



Vulnerability Management and Artificial Intelligence Integration

Securing the Future

**A Thesis Presented to
East Bridge University**

**In Partial Fulfillment
Of the Requirements of the
Executive Doctorate**

By

Kajal zachariah

2026

Title: Vulnerability management and artificial intelligence integration

Author: Kajal zachariah

Research Committee:

Research Advisor / Guide _____ Sundari
Subramanian _____
(Dr. Sundari Subramanian)

EBU Representative _____

(Dr Sanjib Chakraborty)

Date:

All Rights Reserved

**This Research is Approved by
East Bridge University**

Declaration of work

I hereby declare that this thesis is my own original work and has not been submitted, either in whole or in part, for the award of any other degree or qualification at this or any other institution.

All sources of information used in this study have been appropriately acknowledged and referenced in accordance with academic conventions. Where the work of others has been cited, due credit has been given. This research was conducted in compliance with applicable ethical standards and institutional guidelines.

I confirm that this thesis represents an accurate record of the research undertaken and that no part of it has been fabricated, falsified, or plagiarized.

Kajal Zachariah

Acknowledgement

I would like to express my sincere gratitude to all those who supported and encouraged me throughout the journey of completing this doctoral research.

First and foremost, I am deeply grateful to my mother, **Ammu Zachariah**, whose constant encouragement and belief in my abilities inspired me to pursue this doctorate. Her unwavering push, motivation, and sacrifices laid the foundation for this achievement, and I owe this milestone to her faith in me.

I extend my heartfelt thanks to my wife, **Maria Kajal Zachariah**, and my son, **Aarab Kajal Zachariah**, whose patience, understanding, and unconditional support sustained me through the demanding phases of this research. Their encouragement and emotional strength made it possible for me to remain focused and committed, even during challenging times.

I am profoundly thankful to my research guide, **Dr. Sundhari**, for her invaluable guidance, insightful feedback, and continuous support throughout the course of this study. Her clarity, expertise, and willingness to address every doubt played a crucial role in shaping this research.

I would also like to acknowledge my friends, who stood by me with encouragement and motivation, and the professionals who generously participated in this research. Their time, insights, and willingness to share knowledge contributed significantly to the depth and relevance of this study.

Finally, I extend my gratitude to everyone who supported me directly or indirectly in bringing this research to completion. This work is as much a reflection of their support as it is of my effort.

Abstract

The growing nature and magnitude of cyber threats have demonstrated the inadequacy of the conventional vulnerability management methods, which tend to be reactive, resource-heavy, and ineffective in the current dynamic digital world. As a reaction, artificial intelligence (AI) has become a game-changing feature in the field of cybersecurity, especially by improving prioritization, vulnerability detection, and vulnerability response. This dissertation is a critical analysis of the scope of AI in vulnerability management, specifically addressing how AI-based systems determine the effectiveness of threat management systems, ethical governance, and the general decision-making of the organization in cybersecurity cases.

The research approach selected is a qualitative, interpretivist study, and it uses semi-structured interviews with cybersecurity specialists in various roles, such as security operations, governance, application security, cloud security, and leadership roles. The interview data were analyzed with the help of thematic analysis, which allowed identifying the patterns and common points of view on the possibilities and challenges linked to AI-enabled vulnerability management. This will enable an in-depth examination of practitioner experience, as well as offer contextual information about the implementation practices that are typically underrepresented in more technical or quantitative studies.

The results show that AI profoundly transforms the concept of vulnerability management through facilitating the shift of reactive and periodic scanning into proactive, continuous, and risk-based security practices. Respondents claimed that exploitability, threat intelligence, and business impact-based AI-driven systems of prioritizing can cause alert fatigue and remediation focus. These features can be used to detect vulnerabilities quickly and with less dwell time, especially in cloud-based and highly dynamic settings. Nevertheless, the research also points to the fact that the efficiency of AI also depends on long-term human control. The respondents repeatedly pointed out that AI does not consider the context or ethicality and thus, human-in-the-loop models are crucial in ensuring accountability, accuracy, and control over the operations.

The key issues were ethical and governance issues. Questions of privacy, bias, explainability, and over-surveillance are also highly publicized in the conflict between security performance and personal rights. Respondents said that current governance and regulation frameworks were incapable of keeping up with the flexible and opaque nature of AI-driven security systems, which led to gaps between the requirements of compliance and the realities of operations. The results highlight the need to have transparency, explainable artificial intelligence, and well-defined accountability frameworks to have responsible deployment.

The current research is an addition to the current literature, as it is possible to fill the gap regarding the theoretical discussions on AI-driven vulnerability management and the empirical findings of cybersecurity professionals. The study introduces the practical implications of AI adoption in extending the existing literature in the field of technical capability to include ethical responsibility, readiness to govern, and organizational resilience. The results confirm the thesis statement that AI must be used as an addition to human experience and that a responsible and scalable use of AI involves a balanced approach to human control, automation, and ethics. The paper ends by providing some practical recommendations to organizations, security leadership, and policymakers, and defines the future directions in AI-enabled cybersecurity research.

Table of Contents

VULNERABILITY MANAGEMENT AND ARTIFICIAL INTELLIGENCE INTEGRATION	Error! Bookmark not defined.
Declaration of work	3
Acknowledgement	4
Abstract	5
Chapter 1: Introduction	11
1.1 Background of study	11
1.2 Problem Statement	12
1.3 Research Question	12
1.4 Research Objectives	12
1.5 Significance of this Research	12
1.5 Definition of terms	13
Chapter 2: Literature Review	14
Introduction	14
2.1 Historical Context and Background	14
2.1.1 Traditional Approaches to Vulnerability Management	14
2.1.2 Limitations of Current Vulnerability Detection Methods	15
2.2 Theme 1: Role of AI in Automating Vulnerability Detection and Response	16
2.2.1 AI-Driven Threat Detection and Analysis	16
2.2.2 Automation of Response and Remediation Processes	16

2.3 Theme 2: AI's Impact on Reducing Dwell Time for Zero-Day Vulnerabilities	17
2.3.1 AI's Role in Early Detection of Zero-Day Threats	17
2.3.2 Improving Incident Response with AI-Based Systems	17
2.4 Theme 3: Ethical and Governance Challenges in AI-Driven Security Systems.....	18
2.4.1 Ethical Implication of AI in Vulnerability Management.....	18
2.4.2 Governance and Accountability in AI-Driven Security Systems	18
2.5 Literature Gap	19
2.6 Theoretical Framework.....	20
2.6.1 Overview of Key Cybersecurity Models and Frameworks.....	20
2.6.2 Vulnerability Management Cycle	21
2.6.3 Introduction to AI Technologies Applied in Cybersecurity	22
2.6.4 Explanation of the Role of AI in Automating Threat Detection and Vulnerability Assessment.....	22
2.6.5 Connection Between AI and Vulnerability Management in Modern Security Systems	22
2.6.6 Artificial Intelligence (AI) Capabilities	22
2.6.7 Moderating Factor.....	23
2.6.8 Outcomes	23
2.7 Conceptual Framework.....	23
2.8 Conclusion	24
Chapter 3: Research Methodology.....	25
Introduction.....	25
3.1 Research Design.....	25
3.2 Research Location.....	26
3.3 Research Participants	26
3.3.1 Participant Profile	27

3.4 Data-Collection Methods	28
3.5 Sample Size.....	28
3.6 Sample Technique.....	29
3.7 Data Analysis	29
3.8 Research Process.....	30
3.9 Reflexivity.....	30
3.10 Validity	31
3.11 Ethical Considerations	32
Chapter 4: Findings and Discussion	33
4.1 Introduction to the Chapter	33
4.2 Presentation of Findings	33
4.2.1 Theme to objective.....	34
4.3 Analysis and Interpretation	34
4.3.1 Theme 1: AI as a Catalyst for Proactive and Risk-Based Vulnerability Management vs current Methodologies.	34
4.3.2 Theme 2: Human Oversight as a Non-Negotiable Component of AI-Driven Security	35
4.3.3 Theme 3: Dwell time and zero-day vulnerability capability of AI.....	36
4.3.4 Theme 4: Governance, Compliance, and Accountability Challenges in AI Adoption	38
4.3.5 Theme 5: Balancing Automation and Ethical Responsibility in AI-Driven Security..	39
4.4 Chapter Summary	40
Chapter 5: Discussion and Recommendations.....	41
Introduction to the chapter	41
5.1 Overview of Key Findings.....	41
5.2 Interpretation of findings	43
5.2.1 AI-Driven Transformation of Vulnerability Management Practices	43

5.2.2 Human–AI Collaboration and the Limits of Automation	43
5.2.3 Dwell time and zero-day vulnerability	44
5.2.4 Ethical Implications of AI in Vulnerability Management	45
5.2.5 Governance, Compliance, and Accountability in AI-Driven Security	46
5.3 Contribution to knowledge	46
5.4 Practical and Policy Implications.....	48
5.5 Summary	48
Chapter 6: Conclusion and Recommendations	48
6.1 Summary of the study	48
6.2 Major findings and theoretical contribution	49
6.3 Limitations of the study	50
6.5 Final Conclusion	52
References	54
Appendix A: Interview Questions	64
Appendix C: Thematic Coding table	64

List of Figures/tables:

Fig 2(a) Cybersecurity Models and AI Technologies.....	20
Fig 2(b) Conceptual Framework.....	24
Table 3(a) Participant Profile.....	27
Table 4(a) Theme to Objective.....	34
Table 4(b) Thematic / Coding Table.....	62

Chapter 1: Introduction

1.1 Background of study

Cybersecurity requires a vulnerability management process, which might be defined as the attempt to reveal, approximate, set priorities, and deal with the weaknesses of the systems and software of the company. The traditional tools of vulnerability management consist of periodic vulnerability scanning and manual remediation, which may increase vulnerabilities in managing the possible security risks (Hasan, 2024). This approach is highly important during the early years of cybersecurity, yet it cannot be efficient in the contemporary threat landscape that is rapidly changing. With this rapid change, the expectation and need are to identify vulnerabilities as soon as possible and remediate them before the threat can be exploited.

The vulnerability management is becoming a distraction to organizations more because of the augmented complexities related to cyberattacks resulting in vulnerabilities. The standard techniques, such as manual modification and patches, are unable to support the dynamism of the threats. Rather, organizations are resorting to automation and machine learning regarding threat detection, relying on live data, to identify areas of vulnerabilities and correct them before they can be abused (Hashmi, 2024). AI and machine learning have continued to be treasured resources in improving the speed of detection, analysis, and responsiveness around cybersecurity over the last ten years. These technologies can prove to be quite helpful in actively identifying the networks, and in detecting any vulnerabilities and threats; thus, they are much more efficient than the traditional approach.

Use of artificial intelligence in security operations to increase vulnerability management is becoming a common practice. AI algorithms can process large volumes of data in real time, detect patterns, and see possible weaknesses that cannot be noticed directly by human analysts (Komaragiri & Edward, 2022). Machine learning models, such as those, can constantly adapt to emerging dangers as they learn about attack patterns in the past, and, hence, are extremely efficient in identifying zero-day vulnerabilities and other previously unknown exploits. This change to the AI-driven security functions also allows organizations to automate routine operations, minimize human error, and implement a more dynamic perception of detecting and responding to threats.

1.2 Problem Statement

With the rapid growth of IT and adoption of AI in cybersecurity, the main struggle for organization is implementing AI and ML effectively due to the lack of expertise. While 73% of business leaders recognize the need for AI, 72% report insufficient capability to deploy it securely and efficiently (SentinelOne, 2025). The skills gap creates vulnerabilities that could be exploited by cybercriminals, exposing sensitive data and undermining AI-driven decision making. As AI becomes more integrated into the operations of business, robust AI vulnerability management is essential to identify, prioritize and mitigate risks, ensuring secure and compliant deployment.

1.3 Research Question

Analyze the integration of AI into vulnerability management systems and its impact on enhancing threat detection and response.

1.4 Research Objectives

- To evaluate current methodologies in vulnerability management.
- To explore the role of AI in automating vulnerability detection and response and the need for human intervention.
- To assess AI's ability to reduce dwell time for zero-day vulnerabilities.
- To investigate the ethical and governance challenges of AI-driven security systems.

1.5 Significance of this Research

This study reaffirms the importance of AI in terms of its use to improve vulnerability management in cybersecurity systems. Many traditional systems of vulnerability management are failing to cope with the number and rate of attacks, as cyber threats are becoming more complex and sophisticated. AI has the potential to make a tremendous contribution to reducing the time required to detect and tackle vulnerabilities and prevent risks in advance. When vulnerability management brings on board AI, zero-day vulnerabilities, which are usually hard to detect and remediate, can be considerably reduced in dwell time. This has the potential to reduce the speed of response to a threat as well as increase the effectiveness of the distribution of security resources. Furthermore, the research can make its contribution to theoretical and practice-related knowledge around cybersecurity, mentioning the role of AI in extending the existing practices and offering automated

and scalable solutions to the ever-growing issue (Ramamoorthi, 2021). The study should shed more light on the current methodologies on vulnerability management, giving a theoretical and practical perspective so the current drawbacks and areas of improvement can be easily identified.

