinyua, J. and Awuah, L. (2021) ‘AI/ML in Security Orchestration, Automation and Response: Future Research Directions’, *Intelligent Automation & Soft Computing*, 28(2), pp. 527–545. Available at: https://doi.org/10.32604/IASC.2021.016240.

Kitsios, F., Chatzidimitriou, E. and Kamariotou, M. (2023) ‘The ISO/IEC 27001 Information security management standard: how to extract value from data in the IT sector’, *Sustainability*, 15(7), p. 5828.

Koloveas, P. *et al.* (2021) ‘intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence’, *Electronics*, 10(7), p. 818.

Koroniotis, N. *et al.* (2020) ‘A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports’, *IEEE Access*, 8, pp. 209802–209834. Available at: https://doi.org/10.1109/ACCESS.2020.3036728.

Kozubtsov, I. *et al.* (2024) ‘A Method for Calculating Efficiency Indicators of Information Security Systems’, in *2024 35th Conference of Open Innovations Association (FRUCT)*, pp. 388–398.

Krishnan, P. *et al.* (2023) ‘OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure’, *Journal of Cloud Computing*, 12(1), p. 26. Available at: https://doi.org/10.1186/s13677-023-00406-w.

Kroll, J.A., Michael, J.B. and Thaw, D.B. (2021) ‘Enhancing Cybersecurity via Artificial Intelligence: Risks, Rewards, and Frameworks’, *Computer*, 54(6), pp. 64–71. Available at: https://doi.org/10.1109/MC.2021.3055703.

Kumar, P. *et al.* (2023) ‘DLTIF: Deep Learning-Driven Cyber Threat Intelligence Modeling and Identification Framework in IoT-Enabled Maritime Transportation Systems’, *IEEE Transactions on Intelligent Transportation Systems*, 24(2), pp. 2472–2481. Available at: https://doi.org/10.1109/TITS.2021.3122368.

Kumari, S., Tyagi, A.K. and Rekha, G. (2021) ‘Applications of Blockchain Technologies in Digital Forensics and Threat Hunting’, in *Recent Trends in Blockchain for Information Systems Security and Privacy*. CRC Press, pp. 159–173.

Kunduru, A.R. (2023a) ‘Artificial intelligence advantages in cloud Fintech application security’, *Central Asian Journal of Mathematical Theory and Computer Sciences*, 4(8), pp. 48–53.

Kunduru, A.R. (2023b) ‘Industry best practices on implementing oracle cloud ERP security’, *International Journal of Computer Trends and Technology*, 71(6), pp. 1–8.

Kuppingercole (2024) *Advisory Note: Analyst’s View: eXtented Detection and Response (XDR)*. Available at: https://www.kuppingercole.com/research/an81389/analyst-s-view-extented-detection-and-response-xdr?form=MG0AV3 (Accessed: 22 February 2025).

Labu, M.R. and Ahammed, M.F. (2024) ‘Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning’, *Journal of Computer Science and Technology Studies*, 6(1), pp. 179–188.

LaDonna, K.A., Artino Jr, A.R. and Balmer, D.F. (2021) ‘Beyond the guise of saturation: rigor and qualitative interview data’, *Journal of Graduate Medical Education*. The Accreditation Council for Graduate Medical Education, pp. 607–611.

Landauer, M. *et al.* (2023) ‘AMiner: A Modular Log Data Analysis Pipeline for Anomaly-based Intrusion Detection’, *Digital Threats*, 4(1). Available at: https://doi.org/10.1145/3567675.

Laue, T. *et al.* (2021) ‘A SIEM architecture for multidimensional anomaly detection’, in *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 136–142.

Lee, E. *et al.* (2021) ‘A Survey on Standards for Interoperability and Security in the Internet of Things’, *IEEE Communications Surveys & Tutorials*, 23(2), pp. 1020–1047.

Lee, H.-W. (2023) ‘Analysis of Digital Forensic Artifacts Data Enrichment Mechanism for Cyber Threat Intelligence’, in *Proceedings of the 2023 12th International Conference on Software and Computer Applications*, pp. 192–199.

Lee, I. (2021) ‘Cybersecurity: Risk management framework and investment cost analysis’, *Business Horizons* [Preprint].

Lee, M.S.A. and Singh, J. (2021) ‘The landscape and gaps in open source fairness toolkits’, in *Proceedings of the 2021 CHI conference on human factors in computing systems*, pp. 1–13.

Legay, D., Decan, A. and Mens, T. (2020) ‘On Package Freshness in Linux Distributions’, in *2020 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pp. 682–686. Available at: https://doi.org/10.1109/ICSME46990.2020.00072.

Leitner, M., Skopik, F. and Pahi, T. (2024) ‘Operational cyber incident coordination revisited: providing cyber situational awareness across organizations and countries’, *Information Security Journal: A Global Perspective*, pp. 1–22.

Levshun, D. and Kotenko, I. (2023) ‘A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities’, *Artificial Intelligence Review*, 56(8), pp. 8547–8590.

Li, F. *et al.* (2021) ‘Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality’, *Technology in Society*, 64, p. 101487.

Li, L., Huang, C. and Chen, J. (2024) ‘Automated discovery and mapping ATT&CK tactics and techniques for unstructured cyber threat intelligence’, *Computers & Security*, 140, p. 103815.

Li, Y., Nguyen, D. and Xie, M. (2017) ‘Ezsetup: A novel tool for cybersecurity practices utilizing cloud resources’, in *Proceedings of the 18th annual conference on information technology education*, pp. 53–58.

Lin, T. *et al.* (2018) ‘Retrieval of relevant historical data triage operations in security operation centers’, *From Database to Cyber Security: Essays Dedicated to Sushil Jajodia on the Occasion of His 70th Birthday*, pp. 227–243.

Liu, J. *et al.* (2023) ‘Interpreter-Based Secure Centralized Interoperability Method for IoT Devices’, in *2023 IEEE 5th International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, pp. 430–435.

López Velásquez, J.M. *et al.* (2023) ‘Systematic review of SIEM technology: SIEM-SC birth’, *International Journal of Information Security*, pp. 1–21. Available at: https://doi.org/10.1007/S10207-022-00657-9/METRICS.

Macedo, I. *et al.* (2021a) ‘A tool to support the investigation and visualization of cyber and/or physical incidents’, in *World Conference on Information Systems and Technologies*, pp. 130–140.

Macedo, I. *et al.* (2021b) ‘A tool to support the investigation and visualization of cyber and/or physical incidents’, in *World Conference on Information Systems and Technologies*, pp. 130–140.

Maddireddy, Bhargava Reddy and Maddireddy, Bharat Reddy (2021) ‘Evolutionary Algorithms in AI-Driven Cybersecurity Solutions for Adaptive Threat Mitigation’, *International Journal of Advanced Engineering Technologies and Innovations*, 1(2), pp. 17–43. Available at: https://ijaeti.com/index.php/Journal/article/view/319 (Accessed: 8 June 2024).

Madhavram, C. *et al.* (2022) ‘AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance’, *Available at SSRN 5029406* [Preprint].

Madugula, S. *et al.* (2023) ‘Big data for the comprehensive data analysis of IT organizations’, *The Journal of High Technology Management Research*, 34(2), p. 100465.

Magida, A. (2024) ‘The Use of Digital Tools and Emerging Technologies in Qualitative Research—A Systematic Review of Literature’, in J. Ribeiro et al. (eds) *Computer Supported Qualitative Research*. Cham: Springer Nature Switzerland, pp. 257–269.

Mahfouz, A. *et al.* (2020) ‘Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset’, *Future Internet*, 12(11). Available at: https://doi.org/10.3390/fi12110180.

Majid, M.A. and Zainol Ariffin, K.A. (2021) ‘Model for successful development and implementation of Cyber Security Operations Centre (SOC)’. Available at: https://doi.org/10.1371/journal.pone.0260157.

Makani, S.T. and Jangampeta, S. (2024) ‘Devops security tools evaluating effectiveness in detecting and fixing security holes’, *Journal ID*, 1552, p. 5541.

Malatji, M. (2023) ‘Offensive Artificial Intelligence: Current State of the Art and Future Directions’, *2023 International Conference on Digital Applications, Transformation and Economy, ICDATE 2023* [Preprint]. Available at: https://doi.org/10.1109/ICDATE58146.2023.10248780.

Malatji, M. and Tolah, A. (2024a) ‘Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI’, *AI and Ethics 2024*, pp. 1–28. Available at: https://doi.org/10.1007/S43681-024-00427-4.

Malatji, M. and Tolah, A. (2024b) ‘Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI’, *AI and Ethics*, pp. 1–28.

Malatji, M. and Tolah, A. (2024c) ‘Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI’, *AI and Ethics*, pp. 1–28.

Malik, A.W. *et al.* (2024) ‘Cloud digital forensics: Beyond tools, techniques, and challenges’, *Sensors*, 24(2), p. 433.

