The Global Cybersecurity Workforce Shortage and the Potential of Artificial Intelligence.

Karl Flynn

Masters in Business Administration

National College of Ireland

Submitted to the National College of Ireland, August 2024.

National College of Ireland

Project Submission Sheet

Student Name: Karl Flynn………………………………………………………………………………………

Student ID: 22156097………………………………………………………………………………………

Programme: MBANC22…………………………………………… **Year:** 2024……………

Module: MBA Thesis ……………………………………………………………………………………

Lecturer: Dave Hurley……………………………………………………………………………………

Submission Due Date: 10th August 2024………………………………………………………………………………

Project Title: The Global Cybersecurity Workforce Shortage and the Potential of Artificial Intelligence.…………………………………………………………

Word Count: 17,788………………………………………………………………………………………………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: ………………………………………………………………………………………

Date: 10 August 2024………………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

MBANC2 Thesis.

The Global Cybersecurity Workforce Shortage and the Potential of Artificial Intelligence.

Your Name/Student Number	Course	Date
22156097	MBANC2	10/08/2024

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
n/a		
n/a		

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

N/A	
N/A	
N/A	N/A

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

N/A

Additional Evidence:

N/A

The Global Cybersecurity Workforce Shortage and the Potential

of Artificial Intelligence.

By Karl Flynn.

Abstract

As technology becomes more integral to every facet of society, and the modern world becomes increasingly digitised, the threat of cyber-attacks to governments, organisations and individuals represents a significant risk factor. The field of Cybersecurity is tasked with protecting governments, organisations and individuals against these threats. Cyber-attacks are becoming increasingly advanced, threat actors are becoming increasingly sophisticated, new working practices and governmental regulations are increasing the workload of already pressurised Cyber teams. While this is happening, there is a significant and growing shortage of Cybersecurity professionals globally, even though there is global understanding of the criticality of the issue, and some actions have been taken to try and mitigate the issue, demand is still outstripping supply year on year.

This study researches the increasing demand for Cybersecurity professionals, what's driving that and the impact of the Covid-19 pandemic on demand for Cyber professionals. The study also researches the global Cybersecurity workforce shortage and the numbers of Cyber professionals needed globally. The research study also investigates what attempts have been made to mitigate that shortage and how effective those efforts have been. The research study then investigates the capabilities of Artificial Intelligence, and it's potential in helping mitigate the workforce shortage. The primary research consisted of ten in-depth interviews, with open-ended questions. The ten interview subjects, consisted of Cybersecurity stakeholders, five of the interviewees were directly involved in the hiring process as HR professionals or hiring managers, or part of the hiring team. Thematic analysis was used to identify themes and patterns within the data, then an inductive approach was used to identify findings and encourage discussion. The aim of the research is to study the existing literature, gain insights from the primary research interviewees and determine if Artificial Intelligence can help mitigate the Cybersecurity workforce shortage.

Acknowledgements.

I would like to express my sincerest thanks to my supervisor Dave Hurley, who's guidance, sincerity, encouragement and support have been of immense help to me throughout this process.

My sincere thanks also to The National College of Ireland MBA class of 2024, who's support, friendship and comraderie have been invaluable to me throughout this journey, also to all the lecturers and staff of The National College of Ireland who have taught, tutored and supported me in this process.

I would also like to thank all of my primary research interviewees, firstly for taking time out of their busy schedules and helping me with their honest, in-depth and valuable opinions, and helping me with this research study into the world of Cybersecurity and Artificial Intelligence.

I would also like to thank my friends, who have encouraged me, and given me advice and support throughout this process. A very special thanks to my wife Jackie and son Marcus who have been unwaveringly supportive and patient with me throughout this journey. To my incredible sisters Annmarie, Caroline, Catherine, Paula and Vanessa, thank you for providing me with such inspiration and ambition. Thank you also to Mam and Dad, Anne and Tommy, and to Tom, Anthony and Dymphna, and to my wider family.

Table of Contents

Table of Figures.

CHAPTER 1:

INTRODUCTION TO THE RESEARCH TOPIC AND THESIS.

1.1 BACKGROUND TO THE STUDY.

Organisations and governments globally are finding it increasingly difficult to recruit Cybersecurity staff to help them secure and protect their assets against the growing numbers of, and increasingly sophisticated cyber-attacks which are causing financial loss, reputational damage and service disruption. This study will research the existing shortage, the increasing demand, the current attempts to mitigate the shortage, and the potential of Artificial Intelligence in alleviating the shortage.

1.1.1 Global shortage of Cybersecurity Professionals.

The International Information System Security Certification Consortium or ISC2, compile an annual report called the "Cybersecurity Workforce Study". The 2023 report stated that even though there has been an increase in the global workforce of Cybersecurity Professionals by nearly 9% to nearly 5.5 million year on year, as shown in Fig. 1. below. Demand for Cybersecurity professionals has still outgrown supply and the workforce gap has grown by 12.6%, see Fig. 2. below (ISC2, 2023).

Figure 1: 2023 Global Cybersecurity Workforce.

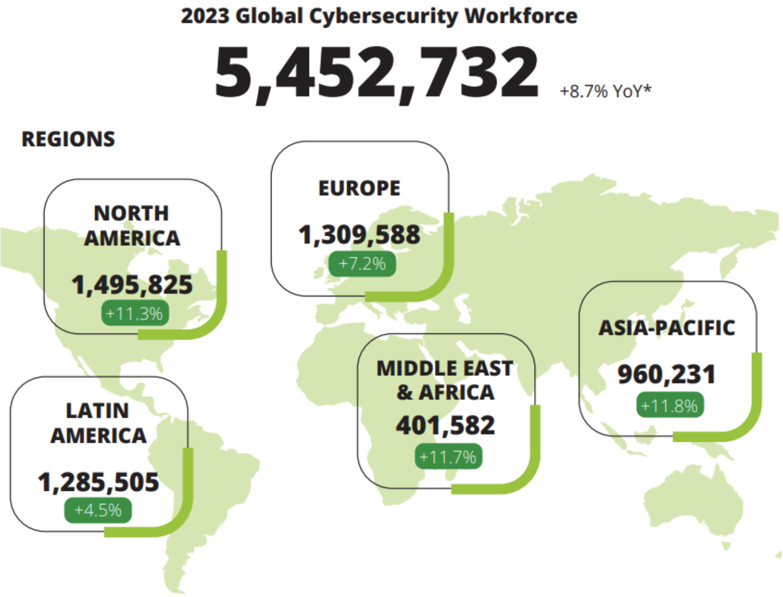
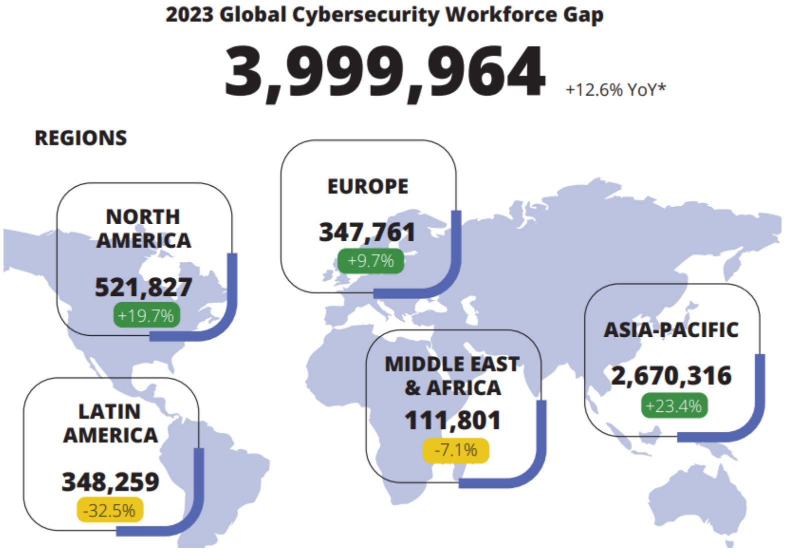


Figure 2: 2023 Global Cybersecurity Workforce Gap



1.1.2 Current approaches to mitigating the shortage of Cybersecurity Professionals.

Organisations such as the European Union Agency for Cybersecurity (ENISA) in Europe, the National Institute of Standards and Technology (NIST) in the US, have developed frameworks to help define roles and responsibilities within the field of Cybersecurity. The ENISA developed the European Cybersecurity Framework (ECSF) (ENISA,2022a). NIST have published the National Institute for Cybersecurity Workforce Framework (NICE) framework (CISA,2024a). The purpose of these frameworks is to guide Cybersecurity managers, HR professionals and Educators in defining roles and responsibilities, creating Job specifications, and developing certifications and educational content. The goal of these initiatives is to help educate, train and develop candidates into Cybersecurity professionals.

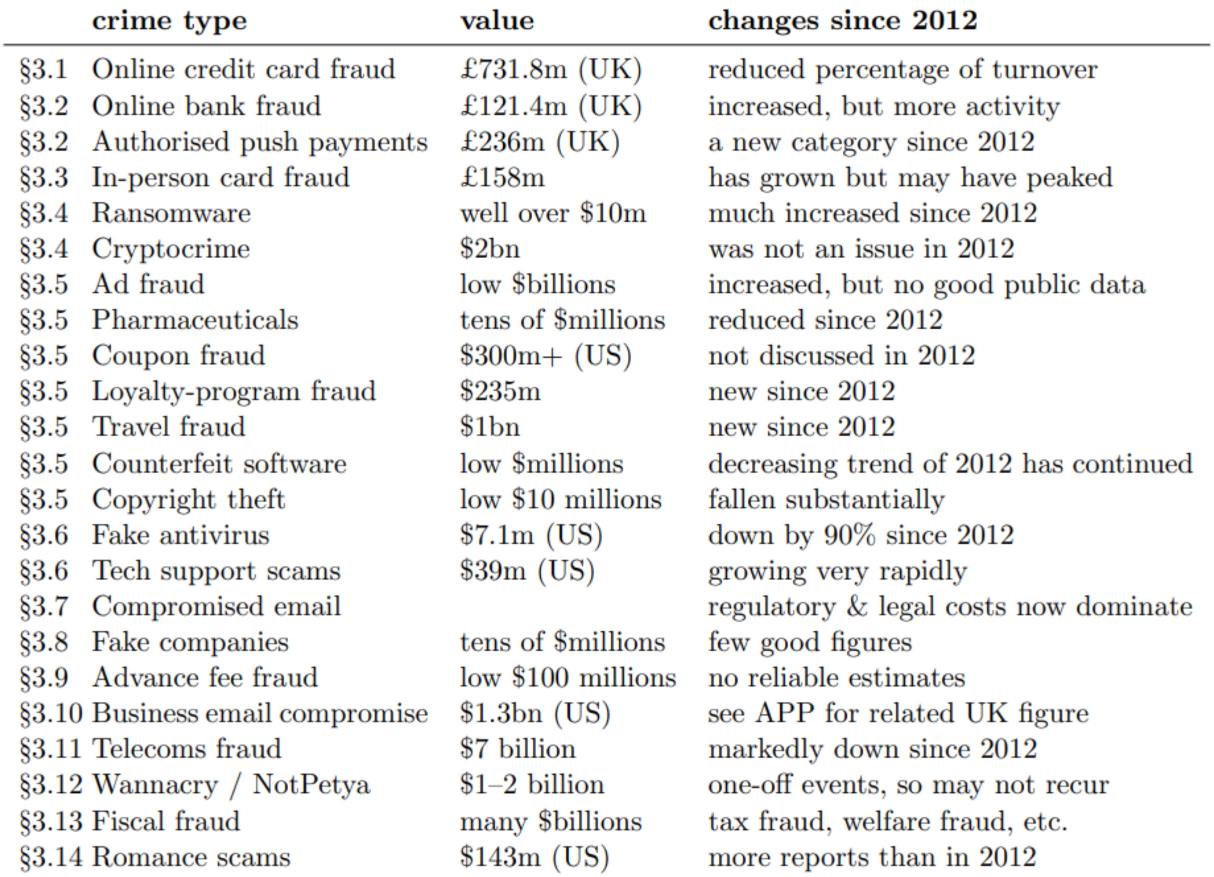
1.1.3 Drivers of Increasing demand for Cybersecurity Professionals.

In the Pre-Covid world, increasing levels of digitisation within global economies, with increasing reliance on online shopping had meant that opportunities for Cyber Criminals had increased. Between 2012 and 2019, new categories of Cybercrime had been introduced, as can be seen in Fig: 3. below (Ross et al., 2019).

During the Covid-19 pandemic, due to the restrictions put in place globally, both shopping and work practices had to change. This presented an opportunity for Cybercriminals who sought to gain from the sudden change in both shopping and working practices (Monteith, 2021).

The Post-Covid Cybersecurity landscape has seen most of the work practices that were introduced remain, at least in some capacity. However there have also been new regulations introduced that have put additional pressure on Cybersecurity teams to achieve compliance (Blazic,2021). All of the above mentioned factors have contributed to an increasing demand for Cybersecurity Professionals as can be seen in the ISC2 Cybersecurity Workforce Study (ISC2,2023).

Figure 3: Changes in UK Cybercrime Categories between 2012 and 2019.



	crime type	value	changes since 2012
§3.1	Online credit card fraud	£731.8m (UK)	reduced percentage of turnover
§3.2	Online bank fraud	£121.4m (UK)	increased, but more activity
§3.2	Authorised push payments	£236m (UK)	a new category since 2012
§3.3	In-person card fraud	£158m	has grown but may have peaked
§3.4	Ransomware	well over $10m	much increased since 2012
§3.4	Cryptocrime	$2bn	was not an issue in 2012
§3.5	Ad fraud	low $billions	increased, but no good public data
§3.5	Pharmaceuticals	tens of $millions	reduced since 2012
§3.5	Coupon fraud	$300m+ (US)	not discussed in 2012
§3.5	Loyalty-program fraud	$235m	new since 2012
§3.5	Travel fraud	$1bn	new since 2012
§3.5	Counterfeit software	low $millions	decreasing trend of 2012 has continued
§3.5	Copyright theft	low $10 millions	fallen substantially
§3.6	Fake antivirus	$7.1m (US)	down by 90% since 2012
§3.6	Tech support scams	$39m (US)	growing very rapidly
§3.7	Compromised email		regulatory & legal costs now dominate
§3.8	Fake companies	tens of $millions	few good figures
§3.9	Advance fee fraud	low $100 millions	no reliable estimates
§3.10	Business email compromise	$1.3bn (US)	see APP for related UK figure
§3.11	Telecoms fraud	$7 billion	markedly down since 2012
§3.12	Wannacry / NotPetya	$1–2 billion	one-off events, so may not recur
§3.13	Fiscal fraud	many $billions	tax fraud, welfare fraud, etc.
§3.14	Romance scams	$143m (US)	more reports than in 2012

1.2 GAPS IN THE LITERATURE.

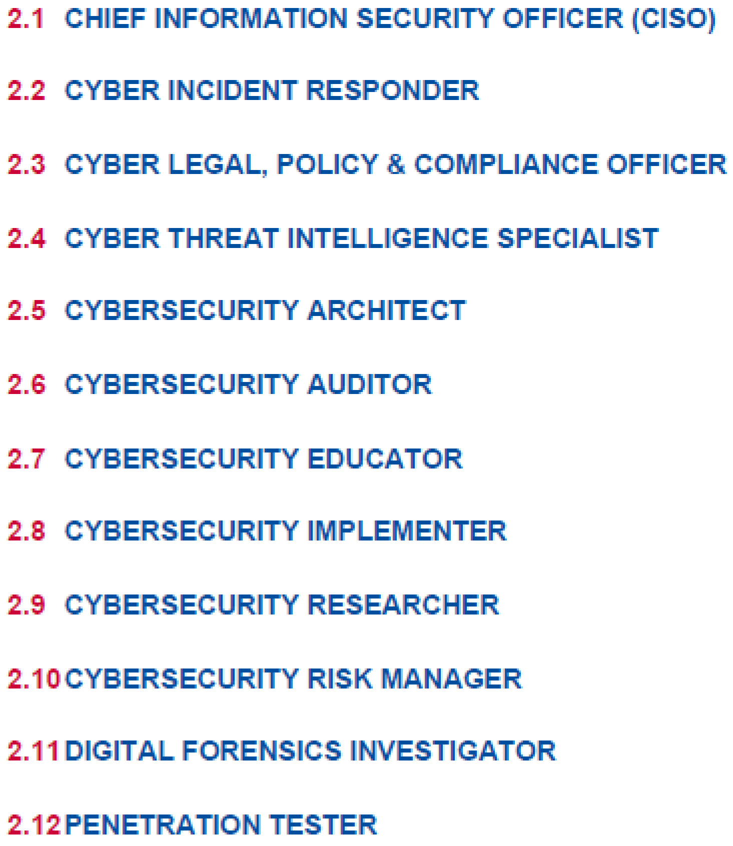
1.2.1 Aligning Artificial Intelligence Cybersecurity Capabilities, with the tasks and roles specified in the competency Frameworks.

Artificial Intelligence (AI) is today used by Security vendors such as Palo Alto Networks. Cisco and Fortinet within their Cybersecurity product suite. These vendors have identified the value that AI can bring in automating tasks like handling large amounts of data, detecting anomalies and identifying malicious behaviour (Gregory, 2024).

The ENISA and NIST have both published frameworks that identify Cybersecurity role profiles, and the main tasks that are carried out by people in those roles. Frameworks such as the ECSF, which lists 12 role profiles (as seen in Fig. 4. below) and gives the main task list and key skills needed to be carried out for each of the Role Profiles, as seen in Fig. 5. below. The NIST:NICE framework lists 7 job categories (as seen in Fig. 6. below), which encapsulate 52 roles and over 2,200 tasks that are to be carried out within the roles (NIST,2020).