Industry is divided in terms of the capability of AI because of lack of knowledge. Some think that AI can change the way industry is conducted now and will be a huge transition when some think that it's a destructive force and can take over humans so this study should clear the confusion and clarify the capability of AI and the need of human intervention rather than having fully autonomous. This should also go in detail on the capability of AI to overcome the zero-day vulnerabilities and help to investigate the ethical and governance challenges of AI-driven security systems. The outcomes of the ongoing study are predicted to fill a current gap between theoretical opportunities of AI and the real execution of the given technology around cybersecurity to help companies to endure the burden of activity within the framework of a complicated security environment.

1.5 Definition of terms

CVSS Common Vulnerability Scoring system - It's an open standardized framework used to measure and rank the severity of cybersecurity vulnerabilities in software and hardware. A numerical score to help security teams to prioritize remediation efforts.

Zero-day Vulnerability - A zero-day vulnerability is a software flaw which is not known to the vendor and there is no patch available. Giving attackers zero days to fix it before they can be exploited to cause data breaches, financial loss or system disruption.

Chapter 2: Literature Review

Introduction

The literature review (LR) is a critical part of any research study, which should be a section in the study to provide a background of the research and analyze the available knowledge critically. The structured literature review is systematic regarding the way it collects, analyses, and synthesizes the studies on the topic. This review provides an overall picture of how AI has already been integrated into the vulnerability management systems, the significant improvements, methodological issues, and challenges that have arisen in the literature. The methodological approach will ensure that the subject under consideration is not only addressed by other researchers but also that they are critically and methodologically examined, therefore making the object in question perceived objectively and exhaustively.

In the context of the study provided on the topic of Vulnerability Management and AI Integration - Securing the Future, the LR is the foundation of understanding the combination of artificial intelligence (AI) and cybersecurity activities regarding vulnerability management. This section will also be applied to identify the gaps in the current study and define the direction of the objectives and the methodology of the study. On a traditional approach the vulnerability management is a time taking process which can lead to potential data loss due to not having the remediation on time. With the use of AI, we are trying to cut down the time required for analysis and remediation, leading to a much safer and secure environment. In this chapter we will be discussing few themes like Ethical, Governance challenges and accountability, Reducing dwell time on zero-day vulnerabilities, Automation in detection and response.

2.1 Historical Context and Background

2.1.1 Traditional Approaches to Vulnerability Management

The manual scanning and patch management have been mainstream processes as far as vulnerability of the legacy systems is concerned. Basuki and Adriansyah (2023) point out that manual scanning is effective in determining the identified vulnerabilities, yet it is time-consuming, especially in complicated environments. The mechanisms might cause delays in patch deployment, which exposes the systems to risks. However, according to Walkowski et al. (2021), despite all these issues, the Common Vulnerability Scoring System (CVSS) offers a formal approach to

vulnerability prioritization in manual-based processes. Nonetheless, it is also true that automated mechanisms are replacing the manual procedures due to their inability to handle the developing threats in good fashion.

Post-breach analysis has been a common practice in traditional vulnerability management as a form of reactive security. Mohammed (2025) notes that post-breach analysis is useful in determining the vulnerabilities after an attack, but it does not usually prevent the initial attacks, thus exposing the system to potential vulnerabilities. Such a reactive service may slow down recovery and undermine the general resilience of the system. Battina (2021), however, claims that reactive measures, when combined in a larger proactive security approach, may aid vulnerability discovery in software development. In the end, as handy as they are, reactive measures on their own will not be able to offer adequate protection against emerging threats.

2.1.2 Limitations of Current Vulnerability Detection Methods

Compulsory but with a significant rate of false positives, the traditional approaches to vulnerability detection might slow down the response and prevent an effective mitigation effort (Bennouk et al., 2024). These techniques are largely manual and signature-based and thus are liable to errors that could flood security personnel with irrelevant alerts, leaving them to do nothing about them. In their turn, Risse et al. (2024) emphasize that even with the latest developments in machine learning to detect vulnerabilities, false positives continue to be a major issue, especially when it comes to detecting vulnerabilities in real-time. Thus, there is a strong need to learn new approaches that will help to minimize such inefficiencies while raising the detection accuracy.

The existing vulnerability detection techniques are not effective in identifying and controlling threats that develop quickly, e.g., zero-day vulnerabilities, in time (Kezron, 2024). Such mechanisms are usually based on a set of known signatures and rules, which reduces their effectiveness when it comes to new vulnerabilities that have not been previously known. According to Zhuang et al. (2021), machine learning models, e.g., graph neural networks, are somewhat promising in terms of identifying a given threat but are also not well-suited to do so in real time. As a result, adaptive detection techniques are increasingly being sought to deal with these new security issues in a more effective manner.

2.2 Theme 1: Role of AI in Automating Vulnerability Detection and Response

2.2.1 AI-Driven Threat Detection and Analysis

Threat detection is more accurate through AI since, with the aid of the tool, it examines massive datasets in real time, which is much higher than that of conventional means (Ma, 2021). This feature enables AI to detect hidden patterns and anomalies, which cannot be detected by traditional systems. Nonetheless, Khalifa and Albadawy (2024) claim that AI has become more accurate, but even now, it is unable to provide reliable outputs, as some of the patterns of data may be challenging. To sum up, AI-based threat detection has huge potential, and it should be further developed to address the existing limitations.

AI allows identifying and addressing vulnerabilities almost immediately, considerably shortening the exposure time (Adeola et al., 2023). AI can help prevent and mitigate threats fast, with the help of machine learning algorithms, which will cause minimal damage. Muppalaneni et al. (2024) mention, however, that the capability of AI to adjust to zero-day attacks is currently low because of the novelty and complexity of such threats. Consequently, the AI can be used to mitigate threats fast; however, additional development is required to cover new, unknown vulnerabilities.

2.2.2 Automation of Response and Remediation Processes

AI is used to automate the process of vulnerability remediation, which greatly speeds up the process of patching and threat mitigation with very little human involvement (Oladayo Aramide, 2025). This automation enables organizations to respond faster to security challenges, and less time is wasted on paperwork for remediating them. Nevertheless, Sehgal (2024) states that there can still be certain complex problems that cannot be addressed by human judgment, and the predetermined answers provided by AI are not always adequate. To conclude, although AI can provide faster response time, human input is essential regarding complex and new security issues.

New threats constantly teach AI systems, and in response, the system is kept informed on emerging changes in the security threats (Nutalapati, 2024). This flexibility can assist systems in identifying and preventing vulnerabilities quickly, which is more effective in the long term. Nevertheless, Obuse et al. (2023) posits that despite its ability to adjust, the ultimate capability of AI to respond to the unexpected threat could, in any case, be under human control, particularly when individual or novel vulnerabilities are introduced. Finally, the fact that AI is learning continuously allows it to increase responsiveness, but total security coverage is still required with human participation.

2.3 Theme 2: AI's Impact on Reducing Dwell Time for Zero-Day Vulnerabilities

2.3.1 AI's Role in Early Detection of Zero-Day Threats

The fact that AI systems can identify unknown vulnerabilities in large datasets with rapid response to real-time analysis enhances their capabilities to detect zero-day threats early and effectively, since they are absent in traditional systems in most cases (Ali et al., 2022). By using machine learning and anomaly detection, AI will help to identify unknown patterns and risks and prevent their utilization. Nonetheless, Morgan (2023) asserts that although AI seems promising, it is unlikely to be able to identify all vulnerabilities of the zero-day, especially in situations where complex and new types of attacks occur. Finally, AI is more effective in early detection, but it should be improved to make it more widely applicable.

The application of AI-powered models may help overcome the challenge of responding only to threats once they occur and instead promptly act against the zero-day threats before anyone can get the chance to exploit the vulnerability (Zichen, 2025). In the use of predictive analytics, AI can detect emergent risks according to the trends of previous attacks. According to Zaib and Zhou (2022), however, predictive models are effective but do not necessarily work to make precise predictions of new vulnerabilities, especially in the dynamic threat environment. Finally, AI is a promising source of foresight; however, it still cannot be considered very effective in predicting new methods of attack.

2.3.2 Improving Incident Response with AI-Based Systems

Smart systems that are powered by AI will be able to react to threats as soon as they are detected, which will greatly shorten the time that it takes to respond and cause less harm due to the vulnerabilities of zero-day threats (Ismail et al., 2025). AI speeds up the mitigation process by automating measures (including patching, isolating compromised systems) and reducing the extent to which network security is affected. Merzae (2022) identifies, however, that although AI is useful in providing quick responses, it may not be able to manage complicated scenarios that may need subtle decision-making. Finally, AI can make the process of incident response faster, but in certain cases, human control is necessary.

AI systems constantly overcome new threats because they learn with each new attack, improving their response approaches over time to handle the changing zero-day vulnerabilities (Ashfaaq et al., 2024). Through the analysis of past attacks, AI can improve its techniques for affecting and

addressing similar threats in the future. According to Kaluvakuri (2024), however, AI is still unable to handle completely new or complicated situations, despite adapting to having known ones. In summary, the flexibility of AI also enhances as time passes, though additional vulnerability might need human intervention.

2.4 Theme 3: Ethical and Governance Challenges in AI-Driven Security Systems

2.4.1 Ethical Implication of AI in Vulnerability Management

The amount of data used in training and functioning of AI granted security systems is great and poses a risk to data privacy and possible misuse of sensitive data (Chitimoju, 2023). These systems process both personal and organizational data, thus restricting the chances of failure or unauthorized access. Vemuri et al. (2023), however, contend that such risks can be addressed by appropriate protective measures such as encryption and anonymization methods. Finally, although the privacy of the data is legitimate, it is possible to implement sophisticated security measures to facilitate ethical processing of sensitive data within AI systems.

AI systems used in cybersecurity can also be biased by training data and, hence, will be discriminatory or unfair regarding the detection and response to threats, and this may discriminate against some groups or organizations (Alvarez Gonzalez et al., 2024). When the training data is biased with the historical data, the AI models might give certain precedence to the threats due to the biased information and therefore affect the reasoning of the system. However, Bruschi & Diomede (2022) believe that even having impartial methodologies and open model reviews can minimize the possibility of biases. To sum up, there is always a risk of AI algorithms, but these risks can be addressed.

2.4.2 Governance and Accountability in AI-Driven Security Systems

Given that AI systems make decisions independently in the sphere of cybersecurity, there is little obvious responsibility regarding what the system does, which is a major concern of accountability in case of mistakes (Ayeola, 2025). Because AI goes hand in hand with human interaction, it becomes impossible to trace the figure of accountability when some errors or outcomes are encountered. Salako et al. (2024), however, posit that putting in place the terms of clear governance and accountability mechanisms can contribute towards the assurance that the decisions made by AI remain ethical and legal in nature. Conclusively, as far as accountability has been a problem, the work can be solved by instating strong governance structures.

The high rate of AI integration in the field of cybersecurity also poses a problem to regulators who will need to introduce suitable frameworks to make AI systems safe, transparent, and responsible (Ademilua & Areghan, 2022). Regulators are finding it difficult to balance both security and privacy issues as AI technologies develop and continue to become agile in the face of innovation, even though they are hard to regulate. Nevertheless, Ahmed (2024) indicates that despite the changing regulatory environment, because there are no consistent international policies, the global regulation of AI in cybersecurity is made more difficult. To sum up, the regulatory frameworks should be constantly adjusted to guarantee that AI is used responsibly in security systems.

2.5 Literature Gap

Even with the rapid improvement of AI-enabled cybersecurity, the research gaps concerning ethical, governance, and technical issues of AI system deployment in vulnerability management are still considerable. Among the most noticeable gaps, we can mention the absence of full frameworks that would cover both the ethical analysis of the AI integration process and the technical one in the context of cybersecurity. Although Baeza-Yates (2022) addresses ethical issues in AI, such as impartial, transparency, and accountability, the question of how the ethical issues are applied to the systems of vulnerability management has not been properly investigated. It is often the case that AI systems work as black boxes and therefore may not make decisions at the level of transparency essential to both user trust and regulatory compliance.

Research on automated threat mitigation of AI-based systems is also developing. The research question on the effectiveness of the mentioned systems in the long term has been underperformed, even though other researchers, such as Komaragiri and Edward (2022), have carried out research about the use of AI as a tool to handle vulnerabilities and mitigate threats. Specifically, how AI adapts to a new threat and acquires new lessons, as well as integrates into the existing cybersecurity systems, is not addressed properly. The research on the scalability of AI to the real-world environment and its adaptation to the needs of a dynamic environment where zero-day threats and sophisticated attackers continuously change should be explored further.

This issue has defined the necessity of the existence of more unified studies that will not only examine the technical truthfulness of AI as an aid in cybercrime but also the ethical aspect of AI. We also require structures that are going to bridge the gap between ethical theory and the practical

applications, which can provide the right direction in the responsive application of AI in the significant critical systems of security.