Mallick, M.A.I. and Nath, R. (2024) ‘Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments’, *World Scientific News*, 190(1), pp. 1–69.

Manchana, R. (2024) ‘AI-Powered Observability: A Journey from Reactive to Proactive, Predictive, and Automated’, *International Journal of Science and Research (IJSR)*, 13(8), pp. 1745–1755.

Manky, D. (2013) ‘Cybercrime as a service: a very modern business’, *Computer Fraud & Security*, 2013(6), pp. 9–13. Available at: https://doi.org/10.1016/S1361-3723(13)70053-8.

Manoharan, A. and Sarker, M. (2023a) ‘Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection’, *DOI: https://www. doi. org/10.56726/IRJMETS32644*, 1.

Manoharan, A. and Sarker, M. (2023b) ‘Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection’, *DOI: https://www. doi. org/10.56726/IRJMETS32644*, 1.

Mansouri, Y., Prokhorenko, V. and Babar, M.A. (2020) ‘An automated implementation of hybrid cloud for performance evaluation of distributed databases’, *Journal of Network and Computer Applications*, 167, p. 102740.

Maosa, H., Ouazzane, K. and Sowinski-Mydlarz, V. (2022) 'Real-time cyber analytics data collection framework', *International Journal of Information Security and Privacy (IJISP)*, 16(1), pp. 1–10.

Marengo, A. (2024) 'Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms', *Internet of Things*, p. 101318.

MarkovML (2024) *Validating Machine Learning Models: A Detailed Overview*. Available at: https://www.markovml.com/blog/ml-model-validation (Accessed: 27 April 2024).

Marru, S. *et al.* (2021) 'User-Centric Design and Evolvable Architecture for Science Gateways: A Case Study', in *2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid)*, pp. 267–276.

Mart\'\in, A.G. *et al.* (2021) 'An approach to detect user behaviour anomalies within identity federations', *computers & security*, 108, p. 102356.

Mart\'\inez-Fernández, S. *et al.* (2020) 'Research directions for developing and operating artificial intelligence models in trustworthy autonomous systems', *arXiv preprint arXiv:2003.05434* [Preprint].

Martins, I. *et al.* (2022) 'Host-based IDS: A review and open issues of an anomaly detection system in IoT', *Future Generation Computer Systems*, 133, pp. 95–113.

Mavrogiorgou, A. *et al.* (2022) 'A catalogue of machine learning algorithms for healthcare risk predictions', *Sensors*, 22(22), p. 8615.

Mccarty, M. *et al.* (2023) 'Cybersecurity Resilience Demonstration for Wind Energy Sites in Co-Simulation Environment', *IEEE Access*, 11, pp. 15297–15313. Available at: https://doi.org/10.1109/ACCESS.2023.3244778.

Mckinsey (2023) *Understanding and mitigating AI risk in services | McKinsey*. Available at: https://www.mckinsey.com/capabilities/operations/our-insights/managing-the-risks-and-returns-of-intelligent-automation (Accessed: 17 June 2023).

McKinsey (2024) *Safeguarding against cyberattack in an increasingly digital world | McKinsey*. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/safeguarding-against-cyberattack-in-an-increasingly-digital-world (Accessed: 27 April 2024).

McLaughlin, K. (2023) ‘INTERWEAVING THE STRANDS OF AI AND SOAR ONTO THE CYBERSECURITY MESH: A DEEP DIVE INTO THE CYBERSECURITY MESH AND ITS ROLE IN MODERN DIGITAL DEFENSE STRATEGIES’, *EDPACS*, pp. 1–7.

McLaughlin, K.L. (2023) ‘DEFENSE IS THE BEST OFFENSE: THE EVOLVING ROLE OF CYBERSECURITY BLUE TEAMS AND THE IMPACT OF SOAR TECHNOLOGIES’, *EDPACS*, pp. 1–7. Available at: https://doi.org/10.1080/07366981.2023.2212484.

Mclaughlin, K.L. and Elliott, E.S.A. (2023) ‘UNLEASHING THE POWER OF MOBILE THREAT HUNTING TOOLKITS: WHY THEY ARE CRUCIAL IN TODAY’S CYBERSECURITY LANDSCAPE’, *EDPACS*, pp. 1–6.

Meydan, C.H. and Akkaş, H. (2024) ‘The role of triangulation in qualitative research: Converging perspectives’, in *Principles of Conducting Qualitative Research in Multicultural Settings*. IGI Global, pp. 98–129.

Michael, K. *et al.* (2019) ‘Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals’, in *2019 IEEE International Symposium on Technology and Society (ISTAS)*, pp. 1–13. Available at: https://doi.org/10.1109/ISTAS48451.2019.8937956.

Microsoft (2023a) *Detect suspicious user activity with UEBA - Microsoft Defender for Cloud Apps | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-suspicious-activity (Accessed: 29 May 2023).

Microsoft (2023b) *Get fine-tuning recommendations for your analytics rules in Microsoft Sentinel | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/azure/sentinel/detection-tuning (Accessed: 29 May 2023).

Microsoft (2023c) *Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics (Accessed: 29 May 2023).

Microsoft (2023d) *Microsoft Sentinel - Cloud SIEM Solution | Microsoft Security*. Available at: https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-sentinel (Accessed: 28 May 2023).

Microsoft (2023e) *Respond to threats in near real-time with custom XDR detections*. Available at: https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/respond-to-threats-in-near-real-time-with-custom-detections/ba-p/3761243 (Accessed: 27 August 2023).

Microsoft (2023f) *Security Operations Center (SOC or SecOps) monitoring in Azure - Microsoft Azure Well-Architected Framework | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/azure/well-architected/security/monitor-security-operations (Accessed: 26 August 2023).

Microsoft (2023g) *What is Incident Response? Plan and Steps | Microsoft Security*. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response (Accessed: 29 May 2023).

Microsoft (2023h) *What is Microsoft Sentinel? | Microsoft Learn*, *Microsoft*. Available at: https://learn.microsoft.com/en-us/azure/sentinel/overview (Accessed: 28 May 2023).

Microsoft (2023i) *What is SIEM? | Microsoft Security*. Available at: https://www.microsoft.com/en-gb/security/business/security-101/what-is-siem (Accessed: 28 May 2023).

Microsoft (2023j) *What Is SOAR? Technology and Solutions | Microsoft Security*. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-soar (Accessed: 29 May 2023).

Microsoft (2024a) *Microsoft Cybersecurity Reference Architectures (MCRA) | Microsoft Learn*. Available at: https://learn.microsoft.com/en-us/security/adoption/mcra (Accessed: 22 February 2025).

Microsoft (2024b) *Microsoft Defender for Office 365 | Microsoft Security*. Available at: https://www.microsoft.com/en-gb/security/business/siem-and-xdr/microsoft-defender-office-365 (Accessed: 27 April 2024).

Microsoft (2024c) *Microsoft Sentinel Simplify security operations with intelligent security analytics and scale as you grow.* Available at: https://azure.microsoft.com/en-gb/products/microsoft-sentinel/ (Accessed: 27 April 2024).

Migliore, G. *et al.* (2022) 'Antecedents to the adoption of mobile payment in China and Italy: An integration of UTAUT2 and innovation resistance theory', *Information Systems Frontiers*, 24(6), pp. 2099–2122.

Mihindu, S. and Khosrow-shahi, F. (2020) ‘Collaborative visualisation embedded cost-efficient, virtualised cyber security operations centre’, in *2020 24th International Conference Information Visualisation (IV)*, pp. 153–159.

Miles, M.B., Huberman, A.M. and Saldaña, J. (2021) ‘Qualitative data analysis: a methods sourcebook. Cetakan III’. New York: SAGE. Diakses pada.

Miloslavskaya, N. (2016) ‘Security Operations Centers for Information Security Incident Management’, in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 131–136. Available at: https://doi.org/10.1109/FiCloud.2016.26.

Mir Abdul Wahid and Ramachandran, R.K. (2021) ‘Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems’, in B.K. and D.S. Dash Subhransu Sekhar and Panigrahi (ed.) *Sixth International Conference on Intelligent Computing and Applications* . Singapore: Springer Singapore, pp. 157–169.

Mishra, S. *et al.* (2023) ‘Using security metrics to determine security program effectiveness’, *Human Factors in Cybersecurity*, 91(91).

Mishra, S. and Tyagi, A.K. (2022) ‘The role of machine learning techniques in internet of things-based cloud applications’, *Artificial intelligence-based internet of things systems*, pp. 105–135.

MISP (2023) *MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing*. Available at: https://www.misp-project.org/ (Accessed: 28 August 2023).

MITRE ATT&CK (2023) *Scheduled Task/Job: Scheduled Task, Sub-technique T1053.005 - Enterprise | MITRE ATT&CK®*. Available at: https://attack.mitre.org/techniques/T1053/005/ (Accessed: 30 January 2024).

