



Matching ESCF Prescribed Cyber Security Skills with the Swedish Job Market: Evaluating the Effectiveness of a Language Model

**Al Ghaith Ahmad
Ibrahim Abd ULRAHMAN**

The authors declare that they are the sole authors of this thesis and that they have not used any sources other than those listed in the bibliography and identified as references. They further declare that they have not submitted this thesis at any other institution to obtain a degree.

Contact Information:

Authors:

Al Ghaith Ahmad

E-mail: alah20@student.bth.se

Ibrahim Abd ULRAHMAN

E-mail: Ibab20@student.bth.se

University advisor:

Dr. Shahryar Eivazzadeh

Department: DIDA

Faculty of Computing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

ABSTRACT

Background: As the demand for cybersecurity professionals continues to rise, it is crucial to identify the key skills necessary to thrive in this field. This research project sheds light on the cybersecurity skills landscape by analyzing the recommendations provided by the European Cybersecurity Skills Framework (ECSF), examining the most required skills in the Swedish job market, and investigating the common skills identified through the findings. The project utilizes the large language model, ChatGPT, to classify common cybersecurity skills and evaluate its accuracy compared to human classification.

Objective: The primary objective of this research is to examine the alignment between the European Cybersecurity Skills Framework (ECSF) and the specific skill demands of the Swedish cybersecurity job market. This study aims to identify common skills and evaluate the effectiveness of a Language Model (ChatGPT) in categorizing jobs based on ECSF profiles. Additionally, it seeks to provide valuable insights for educational institutions and policymakers aiming to enhance workforce development in the cybersecurity sector.

Methods: The research begins with a review of the European Cybersecurity Skills Framework (ECSF) to understand its recommendations and methodology for defining cybersecurity skills as well as delineating the cybersecurity profiles along with their corresponding key cybersecurity skills as outlined by ECSF. Subsequently, a Python-based web crawler, implemented to gather data on cybersecurity job announcements from the Swedish Employment Agency's website. This data is analyzed to identify the most frequently required cybersecurity skills sought by employers in Sweden. The Language Model (ChatGPT) is utilized to classify these positions according to ECSF profiles. Concurrently, two human agents manually categorize jobs to serve as a benchmark for evaluating the accuracy of the Language Model. This allows for a comprehensive assessment of its performance.

Results: The study thoroughly reviews and cites the recommended skills outlined by the ECSF, offering a comprehensive European perspective on key cybersecurity skills (Tables 4 and 5). Additionally, it identifies the most in-demand skills in the Swedish job market, as illustrated in Figure 6. The research reveals the matching between ECSF-prescribed skills in different profiles and those sought after in the Swedish cybersecurity market. The skills of the profiles 'Cybersecurity Implementer' and 'Cybersecurity Architect' emerge as particularly critical, representing over 58% of the market demand. This research further highlights shared skills across various profiles (Table 7).

Conclusion: This study highlights the matching between the European Cybersecurity Skills Framework (ECSF) recommendations and the evolving demands of the Swedish cybersecurity job market. Through a review of ECSF-prescribed skills and a thorough examination of the Swedish job landscape, this research identifies crucial areas of alignment. Significantly, the skills associated with 'Cybersecurity Implementer' and 'Cybersecurity Architect' profiles emerge as central, collectively constituting over 58% of market demand. This emphasizes the urgent need for educational programs to adapt and harmonize with industry requisites. Moreover, the study advances our understanding of the Language Model's effectiveness in job categorization. The findings hold significant implications for workforce development strategies and educational policies within the cybersecurity domain, underscoring the pivotal role of informed skills development in meeting the evolving needs of the cybersecurity workforce.

Keywords: ESCF, ChatGPT, Scraping, Crawler, Prompt Engineering.

| | |
|-------------------------------------------------------------------------------|-----------|
| ABSTRACT | 2 |
| 1. INTRODUCTION | 4 |
| 1.1 BACKGROUND..... | 4 |
| 1.2 SCOPE | 6 |
| 1.3 ETHICAL, SOCIETAL, AND SUSTAINABILITY ASPECTS..... | 6 |
| 1.4 OUTLINE | 6 |
| 2. RELATED WORK..... | 7 |
| 2.1 EUROPEAN CYBERSECURITY SKILLS FRAMEWORK | 7 |
| 2.2 THE CYBERSECURITY WORKFORCE AND SKILLS | 8 |
| 2.3 A PROMPT PATTERN CATALOG TO ENHANCE PROMPT ENGINEERING WITH CHATGPT | 8 |
| 2.4 EVALUATING TOOLS AND TECHNIQUES FOR WEB SCRAPING..... | 9 |
| 3. METHOD..... | 10 |
| 3.1 RESEARCH QUESTIONS | 10 |
| 3.2 DESCRIBING THE RESEARCH METHOD | 10 |
| 3.2.1 <i>Exploring the required skills from ECSF</i> | 10 |
| 3.2.2 <i>Crawling job announcements:</i> | 11 |
| 3.2.3 <i>Prompt engineering and ChatGPT</i> | 13 |
| 3.2.4 <i>Testing ChatGPT's accuracy</i> | 14 |
| 3.3 IMPLEMENTATION AND DESIGN | 17 |
| 3.3.1 <i>Announcements crawler</i> | 17 |
| 3.3.2 <i>Prompt implementation and design</i> | 19 |
| 4. RESULTS AND ANALYSIS | 25 |
| 5. DISSCUSION..... | 35 |
| 6. CONCLUSION AND FUTURE WORK | 38 |
| 6.1 CONCLUSION..... | 38 |
| 6.2 FUTURE WORK..... | 38 |
| 6.2.1 <i>Improving Methodology</i> | 38 |
| 6.2.2 <i>Refinement of Skill Profiling</i> | 39 |
| 6.2.3 <i>Longitudinal Analysis</i> | 39 |
| 6.2.4 <i>Evaluation of Educational Programs</i> | 39 |
| 6.2.5 <i>Collaboration with Industry stakeholders</i> | 39 |
| 6.2.6 <i>Expansion to Other Geographical Contexts</i> | 39 |
| 6.2.7 <i>Integration of Practical Training</i> | 39 |
| 7. REFERENCES | 40 |
| 7. APPENDIX: | 42 |

1. INTRODUCTION

Computer systems have become integral to every facet of our lives, from daily communication to work, recreation, and more. They also control critical infrastructure like electricity, water, and transportation systems. The absence of robust security measures in this digital infrastructure poses a significant risk, potentially leading to cyberattacks. These attacks, increasingly prevalent, threaten to compromise sensitive information of individuals, organizations, and even entire nations [1]. In this context, the proficiency of Language Models (LMs), particularly large-scale ones like ChatGPT, plays a pivotal role. These models have shown promise in automating tasks related to cybersecurity, from threat detection to anomaly identification. Understanding the effectiveness of such models in job profiling and matching is paramount in the quest for a well-equipped cybersecurity workforce. With cyberthreats on the rise, encompassing malicious malware, ransomware, and the advent of advanced persistent threats, the demand for skilled cybersecurity professionals capable of thwarting these attacks has reached unprecedented levels. Consequently, it has become imperative for organizations to cultivate a proficient, knowledgeable, and adequately trained cybersecurity workforce dedicated to safeguarding digital assets and information.

1.1 Background

As stated in the study “The Cybersecurity Workforce And Skills” *“We must not only recognize the need for skills in cybersecurity but must also understand what skills we need in order to ensure that the issue is tackled effectively.”*, [2], yet measuring and determining the competence and capabilities of individuals is a challenging task. There have been many studies that aim to make security procedures more efficient and effective, but do the personnel accomplishing the procedure have enough knowledge and skills to handle that? The area of evaluating the competence of cybersecurity professionals has not received enough attention yet [3]. To address this growing need, it is essential to gain a comprehensive understanding of the required cybersecurity skills, aligning them with industry demands and frameworks. Therefore, in this research, we aim to define the intersection of cybersecurity skills from the European Cybersecurity Skills Framework (ECSF) point of view and the Swedish cybersecurity market demand. To achieve that, we will conduct a review of the ECSF framework to address the proper cybersecurity skills. By implementing a crawler for gathering information about IT-security related job announcements published on the Swedish Employment Agency’s website, to address market demand. The collected announcements will be categorized using Large Language model (LLM), specifically ChatGPT. ChatGPT will be employed to perform job categorization tasks, with a subsequent assessment of its accuracy to measure its effectiveness in this context. The distinctiveness of this project is that it will provide a better understanding of the skills necessary for the cybersecurity workforce from ECSF’s framework and Swedish cybersecurity market demand using modern methods such as web scraping and Natural Language Processing (NLP) that are used by ChatGPT. Exploring the concepts of web scraping/crawling and ChatGPT is necessary to understand their underlying mechanisms and significance.

Important terms

a. Web scraping/crawling:

Web scraping is used to retrieve unstructured data from the World Wide Web (WWW) and convert it into a structured format or store it in an external database. This technique is widely recognized as an effective means of collecting big data, particularly in scenarios where acquiring substantial volumes of data holds significant importance [5]. Web scraping software functions as a bot or web crawler that directly accesses website data over the Hypertext Transfer Protocol or utilizes a web browser to collect exact data from that website. The fetched data is stored in a centralized local database or spreadsheet for future utilization and analysis purposes [6]. Web scraping finds utility in numerous scenarios, encompassing content scraping, weather forecast information, comparing price changes, detecting website changes, and collecting product reviews. For instance, on a microscale, social media feeds can be collectively scraped to explore public sentiments and identify influential figures [7]. On a macro-level, the metadata of almost every website undergoes constant scraping to construct Internet search engines like Bing or Google Search [8]. This software will enable us to systematically extract pertinent information from job listings available in the Swedish market. The gathered data will serve as the foundation for subsequent analysis and investigation, further enhancing our understanding of the job landscape in Sweden and its related required skills.

b. ChatGPT:

ChatGPT is an advanced language model created and developed by Open AI [9] that has attracted a lot of interest in the natural language processing (NLP) community. It represents an innovation in the creation of text that mimics human conversation. The model is based on the architecture of Generative Pre-trained Transformer 3.5 (GPT-3.5), which uses deep learning methods to understand and produce contextually appropriate answers.

ChatGPT functions as a generative language model. It gains knowledge from a big dataset of various text sources, allowing it to pick up a variety of language patterns and information within the right context [9]. Due to its extensive training data, ChatGPT can provide replies that make sense given the input it receives [10]. In the context of this research project, ChatGPT will be employed for the task of classifying and categorizing skills into different profiles. By utilizing ChatGPT for skill classification, this research aims to streamline the process of identifying and organizing the skills mentioned in each job related to cybersecurity in the Swedish job market into one of the twelve profiles defined by the ECSF framework. It is important to note that large language models like ChatGPT have limitations and can occasionally produce incorrect or nonsensical responses. It is always advisable to critically evaluate the outputs and use human judgment to verify the accuracy and appropriateness of the generated content [9]. That is why we did a validation test on some of ChatGPT's classification output by comparing it to our own manual classification.

