The Role of Artificial Intelligence in Incident Response for Digital Domain SMEs

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Esther Oluwawemimo

Supervisors:
Prof. Jouni Isoaho
Dr. Tahir Mohammad

May 2024

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Esther Oluwawemimo
Title: The Role of Artificial Intelligence in Incident Response for Digital Domain SMEs
Number of pages: 80 pages
Date: May 2024

The rate of cybersecurity attacks on small to medium enterprises (SMEs) has been rapidly advancing in recent years. The use of artificial intelligence (AI) is one emerging technology that has grown significantly in the cybersecurity field and has great potential to combat the effects of cyberattacks by enabling more advanced and efficient incident response processes. AI-based incident response solutions can detect and respond to cybersecurity incidents by analysing large amounts of data and identifying suspicious patterns. This technology gives SMEs a security edge by automatically responding to incidents in real-time.

This research study aims to analyse the role of artificial intelligence in incident response for digital domain SMEs. It also evaluates the maturity level of SMEs by measuring their overall security posture regarding the utilisation of AI in incident response. A survey questionnaire is the empirical method used to gather quantitative data systematically in this research study.

53 participants from various digital domain sectors with various years of work experience in cybersecurity made up the sample population pool for this study. The quantitative data were analysed using inferential statistics, with 6 major sections covering general information, cybersecurity awareness, incident response management, security controls and technology, current usage of AI, and experiences.

The study's results show that organisations using AI in their incident response processes can detect and respond to incidents more quickly and at a faster rate than those not utilising AI. Three major areas of limitations in using AI affecting SMEs were indicated: lack of expertise, cost limitations, and difficulty integrating AI solutions with existing systems. This study concluded that a low percentage of SMEs are utilising AI in incident response. Participants provided recommendations regarding the implementation and impact of AI in incident response for SMEs.

Keywords: Artificial intelligence, Incident response, Cybersecurity, SMEs.

Acknowledgements

My gratitude extends first and foremost to God Almighty for wisdom and strength to complete this master's thesis.

To my admirable supervisors, I deeply appreciate your dedication, advice, unwavering support, and guidance throughout this research study.

Special appreciation goes out to all the participants who sacrificed their precious time and provided insightful opinions related to the research. This study has substantial value because of your contributions.

My heartfelt appreciation goes to my partner and my beloved family for constant encouragement and emotional support during the entire process of this study.

Lastly, I would like to dedicate this research to my father, S.A. Oluwawemimo; without you, I never would have discovered my love and passion for cybersecurity. Thank you for being my rock from the beginning of this journey.

Table of contents

List of Figures

List of Tables

1 Introduction

1.1 Background Study

Small to medium enterprises (SMEs) are organisations that fall within the scope of having 10 to 250 employees. Micro enterprises will also be considered in this research; these are enterprises with less than 10 employees. According to (McEvoy, 2024) In 2023, there were more than 24 million SMEs in Europe, as can be seen in Figure 1, which breaks down the growth of micro, small, and medium enterprises over the period of 16 years. This amounts to a great deal of the European economy.

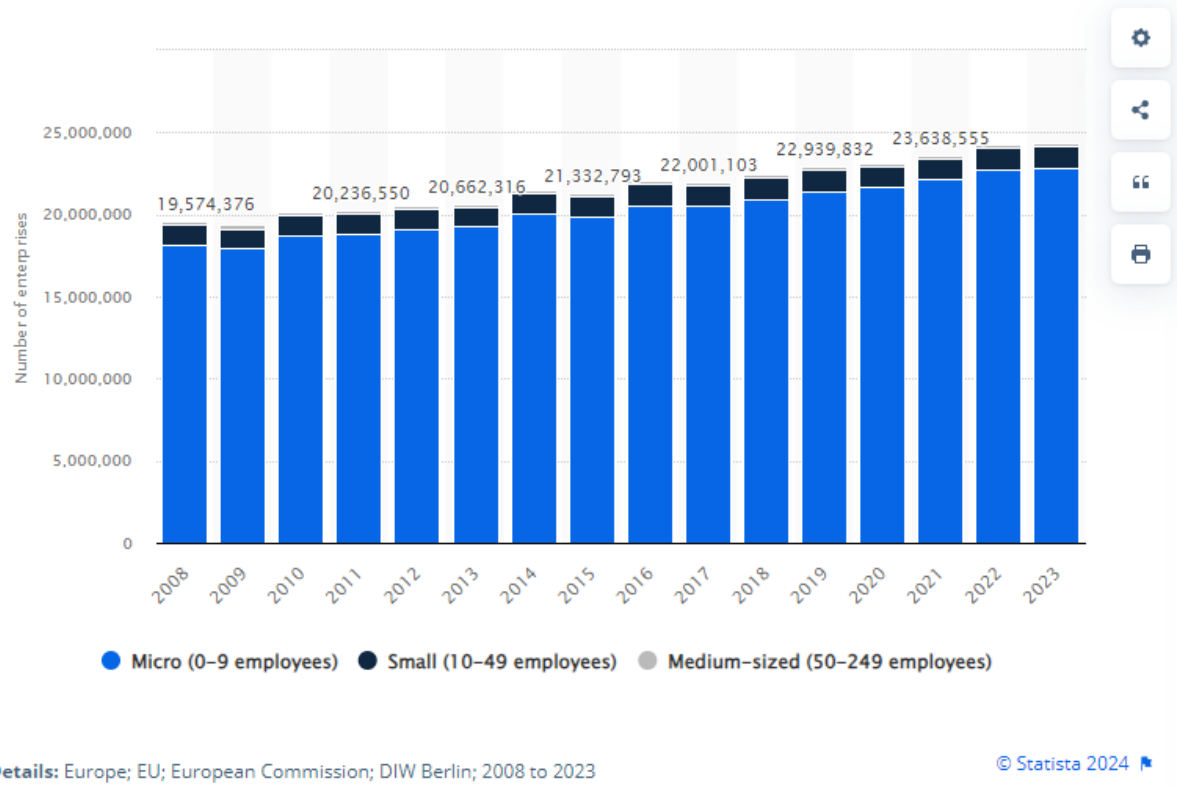

Figure 1: Graphical representation of employees and enterprises number from 2008 to 2023 (McEvoy, 2024)

According to Accenture's Cybercrime study, 43 per cent of cyber-attacks are on small to medium enterprises (SMEs)(Palatty, 2023). Attacks on SMEs are common and frequent because cyberspace keeps getting bigger, and even SMEs use digital technologies, which are prone to various cybercrimes. The attacks against SMEs have grown over the years because of weak corporate cybersecurity and challenges faced with implementing security because of new regulations being passed by the European Union's General Data Protection Regulation (GDPR) (Bada & Nurse, 2019). There are various actions that SMEs can take to improve their overall security, such as implementing a strong security culture and posture. The lack of sufficient employees to allocate to a security team in an SME is a major challenge.

One way to overcome that challenge is handing the enterprise's security to a Managed Security Service Provider (MSSP) to manage.

The risk of cybercrime is a growing risk faced by all organisations in general; using Google search to discover common attacks on SMEs produced attacks such as phishing, ransomware, malware, viruses and password hacking; these are few out of the numerous attacks that are targeted towards SMEs, most cyber-attacks start with intrusions and remain undetected, which makes SMEs have a false sense of protection because there has been no notification of attacks. (Harsch et al., 2014). SMEs can employ the approach of having an incident response management system to mitigate these risks.

Incident response management does not connote that an incident has occurred. It is a proactive strategy to prepare for an incident and take proper measures to respond to an incident that could happen. Incident response management encompasses setting a proper cyber defence strategy to protect an organisation's assets.

Incident response (IR) is the process of detecting and responding to cyber threats and attacks by a cybersecurity team. This can be done with the use of an incident response plan or playbook, which contains the specific ways to respond to specific attacks based on an organisation’s architecture and resources. It involves incident response processes of preparation, detection, containment, eradication, recovery, and lessons learned.

A successful incident can lead to a loss of reputation, financial loss, diminished brands, and loss of investor support, which doesn’t bode well for an organisation. (Schnepp et al., 2017).

The emergence of Artificial Intelligence (AI) is an important and productive technology that makes the process of incident response to cyber security attacks much easier. (Hassan & Ibrahim, 2023).

Artificial intelligence is a field of study that emerged in 1956. It can be used to simulate human intelligence and actions, resulting in the automation of cyber security with the ability to detect security breaches quickly in a network. AI is a solution to the growing need for advanced means of protecting cyberspace against evolving threats. This can be reflected during the COVID-19 pandemic, where cyber threats accelerated due to people working from home and having to oversee their organisation's security individually rather than having a security team in the office overseeing security; this period led to organisations depending on technologies like AI, Machine learning (ML) which is a subset of AI and big data. (Jada & Mayayise, 2023).

The lifecycle of cybersecurity can be impacted positively by AI, and this is worth exploring by organisations because the capabilities of AI, like automation, improved cyber defence, and threat intelligence, are beneficial to organisations. Most SMEs are not sufficiently capable of combating cyber threats because of limited resources, which makes them an easy target for cyber threat actors who are currently evolving in their methods of attacks and making use of services like malware-as-a-service, which can be easily purchased on the dark web to launch attacks, the use of AI technologies such as

automation of processes to defend the security would be advantageous to SMEs as performance and accuracy would be improved (Hofstetter et al., 2020).

Attacks such as malware, social engineering, and phishing emails have been reported by academia and industries as the most common cyber-attacks faced by SMEs (Chidukwani et al., 2022) can be detected easily and more accurately with the use of AI.

Machine Learning (ML), a branch of AI which was developed in the 1980s (Jada & Mayayise, 2023), is defined as the ability of computers to develop a model and learn with time-based on the data available to it, as well as adapt through experience and then improve the model. The use of ML and AI is important in handling data in terms of its management and security in the SME sector. SMEs would need to capitalise on AI and ML to improve their abilities and stay relevant and competitive in the market space. ML is the most common type of AI in cybersecurity, with various techniques to determine characteristic behaviours and patterns for attacks in cyberspace. (Rawindaran et al., 2021).

For AI systems to be valuable to the cybersecurity in SMEs, they must be able to see what human experts cannot see, and they must have the capability to assess security risks, note threats and be aware of vulnerabilities of the SMEs while being user friendly and affordable. (Hofstetter et al., 2020).

1.2 Problem Statement

Technology keeps evolving as the years progress; this has resulted in both positive and negative impacts on the use of technology over the years. Cybersecurity's objective is to ensure the confidentiality, integrity and availability of network systems and infrastructures; the development of AI in Cybersecurity is to help realise that goal. However, like a coin having two sides, AI can both enhance cyber-attacks and strengthen cyber defence.(Kant & Johannsen, 2022).

If attackers are using AI to enhance their cyber-attacks to have a more sophisticated attack on systems, then defending against such attacks with IT systems not integrated with any form of AI will be unsustainable for the security of the IT systems.

The limitations of SMEs concerning Cybersecurity are apparent due to limited resources. However, this does not stop the cyber-attacks faced by SMEs, which, based on the severity of the attack, could potentially shut down an enterprise. This is why it is not only important to deploy more defensive cyber security solutions but to also implement the use of AI in cyber security solutions like incident response systems to enhance the systems to provide smarter and faster crisis responses.

Based on the study from (Kant & Johannsen, 2022), the utilisation of AI is significantly lower in SMEs than in large organisations. This is an issue since SMEs contribute to a large percentage of the economies of numerous countries. There is a need for SMEs to harness the capabilities of AI, which is constantly evolving to protect against cyber-attacks (Jada & Mayayise, 2023). Speed is essential when investigating a suspected cybercrime. (Harsch et al., 2014) states that using AI for IR can help with not only speed but also accuracy in investigating cybercrimes and attacks.

Therefore, this study will focus on AI's impact on IR technologies, both its positive and negative impacts and the constraints on SMEs using AI in their IR management systems. This study will focus on two AI abilities in IR that are essential to SMEs: anomaly detection using a security information and events management (SIEM) system and clustering and categorisation using use cases of intrusion detection, malware detection, and phishing.

1.3 Aim and Objectives

This study aims to explore the role of AI in incident response for SMEs by providing a good background on AI and IR, evaluating the benefits of AI-based Cybersecurity systems used for incident response, and demonstrating how AI can be used to investigate, identify, report, and research in the IR lifecycle.
The objectives of this research are listed below:

1. To ensure that SMEs have adequate plans in place to prevent a cyber-attack on their organisation.
2. To respond to incidents timely so that the mean time to respond (MTTR) is as low as possible with the use of AI integrated cyber security solutions for incident response.
3. To address SMEs' limitations in utilising AI in their Incident Response system.
4. To measure the maturity level of SMEs in relation to the use of AI in their IR processes.

This results in reduced risks, usually accompanying incident events, such as financial loss or reputational damage.

1.4 Research Questions

This research study intends to address the primary research question: What is the role of artificial intelligence in incident response in a digital domain SME?
Below are listed the secondary research questions that will also be considered in answering the main research question:

1. How can AI expedite the response time in a cyber-attack for an SME?
2. How can AI be used to strengthen the cyber defence of SMEs?
3. How can AI be infused into the 6 phases of incident response for SMEs?

1.5 Report Structure

The report structure of this research study consists of six chapters, describing the chapters below.

Chapters 2, 3 and 4 cover the existing knowledge of the underlying concepts of this research study; these chapters contain extensive literature reviews.

Chapter 2 focuses on an overview of artificial intelligence based on literature reviews and findings from the cybersecurity industry. Chapter 3 discusses the 6 IR processes based on the NIST model and the integration and impact of AI in each process. Chapter 4 analyses two use cases of AI abilities in improving IR and a description of the incident response playbook. Chapter 5 focuses on the research methodology and survey design. Chapter 6 analyses information obtained from the survey pool about the role of AI in IR and provides a detailed comparison between industries using AI and industries that do not use AI in their incident response processes.

Chapter 7 is the last chapter, and it focuses on the conclusion results, discussion of findings, and recommendations derived from the survey conducted for this research.

2 State of Artificial Intelligence (AI) in Cybersecurity

2.1 Overview of Artificial Intelligence

The development of machines that can exhibit human behaviours and characteristics without exploiting living organisms is generally termed Artificial Intelligence. (Mijwil, 2015)Various articles state different dates of when AI started, making it difficult to pinpoint the exact date. (Haenlein & Kaplan, 2019). The common period recorded by articles and journals that marked the significant technological advancement dates back to the 1940s and 1950s. The process and timeline for making technological discoveries are not always smooth, and the idea of creating artificial intelligence also experienced a period of stunted growth between the years 1965 and 1970 (Mijwil, 2015), this, however, ended in 1970, when progress in development and knowledge of AI gained momentum after artificial intelligence systems were developed for disease diagnosis successfully. Artificial intelligence has continued to develop over the years and yielding successful and resourceful products that are useful to not just commercial and industrial aspects but also personal lives; it is crucial to note that the achievement of successful works related to artificial intelligence systems is not a cheap feat and requires a substantial amount of financial funding.

AI has advanced progressively in recent times and will continue to develop because of the steady rise in big data and advancements in computing power. (Haenlein & Kaplan, 2019).

2.2 Subsets of AI

There are various subsets of AI that focus on different aspects of AI research and AI applications within the field of AI. Each of these subsets has its own distinct limitations, approaches, applications, and advantages. When combined, they can create a rich, multifaceted field of AI. Subsets of AI can also be regarded as AI techniques such as machine learning, deep learning, natural language processing, computer vision and expert systems, which are used in Cyber security by Cyber security professionals to analyse big data, detect anomalies and identify threats before they escalate into actual attacks. (Thuraisingham, 2020).

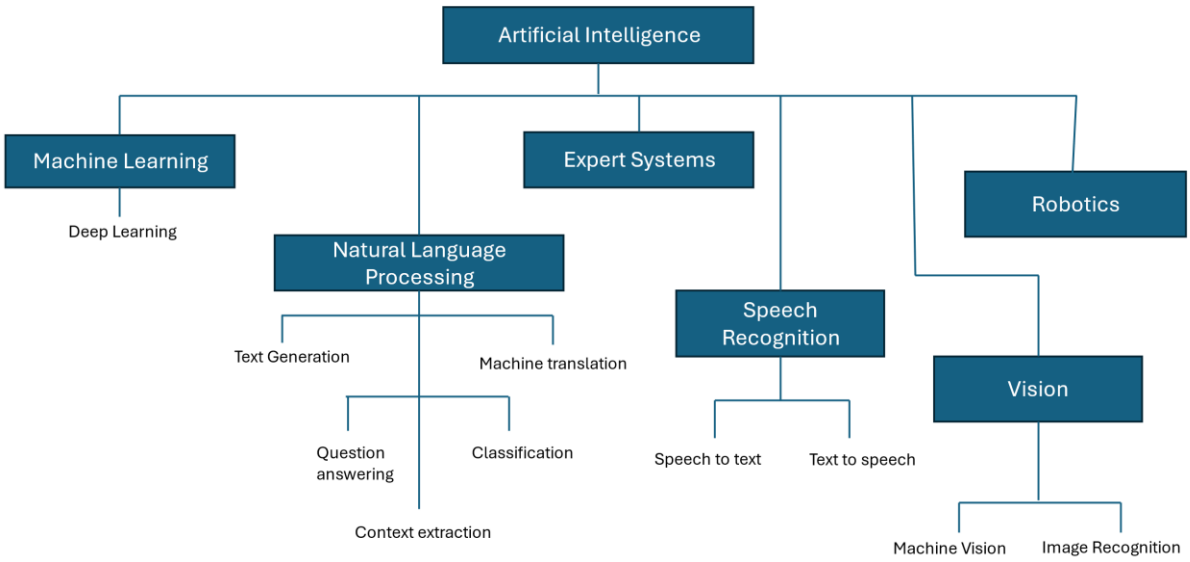

Figure 2: The subset of AI (Tripathi, 2023)

2.2.1 Machine Learning

Machine Learning (ML) is a subset of AI that focuses on creating algorithms and models that resemble the power of the brain for computer systems to learn from data on their own(Tripathi, 2023). It involves training algorithms to predict a response or make decisions based on available data.(Sale, 2023)AI systems utilising ML can learn with minimal human intervention, making them evolve and become more efficient. The concept of ML can be found in most applications of artificial intelligence.

Machine learning algorithms are divided into three models, which are discussed below.

Supervised learning: supervised machine learning algorithm involves using labelled data (Karthick & Gopalsamy, 2022), which has a desired output for each paired input data. The machine learning model is trained on the labelled data, and from the patterns the model discovers from the labelled data, it learns to make predictions on new and unlabelled data. An example of this machine learning can be found in applications such as speech recognition and fraud detection.(Sale, 2023).

Unsupervised learning: The unsupervised machine learning algorithm is the opposite of the supervised machine learning algorithm; it involves training on unlabelled data (Karthick & Gopalsamy, 2022), that is, the desired output for each input data is not known. The model picks up on patterns in the data without any explicit instruction. This is done with techniques such as clustering and dimensionality reduction. (Morovat & Panda, 2020). An example of this machine learning can be found in applications such as anomaly detection and recommendation systems.

Reinforcement learning: reinforcement machine learning algorithm can be likened to a person's natural intelligence; the model learns through trial and error while getting feedback in the form of

rewards or punishment, and the feedback gotten is based on the actions of the model(Tripathi, 2023). An example of this model can be found in robotics and gaming.

2.2.2 Deep learning

Deep learning can be categorised as a subset of AI and Machine Learning. A deep learning model is also referred to as deep neural networks. It focuses on creating artificial neural networks that can learn from data and make decisions and predictions based only on the data. It can extract features from unprocessed data automatically without engineering features.(Tripathi, 2023).

The deep learning model has progressed extensively to surpass human performance in some tasks, resulting in state-of-the-art performance. It is a supervised machine-learning model that trains neural networks to learn patterns from large data.(Sale, 2023). This enables it to make predictions based on learned patterns, and the feedback received by the model during the training process is used to update the model's parameters.