Mohammad, S.M. and Surya, L. (2018) ‘Security automation in Information technology’, *INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)–Volume*, 6.

Moiz, S. *et al.* (2024a) ‘Security and Threat Detection through Cloud-Based Wazuh Deployment’, in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, pp. 1–5.

Moiz, S. *et al.* (2024b) ‘Security and Threat Detection through Cloud-Based Wazuh Deployment’, in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, pp. 1–5.

Mokaddem, S. *et al.* (2019) ‘Taxonomy driven indicator scoring in MISP threat intelligence platforms’, *arXiv preprint arXiv:1902.03914* [Preprint].

Möller, D.P.F. (2023a) ‘NIST cybersecurity framework and MITRE cybersecurity criteria’, in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*. Springer, pp. 231–271.

Möller, D.P.F. (2023b) ‘Threats and threat intelligence’, in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*. Springer, pp. 71–129.

Mughal, A.A. (2019) ‘Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges’, *Applied Research in Artificial Intelligence and Cloud Computing*, 2(1), pp. 1–31.

Mughal, A.A. (2022a) ‘Building and Securing the Modern Security Operations Center (SOC)’, *International Journal of Business Intelligence and Big Data Analytics*, 5(1), pp. 1–15. Available at: https://research.tensorgate.org/index.php/IJBIBDA/article/view/21.

Mughal, A.A. (2022b) ‘Building and Securing the Modern Security Operations Center (SOC)’, *International Journal of Business Intelligence and Big Data Analytics*, 5(1), pp. 1–15.

Muhammad, A.R., Sukarno, P. and Wardana, A.A. (2023) ‘Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning’, *Procedia Computer Science*, 217, pp. 1406–1415. Available at: https://doi.org/https://doi.org/10.1016/j.procs.2022.12.339.

Muhammad, R., Ismail, S.A. and Hassan, N.H. (2024) ‘Botnet Detection and Incident Response in Security Operation Center (SOC): A Proposed Framework.’, *International Journal of Advanced Computer Science & Applications*, 15(3).

Muhammad, T. (2022) ‘A Comprehensive Study on Software-Defined Load Balancers: Architectural Flexibility & Application Service Delivery in On-Premises Ecosystems’, *International Journal of Computer Science and Technology*, 6(1), pp. 1–24.

Mukherjee, M. *et al.* (2024) ‘Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes’, *Information*, 15(2). Available at: https://doi.org/10.3390/info15020117.

Mulyadi, F. *et al.* (2020) ‘Implementing Dockerized Elastic Stack for Security Information and Event Management’, in *2020-5th International Conference on Information Technology (InCIT)*, pp. 243–248.

Mushtaq, M.S. *et al.* (2022) ‘Security, integrity, and privacy of cloud computing and big data’, in *Security and privacy trends in cloud computing and big data*. CRC Press, pp. 19–51.

Mutalib, N.H.A. *et al.* (2024a) ‘Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review’, *Artificial Intelligence Review*, 57(11), p. 297.

Mutalib, N.H.A. *et al.* (2024b) ‘Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review’, *Artificial Intelligence Review*, 57(11), p. 297. Available at: https://doi.org/10.1007/s10462-024-10890-4.

Myers, M.D. (2019) ‘Qualitative research in business and management’.

Nadella, G.S. and Gonaygunta, H. (2024) ‘Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT’. DOI.

Najafi, P., Cheng, F. and Meinel, C. (2021) ‘SIEMA: Bringing Advanced Analytics to Legacy Security Information and Event Management’, in *Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6–9, 2021, Proceedings, Part I 17*, pp. 25–43.

Najafi Pejman and Cheng, F. and M.C. (2021) ‘SIEMA: Bringing Advanced Analytics to Legacy Security Information and Event Management’, in S. and P.R. and D.H. and Y.M. Garcia-Alfaro Joaquin and Li (ed.) *Security and Privacy in Communication Networks*. Cham: Springer International Publishing, pp. 25–43.

Nascimento, B. *et al.* (2024) ‘Availability, Scalability, and Security in the Migration from Container-Based to Cloud-Native Applications’, *Computers*, 13(8). Available at: https://doi.org/10.3390/computers13080192.

Naseer, A. *et al.* (2021) 'Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis', *International Journal of Information Management*, 59, p. 102334.

Naseer, H. *et al.* (2024) 'Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics', *European Journal of Information Systems*, 33(2), pp. 200–220.

Naseer, U. *et al.* (2020) 'Zero downtime release: Disruption-free load balancing of a multi-billion user website', in *Proceedings of the Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication*, pp. 529–541.

Nassar, A. and Kamal, M. (2021a) 'Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies', *Journal of Artificial Intelligence and Machine Learning in Management*, 5(1), pp. 51–63.

Nassar, A. and Kamal, M. (2021b) 'Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies', *Journal of Artificial Intelligence and Machine Learning in Management*, 5(1), pp. 51–63.

Nassar, A. and Kamal, M. (2021c) 'Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies', *Journal of Artificial Intelligence and Machine Learning in Management*, 5(1), pp. 51–63.

Nazir, A. *et al.* (2024) 'Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration', *Journal of King Saud University-Computer and Information Sciences*, p. 101939.

Negoita, O. and Carabas, M. (2020a) 'Enhanced security using elasticsearch and machine learning', in *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3*, pp. 244–254.

Negoita, O. and Carabas, M. (2020b) 'Enhanced security using elasticsearch and machine learning', in *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3*, pp. 244–254.

Negoita, O. and Carabas, M. (2020c) 'Enhanced security using elasticsearch and machine learning', in *Intelligent Computing: Proceedings of the 2020 Computing Conference, Volume 3*, pp. 244–254.

Nemec Zlatolas, L., Welzer, T. and Lhotska, L. (2024) ‘Data breaches in healthcare: security mechanisms for attack mitigation’, *Cluster Computing*, 27(7), pp. 8639–8654. Available at: https://doi.org/10.1007/s10586-024-04507-2.

Ness, S., Rangaraju, S. and Dharmalingam, R. (2023) ‘Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security Product Security Leader at Pure Storage’, *Article in International Journal of Innovative Science and Research Technology*, 8(11). Available at: https://doi.org/10.5281/zenodo.10361289.

Ng, K.K.H. *et al.* (2021) ‘A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives’, *Advanced Engineering Informatics*, 47, p. 101246. Available at: https://doi.org/10.1016/J.AEI.2021.101246.

Nguyen, A. *et al.* (2021) ‘Design principles for learning analytics information systems in higher education’, *European Journal of Information Systems*, 30(5), pp. 541–568.

Nguyen, M.-D. *et al.* (2024) ‘AI4SOAR: A Security Intelligence Tool for Automated Incident Response’, in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, pp. 1–8.

Nicholls, M. (2023) *What is SOAR? (Security Orchestration, Automation and Response) | Redscan*. Available at: https://www.redscan.com/news/what-is-security-orchestration-automation-and-response-soar-and-how-does-it-improve-threat-detection-and-remediation/ (Accessed: 10 June 2023).

Nifakos, S. *et al.* (2021) ‘Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review’, *Sensors 2021, Vol. 21, Page 5119*, 21(15), p. 5119. Available at: https://doi.org/10.3390/S21155119.

Di Nocera, F., Tempestini, G. and Orsini, M. (2023) ‘Usable Security: A Systematic Literature Review’, *Information (Switzerland)*. Multidisciplinary Digital Publishing Institute (MDPI). Available at: https://doi.org/10.3390/info14120641.

Noor, U. *et al.* (2019) ‘A machine learning framework for investigating data breaches based on semantic analysis of adversary’s attack patterns in threat intelligence repositories’, *Future Generation Computer Systems*, 95, pp. 467–487. Available at: https://doi.org/10.1016/j.future.2019.01.022.

Nour, B., Pourzandi, M. and Debbabi, M. (2023a) ‘A Survey on Threat Hunting in Enterprise Networks’, *IEEE Communications Surveys & Tutorials*, p. 1. Available at: https://doi.org/10.1109/COMST.2023.3299519.

Nour, B., Pourzandi, M. and Debbabi, M. (2023b) ‘A survey on threat hunting in enterprise networks’, *IEEE communications surveys & tutorials*, 25(4), pp. 2299–2324.

Nova, K. (2022) ‘Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence’, *International Journal of Information and Cybersecurity*, 6(1), pp. 21–42. Available at: https://publications.dlpress.org/index.php/ijic/article/view/28 (Accessed: 21 May 2024).

Nozari, H., Ghahremani-Nahr, J. and Szmelter-Jarosz, A. (2024) ‘AI and machine learning for real-world problems’, in *Advances In Computers*. Elsevier, pp. 1–12.

Ntoa, S. (2024) ‘Usability and user experience evaluation in intelligent environments: a review and reappraisal’, *International Journal of Human–Computer Interaction*, pp. 1–30.

Nwosu, N.T. (2024) ‘Reducing operational costs in healthcare through advanced BI tools and data integration’, *World Journal of Advanced Research and Reviews*, 22(3), pp. 1144–1156.