So, the goal of our study is to help the employer community to address the important skills and knowledge of cybersecurity besides providing a more extensive understanding of the capabilities and competencies in cybersecurity. In addition, testing the accuracy of the LLM, ChatGPT, in classification tasks. This will reflect indirectly on large part of the society by strengthening and securing digital infrastructure and assets through the development of a well-informed and highly skilled cybersecurity workforce as well as filling the job positions that are highly needed and required on the Swedish market with these skilled personnel. This study will also help educational institutions and organizations to refine their curricula and training programs to align with contemporary cybersecurity requirements, thus fostering a more effective educational environment. Last but not least this project will contribute to the sustainability of digital assets and infrastructure by identifying what skills, knowledge and training should be mastered by the cybersecurity workforce. This will help to enhance the overall security posture of organizations and prevent cyber-attacks, thereby reducing the negative impacts of cyber security incidents on the environment, economy, and society.

1.2 Scope

This study focuses on how the recommended skills in the European Cybersecurity Skills Framework (ECSF) match the needs of the Swedish cybersecurity job market. It closely reviews the skills mentioned in ECSF and conducts an in-depth analysis of the Swedish job landscape. The study further extends to evaluate the effectiveness of a Language Model (ChatGPT) in job categorization based on ECSF profiles. It provides valuable insights for educational institutions and policymakers seeking to enhance workforce development strategies in the cybersecurity sector.

1.3 Ethical, societal, and sustainability aspects

Ethical considerations guide our approach at every step, including the utilization of a web crawler. We ensure responsible data handling, respecting privacy, and legal regulations, and minimizing any potential negative impact on the websites crawled. Transparent and fair practices are maintained throughout the data collection process.

By providing a more extensive understanding of the capabilities and competencies required in this domain, our research endeavors to indirectly benefit a significant portion of society such as students, teachers and job seekers. Strengthening and securing digital infrastructure and assets are pivotal outcomes, contributing to a well-informed and highly skilled cybersecurity workforce. Last but not least this project will also contribute to the sustainability of the digital assets and infrastructure by identifying what skills, knowledge and training should be mastered by the cybersecurity workforce. This will help to enhance the overall security posture of organizations and prevent cyber-attacks, thereby reducing the negative impacts of cyber security incidents on the environment, economy, and society.

1.4 Outline

The thesis begins with an introduction that provides the background of the study, including key terms such as web scraping/crawling and ChatGPT. Then, the scope of the thesis is defined to specify what the research will cover, giving clear boundaries and direction to the study. This outline section shows how the research is structured and describes the flow of information. In the related work section, various sources are described in relation to this study. These include the European Cybersecurity Skills Framework (ECSF), Steven Furnell's work on the cybersecurity workforce and skills, a pattern catalog for enhancing prompt engineering with ChatGPT and an evaluation of tools and techniques used for web scraping. The method section defines the research questions and outlines the research approach. This includes exploring the required skills from the ECSF, crawling job announcements, implementing prompt engineering with ChatGPT, and conducting tests. The validity and reliability of each step in the process are assessed, covering aspects such as ECSF alignment, announcement crawling, and prompt design. The results and discussion section presents the findings of the study and discusses the results obtained through the employed methods. Following this, a summary of the main outcomes and suggestions for future research is presented. This section proposes several directions for further exploration, including longitudinal analysis, evaluation of educational programs, collaboration with industry partners, expansion to other geographical contexts, and integration of practical training. Finally, the references, appendix, and any supplementary materials are provided.

2. RELATED WORK

2.1 European Cybersecurity Skills Framework

ENISA or as known The European Agency for Cybersecurity, is an agency that was built in 2004 to raise awareness and set standards for cybersecurity in the European union. The main goal of ENISA is to:

- Improve European Union policies about cybersecurity to maintain a high level of cybersecurity.
- Set standards to keep products, services, and processes that use modern technology trustworthy and secure [15][4].

The increasing number of cyberthreats and the shortage of workforce in the cybersecurity field drove ENISA to develop a framework called the European Cybersecurity Skills Framework (ECSF), which was published in its final version in April-2022 by the ECSF Ad Hoc working group. The main purpose of developing the ECSF is to create a common language that describes the cybersecurity professionals in both demand and supply manner in the European Union, pointing out the essential skills that improve different cybersecurity roles, and establishing harmony between cybersecurity training, education, and workforce development. Additionally, increasing the level of security in the EU by helping the organizations to develop and provide appropriate education programs, individuals to choose the right career path and recruiters to hire suitable persons in the right positions. The ECSF divides the cybersecurity industry into 12 professional roles and concisely outlines the unique characteristics of each role. The ECSF was developed using a research-based and collaborative methodology by different actors, where a variety of learning program providers and employers contributed to the input data of the framework, While the research part was done by many experts in numerous areas within cybersecurity, where they analyzed existing frameworks, researched the demand in the market, and identified the common perspectives among professionals, The framework was also reviewed, enhanced, and improved by other stakeholders to comply with the existing standards in the EU, such as the information and communication technology framework (ICT). Furthermore, ENISA offers an implementation guide for applying the framework in different areas such as educational programs, employers and for individual seeking jobs [4][16]. Part of the aim of our research is to identify the cybersecurity skills that are most in demand in the Swedish cybersecurity market. Meanwhile, the European Cybersecurity Skills Framework (ECSF) summarizes the most essential skills for 12 distinct roles in cybersecurity. On the other hand, the difference between this research and the ECSF research is that the skills outlined in the ECSF are based on expert research and organizational perspectives, while the skills extracted in this research are based on the needs of employers in the Swedish cybersecurity market.

2.2 The Cybersecurity Workforce And Skills

The need for cybersecurity has grown with the expansion of digitization, where protecting systems and data from attacks is crucial for businesses and organizations. Academic degrees and professional qualifications with a focus on cybersecurity are increasingly prevalent nowadays, but the field of cybersecurity covers a wide range of skills, including technical and non-technical aspects, which make it difficult to identify the right skills, qualifications and certifications required in a specific role. This reason gave motivation to study the cybersecurity landscape to provide a method on how organizations can effectively identify the right skills needed in different roles, besides helping to overcome the lack of cybersecurity skills. the method used to address this problem is by examining and exploring the differences in cybersecurity levels, where in the research the cybersecurity skills have been divided into four parts:

- Academic qualifications
- General professional certifications
- Role based certification.
- Vendor or technology-based certification.

The four parts are also categorized into theoretical and practical qualifications, where academic programs are primarily considered as the most theoretical qualification while the technology-based certification is the most practical qualification. Through an analysis of various certifications within four different categorizations, the research has successfully been able to categorize well-known cybersecurity certifications according to cybersecurity seven professional roles [2]. This research and “The Cybersecurity Workforce And Skills” study share a common focus on investigating cybersecurity skills, while a distinguishing factor between the two is the approach, where the research “The Cybersecurity Workforce And Skills” defines skills based on known cyber security certifications. On the other hand, our work is centered around defining skills according to the twelve profiles of the European Cybersecurity Skills Framework (ECSF).

2.3 A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT

The Conversational large language models (LLMs) revolution in recent years has resulted in conversational AI chatbots that are available for everyone to use around the globe, e.g., CHAT-GPT. The interaction with these chatbots is usually done through prompt input, where the LLM generates a response based on the prompt input. LLMs have proven to be useful in various tasks like automating processes, generating code, and assisting in learning, but to fully utilize their capabilities, it is important to provide high-quality prompts that effectively guide the LLMs. well-designed prompts could maximize the benefits of using these LLMs and enhance their performance by responding with desired output, efficiently and accurately to provided instructions. This study defines prompt patterns and performs comparison with existing known software patterns, while also outlining a documentation method that is based on software patterns documentation standard. The authors describe and explain 16 commonly used patterns that have been applied to solve common problems [17]. The research also provides guidance on how to integrate multiple patterns into new prompts which aligns with our research approach. In our study, we employ a combination of prompt patterns to develop a Job classification prompt. In addition, in our research, we follow the documentation standard to facilitate explaining and understanding of the Job classifier prompt.

2.4 Evaluating Tools And Techniques For Web Scraping

The internet has become a large and valuable source of data in today's world. Organizing and analyzing this data can provide significant benefits to various fields, such as the advertising industry and research in different fields, but manually collecting these large amounts of data is time-consuming and impractical. This is where web crawlers come into play, where it can automate the process and systematically gather data from the internet, according to specific criteria chosen by us. By collecting and structuring the data, web crawlers help us explore, filter, and organize unstructured information and extract meaningful insights. There are several techniques and tools used to crawl and scrape the web, which create a challenge for developers to determine which technique/tool is most suitable in terms of speed, ease of use and reliability. This research deals with the problem by comparing and evaluating 12 tools built with different programming languages. The research evaluated different tools, and one of them was Selenium. After examining the results, we concluded that selenium was the suitable tool to use in our research which created relation to our research but the differences between our implementation and the referenced research implementation of Selenium is that we used Selenium to collect job announcements from a single website, whereas the referenced study utilized Selenium to scrape data from 100 different websites, conducting 100 scrapes on each website.

3. METHOD

In this section, we discuss utilizing a combination of the qualitative and quantitative research method to answer the research questions, where the qualitative method is employed by conducting a thorough review on the ECSF to analyze and extract recommended cybersecurity skills and profiles. On the other hand, the quantitative method is employed to collect, categorize, and conduct statistical analysis of the most required ECSF skills in cybersecurity job announcements on the Swedish job agency website.

The objectives of the study are:

- Investigate the European Cybersecurity Skills Framework (ECSF) comprehensively to understand its key components and skill profiles.
- Analyze the specific skill demands within the Swedish cybersecurity job market, considering the unique requirements and trends.
- Identify commonalities between the skill sets outlined in the ECSF and the skills in demand within the Swedish cybersecurity job market.
- Evaluate the effectiveness of a Language Model (ChatGPT) in accurately categorizing cybersecurity jobs based on ECSF profiles.
- Offer recommendations for educational institutions and policymakers to enhance workforce development based on the identified common cybersecurity skills.

3.1 Research questions

- 1- What are the common cybersecurity skills between the ECSF and Swedish cybersecurity job market demand?
- 2- How effective is the Language Model (LLM) in comparison to human agents in achieving accurate job categorization based on ECSF profiles?

3.2 Research methods

To address the first research question, a case study approach was employed. This involved an in-depth examination and analysis of specific cases, focusing on the alignment between ECSF-prescribed cybersecurity skills and the actual skill demands observed in the Swedish job market.

For the second research question, an experimental method was employed. This involved a controlled and systematic evaluation, utilizing the Language Model (ChatGPT) to classify job positions based on ECSF profiles. Simultaneously, human agents manually categorized jobs, serving as a benchmark for evaluating the accuracy of the Language Model. This experimental setup allowed for a rigorous assessment of the Language Model's performance in job categorization.

3.3 Describing the research method

3.3.1 Exploring the required skills from ECSF.

The first phase of this research is to examine the ECSF to identify the suggested skills for cybersecurity. We chose the ECSF because it was created by the Ad Hoc working group in the European cybersecurity Agency, as mentioned earlier. The ECSF Ad Hoc working group is a group of experts in cybersecurity from different sectors of the industry. The group advises ENISA through its framework about the most needed cybersecurity skills to ensure securing modern technology in Europe. The framework is described according to the creators as it is designed in a way to be:

- Simple and comprehensive: easy to implement but detailed for deep insights.
- Flexible and scalable: modifiable so it fits the stakeholders.
- Open and impartial: available and accessible for everyone.
- European: complies with the European standards [4].

The reasons above make it a trustworthy and suitable framework for our research goals and objectives. After exploring the skills in the ECSF, they will be used to study the Swedish cybersecurity market by crawling job announcements and classifying it according to ECSF skills to extract most required cybersecurity skills.