Existing literature encapsulates the Cybersecurity workforce shortage, the Cybersecurity Frameworks and AI in Cybersecurity, however a literature gap exists in bringing together and aligning the capabilities of AI, with the Categories, roles and tasks of the established frameworks. The existing Body of Knowledge could be enhanced by further research into aligning the tasks and roles AI can perform, with the categories, roles and tasks that have been defined in the established frameworks. This could in turn help organisations identify and utilise AI tools to help mitigate the workforce shortage within their organisations and also within the wider field of Cybersecurity.

Figure 4: ENISA: ECSF 12 Role Profiles.



2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)

2.2 CYBER INCIDENT RESPONDER

2.3 CYBER LEGAL, POLICY & COMPLIANCE OFFICER

2.4 CYBER THREAT INTELLIGENCE SPECIALIST

2.5 CYBERSECURITY ARCHITECT

2.6 CYBERSECURITY AUDITOR

2.7 CYBERSECURITY EDUCATOR

2.8 CYBERSECURITY IMPLEMENTER

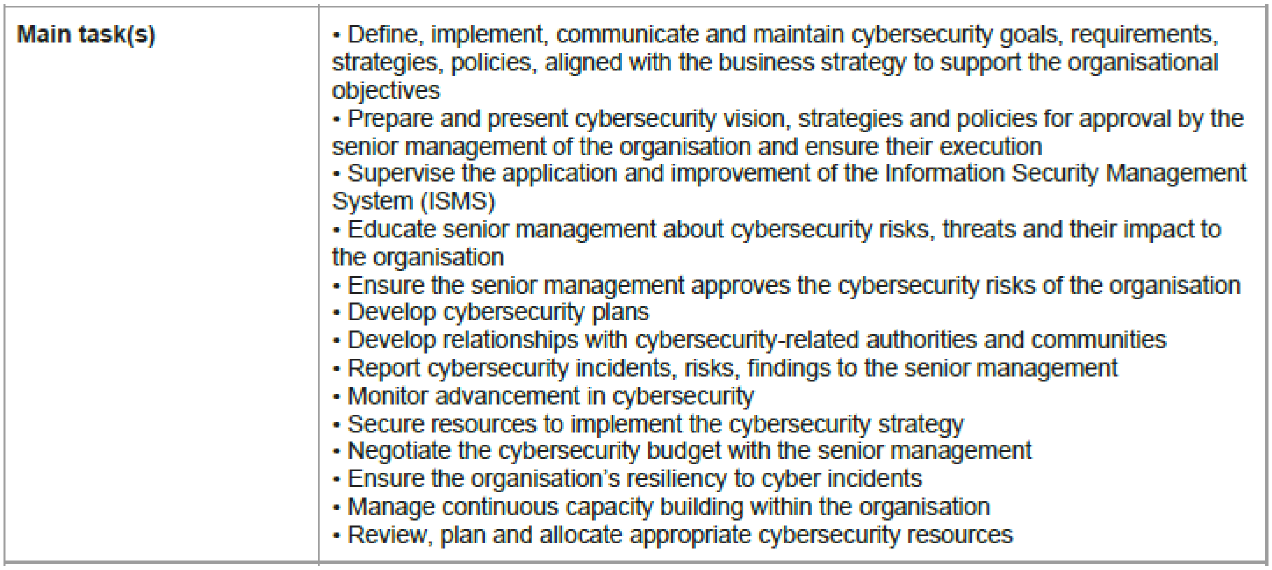
2.9 CYBERSECURITY RESEARCHER

2.10 CYBERSECURITY RISK MANAGER

2.11 DIGITAL FORENSICS INVESTIGATOR

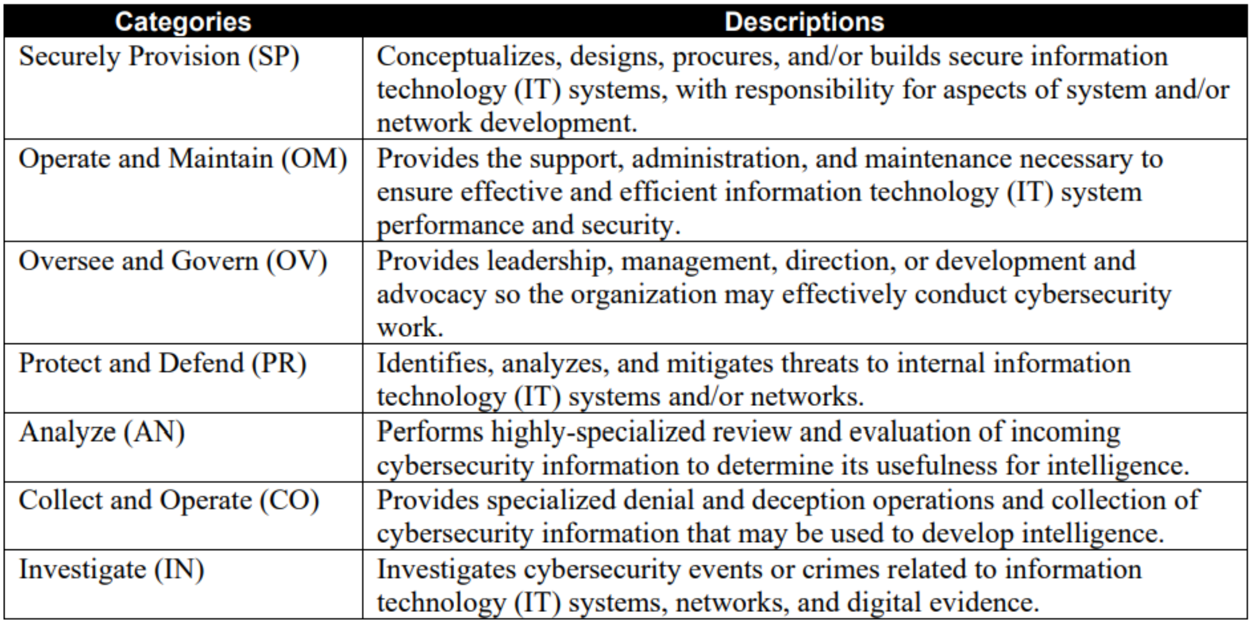
2.12 PENETRATION TESTER

Figure 5 Main Tasks & Key Skills example: Chief Information Security Officer.



Main task(s)	• Define, implement, communicate and maintain cybersecurity goals, requirements, strategies, policies, aligned with the business strategy to support the organisational objectives • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisation and ensure their execution • Supervise the application and improvement of the Information Security Management System (ISMS) • Educate senior management about cybersecurity risks, threats and their impact to the organisation • Ensure the senior management approves the cybersecurity risks of the organisation • Develop cybersecurity plans • Develop relationships with cybersecurity-related authorities and communities • Report cybersecurity incidents, risks, findings to the senior management • Monitor advancement in cybersecurity • Secure resources to implement the cybersecurity strategy • Negotiate the cybersecurity budget with the senior management • Ensure the organisation's resiliency to cyber incidents • Manage continuous capacity building within the organisation • Review, plan and allocate appropriate cybersecurity resources

Figure 6 NIST:NICE Framework Workforce Categories.



Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

1.2.2 Education on the use of AI for Cybersecurity Analysts.

Both the primary and secondary research in this study identifies the area of Security Operations as a key area where the use of Artificial Intelligence can play a role in automating workloads and performing menial repetitive tasks and ultimately freeing up SOC analysts to perform more high level activities and thus making better use of their time (Palo Also Network, 2024c), potentially giving them more job satisfaction and reducing their levels of "alert fatigue". The benefits of the use of AI in this area include reducing burnout and staff turnover, but also potentially the headcount requirement is lower as more workloads, tasks and roles are handled by AI, with the SOC analyst managing the AI. When the AI capabilities have been aligned with the frameworks as suggested in section 1.2.1 above, the next step will be around education. Educational institutions, certification providers and developers of curricula will need to integrate AI training and education into their education programs so that SOC analysts and other Cybersecurity professionals can learn the skills necessary to manage AI in executing workloads, tasks and jobs and to help them achieve efficiencies. The existing body of knowledge on this area could be further developed by more research into exactly how this can best be achieved.

1.2.3 Education on the use of AI for Cybersecurity hiring managers and Leadership*.*

While there is evidence of the existing use of AI within the field of Cybersecurity (Wheatley, 2020). The finding from the primary research revealed that AI was not identified by hiring managers as a technology that they could leverage as an alternative to hiring more SOC analysts or as part of a hiring strategy when recruiting for Cybersecurity roles or building out Cybersecurity capability. Outside being embedded in products from vendors, the use of AI in the field of Cybersecurity is still in the early stages of development and how to leverage this technology is not widely known. There is a gap between being aware of the existence of the Cybersecurity AI tools, products and solutions and actually understanding how they can be leveraged by Cyber leaders and hiring managers within their Cyber strategies to increase efficiencies in their Security Operations teams. There is an opportunity here to carry out additional research, to understand how best to close this gap and add to the existing body of knowledge.

So education is key here. Cybersecurity leaders and hiring manages need to become educated on the specifics of how to leverage AI. When the capabilities of AI have been aligned with the education and certification programs as highlighted above in section 1.2.1. Cybersecurity leaders and hiring managers will need to skill up on how to leverage AI, and then integrate it into their Cyber capability strategy and hiring strategy to realise the efficiencies that AI promises.

1.3 ACADEMIC JUSTIFICATION*.*

According to Stuart Madnick (2024), there has been a 20% increase in data breaches in the US between 2022 and 2023. Madnick also states that there has been an increased number of ransomware attacks. Madnick also mentions that industry vendors are being increasingly targeted. This presents a risk for the customers of these vendors, as their systems could potentially be compromised via the vendor, or via the vendor’s products. Madnick mentions that in the past 2 years, 98% of organisations have a relationship with a vendor that has suffered a breach.

New Cybersecurity regulations have been introduced in the EU in 2024, specifically the NIS2 Directive, which mandates that all EU member states implement a high level of Cybersecurity to protect their critical infrastructure (European Commission, 2024).

While cyber-attacks have been increasing, and new regulations are being introduced, the shortage in Cybersecurity professionals is growing, in 2023 the ISC2 reported that the global cybersecurity workforce shortage increased by 12% to nearly 4 million workers (ISC2, 2023).

The current body of knowledge discusses the Cybersecurity workforce shortage, it also discusses current attempts to mitigate that shortage, however there is an opportunity to add to the body of knowledge with research into the possibility of AI helping mitigating the workforce shortage in Cybersecurity by automating tasks and roles that are currently carried out manually. If realised, and AI can help mitigate the workforce shortage in Cybersecurity, it can potentially help Cybersecurity teams and organisations react to cyber-attacks more quickly and potentially reduce the impact and losses for both business and society.

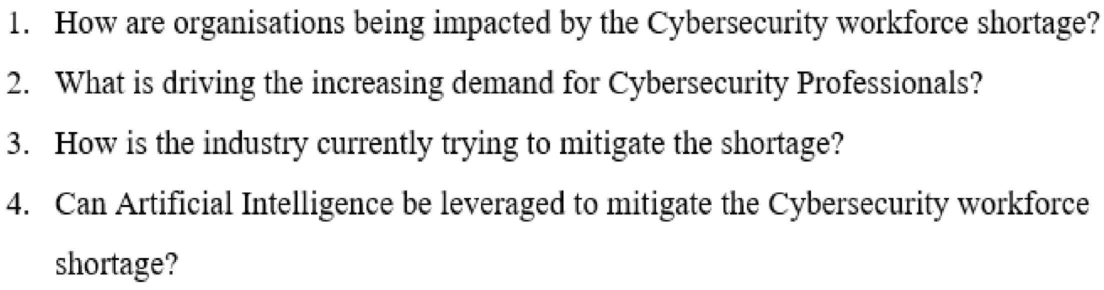
1.4 RESEARCH AIMS.

The research aims for this study are to research the industry literature pertaining to the Global Cybersecurity Workforce Shortage and what effect this shortage is having on organisations. The research further aims to examine industry knowledge around the demand for Cybersecurity professionals, and what’s driving that demand. A further research aim is to understand existing initiatives that have been established to address the Global Cybersecurity Workforce Shortage and finally to provide insight into the potential of Artificial Intelligence to help mitigate the Cybersecurity Workforce Shortage. The ultimate aim of the research is to identify gaps in the existing body of knowledge of the subject, and then to justify further academic research into filling those gaps with the aim of helping organisations mitigate the cybersecurity workforce shortage.

1.5 Research Questions*.*

The research questions shown in Fig. 7. below, serve the purpose of providing direction, focus and scope for the research project. These research questions form the basis of the research objectives, these are highlighted and discussed later in chapter 3. The research objectives form the basis for the Primary Research interview questions.

Figure 7: Research questions derived from Research Objectives.



1. How are organisations being impacted by the Cybersecurity workforce shortage?
2. What is driving the increasing demand for Cybersecurity Professionals?
3. How is the industry currently trying to mitigate the shortage?
4. Can Artificial Intelligence be leveraged to mitigate the Cybersecurity workforce shortage?

1.6 Methods and Scope.

1.6.1 Research methods for the study.

The study of the Cybersecurity workforce shortage and the potential of Artificial Intelligence revealed key issues with both the increasing demand and the inability of the mitigation attempts to produce enough candidates to satisfy demand. The research embarked on a strategy of interviewing ten stakeholders from within the field of Cybersecurity to gather primary data about their experiences, their perspective and their interpretations of the answers to the interview questions and ultimately the research objectives. Due to limitations around sample size for data gathering, and limitations around time, the researcher found that the qualitative research method would be the most appropriate for this study, justification and reasoning behind this decision is discussed in depth in Chapter 3.

The sample parameters included a sample of ten stakeholders from the field of Cybersecurity, a mix of two women and eight men, a mix of experience within the field, five stakeholders with direct experience of hiring for their organisations and five from a vendor background. Three of the interview subjects with less than ten years experience and seven of the interviewees with ten or more years of experience in the field of Cybersecurity.

1.6.2 Scope of the research study.

In-depth interviews have been carried out with ten subjects, the interview subjects fall into two categories, subjects from Cybersecurity vendors, and subjects from organisations that have internal Cybersecurity teams. The interview subjects faced 12 questions that were derived from the 4 objectives listed in Fig. 8. The researcher has sought to gain an objective understanding of the interviewee's knowledge and experience of the Cybersecurity workforce shortage, the interviewee's knowledge and experience of what is driving the demand for Cybersecurity professionals, and the interviewee's knowledge and experience of the current initiatives to mitigate the shortage, and the interviewee's knowledge and experience of Artificial Intelligence and how it could be used to help mitigate the shortage.

Due to limitations in terms of time and access, the scope of this research paper is primarily focused on the Cybersecurity workforce shortage, and the potential for AI to help mitigate that shortage. The scope of this study is confined to the experiences and perspectives of stakeholders within the field of Cybersecurity, their knowledge of the shortage, the existing mitigation efforts and their knowledge of AI. AI experts outside the field of Cybersecurity were not included due to time and access restraints, perhaps further research could be undertaken in this area which included specific AI experts.

1.7 Overview of the research structure.

1.7.1 Chapter 1: Introduction to the research area and Thesis.

Chapter 1 introduces the area of research, the global cybersecurity workforce shortage and the potential of Artificial Intelligence to help mitigate the shortage. This chapter also introduces the research aims and objectives, methodology, the scope of the research study.

1.7.2 Chapter 2: Literature review.

Chapter 2 is made up of an in-depth review of the existing academic literature and body of knowledge relating to the research topic. The existing literature relating to the global Cybersecurity workforce shortage, what is driving the increasing demand, what current efforts are being made and by who, to mitigate the shortage, and the literature on Artificial Intelligence, and it's use within the field of Cybersecurity is reviewed. Also the gaps in this body of knowledge for all of these areas are identified and critically discussed.

1.7.3 Chapter 3: Methodology.

Chapter 3 of the research study is concerned with the research methodology that was used for the study. The research aims and objectives, the research philosophy, approach and strategy, the data collection methods used, the population sample, the data analysis techniques, the ethical considerations and the limitations of the research.

1.7.4 Chapter 4: Findings and Discussion.

Chapter 4 of this study is concerned with the findings and discussion relating to the primary research. A thematic approach is used to analyse the data gathered to reveal the themes, patterns and nuances that provide insight into the research theme of "the global Cybersecurity workforce and the potential of Artificial Intelligence". The insights are further critically discussed, gaps identified and unexpected results explored and references are made back to the literature reviewed in chapter 2.

1.7.5 Chapter 5: Conclusions and Recommendations.

Chapter 5 of the research study draws conclusions from the data gathered from the primary and secondary data, and the findings and insights that have been revealed. The research gaps that have been discovered are put forward for additional research, and recommendations are made for all stakeholders in the field, with the aim of mitigating the Cybersecurity workforce shortage, and helping organisations and governments protect their assets from Cyber criminals more effectively.

CHAPTER 2:

LITERATURE REVIEW.

2.1 INTRODUCTION.

The following chapter will explore the existing body of work that describes the current workforce shortage within the field of Cybersecurity and the potential for Artificial Intelligence to help alleviate that workforce shortage. Initially the literature that describes the field of Cybersecurity and the role of Cybersecurity will be examined and critiqued. Next the literature describing the reasons for the increasing demand for Cybersecurity professionals is explored from the perspective of various academics and professional and governmental bodies within the Cybersecurity sector. The literature describing the threat landscape pre-covid, mid-covid and post-covid is then explored and discussed. Following that, the literature on the workforce shortage that exists within the field of Cybersecurity is examined and critiqued, again from the perspective of academics, professional bodies and governmental agencies. Next specific roles within the field of Cybersecurity where workforce shortages exist are then described, again from the perspective of the various academics, professional bodies and governmental agencies. Then the literature that describes the current approaches to filling those Cybersecurity skills shortages is explored, and the researcher highlights the gaps that exist in this area of the existing literature. The professional bodies and governmental agencies mentioned above include the European Union Agency for Cybersecurity (ENISA), the National Institute of Standards and Technologies (NIST) in the USA, and the International Information System Security Certifications Consortium (ISC2) for a global perspective, with literature from other academics also reviewed.