Nyangaresi, V.O. (2022) ‘Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography’, *Journal of Systems Architecture*, 133, p. 102763.

Nyirenda, L. *et al.* (2020) ‘Using research networks to generate trustworthy qualitative public health research findings from multiple contexts’, *BMC Medical Research Methodology*, 20, pp. 1–10.

Nyre-Yu, M., Gutzwiller, R.S. and Caldwell, B.S. (2019) ‘Observing Cyber Security Incident Response: Qualitative Themes From Field Research’, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 63(1), pp. 437–441. Available at: https://doi.org/10.1177/1071181319631016.

Ofoegbu, K.D.O. *et al.* (2024) ‘Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols’, *Computer Science & IT Research Journal*, 5(8).

Olaoye, F. and Potter, K. (2024) *Enterprise Resource Planning (ERP) Systems*.

Olateju, O. *et al.* (2024) ‘Combating the challenges of false positives in AI-driven anomaly detection systems and enhancing data security in the cloud’, *Available at SSRN 4859958* [Preprint].

Oltsik Jon (2018) *The rise of analyst-centric security operations technologies | CSO Online*. Available at: https://www.csoonline.com/article/3276463/the-rise-of-analyst-centric-security-operations-technologies.html (Accessed: 4 June 2023).

Olukoya, O. (2021) ‘Distilling blockchain requirements for digital investigation platforms’, *Journal of Information Security and Applications*, 62, p. 102969.

Ongun, T. *et al.* (2021) ‘Collaborative information sharing for ml-based threat detection’, *arXiv preprint arXiv:2104.11636* [Preprint].

Onwubiko, C. and Ouazzane, K. (2019) ‘Cyber onboarding is “broken”’, in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pp. 1–13.

Van Oordt, S. and Guzman, E. (2021) ‘On the role of user feedback in software evolution: a practitioners’ perspective’, in *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pp. 221–232.

Or-Meir, O. *et al.* (2019) ‘Dynamic malware analysis in the modern era—A state of the art survey’, *ACM Computing Surveys (CSUR)*, 52(5), pp. 1–48.

Pan, Z. and Mishra, P. (2022) ‘Design of AI Trojans for Evading Machine Learning-based Detection of Hardware Trojans’, in *2022 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 682–687. Available at: https://doi.org/10.23919/DATE54114.2022.9774654.

Paniagua, C. and Delsing, J. (2020) ‘Industrial frameworks for internet of things: A survey’, *IEEE Systems Journal*, 15(1), pp. 1149–1159.

Park, S.-H. *et al.* (2022) ‘Performance evaluation of open-source endpoint detection and response combining google rapid response and osquery for threat detection’, *IEEE Access*, 10, pp. 20259–20269.

Pasdar, A. *et al.* (2024) ‘Cybersecurity solutions and techniques for internet of things integration in combat systems’, *IEEE Transactions on Sustainable Computing* [Preprint].

Pauling, C. *et al.* (2022) ‘A tutorial on adversarial learning attacks and countermeasures’, *arXiv preprint arXiv:2202.10377* [Preprint].

Pearce, J.M. (2020) ‘Economic savings for scientific free and open source technology: A review’, *HardwareX*, 8, p. e00139.

Peffers, K. *et al.* (2007) ‘A design science research methodology for information systems research’, *Journal of management information systems*, 24(3), pp. 45–77.

Peffers, K. *et al.* (2020a) ‘Design science research process: a model for producing and presenting information systems research’, *arXiv preprint arXiv:2006.02763* [Preprint].

Peffers, K. *et al.* (2020b) ‘Design Science Research Process: A Model for Producing and Presenting Information Systems Research’. Available at: https://arxiv.org/abs/2006.02763.

Peffers, K. *et al.* (2020c) ‘Design science research process: a model for producing and presenting information systems research’, *arXiv preprint arXiv:2006.02763* [Preprint].

Perera, A. *et al.* (2021) ‘The Next Gen Security Operation Center’, in *2021 6th International Conference for Convergence in Technology (I2CT)*, pp. 1–9. Available at: https://doi.org/10.1109/I2CT51068.2021.9418136.

Pérez, C.E.B., Serrano, J.E. and Martinez-Santos, J.C. (2021) ‘Cyberattacks Predictions Workflow using Machine Learning’, in *2021 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*, pp. 1–6.

Perifanis, N.-A. and Kitsios, F. (2023) ‘Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review’, *Information*, 14(2), p. 85.

Pilcher, N. and Cortazzi, M. (2024) ‘“Qualitative” and “quantitative” methods and approaches across subject fields: implications for research values, assumptions, and practices’, *Quality & Quantity*, 58(3), pp. 2357–2387. Available at: https://doi.org/10.1007/s11135-023-01734-4.

Poehlmann, N. *et al.* (2021) ‘The organizational cybersecurity success factors: an exhaustive literature review’, *Advances in Security, Networks, and Internet of Things: Proceedings from SAM’20, ICWN’20, ICOMP’20, and ESCS’20*, pp. 377–395.

Pollini, A. *et al.* (2022) 'Leveraging human factors in cybersecurity: an integrated methodological approach', *Cognition, Technology & Work*, 24(2), pp. 371–390.

Prana, G.A.A. *et al.* (2021) 'Out of sight, out of mind? How vulnerable dependencies affect open-source projects', *Empirical Software Engineering*, 26, pp. 1–34.

Prasad, R. and Rohokale, V. (2020) 'Artificial Intelligence and Machine Learning in Cyber Security', in R. Prasad and V. Rohokale (eds) *Cyber Security: The Lifeline of Information and Communication Technology*. Cham: Springer International Publishing, pp. 231–247. Available at: https://doi.org/10.1007/978-3-030-31703-4_16.

Preuveneers, D. and Joosen, W. (2021a) 'Sharing machine learning models as indicators of compromise for cyber threat intelligence', *Journal of Cybersecurity and Privacy*, 1(1), pp. 140–163.

Preuveneers, D. and Joosen, W. (2021b) 'Sharing machine learning models as indicators of compromise for cyber threat intelligence', *Journal of Cybersecurity and Privacy*, 1(1), pp. 140–163.

Preuveneers, D. and Joosen, W. (2021c) 'Sharing machine learning models as indicators of compromise for cyber threat intelligence', *Journal of Cybersecurity and Privacy*, 1(1), pp. 140–163.

Preuveneers, D. and Joosen, W. (2023) 'Privacy-preserving correlation of cross-organizational cyber threat intelligence with private graph intersections', *Computers & Security*, 135, p. 103505.

Prewett, K.W., Prescott, G.L. and Phillips, K. (2020) 'Blockchain adoption is inevitable—Barriers and risks remain', *Journal of Corporate accounting & finance*, 31(2), pp. 21–28.

Prity, F.S. *et al.* (2024) 'Machine learning-based cyber threat detection: an approach to malware detection and security with explainable AI insights', *Human-Intelligent Systems Integration*, pp. 1–30.

Priya, A. (2021) 'Case study methodology of qualitative research: Key attributes and navigating the conundrums in its application', *Sociological Bulletin*, 70(1), pp. 94–110.

Proudfoot, K. (2023) 'Inductive/Deductive hybrid thematic analysis in mixed methods research', *Journal of Mixed Methods Research*, 17(3), pp. 308–326.

P. S. , Dr.V. (2023) ‘How can we manage biases in artificial intelligence systems – A systematic literature review’, *International Journal of Information Management Data Insights*, 3(1), p. 100165. Available at: https://doi.org/https://doi.org/10.1016/j.jjimei.2023.100165.

Putyato, M.M., Makaryan, A.S. and Evsyukov, M. V. (2021) ‘Conceptual Approach to Implementation of Adaptive Protection of Operational Cybersecurity Centers’, *Lecture Notes in Networks and Systems*, 229, pp. 703–713. Available at: https://doi.org/10.1007/978-3-030-77445-5_63.

Qamar, S., Anwar, Z. and Afzal, M. (2023) ‘A systematic threat analysis and defense strategies for the metaverse and extended reality systems’, *Computers and Security*. Available at: https://doi.org/10.1016/j.cose.2023.103127.

Qiu, H. *et al.* (2021) ‘Deepsweep: An evaluation framework for mitigating DNN backdoor attacks using data augmentation’, in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pp. 363–377.

Quintão, C., Andrade, P. and Almeida, F. (2020) ‘How to improve the validity and reliability of a case study approach?’, *Journal of Interdisciplinary Studies in Education*, 9(2), pp. 264–275.

Quintero-Bonilla, S. and del Rey, A. (2020) ‘A new proposal on the advanced persistent threat: A survey’, *Applied Sciences*, 10(11), p. 3874.

Raghav, Y.S. *et al.* (2022) ‘Estimation and optimization for system availability under preventive maintenance’, *IEEE Access*, 10, pp. 94337–94353.