The framework is a set of cybersecurity skills and roles defined by experts within different areas of cybersecurity (Ad Hoc Working Group) [4]. The ECSF identifies the competencies, knowledge, and skills that are necessary for different cybersecurity professionals. The set consists of 12 typical role profiles in the cybersecurity field, where each role profile contains the following:

- Alternative title
- Summary statement
- Mission
- Deliverable(s)
- Main task(s)
- Key skills(s)
- Key knowledge
- E-Competences (from e-CF) is the European competence framework for information and communication technology ICT.

The properties mentioned above are defined in a flexible manner so that stakeholders can alter them to fit their needs. The framework also includes soft skills (behavioral skills) that are also necessary to achieve the professional standard role definition, e.g., A Chief Information Security Officer (CISO) should have high abilities of communication and reporting to achieve the role's mission. Ethics of the role is another element considered in the ECSF where it involves making decisions that are compatible with role values and ethically acceptable [4].

In this research, we mainly focus on the key skills mentioned in the framework explanation above, where these skills will be collected, organized, and studied systematically for each role.

3.3.2 Crawling job announcements:

To answer the first research question, we'll employ a Python-based web crawler using Selenium. This tool will extract specific information about cybersecurity jobs from the Swedish Employment Agency's website. This systematic data collection method enables us to analyze trends and skill requirements in the Swedish cybersecurity job market. In this study, the selected information that will be retrieved by the crawler are job title, date of publication, announcement link and the job's description including the required skills. This data will then be stored on a predetermined database for further analysis and as an input to ChatGPT.

I. Python:

At the moment of writing this thesis, Python is the most popular programming language in the world according to TIOBE index [11] and the Popularity of Programming Language index (PYPL) [12].

| TIOBE Index | | | | | | PYPL Index (Worldwide) | | | | |
|-------------|------------|----------|------------------------|-----------|----------|------------------------|----------|------------------------|---------|----------|
| Jun 2022 ▲ | Jun 2021 ◆ | Change ◆ | Programming language ◆ | Ratings ◆ | Change ◆ | Jun 2022 ▲ | Change ◆ | Programming language ◆ | Share ◆ | Trends ◆ |
| 1 | 2 | ↑ | Python | 12.20% | +0.35% | 1 | | Python | 27.61 % | -2.8 % |
| 2 | 1 | ↓ | C | 11.91% | -0.64% | 2 | | Java | 17.64 % | -0.7 % |
| 3 | 3 | | Java | 10.47% | -1.07% | 3 | | JavaScript | 9.21 % | +0.4 % |
| 4 | 4 | | C++ | 9.63% | +2.26% | 4 | | C# | 7.79 % | +0.8 % |
| 5 | 5 | | C# | 6.12% | +1.79% | 5 | | C/C++ | 7.01 % | +0.4 % |
| 6 | 6 | | Visual Basic | 5.42% | +1.40% | 6 | | PHP | 5.27 % | -1.0 % |
| 7 | 7 | | JavaScript | 2.09% | -0.24% | 7 | | R | 4.26 % | +0.5 % |
| 8 | 10 | ↑ | SQL | 1.94% | +0.06% | 8 | ↑↑↑ | TypeScript | 2.43 % | +0.7 % |
| 9 | 9 | | Assembly language | 1.85% | -0.21% | 9 | ↓ | Objective-C | 2.21 % | +0.1 % |
| 10 | 16 | ↑↑ | Swift | 1.55% | +0.44% | 10 | ↓ | Swift | 2.17 % | +0.4 % |
| 11 | 11 | | Classic Visual Basic | 1.33% | -0.40% | 11 | ↑↑ | Matlab | 1.71 % | +0.2 % |
| 12 | 18 | ↑↑ | Delphi/Object Pascal | 1.32% | +0.26% | 12 | ↓↓ | Kotlin | 1.57 % | -0.2 % |

Figure 1. Python popularity ranking among programming languages.

Python is classified as a strongly typed language since the compiler actively monitors the variable types and ensures that operations are performed on compatible data. This feature helps prevent typing errors during runtime. Python is comparatively more flexible than other strongly typed languages like Perl, allowing variables to be reassigned to different names [13]. Additionally, Python offers an extensive standard library encompassing a wide range of tools, including Selenium. During the evaluation process for the programming language to be employed in this project, multiple alternative programming languages were considered. The final decision to adopt Python was driven by two key factors: the team's previous experience with the language and the existence of the Selenium library, which offers robust functionality for web crawling and automation purposes.

II. Selenium:

Selenium is a widely used open-source framework for web automation and testing, known for its ability to mimic human browsing. It provides tools and modules for browser interaction, enabling tasks like form filling and data extraction. Compatible with multiple programming languages, including Python, C#, JavaScript, Ruby, and Java [14], Selenium WebDriver is the preferred tool for high-level browser interaction, allowing user-like actions and element capture. Our project will use ChromeDriver as WebDriver to automate tasks on the Swedish Employment Agency's website, extracting cybersecurity job details and storing them in a local database. The choice of Selenium was based on a thorough evaluation of available web scraping tools and techniques, with the author's recommendation for Python users and non-speed-critical tasks [5].

III. Visual Studio Code:

We used Visual Studio Code (VS Code) for coding the Python and Selenium-based crawler. Its robust support for Python development, including syntax highlighting, IntelliSense, and code debugging, provided an excellent coding environment. The integrated terminal in VS Code allowed for easy execution and monitoring of the crawler script. This streamlined implementation facilitated seamless integration with Selenium and efficient data extraction from web pages.

IV. Requirement specification:

The development process of a project relies on the creation of comprehensive requirement specifications, which outline the necessary deliverables based on previously defined goals. It is crucial to establish a well-defined requirement specification to provide a clear direction and purpose for the development phase. These specifications articulate the objectives that must be achieved upon project completion, guiding us as a team towards the desired result.

3.3.3 Prompt engineering and ChatGPT

After crawling the jobs, we will use prompt engineering to create classifier prompt with the help of ChatGPT. prompt engineering is designing a set of instructions used to decide how an LLM model should behave. With prompt engineering, we can specify how a user can interact with an LLM, automate processes, manipulate data in a specific way, customize and limit outputs, or essentially apply rules to the behavior, processing, and interaction of LLMs [17]. In this research, prompt engineering is going to be used to design/program ChatGPT to classify job announcements according to specified set of skills (ECSF profiles). ChatGPT has gained significant attention among researchers and has been utilized in studies focused on natural language processing, because of that we considered it as suitable for classification task in this research [17]. The prompts used in this research are based on the research “**A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT**” where the design and technique is a combination of patterns explained in the research. The jobs collected from Crawling phase will be ran into the classifier so it will classify it according to the predefined skills.

3.3.4 Testing ChatGPT's accuracy

An experiment will have been conducted to calculate the accuracy of the ChatGPT classification ability. The experiment started by gathering a dataset consisting of 30 job announcements. These announcements have been carefully analyzed and categorized by humans (Ibrahim and Al-Ghaith) into one of the 12 profiles outlined in the ECSF. Then human classification has been compared to ChatGPT classification.

To ensure the reliability of our findings, we included various scenarios in our tests with different factors that might affect classification accuracy. The test cases did cover the following situations, such as:

- Including diverse jobs that belong to each of the different profiles.
- Job announcements written in both English and Swedish languages.
- Job descriptions of varying lengths (short and long)
- Jobs that are unrelated to cybersecurity
- Jobs that include IT and security terms but are not directly related to cybersecurity.
- Jobs that involve a combination of skills from multiple profiles.

By covering these different cases, we could evaluate the **accuracy** of ChatGPT in difficult scenarios and test its ability to accurately classify job announcements within the given context.

The table below (Table 1) shows the results of the evaluation test and contains the following:

- Job title: the job title written in a job announcement.
- ChatGPT: The classification by LLM ChatGPT
- Ibrahim: Ibrahim's classification of the job description
- Al-Ghaith: Al-Ghaith's classification of job description

| | Job Title | ChatGPT | Ibrahim | Al Ghaith |
|---|--------------------------------------------|-----------------------------------------------------------|-------------------------------------------|-------------------------------------------|
| 1 | Information Security Manager | Classification: Chief Information Security Officer (CISO) | Chief Information Security Officer (CISO) | Chief Information Security Officer (CISO) |
| 2 | Digital Forensic Incident Responder (DFIR) | Classification: Cyber Incident Responder | Cyber Incident Responder | Cyber Incident Responder |
| 3 | Security Compliance Officer | Classification: Cybersecurity Risk Manager | CYBER LEGAL, POLICY & COMPLIANCE OFFICER | CYBER LEGAL, POLICY & COMPLIANCE OFFICER |
| 4 | Threat Hunter, SOC L3 | Classification: Cyber Threat Intelligence Specialist | CYBER THREAT INTELLIGENCE SPECIALIST | CYBER THREAT INTELLIGENCE SPECIALIST |
| 5 | Cyber Security Architect | Classification: Cybersecurity Architect | CYBERSECURITY ARCHITECT | CYBERSECURITY ARCHITECT |
| 6 | Cybersecurity Auditor | Classification: Cybersecurity Auditor | CYBERSECURITY AUDITOR | CYBERSECURITY AUDITOR |
| 7 | Software Security Coach | Classification: Cybersecurity Educator | CYBERSECURITY EDUCATOR | CYBERSECURITY EDUCATOR |
| 8 | DevSecOps Engineer | Classification: Cybersecurity Implementer | CYBERSECURITY IMPLEMENTER / ARCHITECT | CYBERSECURITY IMPLEMENTER |
| 9 | Forskare inom cybersäkerhet | Classification: Cybersecurity Researcher | CYBERSECURITY RESEARCHER | CYBERSECURITY RESEARCHER |

| | | | | |
|----|------------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------------------------|
| 10 | Security Risk Manager | Classification: Cybersecurity Risk Manager | CYBERSECURITY AUDITOR | Cybersecurity Risk Manager |
| 11 | Forensic Investigator | classification: No match found | No match found (non-Digital forensics investigator) | Not Relevant |
| 12 | Senior penetrationstestare | Classification: Penetration Tester | PENETRATION TESTER | PENETRATION TESTER |
| 13 | IT-tekniker / Supporttekniker | Classification: No match found | Supporttekniker (No match found) | Not Relevant |
| 14 | Software Engineer (C++) | Classification: Cybersecurity Implementer (some skills match, but not all) | Software Developer (No match found) | weakly relevant or Implementer |
| 15 | Vacuum System Technician | Classification: No match found | Vacuum System Technician (No match found) | Vacuum System Technician (No match found) |
| 16 | IT Business Analyst for Digital Identity | Classification: Cybersecurity Implementer (some skills match but not all) | IT Business Analyst for Digital Identity (No match found) | Implementer or Architect |
| 17 | Cyber Security konsult | Classification: Cybersecurity Implementer | CYBERSECURITY IMPLEMENTER / AUDITOR | Many roles : Implementer, Educator, Risk Manager or Pen tester |
| 18 | Cloud Security Engineer - Fully Remote | Classification: Cybersecurity Implementer | CYBERSECURITY IMPLEMENTER | IMPLEMENTER & ARCHITECT |
| 19 | Junior SOC-ingenjör | Classification: Cyber Incident Responder | Cyber Incident Responder | Cyber Incident Responder |
| 20 | Senior Cyber Security Consultant | Classification: Chief Information Security Officer (CISO) | CYBERSECURITY AUDITOR/ CYBER THREAT INTELLIGENCE SPECIALIST | CYBERSECURITY RISK MANAGER |
| 21 | IT Security Consultant / Officer | Classification: Cybersecurity Architect | CYBERSECURITY RISK MANAGER | ARCHITECT & AUDITOR |
| 22 | Network Security Consultant - F5 | Classification: Cybersecurity Implementer | CYBERSECURITY IMPLEMENTER | CYBERSECURITY IMPLEMENTER |
| 23 | Security Consultant | Classification: Cybersecurity Implementer | CYBERSECURITY IMPLEMENTER | CYBERSECURITY IMPLEMENTER |
| 24 | Protective Security Operator | Classification: No match found | Protective Security Operator (No match found) | Not Relevant |
| 25 | Security Software Developer | Classification: Cybersecurity Architect | CYBERSECURITY ARCHITECT | CYBERSECURITY |