2.1 WHAT IS CYBERSECURITY AND WHAT IS ITS FUNCTION.

Cybersecurity can be described as the act of protecting the systems, services and devices that are used by organisations and individuals (NSC, 2024). The goal of Cybersecurity is to protect the Confidentiality, Integrity and Availability of these systems, services and devices, meaning that when an individual or an organisation is using them they can do so in a confidential manner, also that the integrity of the data they are accessing is intact, IE: It has not been altered or changed in anyway, also the systems and services that the individuals or organisations are accessing are available and have not had their availability affected by malicious attacks (Nieles et al., 2017).

2.2 THE INCREASING DEMAND FOR CYBERSECURITY PROFESSIONALS.

2.2.1 The Increasing Demand for Cybersecurity Professionals, Pre-Covid, Mid-Covid, Post Covid.

In the pre-Covid world organisations and governments faced increased Cyber threats due to the growth in ecommerce, where more and more consumer transactions were moving online and away from traditional consumer store transactions, this growth of the digital economy created an increasing demand for Cybersecurity professionals, as society became more digitised and reliant on IT systems (Teoh & Mahmood, 2017).

Tiberiu-Marian Georgescu (2021) argues that during the Covid-19 pandemic organisations and governments were forced to change their working practices due to global lockdowns, restricted movement and social distancing rules. These new working practices introduced remote working, put pressure on supply-chains and saw the spread of misinformation through social media networks. This new working landscape was then targeted by cyber criminals for both financial gains and to spread misinformation. Tiberiu-Merian mentions that during Covid-19 there was an increase in Ransomware attacks, where cyber criminals gain access to a system, encrypt files then demand payment of a ransom to un-encrypt the files. An increase in Phishing, where cyber criminals target specific employees within organisations with malicious emails and try and get them to divulge financial information or make bogus payments. Another attack mentioned was data exfiltration, where cyber criminals seek to compromise an organisations systems and steal intellectual property or financial information. As described by Tiberiu-Marian the Cybersecurity landscape was severely impacted by the Covid-19 pandemic, all of the new work practices and attacks put additional pressure on the already undersupplied Cybersecurity workforce, thus increasing demand for Cybersecurity professionals even further that in pre-Covid times.

In the post-Covid landscape demand for Cybersecurity professionals continues to increase, it was projected that the global spend on Cybersecurity including risk management would increase by 11.3% (Gartner, 2022). The remote work practices that were introduced during the Covid pandemic have largely stayed, with some element of Hybrid working being offered by most employers. A shift towards Zero-Trust network access and Cloud has increased the demand for Cybersecurity professionals with these skill sets, while Cloud attacks were reported to had increased by 95% in 2021 (CrowdStrike, 2022).

2.2.2 The increasing demand for Cybersecurity Professionals as described by the European Union Agency for Cybersecurity.

The European Union Agency for Cybersecurity (ENISA) was initially setup in 2004, it is a EU agency that has the remit of preparing Europe for the Cybersecurity landscape of tomorrow, the ENISA contributes to EU wide Cybersecurity policy and helps EU nations prepare for the Cybersecurity challenges of the future (ENISA, 2024a).

As reliance on digital systems and services in a more interconnected world increases so does the potential for Cyber Criminals to intercept, alter or take down those systems and services for financial gain or to disrupt organisations or governments. Globally the Cyber landscape has become more dangerous since the Covid-19 pandemic where cyber criminals have sought to take advantage of the new environment individuals and organisations have found themselves in. Some of these Cyber-attacks since the outbreak of Covid-19 included email campaigns from Cyber criminals purporting as being from the World Health Organisation (WHO) seeking to trick individuals into downloading malware that could be used to compromise their systems, Cyber-attacks on health infrastructure such as the Czech hospital system, the UK National Health Service and fake information websites that direct individuals to malicious websites that steal their payment credentials (Lallie et al., 2021).

The onset of the Covid-19 pandemic forced individuals, organisations and learning institutions into new working patterns and practices. For example the need to implement lockdowns, travel bans, social distancing and quarantines caused organisations to roll out solutions like remote working and remote learning where employees and students typically connected into the systems and services that they needed for their work remotely, from their homes. This has meant that organisations have had to invest in the technology needed to facilitate remote working, like Software as a Service (SaaS) applications which are available over the internet, and Virtual Private Network connectivity that enables remote workers to connect securely into the organisation. The ENISA Threat Landscape Report (Ardagna et al., 2021) reflects the new threat landscape where cyber criminals are seeking to exploit this new working environment, with an increase in Ransomware attacks where cyber criminals will send a malicious email to an unsuspecting user, the user opens the email and attachment, which subsequently can encrypt both the users own PC and potentially any systems on their network, the cyber criminals will then demand a payment to un-encrypt the files. The Covid-19 pandemic period from 2020 to 2021 saw various types of threat actors try and leverage the pandemic to commit Cyber-crime. The 2021 ENISA Threat Landscape Report categorised four main types, State-sponsored, Cyber criminals, hackers for hire and hacktivists. State-sponsored, Cyber criminals and hackers for hire were seeking to make financial gains through the various means mentioned above, to also create confusion amongst the populations of other nations states, and to spread misinformation to disrupt government efforts to contain and limit the damage of the Virus (EURESCOM, 2024).

The increased level of threats facing governments and organisations has increased the strain on existing Cybersecurity teams who have been trying to protect their organisations from exploitation from the various threat actors. Hence the demand for Cybersecurity professionals has increased, in 2021 Europe in general saw an increase of 22% and some countries, namely Romania, Poland and Germany has seen an increase in demand of over 30% (Misheva, 2023).

2.2.3 The increasing demand for Cybersecurity Professionals as described by the National Institute for Standards and Technologies.

The National Institute for Standards and Technology (NIST) is a US governmental agency that is part of the US Department of commerce. In the area of Cybersecurity, it produces guidelines, frameworks and standards that it publishes for Cybersecurity professionals to adopt, follow and comply with. For the June 2023 Cybersecurity Workforce Demand communication, NIST compiled data from various reputable sources that it then presented. A key finding was that the expected increase in demand for Information Security Analysts would be in the region of 35%. (NIST, 2023).

In a post Covid-19 world, with increased digitisation and an ever more connected workforce, securing manufacturing operations is becoming a more complex and challenging task, creating more demand for Cybersecurity professionals (Toth, 2022). The Manufacturing landscape has also changed from a time where manufacturing systems were not connected to IT systems and had no access to the internet, or remote maintenance. Now manufacturing equipment includes connectivity to traditional IT systems, which brings all of the threats associated with that environment and can cause production outages or ransomware attacks. Operational Technology (OT) which includes Industrial Control Systems (ICS), Programable Logic Controllers (PLCs) and Internet of Things devices now have a need for not only connectivity to other IT Systems, but also the Public internet and to be remotely accessible by third party suppliers that provide maintenance, remote monitoring and remote upgrades. Manufacturing systems use customised software, which brings the challenging of introducing security patches to fix the vulnerabilities in the software. As it is customised it is often not patchable by traditional patch releases from the suppliers. Due to this increased connectivity, and customisation these systems are now more susceptible to attack than ever before. Securing these Manufacturing systems creates additional demand for Cybersecurity Professionals.

2.2.4 The increasing demand for Cybersecurity Professionals as highlighted by the International Information System Security Certification Consortium.

The International Information System Security Certification Consortium (ISC2) are a leading Global organisation for Cybersecurity Professionals that was setup in 1989, they offer training and certification in some of the industry's most respected Cybersecurity certifications. The ISC2 also produce an annual Cybersecurity workforce study that highlights opportunities and challenges within the field of Cybersecurity (ISC2, 2024a).

In the US, the decade from 2014 and 2024 has seen an 18% growth in demand of Cybersecurity professionals as reported by the US Bureau of Labour Statistics, however the 2015 ISC2 Global Information Security Workforce study that is compiled and published by the ISC2 displayed that just 10% of the Cybersecurity workforce were Women, and by 2021 the number had improved somewhat to represent 24% of the Cybersecurity workforce (Lingleback, 2023).

Disruption of critical infrastructure, compromised sensitive data and US city governments impacted by cyber-attacks as described by Dom DiFurio's (2023a) article for Drata a Security and Compliance company. These incidents serve as an example of the need for Cybersecurity professionals to protect organisations and governments. DiFurio's article argues that demand in the US for Cybersecurity experts has grown twice as fast as the Cybersecurity workforce has grown, with a demand growing by 9% between 2021 and 2022, while the number of Cybersecurity jobs grew by just 5.5% (DiFurio, 2023b).

The war in Ukraine and increasing global geopolitical tensions have pushed up the demand for Cybersecurity professionals Year on year even further. Even though between the years 2022 and 2023 the number of Cybersecurity professionals increased by 12% globally (Meineke, 2024).

2.3 THE WORKFORCE SHORTAGE THAT EXISTS WITHIN THE FIELD OF CYBERSECURITY.

2.3.1 The Workforce Shortage that exists within the Field of Cybersecurity in Europe and as highlighted by the ENISA.

New legal requirements mandated by the European Union in directive 2023/2841 have called for a minimum level of cybersecurity to be implemented by EU member states (EUR-Lex, 2023). This new EU directive has increased the demand for Cybersecurity professionals in Europe even further, with the European wide Cybersecurity professionals shortage estimated to be around 300,000 in 2022 (ENISA, 2023).

In 2020, the UK Govt Department for Digital, Culture, Media & Sport (DCMS) had a report commissioned investigating the UK Cybersecurity Labour Market. Part of that study involved looking at the workforce shortage within the field of Cybersecurity. The study findings showed that 68% of the businesses that were canvassed had tried to recruit Cybersecurity staff in the preceding three years, of this 68%, 35% of these businesses reported difficulty in filling their advertised positions. With approximately 48% or 653 thousand businesses reporting Basic Cybersecurity Skills Gaps in their workforce, 30% or 408 thousand businesses reporting Advanced Cybersecurity Skills Gaps in their workforce (Pedley et al., 2020).

As argued by Borka Jerman Blazic (2021), the European Cybersecurity labour shortage has had an impact on the readiness of European businesses to comply with the European Union's General Data Protection Regulation (GDPR) that was published in 2018, as a shortage in Cybersecurity professionals in the area of Data Security meant businesses didn't have the expertise to make necessary changes to comply with the new regulations, Blazic estimated this figure at 60% or European businesses.

2.3.2 The Workforce Shortage that exists within the Field of Cybersecurity as highlighted by NIST.

NIST compiled data from various reputable sources, then published the June 2023 Cybersecurity Workforce Demand communication. This communication highlighted some of the challenges facing both US Government agencies and US Private industry in terms of the Cybersecurity workforce shortage within a US context. For example, One of the key findings was that in June 2023 in the US, there were an estimated 663,434 Cybersecurity unfilled job openings, with an estimated 1,129,659 people in the US employed in the field of Cybersecurity. Another key finding was that leadership teams specified that key skills that are needed included Cloud Security, Cyber intelligence and Malware analysis candidates. NIST also quoted that it was expected that by 2025, more than half of serious Cybersecurity incidents would be as a result of human failure, or a lack of talent (NIST, 2023b).

In August 2022 the US government signed into law the Cybersecurity Workforce Data Initiative (CWDI). The purpose of this initiative was to have the US National Center for Science and Engineering Statistics (NCSES) work with other governmental agencies including NIST to produce data around the US Cybersecurity workforce. The four key phases for this project included Scanning the existing definitions and data, Organising stakeholder interviews and workshops, preparing research questions for the survey and conducting a pilot study (NSF, 2024). To produce estimates for the current size of the US Cybersecurity workforce, the CWDI pulled data from numerous sources, as the definition of Cybersecurity worker can vary, the CWDI created two ranges for the estimates. A lower range with strict definitions of Cybersecurity workers and a broader definition of Cybersecurity workers that included workers that had some element of Cybersecurity in their role, but not a Cybersecurity job title. The Stricter definition limited the category to workers with the title of "Information Security Analyst" or "Computer and Information Systems Security. The wider definition included all workers that had an Cybersecurity element to their role, without a specific Cybersecurity job title. The estimates for the existing numbers of US Cybersecurity workers were returned as follows, the low estimate was 164,000 workers and the high estimate was 3,567,000 Cybersecurity workers currently working within the Cybersecurity field. To represent the demand for Cybersecurity Professionals, the CWDI claimed there were an estimated 570,000 Cybersecurity jobs available in the US for 2023 (Hogan et al., 2024).

2.3.3 The Workforce Shortage that exists within the Field of Cybersecurity as highlighted by the ISC2.

The 2020 ISC2 Workforce study presented findings that highlight the shortage that existed in the field of Cybersecurity for that year, the workforce study is a global study that incorporates fourteen countries over four regions globally, North America (NA), Europe Middle East and Africa (EMEA), Latin America (LATAM), and Asia Pacific (APAC). The 2020 study was conducted in the middle of the Covid-19 global pandemic. The study consisted of approximately 3,700 participants from the field of Cybersecurity. In total the worldwide shortage was estimated at 3.1 million Cybersecurity workers (ISC2, 2020).

The 2021 ISC2 Workforce study was compiled from data from a pool of approximately 4700 participants from the field of Cybersecurity. 2021 saw an increase in the number of workers working in the field of Cybersecurity globally by approximately 700,000 new workers, bringing the global number of Cybersecurity Professionals to approximately 4.2 million. This increase in the number of Cybersecurity professionals helped reduced the Cybersecurity shortage from the 2020 figure of 3.1 million, however the shortage of workers for the Cybersecurity field still stood at approximately 2.72 million workers globally (ISC2, 2021).

The 2022 ISC2 workforce study saw the number of Cybersecurity practitioners and decision makers surveyed increase to approximately 11,700 participants globally. The data from the 2022 report stated that the global Cybersecurity workforce stood at approximately 4.7 million globally. Again the survey was conducted in 14 countries across 4 regions globally, North America, Latin America, Europe Middle east and Africa and Asia Pacific. This 4.7 million figure represented an increase of 11.1% or approximately 460,000 jobs on the 2021 Cybersecurity workforce figures. However a global increase in demand saw the global Cybersecurity workforce shortage estimate grow to 3.4 million Cybersecurity Professionals needed (ISC2, 2022).

The 2023 ISC2 workforce study showed an increase in the global Cybersecurity workforce to an estimated 5.5 million Cybersecurity Professionals, an increase of 9% on the 2022 workforce numbers. However in 2023 the demand for Cybersecurity professionals grew again, with the 2023 Cybersecurity workforce shortage reported at approximately 4 million, a 13% increase in the shortage from the 2022 figures (ISC2, 2023). Some of the driver of this increased demand include the War in Ukraine, an increase in the work from home/work from anywhere company policy and an increasing reliance of Cloud based services as stated in the 2023 report.

2.4 CYBERSECURITY FRAMEWORKS THAT DEFINE CYBERSECURITY ROLES WHERE THE SHORTAGES EXIST.

2.4.1 Cybersecurity Roles defined in The European Cybersecurity Skills Framework: ECSF.

The European Cybersecurity Skills Framework (ECSF) was first presented in September 2022, at the Cybersecurity Skills conference (ECSO 2022). Developed by the ENISA, The ECSF is an initiative that was designed to standardise and enhance Cybersecurity Roles, tasks, skills and Competencies across Europe (ENISA, 2022a). The ECSF has five goals, One Goal is to agree on a shared understanding of common terminology across Europe, so that defining roles for Recruitment, job specifications and qualifications is uniform across Europe. This helps hiring managers and HR professionals use a common framework when they are hiring for

Cybersecurity professionals across Europe. Another goal is to provide a reference framework that helps educational institutions and training providers create programs that meet industry standards, ensuring that students and trainees acquire the necessary skills to be employable in the Cybersecurity sector and help mitigate the Cybersecurity skills shortage. A third goal is to help recruiters and HR departments use the framework to craft precise job descriptions, recruitment criteria and career development pathways. A fourth goal is to establish a common framework and understanding for Cybersecurity roles, skills, standards and practices and enable mutual recognition of qualifications and certifications across Europe. The fifth goal of the ECSF framework is to help organisations and government agencies perform workforce capacity planning to upskill employees with the skills needed to perform the relevant Cybersecurity roles (ENISA, 2024b).

The ECSF provides a framework that separates Cybersecurity roles into twelve profiles. Each of these profiles then lists the responsibilities, skills, knowledge and training that is relevant to each of the profiles. These twelve profiles include Chief Information Security Officer, Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Managers, Digital Forensics Investigator, Penetration Tester (ENISA, 2022b).

2.4.2 Cybersecurity Roles defined in The National Initiative for Cybersecurity Education Framework: NICE Workforce Framework.