A deep learning model uses big data, an immense amount of complex training data. The algorithm uses multiple layers in the deep neural network to learn and make decisions without human intervention.(Coombes, 2023). The layers used are referred to as the input layer, which happens to be the first input provided for the AI system, and the hidden layer, which is the layer between the input layer and the output layer; this layer performs the computation for a task, and finally, the output layer, which creates the result of the first input that was provided for the AI system.

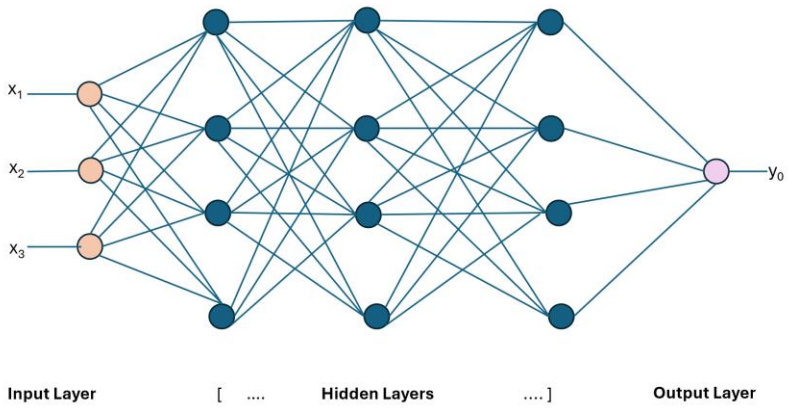

Figure 3: Deep neural network layer (Tripathi, 2023)

2.2.3 Natural Language Processing

Natural Language Processing (NLP) is a subset of AI that focuses on teaching computers human language for proper comprehension, interpretation, and production of human language(Sale, 2023). Various NLP techniques are involved in making computers process, examine and manipulate data, which can be text or speech. NLP allows AI to understand human language by letting machines analyse text data, extract meaning and generate human-like responses(Coombes, 2023). NLP uses techniques such as text analysis, language understanding, machine translation, text generation, question answering and dialogue systems(Tripathi, 2023). NLP uses various methodologies, such as deep learning models and machine learning algorithms. The combination of these techniques and methodologies produces the practical uses of NLP in chatbots, virtual assistants like Alexa and Siri, machine translation tools like Google Translate, and various other types of use cases.

2.2.4 Robotics

Robotics is a subset of AI that bridges the gap between AI and the physical world. It involves programming and designing machines to interact with the environment and carry out tasks normally requiring human intelligence. Robotics uses various AI techniques like machine learning, computer vision, and natural language processing(Sale, 2023).

AI is used to improve the performance of various areas of robotics, such as perception and sensing, planning and control, autonomous navigation, and medical robotics(Tripathi, 2023). Integrating AI and Robotics enables robots to perform difficult tasks with adaptability, greater autonomy, and efficiency. Robotics are not always metallic exoskeletons; the use of algorithms like deep neural networks and machine learning algorithms means that robotics does not always have a physical form and can occupy a digital space(Coombes, 2023).

2.2.5 Expert Systems

Expert systems are a subset of AI that can also be referred to as a knowledge-based system (Corbett & Sajal, 2023). It involves using sets of predefined rules and knowledge to make decisions and provide solutions to problems. One of the interesting features of Expert systems is the ability to replicate the decision-making processes of human specialists in different domains like healthcare, finance, engineering, manufacturing, and several other fields(Sale, 2023).

Expert systems have three components: knowledge base, where the knowledge database with information, rules and facts related to various domains and fields are stored. The inference engine is the second component of expert systems, where the information stored in the knowledge base is processed using inference rules and algorithms to make conclusions, recommendations, and decisions. The user interface is the third component of expert systems; this is the platform that allows users to interact with

the expert systems; it can be in the form of a graphical user interface (GUI) or a command line interface (CLI)(Tripathi, 2023).

2.3 Importance of AI

The role of artificial intelligence is of great importance in various fields and aspects of human life; AI can improve and optimise human life in various fields like the healthcare sector, IT industry, education, climate change, banking industry, and so many others. This proves that AI is a crucial technology for the future.

Below are some factors that showcase the importance of AI in the IT industry.

Enhancing security: AI has been instrumental in enhancing security; AI systems are employed in cybersecurity to protect networks, detect threats, and prevent threats in a security network. The use of machine learning and deep learning algorithms are used to detect trends and anomalies in network traffic, which is used to point to potential cyber-attacks, creating a chance to proactively prevent a successful intrusion (Rizvi, 2023a). AI, together with predictive modelling, can be used to prevent cyber-attacks by discovering potential threats before they occur, such as zero-day attacks. AI is also used for incident response. It fosters a better and faster incident response process, allowing organisations to respond to threats in real time, thereby minimising the effects of successful threats on an organisation.

Efficiency and Scalability: AI systems are regarded as efficient because of the ability to be trained, which results in certain tasks being performed faster and cheaper than when handled by humans. Scalability showcases the ability of AI systems to be able to complete numerous instances of a task (Bhatnagar et al., 2018). This can be reflected in the incident response process of detecting a threat. Using an AI system gives the advantage of being able to scale the task of detecting numerous threats simultaneously.

Error Reduction: The use of AI systems produces accuracy because AI programs and systems make the least amount of error(Nalbant, 2021). This is an important factor in the IT industry because errors can be catastrophic to an organisation's or individual's overall security posture.

Round-the-clock availability: People require time to rest and take breaks to become re-energized to work (Arjun C Vinod et al., 2022)In the case of security operation analysts who must constantly monitor network traffic to catch threats and vulnerabilities in systems and networks, the use of AI can alienate the need for constant human monitoring because AI systems can work indefinitely without needing breaks.

2.4 Threats Associated with AI

AI can be likened to a two-edged sword; as much as it can be used for defensive actions, it can also be utilised for offensive actions (Vaibhav Chandrasen Vaidya & Payal Tekchand Rewatkar, 2023). AI capabilities are inherently dual-use in nature.

AI-powered cyberattacks: The use of AI in cybersecurity creates the potential for AI-powered cyberattacks; threat actors will leverage the use of AI to produce sophisticated and targeted attacks as AI technology continues to evolve (Shanthi et al., 2023). Using AI algorithms to create advanced forms of cyberattacks makes it easier to deceive users and reduces the effectiveness of traditional security measures because the attacks bypass them (Rizvi, 2023a). AI-based algorithms can be implemented to devise evasion attacks, ensuring that attacks will not be detected. Also, attackers can modify data and system context to counteract the countermeasures designed by machine learning (Bergadano & Giacinto, 2023).

AI systems increase anonymity: AI systems have the potential to increase anonymity in security (Bhatnagar et al., 2018), this prevents transparency and accountability in tracing the origin of a threat and increases the risk of lack of non-repudiation, which is a goal of cybersecurity. This allows a threat actor to commit cybercrimes while retaining their anonymity.

Lack of transparency: it is difficult to understand how AI systems make decisions, making it hard to trust the systems. The lack of transparency in AI algorithms is a serious challenge (De Azambuja et al., 2023).

Ethical considerations and governance: when it comes to AI, as advanced as the technology keeps progressing, it has been difficult to incorporate ethics and morality into AI (Arjun C Vinod et al., 2022)This raises the threat of AI's potential if it cannot be controlled; it begs the question of where to draw the line between AI systems that benefit people and those that harm them. (Shanthi et al., 2023) discusses how there is no regulatory framework to oversee the use of AI in cybersecurity.

Unemployment has become rampant: According to (Khanzode & Sarode, 2020)AI systems' ability to perform mundane tasks initially affected only menial jobs, but as AI has progressed to being able to perform more technical and advanced tasks, it has led to an increase in unemployment problems for people whose jobs can now be performed by AI systems better, cheaper, and more efficiently.

2.5 Function of AI in a Cybersecurity Setting

According to (Crume, 2023) The functions of AI in cybersecurity can be categorized into four categories: investigation, identification, reporting, and research methods.

Investigation method: In a cybersecurity setting, if the need to investigate an issue arises, the concept of a knowledge graph can be invoked. A knowledge graph is a way of representing information about the physical or logical world as a data structure. Knowledge graphs are used to represent information so that if an incident occurs, the path to the incident can be mapped to make inferences.

Identification method: To identify a particular incident in detail with the use of AI, we look at logs; systems will record logs once an event occurs; this could be system logs, events logs, or network logs, all of which make up a log record. System logs usually consist of information about the events, such as

the time the event occurred, the date of the event, the entity that performed the event, what was done and the system the event occurred in.

Because of their volume, logs are usually cumbersome to read, so sorting through logs manually to find the source of an anomalous activity can be difficult. However, with machine learning, it becomes easy to spot an anomaly across multiple records.

Reporting method: There is a requirement in security that you make reports. These reports are used to determine whether regulatory requirements are being met. This can be done by gathering log records and processing them. The information gathered from log records can be used to enrich reporting data. Reporting tools such as Power BI can be used here.

Research method: Research can be considered as one of the backbones of cybersecurity. Cybersecurity research has been made easier with natural language processing systems like chatbots that connect to a database to answer questions.

However, (Agrawal et al., 2023) further breaks down how AI can be used to enhance cybersecurity with examples such as threat detection, fraud detection, vulnerability management, security automation, and network security.

AI can analyse data for attack detection and response in various domains of cyberspace (Morovat & Panda, 2020), this is done using AI methods such as ML/DL techniques to identify threats and prevent attacks from occurring. (Truong et al., 2020) take on the functions of AI in cyber security are that AI can be used to discover new changes in attack, as well as handle big data and AI can continuously learn to better respond to threats.

The ability of AI to identify and respond to threats and attacks quickly is a core part of incident response. The use of AI in identifying underlying causes of attacks by performing operations like threat analysis and incident triage is advantageous to security personnel by allowing them to focus on more sophisticated assignments and enabling swift and effective reactions to security issues in a cyber domain (Agrawal et al., 2023).

(Rizvi, 2023b) argues that threat detection and prevention are the major focus of AI in cybersecurity and creating automated incident response systems designed to evaluate data, identify potential threats and risks, and mitigate attacks. This is a stand that (Harel et al., 2017) agrees with, the author argues that automating threat detection and response is the most important function of AI in cybersecurity.

2.6 Related work on the use of AI in SMEs

In the article by (Rawindaran et al., 2022) Detection and Minimization of Malware by Implementing AI in SMEs, the researchers discuss how artificial intelligence can be used as an offensive and defensive mechanism and how SMEs can find a balance between IT expertise and the cost of products using applied machine learning techniques required to secure their data. Threat actors can access malware easily from the dark web with the use of malware-as-a-service (MAAS), which further broadens the

scope of people who can be regarded as threat actors since there is no need to have the skills to develop malware when you can get it with the use of AI technology. AI and ML can also be used to combat the threats of malware, in which, at that point, they act as a defence against cyber threats. The paper further argues that the detection rates of IT systems that do not use AI cannot be sustained as against those that use some form of AI; the security and protection level would be different, especially given that attackers are also utilising AI methods to attack IT systems.

SMEs are susceptible to high risks with big data. Attacks such as phishing, ransomware, spyware, and adware are some variations of malware related to the loss of big data. (ENISA, 2021)The author believes that phishing attacks are the most common cyber incident experienced by SMEs, and they tend to fall victim to them. It is important that SMEs determine the security tools and use secure protocols that can prevent these types of attacks. (Rawindaran et al., 2022) used a survey questionnaire to observe and analyse the use of machine learning cybersecurity (MLCS) software packages for data protection within SMEs, which showed that SMEs still have some work to do regarding human awareness, technology, and organisation. The use of metaheuristic algorithms can be implemented for detecting and predicting malware in SMEs, which helps to focus on resolving the likely malware, thereby optimising security in SMEs.

The financial constraints associated with SMEs make focusing on cyber security dicey. Most SMEs try to maintain a balance in running their business daily, and now there is a need to add protecting assets with the use of technology like MLCS to the mix. Ensuring that the cost of intelligent software needed for cyber security will be economically affordable would depend on the supply and demand of security software's supply chain.

(Rawindaran et al., 2021) the authors of Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries discuss how the use of AI and ML are being utilised by SMEs in developed countries. The use of MLCS techniques allows organisations to identify the causes of breaches as well as the effects of said breaches and show the impacts on SMEs. The article discusses success stories of the adoption of the use of AI in developed countries and the implementation of MLCS in large organisations to show SMEs how to make use of the templates to protect and secure their data.

Big giant technology companies like Google, Facebook, and Amazon Web Services (AWS) are using ML in their cyber security for better threat detection, malware removal, spam filtering and other identification of other threats such as Denial-of-Service (DoS) and virus delivery. Various techniques and algorithms are being used to get the best solutions to fight cyber threats with cyber security software packages which can be adopted by SMEs. Following the wave of the coronavirus (COVID-19), SMEs have had to change how they operate their businesses by increasing online activities to reach their network and having staff work from home, which requires keeping business data safe and secure. This has contributed to the rise of the use of the Internet of Things (IoTs) by SMEs, which has numerous

advantages for SMEs but also presents challenges related to privacy, security and data breaches, making adopting MLCS methodologies more paramount.

One of the challenges experienced by SMEs is the shortage of cybersecurity resources and knowledge available in the organisational structure. This makes SMEs vulnerable to cyber-attacks. Several suggestions, such as using a comprehensive risk assessment approach, advanced aggregation strategies, and threat-based risk assessment approaches, were given to the categorised SMEs facing the above challenge.

AI is not only used for cyber security by SMEs, (Abrokwah-Larbi & Awuku-Larbi, 2023) discusses another aspect of the use of AI by SMEs in their article The impact of artificial intelligence in marketing on the performance of business organisations: evidence from SMEs in an emerging economy. The use of structural equation modelling- path analysis was used to determine the impact of artificial intelligence in marketing (AIM) on the performance of SMEs, the focus study of this article was based on the SMEs located in the Eastern region of Ghana. The use of the AIM approach significantly impacts the SMEs' financial, customer, internal business process, learning and growth performances. Applying AIM determinants such as IoT, collaborative decision-making systems (CDMS), personalisation and virtual and augmented reality (VAR) proved beneficial based on the recorded significant impact on the SMEs' financial, customer, internal business process, learning and growth performances. The study concluded that SMEs should consider AIM an excellent resource capable of positively impacting their performance and sustainability.

3 Development of IR in Cybersecurity

3.1 IR in Cybersecurity

In a cybersecurity setting, there are two activities to watch out for an event and an incident. An event is considered as any occurrence in a system or network, which could be a normal event, such as a user sending a mail or an adverse event, which is an event with a negative consequence, such as a system crash. A security incident has higher stakes because it is a violation of computer security policies, acceptable use policies or standard security practices (Bartock et al., 2016).

The National Institute of Standards and Technology (NIST) introduced a cybersecurity framework to counteract the evolving cyber threats. This framework was introduced in 2014, and it involves cybersecurity policies for identification, protection, detection, response, and recovery processes related to cybersecurity incidents (Ali & Kostakos, 2023).

Organisations are continuously going to be prone to the risk of having a security incident, and trying to develop a structure for protecting organisations has been set by the framework provided by NIST, ensuring that a common taxonomy and mechanism is available for organisations based on certain standards, guidelines, and practices. This helps in knowing the current cybersecurity posture, the target state for cybersecurity, identifying and creating opportunities for improvement, assessing the progress for the target state and communication across all stakeholders about cybersecurity risks (Cybersecurity, 2018).

The need for incident response in digital domain organisations is a no-brainer because attacks frequently compromise business data, and it is important to be able to respond to attacks quickly and curb the effect of a security breach in an organisation.

The use of IR policies, plans, and procedures ensures uniformity across the board in resolving and responding to security incidents. Most IR plans are tailored to specific organisations' security setups and policies. Having IR plans helps to respond to incidents systematically and reduces the mean time to respond (MTTR), which minimises disruption of services caused by incidents.

Incidents are classified based on their severity and impact, and this helps to prioritise incidents and determine the effects of an incident on the organisation (Mitropoulos et al., 2006).

Table 1: Classification of Incidents

S/N	Severity	Impact
1	High	Severe impact
2	Medium	Significant impact
3	Low	Minimal impact

The higher the severity of an incident, the more impact it has on an organisation's security posture. The severity of each class of incident has a different time to respond attached to it; for example, if a low-severity incident occurs, the mean time to respond to such incidents may be 24 hours, while the mean time to respond to a high-severity incident may be assigned 3 to 4 hours since the impact on the organisation's operations is more severe. It is also possible that the mean time to respond to an incident is classified based on the type of incident, and based on each organisation's incident response plan, the timing may differ.

(Cichonski et al., 2012) Having an IR team, otherwise known as a cybersecurity team, is essential for organisations because it is the team that discovers an incident that might be occurring or has occurred in the organisation. Based on the structure of the organisation, an IR team can either be in house which consists of the employees within the organisation, or the team can be partially outsourced to an MSSP who will then identify suspicious activity and report it to the organisation incident response team and lastly there is the option of fully outsourcing the team whereby an onsite contractor completely handles the incident response work.

3.2 NIST model of IR lifecycle

The figure below illustrates the incident response life cycle according to the NIST framework; in this model, the life cycle has been categorised into four by combining the containment, eradication and recovery stages together as one.

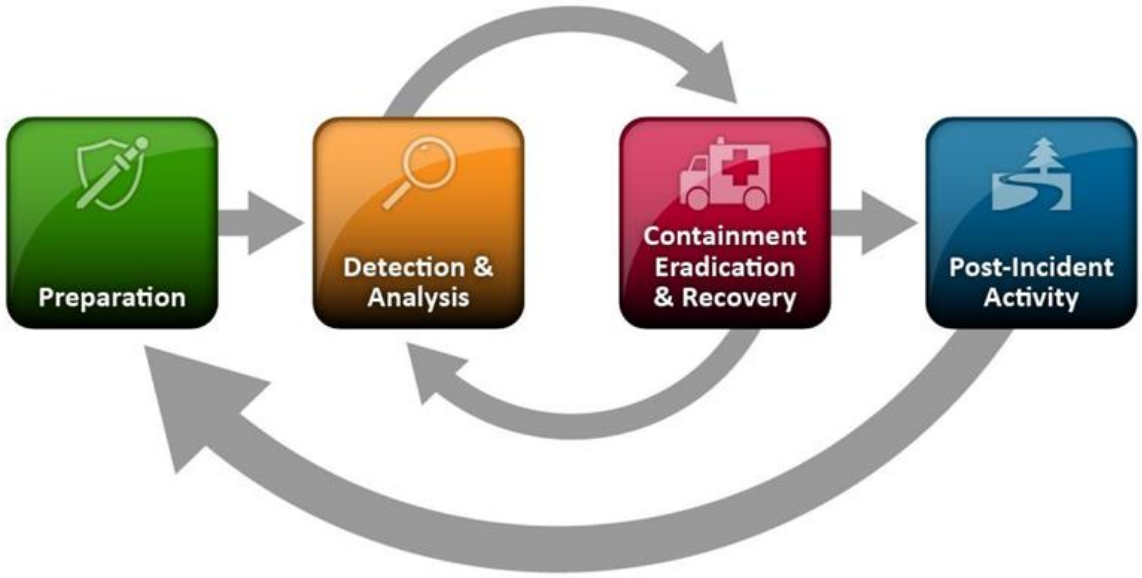

Figure 4: IR lifecycle (Cichonski et al., 2012)

The first stage of the IR lifecycle is the preparation stage. This is a very crucial stage because it is where the incident response capability of an organisation is established, the preparation stage is where an assessment of the organisation's assets is investigated, and incidents are prevented by ensuring that the systems and networks of the organisations are properly secured (Cichonski et al., 2012).

The second stage is referred to as the detection and analysis stage; accurately detecting that an incident is occurring or has occurred can be somewhat challenging because of various factors, such as incidents can be detected through several means with different levels of accuracy, automated detection means which can yield false positives and manual detection means, also there is a need for experts with deep technical knowledge to analyse incident-related data properly. The signs of an incident can be categorised into two: a precursor, which is a sign that an incident will occur in the future, and an indicator, which is a sign that an incident is ongoing or has occurred (Cichonski et al., 2012).