| | | | | |
|----|-------------------------------|----------------------------------------------|--------------------------------------------------------|----------------------------------------------------|
| | | | | IMPLEMENTER & ARCHITECT |
| 26 | IT-Security Specialist | Classification: Cybersecurity Implementer | CYBERSECURITY IMPLEMENTER / AUDITOR | CYBERSECURITY IMPLEMENTER & ARCHITECT |
| 27 | Microsoft Security Consultant | Classification: Cybersecurity Architect | CYBERSECURITY ARCHITECT | CYBERSECURITY IMPLEMENTER & ARCHITECT |
| 28 | Senior Security Consultant | Classification: Penetration Tester | Penetration Tester / CYBERSECURITY RESEARCHER | Threat intelligence specialist & implementer |
| 29 | Experienced Ethical Hacker | Classification: Penetration Tester | Penetration Tester | Penetration Tester |
| 30 | IT-Säkerhets specialist | Classification: Penetration Tester | CYBER THREAT INTELLIGENCE SPECIALIST | Penetration Tester & Incident Responder |

Table 1. Comparing ChatGPT classification to human classification

The accuracy of ChatGPT is determined by comparing its classification to human classification (Ibrahim and Al-Ghaith). Since humans may have different viewpoints when classifying job descriptions, we've established a method to make this comparison more reliable, where Ibrahim takes a strict classifying approach, allowing less tolerance based on the differences when classifying job descriptions to ECSF profiles. On the other hand, Al-Ghaith adopts a softer perspective, allowing for greater tolerance in the classification. Each comparison results in a binary outcome: 1 indicates a match between the human and ChatGPT classification (meaning they agree on the job description), while 0 indicates a non-match. We then calculate the average of these match results to obtain a more precise measure of accuracy.

3.4 Implementation and Design

3.4.1 Announcements crawler

The implemented Python crawler shown in (appendix 1) utilizes the Selenium library to extract information about cybersecurity jobs from the Swedish Employment Agency's website and store this information on a local database. When designing the crawler code, a systematic approach was followed to ensure clarity and maintainability. To visualize the logical flow and structure of the code, a flowchart was created and is shown in figure 2. The flowchart provided a graphical representation of the sequential steps and decision points involved in the data extraction process as well as storing it. By drawing this flowchart, it became easier to identify inconsistencies, perform analysis and spot areas of improvement in the code's design. Flowcharts serve as an effective tool for users to uphold appropriate documentation standards during project development [20]. In addition to the flowchart, a UML (Unified Modeling Language) sequence diagram was utilized to illustrate the dynamic interactions between different components and objects in the code. The sequence diagram depicted the chronological order of method calls and data exchanges between the web driver, web elements, database, and the data collection process. By incorporating both the flowchart and the UML sequence diagram into the design of the crawler code, several benefits were realized. Firstly, the flowchart served as a visual aid, enabling developers to comprehend the overall structure and flow of the code immediately. It facilitated code maintenance and debugging by providing a comprehensive overview of the code's logic. Secondly, the UML sequence diagram helped in understanding the runtime behavior and interactions of the code's components. It aided in identifying potential performance bottlenecks or areas where optimizations could be applied.

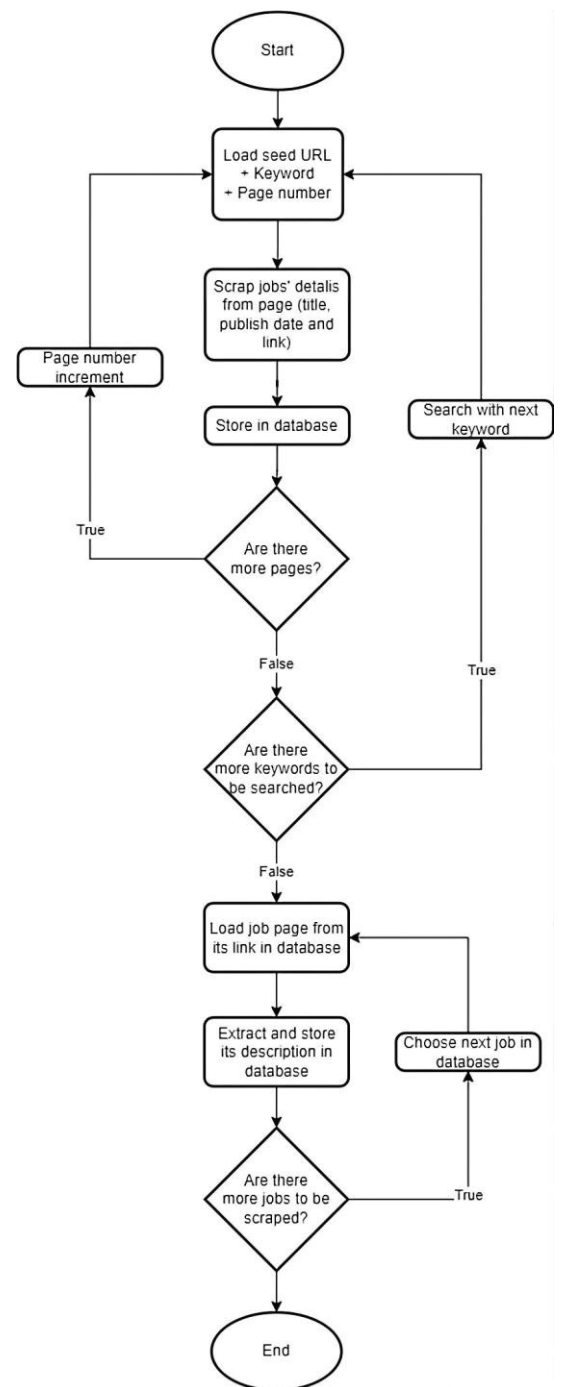


Figure 2: Crawler flowchart

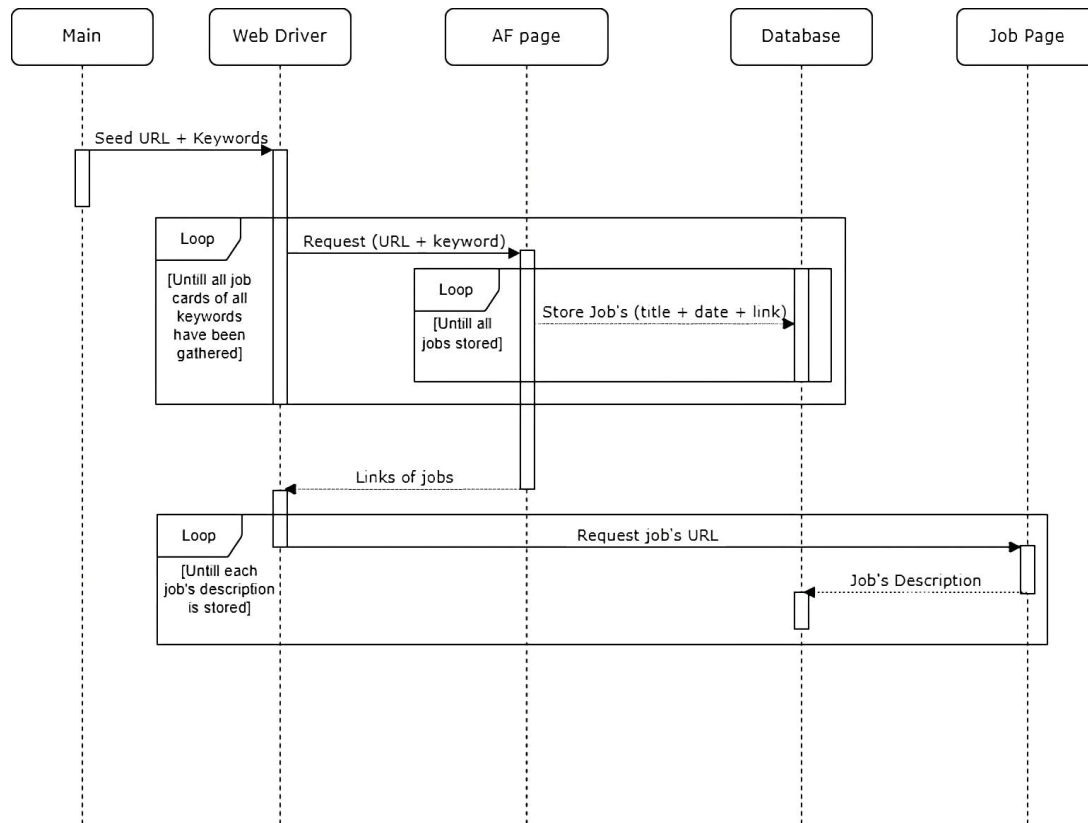


Figure 3: UML Sequence diagram of the Crawler

- The crawler configures the Selenium WebDriver with the Chrome driver for website interaction. It initializes empty lists to store job information and track visited links. Relevant keywords like 'Cyber security', 'IT-Security', 'it-säkerhet', and 'analyst' are defined to search for relevant job postings.
- The crawling process involves iterating over keywords, visiting multiple pages of job listings. URLs are dynamically constructed with the specified keyword and page number. URLs have the following form: "https://arbetsformedlingen.se/platsbanken/annonser?q={keyword}&page={number}". Each page is loaded using WebDriver with a three-second pause for complete loading.
- Within each page, the crawler identifies job elements using CSS selectors, extracting key details like job title, date, and link. Data is then checked and compared by link to prevent duplicates.
- To filter out unrelated jobs, a separate process is employed. The crawler checks each job's title against a list of predefined related keywords. If a relevant keyword is identified or is part of the title, and it's not a duplicate, the job is considered relevant and added to the final list.
- The crawler then navigates to each job's page, waits for three seconds for full loading, and extracts the description using a CSS selector, adding it to the corresponding job information.
- Once all data is collected, the crawler terminates the WebDriver session. Finally, job information is stored in a local JSON file named 'data.json'.

To ensure the accuracy and reliability of the crawler's results, several conditions and requirements were defined for manual testing and validation. These conditions encompassed the following aspects:

- **Search and Collection:** The crawler was expected to retrieve data from all specified keywords. This entailed navigating through various search pages associated with each keyword and extracting essential information such as the job title, date of publication, and corresponding job link. The extracted data would then be stored in a local database for further analysis.
- **Preventing Duplicates:** To avoid redundancy, the crawler was designed to check if a job entry had already been collected before saving it to the database.
- **Description Extraction:** The crawler navigated to each job's page using its link and extracted the core job description. Sensitive information like emails and phone numbers were intentionally excluded. This restriction aimed to respect privacy and prevented the inclusion of sensitive information in the dataset.