In November 2020 the US National Institute for Standards and Technology (NIST) published Revision 1 of the Workforce Framework for Cybersecurity (NICE Framework) under the NIST Special Publication 800-181 (Petersen, et al., 2020). The NICE Framework was developed to standardise common Cybersecurity tasks, knowledge and skills so that businesses, Governmental bodies and academia could use a common framework when creating and defining Cybersecurity roles, creating training and educational content and defining competencies (CISA, 2024a). The Revision 1 release of the NICE Framework was an upgrade on the original version that was released in 2017. Since 2017 the Cybersecurity landscape had changed significantly and a revised framework was needed to satisfy the needs of different stakeholders across organisations and governmental bodies (Santos, 2020). In order to be more dynamic and introduce flexibility, the Revision 1 release created a separate Components document that can be updated separately from the Nice Framework Revision 1 document, the NICE Framework Components v1.0.0 was released in March 2024 (NIST, 2024). The Components v1.0.0 document lists 7 Work Categories which include Oversight & Governance, Design & Development, Implementation & Operation, Protection & Defence, Investigation, Cyberspace Intelligence and Cyberspace Effects. These 7 Work Categories contain 52 Work Roles. These Work Categories and Roles are accompanied by over 2,200 defined Tasks, Knowledge and Skills, and 11 defined Competency Areas which make up the NICE Framework (NIST, 2024b).

2.4.3 The literature gap that exists in the ECSF and NICE frameworks.

The ever increasing demand for Cybersecurity professionals would suggest that broadening the scope of the current mitigation efforts beyond the areas of education and certification in order to bring more Cybersecurity professionals into the field is warranted. The researcher believes there is an academic research opportunity to research further how AI can be leveraged to help mitigate the Cybersecurity workforce shortage, specifically in relation to the existing ECSF and NICE frameworks which already list Cyber tasks and roles. By aligning AI capabilities and tools with the existing frameworks, that would help educational institutions, and AI researchers and developers develop curricula, tools and products that can be leveraged by organisations to supplement existing Cyber workers by automating some of their workloads and thus introducing more efficiencies for Cyber professionals.

2.5 EDUCATION & TRAINING APPROACHES TO FILLING THE CYBERSECURITY WORKFORCE SHORTAGE.

There are various governmental agencies and organisational bodies that are engaged in trying to fill the Cybersecurity shortage. From a standardisation perspective, the ECSF and NICE Frameworks have offered these organisations a framework to help them to produce educational content, training, certifications and define the job roles that are needed to tackle the Cybersecurity Workforce Shortage. From a technical perspective Cybersecurity vendors have already integrated AI into their products, and in some cases developed products and solutions that fulfil some of the activities and job functions that would have traditionally been performed by a human, thus reducing the burden on already overstretched Cybersecurity teams.

2.5.1 Current approaches to filling the Cybersecurity workforce shortage in Europe and the ENISA.

The ENISA launched the Cybersecurity Skills Academy in 2023 to combat the Europe wide Cybersecurity workforce shortage. The ECSF Framework forms the foundation of the Cybersecurity Skills Academy, meaning all of the educational and training material in the Cybersecurity Skills Academy is based off roles, skills and competencies that are defined in the ECSF (Polemi and Kioskli, 2023). The Cybersecurity Skills Academy is based on four areas of activities, Knowledge Generation & Training, this is where citizens and educational institutions can access information on Cybersecurity courses and training, campuses and academies. Funding and Projects is the second activity the Cybersecurity Skills Academy is focused on, where citizens and learning institutions can find information on funding opportunities for Cybersecurity skills and projects. Stakeholder Involvement, Pledges & Strategies is the third activity that the Cybersecurity Skills Academy is focused on, this is where stakeholders are encouraged to make pledges and contribute to strategies in an effort to close the Cybersecurity shortage. Measuring Progress is the fourth activity, this is where the Cyber Skills Academy will make available data indicating progress in upskilling and learning programs that are contributing reducing the shortages in certain Cybersecurity areas (EU, 2024).

2.5.2 Current approaches to filling the Cybersecurity workforce shortage in the US.

In the US, the Cybersecurity & Infrastructure Security Agency (CISA) is a US governmental body that acts as a national coordinator for Industry, small and medium businesses, educational institutions and government bodies. It publishes information about current cyber threats, vulnerabilities in systems, and publishes advisories to help secure businesses and organisations (CISA, 2024b). The National Initiative for Cybersecurity Careers and Studies (NICCS) is an initiative within the CISA, the remit of the NICCS is to be a central source of information about available educational content, career resources and training. It provides resources for the general public, Cybersecurity Professionals and Managers, Educators, College and University students, all level of government and HR managers. The NICCS have dedicated resources for Education and Training, Workforce Development and Cybersecurity Careers (CISA, 2024c). The NICSS education, training, workforce development and career resources are underpinned by the NICE Framework. In addition to the NICSS, the CISA runs a Cybersecurity Education and Training Assistance Program (CETAP), for the past 14 years the CISA has worked with the Cyber.org which is an education and training organisation that has the primary goal of providing resources to educators who cater for the K-12 category of students, IE; Kindergarten to Year 12 students (Cyber.org, 2024). Cyber.org receives funding from CISA, in 2023 they received $6.8m as CETAP recipients (CISA, 2024d). Agencies such as the CISA and dedicated initiatives such as the NICCS have been established to increase Cybersecurity awareness and to provide the educational resources that are needed to combat the Cybersecurity Workforce shortage.

2.5.4 Current approaches to filling the Cybersecurity workforce shortage in the United Kingdom.

The UK Cyber Security Council have been established to support the UK Governments National Cyber Strategy. Their remit is to expand the UK's Cybersecurity knowledge and skills at all levels. In order to achieve this goal, they have developed a career framework that educates on the paths into a career in Cybersecurity. They have mapped and developed the qualifications and certifications that are relevant to each of the Cybersecurity roles across the Cyber industry (UK Cyber Security Council, 2024a). In its efforts to combat the Cybersecurity workforce shortage, the UK Cyber Security Council have established resources that provide guidance and direction to anyone that is interested in a career in Cybersecurity, they explain entry routes into a career in Cybersecurity via training resources and also resources and information on qualifications and a framework that helps map out the training, education and certifications necessary to follow a path to any of the specific careers in Cybersecurity (UK Cyber Security Council, 2024b).

2.5.4 Current approaches to filling the Cybersecurity workforce shortage Globally and ISC2.

The ISC2 offer a myriad of education options, trainings and certifications within the field of Cybersecurity. Regarding the ISC2 Certification Framework Mapping, it maps to various global Cybersecurity Frameworks including the ECSF (ISC2, 2024b).

Knapp, Maurer & Plachkinova (2017) argue that due to the dynamic nature of the everchanging Cybersecurity landscape higher education can struggle to keep their curricula up to date. However due to a more flexible structure, professional Cybersecurity certifications that are designed to specific competencies and tasks and which can be updated more frequently than a College/University curricula can offer both students and employers a closer representation of the skillset of a candidate and a definition of a job specification. The ISC2 is one of the most respected member associations for Cybersecurity Professionals, with over 650,000 members globally (ISC2, 2024c). ISC2 boast some of the industry's most respected and renowned Cybersecurity Certifications, the Certified Information Systems Security Professional (CISSP) is considered throughout the Cybersecurity industry as one of the most valuable certifications, frequently polling in the top 10 list of Cybersecurity certifications (Seiter, 2024). Tommi Äijälä (2018) argues that from a employees perspective, the CISSP certificate offers an industry trusted certification that will display the candidates Cybersecurity knowledge and skillset, while from a recruiter or employer perspective the CISSP certification offers them a level of trust in understanding a candidates knowledge, skillset and level of proficiency within the field of Cybersecurity. By providing certifications such as the CISSP and other industry leading Cybersecurity certifications and training, the ISC2 organisation is helping the Cybersecurity industry develop talent, knowledge and ultimately Cybersecurity professionals that will contribute to closing the workforce shortage within the field of Cybersecurity.

2.6 CYBERSECURITY VENDOR TOOLS AND THEIR USE OF ARTIFICIAL INTELLIGENCE.

The Cyber firm Sophos (2024) describe Artificial Intelligence (AI) in Cybersecurity as a tool that can process vast amounts of data and recognise patterns of behaviour and respond to threats in real time. Machine Learning has been described by Sara Brown (2024) of the Massachusetts Institute of Technology (MIT) as a subfield of Artificial Intelligence that can be used to imitate human behaviour in order to solve difficult problems in the same way a human would.

2.6.1 The Structure of Cybersecurity Teams and their tasks.

The twelve job profiles that are listed within the ECSF are a list of the roles that are defined to help organisations understand how to structure their Cybersecurity teams. Typically within an organisation the top Cybersecurity role is that of Chief Information Security Officer or CISO, The CISO is responsible for among other things building the team needed to carry out the tasks required to secure the organisation and counter any Cyber threats (Menzola and Nunes, 2019). One key function within the wider Cybersecurity team is that of the Security Operations Center or SOC. As described by Arif Ali Mughal (2022), the SOC is the central hub of an organisations Security Operations, the SOC are responsible for both detecting and then responding to any Cybersecurity incidents that arise affecting the organisation, the SOC is staffed by Cybersecurity professionals, typically called SOC Analysts. The SOC Analysts monitor the organisations IT environment for malicious activity. Depending on an organisations size and complexity, a SOC can range from one SOC Analyst for a small organisation up to one hundred SOC Analysts for a large organisation (InfoSecInstitute, 2024). As described by Palo Alto Networks (2024a), there are many levels to the role of SOC Analyst, they are typically described as tiers, each tier will typically focus on certain functions. Tier 1 which is entry level Analyst will typically be responsible for Triage, which involves monitoring the IT environment for malicious activity, this includes monitoring and analysing Network traffic and logs from devices and also for initial response and containment efforts for any incidents and for corelating information and escalating to higher Tier Analysts within the SOC for further investigation. Tier 2 SOC Analysts are typically engaged with Security Incident Investigation, determining the source of the incident and for compiling post-incident reports and remediation recommendations. Tier 3 SOC Analysts is the top tier of SOC Analysts and they are typically engaged in proactively searching for malicious threats and weakness within the organisations security posture. Tier 3 SOC analysts will also carry out forensic level analysis of logs, network traffic and engage in incident response, and compile threat Intelligence report on the environment and provide recommendations for securing the environment further.

2.6.2 The Cybersecurity Tools used by the SOC teams.

The tools that are typically used throughout the SOC would include a Security Information and Event Management (SIEM) tool, this is a tool that is used to gather and analyse events and logs from various security tools to collate them in a central location and learn about the behaviour of various systems on the network, the SIEM tool can also take action if it discovers malicious activity by integrating into other tools such as firewalls to block threats (Podzins and Romanovs, 2019).

Network Intrusion Detection Systems (NIDS), is a security tool that analyses traffic on the network and attempts to identify malicious behaviour, The traffic doesn't have to pass through the NDIS system, the traffic can be sent to it so that it can analyse the behaviour of the systems on the network for malicious activity (Uppal et al., 2014). The NIDS can be used to produce reports that administrators can either look at later, or examine live to try and identify malicious activity on the network. The NDIS cannot however block any traffic or isolate any hosts that are deemed to be behaving in a malicious way.

Network Intrusion Prevention Systems (NIPS) are similar to NDIS systems, as they can be used to analyse network traffic for malicious behaviour or infected systems, the difference however is that the NIPS system can take action to neutralise the threat, it can work with other network devices such as Firewalls to block systems that are acting in a malicious fashion (Goncalves, D.G.V. et al,. 2019).

Another tool that can be used by SOC teams is known as a Security Orchestration, Automation and Response (SOAR). A SOAR tool typically combines three elements, Orchestration where the SOAR tool works with both internal and external tools to collate data and intelligence. Automation, where the SOAR tool will trigger tasks that can react to specific threats, the SOAR tool will perform the actions set out in a playbook when a certain rule is triggered by the identification of a threat. The third element is incident Response, this is where the SOAR tool will act to mitigate or block the threat by instructing other devices like Firewalls or NIPS devices to block the threat (Microsoft, 2024).

Security Analytics Platforms are tools that are considered the next generation of SIEM tools, they collect large amounts of data and logs from a myriad of sources and can trigger alerts for incident response, analysis and investigation (Palo Alto Networks, 2024b). SOC teams also use Endpoint Protection and Response (EDR) tools to help them both mitigate and react to security incidents, EDR tools are installed on systems such as Workstations, Tablets, Laptops, Desktops and Servers and their role is to protect the endpoint device and integrate into other tools to provide threat intelligence data and protect both the device and the wider infrastructure (Chandel et al., 2019).

Extended Detection and Response (XDR) is a tool that integrates into Security tools from multiple vendors, it gathers and inspects data from multiple systems including endpoints, servers, email, networks and cloud workloads, XDR then offers insights and context into threats that are seen within the environment (Cisco, 2024).

2.6.3 How Cybersecurity Vendors use AI within their existing tools.

Some of the biggest challenges Cybersecurity teams face when protecting organisations include correlating and analysing the vast amounts of data they receive from the numerous Cybersecurity tools that they utilize within their environments (Sarker et al., 2020). Sandra Wheatley in her article for Fortinet (2020) argues that organisations can often take months to detect a network breach due to the Cybersecurity team being overwhelmed by the challenge of correlating and analysing large amounts of data from their various Cybersecurity tools. Wheatley argues that AI and ML can be used to essentially build a Virtual Security Analyst that can assist with behavioural analytics, zero day threat detection and with responding to identified threats.

Within the vendor ecosystem of Cybersecurity products and tools, the various vendors have in recent years been seeking to leverage AI and ML to perform tasks and roles to help Cybersecurity professionals with their duties. One such vendor is Palo Alto Networks who are an industry leading Cybersecurity vendor and they leverage the use of AI and ML in their product suite to help Cybersecurity teams detect and mitigate Cyber-attacks. Some of the products and platforms where they use AI and ML include Cortex, Strata and Prisma Cloud. Cortex is a platform for Cybersecurity operations, in its press release "Palo Alto Networks Adds "Bring Your Own AI" Capability To Cortex XSIAM AI-driven Security Operations Platform" (2023). Palo Alto Networks describe the Cortex Security Operations Platform as a Security Operations Center, it collects and correlates data, performs behavioural analysis to detect and prevent threats. It then uses AI to analyse and detect anomalies and incidents which improves the speed and accuracy of the threat detection, this tool directly assists SOC Tier 1 and 2 Analysts with their tasks.

Palo Alto's Strata, Prisma and Cortex platforms all make use of AI through a "Copilot" for each of the solutions, these Copilots are chatbots that are available to Cybersecurity professionals, they allow them to enter plain English text and query the solution on existing threats and help them mitigate these threats and protect the environment (Palo Alto Networks, 2024c). These Copilot chatbots could be useful for Tier 1 and Tier 2 SOC analysts in identifying and mitigating threats found on the network. The underpinning AI technology that Palo Alto has developed to integrate and support each of its products is called "Precision AI", this solution offers protection against advanced threats and facilitates safe AI adoption by protecting users that are using AI solutions such as ChatGPT, these AI solutions assist Cybersecurity Professionals that are using the Palo Alto Product suit as they carry out Tier 1 & 2 SOC tasks by gathering vast amounts of data, analysing it and mitigating attacks (Palo Alto Networks, 2024d).

2.6.4 Literature GAP, education on the use of AI for Cybersecurity analysts.

The education and training approaches to mitigating the Cybersecurity workforce shortage discussed above are having limited success in mitigating the workforce shortage, as can be seen with the ever rising shortage of Cybersecurity workers. When AI capabilities have been aligned with the frameworks as suggested in section 2.4.3, the next step in mitigating the shortage will be for educational institutions, certification providers and developers of curricula to integrate the AI training material into their education programs and certifications so that SOC analysts and other Cybersecurity professionals can learn the skills necessary to manage AI in executing workloads, tasks and jobs, to help them achieve efficiencies. The existing body of knowledge has a gap in relation to how to develop the training modules for integrating AI into Cybersecurity and this represents an opportunity to justify further research in the area.

2.6.5 Literature GAP, education on the use of AI for Cybersecurity hiring managers and leadership.

A literature gap exists in the area of education and training for hiring managers and Cybersecurity leaders, in the capabilities of AI in the field of Cybersecurity. The existing literature does not display hiring managers or Cybersecurity leaders considering AI as a technology that they could leverage as an alternative to hiring more SOC analysts or as part of their hiring plans or capability strategy. Outside being embedded in the products from Cybersecurity vendors, AI in the field of Cybersecurity is still in the early stages of development, and how to leverage this technology is not widely known. There represents an academic research opportunity, to carry out additional research into educating and training Cyber hiring managers and leadership in how they can leverage AI within their hiring plans and capabilities strategies.

CHAPTER 3

RESEARCH DESIGN, PROCESS AND METHODOLOGY.

3.1 INTRODUCTION.

The research process can be described in many ways. In the book “How to research,” Blaxter, Hughes and Tight (2010) describe research as the process of choosing a topic, deciding on methods, reading for research, collecting data, analysing that data, then producing a report that adds to the existing body of knowledge on the subject. The methodology section of a thesis has the aim of conveying the philosophy, approach and the strategy that has been determined to guide the primary research for the thesis. The methodology section of a thesis is key to establishing the reliability of the research. Blair (2016) argues that a well-structured methodology section enhances the credibility of the research by detailing the systematic approach taken to address the research questions. It also addresses the potential limitations of the rejected methodologies and philosophies and offers a comprehensive understanding of the study's scope and context.

The methodology section explains the foundation for the research by detailing the procedures, sampling techniques, data collection methods and analytical strategies that have been employed to collect and analyse the feedback from the primary research interviewees. The methodology section details the research design, which is based on the research aims and objectives. It then discusses the research philosophy and the relevant philosophy chosen to provide a balanced unbiased method of collecting and interpreting the data, but also why other philosophies, strategies and approaches are rejected. By documenting each step of the process, the methodology section seeks to uphold the academic rigor and contribute valuable insights to the existing body of knowledge (Kumar, 2011).

3.2 RESEARCH AIMS AND OBJECTIVES.

Research aims are broad, overarching goals that describe the primary purpose of the research study. They describe what the researcher intends to achieve and sets the general direction for the research. These research aims are typically written in broad terms and reflect the overall ambitions of the research. Research objectives are more specific, with measurable steps that are taken to achieve the research aims. They break the broader aims down into precise findings that the researcher is seeking to establish (Longo, 2024).