To address the research gap, research questions/objectives were derived. As these questions can be best addressed by experts in the field, qualitative analysis was chosen over quantitative. The ability to comprehend the perceptions of cybersecurity practitioners regarding AI-based processes, and how the vulnerability management practices currently in place were assessed required an investigative, open-ended study. For that nine questions were set, and thirty professionals were chosen to obtain comprehensive study. The results will be analyzed into themes which should address the research objective and fill the gap.

2.6 Theoretical Framework

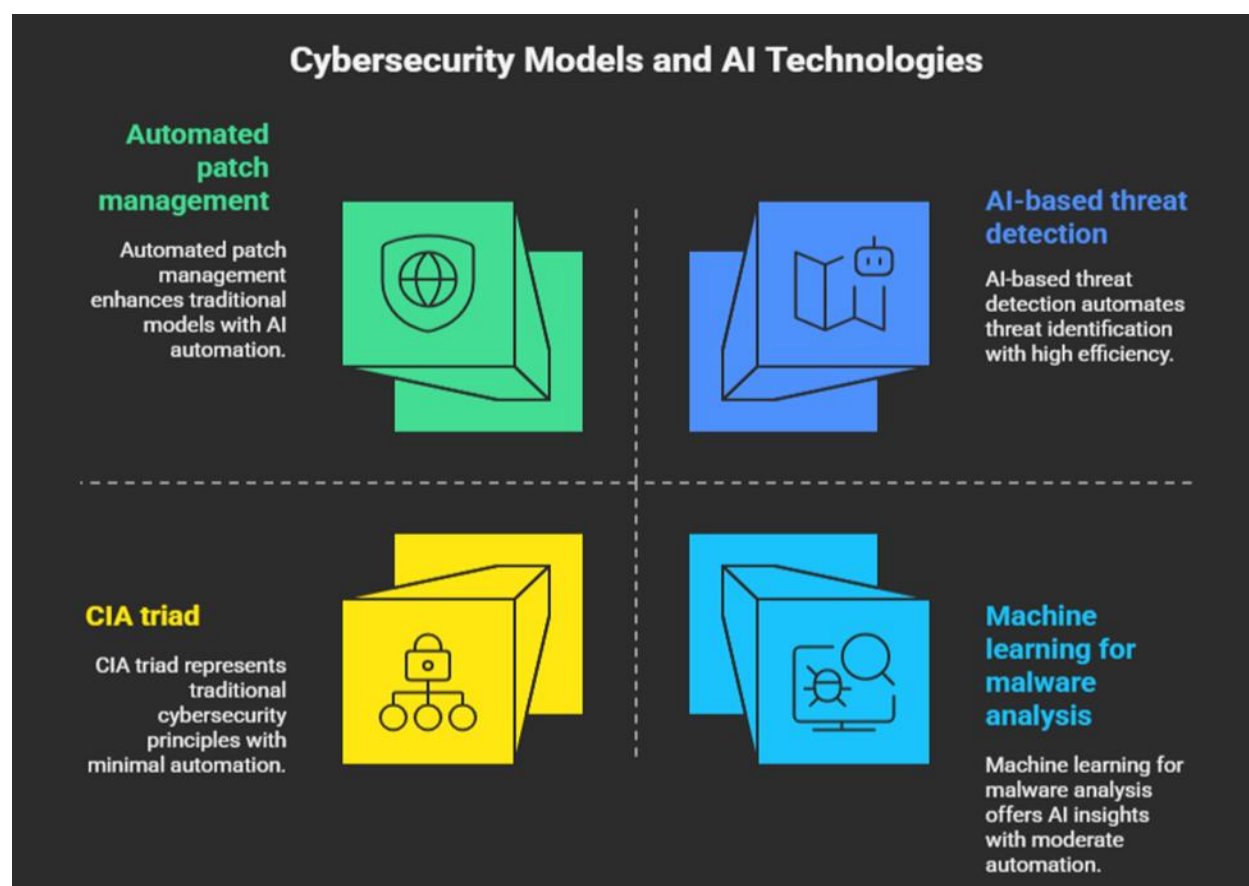


Fig 2 (a) Cybersecurity Models and AI Technologies

2.6.1 Overview of Key Cybersecurity Models and Frameworks

The creation and maintenance of effective security strategies require the development of cybersecurity models and frameworks. Among the most popular models is the CIA triad

(Confidentiality, Integrity, and Availability), which includes the main principles of data protection. Additionally, the risk management models, including the NIST Cybersecurity Framework, can assist organizations in identifying, evaluating, and addressing cybersecurity risks in a systematic manner. These models offer information to the organizations to prevent, identify, react, and recover from security breaches, thus enhancing the overall cybersecurity posture of the organization (Taherdoost, 2022). The other significant model is the Holistic IT Security Model that incorporates the layers of defense of an IT environment of an organization with a focus on human and technological factors (Villalon-Fonseca, 2022).

2.6.2 Vulnerability Management Cycle

The vulnerability management cycle represents the core operational process, consisting of asset discovery, risk assessment, prioritization, remediation and continuous monitoring. Asset discovery being the first in the process is based on the principal “you cannot secure what you do not know exist”. Asset inventory includes software, hardware, cloud resource etc. Using automated tools vulnerability scanning is done to identify vulnerabilities of the assets. Once the vulnerabilities are identified they are analyzed to determine severity and exploitability using scoring systems like CVSS (Common Vulnerability Scoring System). Scoring should be contextual considering the business impact, exposure and other factors. Depending on the vulnerability and business impact vulnerabilities are prioritized, not all vulnerabilities are equally critical. Once prioritized the next step will be remediation, which includes but is not limited to patching and updates, configuration changes, adding compensating controls like firewall, segmentations etc. Once the remediation is marked as completed the verification process kicks in to make sure the remediation efforts are effective by re-scanning systems, penetration testing, validation of the applied patches etc. The last and the most important part in the process is monitoring, continuous monitoring should be in place to make sure of any new threats or vulnerabilities. Integration of SIEM and other tools for real time alerts are used. Most importantly the cycle should continue to identify any new assets introduced and for any new vulnerabilities. AI strengthens each stage by improving the detection accuracy, prioritizing the risk level and automating the repetitive tasks. This integration allows the organization to move away from the static, time consuming, CVSS only approaches towards more risk-driven vulnerability management.

2.6.3 Introduction to AI Technologies Applied in Cybersecurity

Machine learning (ML) and deep learning (DL) AI technologies have transformed cybersecurity. Machine learning is unaccompanied by writing explicit code and works by training algorithms based on colossal amounts of data and identifying patterns. ML Deep Learning is a type of neural network with multiple layers to determine complex patterns in data by extracting features automatically. Very different cybersecurity activities, such as anomaly detection, malware analysis, and network traffic monitoring, are implemented using these technologies, which allow distinguishing possible threats in an automated fashion (Chowdhury et al., 2022).

2.6.4 Explanation of the Role of AI in Automating Threat Detection and Vulnerability

Assessment

In contemporary security systems, AI is important in automating threat detection and vulnerability assessment. The conventional approaches to threat detection can be described as reactive, meaning based on familiar patterns of the known attacks or by humans. Predictive analytics, on its part, uses AI to anticipate vulnerabilities and attack vectors. Given its constant data learning capabilities, AI algorithms can identify the emerging threat (zero-day vulnerability) that the standard system may not notice. Moreover, AI-based tools can automatically classify the severity of vulnerabilities, rank them according to the risk level, and propose mitigation measures in real-time (Taherdoost, 2022).

2.6.5 Connection Between AI and Vulnerability Management in Modern Security Systems

The association of AI with vulnerability management systems improves the capacity of an organization to have a high level of security. AI can be applied in automated patch management to lessen human error, and critical vulnerabilities are measured and reduced in a timely manner. It also makes continuous monitoring possible, so that security systems can adjust according to new threats and respond to them. Vulnerability management powered by AI enhances the efficiency and effectiveness of security measures, minimizing the total exposure of the infrastructure of an organization to risk (Villalon-Fonseca, 2022).

2.6.6 Artificial Intelligence (AI) Capabilities

The main capabilities of AI like machine learning, predictive analytics (anomaly detection), automation (including patching, isolating compromised systems) play a major role in the framework. These features help the security team to identify any security loopholes and allow them to fix the issue before they have been exploited by bad actors. Artificial Intelligence allows

the security team to process large amounts of data at a minimal time allowing it to improve threat feeds which indirectly enhance the vulnerability relevance and accuracy.

2.6.7 Moderating Factor

The effectiveness of AI-driven vulnerability management should be moderated by human oversight, ethical consideration and governance structures. It's not recommended to have a fully automated AI system as it could lead to unexpected errors or outcomes so human expertise should be used to make decisions. Ethical AI practices ensure transparency, fairness, and accountability in automated decision-making, while governance frameworks enforce compliance with regulatory standards and organizational policies. These moderators reduce the risk of over-reliance on automation and ensure responsible AI adoption.

2.6.8 Outcomes

When AI capabilities are effectively integrated and properly moderated, the framework results in measurable outcomes such as risk-based prioritization of vulnerabilities, reduced attacker dwell time, faster remediation cycles and improved decision making. Collectively, these outcomes contribute to a stronger security posture and increased resilience against cyber threats.

2.7 Conceptual Framework

The conceptual framework shows how Artificial Intelligence can add value to the vulnerability management cycle, moderated by experienced professionals, ethical and governance controls which produce the outcome of an improved security model.

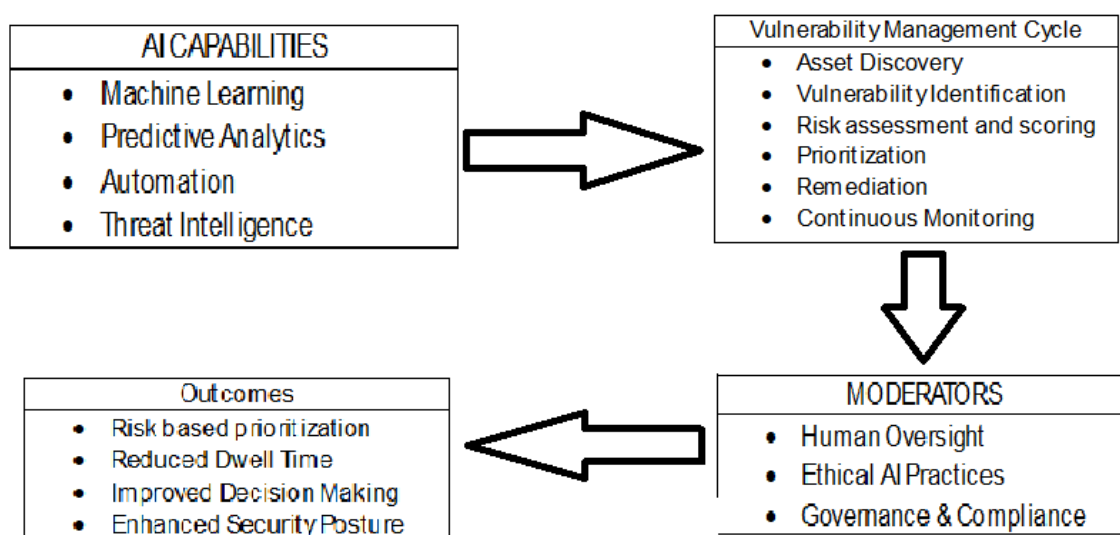


Fig 2(b) Conceptual Framework

2.8 Conclusion

To sum up, the chapter has been a very insightful point of view on the importance of AI in the modern day, on cybersecurity, specifically on vulnerability management. The discussion has shown both the strengths and the weaknesses of the systems available in detecting vulnerabilities, and there is a greater need to have more dynamic and efficient systems. One of the tasks that AI can perform better due to its timeliness, accuracy, and human error reduction is the process of automating vulnerability detection and response. More so, AI's ability to minimize the dwell time on the zero-day vulnerabilities has significant gains, though it is challenging to overcome hurdles to its agility in reacting to new threats. Besides this, ethical and governance concerns of AI in cybersecurity have been noted as having questions of privacy and accountability, as well as being biased in the process of making the decision. Such ethical and regulatory issues will gain more importance as AI is increasingly developed, and that is why they also need an answer in order to make the implementation of AI responsible and transparent. Lastly, the future of AI within the cybersecurity systems is very big, but it requires further research and development to help in removing its present hindrances and utilizing the challenges entirely in the fight against evolving cyber threats.

Chapter 3: Research Methodology

Introduction

Chapter 3 offered the methodological background through which the study was conducted and justified how the research design met the research aim, objectives, and questions. The chapter described the philosophical orientation, research method, and the reason to choose a qualitative methodology that would be appropriate to research the views of experts in cybersecurity (Sreekumar, 2023). It also outlined the theoretical framework that guided the methodological decisions and how they justified methodological decision-making in terms of a systematic exploration of AI-based vulnerability management. Also, the chapter elaborated the steps used in selecting the research site, identifying research participants, establishing the size of the sample, and the sampling method used. There was also a description of the data-collection procedure, research procedures, the aspects of reflexivity, and ethical procedures to maintain the credibility and integrity of the research. Lastly, the chapter concluded with the analytical processes that were applied in interpreting the qualitative one, considering that a clear and systematic methodology was crucial in coming up with valid and reliable findings.