Raghav, Y.Y. and Kait, R. (2024) ‘Edge Computing Empowering Distributed Computing at the Edge’, in *Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models*. IGI Global, pp. 67–83.

Rajamäki, J., Lahdenperä, J. and Shalamanov, V. (2022) ‘Design science research towards ECHO governance and management information system’, in *2022 12th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, pp. 1–7.

Rana, K., Poudel, P. and Chimoriya, R. (2023) ‘Qualitative methodology in translational health research: current practices and future directions’, in *Healthcare*, p. 2665.

Rangaraju, S. (2023) ‘Ai sentry: Reinventing cybersecurity through intelligent threat detection’, *EPH-International Journal of Science And Engineering*, 9(3), pp. 30–35.

Rani, S. *et al.* (2022) ‘Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: State-of-art work’, *Materials Today: Proceedings*, 62, pp. 4671–4676.

Rantos, K. *et al.* (2020) ‘Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem’, *Computers 2020, Vol. 9, Page 18*, 9(1), p. 18. Available at: https://doi.org/10.3390/COMPUTERS9010018.

Reddy, A.R.P. (2021a) ‘THE ROLE OF ARTIFICIAL INTELLIGENCE IN PROACTIVE CYBER THREAT DETECTION IN CLOUD ENVIRONMENTS’, *NeuroQuantology*, 19(12), pp. 764–773.

Reddy, A.R.P. (2021b) ‘THE ROLE OF ARTIFICIAL INTELLIGENCE IN PROACTIVE CYBER THREAT DETECTION IN CLOUD ENVIRONMENTS’, *NeuroQuantology*, 19(12), pp. 764–773.

Rehan, H. (2024) ‘Revolutionizing America’s Cloud Computing the Pivotal Role of AI in Driving Innovation and Security’, *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, 2(1), pp. 239–240.

Remil, Y. (2024) ‘AIOps Solutions for Incident Management: Technical Guidelines and A Comprehensive Literature Review’, *ACM Transactions on Software Engineering and Methodology*, X.

Repetto, M. *et al.* (2021) ‘An autonomous cybersecurity framework for next-generation digital service chains’, *Journal of Network and Systems Management*, 29(4), p. 37.

Repetto, M. (2024) ‘Chaining Digital Services: Challenges to Investigate Cyber-Attacks at Run-Time’, *IEEE Communications Magazine*, 62(5), pp. 88–94. Available at: https://doi.org/10.1109/MCOM.002.2200942.

Repetto, M., Carrega, A. and Rapuzzi, R. (2021) ‘An architecture to manage security operations for digital service chains’, *Future Generation Computer Systems*, 115, pp. 251–266. Available at: https://doi.org/https://doi.org/10.1016/j.future.2020.08.044.

Robinson, N. (2023) ‘HUMAN FACTORS SECURITY ENGINEERING: THE FUTURE OF CYBERSECURITY TEAMS’, *EDPACS*, 67(5), pp. 1–17. Available at: https://doi.org/10.1080/07366981.2023.2211429.

Robinson, O.C. (2022) ‘Conducting thematic analysis on brief texts: The structured tabular approach.’, *Qualitative Psychology*, 9(2), p. 194.

Robles-Durazno, A. *et al.* (2021) ‘Implementation and evaluation of physical, hybrid, and virtual testbeds for cybersecurity analysis of industrial control systems’, *Symmetry*, 13(3), p. 519.

Romero, D.A.V. *et al.* (2024) ‘An open source IoT edge-computing system for monitoring energy consumption in buildings’, *Results in Engineering*, 21, p. 101875.

Rosa-Remedios, C. and Caballero-Gil, P. (2024) ‘Optimizing quantum machine learning for proactive cybersecurity’, *Optimization and Engineering* [Preprint]. Available at: https://doi.org/10.1007/s11081-024-09934-z.

S, Dr.G. (2024) ‘Change Management and User Adoption’, in *Mastering Microsoft Dynamics 365 Business Central: A Comprehensive Guide to Successful Implementation*. Berkeley, CA: Apress, pp. 171–194. Available at: https://doi.org/10.1007/979-8-8688-0230-0_7.

Sadowski, G., Kavanagh, K. and Bussa, T. (2020) ‘Critical Capabilities for Security Information and Event Management’, *Gartner Group Research Note* [Preprint].

Saeed, S. *et al.* (2023a) ‘A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience’, *Sensors*, 23(16). Available at: https://doi.org/10.3390/s23167273.

Saeed, S. *et al.* (2023b) ‘A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience’, *Sensors*, 23(16), p. 7273.

Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023a) ‘Counterattacking cyber threats: A framework for the future of cybersecurity’, *Sustainability*, 15(18), p. 13369.

Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023b) ‘Counterattacking cyber threats: A framework for the future of cybersecurity’, *Sustainability*, 15(18), p. 13369.

Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023c) ‘Counterattacking cyber threats: A framework for the future of cybersecurity’, *Sustainability*, 15(18), p. 13369.

Sagar, G. and Syrovatskyi, V. (2022) ‘System Design: Architecting Robust, Scalable, and Modular Applications’, in G. Sagar and V. Syrovatskyi (eds) *Technical Building Blocks:*

A Technology Reference for Real-world Product Development. Berkeley, CA: Apress, pp. 105–168. Available at: https://doi.org/10.1007/978-1-4842-8658-6_3.

Saini, N. *et al.* (2023) 'A hybrid ensemble machine learning model for detecting APT attacks based on network behavior anomaly detection', *Concurrency and Computation: Practice and Experience*, 35(28), p. e7865.

Salem, A. *et al.* (2022) 'Dynamic backdoor attacks against machine learning models', in *2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, pp. 703–718.

Salem, A.H. *et al.* (2024a) 'Advancing cybersecurity: a comprehensive review of AI-driven detection techniques', *Journal of Big Data*, 11(1), p. 105.

Salem, A.H. *et al.* (2024b) 'Advancing cybersecurity: a comprehensive review of AI-driven detection techniques', *Journal of Big Data*, 11(1), p. 105.

Salem, A.H. *et al.* (2024c) 'Advancing cybersecurity: a comprehensive review of AI-driven detection techniques', *Journal of Big Data*, 11(1), p. 105.

Salih, A. *et al.* (2021) 'A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection', in *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)*, pp. 61–66. Available at: https://doi.org/10.1109/IEC52205.2021.9476132.

Salinas, O. *et al.* (2023) 'An integral cybersecurity approach using a many-objective optimization strategy', *IEEE Access* [Preprint].

Samtani, S. *et al.* (2020) 'Cybersecurity as an industry: A cyber threat intelligence perspective', *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 135–154.

Sankar, N.A. and Fasila, K.A. (2023a) 'Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring', in *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, pp. 350–354.

Sankar, N.A. and Fasila, K.A. (2023b) 'Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring', in *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, pp. 350–354.

Sankar, N.A. and Fasila, K.A. (2023c) ‘Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring’, in *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, pp. 350–354.

Sapkal, M. *et al.* (2024) ‘AI-Driven Software Patch Management System’, *Shweta and Tamboli, Zaid and Sarode, Sahil and Habib, Rutuja, AI-Driven Software Patch Management System (November 15, 2024)* [Preprint].

Saraiva, M. and Mateus-Coelho, N. (2022) ‘CyberSoc Framework a Systematic Review of the State-of-Art’, *Procedia Computer Science*, 204, pp. 961–972.

Saritac, U., Liu, X. and Wang, R. (2022) ‘Assessment of cybersecurity framework in critical infrastructures’, in *2022 IEEE Delhi Section Conference (DELCON)*, pp. 1–4.

Sarker, I.H. *et al.* (2020) ‘Cybersecurity data science: an overview from machine learning perspective’, *Journal of Big Data*, 7(1), p. 41. Available at: https://doi.org/10.1186/s40537-020-00318-5.

Sarker, I.H. (2021a) ‘Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective’, *SN Computer Science*, 2(5), p. 377.

Sarker, I.H. (2021b) ‘Machine Learning: Algorithms, Real-World Applications and Research Directions’, *SN Computer Science*, 2(3), p. 160. Available at: https://doi.org/10.1007/s42979-021-00592-x.

Sarker, I.H. (2023) ‘Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview’, *Security and Privacy*, p. e295.

Sarker, I.H. (2024a) ‘AI for Critical Infrastructure Protection and Resilience’, *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*, pp. 153–172.

Sarker, I.H. (2024b) *AI-driven cybersecurity and threat intelligence: cyber automation, intelligent decision-making and explainability*. Springer Nature.

Sarker, I.H. *et al.* (2024) ‘Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects’, *ICT Express* [Preprint].

Sarker, I.H. (2024c) ‘Introduction to AI-Driven Cybersecurity and Threat Intelligence’, in *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*. Springer, pp. 3–19.