As part of the manual testing process, a specific keyword, "Cybersäkerhet" was selected to evaluate the crawler's performance. The aim was to assess the accuracy and completeness of the data collected from the Swedish Employment Agency's website. The test involved comparing the number of jobs that appeared on the website for the given keyword with the number of jobs stored in the local database by the crawler. Furthermore, to ensure the integrity of the extracted job details, an overview examination was conducted to verify the correctness of the data. This involved reviewing random job entry's information, such as the job title, date of publication, and job link to make sure it matches the original information on the website. As well as ensuring that no empty cells were present on the database. By meticulously assessing the extracted data, any discrepancies or missing information were identified, enabling the evaluation of the crawler's ability to accurately extract and store job details.

3.4.2 Prompt implementation and design

In this section, we will describe the approach we used to develop the prompts used in this research. As mentioned earlier, our prompt development method is based on the research paper "A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT." which in turn is based on software patterns that are commonly used in software engineering.

Software patterns are designed patterns that are used to solve recurring problems within software development. Software patterns usually follows the following documentation standard, each pattern consist of:

- A name and classification
- The intent
- The motivation
- The structure and participants.
- Example code
- Consequences

The documentation standard mentioned above contains an explanation of the problem, implementation guide, information of pros and cons of implementing the solution as well as an example of how to apply the pattern.

In the research **A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT**, there are definition for prompt patterns that are similar to the Software patterns. The prompt patterns defined in the research is a solution for different repeated problems when working with LLM models. The solution provided by the prompt patterns mainly targets the improvement of the conversational LLM, where it helps to produce more logical and coherent responses to user inputs [17]. In the research, it was also suggested a structure of documentation of the prompt pattern. The structure is proceeded from the Software pattern but with slight changes, the pattern is explained in the following table:

| Term | |
|-----------------------------|------------------------------------------------------------------------------------------|
| Name and classification | Prompt pattern identification and categorization |
| Intent and context | Describing the problem and goals of the prompt pattern |
| The motivation | Describing the problem and goals of the prompt pattern |
| The structure and key ideas | Fundamental contextual information provided by the prompt pattern |
| Example implementation | Practical demonstration of how the prompt pattern is applied in the appendix |
| Consequences | Pros and cons of applying the pattern and guidance for adapting it to different contexts |

Table 2. Prompt pattern documentation standard

An initial classification table was also created in the research, the classification table categorized the prompts based on its properties:

| Pattern Category | Prompt Pattern |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------|
| Input Semantics | <i>Meta Language Creation</i> |
| Output Customization | <i>Output Automater</i> <i>Persona</i> <i>Visualization Generator</i> <i>Recipe</i> <i>Template</i> |
| Error Identification | <i>Fact Check List</i> <i>Reflection</i> |
| Prompt Improvement | <i>Question Refinement</i> <i>Alternative Approaches</i> <i>Cognitive Verifier</i> <i>Refusal Breaker</i> |
| Interaction | <i>Flipped Interaction</i> <i>Game Play</i> <i>Infinite Generation</i> |
| Context Control | <i>Context Manager</i> |

Figure 4: Patterns categories and example of prompt

- **Input semantics:** prompts are utilized when the input data is poorly structured and does not follow a specific pattern. These prompts guide the LLM in analyzing the input data to generate a response that is meaningful.
- **Output customization:** prompts categorized here are responsible for formatting and structuring the output in a specific form. For instance, using personas to generate a response based on a chosen role.
- **Error identification:** includes prompts that are designed to help locate, recognize, and fix errors in the generated output.
- **Interaction:** category prompts are employed to guide the model in its interaction with the user. These prompts specify how the LLM should engage with the user to achieve a specific objective.

- **context control** prompts enable control over the context in which the model should operate. This ensures that the output generated by the LLM is relevant to the context in which it is being used.

By utilizing prompt patterns and prompt categories, we have developed a set of rules and instructions that implements job-roles classification in ChatGPT.

Classifier design

The efficiency of LLMs is highly reliant on the quality of the prompt used to guide them [17]. For example, in a study titled “**Design guidelines for prompt engineering text-to-image generative models**”, It is emphasized in the research that a slight change in key words could affect the quality of the generated image in image visualization models [18]. Moreover, prompt engineering goes beyond just writing a prompt to accomplish one task; with the right prompt design, an LLM could be able to perform many advanced tasks and processes [17]. In this section, we review how we combined several prompt patterns from different categorizations to create a prompt that classifies a job description according to specific rules. The prompt created is to classify job descriptions based on certain criteria. The prompt provides a list of job titles and their key skills. The goal of the prompt is to compare the key skills of each job title with the job description given by the user and classify the job description into one of the provided job titles. If the job description does not match any of the provided job titles, the prompt should output "No match found". The output of the prompt will consist of one of the 12 ECSF profiles titles that ChatGPT consider as match (classification) to the job description. The prompt can only classify the job description into one of the provided job titles, and any other job titles are not included. The instructions' part is shown below:

From now on, you are a job description classifier.

Rules to follow:

- *When you receive a job description, you will classify it into one of the profiles provided below (the profiles are defined under PROFILES in this text)*

- *Each profile consists of Title and key skills; your mission is to compare the key skills of each profile to the job description provided by the user and classify the description to one of the profiles.*

- *If the job description given by the user is not near any of the profiles you will output "No match found".*

- *From now on, your output will consist of one row only, which will contain the title of the profile that the description is classified at.*

example of an output:

classification: Cyber Incident Responder "

- *In your output classification is only allowed to be one of the following:*

- *Chief Information Security Officer (CISO)*
- *Cyber Incident Responder*
- *Cyber Legal, Policy & Compliance Officer*
- *Cyber Threat Intelligence Specialist*
- *Cybersecurity Architect*
- *Cybersecurity Auditor*
- *Cybersecurity Educator*
- *Cybersecurity Implementer*
- *Cybersecurity Researcher*
- *Cybersecurity Risk Manager*
- *Digital Forensics Investigator*
- *Penetration Tester*
- *No match found*

Any other titles are not included, only the above.

Through an analysis of each instruction outlined in the prompt, we can create a comprehensive understanding of its classification, intent, context, motivation, structure, and key ideas, as well as its potential consequences. In addition, examining each component of the prompt could help to gain a wider understanding of the purpose and underlying principles besides enabling us to create a documentation of the prompt. the analysis of the prompt goes as following:

1. ***"From now and on, you are a job description classifier."***
Implementing the persona pattern to limit the context of the model to a job description classifier.
2. ***"When you receive a job description, you will classify it into one of the profiles provided below (the profiles are defined under PROFILES in this text)"***
Defining the task and objective to the model.
3. ***"Each profile consists of Title and key skills; your mission is to compare the key skills of each profile to the job description provided by the user and classify the description to one of the profiles."***
Providing details on the profiles and defining a simple algorithm of how to compare the profiles with the input of job description.
4. ***"If the job description given by the user is not near any of the profiles you will output "No match found "***
Defining how to handle the cases that are not included in the scope.
5. ***"From now on, your output will consist of one row only, which will contain the title of the profile that the description is classified at."***
example of an output:
classification: Cyber Incident Responder "
Defining the output format and providing examples to be followed by the model. In this instruction we have used parts of the template pattern to bound and limit the output of the model more.
6. ***"In your output classification is only allowed to be one of the following:"***
Listing the allowed classifications for the job classifier. This instruction provides a list of the allowed classifications for the job classifier, limiting the scope of the classification to a specific set of titles.

The prompt can primarily be categorized as **Output Customization** because most of the instructions are for forming, defining, and restricting the output returned by the model. although it has some characteristics of **Interaction Prompts**, wherein the user inputs a job description, and the model produces a classification of the description according to predefined profiles.

Based on the examination and analysis of the prompt's explanation of instructions, we are now able to establish prompt documentation that can help individuals with different backgrounds understand the prompt and how to use it in LLM. The documentation components become:

1. Name and Classification

The name of the prompt is Job classifier with predefined roles, while the main classification is **output customization** with some of the characteristics of **Interaction Prompts**.

2. Intent and context

Intent: To instruct a language model to classify job descriptions based on predefined skills of the profiles.

Context: The user provides a job description to the language model, which then compares the key skills of the job description to a list of predefined profiles and outputs a classification.

3. Motivation

The motivation for this prompt is to automate the task of job classification, which can make it easier for employers and workers. By providing a pre-defined list of profiles, the language model can quickly and accurately classify job descriptions, saving time and effort.

4. Structure and key Ideas

Contextual Statements Table:

| Contextual Statements |
|----------------------------------------------------------------------------------------|
| Act as a job classifier |
| Your main mission is to classify a job description into one of the predefined PROFILES |
| Analyze the job description and compare it to each profile's key skills |
| Output "undefined" if the description does not fit into any profile |
| Follow this output example |
| Stick to allowed outputs |

Table 3. Explaining the structure and idea of the prompt

5. Example of implementation

see appendix, The prompt attached in appendix is specified to suit Cybersecurity job descriptions, but the prompt is reusable to suit other job descriptions, it is achievable by changing PROFILES and the titles allowed in the output in the last part of the prompt.

6. Consequences

The consequence of using this prompt is increased efficiency in job description classification, time and cost savings for companies and job seekers. While the cons are that this prompt may not be suitable for poorly written job descriptions, language models do not always produce accurate classifications therefore human review may be necessary in some cases.

In order to conduct our analysis, we will utilize the ChatGPT Playground platform and apply the prompt to the system. Then, we will manually input the collected job announcements into the prompt to classify them. The resulting classifications will then be collected for further statistical analysis. The results will then allow us to examine and answer our research question.

The method described in this section is suitable for the research question due to its ability to combine between automatic and manual processes, where the automatic part is time effective besides being appropriate for the dynamically changeable job market. On the other hand, the manual process ensures a controlled and trustworthy method. The tests conducted also ensure the validity and accuracy of the method used to answer research questions.