The third stage of the IR lifecycle is the combination of containment, eradication, and recovery. Containment is the process of separating an incident before resources get overwhelmed and damage is increased; this is a very important stage which requires decision-making of acceptable risks an organisation can handle. There are different containment strategies for varying incidents (Cichonski et al., 2012).

Eradication is the next step after containment; this is where components of an incident need to be eliminated; identifying all affected hosts by an incident for remediation is a part of the eradication strategy. Recovery is when all affected hosts return to normal operation by ensuring that remediations have taken place and systems function as they were designed to function. The time for recovery can either be short or long depending on the scale of the incident that occurred and the preparedness of the organisation for the incident that occurred (Cichonski et al., 2012).

The final stage of the IR lifecycle is referred to as the post-incident activity; this can also be referred to as the lessons learned stage; this can be considered as the most important stage because it involves learning and improving. This is the stage where all stakeholders meet to get closure concerning an incident by reviewing the incident when it occurred, why it occurred, the intervention methods that were taken, how the intervention methods work and steps to take to prevent similar incidents from occurring again in the future (Cichonski et al., 2012).

3.3 Automated IR tools

Automating the IR process with AI makes it easier to resolve more incidents at a greater speed, which results in less time, and of course, with automation, less effort is required from IR team members. Achieving proactive defence by automating the detection of threats and learning from real-time data is done with the use of AI (Kumar et al., 2023). The cybersecurity industry is adapting AI-based IR automation because of reasons such as remote work systems, cost-effectiveness and the reactive nature of cybersecurity(SISA, 2022).

Automated IR tools are defined as software solutions that leverage various technologies like artificial intelligence, machine learning and automation to help organisations improve the efficiency of IR processes. Some of the automated IR tools currently in use are stated below (OpenAI, 2023).

- Security Information and Event Management System (SIEM)
- Endpoint Detection and Response Solution (EDR)
- Security Orchestration, Automation and Response Platforms (SOAR)
- Threat Intelligence Platforms (TIP)
- Security Automation and Orchestration Tools (SAO)
- Incident Response Automation Platforms (IRAPs)

3.4 Integration of AI in IR Process

In the case of an incident, where effective and efficient actions must be taken, the methodologies required to resolve incidents include several distinct parts based on the phases provided by NIST(Mitropoulos et al., 2006). Table 2 below shows how AI concepts and products can be integrated into each incident response process.

Table 2: Examples of AI Integration in IR processes

IR Processes	AI Integration	Explanation
Preparation	Security Awareness training Decision support system Security automation attacks and insider threats (Kumar et al., 2023).	The provision of cyber security awareness training for organisations' employees strengthens the security posture of the organisation by ensuring that employees are trained in line with related cyber security policies, procedures, and agreements(Cybersecurity, 2018). This is done to reduce the notion that humans are the weakest link in security. The implementation of a decision support system which is an application of expert systems in an organisation is that it can be used to guide security teams on how to respond to a security incident and provide recommendations on actions to take based on the type of incident (Agrawal et al., 2023). (Shanthi et al., 2023) discusses how the use of AI-based systems using natural language processing techniques can be utilised for automating security tasks such as deploying security patches and the creation and generation of security policies and security reports.
Detection & Analysis	Firewalls, IDS, User Event Behavioural Analytics (UEBA), AI-based SIEM	Sources such as Firewalls and IDS are used to perform log analysis where information about an incident can be found and initially detected and further analysed (Mitropoulos et al., 2006).

IR Processes	AI Integration	Explanation
		UEBA is a combination of AI and ML that provides a proactive and predictive approach to vulnerability management. It can detect anomalies in an organisation's baseline activity, such as zero-day
Containment	AI-powered end-point security solutions (EDR, XDR)	The use of AI-powered endpoint security can be used to isolate infected devices from the centralised network to prevent the spread of attack (Rizvi, 2023b). This is common with malware-related attacks. Advanced security techniques, such as honeypots, can be used to contain network incidents(Mitropoulos et al., 2006).
Eradication	Intrusion Prevention System (IPS), AI-based SIEM	AI-based SIEM can trigger alerts automatically and implement predefined actions. IPS is a system that can not only detect possible incidents but also stop the incidents from being successful.
Recovery	Vulnerability assessments, penetration tests	Performing vulnerability or penetration tests on the affected systems ensures that possible existing vulnerabilities are disclosed and resolved before systems are reintroduced to the production environment.
Post-incident Activity	Lesson learned meetings.	This is the final stage of the IR process, where all stakeholders are to meet to discuss the incident and the lessons learned from it. Proper documentation of the incident's life cycle must be provided at this stage.

The table above is not an exhaustive list of AI integration in incident response processes.

The use of AI-powered tools helps security teams to detect and respond to threats quickly by analysing large amounts of data automatically, thereby reducing the risk of a successful attack (Kumar et al., 2023), these AI-powered tools can be used to analyse security incidents and determine the appropriate response to the incidents by providing remediation action (Kaloudi & Li, 2020) which is a game changer for incident response in cyber security.

(Harel et al., 2017) argues that automation of threat detection and response is the major advantage of AI in cybersecurity. Threat detection and response are major aspects of incident response. The creation of automated incident response systems is another luxury of AI in cybersecurity because the automated incident response systems can analyse data to identify possible risks and then take actions to mitigate possible attacks, all the while minimising disruption to the regular operation of organisations (Rizvi, 2023b).

It is crucial to ensure AI tools can be integrated with existing systems seamlessly. This is important for automating the incident management process and can be achieved by proper needs assessment and gap analysis, followed by tool selection and configuration (Marc Hornbeek, 2023). Organisations' needs differ based on their structure and nature.

4 AI Use Cases in IR

4.1 Role of AI in IR

The role of Artificial Intelligence in Incidence response can be grouped into two categories which are early detection and rapid response (Hassan & Ibrahim, 2023).

Early detection: Being able to detect threats and anomalies early in a network is crucial to the incident response process. AI can be used for early detection in some of the following ways such as threat detection and response, intrusion detection and prevention, vulnerability management, behavioural analysis, fraud detection, threat hunting (Shanthi et al., 2023).

- Threat detection and response: The use of AI-based systems to detect threats and respond to threats in real-time is essential for the first four stages of incident response processes. AI-based systems use techniques such as machine learning to analyse network traffic to discover potential threats that can lead to possible attacks (Shanthi et al., 2023).
- Intrusion detection and prevention: AI-based systems with machine learning techniques can be used to learn the baseline of organisations for the normal behaviour of the networks and systems used in the organisations; this is to be done to be able to identify any deviation from the baseline which can constitute as an intrusion, thereby helping security team detect the intrusion and take actions to prevent it (Shanthi et al., 2023).
- Fraud detection: Fraudulent activities can be detected easily with the use of AI-based systems with the ability to analyse large amounts of data to identify unusual patterns and actions that could indicate fraudulent behaviour (Agrawal et al., 2023).
- Vulnerability Management: The use of machine learning algorithms in AI-based systems can be used to identify vulnerabilities in networks and systems; this is an important preparation stage of incident response whereby vulnerabilities in the network and systems are identified early and remediated to prevent exploitation by threat actors and also in the recovery stage of incident response to ensure that no back door threat remains on previously infected systems and networks (Agrawal et al., 2023).
- Behavioural analysis: This is like fraud detection. AI techniques can analyse employee behaviour and biometric data to detect suspicious patterns that do not tally with the usual employee behaviour. This can be used to detect anomalies like unauthorised users trying to access data and prevent data loss.
- Threat Hunting: Organizations can use AI-based systems with machine learning and natural language processing techniques to proactively search for threats in networks and systems that traditional security measures may not detect.

Rapid response: Several articles agree that the use of AI in incident response reduces the mean time to respond (MTTR) to cyber incidents, (Rizvi, 2023b) states that AI-powered endpoint security solutions help organisations respond quickly to threats by automatically isolating infected devices from the network. (Bhatele et al., 2019) believes that AI-based incident response systems can automate the response to cyber threats and attacks, which in turn reduces the time required to respond to attacks.(Agrawal et al., 2023) agrees that using AI systems that can analyse a massive amount of data in real-time lets security teams discover and respond to attacks faster and more effectively. (Marc Hornbeek, 2023) says that using the right approach and tool in AI-based incident management can drastically reduce operations downtime, speed up resolution times, and improve system reliability. Using AI to automate IR helps minimise the effect of an attack and shorten the response time required for IR.

4.2 AI abilities in improving IR.

AI is a valuable technology used in cyber defence and general information security because of its numerous abilities based on the different AI technologies available.
The following AI abilities are unique to incident response in a cybersecurity environment (Kant & Johannsen, 2022).

- Evaluation of large data: The ability to efficiently evaluate large volumes of data (in a cyber security company, log files are always gotten from various security sources used by the organisation; the ability to evaluate log files that tend to be large in volume is an improvement to IR).

- Anomaly detection: AI can detect anomalies in a security network. For example, if there are multiple login attempts per second, it can indicate a possible cyber-attack, which is detected by using a SIEM.

- Pattern analysis, prediction and forecast: AI can be used for pattern prediction and forecast based on the baseline of an organisation and how the systems function; AI can study patterns and make predictions and forecasts before an event happens.

- Clustering and categorisation: Clustering and categorisation are also important AI abilities that help detect malware, phishing, or spam emails. Phishing is one of the most common cyber-attacks organisations experience, and using AI to detect cyber-attacks like that helps reduce the number of successful attacks organisations experience.

(Kant & Johannsen, 2022) study focused on evaluating seven use cases of AI abilities for SMEs in the cyber security domain. The seven use cases are malware detection, anti-exploit technology, intrusion detection, endpoint protection and response, user behavioural analysis, scoring risk in a network and security information and event management.
This study, however, will focus on the use cases of AI abilities in SIEM tools and malware detection in SMEs because these two use cases fall under the category of low adaptation complexity and high benefits for SMEs.

4.2.1 SIEM tool use case of AI abilities

SIEM is a tool with high AI-based added value; it can interface with several security features and acts as a centralised point for all security-related information by collecting, integrating and analysing security data from multiple security sources such as network and endpoint security tools; this is particularly useful for SMEs with fewer resources, it is used to detect possible security incidents before they can cause damage to the organisation (Kant & Johannsen, 2022)(Ban et al., 2023). SIEM solutions help to increase the security posture of an organisation's network(Swift, 2006). SIEM solutions have four major functions, which are log consolidation, threat correlation, reporting and incident management, which cover four of the incident response processes from identification to containment to eradication and recovery process(Swift, 2006).
(Ban et al., 2023) a SIEM framework combining AI and data visualisation techniques was proposed to simplify the incident handling process. The framework consists of four modules. The alert generation module, which is the starting point of the framework, is used to collect alerts from various IDS sources, which could be either a Network intrusion detection system (NIDS) or a Host intrusion detection system (HIDS); this enables identification and detection of anomalies in the network. The second module is referred to as the feature processing module, which is used to standardise different log formats and encode data as numerical vectors for uniform representation. The third module is the machine learning module, which uses one of its techniques, supervised learning algorithms, on labelled data to create a prediction model that detects critical alerts. The last investigation module is used to evaluate the prediction model's performance, and data visualisation and alert grouping are used to ensure rapid incident investigation.

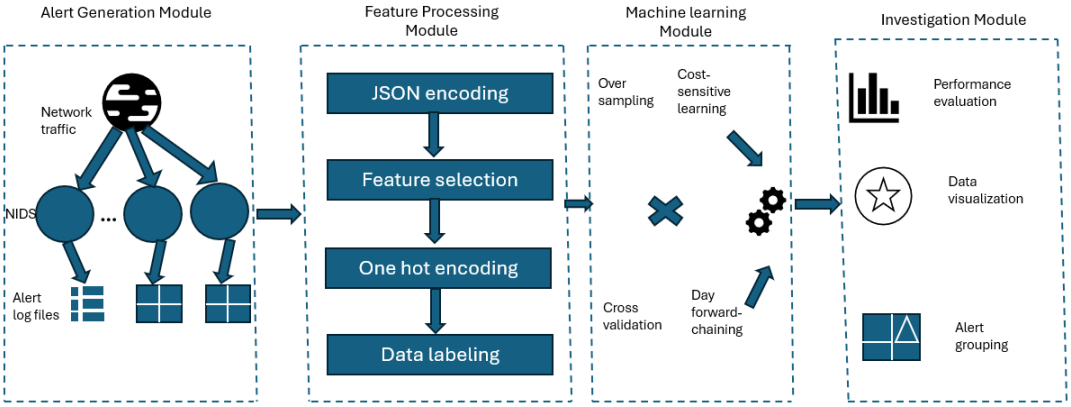

Figure 5: SIEM framework.

Below are two SIEM tools currently integrated with artificial intelligence to enhance cybersecurity industries' incident response life cycle.

Exabeam SIEM tool

Exabeam SIEM tool is an example of how artificial intelligence is used to improve cybersecurity for security teams. The SIEM is designed as a centralised threat management with pre-built investigative tools and automation, which makes the work of security teams easy while increasing productivity. (Exabeam, 2024)The threat centre consists of three modules of threat detection, investigation, and response capabilities, which reduce alert fatigue for security analysts. One of the numerous features of the SIEM is the use of ATT&CK framework TTPs or use cases to filter common threats. Figure 7 represents the working principle of the Exabeam SIEM tool.

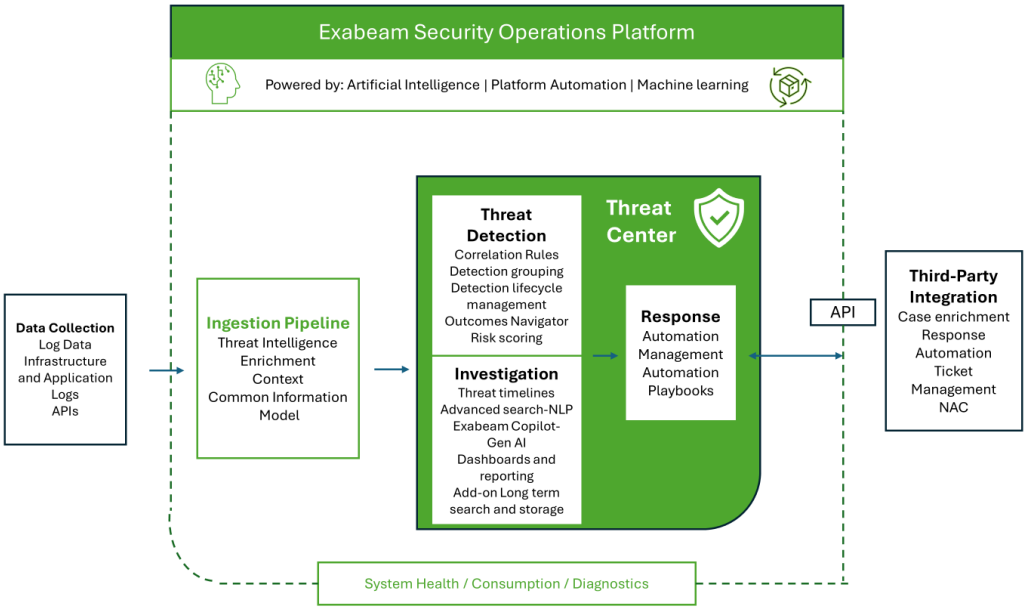

Figure 6: Working principle of Exabeam SIEM tool (Exabeam, 2024).

IBM Qradar SIEM Tool

IBM Qradar SIEM tool uses several layers of AI to improve the quality of threat detection and investigation it carries out; this leads to better alerts generated and increases the efficiency of security analysts. It accelerates threat detection, expands visibility, and uses AI to make more informed decisions by providing recommendations for detected threats. (IBM, 2024). A data exfiltration example is shown in Figure 7 below; the Qradar SIEM is able to search for 132 thousand logs in 42 milliseconds after the SIEM generates a suspicious activity alert. It was from the searched logs that it was seen that the source IP “10.10.10.10” was involved in a content protection violation, which points to data exfiltration. This also showed where the data was attempted to be transferred to, which enabled security analysts to take recommended actions such as removing the system from the network and revoking the user's access. The entire process of detecting and performing investigations where the user was identified, the threat was contained, and the recovery process was instigated at a quick speed. It was performed efficiently with the use of an AI-based SIEM tool.

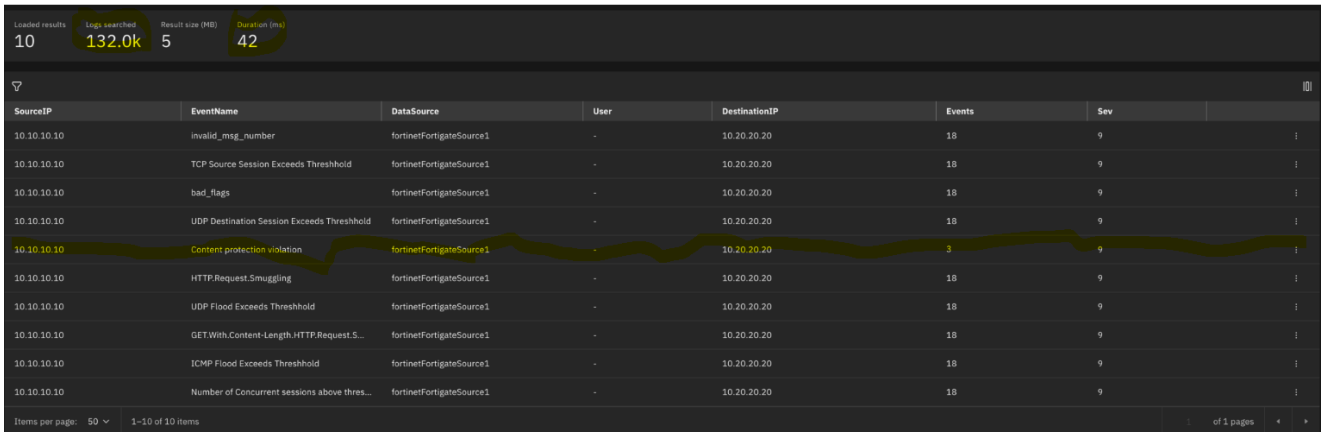

Figure 7: Log analysis of Qradar SIEM tool.

The AI-based SIEM tool went a step further; after detecting and containing the incident, the SIEM tool provided recommendations to the security analysts on the best way to eradicate and recover from the incident; this is advantageous because in cases where a Tier 2 analyst is not available to give instructions and recommend actions to take in the case of such incident, the AI-based SIEM can guide the security analyst on duty, this is not a feature available with traditional SIEMs.

The use of traditional SIEM tools is limited compared to AI-based SIEM tools.

Table 3: Difference between Traditional SIEM and AI-based SIEM (Exabeam, 2024)

S/N	Traditional SIEM	AI-based SIEM
1	It can consolidate, correlate, and analyse data from various sources.	It makes use of AI abilities such as ML algorithms to solve challenges of the past.
2	It relies majorly on signatures from log sources.	It uses ML and predictive analysis to perform proactive threat detection and response.
3	-	It is characterised by data aggregation, normalisation, and enrichment.
4	The timeline from threat detection to response is relatively longer than that of AI-based SIEMs.	The use of AI techniques leads to rapid threat response time.

4.2.2 Malware Detection use case of AI abilities.

Malware is a term used to describe software designed specifically for a nefarious purpose. According to a Google search, phishing is the most common cyber security threat in 2024, followed by ransomware attacks. Phishing is a variant of ransomware and a common delivery method for ransomware. Ransomware is a type of malware that encrypts data, making the data unavailable to users. This causes disruption in organisations' day-to-day activities.

The use of AI and ML-driven intrusion detection protection systems has risen in the SME market because of the increasing number of malwares created daily by threat actors; these malwares are used to infiltrate networks and systems to cause disruptions. (Rawindaran et al., 2022). AI applications used in intrusion detection systems have been successful in network filtering, protection against phishing and botnet control. (Fritsch et al., 2022).

As artificial intelligence continues to develop, researchers are starting to focus on using machine learning and deep learning methods to combat the effects of malware by improving malware file detection and classifications. (Gibert et al., 2020).