3.1 Research Design

The research design used in the study was a primary qualitative research design, which suited discussing the perception of cybersecurity professionals towards the implementation of AI into vulnerability management systems. This design did not conform to an interpretivist philosophical position that presupposed that reality exists as a social construction and could best be learnt through the experiences and interpretations of the participants. Interpretivism placed deep, contextual, and meaning-based analysis before its eyes, thus making it appropriate in the investigation of how the experts comprehended AI-driven processes, ethical issues, and practical issues in cybersecurity settings. The qualitative research suited well since the research questions involved personal, more experience-based answers and not numerical. According to mixed-method scholarship, quantitative methods were unable to create the contextual richness that came with quantitative data, especially in studying interactions involving complex human-technology dynamics (Schoonenboom, 2023). The semi-structured interviews enabled the respondents to explain finer thoughts regarding threat detection, automation, and governance, being part of a comprehensive picture of the arising AI practices.

The use of quantitative techniques was abandoned since they were based on standardized variables and statistical performance, which would not have reflected the logic of the practitioners, interpretations, or life predicaments. Similarly, it did not adopt a mixed-methods approach, since it would involve the mix of numerical and narrative information, which was not needed by the study, based mainly on interpretive observations. Even though mixed methods may provide balanced analysis, they require hybrid methods of analysis, like inductive-deductive integration, which were more complicated than their aims required in this study (Proudfoot, 2022). Consequently, the qualitative design presented the most appropriate and coherent methodological approach for answering research questions.

3.2 Research Location

The research was done in a combination of in person and virtual and geographically the research participant was in USA, UK and India. The study was placed in professional settings that had to work within the realm of cybersecurity, such as Security Operations Centers (SOCs), information departments, and AI-oriented security groups. These environments were the major units of operation that involved the identification of threats, responding to attacks, and entailed in integrating advanced technologies into the defense strategies of the organization. The SOCs were a primary site, especially because real-time monitoring and vulnerability management activities were implemented in centralized locations, and thus, they serve important purposes in understanding AI-driven security practices (Vielberth et al., 2020). The setting was suitable to conduct the study on the concept of AI integration into the vulnerability management team since the units were making greater use of automation, machine learning models, and large language model-based capabilities to improve detection rates and operational efficiency. Recent studies noted that due to the implementation of AI-augmented processes to streamline security practices and multimodal reactions to emerging cyber threats, SOCs are also relevant to the investigation of the experiences of practitioners using AI-assisted vulnerability management (Srinivas et al., 2025). In such a way, the research location allowed gaining direct access to professionals who were involved in the operations of AI-supported cybersecurity.

3.3 Research Participants

The recruitment of participants was done by professional contacts and through the industry networks, the interviews were conducted using a combination of virtual platforms and in-person

meetings. The sample of the research was comprised of professionals who conducted their activities in the sphere of cybersecurity, such as cybersecurity specialists, Security Operations Center (SOC) experts, AI engineers, IT executives, IT security management, and people engaged in the process of vulnerability assessment and threat detection. These organizations were chosen since they actively dealt with tools, processes, and decision-making practices of interest to AI-driven vulnerability management. Their professional activities placed them in a position to give input on the traditional and emerging approaches to security, making them suitable for the objectives of the study.

They were supposed to be individuals who have hands-on experience in dealing with cybersecurity incidents, interpretation of threat intelligence, or automated detection systems. These features were necessary since the questions of the research needed knowledgeable viewpoints on the assets and limitations of the existing vulnerability management activities, the functional consequences of AI, and the related governance issues. This has been highlighted by the existing literature on the need to have domain-specific knowledge in the way decisions are being made in SOC settings, especially by introducing new technologies like AI or cyber deception tools (Reeves and Ashenden, 2023). Thus, the participants of the study who had technical, analytical, or managerial duties in cybersecurity operations offered knowledge depth that allowed addressing the issue of AI integration into vulnerability management systems and how it would change the organizational approach to security practices.

3.3.1 Participant Profile

Cybersecurity Professionals	5
Security Operations Center (SOC) experts	5
AI Engineers	2
IT Executives	8
Security Managers	3
Security Engineers	7

Table 3(a) Participant Profile

3.4 Data-Collection Methods

Semi-structured interviews were used in data collection as a way of ensuring that there were guided but free conversations with the respondents. Semi-structured interviews were used with a combination of fixed questions with the possibility to discuss arising topics, which allows the participants to expound on their experiences regarding AI-based vulnerability management and cybersecurity activities. It was commonly known that this approach can ensure high-quality, detailed qualitative data, but there is a framework that adheres to the purposes of the study (Adeoye-Olatunde and Olenik, 2021). The interview guide was constructed through the analysis of the gap that was found in the literature, and according to the goal of the research, the questions were developed. The limitations of traditional vulnerability management, AI-driven automation, reducing dwell time, and governance issues have been incorporated into the guide to cover all aspects. The research on AI implementation in cybersecurity practitioners also informed the formulation of the interview questions, which are applicable and context-specific (Clough, 2025).

The interviews were carried out either virtually or face-to-face, whenever the participants were available. The length of the sessions was usually 30-45 minutes. Secure digital tools were used to record the audio recordings, and verbatim transcribing of each interview was done to guarantee accuracy and reliability of the data. The advantages of semi-structured interviews were that they were flexible, in-depth, and led to clarification of complex technical issues. Shortcomings were, however, noted to include possible interviewer bias, variation in the responses of participants, and the fact that data is time-consuming due to transcription and interpretation. Notwithstanding such limitations, the approach was successful in terms of investigating the expert opinion on AI-enabled vulnerability management.

3.5 Sample Size

The proposed sample size of the research is from thirty participants, and it was appropriate to the available practices in the field of qualitative research. This number was deemed to be appropriate since the qualitative inquiry process was based on depth, and not breadth, attaining insightful in-depth information on the participants who had relevant knowledge. The sample size was determined based on the principle of data saturation, which took place when no new themes or information that was informative were obtained after the interviews with additional people were conducted. Empirical research proved that saturation in qualitative research was frequently

realized in quite limited samples, especially when the participants had some specific knowledge or experience (Hennink and Kaiser, 2022). The goal of a qualitative study did not presuppose big numerical samples, as the aim of the study was to understand the complicated phenomena in-depth instead of statistically generalizing them. Hence, a targeted and carefully chosen sample group was able to offer adequate data to answer the research questions and ensure analytical quality.

3.6 Sample Technique

It used a purposive and convenience sampling method, that is, expert sampling, as its sampling method to select the respondents who had considerable experience in the field of cybersecurity, vulnerability management, and AI-related security operations. The purposive sampling was suitable since it provided the opportunity to choose individuals with the specific knowledge needed to answer the research questions properly. This method corresponded to the qualitative research practice according to which participants were not selected randomly but recruited based on their expertise (Campbell et al., 2020). Experts in the field of cybersecurity were required since the research focused on extremely technical processes and decision-making methods, and new issues related to integrating AI. It is possible that only people who have had hands-on experience with SOC functions, threat identification processes, or AI-based products may be able to give valuable analysis. Other methods of sampling, like random sampling or convenience sampling, were not adopted since they would not guarantee the selection of individuals with expertise that would be needed. These techniques could also be a threat to generating data that is irrelevant or lacks technical accuracy.

3.7 Data Analysis

Thematic Analysis was employed to analyze the data and based on the commonly known six-step model created by Braun and Clarke. This procedure provided a systematic and adjustable system for discovering substantial patterns in qualitative information. This analysis started with familiarization, whereby the transcripts were read several times to get a holistic view of the perspectives of the participants. The second step was the coding, in which important parts of the text were marked to get crucial concepts concerning the research questions.

The third stage involves the grouping of the codes to come up with the initial themes, which are the high-level ideas that exist in the results of the data. In the fourth phase, it was necessary to review the themes to verify their internal consistency, coherence, and correspondence with the

dataset. The fifth step was the characterization and naming of themes, whereby boundaries of themes were sharp and descriptive words were formulated. Lastly, the sixth phase, which was reporting, involved the synthesis of the themes into a logical story with illustrative quotations, which is consistent with the best qualitative practices (Byrne, 2021). Inductive as well as deductive coding methods were considered. Deductive coding and inductive coding entailed using preexisting concepts offered by literature and letting themes emerge through the accounts given by the participants, respectively. The study being exploratory and considering the expert experiences as the main research matter, an inductive approach was primarily employed. This enabled the analysis to still be based on participant views, but still to have the wider theoretical framework. Thematic Analysis as such offered a rigorous and clear way of interpreting complex qualitative information pertaining to AI-enabled vulnerability management.

3.8 Research Process

The study used a step-by-step approach to the research to achieve methodological rigor and correspondence with the purpose of the study. It has been initiated by the in-depth literature review, which revealed the gaps that pertain to AI-based vulnerability management and guided the study. The literature input allowed for formulating the semi-structured interview questions while ensuring that the leading themes, including automation, threat detection, and governance, were satisfied.

Then, the recruitment of participants was undertaken, and the focus was on cybersecurity professionals having expertise in the area. After the recruitment, interviews were recorded and transcribed verbatim transcription, and the verbatim transcription was carried out later, to maintain the precision of the comprehensibility of the responses of the participants.

The data were then subjected to thematic analysis, which is an organized approach that aided recognition, categorization, and explanation of repeated themes in the data. This step-by-step methodology suggested in the qualitative research provided support in the transition of raw data into some meaningful themes (Naeem et al., 2023). The stages were completed by interpreting and reporting findings.

3.9 Reflexivity

The aspect of reflexivity played a significant role in the research process because it allowed considering a certain impact of the researcher's positionality and possible bias on the data collection and interpretation. Such knowledge and intentions regarding cybersecurity and related

AI technologies presupposed awareness of previous knowledge, professional background, and assumptions, which contributed to the preservation of objectivity. Reflexive practice acknowledged that these elements might have an unwanted influence on interview processes or the interpretation of the experience of participants (Wilson et al., 2022). In the case of neutrality, a few strategies were utilized. An informative journal has been kept during the research process to record assumptions, decisions, and arising reflections to encourage continuous self-awareness. The data was analyzed using bracketing methods to brush off prior preconceived ideas and enabled themes to be developed based on the views of the participants and not the expectations of the researcher. Moreover, feedback from peers was requested to review interpretations and minimize bias. These actions increased the validity of the results and made the analysis based on the input of the participants and were not subjective.

3.10 Validity

The objective of the research was to get expert opinion on the AI integration on vulnerability management. The sample of the research was comprised of professionals who conducted their activities in the sphere of cybersecurity, such as cybersecurity specialists, Security Operations Center (SOC) experts, AI engineers, IT executives, IT security management, and people engaged in the process of vulnerability assessment and threat detection. These organizations were chosen since they actively dealt with tools, processes, and decision-making practices of interest to AI-driven vulnerability management. Their professional activities placed them in a position to give input on the traditional and emerging approaches to security, making them suitable for the objectives of the study.

They were supposed to be individuals who have hands-on experience in dealing with cybersecurity incidents, interpretation of threat intelligence, or automated detection systems. These features were necessary since the questions of the research needed knowledgeable viewpoints on the assets and limitations of the existing vulnerability management activities, the functional consequences of AI, and the related governance issues.

On the pilot testing phase, a ten-member research participant was chosen to identify if the research is in line with the research objective and the chosen participants were the right candidate who could provide the relevant insight on the topics which should lead to the research objectives.

3.11 Ethical Considerations

The research complied with the accepted level of ethics to safeguard the participants and avoid irresponsible management of the sensitive information on cybersecurity matters. Participation was done with informed consent in place, and people knew the purpose and procedures of the study, and their rights. Anonymity and confidentiality were ensured by withholding any shows of identities by excluding them in transcripts and reporting the findings in a non-attribution way. These safeguards were especially significant in studies of cybersecurity, where the exposure of practice and security flaws may be risky (Macnish and van der Ham, 2020). I have upheld the confidentiality and anonymity of the research participants who have participated in the interviews.

The data were saved safely with encrypted digital folders that could only be accessed by researchers who were authorized. All participants would have the freedom to discontinue the research without compensation, and subsequently, any information relating to their involvement would be deleted on request. One of the other areas of priority in the study was ensuring non-harm through the fact that no interview questions led to disclosure of organizational information that was classified, proprietary, or sensitive.

Since qualitative data comprised this type of data, ethical considerations were also extended to secure storage and responsible processing of transcripts and recordings, as the issues of data protection practices in qualitative research made in prior studies (Mozersky et al., 2020). Prior to the start of data collection, the ethics were approved by the institution's review body appropriately, which upheld the standards of institutional and disciplinary approval.

All the information obtained from the participant with respect to the research was treated with strict confidentiality. None of the details identifying the participants' identity was recorded. Also, it was made sure that none of the questions or datasets shall directly or indirectly imply the identity of the participant. Data was used explicably for academic research and wasn't used for any other purpose. All the findings from the research are presented in aggregated form, without mentioning any name instead a number was used to ensure confidentiality is maintained throughout the research.