4. RESULTS AND ANALYSIS

Based on the methodology described in the Method section, we have obtained the results that will be presented in this section. The first part to be mentioned is the analysis of the European Cybersecurity Skills Framework (ECSF), from which we extracted the key skills associated with the 12 profiles, the information exists on the following table are cited from the ECSF [2]:

| Job title | Key Skills |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chief Information Security Officer (CISO) | <ul style="list-style-type: none"> • Assess and enhance an organization's cybersecurity posture • Analyze and implement cybersecurity policies, certifications, standards, methodologies, and frameworks • Analyze and comply with cybersecurity-related laws, regulations and legislations • Implement cybersecurity recommendations and best practices • Manage cybersecurity resources • Develop, champion, and lead the execution of a cybersecurity strategy • Influence an organization's cybersecurity culture • Design, apply, monitor, and review Information Security Management System (ISMS) either directly or by leading its outsourcing • Review and enhance security documents, reports, SLAs and ensure the security objectives • Identify and solve cybersecurity-related issues • Establish a cybersecurity plan • Communicate, coordinate, and cooperate with internal and external stakeholders • Anticipate required changes to the organization's information security strategy and formulate new plans • Define and apply maturity models for cybersecurity management • Anticipate cybersecurity threats, needs and upcoming challenges • Motivate and encourage people |
| Cyber Incident Responder | <ul style="list-style-type: none"> • Practice all technical, functional, and operational aspects of cybersecurity incident handling and response • Collect, analyze, and correlate cyber threat information originating from multiple sources • Work on operating systems, servers, clouds, and relevant infrastructures • Work under pressure • Communicate, present and report to relevant stakeholders • Manage and analyze log files |
| Cyber Legal, Policy & Compliance Officer | <ul style="list-style-type: none"> • Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements. • Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organizational processes, finance and business strategy • Lead the development of appropriate cybersecurity and privacy policies and |

| | |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <p>procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it.</p> <p>between the involved parties</p> <ul style="list-style-type: none"> • Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools. • Explain and communicate data protection and privacy topics to stakeholders and users • Understand, practice and adhere to ethical requirements and standards • Understand legal framework modifications implications to the organization's cybersecurity and data protection strategy and policies • Collaborate with other team members and colleagues |
| Cyber Threat Intelligence Specialist | <ul style="list-style-type: none"> • Collaborate with other team members and colleagues • Collect, analyze and correlate cyber threat information originating from multiple sources • Identify threat actors TTPs and campaigns • Automate threat intelligence management procedures • Conduct technical analysis and reporting • Identify non-cyber events with implications on cyber-related activities • Model threats, actors and TTPs • Communicate, coordinate, and cooperate with internal and external stakeholders • Communicate, present and report to relevant stakeholders • Use and apply CTI platforms and tools |
| Cybersecurity Architect | <ul style="list-style-type: none"> • Conduct user and business security requirements analysis • Draw cybersecurity architectural and functional specifications • Decompose and analyze systems to develop security and privacy requirements and identify effective solutions. • Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles • Guide and communicate with implementers and IT/OT personnel • Communicate, present and report to relevant stakeholders • Propose cybersecurity architectures based on stakeholder's needs and budget. • Select appropriate specifications, procedures, and controls • Build resilience against points of failure across the architecture • Coordinate the integration of security solutions |
| Cybersecurity Auditor | <ul style="list-style-type: none"> • Organize and work in a systematic and deterministic way based on evidence • Follow and practice auditing frameworks, standards and methodologies • Apply auditing tools and techniques |

| | | |
|----------------------------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | <ul style="list-style-type: none"> • Analyze business processes, assess, and review software or hardware security, as well as technical and organizational controls. • Decompose and analyze systems to identify weaknesses and ineffective controls • Communicate, explain, and adapt legal and regulatory requirements and business needs • Collect, evaluate, maintain, and protect auditing information • Audit with integrity, being impartial and independent |
| Cybersecurity Educator | | <ul style="list-style-type: none"> • Identify needs in cybersecurity awareness, training, and education • Design, develop and deliver learning programs to cover cybersecurity needs • Develop cybersecurity exercises including simulations using cyber range environments • Provide training towards cybersecurity and data protection professional certifications • Utilize existing cybersecurity-related training resources • Develop evaluation programs for the awareness, training, and education activities • Communicate, present and report to relevant stakeholders • Identify and select appropriate pedagogical approaches for the intended audience • Motivate and encourage people |
| Cybersecurity Implementer | | <ul style="list-style-type: none"> • Communicate, present and report to relevant stakeholders • Integrate cybersecurity solutions to the organization's infrastructure • Configure solutions according to the organization's security policy • Assess the security and performance of solutions • Develop code, scripts, and programs • Identify and solve cybersecurity-related issues • Collaborate with other team members and colleagues |
| Cybersecurity Researcher | | <ul style="list-style-type: none"> • Generate new ideas and transfer theory into practice • Decompose and analyze systems to identify weaknesses and ineffective controls • Decompose and analyze systems to develop security and privacy requirements and identify effective solutions • Monitor new advancements in cybersecurity-related technologies • Communicate, present and report to relevant stakeholders • Identify and solve cybersecurity-related issues • Collaborate with other team members and colleagues |
| Cybersecurity Risk Manager | | <ul style="list-style-type: none"> • Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards • Analyze and consolidate organization's quality and risk management practices • Enable business assets owners, executives, and other stakeholders to make risk informed decisions to manage and mitigate risks • Build a cybersecurity risk-aware environment • Communicate, present and report to relevant stakeholders • Propose and manage risk-sharing options |

| | | |
|----------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Digital Investigator | Forensics | <ul style="list-style-type: none"> • Work ethically and independently; not influenced and biased by internal or external actors • Collect information while preserving its integrity • Identify, analyze and correlate cybersecurity events • Explain and present digital evidence in a simple, straightforward and easy to understand way • Develop and communicate, detailed and reasoned investigation reports |
| Penetration Tester | | <ul style="list-style-type: none"> • Develop codes, scripts and programs • Perform social engineering • Identify and exploit vulnerabilities • Conduct ethical hacking • Think creatively and outside the box • Identify and solve cybersecurity-related issues • Communicate, present and report to relevant stakeholders • Use penetration testing tools effectively • Conduct technical analysis and reporting • Decompose and analyze systems to identify weaknesses and ineffective controls • Review codes assess their security |

Table 4. Recommended key skills for cybersecurity roles defined by the ECSF.

From the previously mentioned table of key skills sourced from the ECSF, it is evident that these skills provide a comprehensive understanding of the competencies, abilities, and experiences required for individuals to excel in their prescribed roles. These skills incorporate both technical and soft skills. The skills "Communicate, present, and report to relevant stakeholders" and "Collaborate with other team members and colleagues" serve as examples of soft skills that are requisite in many roles. An interesting observation is that certain cybersecurity skills are mentioned multiple times across different roles. The table below presents these skills along with the frequency of their occurrence in various profiles:

| Skill | Occurrences in different profiles |
|-------------------------------------------------------------------------------------------------------------|-----------------------------------|
| Identify and solve cybersecurity-related issues | 4 |
| Decompose and analyze systems to identify weaknesses and ineffective controls. | 3 |
| Decompose and analyze systems to develop security and privacy requirements and identify effective solutions | 2 |
| Collect, analyze, and correlate cyber threat information originating from multiple sources | 2 |
| Conduct technical analysis and reporting | 2 |
| Develop codes, scripts, and programs | 2 |
| Risk management standards, methodologies, and frameworks | 2 |

Table 5. common Cybersecurity skills between ECSF profiles

Upon reviewing the skills outlined in Table 5 and conducting further analysis, it becomes evident that there are shared skills among 9 out of the 12 profiles mentioned in Table 4. This means that these profiles share certain common skills. The three other profiles are "Cyber Legal/Policy & Compliance Officer", "Cyber Security Educator", and "Digital Forensics Investigator", which do not have any skills in common with the other profiles. These three profiles have unique skills that do not overlap with other ECSF profiles.

The result of studying 100 job announcements on the Swedish Employment Agency's site

| | |
|------------------------------------|----|
| IMPLEMENTER | 43 |
| ARCHITECT | 15 |
| CISO | 10 |
| RISK MANAGER | 9 |
| INCIDENT RESPONDER | 5 |
| RESEARCHER | 5 |
| THREAT INTELLIGENCE SPECIALIST | 4 |
| AUDITOR | 3 |
| PENETRATION TESTER | 3 |
| EDUCATOR | 2 |
| LEGAL, POLICY & COMPLIANCE OFFICER | 1 |
| DIGITAL FORENSICS INVESTIGATOR | 0 |

Table 6. Classifications results of 100 announcements.

Based on the classification results from ChatGPT, it was observed that the most in-demand cybersecurity job among the analyzed job announcements is the Cyber Security Implementer, with 43% of the total hundred announcements. Another observation is that the least required job was found to be the Digital Forensics Investigator, where none of the announcements were classified under this Title, which raised suspicions about the accuracy of the classification. To ensure the reliability of this result, a manual investigation was conducted where we searched for the term "forensics" on the Swedish Employment Agency's announcement site, the result of the search returned with only two announcements.

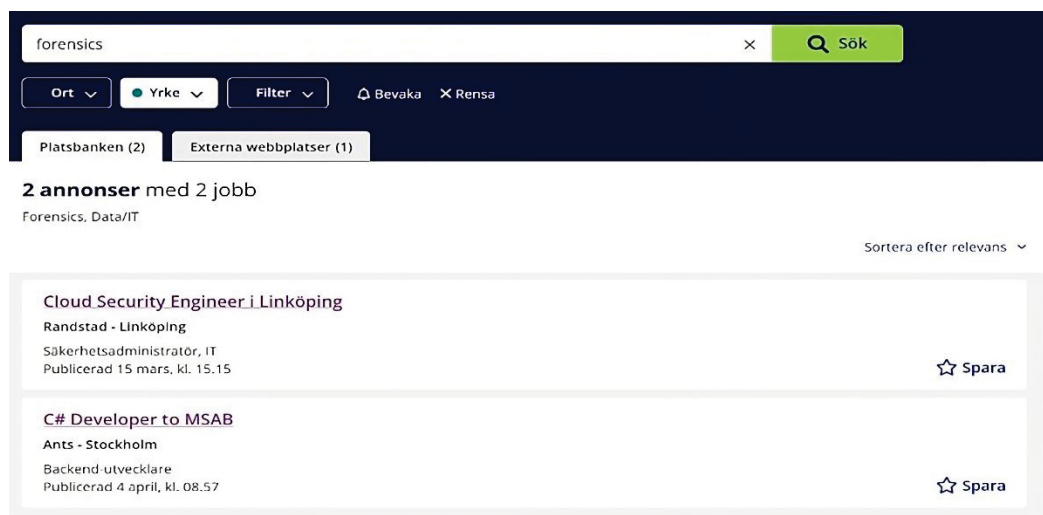


Figure 5: Forensics search results

A further investigation has been done on the found job descriptions which returned two job announcements:

- The first job announcement was included in the one hundred classifications, and it was classified as a cybersecurity architect, with closer examination, it was observed that the announcement included responsibilities related to forensics work, but it was not the focus of the job. Considering the overall content, the classification of cybersecurity architect seemed more appropriate for this role.

- The second job announcement was not included in the one hundred classified announcements. When analyzing, it was observed that the job mainly focuses on development work for forensics tools owned by the company. which is considered as non-relevant for cybersecurity scope.

When arranging the profiles in a bar chart according to the classification from the most selected to the least selected, the form become:

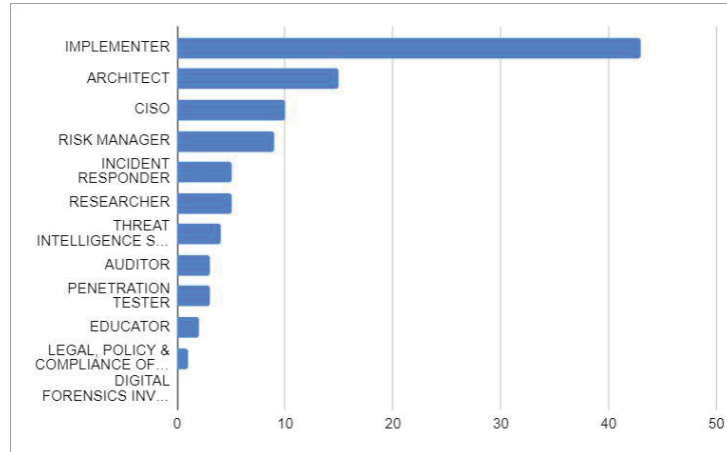


Figure 6: Bar chart of 100-classification of job announcements

Out of the results of one hundred announcements classification, it's clearly seen that nearly 58% of the job announcements point out cybersecurity implementer and architect skills. These two profiles focus mainly on defining, structuring, implementing, analyzing, evaluating, and designing cybersecurity solutions for organizations and companies.