(Marais et al., 2022) focused on using machine learning and deep learning models to detect and classify malware and ransomware. The methodology focused on three segments: datasets, features, and models. Three different datasets were used: the PE machine learning dataset, the Bodmas dataset and the Ember dataset; the datasets collected contained both malicious files and benign files. The next step involved training the models for detecting malware, which means extracting features, also known as information, from the PE files, which was carried out with two pre-processing algorithms, the ember method and the grayscale method. After the feature extraction, four ML and DL models, which are Light GBM, XG Boost, Dense neural network (DNN) and Convolution neural network (CNN), were used to test the subsets and the result was categorised on accuracy and F1 scores of each model. The author concluded that the CNN model did not perform as well as the other models for malware detection.

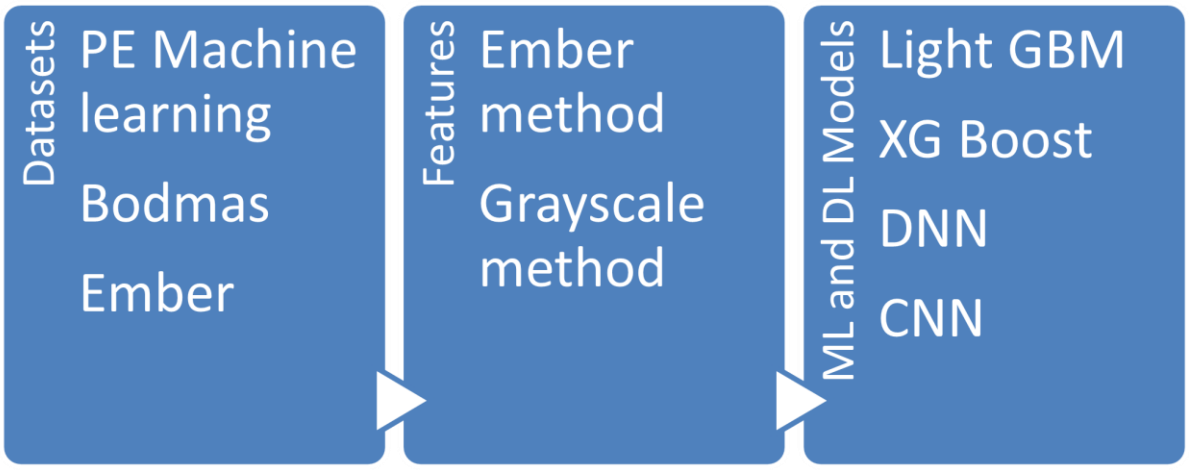

Figure 8: Machine learning model for malware detection.

4.3 Comparison of IR playbook integrated with AI and without AI

(Shaked et al., 2022) describes a playbook as an aggregation of workflows. It combines different elements of IR to address an incident in a hierarchical structure. It includes step-by-step actions to take

in the case of an incident following the IR process and security structure of organisations. An IR playbook is a process model that describes response processes and related information for responding to an incident.

Cyber incidents are synonymous with emergencies, and if not responded to or controlled timely, they can lead to severe consequences for organisations, such as reputational damages, financial loss, service disruptions, loss of data, etc. Cases, whereby cyber incidents are not responded to promptly, are likely due to a lack of a standard IR playbook containing operative procedures and actions to take for related incidents. (Onwubiko & Ouazzane, 2022).

Some SOCs have playbooks, but those playbooks are sometimes not updated or inadequate; in the cases where some stakeholders have left their positions or the organisations and an incident occurs, those making use of the playbooks will not know who to escalate incidents in that case to and this prolongs the timeline of the incident which can lead to substantial damages to the organisation. (Bartock et al., 2016), if an organisation's playbook is integrated with AI, playbooks can be suggested and developed as quickly and as often as needed to resolve incidents, eliminating the presence of inadequate playbooks. Having standardised playbooks to manage and resolve cyber incidents appropriately is essential for organisations. (Onwubiko & Ouazzane, 2022).

There are different frameworks used to develop playbooks, (Kick, 2014) MITRE developed a cyber playbook in 2014, which can be used as a guide in creating playbooks suited to the structure of different organisations. The playbook focuses on cyber-attack kill chains, adversarial tactics, techniques, and procedures (TTP), and threat intelligence sharing information methods.

Phishing is a cyber threat that is a delivery method for ransomware. It is designed to contain harmful links or malicious files sent as an email to users and present itself as legitimate, but it is not. Phishing is the first cyber security threat in the top 10 cyber security threats in 2024, as recorded by(SYTECH, 2024)Therefore, this research will use a sample playbook for a phishing incident scenario. The researcher designed the phishing playbook based on her experience in the industry.

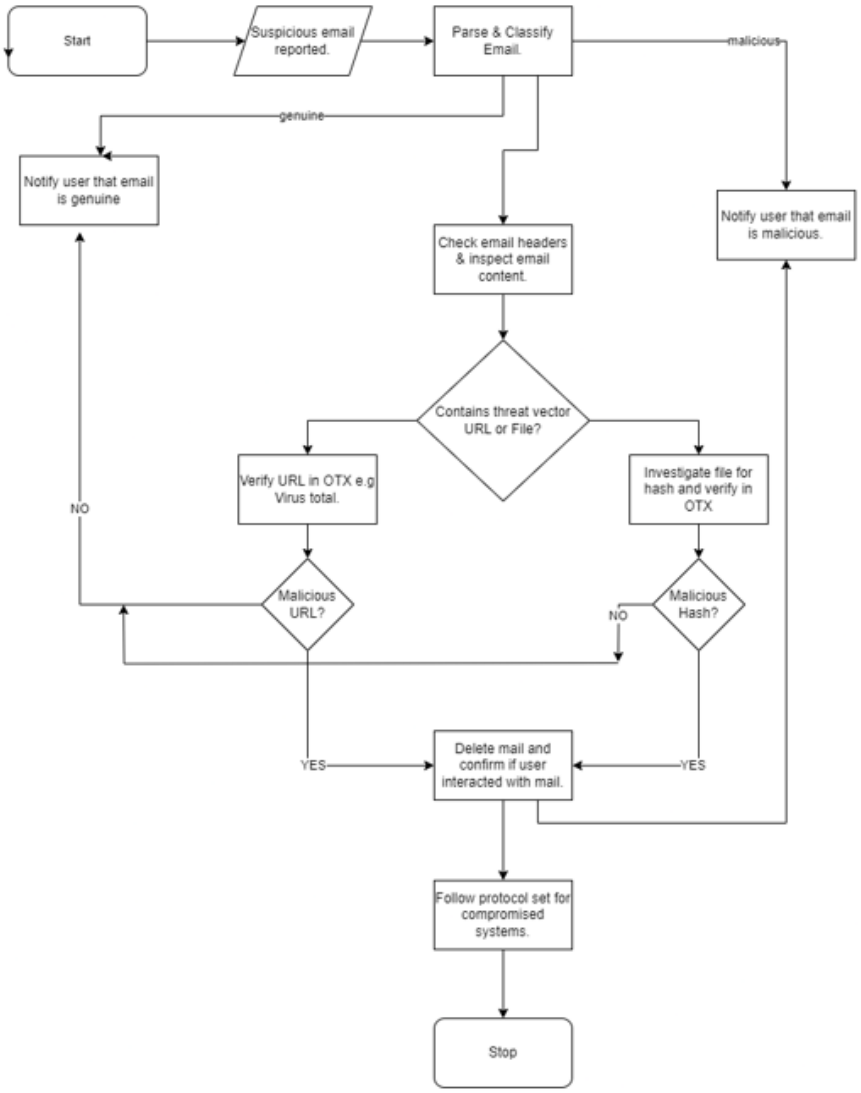

Figure 9: Phishing playbook.

Figure 9 represents a detailed phishing playbook for analysts to follow in the case of a phishing threat. However, following all these steps can be time-consuming. Having AI integrated into the security technology tools used in an organisation can automate most of the steps in the playbook, thereby reducing the time and effort analysts invest in resolving a phishing threat.

5 Research Methodology

Research Methodology is referred to as the procedures and processes a researcher takes in describing and explaining the phenomena of their work.(Rajasekar & Verma, 2013). It is a systematic way of solving research problems. (Balwan et al., 2022) states that research methodology is the analysis of research methods applied to a field of study involving various techniques and tools used to conduct the scientific research study. This chapter describes the methods used to collect and analyse data and how the research process has been completed. The data selection of data collection methods for this research depends on the scope, aim, and objectives of this research, which are introduced in Chapter 1 of this research.

5.1 Research Design

A research design aims to create an appropriate framework for a study. The process of research design involves many connected decisions. (Sileyew, 2019). (Almalki, 2016) refers to five important questions that must be addressed at the beginning of any research: the what, why, who, where, and when questions of the research.

The “what” question addresses the specific topic of the research being undertaken. Answering the “what” question for this research is simply finding the role and importance of artificial intelligence in incident response for digital domain SMEs.

The “why” question describes the reason for undertaking the research. In response to that, this research is being done as a requirement for a master’s study and because it is a topic of interest to the researcher.

The “who” question requires the researcher to identify those who will likely participate in their study; for this research, the targeted people to generate the information required to answer the research questions are cyber security employees of both digital domain SMEs and large organisations.

The “where” question addresses the location of where the research is being carried out. Since this research uses a survey as its data collection method, there was no need to find a suitable venue for participants; however, most of the participants were located around Europe and Nigeria.

The “when” question covers the time scale used to conduct the research. The survey for this research was a time-based frame, and given the timeline of four weeks, this was to give a condensed window for all participants to fill out the survey questionnaire and receive quick and effective results for the study.

5.1.1 Types of Research

There are various types of research, and each type has its own purpose and importance. (Dr. Swarooprani. K, 2022). There are two main classes of research. (Rajasekar & Verma, 2013) which are fundamental or basic research and applied research.

- Basic or Fundamental Research: Studies of natural phenomena or investigations related to pure sciences are classified as basic research. It is usually based on basic principles and discovering the reasons for the occurrence of certain events or processes. Basic or fundamental research can also be referred to as theoretical research(Rajasekar & Verma, 2013)Basic research's purpose is to override indefinite facts, improve information, and formulate new speculations. It is usually based on generalisation. (Dr. Swarooprani. K, 2022). The result of basic research forms the foundation for much-applied research.
- Applied Research: (Rajasekar & Verma, 2013)Applied research is the type of research that aims to solve distinct problems using well-known and accepted theories and principles. It defers from basic research in that it studies specific cases without generalising, and its purpose is to discover solutions to practical problems that require immediate use. Applied research aims to solve problems currently faced by the community, society, business, or institutions. (Dr. Swarooprani. K, 2022).

Literature has introduced several other types of research, such as empirical, conceptual, descriptive, analytical, qualitative, and quantitative. (Balwan et al., 2022). This research is classified as applied research because it focuses on the specific case of the role of artificial intelligence in incident response for digital domain SMEs.

5.1.2 Research Philosophies

Research philosophy can be defined as the truth, reality, and knowledge that a researcher believes in. It describes the principles and ideals that guide the research design, data analysis, and data collection used in a research study. (Ryan, 2018). Several philosophical approaches have been introduced by literature, and these will be discussed in this chapter.

Epistemological and Ontological considerations are two research philosophies with several approaches linked to them. When considering epistemological concerns, which seek to discover what acceptable knowledge should be regarded as in a discipline, various positions exist, such as positivism, realism, and interpretivism. (Bryman, 2016).

Interpretivism focuses on the importance of understanding a participant's interpretation of the world; it involves understanding the subjective meaning of social action. Interpretivism is an epistemology that is referred to as the opposite of positivism.(Bryman, 2016), it is not considered for this research because it uses qualitative methods. According to (Bryman, 2016), realism is known to share some similarities with positivism since it believes that both natural and social sciences should use the same approach for data collection and explanation.

Finally, positivist philosophy uses structured methodologies, such as quantitative methods (Veiga, 2016) (Ryan, 2018). In the event of a cyber security incident, collecting and analysing the incident-related data often involves quantitative research methods such as surveys, experiments, and statistical analysis. The

goal of positivism is to gather reliable, consistent, and replicable research results to represent reality. In this research, the epistemological assumptions lean towards **positivism** because it emphasises empirical and verifiable data (Ryan, 2018). This is done with the use of survey questions tailored to fit the research questions of understanding the role of artificial intelligence in incident response for digital domain SMEs, which were sent to cybersecurity professionals with acceptable knowledge to help attain the aim and objective of this research study.

Ontological concerns, however, are based on the nature of social entities; there are two approaches to ontological considerations: objectivism and constructionism. (Bryman, 2016)In this research, the ontological assumptions refer to assumptions about the function of artificial intelligence in incident response. The ontological assumption considered here is objectivism, which is in reference to the objectives of this research in chapter 1.3, which is to measure the current maturity level of SMEs in relation to their use of AI in their IR processes, which is a fixed knowledge.

5.1.3 Research Approaches and Methods

According to Melnikova's research onion model, two research approaches, the deductive approach and the inductive approach, should be considered for research purposes.
The inductive approach involves generating a theory with little research on the topic. (Bryman, 2016) (Melnikovas, 2018). Inductive approaches are associated with focus groups or interviews, making them unsuitable for this research. The second approach, the deductive approach, involves testing an existing theory. (Bryman, 2016), with the use of questions and data collection to agree or disagree with a hypothesis (Melnikovas, 2018). Deductive approach is usually associated with a survey. (Veiga, 2016). In reference to this research study, taking note of the cybersecurity culture of an organisation can be used to test certain security-related hypotheses. It can be deduced that organisations that provide their employees with regular cyber security awareness training will have a stronger security posture when compared to organisations that provide little to no cyber security awareness training for their employees. A **deductive approach** was used for this research since it is survey-based.

Regarding research methods, several kinds of literature have settled on three distinct methods for connecting research, which is qualitative, quantitative, and mixed methods (Almalki, 2016) (Shameli-Sendi et al., 2016). Qualitative research is exploratory research that is descriptive and uses words; the goal is to get the meaning and describe a situation; it is a type of research concerned with quality(Rajasekar & Verma, 2013). One of the characteristics of qualitative research is that it draws meaning from the experiences and perspectives of participants, and it is usually characterised as inductive (Almalki, 2016). The second method, **Quantitative method,** is the method that was utilised in this research. (Veiga, 2016) is of the stand that quantitative research method is a method that has been

used successfully in the discipline of information security, which makes it perfect for this research since it is based on the specific area of the function of artificial intelligence among digital domain SMEs in regards to incident response management processes, using quantitative method is beneficial to this research since it ensures that the area of concern can be determined. The results of quantitative methods are often presented in tables and graphs (Rajasekar & Verma, 2013), which can be seen in Chapter 6 under result analysis.

The last method, mixed-method research, is empirical research that involves collecting and analysing both qualitative and quantitative data. (Almalki, 2016), it provides flexibility for the researcher to change quantitative inputs to qualitative outputs and vice versa as the need arises(Shameli-Sendi et al., 2016).

5.1.4 Research Process

The research process follows a sequential component: selection of a research topic, formulation of the research problem, extensive literature survey, development of a working hypothesis, preparation of the research design, analysis of data, and interpretation of data. (Balwan et al., 2022)(Rajasekar & Verma, 2013).

The selection of a research topic was made based on the researcher's industry experience as an incident response analyst, in conjunction with the rise of the concept and use of artificial intelligence in the cyber security space, as well as extensive discussion with research supervisors. The research problem was then defined as seen in Chapter 1.2; extensive literature study and referencing report connected to the research problem were covered in Chapters 2, 3 and 4. The next process followed in this research was the development of a working hypothesis that the use of artificial intelligence in incident response is beneficial to the security posture of digital domain SMEs. The research design discussing the research philosophies, research methods and research approach used in this research can be found in Chapter 5 of this report. Finally, the last two steps of data analysis and interpretation of results will be discussed in the latter part of this report.

5.2 Data Collection

This research utilised primary and secondary data collection methods (Dr. Swarooprani. K, 2022) following a systematic and structured method to answer the research questions. The secondary data collection method the researcher uses involves published data in books, academic journals, industry-related websites, scientific journals, and the Internet. The primary data collection method based on the direction of the research was collected quantitatively using survey questionnaires. The survey questionnaire was designed in a way that can achieve the aims and objectives of the research. The use of a survey in this research helped to observe how artificial intelligence is being used in IR by digital domain SMEs, the limitations faced by SMEs in relation to the role of AI in IR and how improvements can be made.

Surveys are particularly appealing because of the low-cost budget associated with it and the possibility of a large user sample being able to participate with little resource requirements. They are used traditionally to evaluate behavioural content related to the attitudes and opinions of participants; this is done by systematically collecting data from a sample population for a certain objective. (Veiga, 2016). For this research, the security posture of digital domain organisations in relation to artificial intelligence and incident response practices was assessed by the attitudes and opinions of cyber security users regarding the use of security controls, emerging technology and cyber security culture and practices used in their respective organisations. Through the analysis of the cybersecurity employee's perceptions of the cyber security posture of their organisations, various factors can be deduced for the level of security maturity of SMEs and aspects are identified for improvement and recommendations to improve the security posture to a stronger level, thereby fulfilling the goal of information security.

A cross-sectional time horizon approach was used in this research because it consumes fewer resources and time; a time frame of four weeks was given to the participant for the completion of the survey, which is a characteristic of cross-sectional time horizon that is commonly referred to as short term study that involves data collection at a specific point in time. (Melnikovas, 2018).

The survey was sent to over 100 members of cybersecurity industry professionals via email and the social media professional site LinkedIn. 53 participants completed the survey, while others could not fill the survey due to personal reasons, vacation and leave periods, outdated email addresses and rejection by the recipient's email systems. The merits of using the survey method in this research involved low cost of delivery and return, wide potential coverage, which can be seen in the variety of countries the survey participants were in and ease of completion; the survey was estimated to be completed within 10 to 15 minutes and was designed to be completed easily on either desktops or mobile devices. The disadvantage associated with this method involves the response rate, as reflected in the report that only 53 participants were able to complete the survey.(Rajasekar & Verma, 2013).

Taking note of ethical considerations and as a requirement of GDPR, participation was voluntary, and all responses were kept anonymous. The survey questionnaire is referenced under Appendix A in the appendix section at the end of this report.

5.2.1 Sample Population and Selection Approach

As described by (Rahman et al., 2022) , the process of choosing a sample from a population is known as sampling.

As stated above, over 100 participants were requested to fill out the survey questionnaire, of which 53 participants were able to fill out the survey; this number of participants forms the sample population for the survey questionnaire for this research. This sample size was considered sufficient for achieving the research objectives.

This study uses a purposive sampling approach to select the participants for this study. It is a non-probability sampling approach in which the researcher selects participants consciously based on their knowledge and understanding of the research questions. All participants in this research study are cybersecurity professionals with many years of work experience in the industry. Selecting purposive sampling for this study was ideal since it requires specialised participants with an understanding of cybersecurity concepts such as artificial intelligence and incident response to get insights into participants' perspectives on the research topic and gather sufficient data on the security maturity level of the participants' organisations. One of the advantages of this sampling method is the soft and easy way of attaining a diverse range of responses.

5.2.2 Survey Questionnaire Design

The survey questionnaire was designed using Google Forms, and 32 investigative questions were set based on the research objectives, with a combination of 25 multi-choice questions, 4 rating scale questions and 3 text-based questions. The questions were categorised into 6 sections:

1. General information
2. Cybersecurity Awareness
3. Incident response management
4. Security controls and technology
5. Current usage of AI
6. Experience.

The survey started by getting general information containing details of the participant's organisation and participant experiences, such as the size of the organisation, the industry sector of the organisation, the geographical location of the organisation and the years of experience of the participants. The next question focused on the level of cybersecurity preparedness of the participant's organisations, which was measured by checking the frequency of cybersecurity awareness programs conducted in each organisation and the presence or absence of cybersecurity teams in the organisations. This then led to questions about security incidents experienced and the availability of equipment to combat the incidents. The survey touched upon the specific security controls and technologies put in place by the organisations, plus the opportunities for improvement. The next question was to measure the current usage of artificial intelligence in the organisation and the participants' perspective about the advantages and limitations that their organisations may experience. The survey ended by asking about the participants' experiences with the AI-driven incident response solution.