Sarker, I.H., Furhad, M.H. and Nowrozy, R. (2021a) ‘AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions’, *SN Computer Science*, 2(3), p. 173. Available at: https://doi.org/10.1007/s42979-021-00557-0.

Sarker, I.H., Furhad, M.H. and Nowrozy, R. (2021b) ‘Ai-driven cybersecurity: an overview, security intelligence modeling and research directions’, *SN Computer Science*, 2, pp. 1–18.

Saunders, M., Lewis, P. and Thornhill, A. (2018) ‘Research Methods for Business Students. Eighth Edition’, in *Synthese*.

Saunders, M., Lewis, P. and Thornhill, A. (2019) ‘Research Methods for Business Students Eight Edition’, *QualitativeMarket Research: An International Journal* [Preprint].

Schlette, D., Caselli, M. and Pernul, G. (2021) ‘A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective’, *IEEE Communications Surveys & Tutorials*, 23(4), pp. 2525–2556. Available at: https://doi.org/10.1109/COMST.2021.3117338.

Schlette, D., Vielberth, M. and Pernul, G. (2021) ‘CTI-SOC2M2–The quest for mature, intelligence-driven security operations and incident response capabilities’, *Computers & Security*, 111, p. 102482.

Schneller, L., Porter, C.N. and Wakefield, A. (2022) ‘Implementing converged security risk management: Drivers, barriers, and facilitators’, *Security Journal*, p. 1.

Secureframe (2024) *7 Benefits of Continuous Monitoring & How Automation Can Maximize Impact*. Available at: https://secureframe.com/blog/continuous-monitoring-cybersecurity (Accessed: 27 April 2024).

Shafiq, D.A., Jhanjhi, N.Z. and Abdullah, A. (2022) ‘Load balancing techniques in cloud computing environment: A review’, *Journal of King Saud University-Computer and Information Sciences*, 34(7), pp. 3910–3933.

Shah, N., Willick, D. and Mago, V. (2022a) ‘A framework for social media data analytics using Elasticsearch and Kibana’, *Wireless networks*, pp. 1–9.

Shah, N., Willick, D. and Mago, V. (2022b) ‘A framework for social media data analytics using Elasticsearch and Kibana’, *Wireless networks*, 28(3), pp. 1179–1187.

Shah, N., Willick, D. and Mago, V. (2022c) ‘A framework for social media data analytics using Elasticsearch and Kibana’, *Wireless networks*, 28(3), pp. 1179–1187.

Shah, N., Willick, D. and Mago, V. (2022d) ‘A framework for social media data analytics using Elasticsearch and Kibana’, *Wireless networks*, 28(3), pp. 1179–1187.

Shah, V. (2021a) ‘Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats’, *Revista Espanola de Documentacion Cientifica*, 15(4), pp. 42–66.

Shah, V. (2021b) ‘Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats’, *Revista Espanola de Documentacion Cientifica*, 15(4), pp. 42–66.

Shah, V. and Konda, S.R. (2022) ‘Cloud Computing in Healthcare: Opportunities, Risks, and Compliance’, *Revista Espanola de Documentacion Cientifica*, 16(3), pp. 50–71.

Shahjee, D. and Ware, N. (2022a) ‘Integrated Network and Security Operation Center: A Systematic Analysis’, *IEEE Access*, 10, pp. 27881–27898. Available at: https://doi.org/10.1109/ACCESS.2022.3157738.

Shahjee, D. and Ware, N. (2022b) ‘Integrated Network and Security Operation Center: A Systematic Analysis’, *IEEE Access*, 10, pp. 27881–27898. Available at: https://doi.org/10.1109/ACCESS.2022.3157738.

Shaik, A.S. and Shaik, A. (2024) ‘AI Enhanced Cyber Security Methods for Anomaly Detection’, in *International Conference on Machine Intelligence, Tools, and Applications*, pp. 348–359.

Shania, M., Handayani, P.W. and Asih, S. (2023) ‘Designing High-Fidelity Mobile Health for Depression in Indonesian Adolescents Using Design Science Research: Mixed Method Approaches’, *JMIR Formative Research*, 7, p. e48913.

Shankar, P. *et al.* (2020) ‘Towards the formalization of non-functional requirements in conceptual design’, *Research in Engineering Design*, 31(4), pp. 449–469. Available at: https://doi.org/10.1007/s00163-020-00345-6.

Sharma, A., Kumar, V.G. and Poojari, A. (2024) ‘Prioritize Threat Alerts Based on False Positives Qualifiers Provided by Multiple AI Models Using Evolutionary Computation

and Reinforcement Learning', *Journal of The Institution of Engineers (India): Series B*, pp. 1–18.

Shashkov, A. *et al.* (2023) 'Adversarial agent-learning for cybersecurity: a comparison of algorithms', *The Knowledge Engineering Review*, 38, p. e3.

Shukla, S. *et al.* (2022) 'Data security', in *Data Ethics and Challenges*. Springer, pp. 41–59.

Sibi Chakkaravarthy, S., Sangeetha, D. and Vaidehi, V. (2019) 'A Survey on malware analysis and mitigation techniques', *Computer Science Review*, 32, pp. 1–23. Available at: https://doi.org/https://doi.org/10.1016/j.cosrev.2019.01.002.

Singh, J. and Rahman, N.A.A. (2023) 'Cybercrime-As-A-Service (Malware)', *2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques, EASCT 2023* [Preprint]. Available at: https://doi.org/10.1109/EASCT59475.2023.10392459.

SIRP (2023) *SOAR Implementation: Challenges And Countermeasures - SIRP*. Available at: https://www.sirp.io/blog/soar-implementation-challenges-and-countermeasures/ (Accessed: 23 May 2023).

Sklavidis, I. *et al.* (2021) 'Enhancing siem technology for protecting electrical power and energy sector', in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 473–478.

Skopik, F. *et al.* (2022) 'From scattered data to actionable knowledge: flexible cyber security reporting in the military domain', *International Journal of Information Security*, 21(6), pp. 1323–1347.

Slade, P. *et al.* (2021) 'An open-source and wearable system for measuring 3D human motion in real-time', *IEEE Transactions on Biomedical Engineering*, 69(2), pp. 678–688.

Sobb, T., Turnbull, B. and Moustafa, N. (2020) 'Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions', *Electronics 2020, Vol. 9, Page 1864*, 9(11), p. 1864. Available at: https://doi.org/10.3390/ELECTRONICS9111864.

Soewito, B. (2024) 'SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive', *IJACSA) International Journal of Advanced Computer Science and Applications*, 15(9). Available at: www.ijacsa.thesai.org (Accessed: 23 February 2025).

Splunk (2023) *What is SIEM? Security Information and Event Management | Splunk*. Available at: https://www.splunk.com/en_us/data-insider/what-is-siem.html (Accessed: 28 May 2023).

Splunk (2024) *Splunk Phantom*. Available at: https://docs.splunk.com/Documentation/Phantom/4.10.7/User/Intro (Accessed: 27 April 2024).

Sridharan, A and Kanchana, V. (2022) 'SIEM integration with SOAR', in *2022 International Conference on Futuristic Technologies (INCOFT)*, pp. 1–6. Available at: https://doi.org/10.1109/INCOFT55651.2022.10094537.

Sridharan, Anish and Kanchana, V. (2022) 'SIEM integration with SOAR', in *2022 International Conference on Futuristic Technologies (INCOFT)*, pp. 1–6. Available at: https://doi.org/10.1109/INCOFT55651.2022.10094537.

Srinivas, K. *et al.* (2022) 'A novel machine learning inspired algorithm to predict real-time network intrusions', *International Journal of Information Technology*, 14(7), pp. 3471–3480. Available at: https://doi.org/10.1007/s41870-022-00925-w.

Srivastava, G. *et al.* (2022) 'XAI for Cybersecurity: State of the Art, Challenges, Open Issues and Future Directions', *ACM Comput. Surv*, 1(1). Available at: https://doi.org/10.1145/1122445.1122456.

Stanković, S., Gajin, S. and Petrović, R. (2022) 'A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis'.

Staves, A. *et al.* (2022) 'A cyber incident response and recovery framework to support operators of industrial control systems', *International Journal of Critical Infrastructure Protection*, 37, p. 100505.

Stedmon, A. and Paul, D. (2021) 'Conducting ethical research in sensitive security domains: Understanding threats and the importance of building trust', in *Ethical Issues in Covert, Security and Surveillance Research*. Emerald Publishing Limited, pp. 159–176.

Stojkovski, B. *et al.* (2021) 'What's in a cyber threat intelligence sharing platform? A mixed-methods user experience investigation of MISP', in *Proceedings of the 37th Annual Computer Security Applications Conference*, pp. 385–398.

Stoleriu, R., Puncioiu, A. and Bica, I. (2021) ‘Cyber attacks detection using open source ELK stack’, in *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pp. 1–6.

Straßburg, S. *et al.* (2021) ‘Identification of Issues in Design Science Research Evaluation-A Literature Review.’, in *AMCIS*.