The research aims for this study are to research the industry knowledge pertaining to the Global Cybersecurity Workforce Shortage and what affect this shortage is having on organisations. The research further aims to examine industry knowledge around the demand for Cybersecurity professionals, a further research aim is to understand existing initiatives to address the Global Cybersecurity Workforce Shortage and finally to provide insight into the potential of Artificial Intelligence to help mitigate the Cybersecurity Workforce Shortage.

The research objectives that have been devised to realise the aspirations of the research aims are set out below in Fig. 8.

Figure 8: Research Objectives.

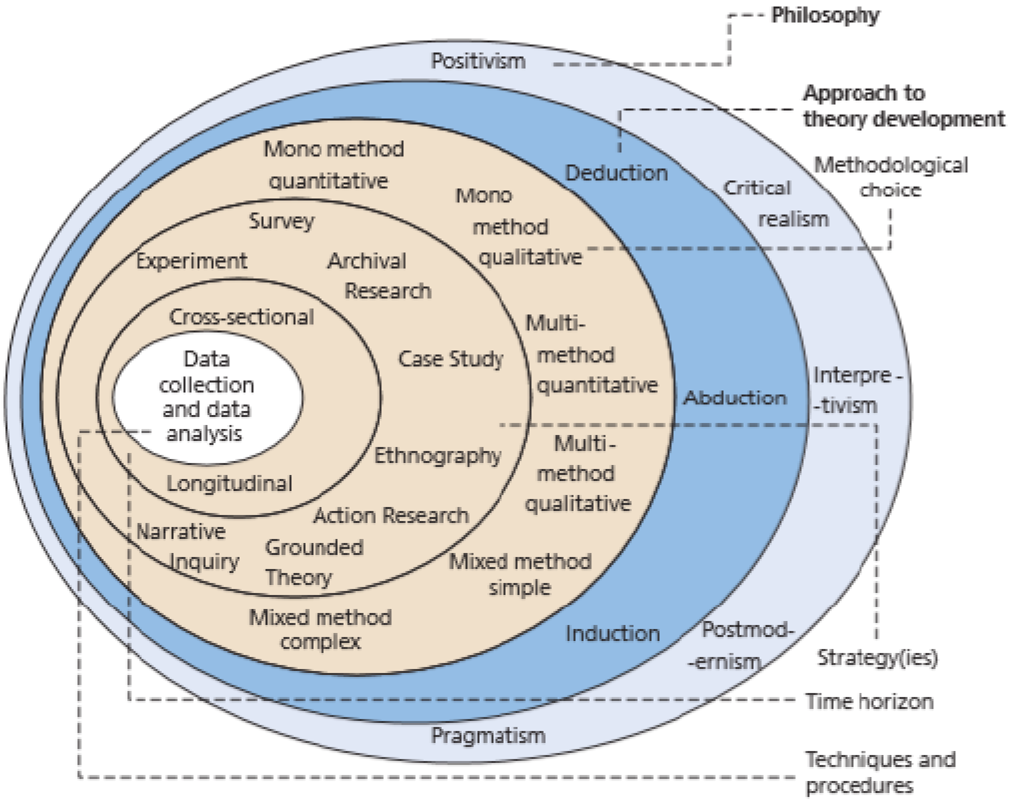
Research Objective 1:	Investigate the awareness and understanding of the global cybersecurity workforce shortage.
Research Objective 2:	Examine the factors driving the increasing demand for cybersecurity professionals.
Research Objective 3:	Assess knowledge and perspectives on education and training approaches to addressing the Cybersecurity Workforce Shortage.
Research Objective 4:	Examine knowledge and perspectives on the use of AI in mitigating the Cybersecurity Workforce Shortage.

3.3 PROPOSED RESEARCH METHODOLOGY.

The Research Onion is a tool that was first developed by Mark Saunders, Philip Lewis and Adrian Thornhill in the fourth edition of their book "Research Methods for Business Students (2007), The Research Onion (as seen below in Fig: 9) assists in the design of research studies by defining six layers, each layer representing a key element of the research process. The researcher starts at the outer layer and works their way through the layers to the center layer. These layers help guide researchers through the different stages of philosophy, approach, methodological choices, strategy, time horizon, data collection and analysis methods.

The research onion has been used by the researcher as a guide to work through the various aforementioned elements of the research process with the goal of answering the research questions that have been discussed in Chapter 1. Some of the criticisms that have been levelled at the Research Onion would include oversimplification. Due to the oversimplified nature of the Research Onion with its step by step approach, it can miss the dynamic and more complex nature of some research. A second criticism of the Research Onion is that of its linear and rigid structure which can mean the research is not accurately reflecting the true nature of research where researchers will revisit research when new insights have been discovered.

Figure 9 The Research Onion.



3.4 Research Philosophy

According to Kirongo & Odoyo (2020a), research can be described as study that's carried out into a particular field or topic, with the aim of investigating a particular problem and adding to the existing body of knowledge of that particular topic. Because there can be different interpretations of what constitutes valid research, there has been an effort to organise, structure, and develop research philosophies, elements and methodologies that align with the belief systems and aims of researchers that are seeking to solve problems and add to the existing bodies of knowledge. Ontology, epistemology and axiology are such elements, they underpin research philosophies and shape the way researchers approach their studies, influencing their choice of methods and the approach to gathering and analysing the data.

Kirongo & Odoyo (2020b) argue that ontology is about one's own experience of reality, about the nature of reality and how this impacts one's experience of everything around us, using the ontology philosophical element means the rest of the research is guided by the perception of reality of the researcher.

Epistemology is another key element that is used to shape the approach to research, Mauthner (2020) argues that epistemology is concerned with the very nature of knowledge, how it is acquired and what constitutes knowledge.

Axiology is the final key element relevant to this research, axiology is the research element that is concerned with the values of the researcher, and how those values shape the approach to the research process (Hart, 1971).

Positivism, Interpretivism, Realism, and Pragmatism are terms that are used to describe the four main research philosophies (Winit-Watjana, 2016). These four main research philosophies are found in the outer layer of the Research Onion (Saunders et al., 2019).

The Positivism research methodology is concerned with removing the influence of human interpretation or bias in a study and focusing on facts, data and exact evidence that is observable and measurable (Alharahsheh & Pius, 2020).

Interpretivism is a research philosophy that is concerned with the understanding from the perspective of the individuals involved in the research, the experience of the individuals is paramount and their interpretation of the subject is what is researched through this philosophy (Scotland, 2012).

Realism, or Critical Realism as it is also known is a research philosophy that embodies aspects of both positivism and interpretivism to offer an alternative to each as a research philosophy (Lawani, 2020).

Pragmatism is a research philosophy that doesn’t subscribe to the strict concepts that concern both positivism and interpretivism, but seeks to accept that there can be multiple realities that can be open to research (Kaushik & Walsh, 2019).

For the purposes of this research, the researcher has chosen interpretivism as the research philosophy, with the underpinned element of epistemology. Interpretivism through the paradigm of epistemology asserts that reality is subjective and established through the social interactions and interpretation of the subject, in this case the researcher and the interviewees (Junjie & Yingxin, 2022). The logic behind this decision is based on the researchers understanding that answering the key question of whether AI can help mitigate the global workforce shortage is best served by conducting in-depth interviews with stakeholders within the field of cybersecurity. The interviewees knowledge and interpretation of the workforce shortage, their knowledge and interpretation of the current approaches to mitigating it and their knowledge and interpretation of the capabilities of Artificial Intelligence and how it can leveraged are paramount to answering the question and serve in the opinion of the researcher as the best philosophy to tackle this research. Positivism has been rejected as it is a philosophy that it frequently requires a scientific approach with exact measurement and results, and is more closely associated to a quantitative approach (Yoon Soo et al., 2020), and given the time restraints and lack of access to scientific measuring resources, for the purposes of this research Interpretivism with epistemology was considered by the researcher a better philosophy. Both the philosophies of pragmatism and realism, which were described above, were also rejected. The logic behind their rejection is the same reasoning behind the rejection of positivism. Pragmatism being a philosophy that doesn’t align with either interpretivism or positivism and tends to rely on a mixed methods approach using both qualitative and quantitative approach (Allemang et al., 2021), was not considered optimal by the researcher because of time restraints and access restraints.

3.5 Research Approach

Inductive and deductive research approaches guide how research studies are carried out. They are both different approaches to conducting research and are each better suited to different kinds of studies. Saunders et al. (2007), lists the research approaches of inductive and deductive at the second layer of the research Onion (see Figure 9 above). So having decided on a research philosophy at the outer layer of the research onion, the researcher now chooses a research approach at the second layer of the research onion.

Soiferman (2010) describes inductive research as having a bottom up approach, beginning with the specific and moving to the general. In contrast, Soiferman describes deductive research as a top down approach, beginning with the general and moving to the specific. Trochim & Donnelly (2006) argue that with the inductive research approach, researchers will start with an observation, then collect data without having already formed a hypothesis or theory, then analyse that data for patterns or themes. The researcher will then form a theory or hypothesis based on those observations. Inductive research is more closely associated with developing new theories, or gaining new insights. Dr Kara (2022) argues that this approach is based on inductive reasoning, and therefore is more closely aligned with or appropriate for a Qualitative research approach.

Deductive research as described by Soiferman (2010) being top down research will start with a general hypothesis or theory already formed, then collect data for the purpose of specifically proving or testing the existing hypothesis, then upon analysing the collected data the researcher will conclude the outcome, either agreeing with the hypothesis or refuting the hypothesis. Because of this approach deductive research is more commonly used for testing theories or hypothesis that already exist. Dr Kara (2022) argues that this deductive approach is more closely aligned to or apt for Quantitative research.

For the purposes of this research study, the researcher has chosen the inductive research approach. The logic behind this decision is because the researcher starts with the observation that there is a global Cybersecurity workforce shortage, then gathers data in the form of research questions put to stakeholders in the field of Cybersecurity, then gathers the responses and correlates the data with the potential of developing a new framework that will align Cybersecurity tasks and roles that are in demand, and tasks and roles that AI can carry out.

The deductive research approach has been rejected as a preconceived hypothesis is not driving the research. The researcher has sought to explore the data in the form of interview question answers, then draw conclusion from that data, as opposed to trying to prove trying to prove an existing hypothesis.

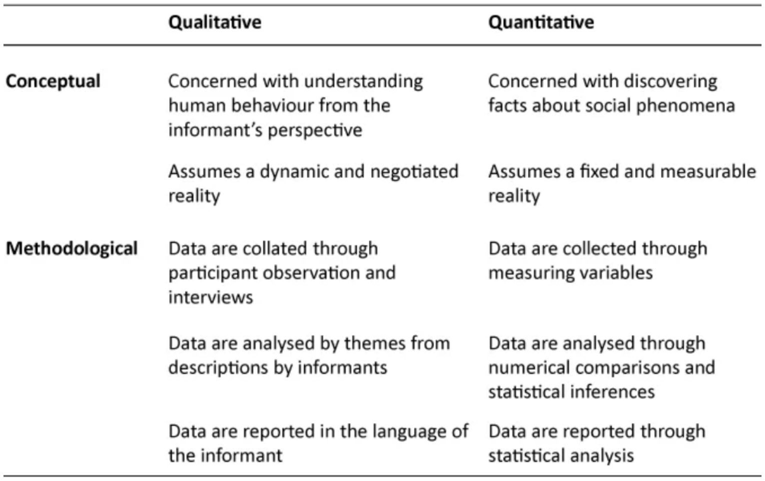
3.6 Research Strategy

Qualitative and Quantitative are the two fundamental research methods used in the field of research. Each approach has its relevance to certain topics within the field of research, and each approach has its strengths and weaknesses when approaching differing research topics. Quantitative research is concerned with collecting numeric data, such as statistics, financial or mathematical data and specifically measurable data, Qualitative research is concerned with collecting information about subjective experience, expert opinion and attitudes (McCleod, 2023).

The Quantitative research method is very much concerned with numerical data, that can include mathematical, computational or statistical data and the relationship that data has between different variables. The data collection techniques used are typically surveys, questionnaires and existing numerical data. The analysis techniques used include statistical analysis and numerical analysis. Quantitative research is typically used to test or prove existing theories. The data sample sizes tend to be large as statistical or numerical analysis is better suited to large data sets for predicting results. Some of the disadvantages of using quantitative research methods include it needs large data sets which can be difficult and time consuming to acquire (Black,1999). Quantitative research methods attributes are listed in Figure 10 below.

Qualitative research methods are concerned with the experience, attitudes and perspective of those running and taking part in the research. The data collection methods include interviews, surveys and focus groups. The analysis techniques used include thematic analysis and narrative analysis. Sample sizes tend to be limited and small in size and focused on specific areas. Some of the disadvantages of the qualitative research method include a possibility of influence of researcher bias (Braun, 2006a). Figure 10 below lists qualitative research methods attributes.

Figure 10: Qualitative and Quantitative attributes



	Qualitative	Quantitative
Conceptual	Concerned with understanding human behaviour from the informant's perspective	Concerned with discovering facts about social phenomena
	Assumes a dynamic and negotiated reality	Assumes a fixed and measurable reality
Methodological	Data are collated through participant observation and interviews	Data are collected through measuring variables
	Data are analysed by themes from descriptions by informants	Data are analysed through numerical comparisons and statistical inferences
	Data are reported in the language of the informant	Data are reported through statistical analysis

Source: Minichiello et al. (1990, p.5).

The Qualitative research method was the research method applied to this study by the researcher. The logic behind that choice was that the research was best served by understanding the experiences, opinions, perspective and interpretation of interviews that are stakeholders in the field of Cybersecurity. The data was gathered from the stakeholders through in-depth interviews and thematic analysis was performed on the data to identify themes and patterns and then to produce insights relating to the topic. The data collection method of In-depth interviews was chosen as it allows the researcher to gather deep insights and a thorough understanding of the subjects knowledge, experience, perspective and interpretation.

Quantitative research methods were rejected as a research method for the purposes of this study, as due to the numerical and statistical nature of quantitative research, it was not considered by the researcher to be an optimal way to gather the experiences, perspectives and interpretations of the topic.

Izhar Oplatka (2021) argues that there can be some downsides or pitfalls to using in-depth interviews, including asking the wrong people. Oplatka argues that selecting interviewees that don't have the relevant knowledge or experience on the research topic can give vague data and offer little in the way of insights. Formulating interview questions that are too narrow and specific with very little scope for developing an answer is also a potential pitfall. In order to get valuable data for qualitative research open-ended questions are recognised as being the most appropriate and beneficial.

including the difficulty of gathering enough subjects that agree to interviews that can be time consuming, also it can be quite an manual effort of organising and analysing the data can mean it is quite time consuming to eventually gather the insights from the data by the researcher.

3.7 Data Collection Method.

The primary collection method for data for this research study is via in-depth interviews. The subjects being interviewed are all stakeholders within the field of Cybersecurity. Donatella della Porta (2014) describes in-depth interviews as a fundamental research method for gathering knowledge and information from subjects being interviewed. Della Porta also argues that interviews are the most commonly used method of collecting data of differing types. Rathbun (2008) states the positive value of using in-depth interviews in qualitative research, describing them as best suited to gleam the perceptions, knowledge, ethics, learning and cognition of the interviewees.

An in-depth interviews approach was chosen for this research study because they offer flexibility in interviewee responses, where the subject has the flexibility within the interview to offer broader answers and offer more insight into the topic of research, in-depth interviews are also arguably more suitable to gather deep understanding of the subjects own experiences, perceptions and knowledge of the research topic and research problem (Seidman, 2006a). The type of questions chosen for the research study were open-ended questions, this style of question is designed to encourage the interviewee to develop and expand on their answer giving a deeper insight into their knowledge, experience, perspectives and attitudes to the research topic (Seidman, 2006b).

3.8 Populations sample

The sample parameters for this research study included the interviewing of ten research subjects. A key requirement and a pitfall to be avoided was a requirement to interview the correct candidates, in the context of this research project that meant interviewing stakeholders within the field of Cybersecurity. The importance of selecting stakeholders within the field of cybersecurity was that they would already have knowledge of the industry and the challenges the industry faces, and indeed that they would have potentially faced themselves or know of others colleagues within the industry would have faced those challenges. All ten of the interviewees had experience of the global cybersecurity workforce shortage, the increasing demand for cybersecurity professionals, the existing initiatives to try and mitigate the shortage, and the potential for AI within the field.

Of the ten interviewees, five were either hiring managers or HR professionals that would be involved in searching for cybersecurity talent and would have had a need to hire cybersecurity professionals within the past six months. Six interviewees were Cybersecurity professionals that work for Cybersecurity vendors, within Cybersecurity teams that have experience, perceptions, interpretations of the Cybersecurity field, of the workforce shortage and also for the existing use of AI within Cybersecurity.

The interviews were conducted by voice/video call and all interviewees consented to the calls being recorded for the purposes of this study. Of the ten interviewees, eight were men, and two women, with only one of the women being a Cybersecurity professional and the other being a HR professional. This lack of diversity in this study is unfortunately reflective of the shortage of women professionals within the wider field of Cybersecurity (Gonzales, 2015).