Chapter 4: Findings and Discussion

4.1 Introduction to the Chapter

The findings and discussion of the study in this chapter discuss the research purpose of this study, that is, to conduct research investigating how artificial intelligence can be incorporated into the vulnerability management system and how it will influence the improvement of threat detection, response, and governance in the process of cybersecurity. The chapter is based on the analysis of qualitative data obtained using semi-structured interviews with cybersecurity professionals in various positions guided by research questions. The aim of this chapter is to make sense of the experience and views of the participants to come up with a more profound learning of the practical, ethical, and organizational implications of AI-enabled vulnerability management. This chapter should also address the research objective “Analyze the integration of AI into vulnerability management systems and its impact on enhancing threat detection and response.”

To be analytically clear, Section 4.3 gives the results of a thematic analysis of the interview data, and the themes reflect repeating patterns in the responses of the participants. This part is still evidence-based and participant-oriented, which aims at interpreting empirical findings without referring to an existing theory, however the end of each theme is given a summary about what was discussed and what it compared to the theoretical context. In line with a qualitative and interpretivist research method, the analysis is based on meaning, context, and subjective interpretation as opposed to measurement and generalization. For the analysis and to generalize into themes no automated tools were used instead manual process was implemented to find themes regarding each questionnaire and to put in align with the objectives derived.

4.2 Presentation of Findings

From the interview responses five themes were developed, which meets our four research objectives.

1. AI as a catalyst for proactive and risk-based vulnerability management.
2. Human oversight is a non-negotiable component of AI driven security.
3. Dwell time and zero-day vulnerability capability of AI.
4. Governance, Compliance and Accountability challenges in AI adoption.

5. Balancing automation and Ethical responsibility in AI-Driven security.

4.2.1 Theme to objective

OBJECTIVE	THEME
1. What were the strengths and limitations of current methodologies in vulnerability management?	Theme 1: AI as a Catalyst for Proactive and Risk-Based Vulnerability Management
2. How did AI contribute to automating vulnerability detection and response in cybersecurity and the need of human intervention?	Theme 2: Human Oversight as a Non-Negotiable Component of AI-Driven Security.
3. To what extent was AI able to reduce the dwell time for zero-day vulnerabilities in cybersecurity systems?	Theme 3: Dwell time and zero-day vulnerability capability of AI.
4. What were the ethical and governance challenges associated with the use of AI-driven security systems?	Theme 4: Governance, Compliance, and Accountability Challenges in AI Adoption Theme 5: Balancing Automation and Ethical Responsibility in AI-Driven Security

Table 4(a) Theme to Objective

4.3 Analysis and Interpretation

4.3.1 Theme 1: AI as a Catalyst for Proactive and Risk-Based Vulnerability Management vs current Methodologies.

Respondents repeatedly mentioned AI as a disruptive force that takes the vulnerability management paradigm out of the traditionally reactive approach and the risk-based one. Instead of having periodic scans and after the disclosure reaction, AI was seen as a means of having full-time monitoring and pre-emptive assessment, enabling organizations to foresee vulnerabilities before they are proactively exploited.

Participant 1 also noted that AI enhances the speed and scope of vulnerability detection, and it can go beyond manual and signature-based methods compared to traditional approach:

“Traditional methods relied heavily on signature-based scanning and manual analysis, which are often reactive AI-driven systems can analyze massive volumes of network traffic, system logs, and

vulnerability data in real time to identify patterns and anomalies that may indicate unknown or zero-day vulnerabilities.”

Multiple participants compared continuous AI-based monitoring to traditional periodical scanning. Participant 2 has mentioned that AI allows continuous evaluation in a dynamic environment, especially in cloud-based systems:

“AI enables continuous vulnerability assessment rather than periodic scanning, which is especially important in dynamic environments like cloud and containerized systems.”

Another common element of this theme was AI-based prioritization. The respondents highlighted that AI is useful in assisting security teams to prioritize vulnerabilities that present the greatest real-world risk based on exploitability, threat intelligence, and business impact. Participant 3 described this change in the following way:

“AI enables better prioritization of remediation efforts based on business impact, asset criticality, and real-world threat intelligence rather than raw vulnerability counts.”

This prioritization, which was risk-based, was also associated with less alert fatigue and better decision-making. Participant 4 explained that AI correlation features allow analysts to concentrate on what they can do with:

“AI helps correlate vulnerability data with threat intelligence and live attack indicators, which allows analysts to focus on vulnerabilities that are actually being exploited.”

In general, the results reveal that AI influences the concept of security decision-making by changing the paradigm of vulnerability management as an ongoing and intelligence-informed process that allows allocating resources more strategically and conducting remediation activities more intelligently. AI moves away from the traditional signature-based approach to more robust security model.

4.3.2 Theme 2: Human Oversight as a Non-Negotiable Component of AI-Driven Security

In all the interviews, respondents made it very clear that human supervision is critical in AI-assisted vulnerability management and threat response. Although AI was generally accepted as fast, scalable, and analytical, participants kept claiming that it cannot provide situational awareness, ethical reasoning, and contextual judgment needed to make important security decisions.

Participant 1 expressed the drawbacks of using AI without human validation, emphasizing the need to have experts interpret it:

“AI can process data faster than humans, but it lacks contextual understanding and judgment. Security analysts are needed to validate AI findings and make final decisions on incident response.”

Participant 2 also shared this opinion and noted that hybrid methods provide more dependable results:

“AI excels at detection and correlation, but humans are needed to assess intent, business context, and the potential collateral impact of response actions.”

Some of the respondents cautioned against the dangers of over-automation. Participant 4, who has a SOC perspective, remarked how automated replies in the absence of supervision might be disruptive to the running of the operation:

“Automated actions without human review could lead to system outages or unnecessary account lockouts.”

Regarding governance and leadership, Participant 8 reiterated that accountability cannot be assigned to AI systems:

“Human oversight is essential and non-negotiable. AI provides valuable insights, but strategic decisions and accountability must remain with people.”

Ethical responsibility was also identified as human oversight by the participants. Participant 5 added a warning against handing over to AI-generated outputs blindly:

“Without human oversight, AI-generated results may lead to false confidence in an organization's security posture.”

In general, it can be concluded that the paper has found a strong agreement that AI should be used as a decision-support tool and not as an independent authority. It was strongly suggested to design the models in keeping human as decision authority rather than fully autonomous AI system. It was considered imperative to ensure accuracy, accountability, and ethical integrity in AI-based cybersecurity practices using human-in-the-loop models.

4.3.3 Theme 3: Dwell time and zero-day vulnerability capability of AI

Most of the participants mentioned about the dwell time and the zero-day vulnerability as an advantage of the AI integrated verses the traditional signature based. Which means a malicious activity is found as soon as they enter rather than after the exploitation. AI can learn anomalies faster and flag activity in real time which could have taken days in traditional system.

Participant 1 mentions the advantage of AI as it could flag anomalies in real time.

“Vulnerability data in real time to identify patterns and anomalies that may indicate unknown or zero-day vulnerabilities. AI can flag anomalies in real time even without signatures. Machine learning models also help prioritize vulnerabilities based on exploitability and business impact, allowing teams to focus on the most critical risks rather than treating all vulnerabilities equally”.

Participant 10 mentions the connection between vulnerability management and incident response pointing towards the zero-day vulnerabilities.

“AI has improved the connection between vulnerability management and incident response. By correlating vulnerability data with real-time threat indicators, AI helps incident response teams identify which vulnerabilities are actively being exploited during an attack. This allows for faster containment and more targeted remediation efforts.”

Participants 11, 16 and 27 point out the advantages of AI as a tool which can predict the attack which points towards proactive protection...

“AI helps identify which vulnerabilities are most likely to be targeted” (Participant 11)

“AI can adapt to new traffic behaviors and detect previously unknown weaknesses, enabling faster identification and mitigation of network vulnerabilities” (Participant 16)

“AI models can predict which vulnerabilities are most likely to be exploited, allowing organizations to focus on the highest-risk issues.” (Participant 27)

Participant 15 mentions the integration between vulnerability management and automated workflow.

“AI has enabled tighter integration between vulnerability management and automated response workflows. By correlating vulnerability data with real-time alerts, AI helps prioritize remediation and trigger automated actions for known, high-confidence issues. This improves response times and allows security teams to focus on more complex threats.”

In general, most of the participants mention dwell time and zero-day vulnerability as an added advantage of AI over the traditional approach. Participants believe that AI can learn the normal behavior and any alteration or deviation could immediately trigger a red flag and alert within

minutes rather than days, which can be considered as a new finding as the available literature tends to believe that AI can only identify and detect a vulnerability which happened before. It is also noted that AI has the capability to look for any changes in the codes and could predict the outcomes in real time.

4.3.4 Theme 4: Governance, Compliance, and Accountability Challenges in AI Adoption

Governance, compliance, and accountability remained key challenges that were always cited by participants as they attempted to introduce AI into vulnerability management systems. Whereas AI is beneficial in the detection and prioritization, the compatibility of AI-based outputs with current regulatory, audit, and governance frameworks was characterized as convoluted and resource-consuming.

Participant 1 has mentioned regulatory limitations in the implementation of AI, in terms of data protection requirements:

“When deploying AI-driven log analysis tools, we faced concerns related to data retention and access controls under regulations such as GDPR.”

Some of the participants highlighted challenges in trying to match AI-generated risk scores with existing compliance and audit models. Participant 3 reported organizational governance difficulties:

“An AI-based vulnerability prioritization tool conflicted with our existing risk assessment methodology required by internal audit.”

Regarding the consulting perspective, Participant 6 described that the issue of governance misalignment usually involves a need to change how structures are made:

“We had to redesign reporting outputs and governance workflows to ensure that AI results aligned with regulatory expectations and internal audit requirements.”

Auditability and explainability were also identified as critical issues that were raised. Participant 24 emphasized that AI systems should promote the transparent decision-making process to meet the requirements of the audit:

“An AI-based vulnerability prioritization tool lacked detailed logs explaining how decisions were made, which required remediation to improve traceability.”

Responsibility was an aspect of human and not technical responsibility. Participant 8 supported this stand from a leadership standpoint:

“Accountability should always rest with leadership and designated system owners. AI should support, not replace, decision-making.”

Overall, the governance issues were identified as a serious hindrance by the participants, who had to improve documentation, audit trails, role definition, and explainable AI mechanisms. The evidence shows that even though AI brings about operational efficiency, it also requires stronger governance frameworks in place to enhance compliance, transparency, and responsible security decision-making.

4.3.5 Theme 5: Balancing Automation and Ethical Responsibility in AI-Driven Security

A common consensus among the participants was that the advantages of AI-based automation in vulnerability management must be carefully weighed with ethical responsibility and control of operations. Instead, they recommended full automation; the participants instead recommended controlled risk-based models of automation that would retain human agency over high-impact decision-making.

Participant 2 stressed the need to establish clear limits of automation:

“Low-risk actions can be fully automated, while high-risk or high-impact decisions require human approval.”

Participant number 4 echoed this level approach, in which he emphasized the dangers of automated enforcement in security operations:

“AI can automatically flag and rank vulnerabilities, but remediation actions such as blocking traffic or disabling accounts should involve human approval.”

Some of the participants emphasized that automation must not reduce accountability but efficiency. Participant 15 described this balance within the framework of the automation of security operations:

“AI is very effective at triage and recommendation, but humans must approve or oversee actions such as account suspension or network isolation.”

Ethical automation also enablers were found to be training and governance. Participant 25 emphasized the importance of organizational preparedness:

“Automation should be paired with education, so teams understand AI limitations and ethical responsibilities.”

Participant 20 added to the idea of human management of client environments:

“AI-driven recommendations and actions must be reviewed by human analysts to ensure they align with client-specific policies.”

Overall, the results indicate that a responsible approach to AI use is the adoption of tiered automation, effective governance systems, constant monitoring, and employee education. Contributors did not see ethical responsibility as a constraint on automation, which, according to them, is a precondition to maintain a sustainable and reliable AI-managed vulnerability management.

4.4 Chapter Summary

- AI-driven transformation of Vulnerability management: From the traditional approach, AI driven vulnerability management has changed drastically from reactive to predictive, risk-based approaches resulting in faster detection, improved prioritization and reduction in dwell time.
- Human-AI collaboration: The need for human intervention is a must while AI enhances efficiency and pattern recognition. The decision-making power should remain with humans to prevent operational risks, maintain accountability and balance automation with responsible governance.
- Dwell time and zero-day Vulnerability: AI is more capable of detecting any changes and predicting the outcomes, also accelerating the response from minutes to days on a traditional model.
- Governance, Compliance and Accountability in AI-Driven Security: It is noted that AI brings about operational efficiency, it also requires stronger governance frameworks in place to enhance compliance, transparency, and responsible security decision-making.
- Ethical Implications of AI in Vulnerability Management: Ethical responsibility is not a constraint in automation however there are very little frameworks in place regarding ethics in vulnerability management and needs to be developed.