5.2.3 Demographic factors considered for research.

According to (Veiga, 2016) different comparisons can be made with data based on regions, departments, age, and other biographical traits. This research gathered the following demographic factors of the participants that responded to the survey questionnaire: size of organisations, industry sector, location of organisations and year of work experience of the participants; these factors were obtained from the general information section of the survey. These clusters will be used for data analysis to measure the organisations' cyber security culture and security posture; this enables the questionnaire to be validated and tested for reliability.

Below is a brief discussion of the demographic statistics of the participants.

Size of organisations

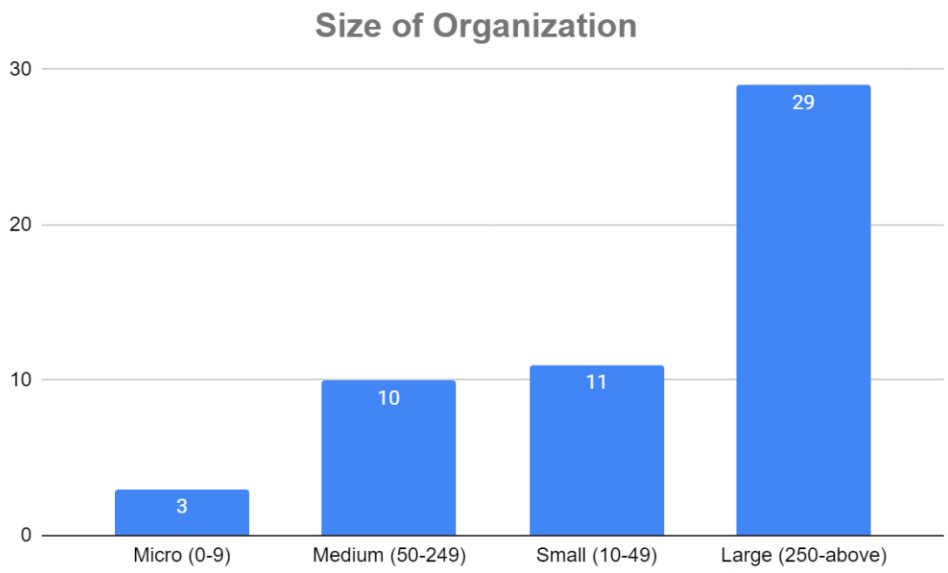

Figure 10: Size of Organizations

The above figure represents the size of the organisation in which each participant of this study works; it shows a total number of 29 participants, which is a significant number of participants who work in large organisations that have 250 and above employees in their organisation. 24 participants fall under the SME categories, with 3 participants from micro-organizations, 11 participants from small organisations and 10 participants from medium organisations.

Industry Sector

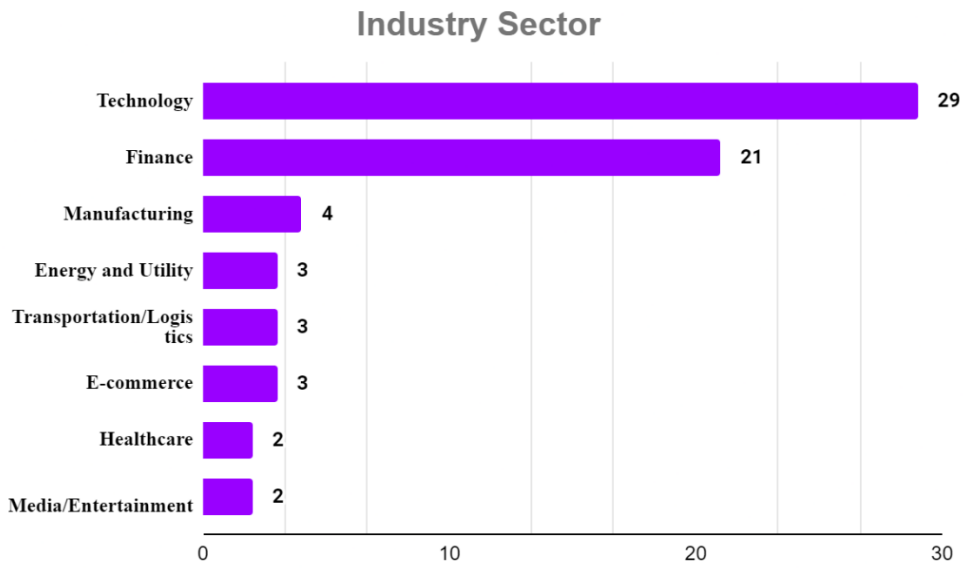

Figure 11: Industry sector of participants.

Figure 11 shows the different industries that participants of this study work with. The industry sectors are 8 different digital domain-related sectors ranging from technology, finance, manufacturing, energy and utility, transportation and logistics, e-commerce, healthcare and media/entertainment. All 8 industry sectors utilise information security in their day-to-day operations. The technology category has the highest data, with 29 participants working in that sector. This is followed by the finance category with 21 participants, and the remaining 6 categories, manufacturing, energy and utility, transportation/logistics, e-commerce, healthcare and media/entertainment, all have participants ranging from 2 to 4 participants scattered across the sectors.

Location of organisations

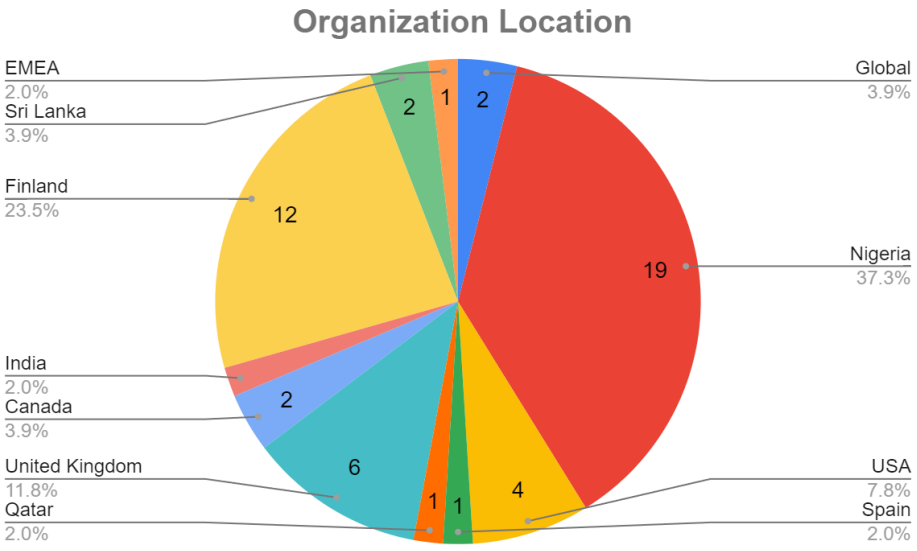

Figure 12: Organization location.

The diagram above represents the geographic location of the organisations of each participant; the study shows a notable representation of 10 distinct geographic locations and a generalised geographical location represented as global. 19 participants work in organisations located in Nigeria, which was the highest geographical representation; this was followed by 12 participants in Finland, giving a good representation of a Nordic area, the United Kingdom contributed 6 participants, and the United States of America had 4 participants. The inclusion of Sri Lanka with 2 participants, Canada with 2 participants, Spain, Qatar, India and EMEA with 1 participant each shows a global perspective of this research.

Work Experience

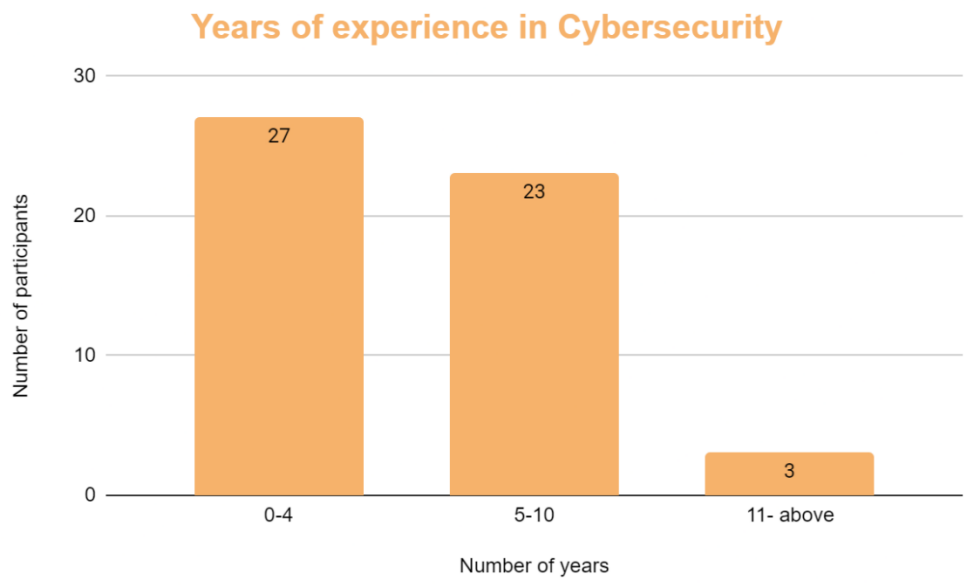

Figure 13: Work Experience of participants.

The years of experience of each participant in cybersecurity is essential to attaining substantial information about their perspective on the research subject and getting informed data about the state of security of the participant's organisations. This study has participants with a varying range of years of experience in cybersecurity, 0-4 years of experience has 27 participants, which accounts for the highest range in the study, followed by 23 participants with 5-10 years of experience, and lastly, 3 participants have 11 and above number of years of experience.

5.3 Data Analysis

As previously mentioned in subchapter 5.2, this research used survey questionnaires, which have been collected and structured to facilitate data analysis for report results. In regards to the role of artificial intelligence in incident response for digital domain SMEs, which is the aim of this research, the data analysis method chosen for this study helps to highlight the objectives of the study, that is, to measure the maturity level of SMEs in reference to the focal point of the research topic and ensure that adequate

plans are in place to prevent cyber-attacks and finally shed light on the limitations facing SMEs in the use of AI for IR processes in their organisation. Literature describes quantitative data analysis as a way of understanding the relationship between data and connecting the discovered relationships to the research context (Albers, 2017).

According to (Albers, 2017) there are three major methods used for quantitative data analysis: descriptive statistics, inferential statistics, and mixed methods of descriptive and inferential statistics. Inferential statistics is the most suitable method for data analysis for this research study based on the type of research questions and the aims and objectives of this study. (Sullivan-Bolyai & Bova, 2014) describes inferential statistics as a statistical procedure that enables researchers to estimate how reliable their findings can be used to make predictions and generalisations based on collected data; this data analysis method combines mathematical processes and logic.

Inferential statistics is known to have three major characteristics: to measure differences between groups, which will be done in the research by measuring the differences in the maturity level between SMEs and Large organisations. The second characteristic of inferential statistics is to assess relations between variables, and this will be done by assessing the relationship between variables such as security technology, security teams and security incidents in SMEs. The final characteristic of inferential statistics is to test hypotheses scientifically, which is the main reason for the research study.

In this inferential statistics, two statistical tests are utilised: the t-test, which tests the difference between two groups, and the analysis of variance, commonly known as the ANOVA test. Like the t-test, the ANOVA test differs by giving the opportunity to consider the variation between groups and within groups, which will be seen in the next chapter.

6 Result Analysis

The survey questions for this research study were structured into six different parts: the first part dealing with the general information of the participants and their organisations, the last part collecting data about the experiences of the participants, the other four parts, namely cybersecurity awareness, incident response management, security controls and technology and current usage of AI are the major factors that will be used to measure the role of artificial intelligence in incident response for digital domain SMEs through data analysis, which will be analysed and observed in this chapter.

6.1 Analysis of Cybersecurity Awareness

This aspect of the survey question focuses on gaining insight into the level of cyber security preparedness of the participants' organisations by measuring whether and how often they conduct cybersecurity training; it also delves into the status of the organisations' cyber security teams. This was done using a five-point linear scale, multichoice options, and yes or no radio buttons.

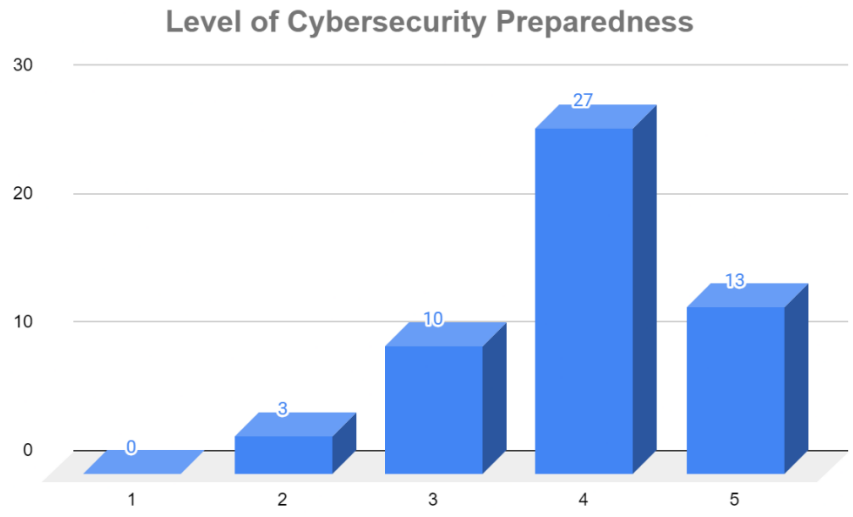

Figure 14: User responses on cybersecurity preparedness of organisations.

Figure 14 is a graphical representation of the answer to the question “How would you rate your organization's current level of cybersecurity preparedness?” This was measured using a 5-point scale: 1 = very low, 2 = low, 3 = medium, 4 = high, and 5 = very high.

Out of 53 responses recorded, 13 participants making 24.6%, rated their organisations as low and medium, while there was a higher percentage of 75.4% participants rated their organisations as high and very high.

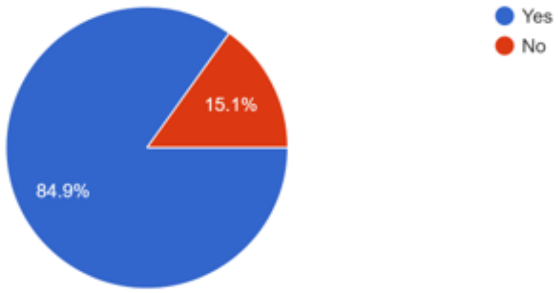

Figure 15: User responses on cybersecurity training and awareness program.

53 responses were recorded, of which 84.9% claim to have cybersecurity training and awareness programs in their organizations, and only 15.1% reported that they do not.

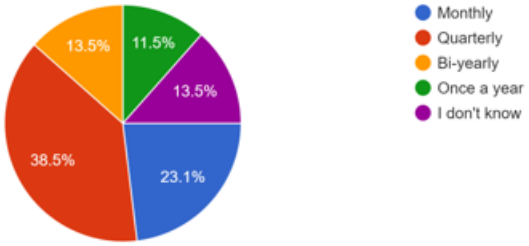

Figure 16: User responses on the frequency of cybersecurity programs.

Under this category of the question, "How frequently are cybersecurity training and awareness programs performed in your organization?", 52 responses were recorded of which 38.5% have training programs quarterly, 23.1% have trainings monthly, two different categories of bi-yearly and those who do not have the information were 13.5% and 11.5% have cybersecurity training programs once a year.

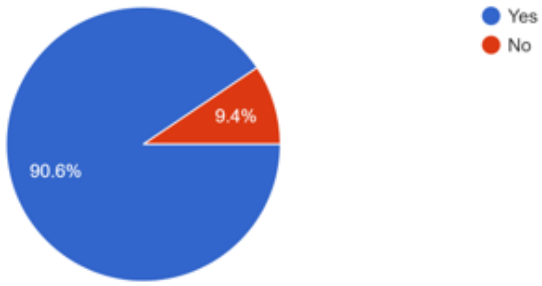

Figure 17: User responses on designated cybersecurity teams.

53 responses were recorded for the question, "Do you have a designated individual or team responsible for cybersecurity within your organization?", 90.6% gave a positive response and 9.4% gave a negative response to the question.

The next part of this analysis combines the participants who rated their organisations 4 and 5 together; this makes a total of 40 participants, as can be referenced in Figure 14. Of this number, most of the organizations are in Nigeria with 13 organizations and Finland with 8 organizations, the remaining 19 organizations are spread across the remaining geographical locations of the participants in this study.

To properly measure the authenticity of the rate of cybersecurity preparedness of the organizations provided by the participants, follow questions were asked such as if cybersecurity trainings are provided in the organizations, then the frequency of the cybersecurity training programs and whether the organizations have either in-house security teams or outsourced security team.

Figure 18: User responses on cybersecurity training for highly-rated organisations.

37 participants out of 40 participants have cybersecurity training programs in their organisation and only 38 participants have designated teams responsible for cybersecurity, of which 21 of the organizations is technology industry and 15 belongs to the finance industry with the rest sparsely spread across the other industry sectors in this study.

Table 4: Breakdown of Cybersecurity training Frequency in Organizations

Frequency	Micro	Small	Medium	Large	Total
Quarterly	-	2	3	11	16
Monthly	1	-	3	6	10
Bi-yearly	-	2	1	2	5
Once a year	-	4	-	1	5
I don’t know	-	1	1	2	4
Total	1	9	8	22	40

Large organisations conduct cybersecurity training for their employees more frequently. There were 40 participants in total, 22 of whom were large organizations and 18 SMEs.

Observations about Participants that rated their organizations high and very high in level of cybersecurity preparedness: Majority of the entire sample population rated their organizations level of cybersecurity preparedness high and very high, this lead to further investigation of checking the

validity of the votes by asking checking if cybersecurity training programs are organized in the organizations which is a means of preparing employees for cyber security incidents and improving security posture of the organizations, it was confirmed that 37 participants that rated their organization high and very high also have cybersecurity training programs available for them, the next means of validity check was done by asking if there was a designated team responsible for cybersecurity and 38 participants out of 40 indicated that they have a designated in house team responsible for their cybersecurity and finally the frequency of the cybersecurity training programs were measured, this result of this check showed that 26 participants organization have cybersecurity training programs more frequently monthly and quarterly as against the remaining 14 participants organizations that have trainings done bi-yearly, once a year and those who do not know.

It can be inferred from this analysis that organizations that have cybersecurity training programs in their organizations frequently and have designated teams responsible for cybersecurity can be regarded as having a high level of cybersecurity preparedness.

6.2 Analysis of Incident Response Management

Incident response management has been discussed in depth in Chapter 3 of this research study.

5-point scale questions, yes or no radio button and multichoice questions were asked to the participants about the incident response management status of their organization. The results are illustrated below:

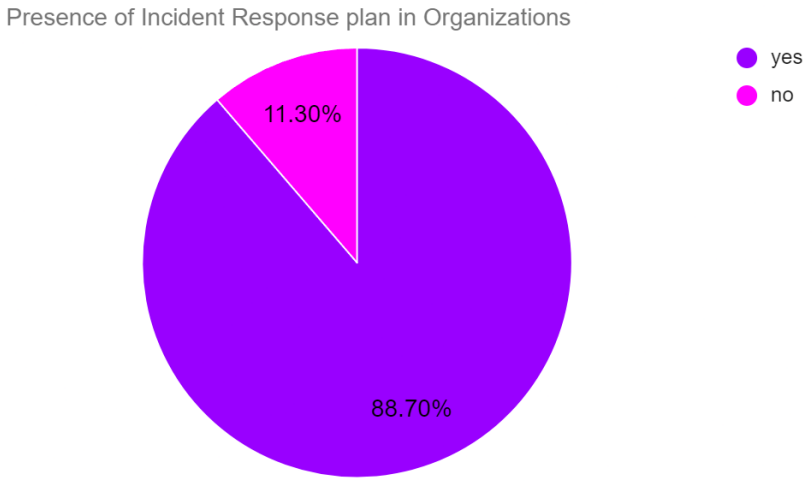

Figure 19: User response on the presence of incident response plan.

53 responses were recorded for the question, “Do you have an incident response plan in place to address cybersecurity incidents?” 88.7% of the respondents agreed that they have an incident response (IR) plan in their organizations, and 11.3% do not.