We can conclude the answer of the first research question now, the most common skills are the skills of cybersecurity implementer and architect, besides the repeated skills in table 5. The skills are presented in the following table:

| | |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The skills mentioned in different profiles | <ul style="list-style-type: none"> • Identify and solve cybersecurity-related issues. • Decompose and analyze systems to identify weaknesses and ineffective controls. • Decompose and analyze systems to develop security and privacy requirements and identify effective solutions. • Collect, analyze, and correlate cyber threat information originating from multiple sources. • Conduct technical analysis and reporting. • Develop codes, scripts, and programs. • Risk management standards, methodologies, and frameworks |
| Cybersecurity Implementer unique skills | <ul style="list-style-type: none"> • Integrate cybersecurity solutions to the organization's infrastructure. • Configure solutions according to the organization's security policy. • Assess the security and performance of solutions. |
| Cybersecurity Architect unique skills | <ul style="list-style-type: none"> • Conduct user and business security requirements analysis. • Draw cybersecurity architectural and functional specifications. • Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles. • Guide and communicate with implementers and IT/OT personnel. • Propose cybersecurity architectures based on stakeholder's needs and budget. • Select appropriate specifications, procedures, and controls. • Build resilience against points of failure across the architecture. |

| | |
|--|-------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Coordinate the integration of security solutions. |
|--|-------------------------------------------------------------------------------------------------------|

Table 7. The common cybersecurity skills of ECSF and Swedish cybersecurity job market

To answer the second question, we created the table with the following columns represent:

- Job Id
- Job title
- ChatGPT classification
- Matching to Ibrahim's classification (it will have the value 1 if ChatGPT and Ibrahim's classification are the same, otherwise it will be 0)
- Matching to Al-Ghaith's classification (it will have the value 1 if ChatGPT and Al-Ghaith's classification are the same, otherwise it will be 0)

| Id | Job Title | ChatGPT | matching to Ibrahim classification | matching to Al Ghaith classification |
|----|--------------------------------------------|-----------------------------------------------------------|------------------------------------|--------------------------------------|
| 1 | Information Security Manager | Classification: Chief Information Security Officer (CISO) | 1 | 1 |
| 2 | Digital Forensic Incident Responder (DFIR) | Classification: Cyber Incident Responder | 1 | 1 |
| 3 | Security Compliance Officer | Classification: Cybersecurity Risk Manager | 0 | 0 |
| 4 | Threat Hunter, SOC L3 | Classification: Cyber Threat Intelligence Specialist | 1 | 1 |
| 5 | Cyber Security Architect | Classification: Cybersecurity Architect | 1 | 1 |
| 6 | Cybersecurity Auditor | Classification: Cybersecurity Auditor | 1 | 1 |
| 7 | Software Security Coach | Classification: Cybersecurity Educator | 1 | 1 |

| | | | | |
|----|---------------------------------------------|----------------------------------------------------------------------------------------|---|---|
| | | | | |
| 8 | DevSecOps Engineer | Classification: Cybersecurity Implementer | 1 | 1 |
| 9 | Forskare inom cybersäkerhet | Classification: Cybersecurity Researcher | 1 | 1 |
| 10 | Security Risk Manager | Classification: Cybersecurity Risk Manager | 0 | 1 |
| 11 | Forensic Investigator | classification: No match found | 1 | 1 |
| 12 | Senior penetrationstestare | Classification: Penetration Tester | 1 | 1 |
| 13 | IT-tekniker / Supporttekniker | Classification: No match found | 1 | 1 |
| 14 | Software Engineer (C++) | Classification: Cybersecurity Implementer (some skills match, but not all) | 0 | 0 |
| 15 | Vacuum System Technician | Classification: No match found | 1 | 1 |
| 16 | IT Business Analyst for Digital Identity | Classification: Cybersecurity Implementer (some skills match but not all) | 0 | 1 |

| | | | | |
|----|----------------------------------------------|-----------------------------------------------------------------|---|---|
| 17 | Cyber Security konsult | Classification: Cybersecurity Implementer | 1 | 1 |
| 18 | Cloud Security Engineer - Fully Remote | Classification: Cybersecurity Implementer | 1 | 1 |
| 19 | Junior SOC-ingenjör | Classification: Cyber Incident Responder | 1 | 1 |
| 20 | Senior Cyber Security Consultant | Classification: Chief Information Security Officer (CISO) | 0 | 0 |
| 21 | IT Security Consultant / Officer | Classification: Cybersecurity Architect | 0 | 1 |
| 22 | Network Security Consultant - F5 | Classification: Cybersecurity Implementer | 1 | 1 |
| 23 | Security Consultant | Classification: Cybersecurity Implementer | 1 | 1 |
| 24 | Protective Security Operator | Classification: No match found | 1 | 1 |
| 25 | Security Software Developer | Classification: Cybersecurity Architect | 1 | 1 |
| 26 | IT-Security Specialist | Classification: Cybersecurity Implementer | 1 | 1 |

| | | | | |
|----|-------------------------------|--------------------------------------------|---|---|
| 27 | Microsoft Security Consultant | Classification: Cybersecurity Architect | 1 | 1 |
| 28 | Senior Security Consultant | Classification: Penetration Tester | 1 | 0 |
| 29 | Experienced Ethical Hacker | Classification: Penetration Tester | 1 | 1 |
| 30 | IT-Säkerhets specialist | Classification: Penetration Tester | 0 | 1 |

Table 8. The common cybersecurity skills of ECSF and Swedish cybersecurity job market

| | |
|----------------------------------------------|----------------------|
| ChatGPT classification matching to Ibrahim | 23/30 or 76.6% match |
| ChatGPT classification matching to Al-Ghaith | 26/30 or 86.7% match |

Table 9. The common cybersecurity skills of ECSF and Swedish cybersecurity job market

The test results indicate that ChatGPT achieved an average of 81.7% accuracy in classifying job descriptions compared to human classification. When comparing ChatGPT to Ibrahim, it had 23 correct matches out of 30, resulting in a 76.6% accuracy rate. In contrast, when compared to Al-Ghaith, ChatGPT achieved 26 out of 30 correct classifications, or 86.7% accuracy. When calculating the average accuracy, we find that ChatGPT achieved an 81.7% accuracy rate in classifying job descriptions into ECSF profiles. It's also worth noting that ChatGPT successfully classified non-cybersecurity jobs as well, where in job announcements numbered 11, 13, 15, and 24, ChatGPT correctly identified them as "No match found", correctly categorizing them as non-cybersecurity positions. In another job announcement (number 14), human classification had differing opinions, where Ibrahim considered it not relevant to cybersecurity due to its clear development role, while Al-Ghaith viewed it as weakly relevant due to the presence of some security solution implementation and development aspects. Notably, in classifying the same job announcement, ChatGPT provided an interesting response, stating that "some skills match, but not all", breaking from the standard classification "response pattern". This suggests that ChatGPT's classification abilities are almost as accurate as human classification when analyzing job descriptions.

5. DISSCUSSION

In this research, we aim to identify the intersection of cybersecurity skills between ECSF and the Swedish cybersecurity market demand. Defining these skills will help different parts of society, where educational institutions will have insights into the skills which could help to develop more directed programs toward these skills. Another beneficiary is assisting organizations in addressing the most important cybersecurity skills needed. By answering the research questions, we have achieved the goal of the research. This was done by following the methodology mentioned in the Method section. We first answered the initial sub-results and were then successfully able to obtain an answer to the main research question:

1. What are the common cybersecurity skills between the ECSF and Swedish cybersecurity job market demand?

The recommended skills for the 12 profiles in the ECSF are listed in Table 4, and based on the analysis of Table 4, certain skills are repeatedly observed in different profiles as shown in Table 5. This repetition highlights the importance of these skills within the field of cybersecurity, where these skills are technical in nature, and emphasizes the importance of conducting several forms of technical analysis, such as threat analysis, risk analysis, vulnerability analysis, and even code analysis. Having these skills impacts the effectiveness of cybersecurity professionals in their work, but it is important to note that the non-repeated skills in each profile also contribute to the unique characteristics of each profile. Based on the results and analysis, we observed that the roles of cybersecurity implementer and architect accounted for nearly 58% of the total classifications. The cybersecurity implementer role constituted nearly 43% of the classifications, and 15% respectively. When analyzing the skills associated with the cybersecurity implementer role, it was found that this role had the lowest number of skills, with only seven skills identified, where four of these skills were common and shared with other profiles so they appeared in the repeated skills listed in Table 5, while the remaining three skills were unique to this role but at the same time described general responsibilities. Based on the former finding, we can draw another conclusion regarding the high number of classifications for the implementer role. The repeated skill in this role creates a situation where it frequently competes with other profiles. Further research is necessary to understand the factors driving the prominence of this role and the precise skill set that distinguishes it from others. The presence of common skills shared between the Cyber Security Implementer and other profiles suggests a degree of overlap in skill requirements across different cybersecurity roles. The finding puts into question the idea that each role requires specific and unique skill sets.

2. How effective is the Language Model (LLM) in comparison to human agents in achieving accurate job categorization based on ECSF profiles?

The effectiveness of the Language Model ChatGPT in job categorization based on ECSF profiles was a critical aspect of this research. The evaluation of the Language Model's (LLM) performance in job categorization reveals valuable insights into its effectiveness compared to human agents. With an impressive average accuracy rate of 81.7%, the LLM demonstrates noteworthy proficiency in aligning job positions with ECSF profiles. This indicates a promising advancement in automated job categorization within the cybersecurity domain. The LLM's capacity to consistently achieve accurate results signifies its potential to significantly enhance efficiency in workforce management and job placement processes. However, it's important to acknowledge that while the LLM performs remarkably well, human agents still play a crucial role in nuanced decision-making, especially in scenarios requiring contextual understanding and subjective judgment. Therefore, a collaborative approach, leveraging the strengths of both LLM and human agents, presents a powerful strategy for optimizing job categorization in the cybersecurity sector.

In our study, we used a practical method that involves automating certain tasks and evaluating the accuracy of the automation through tests and manual checks, to ensure precise results to the best of our abilities. Some individuals might believe that fully manually conducting the experiment would result in higher accuracy and better outcomes, but there are challenges and difficulties with this approach. Manual classification takes a long time, and considering that the market is dynamically changing because of changes, deletions, and additions to job announcements, it would cause delays in keeping the classification up to date.

While the analysis of our results introduced valuable insights into the intersection of the recommended skills outlined in the ECSF and the actual skill demands in the Swedish job market, it is important to acknowledge and evaluate any conflicting data that may have occurred during the workflow of this study. And within this subset of common skills, we consider that conflicting explanations and variations may exist. One potential explanation for conflicting data could be the contextual differences between the ECSF recommendations and the specific skills demands identified in the Swedish job market. It is possible that industry requirements might differ in some way from the more general guidelines of ECSF as a result of local requirements, priorities, and latest trends. When combining the two sources, these variations could result in conflicting interpretations.

When addressing conflicting data, methodological factors should also be taken into account. The data collection process involved the utilization of a web crawler to extract job announcements, which may introduce biases or limitations. Factors such as the selection criteria, the specificity of job descriptions, and the representation of different organizations in the data set may contribute to conflicting data of the observed skill demands.