Striepe, M. (2021) ‘Combining concept mapping with semi-structured interviews: adding another dimension to the research process’, *International Journal of Research & Method in Education*, 44(5), pp. 519–532.

Subramanian, K. and Meng, W. (2021) ‘Threat Hunting Using Elastic Stack: An Evaluation’, *2021 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2021* [Preprint]. Available at: https://doi.org/10.1109/SOLI54607.2021.9672347.

Sumo Logic (2024) *Cloud Log Management, Monitoring, SIEM Tools | Sumo Logic*. Available at: https://www.sumologic.com/ (Accessed: 27 April 2024).

Sun, N. *et al.* (2023) ‘Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives’, *IEEE Communications Surveys and Tutorials*, 25(3), pp. 1748–1774. Available at: https://doi.org/10.1109/COMST.2023.3273282.

Suricata Documentation (2023) *2. Quickstart guide — Suricata 8.0.0-dev documentation*. Available at: https://docs.suricata.io/en/latest/quickstart.html (Accessed: 12 May 2024).

Suryantoro, T., Purnomosidi, B.D.P. and Andriyani, W. (2022) ‘The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods’, in *2022 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 1–6. Available at: https://doi.org/10.1109/ISRITI56927.2022.10052950.

Swann, M. *et al.* (2021) ‘Open source and commercial capture the flag cyber security learning platforms-a case study’, in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 198–205.

Swimlane (2024) *Swimlane: AI Enabled Security Automation, SOC Automation, SOAR*. Available at: https://swimlane.com/ (Accessed: 27 April 2024).

Sworna, Z.T., Ali Babar, M. and Sreekumar, A. (2023) ‘IRP2API: Automated Mapping of Cyber Security Incident Response Plan to Security Tools’ APIs’, in *2023 IEEE*

International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 546–557. Available at: https://doi.org/10.1109/SANER56733.2023.00057.

Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020) 'A survey on security challenges in cloud computing: issues, threats, and solutions', *The journal of supercomputing*, 76(12), pp. 9493–9532.

Taherdoost, H. (2022a) 'Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview', *Electronics*, 11(14), p. 2181.

Taherdoost, H. (2022b) 'Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview', *Electronics 2022, Vol. 11, Page 2181*, 11(14), p. 2181. Available at: https://doi.org/10.3390/ELECTRONICS11142181.

Tahmasebi, M. (2024) 'Beyond defense: Proactive approaches to disaster recovery and threat intelligence in modern enterprises', *Journal of Information Security*, 15(2), pp. 106–133.

Tahmasebi, M. and Tahmasebi, M. (2024) 'Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises', *Journal of Information Security*, 15(2), pp. 106–133. Available at: https://doi.org/10.4236/JIS.2024.152008.

Tamminen, K.A. and Poucher, Z.A. (2020) 'Research philosophies', in *The Routledge international encyclopedia of sport and exercise psychology*. Routledge, pp. 535–549.

Tandon, A. *et al.* (2020) 'Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda', *Computers in Industry*, 122, p. 103290.

Tang, M., Li, M. and Zhang, T. (2016) 'The impacts of organizational culture on information security culture: a case study', *Information Technology and Management*, 17(2), pp. 179–186. Available at: https://doi.org/10.1007/s10799-015-0252-2.

Tariq, A. *et al.* (2023) 'Open source SIEM solutions for an enterprise', *Information & Computer Security*, 31(1), pp. 88–107.

Tatineni, S. (2023) 'AI-infused threat detection and incident response in cloud security', *International Journal of Science and Research (IJSR)*, 12(11), pp. 998–1004.

TechTarget (2023) *What is SOAR (Security Orchestration, Automation and Response)? | Definition from TechTarget*. Available at: https://www.techtarget.com/searchsecurity/definition/SOAR (Accessed: 23 May 2023).

Tekinerdogan, B. and Verdouw, C. (2020) 'Systems architecture design pattern catalog for developing digital twins', *Sensors*, 20(18), p. 5103.

Templ, M. and Sariyar, M. (2022) 'A systematic overview on methods to protect sensitive data provided for various analyses', *International Journal of Information Security*, 21(6), pp. 1233–1246. Available at: https://doi.org/10.1007/s10207-022-00607-5.

Tewari, S.H. (2021) 'Necessity of data science for enhanced cybersecurity', *International Journal of Data Science and Big Data Analytics*, 1(1), pp. 63–79.

Thakur, M. (2024) 'Cyber security threats and countermeasures in digital age', *Journal of Applied Science and Education (JASE)*, 4(1), pp. 1–20.

'The NIST Cybersecurity Framework (CSF) 2.0' (2024). Available at: https://doi.org/10.6028/NIST.CSWP.29.

TheHive Project (2023) *TheHive Project*. Available at: https://thehive-project.org/ (Accessed: 21 August 2023).

Thuan, N.H. *et al.* (2023) 'Special Issue Editorial: Introduction to Design Science Education', *Journal of Information Systems Education*, 34(3), pp. 256–263.

Tilbury, J. and Flowerday, S. (2024) 'Humans and Automation: Augmenting Security Operation Centers', *Journal of Cybersecurity and Privacy*, 4(3), pp. 388–409. Available at: https://doi.org/10.3390/jcp4030020.

Tomaszewski, L.E., Zarestky, J. and Gonzalez, E. (2020) 'Planning qualitative research: Design and decision making for new researchers', *International Journal of Qualitative Methods*, 19, p. 1609406920967174.

Tounsi, W. and Rais, H. (2018) 'A survey on technical threat intelligence in the age of sophisticated cyber attacks', *Computers \& security*, 72, pp. 212–233.

Trajkovski, G. (2024) 'Bridging the public administration-AI divide: A skills perspective', *Public Administration and Development*, 44(5), pp. 412–426.

Tronnier, F. *et al.* (2022) ‘A discussion on ethical cybersecurity issues in digital service chains’, in *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*. Springer International Publishing Cham, pp. 222–256.

Tsochev, G. *et al.* (2020) ‘Cyber security: Threats and challenges’, in *2020 International Conference Automatics and Informatics (ICAI)*, pp. 1–6.

Tufail, S. *et al.* (2021) ‘A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid’, *Energies*, 14(18), p. 5894.

Turner III, D.W. and Hagstrom-Schmidt, N. (2022) ‘Qualitative interview design’, *Howdy or Hello? Technical and professional communication* [Preprint].

Usmani, U.A., Happonen, A. and Watada, J. (2023) ‘Advancements in industry 4.0 asset management: Interoperability and cyber security challenges and opportunities’, in *Proceedings of the Future Technologies Conference*, pp. 468–488.

Vassilev, A., Booth, H. and Souppaya, M. (2022) ‘MITIGATING AI/ML BIAS IN CONTEXT Establishing Practices for Testing, Evaluation, Verification, and Validation of AI Systems’. Available at: https://www.nccoe.nist.gov/. (Accessed: 27 April 2024).

Vast, R. *et al.* (2021) ‘Artificial Intelligence based Security Orchestration, Automation and Response System’, in *2021 6th International Conference for Convergence in Technology (I2CT)*, pp. 1–5. Available at: https://doi.org/10.1109/I2CT51068.2021.9418109.

Vielberth, M *et al.* (2020) ‘Security Operations Center: A Systematic Study and Open Challenges’, *IEEE Access*, 8, pp. 227756–227779. Available at: https://doi.org/10.1109/ACCESS.2020.3045514.

Vielberth, Manfred *et al.* (2020a) ‘Security Operations Center: A Systematic Study and Open Challenges’, *IEEE Access*, 8, pp. 227756–227779. Available at: https://doi.org/10.1109/ACCESS.2020.3045514.

Vielberth, Manfred *et al.* (2020b) ‘Security operations center: A systematic study and open challenges’, *IEEE Access*, 8, pp. 227756–227779.

Vielberth, Manfred *et al.* (2020c) ‘Security Operations Center: A Systematic Study and Open Challenges’, *IEEE Access*, 8, pp. 227756–227779. Available at: https://doi.org/10.1109/ACCESS.2020.3045514.

Vielberth, M., Böhm, F. and Fichtinger, I. (2020) 'Security Operations Center: A Systematic Study and Open Challenges'. Available at: https://doi.org/10.1109/ACCESS.2020.3045514.

Villegas-Ch, W. *et al.* (2024) 'Effectiveness of an Adaptive Deep Learning-Based Intrusion Detection System', *IEEE Access*, 12, pp. 184010–184027. Available at: https://doi.org/10.1109/ACCESS.2024.3512363.

Villegas-Ch, W., Ortiz-Garcés, I. and Sánchez-Viteri, S. (2021) 'Proposal for an implementation guide for a computer security incident response team on a university campus', *Computers*, 10(8), p. 102.

Wang, L. and Jones, R. (2021) 'Big data analytics in cyber security: network traffic and attacks', *Journal of Computer Information Systems*, 61(5), pp. 410–417.