The chapter introduced the results and the discussion of the research, and five major themes were outlined to reveal how AI is transforming the nature of vulnerability management with predictive, risk-oriented practices, and the importance of human regulation, ethical accountability, and strong

governance. The results are mostly consistent with the literature that already exists and give an extension to it that incorporates practitioner-based knowledge about the issues of automation, compliance, and accountability in AI-driven security systems. It's found that from the traditional approach AI driven vulnerability management has changed drastically from reactive to predictive, risk-based approaches resulting in faster detection, improved prioritization and reduction in dwell time. It's also noted that the human in the loop is the right approach rather than a fully autonomous model. The decision-making power should be with humans which will ensure accountability. One of the capabilities of the AI integrated vulnerability systems is the ability to detect any changes and predict the outcome. Machine learning detects any anomalies in the code and finds a potential threat and mitigates it before the vulnerability has materialized. A need for a stronger governance and ethical framework is required as the current models focus more on the traditional approach and are not well suited for the AI based technologies.

The study provides a more in-depth insight into the practical contexts of AI adoption in cybersecurity through a qualitative analysis. The insights are the basis of the following chapter that will be devoted to implications, recommendations, and final reflections.

Chapter 5: Discussion and Recommendations

Introduction to the chapter

This chapter Discussion and Recommendations will be more aligned towards what we have identified over the course of this research. We will discuss further the main findings from chapter 4 and how the research answers our research objectives. We will also discuss the summarized answers in detail from the research participant over the research questions.

5.1 Overview of Key Findings

Regarding the vulnerability management practices from the study conducted and comparing with theoretical knowledge, this study confirms the existing research by demonstrating that AI-driven vulnerability management shift from the reactive based management to predictive, risk-based approach resulting in faster detection and improved remediation. The findings give a detailed overview of what the current practices are and what AI assisted vulnerability management can

offer. This address the first objective of the research, “what were the strengths and limitations of current methodologies in vulnerability management”.

Human-AI collaboration and the limits of automation explain that the study supports the existing literature by showing that effective and ethical cybersecurity depends on human-AI collaboration, while AI enhances technical expertise, but human intervention is required to avoid operational risks, maintain accountability and have responsible governance. The experience of the participants proves these concerns since most of them mentioned that organizational reluctance to allow AI to perform actions with high impact without human confirmation. This part addresses our second objective of this research, “How did AI contribute to automating vulnerability detection and response in cybersecurity and the need of human intervention”.

Dwell time and zero-day vulnerability, research shows that AI is more capable of detecting the novel threats and accelerating response in terms of remediating those vulnerabilities. The need for human intervention is stressed as the research doesn’t recommend having a fully autonomous AI powered vulnerability management system. Its is also noted that it’s a two-edged sword as AI strengthens both defense and attack capabilities. The similar way AI can be used to protect it can also be used for destruction, so human oversight is essential in increasingly fast-paced threat landscape. This address our third objective, “To what extent was AI able to reduce the dwell time for zero-day vulnerabilities in cybersecurity systems?”.

The research confirms existing concerns about privacy, bias in AI, highlighting that ethical risks are practical and operational. The current ethical frameworks are insufficient in the real-world challenges, making ethics by design, transparency and human oversight essential components of AI vulnerability management systems. It is also noted that though governance and accountability frameworks are well defined in theory, the research reveals practical challenges in applying them to AI-driven vulnerability management, as the existing standards struggle to address AI’s dynamic, decentralized decision-making process. This part addresses our last objective, “What were the ethical and governance challenges associated with the use of AI-driven security systems?”.

5.2 Interpretation of findings

5.2.1 AI-Driven Transformation of Vulnerability Management Practices

The results of this research comply closely with and build on the reviewed literature in Chapter 2, especially as far as the transformation towards predictive, intelligence-based vulnerability management is concerned. The descriptions of continuous monitoring and proactive risk assessment offered by participants will prove the scholarly claims that AI can help organizations to transcend reactive and signature-based security models and adopt predictive ones to predict the line of exploitation before the attacks happen (Ma, 2021; Taherdoost, 2022). This empirical study confirms theoretical assertions that AI helps to improve situational awareness by matching vulnerable information with current threat intelligence.

In line with previous studies, participants identified AI-based prioritization as a decisive enhancement of the conventional vulnerability scoring systems. According to the literature, AI-based prioritization enhances the efficiency of remediation because it incorporates exploitability, asset criticality, and business impact in risk assessment operations (Komaragiri & Edward, 2022; Walkowski et al., 2021). The results of the study testify to these claims in fact and prove that AI-based prioritization minimizes alert fatigue, and it helps security teams to draw attention to the vulnerabilities that represent actual and direct threats.

Moreover, the study gives practical validation to the claims of dwelling time reduction of vulnerabilities, especially zero-day threats. According to previous research, AI's capacity to identify abnormalities and match clues of compromise may dramatically decrease the time gap between the appearance of vulnerabilities and their elimination (Ali et al., 2022; Adeola et al., 2023). The experience of participants supports this point of view, meaning AI-enhanced vulnerability management is found faster in detecting and responding due to integrating security decision-making into ongoing operational processes. Overall, all the findings support and frame the theoretical points of view by illustrating the transformation of AI-driven approaches into quantifiable improvements of the real-world vulnerability management practices.

5.2.2 Human–AI Collaboration and the Limits of Automation

The research results in the given study greatly support the available literature, according to which human-AI collaboration is at the core of effective and ethical cybersecurity practices. The focus of participants on human control is supported by other studies that recommend human-in-the-loop security models, where AI is not designed as an autonomous decision-maker, but a system that

supports a human decision (Chowdhury et al., 2022; Schoonenboom, 2023). This strategy represents theoretical arguments of how AI is fast and capable of recognizing patterns, but human expertise is needed to interpret context, make ethical decisions, and strategize.

The differentiation between the decision-support and fully autonomous AI systems is noticeable, especially in the findings. According to the previous research, autonomous AI responses related to security may pose operational and ethical risks, such as false positives, unintentional service disruption, and less accountability (Sehgal, 2024; Obuse et al., 2023). The experience of the participants proves these concerns since most of them mentioned that organizational reluctance to allow AI to perform actions with high impact without human confirmation. This empirical fact upholds the argumentation of the literature that AI autonomy must be limited within well-delineated parameters.

Nevertheless, the results also demonstrate a constant conflict between productivity and authority. Although AI automation can increase the speed of detection and decrease the number of analysts, the respondents were concerned that automation could lead to the loss of human judgment and responsibility. This conflict is based on the literature debates about the trade-off between operational efficiency and rigor of governance in AI-based security systems (Proudfoot, 2022; Taherdoost, 2022). Overall, the results can be consistent with the literature and have been further elaborated by demonstrating how organizations proactively negotiate such trade-offs within real-world security settings and do not go into fully autonomous AI solutions.

5.2.3 Dwell time and zero-day vulnerability

The result of the research falls 70% to the literature review on chapter 2, however it cannot be considered 100% as there are some discrepancies which came up on the research. According to Kaluvakuri (2024), Through the analysis of past attacks, AI can improve its techniques for affecting and addressing similar threats in the future. However, AI is still unable to handle completely new or complicated situations, despite adapting to having known ones. However, from the research it's clear that AI has the capability of finding the anomaly through machine learning, the use of behavioral analysis and anomaly detection can spot previously unseen attacks. It identifies the normal behavior pattern and any changes to the normal cycle. AI not only can trigger and alert but if mentioned, automation can be used to stop the attack. AI can significantly shorten the detection and the response times. So indirectly AI can be used as a predictive tool for threat prevention.

The use of full automation is not recommended in the research as it could lead to potential loss of accounts and unwanted downtime as the recommendation is to have human intervention and the decision-making power to be left on human shoulder.

The theoretical review of the incident management with AI enabled system is in line with the research as the alert and incident creation can happen in no time when the traditional approach could take days as it requires manual intervention. It also needs to be mentioned that AI can be a double-edged sword as attackers are also making use of AI for automating the discovery and exploitation. So, it's true that it shortens the dwell time however it speeds up the attack velocity as historically attack and defense had a grace period however now both usually happen in minutes.

5.2.4 Ethical Implications of AI in Vulnerability Management

The results of the present research indicate some ethical issues that are similar but are not confined to the current discussions on AI ethics and cybersecurity. The issues of privacy, bias, and over-surveillance expressed by the participants are well-documented risks of AI-based security systems that are based on mass data gathering and analysis of behavior (Chitimoju, 2023; Vemuri et al., 2023). The application of sensitive logs, data showing how human beings behave, and network telemetry leaves the question of proportionality, consent, and data minimization a critical concern, especially in regulated settings.

Another vital question of ethics was bias, which Gates et al. (2022) later found may be associated with training AI models on incomplete or biased datasets to make unfair or inaccurate security judgments. According to the experiences of the participants, this bias may result in blind spots in vulnerability identification or excessive focus on a particular system or user, which may provide a practical complement to the abstract concept of algorithmic fairness. These results highlight the fact that ethical risks are operational but not abstract in AI-enabled vulnerability management.

Although governance frameworks, including GDPR, ISO standards, or AI ethics guidelines, are meant to deal with these issues, participants expressed their insufficiency in practice. Current frameworks focus on compliance and accountability, but in many cases do not give much advice on how to address ethical tensions that occur due to constant monitoring and automated decisions (Baeza-Yates, 2022; Macnish & van der Ham, 2020). The results thus contribute to the current ethical discussions by proving the gap between the intentions of regulations and the realities of their operations and showing that ethics-by-design thinking and the inclusion of privacy protection,

transparency, and human control as direct components of AI-based security mechanisms are critical.

5.2.5 Governance, Compliance, and Accountability in AI-Driven Security

The results of the current research indicate the existence of a definite discrepancy between the models of governance offered in literature and the reality of applying AI-based vulnerability management to practice. Current studies highlight the application of structured governance frameworks, including the NIST Cybersecurity Framework and the ISO/IEC 27001, as the means of risk, accountability, and compliance management in security operations (Taherdoost, 2022; Vielberth et al., 2020). Nevertheless, the experiences of participants indicate that such frameworks were not initially created in such a way as to support the dynamic, adaptive, and opaque nature of AI systems.

Other common issues reported by participants were the inability to match AI-generated output with existing regulatory standards, especially data protection, auditability, and explainability. Although regulatory tools, including GDPR, entail visibility and responsibility, the interviewees reported difficulties in the implementation of these principles in situations where AI systems generate decision logic that is hard to understand or interpret (Ahmed, 2024; Salako et al., 2024). This observation confirms prevailing criticism that systems of governance tend to keep pace with technological advancement and provide ambiguity in compliance with AI-supported security settings.

The accountability mechanisms that have been identified in the literature focus on well-defined ownership, audit trails, and decision traceability (Ayeola, 2025; Bruschi & Diomedede, 2022). Even though the participants saw the significance of these mechanisms, they claimed that additional work, which includes improved documentation, redesigning of governance, and the coordination of stakeholders, is needed to implement the mechanisms within AI-driven systems. These obstacles seem peculiar to the AI-enabled security systems, with decision-making being decentralized between algorithms and humans. In general, the results can contribute to the literature by showing how governance and accountability, though their definitions are theoretically clear, are difficult to implement successfully in AI-based cybersecurity situations.

5.3 Contribution to knowledge

From the study and research conducted, the contribution to existing knowledge is as follows.

- Research reiterates the significant value of integrating AI into vulnerability management, demonstrating a clear shift from the traditional reactive approach to more proactive and predictive security models. The conventional methods relied on known threat signatures and concentrated on the post threat responses while the AI based systems enabled continuous monitoring, real-time analysis and early detection. The early detection helped to reduce the vulnerability dwell time there by limiting the window of opportunity for exploitation.
- Another key contribution of this study is its practical validation of AI's effectiveness in addressing the zero-day threats. All the prior research suggested that AI relies on the existing threat database and can only identify known patterns of exploitation. However, the findings of this study challenges that assumption by demonstrating that AI can analyze anomalies in the code and predict protentional exploit path without prior knowledge. This indicates that AI is not just a detection tool but also a predicative mechanism capable of anticipating and mitigating threats before they have materialized.
- Earlier studies have suggested a fully automated process as a capability of AI and suggested human in the loop models; this research takes a more defined stance by emphasizing that decision making capacity should be left on human experts. Rather than supporting the fully autonomous models, this study highlights the importance of human oversight to ensure contextual understanding, ethical judgement and accountability. AI should be an addition instead of replacing human capabilities.
- Finally, the research identifies a critical gap in current governance and compliance frameworks. Even though a governance structure exists, they are more for static systems and are not well suited for the adaptive and evolving nature of AI based models. This mismatch creates challenges in ensuring accountability, transparency and regulatory compliance. As a result, the study underscores the need for robust, AI specific governance models that can ensure secure, ethical and aligned with organizational and regulatory models.

5.4 Practical and Policy Implications

It's very evident that the current governance model is inadequate for the AI assisted security models so the research should help people associated with vulnerability management with the need to create a stronger governance model. The research should fill the research gap which is present regarding the zero-day vulnerabilities and the need for a stronger Ethics model in terms of AI assisted vulnerability management models.