Figure 11: Interviewee Population Sample

Number	Role	Vertical	Years in Field	Gender
1	HR hiring for Cyber	Corporate	5	Male
2	Cybersecurity Hiring Mgr	Corporate	10+	Male
3	Cybersecurity Architect, on hiring panel	Vendor	10+	Male
4	Snr Cybersecurity Stakeholder	Vendor	10+	Male
5	Snr Cybersecurity stakeholder	Vendor	10+	Male
6	Cybersecurity Architect	Vendor	9	Female
7	HR hiring for Cyber	Corporate	5	Female
8	Snr Cybersecurity stakeholder	Vendor	10+	Male
9	Cybersecurity Hiring Mgr	Corporate	10+	Male
10	Snr Cybersecurity stakeholder	Vendor	10+	Male

3.9 Analysing Qualitative Data.

The interviews were carried out using Microsoft Teams, and recorded with transcripts. The transcriptions were then gathered and answers aligned with each question and research objective. The techniques used were appropriate for this form of research study, because it allowed both the use of audio and video to be recorded, thus giving additional feedback to the researcher in terms of answers as body language could also be observed. This technique also allowed the producing of a transcript of the call, using MS Teams for this is especially beneficial as it not only produces and transcript, but if a section of the transcript is clicked, the video recording will play at the point clicked. Another reason these techniques were appropriate was they gave the researcher the opportunity to encourage the interviewee to give in depth answers with lots of insights that can be analysed. Each interview was then analysed and insights were derived to contribute to findings and discussion section.

Thematic analysis is a form of analysis that seeks out themes, patterns and narratives within the interview answers. Thematic analysis defines six phases that are to be used to get from phase one, getting familiar with the data. To phase six, producing a report (Braun, 2006b). Some of the pitfalls associated with thematic analysis are as follows, The purpose of the thematic analysis to derive insights into the data, and go beyond the initial answer, a problem can occur when thematic analysis is used, but there is no in-depth analysis of the answer

(Braun, 2006c). Another pitfall with thematic is one where the themes are not distinct enough from each other, and there is overlap this leads to analysis that is unconvincing (2006c).

3.10 Ethical Considerations

Protecting human subjects during a qualitative research project is paramount, ethical consideration must be given to the subjects, their background and the relevance of the questions to the topic (Roshaidai & Arifin, 2018). Care has been taken by the researcher to adhere to the guidelines laid out by the National College of Ireland in the document named "Ethical Guidelines and Procedures for Research involving Human Participation", this document has been followed and all ethical considerations adhered to, with the understanding that guidelines that must be followed to protect human subjects during research projects. The National College of Ireland's "Ethical Review Application Form" has been completed and submitted for review of the Ethics board well in advance of the interviews. All interviewees were advised of the topic of the study, and asked for and gave their consent prior to the interview and subsequent recording.

3.11 Limitations To The Research

The nature of qualitative research with in-depth interviews can mean that certain limitations can present during the research process. The researcher and ultimately the data gathered from the interviewees is dependent on the interview subjects own interpretations and experiences, so being able to later collate that data into specific themes and patterns may prove difficult and time consuming for the researcher. Another limitation is that the scientific community often don't consider the results of qualitative research as scientific (Anderson, 2010).

With qualitative research, it can be difficult to replicate findings as the data is dependent on the experiences and perception of the interview subjects at that particular moment in time, another critical limitation is that of sample size and being able to apply findings from a relatively small sample size to conclude generalisations about a wider field (Mwita, 2022). With qualitative research interview questions, sample sizes are typically much smaller that sample sizes used in quantitative research, it is common for between 6 and 20 interviewees to contribute the data for qualitative research. With quantitative research large data samples can be common and use data from 10’s or 100’s or even millions of subjects. With more time available, less time constraints, and access to a broader field of subjects, the researcher would have increased the sample size in an effort to gather further data in an attempt to garner further and deeper insights into the research problem and potential solution.

CHAPTER 4

RESEARCH FINDINGS AND DISCUSSIONS

4.1 Introduction.

The primary research for this research study comprised of ten in-depth interviews of stakeholder within the field of Cybersecurity. The interviews took the form of open-ended questions that probed the interviewees on the research objectives. The research objectives sought to understand the interviewees knowledge, experience and interpretations of the existing shortage of Cybersecurity professionals, the impact that is having on the field, the current efforts to mitigate the shortage and the potential for AI to help alleviate the shortage.

This findings and discussion section will examine the interviewees answers, essentially the collected data, to discover themes, patterns and nuances that will provide insight into the research theme of “the global cybersecurity workforce shortage and the potential of Artificial Intelligence”. The findings and discussion section will also seek to draw conclusions based on the insights gained from the primary research, and from the literature gathered and reviewed in chapter 2. The findings and discussion section will also seek to critically evaluate the identified gaps in the existing literature and the potential for the study to add to the existing body of knowledge on the topic.

4.2 Research Findings.

Ten interviewees participated in the primary research study, of the ten, two were female and eight were men, this is somewhat indicative of the field of cybersecurity where there is an acute shortage of females in the industry (Gates, 2024). Five of the interview participants were either hiring managers or HR professionals, and the remaining five were Cybersecurity stakeholders that worked for Cybersecurity vendors.

4.2.1 Objective 1: "Investigate the awareness and understanding of the global Cybersecurity workforce shortage".

4.2.1.1 Stakeholder awareness of the Global Cybersecurity workforce shortage.

100% of those interviewed, ten out of ten, expressed knowledge of and experience with the Cybersecurity workforce shortage, so awareness of the workforce shortage is high among the interviewees. 50% were aware it is a global shortage and 40% were able to list estimates for the actual numbers globally, with an estimate of between three and six million Cybersecurity professionals needed. Six of those interviewed listed a difficulty of finding candidates with the right mix of experience and skillset as a challenge, as described by interviewee No. 4 (Figure 11), "*A major problem with resourcing, but also with quality, It's Cybersecurity is, it's not just regular IT, it's IT on steroids… You need to be very experienced, you need to have underlying technical skills, programming and network engineering, and database…. and to understand Cybersecurity on top*".

The interviewees experiences of the shortage are very much in line with the secondary research from the literature review in Chapter 2. The global cybersecurity workforce shortage is well documented, one example from the literature review describes a UK study by Pedley, et al. (2020) where 35% of businesses that had been canvassed, reported difficulty filling Cybersecurity roles in the past 3 years. The literature also documents the shortage by describing the results of the 2023 ISC2 workforce study, this study reported that the 2023 Global Cybersecurity workforce shortage stood at approx. 4 million Cyber Professionals (ISC2, 2023).

The researcher encountered an unexpected finding which was mentioned in the primary research interviews (interviewee 10), a phenomenon the interviewee described as "*negative employment*", essentially it meant organisations hiring underqualified staff into senior roles with the intention of bringing them up to the level they would need to be at to carry out the role effectively, "*I've also heard from customers… what they are referring to as negative* *employment, and I wasn't too sure what that meant when I first heard the term. But essentially what they mean by that is they're hiring junior people into more Senior roles, essentially because they just can't get the more senior people in it*". This approach by organisations is commendable and shows a willingness to both invest in developing talent and to think outside the box in terms of tackling the workforce shortage. In terms of the other nine interviewees, this was not a widely experienced approach.

An identified gap in the existing literature would include the concept of reskilling, or cross skilling existing IT professionals into Cybersecurity roles. Currently the body of knowledge does not include a pathway, that would map out what further education or certification path an existing IT professional could take to becoming a Cybersecurity professional, the body of knowledge could be further developed by research into aligning existing IT roles and the Cybersecurity frameworks ECSF and NICE, this would help educators develop courses that bring existing IT professionals from one career path to a Cyber career path, and would help organisations identify how to develop internal talent into cybersecurity roles.

4.2.1.2 Stakeholder view of the impact of the Global Cybersecurity Workforce shortage.

The difficulty in hiring for Cyber roles remained to be a theme reported amongst the interviewee answers for this heading. With 80% of the respondents reporting that an impact of the shortage was that they, or someone they knew within the Cyber field had difficulty hiring for Cyber roles.

Another theme in the data was that of impact on Cyber project delivery. Two of the interviewees (interviewee 9, 10) reported an impact on the delivery of Cybersecurity projects, affecting both the speed of delivery and the ability to deliver at all, due to the shortage. Interviewee 9 expressed, "*we have a lot of business demands coming in and you know in terms of making security assessments and looking at designs to make sure that what has been built by other architects is secure and fit for purpose, and as a conveyor belt of those demands come in, we just don't have the resources or the expertise to actually get through those*." This impact and theme has also been expressed in the literature reviewed in Chapter 2, where Blazic (2021) argued that the workforce shortage impacted European businesses with the implementation of the GDPR directive from the EU, as organisations struggled to recruit specialist Cyber staff to carry out the projects to achieve compliance.

Two of the HR professionals interviewed reported another theme, that a company's preference for onsite working can cause problems recruiting Cyber professionals, as the in demand candidates expressed a preference for hybrid or fully remote working, Interviewee 1 reporting "*They've really struggled where they've been looking to have onsite or in person roles, as opposed to hybrid roles, and really struggling to fill those roles there*." A second HR person (Interviewee 7) reported, "*The market obviously is looking for a work life balance for flexibility into working from home, let's say four days per week*." Interviewees are listed in Figure 11, Interviewee Population Sample.

One gap in the literature which is not significantly developed is that of burnout within the field of Cybersecurity, interviewee 3 reported that "*We have a lot of work, a lot of backlog and we can't cover the work with the people that are there, and we tend to overwork the people that are inside (the company)*". There is not a significant amount of literature in the existing body of knowledge that links burnout with the impact of the workforce shortage. The research identifies an opportunity to conduct additional research into avoiding burnout with the field of cybersecurity so as to help alleviate the workforce shortage.

4.2.1.3 Stakeholder view of the impact of the workforce shortage on organisations.

Organisations have come under increasing pressure to comply with regulations in the field of Cybersecurity, regulations like GDPR and NIS2 which are both EU directives, have put increasing pressure on board level executives (KPMG, 2024). Three of the primary research interviewees (Interviewees 3,4 & 5) have reported that the tenure of a CISO within an organisation is also decreasing due to the increasing pressures from Executive Boards, who are now under pressure to comply with industry regulations and standards or face large fines or legal recourse if negligence is proven. This theme is highlighted by interviewee 5 "*Now anything up to you know, 1.5 to two years maximum and even the pressure that is exerted on perhaps*

CISO type roles as well…. But yet the demands are increasing such that it's such a pressure cooker that I think even the life of the CISO is a very short lived tenure." Interviewee 3 repeated this theme with the following comments "*There's a lot of pressure coming from the different areas of the business because Cybersecurity, I wouldn't say its trendy, but it's necessary and it's growing a lot, and there is a lot of awareness on leadership inside of it.*" This theme shows the impact the workforce shortage is having on organisations.

Organisations under pressure due to regulations, and the limited resources they have to gain compliance is well documented, and this theme is well represented in the existing body of knowledge and literature review in Chapter 2 (Blazic, 2021), regulations such as NIS2, and GDPR carry significant fines if not adhered to (European Commission, 2024).

Organisations retention rates for Cybersecurity professionals is another theme identified in the data, two interviewees, Interview 5 and 6 mentioned that retention rates for staff are low with Cyber professionals changing roles around the two to four years timeframe. Interviewee 6 stated, "*So retention rates are really, really low right…… you see a lot of people kind of leaving, like literally after between two and four years*". This can cause significant impact to organisations that have to find replacements and lose knowledge when an employee leaves.

4.2.2 Objective 2: "Examine the factors driving the increasing demand for Cybersecurity professionals".

4.2.2.1 The Demand for Cybersecurity Professionals.

100% of the interviewees agreed that the demand for Cybersecurity professionals we increasing. A theme that emerged in the data was that the structure of Cybersecurity teams has changed, with three of the interviewees reporting that Cyber teams now contain a myriad of roles, where historically they would have been much more limited in size and scope, also that the reporting has also changed where the Cyber function is no longer under the IT remit, but a separate Cyber division within the organisation, Interviewee 2 commented that "*Previously Cyber maybe sat under or was done as part of a role for IT, or a business or as a compliance* *role, they now certainly need to set up Cybersecurity, they now need a CISO or a head of Security at a minimum*".

4.2.2.2 Driving factors increasing demand for Cybersecurity Professionals.

A common theme among four of the primary research study interviewees was that of an increasing reliance on technology as a driving factor increasing demand for Cybersecurity professionals. Society in general is becoming increasingly digitised, interviewee 10 argued "*I think what it really comes back to is a reliance on IT, and I think that was proven very much so in recent times and the recent weeks where you know there was a security incident and planes stopped flying, trains stopped running, hospitals stopped running and so forth and so on. So as a civilisation, we have become uber reliant on IT for our daily lives*." The incident the interviewee was discussing was an incident that effected systems globally and originated as an update from a major Cybersecurity firm. This heavy reliance is also reflected in the existing body of knowledge and highlighted in the literature review in Chapter 2, where Teoh & Mahmood (2017) describe it in their "Cybersecurity Workforce Development for Digital Economy" paper. The primary and secondary research indicate that the existing body of knowledge describes the driving factors that are increasing demand for Cybersecurity professionals.

Regulation compliance was again listed as a driving factor for increasing the demand of Cyber professionals as listed in section 4.2.1.3, this theme was listed by five of the ten interviewees as a factor increasing the demand for Cyber professionals.

4.2.2.3 The Cybersecurity landscape, pre, mid and post Covid-19 pandemic.

One finding regarding the pre-Covid Cyber landscape and demand for Cybersecurity professionals has been the description of the workforce demand as "steady" by six of our ten interviewees. All six of these interviewees are hiring managers or part of the wider hiring team within their organisations, so this represents a common theme among those with direct experience of trying to hire Cybersecurity professionals in the pre-Covid landscape. Interviewee 2 commented, "*So I guess pre-Covid there was kind of just a steady demand, the industry was growing, you know, bit by bit Cyber threats, adoption of technology, some new regulations coming into the market. There was kind of a, you know, a gradual growth*." This perception of the pre-Covid landscape is reflected in the literature reviewed in Chapter 2. As mentioned above, Teoh & Mahmood (2017) described the pre-Covid landscape in their "Cybersecurity Workforce Development for Digital Economy", where demand for Cyber professionals was growing, but at a steady rate as global economies became more digitised.

During the Covid pandemic, as a new paradigm in work practices was forced upon organisations globally, the workload on existing Cybersecurity professionals increased dramatically as they worked to facilitate remote working and secure Software as-a-service cloud applications and platforms. Seven of the ten interviewees referenced this common theme, interviewee 3 noted "*So for vendors like the one where I'm working, that was insane, building everything so rapidly*". Interviewee 5 also argued "*Then mid-Covid, there was a huge rush to enable remote working and granted an awful lot of organisations did very well to facilitate that, and in a short space of time*". Another finding was that even though, as noted by the majority of interviewees, workload on existing Cybersecurity professionals grew mid-Covid, both of the HR professionals noted that the mid-Covid demand to recruit Cyber people was not as great as it became post-Covid, interviewee noted "*I still don't think there was a huge explosion in Cyber Professionals, in the need for, sorry for the push for Cyber Professionals, at the rate it is now, I very much think it's increased post-Covid*."

Post-Covid, a common theme among 70% of our primary research interviewees, is that of a reported increase in demand for Cyber professionals. Interviewee 10 reported, "*I think one big thing that has changed is that it's easier to get budget for security projects today than it ever was before Covid, and although you have the money, you just can't spend it because you actually can't find the people*." This is a very salient point and a key finding from the interviews is that the Covid pandemic, has shone a light on the Cyber profession and highlighted it's importance like never before, this has freed up budget, however the workforce shortage is hampering the progress of such initiatives. The post covid demand for Cyber people is well documented in the literature reviewed in Chapter 2, with a number of factors listed as the drivers, increased advanced threats (EURESCOM, 2024), new working paradigm (Ardagna et al., 2021), increased regulation (KPMG, 2024).

4.2.3 Objective 3: “Assess knowledge and perspectives on education and training approaches to addressing the Cybersecurity Workforce Shortage”.

4.2.3.1 Awareness of organisations working on mitigating the Cybersecurity workforce shortage.

Of the ten interviewees, only one could name the main bodies within Europe and the US that were working on mitigating the workforce shortage. Five others were aware of local government initiatives, and had varying degrees of knowledge of who they are and what they are trying to do. Four interviewees had no knowledge of organisations or bodies that are working to mitigate the workforce shortage. With the exception of one interviewee, the findings suggested that there was little knowledge of what organisations/bodies were laying down frameworks, establishing initiatives etc to help mitigate the global Cybersecurity workforce shortage. Interviewee 1, reported “*I know the EU have their own ones, the UN and then the US would have a variety of other ones. But they’re probably the main global ones I’ve seen. I wouldn’t have too much information.*” This was a common theme among the majority of the interviewees.

We know from the literature review in chapter 2, that the ENISA, the CISA, NIST and the ISC2 have put significant effort into developing frameworks, Cybersecurity policy, guidelines and standards to help organisations and governments deal with the workforce shortage (ENISA, 2024a), (NIST, 2023), (CISA, 2024a), (ISC2, 2024a). This finding would highlight a gap in the stakeholder knowledge of who these bodies are, this could potentially represent an opportunity to justify further research into how these organisations could better engage with cybersecurity stakeholders.

4.2.3.2 Awareness of efforts to reduce the shortage through education and training.

The findings gathered indicated that there was a good overall awareness of the education, training and certification initiatives that are in place to help mitigate the shortage. A common theme emerged where seven of the ten subjects highlighted their awareness of 3rd level institutions and their initiatives. Interviewee 1 noted “*there is another, being huge huge investment into universities globally to you know offer, to have more offerings within Cyber Security and you know specific to cyber, and how historically a lot of them would be focused* *largely on computer science and you know to be quite general degrees and by now…. many have branched off into more specialist areas globally and to add on to that, there's more masters degrees than ever I think in Cyber, and PHD's."* Nine out of ten of the subjects also listed their awareness of vendor certifications as an education and training initiative.