Wangen, G. (2019) 'Quantifying and Analyzing Information Security Risk from Incident Data', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11720 LNCS, pp. 129–154. Available at: https://doi.org/10.1007/978-3-030-36537-0_7.

Wazuh (2023a) *Wazuh · The Open Source Security Platform*. Available at: https://wazuh.com/ (Accessed: 28 May 2023).

Wazuh (2023b) *Wazuh documentation*. Available at: https://documentation.wazuh.com/current/index.html (Accessed: 8 May 2023).

Wazuh Blog (2024) *Extending Wazuh detection with Elastic Stack integration | Wazuh*. Available at: https://wazuh.com/blog/detection-with-elastic-stack-integration/ (Accessed: 23 February 2025).

Weichbroth, P. (2024) 'Usability Testing of Mobile Applications: A Methodological Framework', *Applied Sciences*, 14(5). Available at: https://doi.org/10.3390/app14051792.

Weilkiens, T. *et al.* (2022) *Model-based system architecture*. John Wiley & Sons.

Wen, S.-F., Shukla, A. and Katt, B. (2024) 'Artificial intelligence for system security assurance: A systematic literature review', *International Journal of Information Security*, 24(1), p. 43. Available at: https://doi.org/10.1007/s10207-024-00959-0.

Wermke, D. *et al.* (2022) ‘Committed to trust: A qualitative study on security & trust in open source software projects’, in *2022 IEEE symposium on Security and Privacy (SP)*, pp. 1880–1896.

Whitman, M.E. and Mattord, H.J. (2021) *Principles of incident response and disaster recovery*. Cengage Learning.

Whyte, C. (2020) ‘Problems of Poison: New Paradigms and “agreed” Competition in the Era of AI-Enabled Cyber Operations’, *International Conference on Cyber Conflict, CYCON*, 2020-May, pp. 215–232. Available at: https://doi.org/10.23919/CYCON49761.2020.9131717.

Winter, R. and vom Brocke, J. (2021a) ‘Teaching Design Science Research.’, in *ICIS*.

Winter, R. and vom Brocke, J. (2021b) ‘Teaching Design Science Research.’, in *ICIS*.

Wu, Y. *et al.* (2024) ‘Information security outsourcing strategies in the supply chain considering security externality’, *Journal of the Operational Research Society*, pp. 1–16.

Wylde, V. *et al.* (2022) ‘Cybersecurity, Data Privacy and Blockchain: A Review’, *SN Computer Science*, 3(2), p. 127. Available at: https://doi.org/10.1007/s42979-022-01020-4.

Xin, Y. *et al.* (2018) ‘Machine learning and deep learning methods for cybersecurity’, *Ieee access*, 6, pp. 35365–35381.

Yadav, A., Kumar, A. and Singh, V. (2023) ‘Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security’, *Artificial Intelligence Review*, 56(11), pp. 12407–12438. Available at: https://doi.org/10.1007/s10462-023-10454-y.

Yadav, D. (2022) ‘Criteria for Good Qualitative Research: A Comprehensive Review’, *The Asia-Pacific Education Researcher*, 31(6), pp. 679–689. Available at: https://doi.org/10.1007/s40299-021-00619-0.

Yadav, G. and Paul, K. (2021) ‘Architecture and security of SCADA systems: A review’, *International Journal of Critical Infrastructure Protection*, 34, p. 100433.

Yamin, M.M. and Katt, B. (2022a) ‘Modeling and executing cyber security exercise scenarios in cyber ranges’, *Computers & Security*, 116, p. 102635. Available at: https://doi.org/https://doi.org/10.1016/j.cose.2022.102635.

Yamin, M.M. and Katt, B. (2022b) ‘Modeling and executing cyber security exercise scenarios in cyber ranges’, *Computers & Security*, 116, p. 102635.

Yang, L. *et al.* (2019) ‘Towards big data governance in cybersecurity’, *Data-Enabled Discovery and Applications*, 3, pp. 1–12.

Yaseen, A. (2022) ‘Accelerating the SOC: Achieve greater efficiency with AI-driven automation’, *International Journal of Responsible Artificial Intelligence*, 12(1), pp. 1–19.

Yaseen, A. (2024a) ‘Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures’, *Quarterly Journal of Emerging Technologies and Innovations*, 9(1), pp. 38–60. Available at: https://vectoral.org/index.php/QJETI/article/view/68 (Accessed: 1 June 2024).

Yaseen, A. (2024b) ‘Enhancing Cybersecurity through Automated Infrastructure Management: A Comprehensive Study on Optimizing Security Measures’, *Quarterly Journal of Emerging Technologies and Innovations*, 9(1), pp. 38–60.

Yazdi, M. (2024) ‘Reliability-Centered Design and System Resilience’, in *Advances in Computational Mathematics for Industrial System Reliability and Maintainability*. Springer, pp. 79–103.

Yeboah-Ofori, A. *et al.* (2021) ‘Cyber threat predictive analytics for improving cyber supply chain security’, *IEEE Access*, 9, pp. 94318–94337.

Young, S. (2021) ‘Automated systems only: why CISOs should switch off their dumb machines’, *https://doi.org/10.1016/S1353-4858(19)30106-0*, 2019(9), pp. 6–8. Available at: https://doi.org/10.1016/S1353-4858(19)30106-0.

Yuan, X. *et al.* (2019) ‘Adversarial Examples: Attacks and Defenses for Deep Learning’, *IEEE Transactions on Neural Networks and Learning Systems*, 30(9), pp. 2805–2824. Available at: https://doi.org/10.1109/TNNLS.2018.2886017.

Zajdel, S., Costa, D.E. and Mili, H. (2022) ‘Open source software: an approach to controlling usage and risk in application ecosystems’, in *Proceedings of the 26th ACM International Systems and Software Product Line Conference-Volume A*, pp. 154–163.

Zamfir, V.-A. *et al.* (2019) ‘Systems Monitoring and Big Data Analysis Using the Elasticsearch System’, in *2019 22nd International Conference on Control Systems and Computer Science (CSCS)*, pp. 188–193. Available at: https://doi.org/10.1109/CSCS.2019.00039.

Zare, F. *et al.* (2024) ‘Bridging practice and science in socio-environmental systems research and modelling: A design science approach’, *Ecological Modelling*, 492, p. 110719.

Zarina I, K., Ildar R, B. and Elina L, S. (2019) ‘Artificial Intelligence and Problems of Ensuring Cyber Security.’, *International Journal of Cyber Criminology*, 13(2).

Zeadally, S., Adi, E., Baig, Z. and Khan, Imran A (2020) ‘Harnessing artificial intelligence capabilities to improve cybersecurity’, *Ieee Access*, 8, pp. 23817–23837.

Zeadally, S., Adi, E., Baig, Z. and Khan, Imran A. (2020) ‘Harnessing artificial intelligence capabilities to improve cybersecurity’, *IEEE Access*, 8, pp. 23817–23837. Available at: https://doi.org/10.1109/ACCESS.2020.2968045.

Zhang, F. *et al.* (2020) ‘A Machine Learning-based Approach for Automated Vulnerability Remediation Analysis’, *2020 IEEE Conference on Communications and Network Security, CNS 2020* [Preprint]. Available at: https://doi.org/10.1109/CNS48642.2020.9162309.

Zhang, S., Xie, X. and Xu, Y. (2020) ‘A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity’, *IEEE Access*, 8, pp. 128250–128263. Available at: https://doi.org/10.1109/ACCESS.2020.3008433.

Zhang, Y. *et al.* (2021) ‘Understanding and detecting software upgrade failures in distributed systems’, in *Proceedings of the ACM SIGOPS 28th Symposium on Operating Systems Principles*, pp. 116–131.

Zhang, Y., Xu, C. and Muntean, G. (2021) ‘A Novel Distributed Data Backup and Recovery Method for Software Defined-WAN Controllers’, in *2021 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6. Available at: https://doi.org/10.1109/GLOBECOM46510.2021.9685291.

Zhou, C. *et al.* (2020a) ‘A unified architectural approach for cyberattack-resilient industrial control systems’, *Proceedings of the IEEE*, 109(4), pp. 517–541.

Zhou, C. *et al.* (2020b) ‘A unified architectural approach for cyberattack-resilient industrial control systems’, *Proceedings of the IEEE*, 109(4), pp. 517–541.

Zidan, K. *et al.* (2024) ‘Assessing the Challenges Faced by Security Operations Centres (SOC)’, in *Future of Information and Communication Conference*, pp. 256–271.

Zunair Ahmed Khan, M., Mubashir Khan, M. and Arshad, J. (2022) ‘Anomaly Detection and Enterprise Security using User and Entity Behavior Analytics (UEBA)’, *3rd International Conference on Innovations in Computer Science and Software Engineering, ICONICS 2022* [Preprint]. Available at: https://doi.org/10.1109/ICONICS56716.2022.10100596.