5.5 Summary

This chapter we identified the key findings and the interpretations of the findings. It's clear that even though some of the objectives were in line with technical papers already published but there were few findings regarding the zero-day vulnerabilities, Ethical and Governance models which were found differently compared to the published papers. So, it's noted that this research should help professionals associated with security side in creating a stronger governance structure. Overall, the study adds to the body of existing research, which has been filling the gap between the theoretical discourse of AI-based vulnerability management and practical practitioner-based results. The next chapter will provide the conclusion and final recommendations and conclude with the research.

Chapter 6: Conclusion and Recommendations

6.1 Summary of the study

The research aim was used to guide the study in the context of analyzing how AI is integrated into vulnerability management systems and the effects of AI integration on the improvement of threat detection and response. Based on this objective, the research questions were restated as follows to guide the methodology approach:

1. What were the strengths and limitations of current methodologies in vulnerability management?
2. How did AI contribute to automating vulnerability detection and response in cybersecurity and the need for human intervention?
3. To what extent was AI able to reduce the dwell time for zero-day vulnerabilities in cybersecurity systems?
4. What were the ethical and governance challenges associated with the use of AI-driven security systems?

These were the questions that needed a qualitative investigation as they were based on professional experience, expert opinions, and contextual interpretations, and not numbers. The ability to comprehend the perceptions of cybersecurity practitioners regarding AI-based processes, how the new ethical issues were perceived, and how the vulnerability management practices currently in place were assessed required an investigative, open-ended study. The semi-structured interviews gave the participants room to discuss some of the subtle topics like automation, interaction between people and machines, and the organizational problems, aspects that were not effectively addressed using quantitative tools. Accordingly, the methodological process was consistent with the objective of the study, which was creating rich and in-depth insights into the role of AI in the contemporary vulnerability management process. The recruitment of participants was done by professional contacts and through the industry networks, the interviews were conducted using a combination of virtual platforms and in-person meetings. Duration for most of the interviews was 30-40 minutes. The sample of the research was comprised of professionals who conducted their activities in the sphere of cybersecurity, such as cybersecurity specialists, Security Operations Center (SOC) experts, AI engineers, IT executives, IT security management, and people engaged in the process of vulnerability assessment and threat detection. Thematic Analysis was employed to analyze the data; five themes were generated which address all four objectives of the research. Through research we were able to analyze the strengths and limitations of current methodologies in vulnerability management. We were also able to identify the need for human intervention in AI integration rather than having fully autonomous AI. From this research we were also able to identify unexplored areas of zero-day vulnerabilities, which were different to available literature, so this was an added contribution. Also identified the need for better framework for Ethical and Governance models.

6.2 Major findings and theoretical contribution

According to Kaluvakuri (2024), Through the analysis of past attacks, AI can improve its techniques for affecting and addressing similar threats in the future. However, it's found that AI can handle new and complicated vulnerabilities through machine learning capabilities, AI can analyze the codes and can predict any loopholes present. Which will help to be predictive compared to reactive. The use of full automation is not recommended in the research as it could lead to potential loss of accounts and unwanted downtime as the recommendation is to have human intervention and the decision-making power to be left on human shoulder.

In terms of governance framework, Participants expressed their insufficiency in practice despite having frameworks including GDPR, ISO or AI Ethic guidelines. Current frameworks focus on compliance and accountability, but in many cases do not give much advice on how to address ethical tensions that occur due to constant monitoring and automated decisions (Baeza-Yates, 2022; Macnish & van der Ham, 2020). The results thus contribute to the current ethical discussions by proving the gap between the intentions of regulations and the realities of their operations and showing that ethics-by-design thinking and the inclusion of privacy protection, transparency, and human control as direct components of AI-based security mechanisms are critical.

We were also able to reiterate the need for AI in vulnerability management and how it contributes to a better security model.

6.3 Limitations of the study

Despite the contribution, there are several limitations that this study can be attributed to. To begin with, the study used a qualitative approach and a purposive sample of cybersecurity professionals. Although it allowed the in-depth research of the expert viewpoints, no statistical generalization of the findings to all organizations and industries is possible. The findings are rather contextual, based on the experience of participants, which can differ with organizational maturity, sector, and regulatory conditions.

Second, the paper paid more attention to the perceptions of practitioners concerning AI-enabled vulnerability management instead of measuring the performance of the system or quantitative security results. Because of this, the findings of better detection accuracy, shorter dwell times, or operational efficiency are drawn based on the reported experiences, not on empirical measures of performance. These findings can be reinforced by studies in the future that involve quantitative validation.

Third, the dynamic character of AI technologies and regulatory approaches is a limitation. AI-based security applications, governance systems, and compliance policies keep evolving; that is why there are some insights that might not be as relevant in the future as AI-based technologies and AI-related governance standards grow (Afolalu & Tsoeu, 2025). Also, the research involved self-reported information that can be professionally biased or restricted by the organization from reporting on sensitive security practices.

Lastly, the research scope, given the focus on vulnerability management, did not extensively investigate the related fields like adversarial AI, abusive use of AI in offensive security, or long-

term socio-technical effects. Although the issues raised in these discussions were indirect in the discussion of the participants, these topics were not within the scope of the study, but they should be investigated.

6.4 Future Scope

Resting on the findings and limitations identified, several recommendations regarding future research, practice, and policy may be advised. In the case of organizations, AI use in vulnerability management is suggested to be in a risk-based and tiered automation strategy. Detection, correlation, and prioritization, which present a low risk, may be automated, and the high-impact remediation actions should be left to humans. Companies must also make efforts in lifelong learning as a way of making sure that security personnel are familiar with AI-generated information, restrictions, and ethical implications (Farghaly et al., 2025; Kamya, 2025).

Governance and leadership-wise, explainability, auditability, and accountability should be prioritized by security leaders when implementing the work of AI-driven systems. Bringing explainable AI mechanisms into the work process and keeping audit trails in detail can contribute to finding the gap between what is required by regulations and how it is used in practice (Lizzy Ofusori et al., 2025). The leadership must also make sure that there is a match between the AI's ability and the organizational risk tolerance, which supports the human-in-the-loop decision-making systems.

The findings can inform policymakers and regulators to employ adaptive governance frameworks that accommodate the peculiarities of the AI-enabled security systems. The current regulatory tools are to be further increased to give more precise advice regarding the transparency, accountability, and ethical application of AIs in cybersecurity scenarios (Afolalu & Tsoeu, 2025). Regulators, industry practitioners, and researchers need to work closely to ensure that the governing structures are relevant and effective.

Future scholarly studies need to consider mixed techniques that will integrate qualitative findings with quantitative performance measurement of AI-based vulnerability management systems. The longitudinal studies of AI adoption with time would also be of great interest in terms of sustainability, trust, and organizational learning. Also, it is necessary to study more privacy-preservation AI methods, bias or alleviation, and defensive consequences of AI abuse by competitors (Komaragiri & Edward, 2022; Raju & Nadella, 2024).

Conclusively, although AI can be used to boost the effectiveness of managing vulnerabilities and increasing cybersecurity resilience, the achievement of this concept relies on the responsible usage that balances automation with morality, management, and human knowledge. The future of secure and trustworthy AI-driven cybersecurity systems will be hinged on the issues raised to address them.

6.5 Final Conclusion

This paper aimed to review how artificial intelligence (AI) can be integrated into vulnerability management systems and the influence of AI on threat detection, response effectiveness, ethical governance, and organizational decision-making as a part of cybersecurity practices. Using qualitative information gathered during conversations with cybersecurity practitioners, the study proves that AI has already become a disruptive element of the vulnerability management framework that allows replacing the reactive and periodic scan with a predictive, continuous, and risk-based approach to security. These results confirm the emerging belief that AI is a fundamental next level in cyber defense as it is more scalable, faster, and has a better analytical capacity than traditional methods (Afolalu & Tsoeu, 2025; Kamya, 2025).

The research validates that AI-based prioritization of vulnerabilities enhances the effectiveness of remediation by considering contextual data like the likelihood of exploits, asset-criticality, and the impact of operation. This is consistent with the fact that machine learning-based scoring mechanisms have been shown to be more efficient than the severity models that are not dynamic (Balsam et al., 2025; Komaragiri & Edward, 2022). Participants repeatedly pointed out that this kind of prioritization helps to decrease the level of fatigue among the people in charge of their respective alerts, as well as enables the security teams to be more strategic in resource allocation. Also, the results indicate that AI helps to decrease the dwell time of vulnerabilities as it allows timely detection and reaction to them, especially in dynamic and cloud-based settings (Raju & Nadella, 2024).

Nonetheless, the study also points to the fact that the implementation of AI also brings up major ethical, governance, and accountability issues. The study participants were deeply worried about privacy, bias, explainability, and over-automation, which supports the claims in the literature that AI-driven security systems must be developed so that transparency and explainability are

considered (Lizzy Ofusori et al., 2025). Notably, the results highlight the fact that AI can neither work as a force nor ethically in the absence of human control. Human-in-the-loop frameworks were always regarded as critical to contextual judgment, responsibility, and moral control, and argued in favor of hybrid human-AI systems suggested in the recent research (Farghaly et al., 2025).

Overall, the study adds to the body of existing research, which has been filling the gap between the theoretical discourse of AI-based vulnerability management and practical practitioner-based results. It shows that AI can positively impact the security functions, although its value will depend on the responsible use, effective governance frameworks, and ongoing human engagement. These findings support the rationale of the balanced measures in AI adoption that would ensure that technological innovation can be in line with moral responsibility and organizational sustainability.

References

- Ademilua, D. A., & Areghan, E. (2022). AI-Driven Cloud Security Frameworks: Techniques, Challenges, and Lessons from Case Studies. *Communication in Physical Sciences*, 8(4), 674–688. <https://journalcps.com/index.php/volumes/article/view/536>
- Adeola, S., Ige, B., Chukwuemeka, C., Adeyemo, P., Oladipupo Amoo, N., & Adeoye, N. (2023). AI-driven security for next-generation data centers: Conceptualizing autonomous threat detection and response in cloud-connected environments. *GSC Advanced Research and Reviews*, 15(2), 162–172. <https://doi.org/10.30574/gscarr.2023.15.2.0136>
- Adeoye-Olatunde, O., & Olenik, N. (2021). *Research and Scholarly Methods: Semi-structured Interviews*. Department of Pharmacy Practice Faculty Publications. <https://docs.lib.purdue.edu/phprpubs/6>
- Ahmed, F. (2024). Cybersecurity Policy Frameworks for AI in Government: Balancing National Security and Privacy Concerns. *Golden Sun-Rise International Journal of Multidisciplinary on Science and Management*, 1, 3048–5037. <https://doi.org/10.71141/30485037/V1I4P107>
- Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., & Kim, K.-I. (2022). Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. *Electronics*, 11(23), 3934. <https://doi.org/10.3390/electronics11233934>
- Álvarez González, M., Moreno Espino, C., Hadfeg Fernández, Y., & Cepero Pérez, N. (2024). Ethics in Artificial Intelligence: an Approach to Cybersecurity. *Inteligencia Artificial*, 27(73), 38–54. <https://doi.org/10.4114/intartif.vol27iss73pp38-54>

- Ashfaaq, M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2024). AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments. *ArXiv.org*. <https://arxiv.org/abs/2404.05602>
- Ayeola, F. (2025). AI-Driven Anomaly Detection and Data Governance: Securing Financial Systems, Cybersecurity Networks, and Regulatory Compliance in Multicultural Digital Ecosystems. <https://doi.org/10.2139/ssrn.5439102>
- Baeza-Yates, R. (2022). Ethical Challenges in AI. *Proceedings of the Fifteenth ACM International Conference on Web Search and Data Mining*. <https://doi.org/10.1145/3488560.3498370>
- Basuki, A., & Adriansyah, A. (2023). Response time optimization for vulnerability management system by combining the benchmarking and scenario planning models. *International Journal of Electrical and Computer Engineering (IJECE)*, 13(1), 561–570. <https://doi.org/10.11591/ijece.v13i1.pp561-570>
- Battina, D. S. (2021). The Challenges and Mitigation Strategies of Using DevOps during Software Development. *Papers.ssrn.com*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4004335
- Bennouk, K., Ait Aali, N., El, Y., Sebai, B., Faroukhi, A. Z., & Mahouachi, D. (2024). A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies. *Journal of Cybersecurity and Privacy*, 4(4), 853–908. <https://doi.org/10.3390/jcp4040040>

- Bruschi, D., & Diomedede, N. (2022). A framework for assessing AI ethics with applications to cybersecurity. *AI and Ethics*. <https://doi.org/10.1007/s43681-022-00162-8>
- Byrne, D. (2021). A Worked Example of Braun and Clarke's Approach to Reflexive Thematic Analysis. *Quality & Quantity*, 56(1), 1391–1412. <https://doi.org/10.1007/s11135-021-01182-y>
- Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive Sampling: Complex or Simple? Research Case Examples. *Journal of Research in Nursing*, 25(8), 652–661. <https://doi.org/10.1177/1744987120927206>
- Chitimoju, S. (2023). Ethical Challenges of AI in Cybersecurity: Bias, Privacy, and Autonomous Decision-Making. *Journal of Computational Innovation*, 3(1). <https://researchworkx.com/index.php/jci/article/view/69>
- Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A Delphi method-based study. *Computers & Security*, 113, 102551. <https://doi.org/10.1016/j.cose.2021.102551>
- Clough, M. (2025). Adoption of artificial intelligence-based cybersecurity tools at Georgia's two-year colleges. *Issues in Information Systems*, 26(1), 265–278. https://doi.org/10.48009/1_iis_2025_120
- European Union Agency for Cybersecurity (ENISA). (2025). *EUCC scheme – Guidelines on vulnerability management and disclosure (Version 1.1)*. <https://certification.enisa.europa.eu/document/download/5f61edd4-0151-4687-8a08->