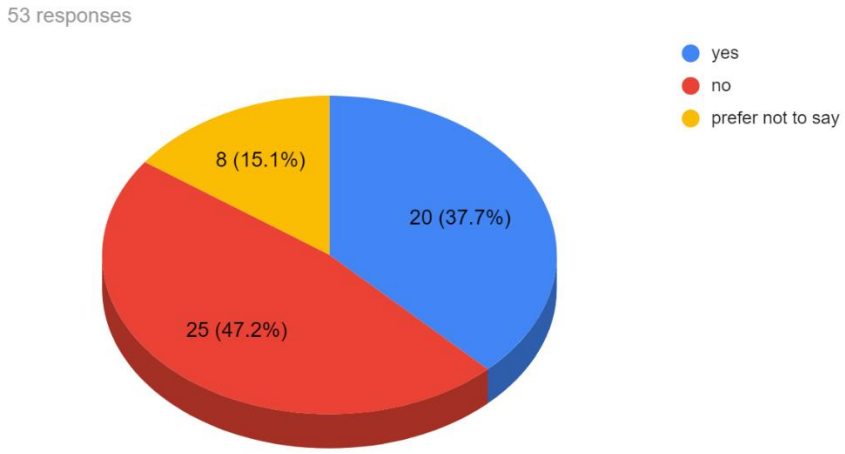

Figure 20: User response on cybersecurity incidents experienced in the past year.

Figure 20 shows the graphical representation of the 53 participants' responses to the question “Have you experienced any cybersecurity incidents or breaches in the past year?” Using a yes or no radio button, 47.2% of the participants claimed not to have experienced any cyber security incidents in the past year, 37.7% of participants said they had experienced security incidents, and 15.1% preferred not to respond to the question.

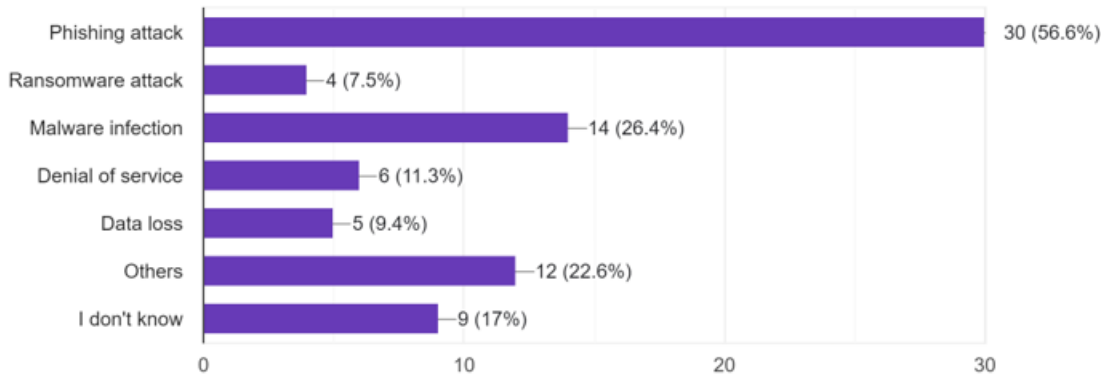

Figure 21: User response on type of cybersecurity incidents experienced.

The next question involved the 5 most common cybersecurity incidents experienced in 2024, asking the respondents to indicate which of the incidents they had experienced in their organisations. Phishing attacks were the most experienced cybersecurity incident by the participants, with a percentage of 56.6%.

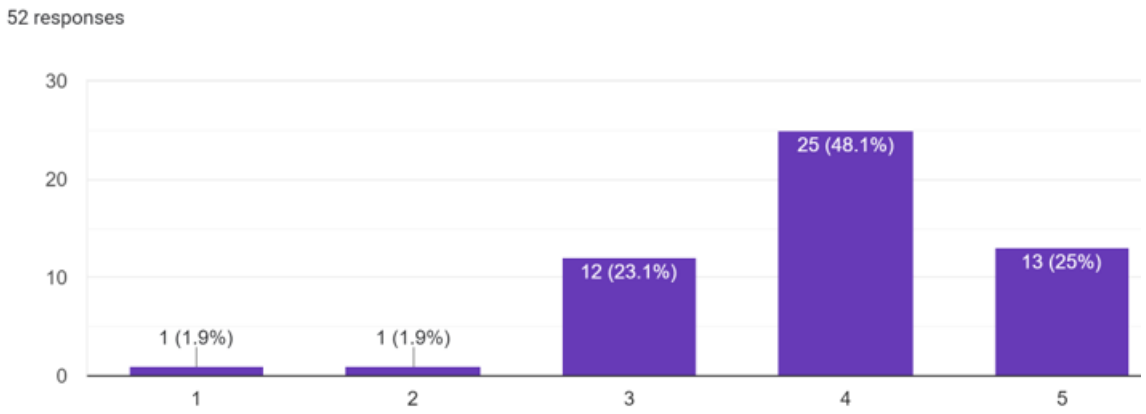

Figure 22: User response on the speed of responding to incidents.

52 responses were gotten from the participants to the question, “How quickly can your organisation respond to a cybersecurity incident?” a 5-point scale was used to measure this question, with the value 1 representing slowly and value 5 representing immediately, a high percentage of the participants believes that their organisation can detect and respond to cyber security incidents swiftly with 48.1% choosing the option quickly and 25% choosing the option immediately.

Observation about participants that have incident response plans in their organisations: Out of the 53 respondents, 47 of them stated that there is a provision for an incident response plan, which is defined as a document with a set of guidelines used to mitigate and recover from cybersecurity incidents. These 47 participants all rated the speed of their organisation's ability to respond and detect cybersecurity incidents positively, with 12 participants saying their organisations can respond immediately to cybersecurity incidents, 23 participants voting very quickly, and 11 participants voting quickly and also out of these 47 participants with incident response 23 participants claim not to have experienced any incidents, 16 participants have experienced incidents, and 8 participants prefer not to say. It can be inferred from this analysis that organisations with incident response plans in place can detect and respond quickly to cybersecurity incidents, giving them a lower chance of experiencing cybersecurity incidents.

6.3 Analysis of Security Controls and Technology

The need for security controls and technology is essential for incident response and the security posture of any organization; this has been discussed in previous chapters. The participants were provided with yes-or-no radio buttons, multi-choice options, and text-based answers to questions related to security controls and technology in their various organizations.

The breakdown of the security control and technology questions is provided below:

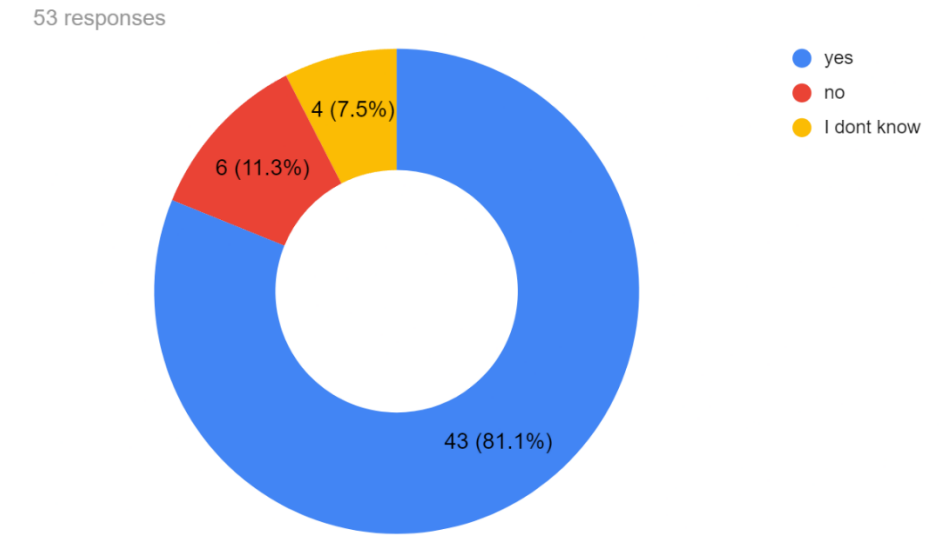

Figure 23: User response to a question about regulatory compliance framework.

53 responses were acquired for the question, "Is your organization currently using any regulatory compliance framework and standards?" 81.1% of the respondents utilize regulatory compliance framework and standards, 11.3% of the respondents do not use regulatory compliance framework and standards in their organization and 7.5% of the respondents do not know whether their organization uses regulatory compliance framework and standards.

Of the 43 participants whose organizations use regulatory compliance frameworks and standards, the most common are GDPR, NIST, ISO/IEC 27001, and PCI DSS. Other notable frameworks and standards recorded are CIS benchmarks, CIS control standards, HIPAA, IEC 62443, Cyber Resilience Act, NIS2, Machinery regulations, and NDPR.

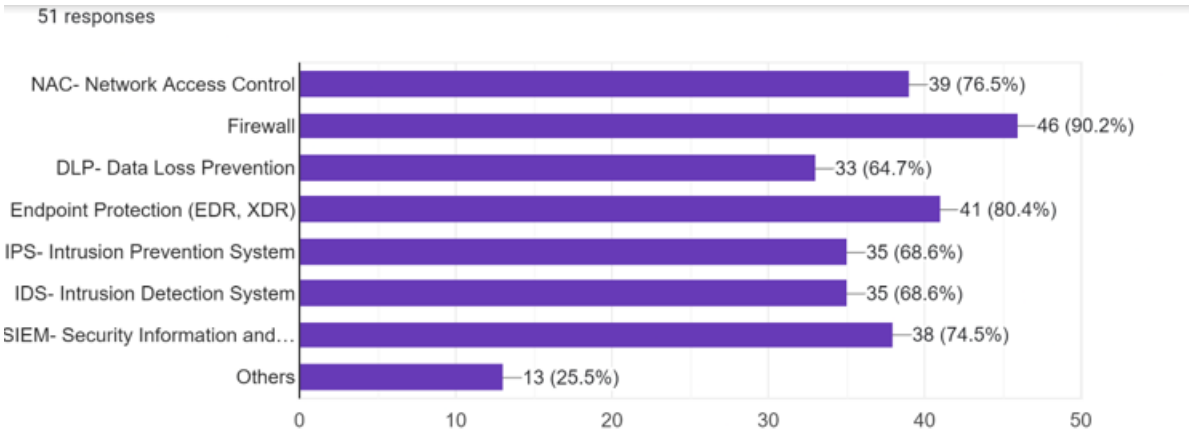

Figure 24: User response on types of security controls and technologies utilised in organisations.

Figure 24 illustrates the different security controls and technologies the participants currently use to protect their organization's assets.

Of 51 participants in descending order:

Firewall- used by 90.2%.

Endpoint Protection (EDR, XDR)- used by 80.4%.

NAC- Network Access Control- used by 76.5%.

SIEM- Security Information and Events Management- used by 74.5%.

IPS- Intrusion Prevention System – Used by 68.6%

IDS- Intrusion Detection System- Used by 68.6%

DLP-Data Loss Prevention – used by 64.7%.

Others- used by 25.5%.

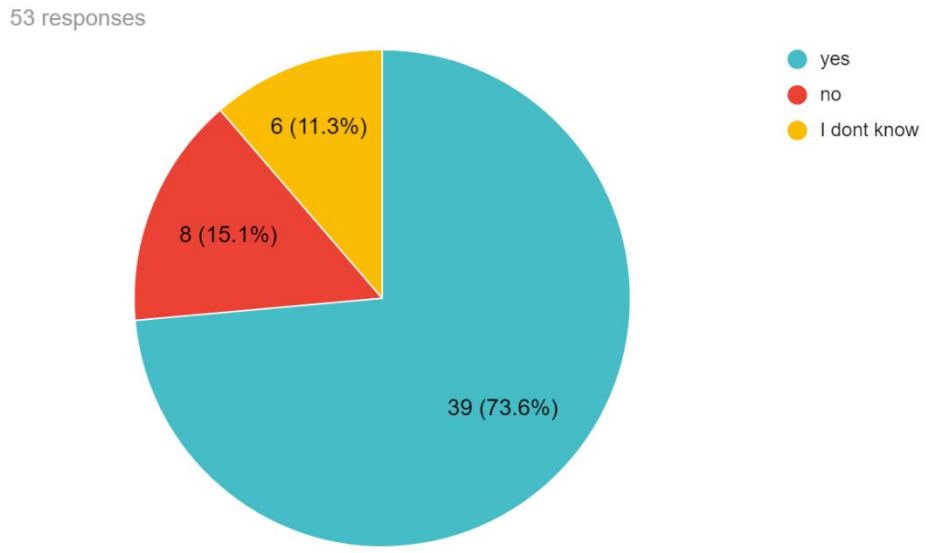

Figure 25: User response on emerging technologies or trends.

Figure 25 is a representation of the participants answer to the question “Do you leverage any emerging technologies or trends (AI) to enhance your cybersecurity posture?” 73.6% leverage emerging technologies like AI to enhance the organization's cybersecurity posture, 15.1% don’t and 11.3% do not know if their organization uses any emerging technologies or trends.

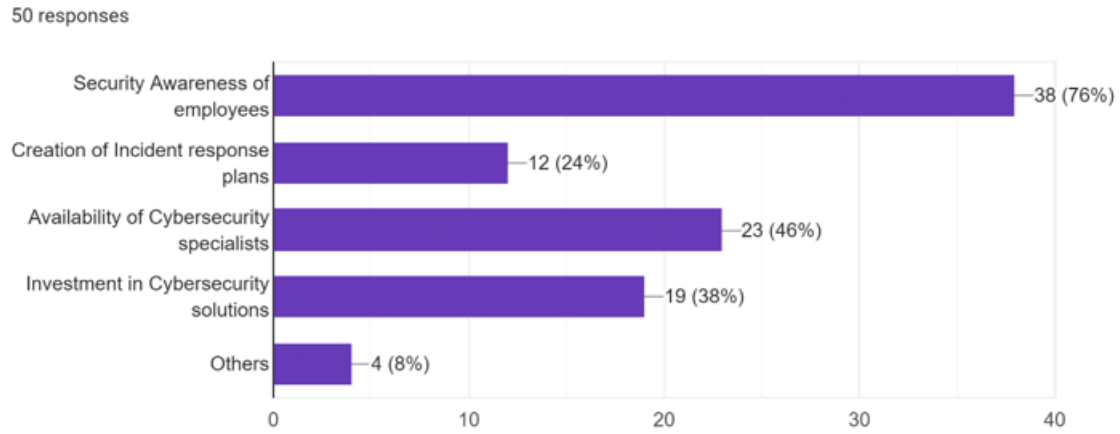

Figure 26: User response on areas of cybersecurity needing improvement.

50 responses were collected regarding the areas of cybersecurity participants consider most critical for improvement within their organisations. 38 participants recognise the need for security awareness of employees, 23 participants are of the opinion that availability of cybersecurity specialists is their prominent need, 19 participants think their organization should invest in cybersecurity solutions, 12 participants voted for the creation of incident response plans and 4 participants chose the option of others.

6.4 Analysis of Current Usage of AI

This section of the survey dives into the current usage of artificial intelligence for incident response in the participants organizations. The importance of this section has been discussed in Chapter 4 of literature review. The use of a 5-point rating scale, multichoice options and yes or no radio button were utilized in this section to answer the questions provided.

The analysis of the responses of the respondents is detailed below:

This section starts with trying to understand the familiarity of the concept of using AI for incident response by the participants; out of 53 responses, 43 participants have medium to high familiarity with the concept, while the remaining 10 are not familiar with the concept of using AI for incident response.

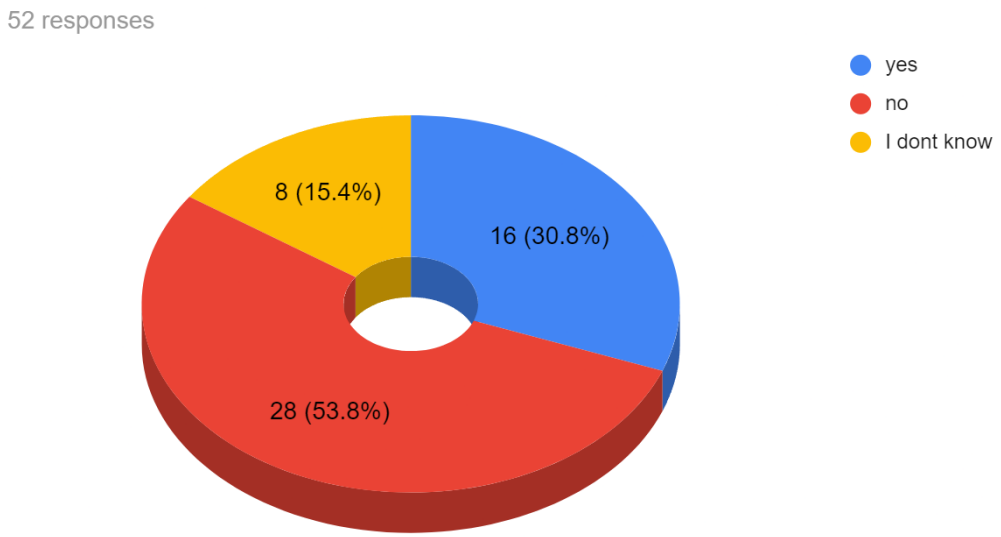

Figure 27: User response on the use of AI technologies for IR.

The next step involved gathering data about the current utilisation of AI-driven technologies or solutions for incident response within the participants organization, out of 52 participants that answered the question,53.8% do not utilize AI-driven technologies for IR in their organization, 30.8% are currently using AI-driven technologies for IR and 15.4% do not know about the status of their organization.

Out of the 30.8% of participants whose organisations are already using AI-driven technologies, 68.4% have been using AI-driven technologies for incident response for 1-5 years, and 26.3% for less than a year, finally, 5.3% have been in the practice of using AI-driven technologies for IR for 6 years and above.

Out of 53.8% participants with organizations not utilizing AI-driven technologies for incident response, when asked if there is any plan to use AI-driven technologies for incident response in the future, 43.9% stated that there are plans in place for that and 48.8% do not know if there are plans or not and 7.3% have no plans to utilize AI-driven technologies for IR.

Further into the investigation of the current use of AI for IR in the participants organization, the participants were asked if they believe AI can improve the speed and effectiveness of incident detection and response, of which out of 53 respondents, 94.3% believe that AI can indeed improve the speed and effectiveness of incident detection and response, 3.8% do not agree with the notion and 1.9% claim not to know.

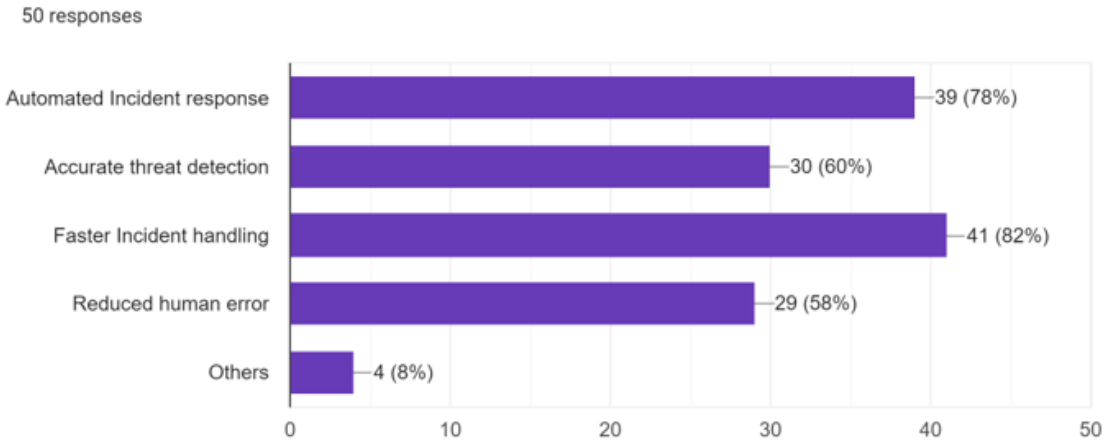

Figure 28: User response on expected benefits of AI-driven IR solutions.