The literature reviewed in chapter 2 suggests that the efforts to mitigate the shortage through education and training initiatives are well documented, such as the EU's Cyber Skills Academy (EU, 2024), and in the US with the CISA's National Initiative for Cybersecurity Careers and Studies (CISA, 2024c).

One gap that was observed however was in relation to the ECSF and NICE frameworks, and the job roles and tasks that the training courses and certifications were preparing people to carry out. There was no knowledge amongst the interviewees of the alignment between the Cyber roles and tasks listed in the frameworks, and the training programs or certifications that the training institutions or certification providers offered. This suggests that organisations and hiring managers could benefit from a well-defined frameworks, that also highlighted what roles and certifications aligned with what courses and certificates.

4.2.3.3 Effectiveness of educations and training initiatives in mitigating the shortage.

A common theme mentioned by seven out of the ten interviewees was that these education and training initiatives "*are helping*" regarding the workforce shortage, however there is a caveat. Four out of the seven interviewees mentioned that even though they are helping, they are not producing enough candidates to keep up with the growing demand for workers. Interviewee 10 stated, "*There's just not enough of them, so individually absolutely every program is going to help, but I just think that it's just not doing a good job at these things. It's just the increase that they're getting from these is being surprised by the increase in need for the security professionals and hence the number is constantly growing*".

This finding would suggest that from the perspective of the majority of those in the Cyber industry, the education and training initiatives are producing candidates, however not at a fast enough rate to satisfy the increasing demand, in Chapter 2, there is a myriad of references to agencies and bodies such as the ENISA, the CISA and ISC2 who are working to educate and train talent to help mitigate the shortage, however the data we see from the 2023 ISC2 annual workforce study showed that even though the Cyber workforce grew by around 9% between 2022 and 2023, the workforce shortage grew by 13% for the same period (ISC2, 2023).

4.2.4 Objective 4: "Examine knowledge and perspectives on the use of AI in mitigating the Cybersecurity Workforce Shortage".

4.2.4.1 Awareness of the use of AI in Cybersecurity.

All of the interviewees were aware of the use of AI in Cybersecurity, eight out of ten interview subjects reported being aware of the use of AI for analysing large data sets for anomalies, malicious behaviour detection. So the interviewees demonstrated a knowledge of the use of AI in Cybersecurity. Interviewee 3 stated, "*AI and Machine Learning in general are much better in general at reading large amounts of data sets*". The awareness of the use of AI within the field of Cybersecurity amongst the interviewees is also reflected in the literature review from Chapter 2, where the use of AI for processing large amounts of data is described by the Cybersecurity company Sophos (2024).

4.2.4.2 Awareness of the tasks and roles AI can help perform in Cybersecurity.

All ten of the interviewees showed some awareness of the tasks and roles that AI can perform within the field of Cybersecurity, with differing degrees of knowledge expressed amongst the interview subjects. The interviewees from a Cyber vendor background and one Cybersecurity manager expressed a deeper understanding of what tasks AI can currently carry out, and how recent developments in Generative AI can help develop those AI capabilities further. The data correlated from this interview question would suggest that there is an awareness amongst stakeholders about the use of AI in the field of Cybersecurity, however one theme that emerged was that the level of knowledge varied amongst the interviewees. Another finding was the potential of AI to carry out tasks that can specifically assist SOC analysts, five of the interviewees expressly mentioned Security Operations tasks, that they could see AI helping with. Interviewee 2 argued, "*The SOC incident response, it's probably the biggest opportunity,* *just the scale of information…. Their SOC tools, to help with the kind of processing analysis of everything that's coming through the log monitoring and analytics, to you know identify patterns that maybe a SOC analyst mightn't spot, or might take longer to spot*." With a deeper understanding of what roles and tasks AI can perform within the field of Cybersecurity, hiring managers, and HR professionals could potentially seek out new products, tools or services that could either take on some tasks and automate in order to take some of the workload off the existing Cyber professionals.

4.2.4.3 The effectiveness of AI in mitigating the Cybersecurity workforce shortage.

Nine out of ten of the interviewees reported that they believed that AI can indeed help reduce the workload of existing Cyber professionals, and eight out of ten reported that they believed that AI will be able to help mitigate the Cybersecurity workforce shortage. Interviewee 2 stated "*But where it will be able to help is just to allow those teams to scale as they build up… every time your cyber workforce, it shouldn't be a you know, a line going straight up. You should start to see the workforce shortage and the demand for workforce start to kind of flatten out a little bit because we should be able to do more with the same volume of workforce*."

The primary research also revealed that nine out of the ten interviewees believed that AI will able to help by carrying out tasks the Security Operations teams would typically do, ie: would be able to automate repetitive workloads, data and behavioural analysis, incident detection etc, Interviewee 4 noted, "*You might be able to have automation and AI…. You might be able to reduce the amount of people, say in a SOC… That are monitoring alerts all of the time*." Five out of ten of the interviewees also reported that they there would be a need to introduce training for the analysts that would need to leverage AI, this could introduce some cost overhead and some delay in getting the workforce up to speed with the new technology. One unexpected and intuitive observation from interviewee 3, was that by the introduction of AI in cyber would introduce a new skillset, and this skillset could potentially be in big demand, and in itself could create an AI workforce shortage, "*We're gonna create an AI shortage as well, so that's another problem to think about, right, you still need to get AI engineers today. I think we are gonna have two different shortages, but still I think it will be a bit better*." Overall as exhibited above, the interviewees were positive about the impact AI can have on reducing the workload on Cyber professionals, and also on the potential for AI to help mitigate the workforce shortage.

4.3 Study Limitations.

Certain limitations can exist when using any research method, strategy and approach. This research study used qualitative research, with the primary data derived from in-depth interviews which comprised of open-ended questions. The open-ended questions were put to ten interview subjects that were all stakeholders within the field of Cybersecurity. Two were Human Resources personnel who were tasked by hiring managers with recruiting for Cybersecurity positions. Two more were Cybersecurity managers who were hiring managers for Cybersecurity roles within their teams, and the six others were Cybersecurity professionals from Cyber vendors, one of which was on the hiring team for bringing in new talent. The findings and themes from the interview questions were very much in line with what was identified in the secondary research in Chapter 2, the Literature Review. With some unexpected answers offering additional insights. The data gathered from the primary research interviews and the literature review allowed the researcher to identify gaps in the research that can justify additional research for the purposes of adding to the existing body of knowledge. Because qualitative research using in-depth interviews relies heavily on the interview subjects own experiences, perspective and knowledge, this method can be prone to both research bias and bias on behalf of the subjects (Bergen & Labonté, 2019). However due to the sample size of 10 subjects and the use of open-ended questions, the researcher tried to ensure the results of the study are objective and thorough.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS.

5.1 Study Conclusions and recommendations.

5.1.1 Aligning AI Cybersecurity Capabilities, with the tasks and roles specified in the competency Frameworks.

The existing body of literature focusing on the field of Cybersecurity and the problem of the workforce shortage has been extensively reviewed in this research study. Some of the key conclusions include the realisation that the demand for Cybersecurity professionals is growing, this has been established in both the literature review (ISC2, 2023), and the data gathered in the primary research interviews. This would indicate that the current efforts to mitigate the shortage by organisations like the ENISA, CISA, NIST and the ISC2 are not succeeding at the rates needed to mitigate the shortage effectively. Therefore broadening the scope of the current mitigation efforts beyond the areas of education and certification in order to bring more Cybersecurity professionals into the field is warranted. The researcher believes there is an academic research opportunity to research further how AI can be leveraged to mitigate the Cybersecurity workforce shortage, specifically in relation to the existing ECSF and NICE frameworks which already list Cyber tasks and roles. By aligning AI capabilities and tools with the existing frameworks that would help educational institutions, AI researchers and developers develop curricula, tools and products that can be leveraged by organisations to supplement existing Cyber workers by automating some of their workloads, meaning potentially, less analysts are needed.

5.1.2 Education on the use of AI for Cybersecurity analysts**.**

Both the primary and secondary research identified Security Operations as a key area where the use of Artificial Intelligence can play a role in automating workloads and performing menial repetitive tasks and ultimately freeing up SOC analysts to perform more high level activities and thus making better use of their time (Palo Alto Networks, 2024c), potentially giving them more job satisfaction, reducing their levels of "alert fatigue". The benefits of the use of AI in this area include potentially reducing burnout, and thus staff turnover, but also potentially the headcount requirement is lower, as more workloads, tasks and roles are handled by AI with the SOC analyst managing the AI. When the AI capabilities have been aligned with the frameworks as suggested in section 5.1.1, the next step will be around education. Educational institutions, certification providers and developers of curricula will need to integrate the AI training and education into their education programs so that SOC analysts and other Cybersecurity professionals can learn the skills necessary to manage AI in executing workloads, tasks and jobs, to help them achieve efficiencies. The existing body of knowledge on this theme could be further developed by more research into exactly how this can be best achieved.

5.1.3 Education on the use of AI for Cybersecurity hiring managers and leadership.

While there is evidence of the existing use of AI within the field of Cybersecurity (Wheatley, 2020). The findings from the primary research revealed that AI was not identified by hiring managers as a technology that they could leverage as an alternative to hiring more SOC analysts or as part of a hiring strategy when recruiting for Cybersecurity roles or building out Cybersecurity capability. Outside being embedded within products from vendors, new uses of AI in the field of Cybersecurity are still in the early stages of development and how to leverage this technology is not widely known. There appears to be a gap between being aware of the existence of the Cybersecurity AI tools, products and solutions and actually understanding how they can be leveraged by Cyber leaders and hiring managers within their Cyber strategies to increase efficiencies in their Security Operations teams. There is an opportunity here to carry out additional research, to understand how best to close this gap and add to the existing body of knowledge.

Education is key here. Cybersecurity leaders and hiring managers need to become educated on the specifics of how to leverage AI. When the capabilities of AI have been aligned with the education and certification programs as highlighted above in section 5.1.1. Cybersecurity leaders and hiring managers will need to skill up on how to leverage AI, and then integrate it into their Cyber capability strategy and hiring strategy to realise the efficiencies that AI promises.

5.2 Summary.

The theme of the research paper has been "The Global Cybersecurity Workforce Shortage and the Potential for Artificial Intelligence. The aim of the research has been to examine the existing body of knowledge of this subject via secondary research, identify gaps in the existing body of knowledge and suggest potential areas for further research. To conduct primary research, and gather insights and critically discuss them. To explain and justify the research methodology used to conduct this research. The value of the research lies with identifying the existing research gaps, and also with helping organisations recognise the potential of Artificial Intelligence in helping mitigate the Cybersecurity workforce shortage.

References:

Äijälä, T. (2018). *CISSP certification – accreditation value for employees and recruiters*. Available at: https://www.theseus.fi/bitstream/handle/10024/148953/Tommi_Aijala.pdf [Accessed 27th May 2024].

Allemang, B, Sitter, K, Dimitropoulos, G. (2021). *Pragmatism as a paradigm for patient-orientated research*. Available at: https://doi.org/10.1111/hex.13384 [Accessed 27th May 2024].

Alharahsheh, A., Pius, A. (2020). *A Review of key paradigms: Positivism V's Interpretivism.* p.41. Available at: https://gajrc.com/media/articles/GAJHSS_23_39-43_VMGJbOK.pdf [Accessed 27th May 2024].

Anderson, Claire.(2010). *Presenting and Evaluating Qualitative Research*. Available at: https://doi.org/10.5688/aj7408141 [Accessed 27th May 2024].

Ardagna, C., Corbiaux, S., Sfakianakis, A., Douligeris, C. (2021). *ENISA Threat Landscape 2021* Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 [Accessed 27th May 2024].

Bergen, N., Labronté, R (2019). *"Everything is Perfect, and We Have No Problems": Detecting and Limiting Social Desirability Bias in Qualitative Research.* Available at : https://journals.sagepub.com/doi/full/10.1177/1049732319889354 [Accessed 27th May 2024].

Black, T.R. (1999). *Doing quantitative research in the social sciences: An integrated approach to research design, measurement and statistics.* Guildford. Sage publications Ltd.

Blair, Lorrie. (2016). *Writing a Graduate Thesis or Dissertation.* Available at: *https://brill.com/display/book/9789463004268/BP000007.xml* [Accessed 27th May 2024].

Blaxter, L., Hughes, C., Tight, M.(2010) *How to Research.* Fourth Edition, London: Open University Press.

Blazic, Borka Jerman (2021). *The Cybersecurity Labour Shortage in Europe: Moving to a new concept for education and training.* Available at: https://doi.org/10.1016/j.techsoc.2021.101769 [Accessed 27th May 2024].

Braun, V., Clarke, V. (2006a). *Using thematic analysis in psychology. Qualitative Research in Psychology.* pp.4-11. Available at: https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology#fullTextFileContent [Accessed 27th May 2024].

Braun, V., Clarke, V. (2006b). *Using thematic analysis in psychology. Qualitative Research in Psychology*. pp.17-28. Available at: https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology#fullTextFileContent [Accessed 27th May 2024].

Braun, V., Clarke, V. (2006c). *Using thematic analysis in psychology. Qualitative Research in Psychology*. pp.25-28. Available at: https://www.researchgate.net/publication/235356393_Using_thematic_analysis_in_psychology#fullTextFileContent [Accessed 27th May 2024].

Brown, S. (2021) *Machine Learning, explained*. Available at: https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained [Accessed 27th May 2024].

Chandel, S., Sun, Y,. Yitian, T., Zhili, Z., Yusheng, H. (2019) *Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat.* Available at: https://ieeexplore.ieee.org/abstract/document/8945852 [Accessed 27th May 2024].

CISA (2024a). *Workforce Framework for Cybersecurity: Nice Framework Now Updated.* Available at: https://niccs.cisa.gov/workforce-development/nice-framework [Accessed 21st June 2024].

CISA (2024b). *America's Cyber Defence Agency*. Available at: https://www.cisa.gov/ [Accessed 27th May 2024].

CISA (2024c). *NICCS, National Initiative for Cybersecurity Careers and Studies*: *About NICCS.* Available at: https://niccs.cisa.gov/about-niccs [Accessed 27th May 2024].

CISA (2024d). *Cybersecurity Education & Career Development.* Available at: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-education-career-development [Accessed 27th May 2024].

Cisco (2024). *What is Extended Detection and Response (XDR)?* Available at: https://www.cisco.com/c/en/us/products/security/what-is-xdr.html [Accessed 27th May 2024].

Creswell, J.W., Creswell, J.D.(2017) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Fifth Edition. Available at: https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf [Accessed 27th May 2024].

CrowdStrike. (2022). *2023 Global Threat Report*. Available at: https://go.crowdstrike.com/2023-global-threat-report.html [Accessed 27th May 2024].

Cyber.org (2024). *About Us.* Available at: https://cyber.org/about-us [Accessed 27th May 2024].

della Porta, Donatella (2014). Methodological Practices In Social Movement Research. pp. 228-262. Available at: https://bit.ly/3Sz4PkW [Accessed 27th May 2024].

DiFurio, D. (2023a). *Demand for Cybersecurity Analysts is Growing Twice as Fast as the workforce.* Available at: https://drata.com/blog/demand-for-cybersecurity-analysts [Accessed 7th July 2024]. [Accessed 27th May 2024].

DiFurio, D. (2023b). *Demand for Cybersecurity Analysts is Growing Twice as Fast as the workforce*: *Demand for Cybersecurity Professionals is Growing Twice as Fast as the Workforce.* Available at: https://drata.com/blog/demand-for-cybersecurity-analysts [Accessed 7th July 2024].

ECSO (2022). *ENISA Introduces the European Cybersecurity Skills Framework.* Available at: https://ecs-org.eu/enisa-introduces-the-european-cybersecurity-skills-framework/ [Accessed 27th May 2024].

ENISA (2022a). *Developing a Strong Cybersecurity Workforce: Introducing the European Cybersecurity Skills Framework.* Available at: https://www.enisa.europa.eu/news/developing-a-strong-cybersecurity-workforce-introducing-the-european-cybersecurity-skills-framework [Accessed 7th July 2024].

ENISA (2022b). *European Cybersecurity Skills Framework Role Profiles.* Available at: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles [Accessed 7th July 2024].

ENISA (2023). *Cybersecurity Skills Conference: Strengthening human capital in the EU.* Available at: https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu [Accessed 27th May 2024].

ENISA (2024a). *About ENISA – The European Union Agency for Cybersecurity*. Available at: https://www.enisa.europa.eu/about-enisa [Accessed 27th May 2024].

ENISA (2024b). *ECSF Goals in Brief.* Available at: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework [Accessed 27th May 2024].

EU (2024). *Cybersecurity Skills Academy.* Available at: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy [Accessed 27th May 2024].

EURESCOM (2024). *ENISA threat landscape report highlights surge in Cybercrime*. Available at: https://www.eurescom.eu/eurescom-messages/winter-2021/enisa-threat-landscape-report-highlights-surge-in-cybercrime/ [Accessed 27th May 2024].

EUR-Lex (2023). *Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.* Available at: http://data.europa.eu/eli/reg/2023/2841/oj [Accessed 27th May 2024].

European Commission (2024). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).* Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive [Accessed 27th May 2024].

Gartner (2022). *Gartner Identifies Three Factors Influencing Growth in Security Spending*. Available at: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i [Accessed 27th May 2024].

Gates, M. (2024). *ISC2 Report: The Number of Women in Cybersecurity Remains Stagnant, Despite Ongoing Workforce Gap*. Available at: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2024/april/The-Number-of-Women-in-Cyber/ [Accessed 27th May 2024].