[c11c103498f3_en?filename=EUCC_guidelines_vulnerability%20management%20and%20disclosure_v1.1_0.pdf](https://doi.org/10.1108/c11c103498f3_en?filename=EUCC_guidelines_vulnerability%20management%20and%20disclosure_v1.1_0.pdf)

Farghaly, M. S., Aslan, H. K., & Abdel Halim, I. T. (2025). A hybrid human–AI model for enhanced automated vulnerability scoring in modern vehicle sensor systems. *Future Internet*, 17(8), 339. <https://doi.org/10.3390/fi17080339>

Hasan, R. (2024). Blockchain and AI: Driving the future of data security and business intelligence. *World Journal of Advanced Research and Reviews*, 23(1), 2559–2570. <https://doi.org/10.30574/wjarr.2024.23.1.2273>

Hashmi, E., Muhammad Mudassar Yamin, & Sule Yildirim Yayilgan. (2024). Securing tomorrow: a comprehensive survey on the synergy of Artificial Intelligence and information security. *AI and Ethics*. <https://doi.org/10.1007/s43681-024-00529-z>

Hennink, M., & Kaiser, B. N. (2022). Sample Sizes for Saturation in Qualitative Research: A Systematic Review of Empirical Tests. *Social Science & Medicine*, 292(1), 1–10. <https://doi.org/10.1016/j.socscimed.2021.114523>

Ismail, B. I., Abdul, S., Khan, S. M., Sattar, S. A., & Muhammad, S. (2025). AI for Cyber Security: Automated Incident Response Systems. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5477114>

Kaluvakuri, V. P. K. (2024). Revolutionizing Fleet Accident Response with AI: Minimizing Downtime, Enhancing Compliance, and Transforming Safety. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4927192>

- Kezron, I. E. (2024). Securing the AI supply chain: Mitigating vulnerabilities in AI model development and deployment. *World Journal of Advanced Research and Reviews*, 22(2), 2336–2346. <https://doi.org/10.30574/wjarr.2024.22.2.1394>
- Khalifa, M., & Albadawy, M. (2024). AI in diagnostic imaging: Revolutionising accuracy and efficiency. *Computer Methods and Programs in Biomedicine Update*, 5(100146), 100146–100146. <https://doi.org/10.1016/j.cmpbup.2024.100146>
- Komaragiri, V. B., & Edward, A. (2022). AI-Driven Vulnerability Management and Automated Threat Mitigation. *International Journal of Scientific Research and Management*, 10(10), 980–998. <https://doi.org/10.18535/ijstrm/v10i10.ec05>
- Lizzy Ofusori, Bokaba, T., & Mhlongo, S. (2025). Explainability and interpretability of artificial intelligence use in cybersecurity. *Deleted Journal*, 28(1). <https://doi.org/10.1007/s10791-025-09760-6>
- Ma, T. J. (2021). Remote sensing detection enhancement. *Journal of Big Data*, 8(1). <https://doi.org/10.1186/s40537-021-00517-8>
- Macnish, K., & van der Ham, J. (2020). Ethics in cybersecurity research and practice. *Technology in Society*, 63, 101382. <https://doi.org/10.1016/j.techsoc.2020.101382>
- McCombes, S. (2019). How to Write a Literature Review. Scribbr. <https://www.scribbr.com/dissertation/literature-review/>

- Merzae, S. (2022). AI in Enhancing Cybersecurity Incident Response. *International Journal of Artificial Intelligence and Machine Learning*, 6(8).
<https://itaimle.com/index.php/ijaiml/article/view/138>
- Mell, P., Bergeron, T., & Henning, D. (2005). *Creating a patch and vulnerability management program: Recommendations of the National Institute of Standards and Technology (NIST)* (NIST Special Publication 800-40ver2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-40ver2>
- Mohammed, A. (2025). Transforming SOC Operations: Harnessing the Power of AI and ML for Enhanced Threat Detection. *SSRN Electronic Journal*.
<https://doi.org/10.2139/ssrn.5197098>
- Morgan, K. (2023). Role of AI in Threat Detection and Zero-day Attacks. *Cybersecurity Undergraduate Research Showcase*. <https://digitalcommons.odu.edu/covacci-undergraduateresearch/2023spring/projects/4/>
- Mozersky, J., Walsh, H., Parsons, M., McIntosh, T., Baldwin, K., & DuBois, J. M. (2020). Are we ready to share qualitative research data? Knowledge and preparedness among qualitative researchers, IRB members, and data repository curators. *IASSIST Quarterly*, 43(4), 1–23. <https://doi.org/10.29173/iq952>
- Muppalaneni, R., Inaganti, A. C., & Ravichandran, N. (2024). AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning. *Journal of Computing Innovations and Applications*, 2(1). <https://ciajournal.com/index.php/jcia/article/view/8>

- Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. *International Journal of Qualitative Methods*, 22(1), 1–18. <https://doi.org/10.1177/16094069231205789>
- National Institute of Standards and Technology. (2020). *NIST special publication 800-53, revision 5: Security and privacy controls for information systems and organizations* (NIST SP 800-53r5). <https://doi.org/10.6028/NIST.SP.800-53r5>
- Nutalapati, P. (2024). Automated Incident Response Using AI in Cloud Security. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 2(1), 1301–1311. <https://doi.org/10.51219/jaimld/pavan-nutalapati/299>
- Obuse, E., Etim, E. D., Essien, I. A., Cadet, E., Ajayi, J. O., Erigha, E. D., & Babatunde, L. A. (2023). AI-Powered Incident Response Automation in Critical Infrastructure Protection. *Deleted Journal*, 3(1), 1156–1171. <https://doi.org/10.62225/2583049x.2023.3.1.4899>
- Oladayo Aramide, O. (2025). AI-Driven Automated Incident Response and Remediation in Networks. *International Journal of Technology, Management and Humanities*, 11(02), 1–9. <https://doi.org/10.21590/ijtmh.11.02.09>
- Pan, S. C. (2023). Writing a Literature Review. Psychology.ucsd.edu. <https://psychology.ucsd.edu/undergraduate-program/undergraduate-resources/academic-writing-resources/writing-research-papers/writing-lit-review.html>
- Proudfoot, K. (2022). Inductive/Deductive Hybrid Thematic Analysis in Mixed Methods Research. *Journal of Mixed Methods Research*, 17(3), 308–326. <https://doi.org/10.1177/15586898221126816>

- Ramamoorthi, V. (2021). AI-driven cloud resource optimization framework for real-time allocation. *Journal of Advanced Computing Systems*, 1(1), 8–15. <https://doi.org/10.69987/>
- Reeves, A., & Ashenden, D. (2023). Understanding decision making in security operations centres: building the case for cyber deception technology. *Frontiers in Psychology*, 14. <https://doi.org/10.3389/fpsyg.2023.1165705>
- Risse, N., Böhme, M., & Böhme, M. P. I.-Sp, M. (2024). Uncovering the Limits of Machine Learning for Automatic Vulnerability Detection. <https://www.usenix.org/system/files/usenixsecurity24-risse.pdf>
- Salako, A. O., Fabuyi, J. A., Taiwo, A. N., Selesi-Aina, O., Louisa, D.-O. D., & Olaniyi, O. O. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance. *ScienceOpen Library*. <http://journal.submanuscript.com/id/eprint/2644/1/Salako17122024AJRCOS127573.pdf>
- Schoonenboom, J. (2023). The Fundamental Difference Between Qualitative and Quantitative Data in Mixed Methods Research. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 24(1). <https://doi.org/10.17169/fqs-24.1.3986>
- Sehgal, J. (2024). Enhancing Site Reliability Engineering: Scalable Strategies for Automated Incident Response and System Resilience. *Journal of Artificial Intelligence, Machine Learning and Data Science*, 2(4), 2484–2488. <https://doi.org/10.51219/jaimld/jaya-sehgal/533>

SentinelOne. (2025). AI Vulnerability Management: Risks, Tools & Best Practices. SentinelOne.

<https://www.sentinelone.com/cybersecurity-101/cybersecurity/ai-vulnerability-management/>

Sreekumar, D. (2023). *What is research methodology? Definition, types, and examples*. Paperpal.

<https://paperpal.com/blog/academic-writing-guides/what-is-research-methodology>

Srinivas, S., Kirk, B., Zendejas, J., Espino, M., Boskovich, M., Bari, A., Dajani, K., & Alzahrani, N. (2025). AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation.

Journal of Cybersecurity and Privacy, 5(4), 95. <https://doi.org/10.3390/jcp5040095>

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics*, 11(14), 2181.

<https://doi.org/10.3390/electronics11142181>

Vemuri, N., Thaneeru, N., & Tatikonda, V. M. (2023). Securing Trust: Ethical Considerations in AI for Cybersecurity. *Journal of Knowledge Learning and Science Technology ISSN*

2959-6386 (Online), 2(2), 167–175. <https://doi.org/10.60087/jklst.vol2.n2.p175>

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, 8, 227756–227779.

<https://doi.org/10.1109/access.2020.3045514>

Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers & Security*, 120,

102805. <https://doi.org/10.1016/j.cose.2022.102805>

Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability Management Models Using a Common Vulnerability Scoring System. *Applied Sciences*, 11(18), 8735.

<https://doi.org/10.3390/app11188735>

Wilson, C., Janes, G., & Williams, J. (2022). Identity, positionality and reflexivity: Relevance and application to research paramedics. *British Paramedic Journal*, 7(2), 43–49.

<https://pmc.ncbi.nlm.nih.gov/articles/PMC9662153/>

Zaib, R., & Zhou, K.-Q. (2022). Zero-Day Vulnerabilities: Unveiling the Threat Landscape in Network Security. *Mesopotamian Journal of CyberSecurity*, 2022, 57–64.

<https://doi.org/10.58496/MJCS/2022/007>

Zhuang, Y., Liu, Z., Qian, P., Liu, Q., Wang, X., & He, Q. (2021). Smart Contract Vulnerability Detection Using Graph Neural Networks.

<https://www.ijcai.org/proceedings/2020/0454.pdf>

Zichen, R. (2025). AI-driven Threat Detection in Zero Trust Environments.

<https://doi.org/10.2139/ssrn.5146272>

Appendix A: Interview Questions

Q1. How do you think the AI is changing the way vulnerabilities are detected and managed in cybersecurity and the techniques used?

Q2. What ethical concerns do you associate with the use of AI in security systems?

Q3. In your experience, how important is maintaining human oversight alongside AI in threat detection and response?

Q4. Have you encountered any challenges related to compliance or governance when implementing AI-based security solutions? If so, please provide an example.

Q5. What steps should organizations take to ensure transparency in AI-driven vulnerability management systems and the privacy risks associated with AI?

Q6. How can accountability be ensured when AI is responsible for making security decisions?

Q7. How can organizations balance the benefits of automation with the need for ethical responsibility in AI security tools?

Q8. Are you aware of any existing (global or local) policies or frameworks that effectively govern AI applications in vulnerability management?

Q9. Looking forward, how do you see AI evolving to better address both technical and ethical challenges in cybersecurity?

Appendix C: Thematic Coding table

Table 4(b) Thematic / Coding Table

Theme	Sub-Themes	Initial Codes (Examples)	Illustrative Participant Evidence (Indicative)
Theme 1: AI as a Catalyst for Proactive and Risk-Based Vulnerability Management	Predictive security Continuous monitoring Risk-based prioritization	Proactive detection Real-time analysis Exploit likelihood Business impact	“AI enables continuous vulnerability assessment rather than periodic scanning” (P2)

Theme 2: Human Oversight as a Non-Negotiable Component of AI-Driven Security	Human-in-the-loop models Decision validation Contextual judgment	Human approval Expert judgment False positive risk Operational impact	“AI lacks contextual understanding and judgment” (P1)
Theme 3: Dwell time and zero-day vulnerability capability of AI	Dwell time zero-day Over-surveillance	Adapt User monitoring Faster Identification Automation	“AI can adapt to new traffic behaviors and detect previously unknown weaknesses, enabling faster identification and mitigation of network vulnerabilities” (P16)
Theme 4: Governance, Compliance, and Accountability Challenges in AI Adoption	Regulatory compliance Auditability Accountability structures	GDPR constraints Explainability gaps Audit trails Role ownership	“AI-based tools conflicted with our existing audit requirements” (P3)
Theme 5: Balancing Automation and Ethical Responsibility in AI-Driven Security	Theme 5: Balancing Automation and Ethical Responsibility in AI-Driven Security	Low-risk automation High-impact human approval Policy enforcement Staff awareness	“Automation should enhance, not replace, human expertise” (P25)