Figure 28 depicts the responses of the participants to the question, "What benefits do you expect AI-driven incident response solutions to provide for your organisation?"

50 respondents voted "Faster incident handling" as the most popular option with 82% expecting faster incident handling to be beneficial to their organization, this is in line with one of the objectives of this research study "To respond to incidents timely so that the mean time to respond (MTTR) is as low as possible with the use of AI integrated cyber security solutions for incident response."

78% of the respondents believe that automated incident response will be an expected benefit of using AI-driven incident response solutions, 60% chose accurate threat detection, and 58% chose reduced human error as the benefits they expect from utilising AI-driven incident response solutions. All of these options also answer one of the research questions of this study, which is "How can AI be used to strengthen the cyber defence of SMEs?" and also show how AI-integrated IR tools can provide a security edge for digital domain organisations.

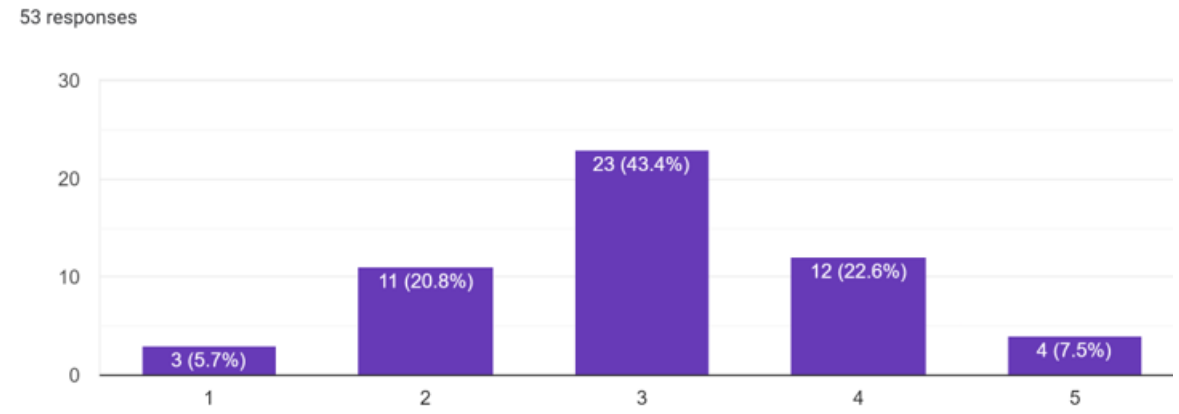

Figure 29: User response on the ease of integrating AI-driven IR solutions into existing infrastructure.

53 responses were recorded from the question, "How easily do you think AI-driven incident response solutions can be integrated into your existing cybersecurity infrastructure?" a 5-point scale, with 1 being easily and 5 being difficult, was set for the participants to answer the question. Based on the graphical

representation of the answer in Figure 29, most participants fall into the category of AI-driven incident response solutions being difficult to integrate into existing cybersecurity infrastructure.

This led to the next question of asking the participants if there is a need for additional training or upskilling of personnel to be able to effectively use AI-driven incident response solutions; 88.7% of the 53 respondents anticipate the need for upskilling of personnel, and 5.7% both do not anticipate a need for training personnel and don't know whether there will be a need or not for additional training of personnel to effectively use AI-driven incident response solutions.

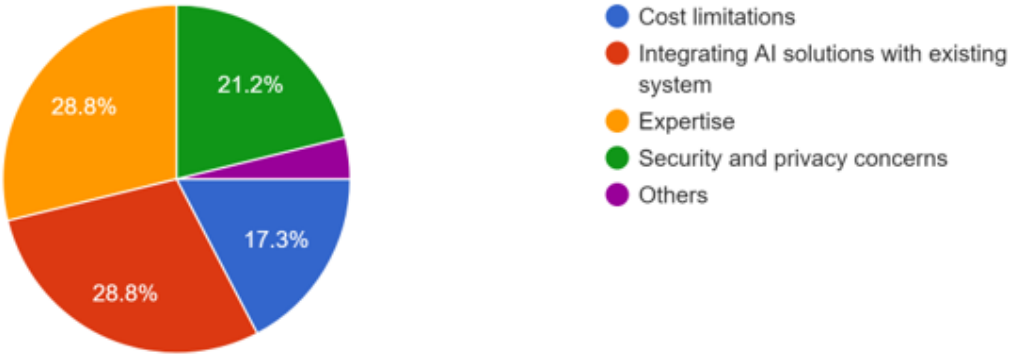

Figure 30: User responses on challenges foreseen in implementing AI-driven IR solutions.

Figure 30 illustrates the challenges participants foreseen in implementing AI-driven incident response solutions in their organisations.

Out of 52 participants:

28.8% foresee the challenges of integrating AI solutions with existing systems and expertise.

21.2% foresee the challenge of security and privacy concerns.

17.3% foresee the challenge of cost limitations.

6.5 Comparison between various Entities

There are different relationship connections and differences between several entities that help to better understand the role of artificial intelligence in incident response for digital domain SMEs, which are discussed in this sub-chapter.

6.5.1 Comparison between organisations using AI and those not using AI.

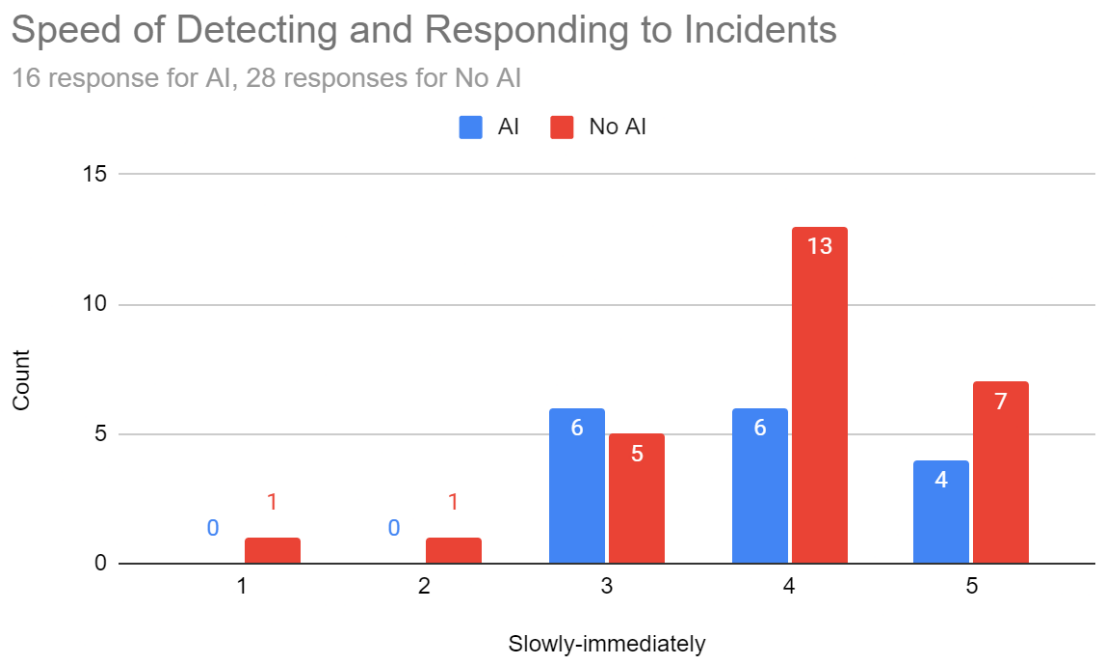

Figure 31: Speed of incident response between AI industries and No AI industries.

The speed for measuring how quickly organisations can detect and respond to cybersecurity incidents was measured using a 5-point scale where the value 1 represents slowly, 2 represents average speed, 3 represents quickly, 4 represents very quickly and 5 represents immediately.

Organisations utilising AI have a 100% speed rate for detecting and responding to cybersecurity incidents. Of these, 75% are able to detect and respond to incidents quickly and very quickly and 25% have the capacity to respond immediately, making organisations using AI have a 100% speed rate when it comes to detecting and responding to cybersecurity incidents.

As for organisations that do not make use of AI, 7% detect and respond to cybersecurity incidents slowly, 17.9% are able to detect and respond quickly, 46.6% can detect and respond to incidents very quickly and 25% fall into the category of immediately. This amounts to only 93% being able to detect and respond to cybersecurity incidents quickly, with 7% having slow detection and response speed to security incidents.

This data suggests that the use of AI in incident response guarantees a 100% high speed of detecting and responding to cybersecurity incidents. This correlates with AI's ability to provide faster incident handling, which in turn reduces the mean time to respond (MTTR) to cybersecurity incidents.

6.5.2 Comparison between Technology Industries and Finance Industries

In the general information sector in Chapter 5, under demographic factors, the technology industry sector and the finance industry sector were the most common industry sectors for digital domain organisations, with Technology having 56.9% and Finance having 41.2% of the sample responses. The table below shows the comparison between both industries as related to the focus of this research study.

Table 5: Differences between Technology and Finance industries.

Characteristics	**Technology Industries**	**Finance Industries**
Most responses from country	Finland	Nigeria
Presence of Cybersecurity training and awareness program	70%	100%
Presence of a designated cybersecurity team	80%	100%
Presence and use of incident response plan	85%	93%
Speed of detecting and responding to cybersecurity incidents	90% can detect and respond quickly to cybersecurity incidents	100% can detect and respond quickly to cybersecurity incidents
Utilisation of regulatory compliance frameworks and standards	70%	100%
Use of AI-driven incident response solutions	30%	43%
Stand on whether AI can improve the speed and effectiveness of IR	95% agree	100% agree

Observation: The finance industry sector appears to have a better security posture in their organisations regarding cybersecurity maturity and the use of artificial intelligence in incident response. The technology industries are also well equipped but have room for improvement of security posture, especially in areas such as the use of AI-driven incident response solutions, utilisation of regulatory compliance framework and standards and the presence of cybersecurity training and awareness programs for employees.

6.5.3 Comparison between Technology Industries in Finland and Nigeria

According to the survey results, 20 participants work in technology industries, of which 9 are from Finland and 3 are from Nigeria. This section is a comparative analysis between Nigeria and Finland because the two countries are the most populated countries in this research survey sample pool. All the Technology industries between the two countries fall under the SME sector, and neither of them belongs to large organisations.

Table 6: Differences between Technology industries in Finland and Nigeria (SMEs)

Characteristics	Finland	Nigeria
Presence of Cybersecurity training and awareness program	44.4%	100%
Presence of a Designated cybersecurity team	77.8%	66.7%
Presence and use of incident response plan	66.7%	100%
Currently leveraging emerging technologies (AI/Cloud)	33.3%	100%
Use of AI-driven incident response solutions	Nil	66.7%

Observation: Technology industries in Nigeria appear to have a higher percentage of security posture in the various aspects, presence of cybersecurity training and awareness programs, presence and use of incident response plan, leveraging of emerging technologies and the use of AI-driven incident response solutions, while technology industries in Finland have the upper hand in the presence of designated cybersecurity teams. The limited number of respondents in the targeted countries impacts the statistical analysis of the research study.

A comparative analysis of Finance industries between Nigeria and Finland could not be conducted because none of the participants worked in the Finance industry from Finland.

6.5.4 Comparison between SMEs and Large Organizations

Out of 53 respondents, 29 work in large enterprises and 24 work in SMEs; this section will highlight major differences between the two sectors.

Table 7: Comparison between SMEs and Large organisations.

Characteristics	SMEs	Large
Presence of Cybersecurity training and awareness program	66%	100%
Presence of a Designated cybersecurity team	79%	100%
Presence and use of incident response plan	79%	97%
Utilisation of regulatory compliance frameworks and standards	63%	97%
Use of AI-driven incident response solutions	21%	38%
Most challenges faced in implementing AI-driven IR solutions.	-Expertise -Cost Limitations -Integrating AI solutions with existing system	Security and privacy concerns

Observations: From the data above, it can be inferred that large organisations have a better security posture regarding incident response, with a very high percentage of them having the presence of cybersecurity training and awareness programs, presence of designated cybersecurity teams, presence and use of incident response plan and the use of regulatory compliance framework and standards as against SMEs who still have a range of characteristics needing improvement. Large organisations also use more AI-driven incident response solutions than SMEs, with their major challenge in implementing AI-driven IR solutions being security and privacy concerns, whereas SMEs are faced with more challenges, such as insufficient expertise, cost limitations and the ability to integrate AI solutions with existing systems.

6.5.5 Comparison between Large Enterprises in Finland and Nigeria

The total number of large enterprises in this study amounts to 29, of which 15 are in Nigeria and 2 are from Finland. The table below shows the different characteristics between the two countries regarding their security posture and use of artificial intelligence.

Table 8: Difference between Large enterprises in Finland and Nigeria

Characteristics	Finland	Nigeria
Presence of Cybersecurity training and awareness program	100%	100%
Presence of a Designated cybersecurity team	100%	100%
Presence and use of incident response plan	100%	93.3%
Utilisation of regulatory compliance frameworks and standards	100%	100%
Currently leveraging emerging technologies (AI/Cloud)	50%	93.3%
Use of AI-driven incident response solutions	50%	46.7%
Stand on whether AI can improve the speed and effectiveness of IR	100%	100%

Observations: There are numerous similarities between the large organisations in Finland and Nigeria; they both have strong foundations in cybersecurity training programs, designated cybersecurity teams, presence and use of incident response plans and the use of regulatory compliance frameworks and standards. However, they differ in the aspect of leveraging emerging technologies such as AI and Cloud technologies, with only 50% of large organisations in Finland leveraging emerging technologies, whereas a large percentage of 93.3% leverage emerging technologies in Nigeria. The use of AI-driven incident response solutions is average in Finland, with only 50% of the large organisations utilising AI-driven incident response solutions, while in Nigeria, the use of AI-driven incident response solutions is slightly below average, with 46.7% falling into that category. Both countries agree fully that AI can improve the speed and effectiveness of incident response.

6.5.6 Differences between Micro, Small and Medium Enterprises

Micro, small, and medium enterprises make up 24 participants in this study, with micro enterprises having 3 participants, small enterprises having 11 participants, and medium enterprises having 10 participants. The SMEs are mainly technology industries, with most of them geographically populated in Finland, followed by Nigeria and then the United Kingdom. There are several similarities between these enterprises, but this section of this research study focuses on the major differences between the enterprises.

Table 9: Differences between Micro, Small and Medium Enterprises.

Characteristics	MICRO	SMALL	MEDIUM
Presence of Cybersecurity training and awareness program	33.3%	73%	70%
Frequency of Cybersecurity training and awareness program	-	Once a year	Monthly
Most experienced cybersecurity incidents	Denial of Service (DOS)	Phishing attacks	Phishing attacks
Areas needing improvement within enterprises	Investment in Cybersecurity solutions	Security Awareness of employees	Availability of Cybersecurity specialist
Most challenges faced in implementing AI-driven IR solutions.	Lack of expertise	Integrating AI solutions with existing systems	Cost limitations

Observations: The differences between micro, small, and medium organisations vary, as can be seen in the table above; the presence of cybersecurity training and awareness programs has a significantly low percentage in micro-enterprises compared to small and medium enterprises. As a result of the low presence of security training in micro organisations, there appears to be a non-existent frequency of cybersecurity training, whereas, in small organisations, cybersecurity training is commonly performed once a year and monthly in medium organisations.

Small and medium enterprises experience more phishing attacks than micro-organizations, and all three enterprises face different challenges when implementing AI-driven IR solutions.

6.5.7 Comparison between SMEs in Finland and Nigeria

Out of the 24 respondents from SMEs, 14 are from Finland and Nigeria, with 10 from Finland and 4 from Nigeria. The other 10 are from the remaining different countries represented in this study. This section gives a comparative analysis of the state of SMEs in the two countries.

Table 10: Differences between SMEs in Finland and Nigeria

Characteristics	Finland	Nigeria
Presence of Cybersecurity training and awareness program	50%	100%
Presence of a designated cybersecurity team	80%	75%
Presence and use of incident response plan	70%	100%
Utilisation of regulatory compliance frameworks and standards	60%	100%
Use of AI-driven incident response solutions	Nil	50%
Stand on whether AI can improve the speed and effectiveness of IR	90% agree	100% agree

Observations: it can be inferred from the analysis in Table 8 that SMEs in Nigeria have a better security posture than SMEs in Finland, it can be noted that SMEs in Nigeria are more open to the concept of using AI-driven incident response solutions than SMEs in Finland that are not using AI-driven incident response solutions in their organizations.

The number of participants and understanding of the participants regarding the survey questions in this comparative analysis are variables that might influence the result of this study.

6.5.8 Security posture of organisations with NO designated security team.

5 respondents have no designated security team for their organisations, neither an in-house team nor an outsourced team. This segment shows the organisations' security posture.

Figure 32: Security posture of enterprises with no security team.

Figure 32 illustrates four areas of the security posture of enterprises without a designated security team. The area of cybersecurity with the most critical need for improvement is security awareness of

employees, the most experienced cybersecurity incident by the organisations is a phishing attack, while measuring the speed at which the organisation can detect and respond to cybersecurity incidents is at an average speed. All the participants anticipate the need for additional training or upskilling of personnel to effectively use AI-driven incident response solutions.

7 Conclusion

This chapter concludes the research study by discussing its findings, recommendations to digital domain SMEs, limitations, and future work on the research topic.

7.1 Discussion of findings

The researcher discussed in Chapter 1 of this study that SMEs constitute a large part of any economy, and they also experience 43% of cyber-attacks, of which successful incidents can lead to loss of reputation and financial loss. That is not a favourable outcome for any organisation. Several pieces of literature hold the opinion that the use of artificial intelligence gives organisations a positive edge in the process of incident response to cyber security attacks. This research focused on understanding the role of artificial intelligence in incident response for digital domain SMEs by exploring the concept of artificial intelligence, incident response and related works on the subject topic together with the use case of AI in IR. To assess the maturity level of organisation and measure their security posture, the opinions of users regarding cybersecurity awareness, incident response management, security controls and technologies and the current usage of AI were determined with the use of quantitative data, the analysis of the participant's perceptions helped determine the areas needing improvement and the limitations being faced by SMEs and well-detailed responses to the impact of artificial intelligence in incident response. The survey questionnaire was the empirical quantitative data analysis method used in this study, which was used to support the three research questions of this research and four main objectives.

Research question 1 asked how AI can be used to expediate the response time in a cyber-attack for SMEs. It was well explained in Chapter four. Survey analysis was also conducted to correlate the theoretical response from literature reviews with practical answers from respondents, where 94.3% of respondents agreed that artificial intelligence can improve the speed and effectiveness of incident detection and response.

Research question 2 asked how AI can be used to strengthen the cyber defence of SMEs; this was well detailed in Chapter 2 of the literature review in the sub-section discussing the importance of artificial intelligence. Survey results were used to support the answers provided in the literature review, with 82% of participants agreeing that faster incident handling is a benefit of AI in IR, 78% of participants see automated incident response as a beneficial characteristic of AI in IR, 60% of participants believe that the use of AI in IR produces accurate threat detection and 58% participant agree that the utilisation of AI in IR leads to reduced human error.

Research question 3 asked how artificial intelligence can be infused into the six phases of IR for SMEs; the answer to this research question is properly detailed in Chapter 4 of this research study.

The survey analysis also shows participants with a high percentage of use for different security controls and technologies that work efficiently in the six phases of incident response, such as endpoint protections, security information and event management (SIEM), and intrusion detection and protection systems (IDS/IPS), among others.

The four main objectives of the research were achieved using the quantitative data obtained from all 53 participants.

Objective 1 of this study focused on ensuring that SMEs have adequate plans in place to prevent a cyber-attack on their organisation. 88.7% of the participants have incident response plans in place in their organisations, which provide a detailed set of procedures that outline how an organisation will detect, respond, mitigate, and recover from cybersecurity incidents.

Objective 2 of this study is concerned with how to respond to incidents in a timely so that the mean time to respond is as low as possible with the use of AI-integrated cyber security solutions for incident response. The mean time to respond to an incident is the highest amount of time an enterprise can afford to respond and take action against a cybersecurity incident before it leads to disruption of the organisation's operations. The majority of the participants, 82%, are of the opinion that faster incident handling is a major benefit of using AI-integrated cyber security solutions for incident response.