Goncalves, D.G.V., Filho, F.L.C., Martins, L.M.C.E., Kfouri, G.O., Dutra, B., Albuquerque, R.O., Sousa, R.T., (2029). *IPS Architecture for IoT networks overlapped in SDN.* Available at: https://ieeexplore.ieee.org/abstract/document/8896297 [Accessed 27th May 2024].
Gregory, M.(2024). Back to Basics: The role of AI in Cybersecurity. Available at: https://healthtechmagazine.net/article/2024/04/back-basics-role-ai-cybersecurity [Accessed 27th May 2024].

Gonzalez, M.D. (2015). *Building a Cybersecurity Pipeline to Attract, Train and Retain Women*. Business Journal for Entrepreneurs. pp.24-41.

Hart, S.L (1971). *Philosophy and Phenomenological Research.* pp. 29-41 Available at: https://doi.org/10.2307/2105883 [Accessed 27th May 2024].

Hogan M., Lilienthal, K., Bean de Hernandez, A., McHugh, P., Arbeit, C.A., Sullivan. (2024); National Center for Science and Engineering Statistics. *Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Supply and Demand Report*. Alexandria, VA: National Science Foundation. Available at https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative [Accessed 27th May 2024].

InfoSecInstitute (2024). *SOC analyst Careers.* Available at: https://www.infosecinstitute.com/roles/soc-analyst-careers/ [Accessed 27th May 2024].

ISC2 (2020). *Cybersecurity Professionals stand up to the Pandemic. CYBERSECURITY WORKFORCE STUDY 2020.* Available at*: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-cybersecurity-workforce-study--2020.pdf* [Accessed 27th May 2024].

ISC2 (2021). *A Resilient Cybersecurity Profession Charts the Path Forward. CYBERSECURITY WORKFORCE STUDY 2021.* Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2021.pdf [Accessed 27th May 2024].

ISC2 (2022). *CYBERSECURITY WORKFORCE STUDY. A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution 2022.* Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf [Accessed 27th May 2024].

ISC2 (2023). *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023.* Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf [Accessed 27th May 2024].

ISC2 (2024a). *Your Future. Secured. What We Do at ISC2*. Available at: https://www.isc2.org/about [Accessed 27th May 2024].

ISC2 (2024b). *ISC2 Certification Framework Mappings*. Available at: https://www.isc2.org/certifications/frameworks [Accessed 27th May 2024].

ISC2 (2024c). *Our Vision.* Available at: https://www.isc2.org/about [Accessed 27th May 2024].

Junjie, M., Yingxin, M. (2022). *The Discussions of Positivism and Interpretivism*. p.11. Available at: https://files.eric.ed.gov/fulltext/ED619359.pdf Accessed 27th May 2024].

Kaushik, V., Walsh, C.A. (2019) *Pragmatism as a Research Paradigm and Its Implications for Social Work Research. p.3.* Available at: **https://doi.org/10.3390/socsci8090255** [Accessed 27th May 2024].

Kirongo, A.C.. Osoyo, C.O.(2020a). *Research Philosophy Design and Methodologies: A Systematic Review or Research Paradigms in Information Technology*, p35. Available at: https://www.globalscientificjournal.com/researchpaper/Research_Philosophy_Design_and_Methodologies_A_Systematic_Review_of_Research_Paradigms_in_Information_Technology_.pdf [Accessed 27th May 2024].

Kirongo, A.C.. Osoyo, C.O.(2020b). *Research Philosophy Design and Methodologies: A Systematic Review or Research Paradigms in Information Technology*, p36. Available at: https://www.globalscientificjournal.com/researchpaper/Research_Philosophy_Design_and_Methodologies_A_Systematic_Review_of_Research_Paradigms_in_Information_Technology_.pdf [Accessed 27th May 2024].

Knapp, K.J,. Maurer, C., Plachkinova, M (2017). *Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance.* Available at: https://jise.org/Volume28/n2/JISEv28n2p101.pdf [Accessed 27th May 2024].

KPMG (2024). *SEC's final cybersecurity rules: A boards lens.* Available at: https://kpmg.com/us/en/board-leadership/articles/2023/sec-final-cybersecurity-rules-a-board-lens.html [Accessed 27th May 2024].

Kumar, R.(2011). *Research Methodology: A step-by-step guide for beginners*. Available at: http://www.sociology.kpi.ua/wp-content/uploads/2014/06/Ranjit_Kumar-Research_Methodology_A_Step-by-Step_G.pdf [Accessed 27th May 2024].

Lallie, S.L., Shepherd, L.A,. Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X. (2021). *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.* Available at: https://www.sciencedirect.com/science/article/pii/S0167404821000729#bib0054 [Accessed 27th May 2024].

Lawani, A. (2020). *Critical realism: what you should know and how to apply it*. p. 321. Available at: https://www.emerald.com/insight/content/doi/10.1108/QRJ-08-2020-0101/full/html [Accessed 27th May 2024].

Lingleback, K.(2023). *A study of female Cybersecurity professionals*. Available at: https://doi.org/10.48009/3_iis_2023_108 [Accessed 27th May 2024].

Longo, Luca.(2024). *Research aims and objectives.* Available at: *http://researchdesign.lucalongo.eu/material/RESEARCH_DESIGN___research_aims_and_objectives.pdf* [Accessed 27th May 2024].

Madnick, S. (2024). *Why Data Breaches Spiked in 2023*. Available at: https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 [Accessed 27th May 2024].

Mauthner, N.S. (2020). *How to keep your Doctorate on Track,* Chapter 12.pp76-86. Available here: https://doi.org/10.4337/9781788975636.00018 [Accessed 27th May 2024].

McLeod, S.(2023). *Qualitative V's Quantitative Research Methods & Data Analysis*. Available at: https://www.simplypsychology.org/qualitative-quantitative.html [Accessed 27th May 2024].

Meineke, M.(2024). *The Cybersecurity industry has an urgent talent shortage. Here's how to plug the gap*. Available at: https://www.weforum.org/agenda/2024/04/cybersecurity-industry-talent-shortage-new-report/ [Accessed 27th May 2024].

Minichielo, V. (1990). *In-depth interviewing: Researching People*. p.5. Longman. Cheshire.

Monteith, S,. Bauer, M., Alda, M., Geddes, J., Whybrow, P.C., Glenn, T.(2021) *Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry.* Available at: https://doi.org/10.1007/s11920-021-01228-w [Accessed 27th May 2024].

Monzelo, P,. Nunes, S. (2019). *The Role of the Chief Information Security Officer (CISO) in Organisations.* https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=capsi2019 [Accessed 27th May 2024].

Microsoft (2024). *What is SOAR?* Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-soar [Accessed 27th May 2024].

Misheva, G,. (2023). *Mind the Cyber Skills Gap: a deep dive.* Available at: https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive [Accessed 27th May 2024].

Mughal, A.A.(2022) *Building and Securing the Modern Security Operations Center (SOC).* Available at: https://research.tensorgate.org/index.php/IJBIBDA/article/view/21/20 [Accessed 27th May 2024].

Mwita, K.M. (2022). *Strengths and weaknesses of qualitative research in social science studies*. Available at: https://doi.org/10.20525/ijrbs.v11i6.1920 [Accessed 27th May 2024].

NCISS (2024). *Education & Training*. Available at: https://niccs.cisa.gov/education-training [Accessed 27th May 2024].

NCSC (2024). *What is Cyber security?* Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security [Accessed 27th May 2024].

Nieles, M., Dempsey, Kelley,. Pillitteri, V.Y. (2017) *An Introduction to Information Security.* Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf [Accessed 27th May 2024].

NIST (2020). *Workforce Framework for Cybersecurity (NICE Framework). Revision 1*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf [Accessed 27th May 2024].

NIST (2023). *Cybersecurity Workforce Demand.* Available at: https://www.nist.gov/system/files/documents/2023/06/05/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf [Accessed 27th May 2024].

NIST (2024a). *NICE Framework Components v1.0.0.* Available at: https://www.nist.gov/system/files/documents/2024/03/04/NICE%20Framework%20Components%20v1.0.0_Summary%20of%20Changes_March2024.pdf [Accessed 27th May 2024].

NIST (2024b). *Getting Started with the NICE Framework.* Available at: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/getting-started [Accessed 27th May 2024].

NSF (2024). *Cybersecurity Workforce Data Initiative*. Available at: https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative [Accessed 27th May 2024].

O'Gorman, K., MacIntosh, R.(2015). *Research Methods for Business and Management. A Guide to Writing Your Dissertation.* Second Edition. Oxford: Goodfellow Publishers Limited.

Oplatka, I. (2021). Eleven Pitfalls in Qualitative Research: Some Perils Every Emerging Scholar and Doctoral Student Should be Aware Of! pp. 1882–1885. Available at: https://doi.org/10.46743/2160-3715/2021.4783 [Accessed 27th May 2024].

Palo Alto Networks (2023). *Palo Alto Networks Adds "Bring Your Own AI" Capability To Cortex XSIAM AI-driven Security Operations Platform*. Available at: https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-adds--bring-your-own-ai--capability-to-cortex-xsiam-ai-driven-security-operations-platform [Accessed 27th May 2024].

Palo Alto Networks (2024a). *What is a Security Operations Center* (SOC)? Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc [Accessed 27th May 2024].

Palo Alto Networks (2024b). *Security Analytics: What is Security Analytics?* Available at: https://www.paloaltonetworks.com/cyberpedia/security-analytics [Accessed 27th May 2024].

Palo Alto Networks (2024c). *Strata Cloud Manager.* Available at: https://www.paloaltonetworks.com/company/press/2024/palo-alto-networks-delivers-more-autonomous-cybersecurity-through-copilots-for-strata--prisma-and-cortex-platforms [Accessed 27th May 2024].

Palo Alto Networks (2024d). *Palo Alto Networks Launches New Security Solutions Infused with Precision AI to Defend Against Advanced Threats and Safeguard AI Adoptions*. Available at: https://www.paloaltonetworks.com/company/press/2024/palo-alto-networks-launches-new-security-solutions-infused-with-precision-ai-to-defend-against-advanced-threats-and-safeguard-ai-adoption [Accessed 27th May 2024].

Pedley, D, Borges, T, Bollen, A, Shah, J.N,. (2020). *Cybersecurity Skills in the UK Labour Market 2020.* Available at: https://assets.publishing.service.gov.uk/media/60213acbd3bf7f70c3a49660/Cyber_security_skills_report_in_the_UK_labour_market_2020_V2.pdf [Accessed 27th May 2024].

Petersen, R,. Santos, D,. Smith, M.C,. Wetzel, K.A,. Witte, G. (2020). *NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity (NICE Framework).* Available at:

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf [Accessed 27th May 2024].

Podzins, O,. Romanovs, A. (2019) *Why SIEM is Irreplaceable in a Security IT Environment?* Available at: https://ieeexplore.ieee.org/abstract/document/8732173 [Accessed 27th May 2024].

Polemi, N,. Kioskli, K,. (2023). *Enhancing Practical Cybersecurity Skills: The ECSF and the CyberSecPro European Efforts.* Available at: https://www.researchgate.net/profile/Kitty-Kioskli-2/publication/371992682_Enhancing_practical_cybersecurity_skills_The_ECSF_and_the_CyberSecPro_European_efforts/links/6528e8e92e1ba453041e6ed9/Enhancing-practical-cybersecurity-skills-The-ECSF-and-the-CyberSecPro-European-efforts.pdf [Accessed 27th May 2024].

Rathbun, B.C. (2008). *Oxford Handbook of Political Methodology*. pp. 685-690. Oxford. Oxford University Press.

Roshaidai, S., Afifin, M. (2018). Ethical Considerations in Qualitative Study. Available at: https://doi.org/10.31436/ijcs.v1i2.82 [Accessed 27th May 2024].

Ross, A., Barton, C., Böhme, R., Clayton, R., Hernandez Ganan, C., Grosso, T., Levi, M., Moore, T., Vasek, M.(2019) *Measuring the Changing Cost of Cybercime*. Available at: https://pure.tudelft.nl/ws/portalfiles/portal/54190531/Measuring_the_Changing_Cost_of_Cybercrime_WEIS_1.pdf [Accessed 27th May 2024].

Santos, D (2020). *Back to Basics: Announcing the New NICE Framework*. Available at: https://www.nist.gov/comment/118481 [Accessed 27th May 2024].

Sarker, I.H,. Kayes, A.S.M,. Badsha, S,. Alqahtani, H,. Watters, P,. Ng, Alex. (2020) *Cybersecurity data science: an overview from Machine Learning perspective.* Available at: https://link.springer.com/article/10.1186/s40537-020-00318-5 [Accessed 27th May 2024].

Saunders, M., Lewis, P., Thornhill, A. (2007). *Research methods for business students.* Fourth edition. England: Pearson Education Limited.

Saunders, M., Lewis, P., Thornhill, A. Bristow, A (2019). *Research Methods for Business Students. 8th Edition*. England: Pearson Education Limited. Chapter 4, pp. 144-151.

Scotland, J. (2012). Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology to Methodology and Methods of the Scientific, Interpretive, and Critical Research Paradigms. p.12. Available at: https://files.eric.ed.gov/fulltext/EJ1080001.pdf [Accessed 27th May 2024].

Seidman, I.(2006a). *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences.* 3rd Edition. pp. 10-14. Available at: https://www.researchgate.net/file.PostFileLoader.html?id=563ce2da6225ff3cae8b4590&assetKey=AS%3A292843798188032%401446830810198 [Accessed 27th May 2024].

Seidman, I.(2006b). *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences.* 3rd Edition. pp. 10-14. Available at: https://www.researchgate.net/file.PostFileLoader.html?id=563ce2da6225ff3cae8b4590&assetKey=AS%3A292843798188032%401446830810198 [Accessed 27th May 2024].

Seiter, C (2024). *Check Out the 10 Best Cybersecurity Certifications*. Available at: https://www.forbes.com/advisor/education/certifications/best-cybersecurity-certifications/ [Accessed 27th May 2024].

Soifer, K.L.(2010). Compare and Contrast Inductive and Deductive Research Approaches. Available at: https://bit.ly/3LOwP02 [Accessed 27th May 2024].

Sophos (2024). *What is AI in Cybersecurity?* Available at: https://www.sophos.com/en-us/cybersecurity-explained/ai-in-cybersecurity [Accessed 27th May 2024].

Teoh, C.S., & Mahmood, A.K,. (2017). *Cybersecurity Workforce Development for Digital Economy. The Educational Reviewing,* USA, 2(1), 136-146. Available at: http://dx.doi.org/10.26855/er.2018.01.003 [Accessed 27th May 2024].

Georgescu, T.M,. (2021). *A Study on how the Pandemic Changed the Cybersecurity Landscape.* Available at: http://doi.org/10.24818/issn14531305/25.1.2021.04 [Accessed 27th May 2024].

Toth, P,. (2022). *Cybersecurity – A Critical Component of Industry 4.0 Implementation.* Available at: https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-critical-component-industry-40-implementation [Accessed 27th May 2024].

UK Cyber Security Council (2024). *Our Vision and Mission.* Available at: https://www.ukcybersecuritycouncil.org.uk/about-the-council/vision-and-mission/ [Accessed 27th May 2024].

UK Cyber Security Council (2024). *Routes to and Through a Cyber Security Career.* Available at: https://www.ukcybersecuritycouncil.org.uk/careers-and-learning/ [Accessed 27th May 2024].

Uppal, H. A. M,. Javed, M,. Arshad, M.J.(2014). *An Overview of Intrusion Detection Systems (IDS) along with its Commonly Used Techniques and Classifications.* Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ad2e6f2ddf676cbe22ddaffab23973ce263f7f41 [Accessed 27th May 2024].

Winit-Watjana, W (2016). *Research philosophy in pharmacy practice: necessity and relevance, International Jorunal of Pharmacy Practice,* Volume 24. pp. 428-436. Available at: https://doi.org/10.1111/ijpp.12281 [Accessed 27th May 2024].

Wheatley, S. (2020) *Bridging the Cybersecurity Skills Gap through Artificial Intelligence*. Available at: https://www.fortinet.com/blog/industry-trends/bridging-the-cybersecurity-skills-gap-through-artificial-intelligence [Accessed 27th May 2024].

Yoon Soo, P., Konge, L., Artino, A.R.Jr. (2020). *The Positivism Paradigm of Research*. Available at: https://doi.org/10.1097/ACM.0000000000003093 [Accessed 27th May 2024].

Appendix 1 Interview Questions

Part 1. Awareness of the Global Cybersecurity workforce shortage.

Q. 1 *What do you know about the Global Cybersecurity workforce shortage?*

Q, 2 *Generally where have you seen the impact of the Global Cybersecurity workforce shortage?*

Q. 3 *How have you seen the impact of the Global Cybersecurity workforce shortage in your organisation?*

Part 2. The factors driving the increasing demand for cybersecurity professionals.

Q.1 *Have you seen an increasing demand for Cybersecurity Professionals?*

Q. 2 *What is driving the increasing demand for Cybersecurity Professionals?*

Q. 3 *What were the affects, pre-Covid, Mid-Covid and post-Covid on the demand for Cybersecurity Professionals?*

Part 3. Assess knowledge and perspectives on education and training approaches to addressing the Cybersecurity Workforce Shortage.

Q. 1 *What global bodies are working to help mitigate the Cybersecurity workforce shortage?*

Q. 2 *What educational, training or certification initiatives are working towards mitigating the workforce shortage?*

Q. 3 *How effective are these education and training initiatives in mitigating the Cybersecurity professional workforce shortage?*

Part 4. Examine knowledge and perspectives on the use of AI in mitigating the Cybersecurity Workforce Shortage.

Q. 1 *What do you know about how Artificial Intelligence can be used in Cybersecurity?*

Q. 2 *What roles within Cybersecurity can Artificial Intelligence help with?*

Q. 3 *How effective can Artificial Intelligence be in reducing workload of Cybersecurity Professionals.*