Objective 3 of this research addresses the limitations facing SMEs in utilising AI in their incident response processes. Among the participants working in SMEs, three major challenges were addressed as the limitations affecting SMEs in using AI in their IR response, they are cost limitations, lack of expertise and difficulty integrating AI solutions with existing systems.

Objective 4 focused on measuring the maturity level of SMEs in relation to the use of AI in their processes; only 21% of SME participants make use of AI-driven incident response solutions in their organisations, which is below average out of the 79% of SMEs that do not utilise AI-driven incident response solution, only 40 % have future plans of introducing the use of AI-driven incident response solutions in their organisations, this points to a low maturity level for SMEs.

It can be concluded that the current use of AI-driven incident response solutions is below average, with 21% and 38% of SMEs and large organisations, respectively, actively using AI-driven incident response solutions. However, the reason for the low use of AI was identified as cost limitations, lack of expertise, and difficulty integrating AI into existing systems. The role of Artificial Intelligence in incident response was recognised in this research study, with a total of 98% of the participants agreeing that AI can improve the speed and effectiveness of incident response and faster incident handling being the most voted benefit of using AI-driven incident response solutions in numerous organisations.

7.2 Recommendations

The following are some of the insightful recommendations provided by the participants regarding the role of artificial intelligence in incident response in digital domain SMEs. Two recommendations are provided by participants with 0-4 years and 5-10 years of cybersecurity experience, and one recommendation is from a participant with 11 years or more of cybersecurity working experience.

"The deployment of AI-driven incident response is a great leap in the security architecture of any company. I recommend it should be done in a phased approach and adequate training provided to the security analyst to derive maximum value".

"*AI-driven IR solutions should be highly considered as it is a more effective way to stay ahead of advanced threats. Organisations should also consider the ease of integration with AI-driven IR solutions with their existing security solutions*".

"*It's highly recommended to adopt AI-driven solution for Incident response; it reduces compromise level and contributes as a major factor to protect the business reputation*".

"*The core issue with AI-driven IR is privacy. AI will, most of the time, need data for training, and some of this data can be PII. The concern is whether organisations can trust their confidential data to AI solutions. I recommend that organisations scope data requirements of AI solutions and design systems that prevent privacy and data loss*."

"*They clearly have potential, but right now, we lack solutions that are easy to integrate and affordable*".

The data analysis of the sample population of this research study shows that digital domain SMEs are not utilising AI in their incident response processes due to issues like cost limitations, lack of expertise and integration of AI solutions with existing systems. Digital domain SMEs need to use AI methods to remain competitive. Therefore the cost of cybersecurity technologies, such as AI, should be considered as part of the operational cost of the organisation with a high level of priority because it is a rewarding investment, in the long run, to stay ahead of cyber adversaries actively.

7.3 Limitations of study

Listed below are some of the limitations of this research study:
Firstly, the number of representations of SME employees is considerably low compared to that of large organisations, which significantly impacted the comparison of different parameters between various entities in the research study.

Secondly, this study utilised only one method of data collection, which was quantitative data; the use of a mixed data collection method would have been better because although the quantitative data gives a precise and accurate measure of the role of AI in incident response, the questions in the survey might not have been interpreted in the same manner by all the participants, the use of qualitative method would have provided more in-depth information on certain variables related to the research topic.
Lastly, the researcher could not get sufficient representation of employees from countries other than Finland and Nigeria.

7.4 Future works

Some suggested future work for this study includes getting more SME cybersecurity employees working in digital domain enterprises as participants for the study. Secondly, future research should utilise the mixed data collection method to get both statistical data and in-depth information about the study. Finally, focusing on a particular geographical location instead of numerous ones can help drill down to specific perspectives of the research study.

References

Abrokwah-Larbi, K., & Awuku-Larbi, Y. (2023). The impact of artificial intelligence in marketing on the performance of business organizations: evidence from SMEs in an emerging economy. *Journal of Entrepreneurship in Emerging Economies*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/JEEE-07-2022-0207

Agrawal, J., Kalra, S. S., & Gidwani, H. (2023). AI in cyber security. *International Journal of Communication and Information Technology*, *4*(1), 46–53. https://doi.org/10.33545/2707661x.2023.v4.i1a.59

Albers, M. J. (2017). Quantitative Data Analysis—In the Graduate Curriculum. *Journal of Technical Writing and Communication*, *47*(2), 215–233. https://doi.org/10.1177/0047281617692067

Ali, T., & Kostakos, P. (2023). *HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs)*. http://arxiv.org/abs/2309.16021

Almalki, S. (2016). Integrating Quantitative and Qualitative Data in Mixed Methods Research—Challenges and Benefits. *Journal of Education and Learning*, *5*(3), 288. https://doi.org/10.5539/jel.v5n3p288

Arjun C Vinod, A Ananthakrishnan, A.R Abhishek, S. Adithyan, & Tintu Varghese. (2022). Is Artificial Intelligence a Threat or a Benefit? *International Journal of Engineering Technology and Management Sciences*, *6*(5), 553–555. https://doi.org/10.46647/ijetms.2022.v06i05.087

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393–410.

Balwan, A. K., Balwan, W. K., & Saba, N. (2022). Glance of Research Methodology for Researchers: A Logical Assessment. *Scholars Bulletin*, *8*(3), 95–100. https://doi.org/10.36348/sb.2022.v08i03.004

Ban, T., Takahashi, T., Ndichu, S., & Inoue, D. (2023). Breaking Alert Fatigue: AI-Assisted SIEM Framework for Effective Incident Response. *Applied Sciences (Switzerland)*, *13*(11). https://doi.org/10.3390/app13116610

Bartock, M., Cichonski, J., Souppaya, M., Witte, G., & Scarfone, K. (2016). *Guide for cybersecurity event recovery*.

Bergadano, F., & Giacinto, G. (2023). Special Issue "AI for Cybersecurity: Robust Models for Authentication, Threat and Anomaly Detection." In *Algorithms* (Vol. 16, Issue 7). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/a16070327

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). The role of artificial intelligence in cyber security. In *Countering cyber attacks and preserving the integrity and availability of critical systems* (pp. 170–192). IGI Global.

Bhatnagar, S., Cotton, T., Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Héigeartaigh, S. Ó., Beard, S., Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation Authors are listed in order of contribution Design Direction*.

Bryman, A. (2016). *Social research methods*. Oxford university press.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3197899

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.800-61r2

Coombes, D. (2023, April 26). *Subsets Of AI: The Ultimate Overview*. https://topapps.ai/blog/subsets-of-ai/

Corbett, M., & Sajal, S. (2023). AI in Cybersecurity. *2023 Intermountain Engineering, Technology and Computing, IETC 2023*, 334–338. https://doi.org/10.1109/IETC57902.2023.10152034

Crume, J. (2023, May 31). *Artificial Intelligence (AI) Cybersecurity | IBM*. https://www.ibm.com/ai-cybersecurity?mhsrc=ibmsearch_a&mhq=AI%20in%20cybersecurity

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: Https://Nvlpubs. Nist. Gov/Nistpubs/CSWP/NIST. CSWP*, *4162018*, 7.

De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920.

Dr. Swarooprani. K. (2022). An Study of Research Methodology. *International Journal of Scientific Research in Science, Engineering and Technology*, 537–543. https://doi.org/10.32628/ijsrset2293175

ENISA. (2021, June 28). *Phishing most common Cyber Incident faced by SMEs — ENISA*. https://www.enisa.europa.eu/news/enisa-news/phishing-most-common-cyber-incidents-faced-by-smes

Exabeam. (2024). *AI SIEM: How SIEM with AI/ML is Revolutionizing the SOC*. https://www.exabeam.com/explainers/siem/ai-siem-how-siem-with-ai-ml-is-revolutionizing-the-soc/

Fritsch, L., Jaber, A., & Yazidi, A. (2022). An Overview of Artificial Intelligence Used in Malware. In E. Zouganeli, A. Yazidi, G. Mello, & P. Lind (Eds.), *Nordic Artificial Intelligence Research and Development* (pp. 41–51). Springer International Publishing.

Gibert, D., Mateu, C., & Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications*, *153*, 102526.

Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, *61*(4), 5–14. https://doi.org/10.1177/0008125619864925

Harel, Y., Gal, I. Ben, & Elovici, Y. (2017). Cyber security and the role of intelligent systems in addressing its challenges. In *ACM Transactions on Intelligent Systems and Technology (TIST)* (Vol. 8, Issue 4, pp. 1–12). ACM New York, NY, USA.

Harsch, A., Idler, S., & Thurner, S. (2014). Assuming a state of compromise: A best practise approach for SMEs on incident response management. *2014 Eighth International Conference on IT Security Incident Management & IT Forensics*, 76–84.

Hassan, S. K., & Ibrahim, A. (2023). The role of Artificial Intelligence in Cyber Security and Incident Response. *International Journal for Electronic Crime Investigation*, *7*(2).

Hofstetter, M., Riedl, R., Gees, T., Koumpis, A., & Schaberreiter, T. (2020). Applications of AI in cybersecurity. *2020 Second International Conference on Transdisciplinary AI (TransAI)*, 138–141.

IBM. (2024). *Security QRadar | IBM*. https://www.ibm.com/qradar

Jada, I., & Mayayise, T. O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 100063.

Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), 1–34.

Kant, D., & Johannsen, A. (2022). Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). *J. Electron. Imaging*, *34*, MOBMU-387.

Karthick, A. V., & Gopalsamy, S. (2022). Artificial Intelligence: Trends and Challenges. *PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing*, 7–12. https://doi.org/10.1109/PDGC56933.2022.10053238

Khanzode, K. C. A., & Sarode, R. D. (2020). Advantages and disadvantages of artificial intelligence and machine learning: A literature review. *International Journal of Library & Information Science (IJLIS)*, *9*(1), 3.

Kick, J. (2014). Cyber exercise playbook. *The MITRE Corporation*.

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence. *Journal of Computers, Mechanical and Management*, *2*(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

Marais, B., Quertier, T., & Morucci, S. (2022). *AI-based Malware and Ransomware Detection Models*. http://arxiv.org/abs/2207.02108

Marc Hornbeek. (2023, August 15). *Unleashing AI in SRE: A New Dawn for Incident Management*. https://devops.com/unleashing-ai-in-sre-a-new-dawn-for-incident-management/

McEvoy, O. (2024, March 14). *SMEs in the EU 2023, by size | Statista*. https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/

Melnikovas, A. (2018). Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies. *Journal of Futures Studies*, *23*(2).

Mijwil, M. M. (2015). *History of Artificial Intelligence*. https://doi.org/10.13140/RG.2.2.16418.15046

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers and Security*, *25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Morovat, K., & Panda, B. (2020). A Survey of Artificial Intelligence in Cybersecurity. *Proceedings - 2020 International Conference on Computational Science and Computational Intelligence, CSCI 2020*, 109–115. https://doi.org/10.1109/CSCI51800.2020.00026

Nalbant, K. G. (2021). The importance of artificial intelligence in education: a short review. *Journal of Review in Science and Engineering*, *2021*, 1–15.

Onwubiko, C., & Ouazzane, K. (2022). SOTER: A Playbook for Cybersecurity Incident Management. *IEEE Transactions on Engineering Management*, *69*(6), 3771–3791. https://doi.org/10.1109/TEM.2020.2979832

OpenAI. (2023). *ChatGPT 3.5*. https://chat.openai.com/chat

Palatty, N. J. (2023, December 22). *51 Small Business Cyber Attack Statistics 2024*. https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/

Rahman, M. M., Tabash, M. I., Salamzadeh, A., Abduli, S., & Rahaman, M. S. (2022). Sampling techniques (probability) for quantitative social science researchers: a conceptual guideline with examples. *Seeu Review*, *17*(1), 42–51.

Rajasekar, D., & Verma, R. (2013). *Research methodology*. Archers & Elevators Publishing House.

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11), 150.

Rawindaran, N., Nawaf, L., Bentotahewa, V., Prakash, E., Jayal, A., Hewage, C., & Alghazzawi, D. M. N. (2022). Detection and Minimization of Malware by Implementing AI in SMEs. In E. Babulak (Ed.), *Malware* (p. Ch. 3). IntechOpen. https://doi.org/10.5772/intechopen.108229

Rizvi, M. (2023a). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, *10*(5).

Rizvi, M. (2023b). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, *10*(5), 055–060. https://doi.org/10.22161/ijaers.105.8

Ryan, G. (2018). Introduction to positivism, interpretivism and critical theory. *Nurse Researcher*, *25*(4), 41–49.

Sale, A. (2023, February 23). *AI: What are the different Domains/Subsets of Artificial Intelligence? | by Antonello Sale | Medium*. https://medium.com/@a.sale/ai-what-are-the-different-domains-subsets-of-artificial-intelligence-4cfd5477584

Schnepp, R., Vidal, R., & Hawley, C. (2017). *Incident management for operations*. "O'Reilly Media, Inc."

Shaked, A., Cherdantseva, Y., & Burnap, P. (2022, August 23). Model-Based Incident Response Playbooks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3538969.3538976

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers and Security*, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

Shanthi, R. R., Sasi, N. K., & Gouthaman, P. (2023). A New Era of Cybersecurity: The Influence of Artificial Intelligence. *Proceedings of the 1st IEEE International Conference on Networking and Communications 2023, ICNWC 2023*. https://doi.org/10.1109/ICNWC57852.2023.10127453

Sileyew, K. J. (2019). *Research design and methodology* (Vol. 7). Cyberspace.

SISA. (2022). *AI in Cybersecurity: Incident Response Automation Opportunities*. https://www.sisainfosec.com/blogs/ai-in-cybersecurity-incident-response-automation-opportunities/

Sullivan-Bolyai, S., & Bova, C. (2014). Data analysis: Descriptive and inferential statistics. *Nursing Research-E-Book: Methods and Critical Appraisal for Evidence-Based Practice*, *310*.

Swift, D. (2006, December 23). *A Practical Application of SIM/SEM/SIEM Automating Threat Identification*. https://sansorg.egnyte.com/dl/wGohjgzmXb

SYTECH. (2024, March 10). *Top 10 Cyber Security Threats in 2024 | SYTECH*. https://sytech-consultants.com/top-10-cyber-security-threats-in-2024/

Thuraisingham, B. (2020). The role of artificial intelligence and cyber security for social media. *2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, 1–3.

Tripathi, A. S. (2023, July 7). *The Subsets of Artificial Intelligence - Scaler Topics*. https://www.scaler.com/topics/artificial-intelligence-tutorial/subsets-of-ai/

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry*, *12*(3), 410.

Vaibhav Chandrasen Vaidya, & Payal Tekchand Rewatkar. (2023). Artificial Intelligence's Advantages and Disadvantages in Terms of Cybersecurity and Phishing Attacks. *International Journal of Advanced Research in Science, Communication and Technology*, 512–516. https://doi.org/10.48175/ijarsct-11677

Veiga, A. Da. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *2016 SAI Computing Conference (SAI)*, 1006–1015. https://doi.org/10.1109/SAI.2016.755610

Appendices

Appendix 1: Survey Questions

Answering the survey takes approximately 10-15 minutes. All answers will be handled anonymously, and the answers will be used in a master's thesis on the role of AI in Incident Response for SMEs.
No data about the organisation or employee will be used, and the survey is purposely for gathering statistics for educational purposes.
The survey contains 6 sections covering General information, Cybersecurity Awareness, Incident Response Management, Security controls and technologies, Current usage of AI, and Experiences.

Survey Questions

General Information

• What is the size of your organisation (number of employees)?

1. Micro (0-9), 2. Small (10-49), 3. Medium (50-249) 4. Large (250-above)

• What industry sector does your organisation operate in?

1. Technology 2. Finance 3. Healthcare 4. E-commerce 5. Manufacturing 6. Transportation/Logistics 7. Energy and Utility 8. Media/ Entertainment

• How many years of experience do you have in Cybersecurity?

1. (0-4) 2. (5- 10) 3. (11 and above)

Cybersecurity Awareness

• How would you rate your organisation's current level of cybersecurity preparedness on a scale of 1 to 5

• How frequently are cybersecurity training and awareness programs performed in your organisation?

1. Very low 2. Low 3. Medium 4. High 5. Very High

• Do you have cybersecurity training and awareness programs in your organisation?

1. Yes 2. No

• How frequently do you think cybersecurity training and awareness programs should be done?

1. Monthly 2. Quarterly 3. Bi-yearly 4. Once a year 5. I don’t know.

• Do you have a designated individual or team responsible for cybersecurity within your organisation?

1. Yes 2. No

• If No to the above question, do you have an outsourced Cybersecurity team for your organisation?
1. Yes 2. No

Incident Response Management

• Do you have an incident response plan to address cybersecurity incidents? (An incident response plan is a documented set of guidelines that outlines how an organisation will detect, respond, mitigate, and recover from cybersecurity incidents.)
1. Yes 2. No

• Have you experienced any cybersecurity incidents or breaches in the past year?
1. Yes 2. No 3. Prefer not to say.

•Have you experienced any of the following cybersecurity incidents in your organisation? (you can pick more than one option)
1. Phishing attack 2. Ransomware attack 3. Malware infection 4. Denial of service. 5. Data loss 6. Others 7. I don't know.

• How quickly can your organisation detect and respond to a cybersecurity incident?
1. Slowly 2. Average speed 3. Quickly 4. Very quickly 5. Immediately

Security Controls and Technologies

•Is your organisation currently using any regulatory compliance framework and standards (GDPR, ISO/IEC 27001, NIST, HIPAA, PCI DSS)?
1. Yes 2. No 3. I don't know.

• If yes, can you specify which regulatory compliance framework and standards are being implemented?

• If No, is there any plan to utilise any regulatory compliance framework and standards?
1. Yes 2. No 3. I don't know.

• Which security controls and technologies do you currently have in place to protect your organisation's assets? (you can pick more than one option)

1. NAC- Network Access Control
2. Firewall
3. DLP- Data Loss Prevention
4. Endpoint Protection

5. IPS- Intrusion Prevention System
6. SIEM- Security Information and Event Management
7. Others
8. I don't know.

• What areas of cybersecurity do you consider most critical for improvement within your organisation? (you can pick more than one option)

1. Security Awareness of employees
2. Creation of Incident response plans
3. Availability of Cybersecurity specialists
4. Investment in Cybersecurity solutions
5. Others
6. I don't know.

• Do you leverage any emerging technologies or trends (e.g., AI, cloud security) to enhance your cybersecurity posture?

1. Yes 2. No 3. I don't know.

Current Usage of AI

• How familiar are you with the concept of using AI for incident response?

1. Not familiar 2. Mildly familiar 3. Very familiar

• Are you currently utilising any AI-driven technologies or solutions for incident response within your organisation?

1. Yes 2. No 3. I don't know.

• What benefits do you expect AI-driven incident response solutions to provide for your organisation? (you can pick more than one option)

1. Automated Incident response
2. Accurate threat detection
3. Faster Incident handling
4. Reduced human error
5. Others
6. I don't know.

• Do you believe AI can improve the speed and effectiveness of incident detection and response?

1. Yes 2. No 3. I don't know.

• How easily do you think AI-driven incident response solutions can be integrated into your existing cybersecurity infrastructure?
1. Very easily 2. Easily 3. Neutral 4. Difficult 5. Extremely difficult

• Do you anticipate the need for additional training or upskilling of personnel to effectively use AI-driven incident response solutions?
1. Yes 2. No 3. I don't know.

• What challenges do you foresee in implementing AI-driven incident response solutions in your organisation?
1. Cost limitations
2. Integrating AI solutions with existing systems
3. Expertise
4. Security and privacy concerns
5. I don't know
6. Others

Experiences

• Have you heard of or encountered any success stories or case studies related to AI-driven incident response in similar organisations?
1. Yes 2. No

• Are you open to sharing additional feedback or insights from your own experiences with AI-driven incident response solutions?

• What recommendations would you give to organisations regarding the use of AI-driven incident response solutions?