Despite the valuable insights gained from this research study, it is essential to acknowledge the presence of certain limitations and weaknesses that may impact the interpretation and validity of the findings. These limitations highlight areas for improvement and serve as important considerations for future research endeavors. One potential limitation of the study is the manual classification process employed for job announcements using ChatGPT. The classification involved the manual process of copying the job descriptions and pasting them into ChatGPT's playground, with the model providing the classification output. This manual approach introduces the possibility of human error, as the process relies heavily on accurate input and interpretation of job descriptions. In addition, the time consumed in doing this process could be utilized to improve other sections of the study. Automating the classification process through the integration of ChatGPT's API with the implemented crawler could address this limitation, enhancing efficiency and reducing potential human-related inconsistencies as well as minimizing the time consumption, especially if more announcements are investigated.

Another weakness in the project lies in the scraping process of job announcements. Currently, the code utilizes a static sleep or pause time to allow for page loading before extracting information. However, this approach does not account for variations in internet connection speeds or individual circumstances, which may result in inconsistent page loading times. This weakness can introduce potential biases or incomplete data collection, impacting the comprehensiveness and accuracy of the gathered job information. Implementing a more robust mechanism that ensures the scraping process is initiated only when the pages are fully loaded would enhance the reliability and consistency of data acquisition.

The findings of this research study have significant implications for both research and practice in the field of cybersecurity skills alignment. From a research perspective, the study provides valuable insights into the recommended cybersecurity skills that overlap between the European Cybersecurity Skills Framework (ECSF) and the Swedish cybersecurity job market. By examining the ECSF, the research identified the key skills repeatedly observed across different profiles, highlighting their importance within the field of cybersecurity. Additionally, the study analyzed the recent skill demands in the Swedish job market, contributing to a better understanding of the specific skills in high demand. This analysis adds a practical perspective to the research, showing the state of the cybersecurity skill landscape today and informing future studies on industry demands. For practice, the findings offer a new perspective for universities and organizations involved in cybersecurity education and training. The identified common cybersecurity skills bridge the gap between academia and industry, providing a framework for designing educational programs. Educational institutions can align their educational programs with the recommended skills from the ECSF and the current demands in the job market,

ensuring that students have the necessary competencies that are needed by employers. This alignment enhances the effectiveness of cybersecurity education, producing graduates who are well-prepared to meet industry expectations and contribute effectively to the field. Moreover, the use of ChatGPT, a Large Language Model, for job categorization and skill profiling demonstrates the potential of advanced natural language processing techniques in automating and streamlining the skill assessment process. This has practical implications for organizations involved in talent acquisition and human resource management, as they can leverage such models to efficiently match job requirements with candidates' skill sets. This contributes to more accurate and efficient hiring processes, leading to the development of a skilled and capable cybersecurity workforce. The results of the study and their conclusions have significant implications for improving education and providing cybersecurity training for organizations in response to the identified problem of aligning cybersecurity education and industry demands. By examining Table 7, which illustrates the common cybersecurity skills identified from both the European Cybersecurity Skills Framework (ECSF) and the Swedish cybersecurity job market, the study highlights the shared skillset that holds significance for both academia and industry. This finding holds significant importance in the realm of education and organizations, as it offers valuable insights into the specific skills that are currently in high demand and recognized as essential.

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

In this research study, we aimed to identify the intersection of skills by investigating the recommended skills according to the European Cybersecurity Skills Framework (ECSF) and analyzing the recent skill requirements in the Swedish job market. Firstly, we thoroughly reviewed the ECSF to identify the recommended cybersecurity skills. Through our study, analysis, and conclusion of ECSF, we gained a comprehensive understanding of the key skills expected from cybersecurity professionals. In the next phase, we analyzed the Swedish job market, by employing a web crawler to collect job announcements and extract information about the required cybersecurity skills. This allowed us to capture the ECSF skills that are most in demand in the Swedish cybersecurity job market. By examining a hundred cybersecurity related job announcements listed in the Swedish employment agency website, we gained a valuable understanding of the needs of skilled employers in the cybersecurity field. From this, we could identify the common cybersecurity skills between the recommended skills by ECSF and the skills in high demand in the Swedish cybersecurity job market. This analysis provided a comprehensive understanding of the skillset that holds significance for both industry requirements and educational institutions. To automate the classification process and ensure scalability, we utilized the power of ChatGPT, a Large Language model, to categorize job descriptions into the predefined skill profiles identified in our earlier investigations. The accuracy test conducted with ChatGPT demonstrated its effectiveness in classifying common cybersecurity skills with more than 81% accuracy, which indicates that using a Large Language Model is a promising approach for skill profiling and job categorization. In conclusion, this thesis has successfully answered the research questions, shedding light on the recommended cybersecurity skills, the current skill demands in the Swedish job market, and the common cybersecurity skills that bridge the gap between academia and industry. By utilizing advanced NLP techniques and automation, our research provides a valuable contribution to the field of cybersecurity education. It equips universities and organizations with the necessary insights to improve their educational programs and training, and align them with industry expectations, ultimately enhancing the quality of cybersecurity education and supporting the development of a skilled cybersecurity workforce.

6.2 Future Work

While this research study has made interesting results in addressing the alignment of cybersecurity education with industry demands, there are several developments that can be conducted for future exploration and potential follow-up projects. The following sections mention potential areas of future work that can build on this research's findings and contribute to the continued advancement of cybersecurity education.

6.2.1 Improving Methodology

Developing and improving the approach will help to address the problem in a deeper manner. for example, merging multiple frameworks such as National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) which could lead to a more extensive understanding of the skills, besides addressing the problem from different perspectives and factors. Another improvement could be made by using Open Ai's API to automate the entire process which enables processing more job announcements in less time.

Considering more factors than key skills is another way to improve the approach, where the ECSF defines the Main tasks, Key knowledge, and Competencies of each profile which could provide deeper understanding of the problem. Another improvement to decide the exact ChatGPT accuracy in the future could be using a bigger labeled dataset and utilize other validation measures to exactly identify the accuracy of the categorization.

6.2.2 Refinement of Skill Profiling

The classification of cybersecurity skills into predefined profiles using ChatGPT provides a promising foundation. Future work could focus on refining the accuracy of the classification process by combining several data sources, enhancing, and developing more advanced prompts with higher precision. This would ensure more precise skill classifying and facilitate better alignment with industry demands.

6.2.3 Longitudinal Analysis

To capture the dynamic nature of the cybersecurity field, future research can investigate the changes in skill requirements, i.e., exploring the required skills in the job market for a longer period than the one done in this project. By conducting a longitudinal analysis of job announcements and industry demands over a longer period, researchers can identify growing skills, development of skills, and future skill needs. This would enable educational institutions and companies to update their curriculum and ensure the continuous relevance of cybersecurity education and training.

6.2.4 Evaluation of Educational Programs

In the future, it may be necessary to measure cybersecurity educational programs and teaching strategies to measure how educational programs match industry demand. Surveys, interviews, and evaluations of student's skills in relation to the identified common cybersecurity level of competencies can help build new teaching strategies and offer helpful analysis for programs development.

6.2.5 Collaboration with Industry stakeholders

Establishing connections with industry stakeholders can develop the research process by gaining access to filed related data. Establishing also collaborative projects with organizations and cybersecurity professionals can provide a better understanding of industry needs, facilitate the evaluation of skill requirements, and advance knowledge exchange between educational institute and industry.

6.2.6 Expansion to Other Geographical Contexts

While this research focused on the Swedish IT-security market, future studies can cover the analysis of other geographical regions e.g., covering all European Union. By comparing skill demands across different countries, researchers can identify similarities and differences in cybersecurity skill requirements and demand, which could result in a more comprehensive understanding of industry needs.

6.2.7 Integration of Practical Training

Establishing cybersecurity practical education and trainings. Future work can introduce practical exercises, simulations, and real-world scenarios projects into educational programs. This would provide students with a chance to apply their skills, gain more practical experiences, and minimize the gap between theory and practice in cybersecurity.

7. REFERENCES

- [1] R. K. Nilsen, "Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knowledge, Skills, and Abilities Necessary for Organizational Network Access Privileges," College of Engineering and Computing, Nova Southeastern University, 2017.
- [2] S. Furnell, "The cybersecurity workforce and skills," University of Nottingham School of Computer Science, Nottingham, United Kingdom, 2020.
- [3] Rickhard Alén, "Measuring the Effectiveness of Information-Security Education, Training, and Awareness," Department of Computer and Systems Sciences, Stockholm University, 2019
- [4] European Union Agency for Cybersecurity (ENISA), "European Cybersecurity Skills Framework," March 2023.
- [5] E. Persson, "Evaluating tools and techniques for web scraping," KTH Royal Institute of Technology School of Electrical Engineering and Computer Science, 2019.
- [6] O. Castrillo-Fernández, "Web scraping: applications and tools," European Public Sector Information Platform, 2015.
- [7] J. C.-E. Liu and B. Zhao, "Who speaks for climate change in China? Evidence from Weibo," *Climatic Change*, vol. 140, no. 3, pp. 413–422, 2016.
- [8] R. Snyder, "Web search engine with graphic snapshots," Google Patents, 2003.
- [9] "OpenAI. (2021, September 28). ChatGPT: Language Models as Virtual Assistants. Available: [OpenAI](#)" (Accessed: 15 May 2023)
- [10] "Awesome Screenshot. (n.d.). What is Chat GPT?" .Available: [awesomescreenshot](#)" (Accessed: 15 May 2023)
- [11] Tiobe index (2022) TIOBE. Available at: [tiobe](#) (Accessed: 16 May 2023).
- [12] PYPL popularity of Programming Language index. Available at: [pypl](#). (Accessed: 16 May 2023).
- [13] Python, "Why is Python a dynamic language and also a strongly typed language," Available: [python.org](#) (Accessed: 16 May 2023).
- [14] Selenium.dev. Available: [selenium.dev](#). (Accessed: 16 May 2023).
- [15] European Union Agency for Cybersecurity (ENISA), "About ENISA," ENISA – European Union Agency for Cybersecurity. Available: [about-enisa](#). (Accessed: 17 May 2023).
- [16] European Committee for Standardization (CEN), "European e-Competence Framework 3.0Part 1: A common European framework for ICT Professionals in all industry sectors," Joinup, [Online]. Available: [About:part-1-common-european-framework-ict-professionals](#)

- [17] J. White, Q. Fu, S. Hays, M. Sandborn, C. Olea, H. Gilbert, A. Elnashar, J. Spencer-Smith, and D. C. Schmidt, "**A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT**," Department of Computer Science, Vanderbilt University, Tennessee, Nashville, TN, USA.
- [18] V. Liu and L. B. Chilton, "Design guidelines for prompt engineering text-to-image generative models," Columbia University, USA, September 2021.
- [19] "Sök lediga jobb i Platsbanken," Arbetsförmedlingen.
arbetsformedlingen.se(Accessed: 17 May 2023).
- [20] "What is a Flowchart, and Why Is It Important?," What is a Flowchart, and Why Is It Important?. Available: [integrify/flowchart](https://integrify.com/flowchart) (Accessed: 20 May 2023).

7. APPENDIX:

3. Crawler:

```
from selenium import webdriver
from selenium.webdriver.common.by import By
import time

d = webdriver.Chrome("C:/Users/ghaet/Desktop/chromedriver_win32/chromedriver.exe") #you have to install chrome
and chrome driver
jobs = []
links = []
keywords = ['cybersäkerhet','soc', 'it-säkerhet', 'analyst', 'Cyber security', 'IT-Security', 'Threat intelligence']
#Extract jobs from arbetsförmedlingen by searching each keyword
for keyword in keywords:
    for i in range(1,13): #maximum 300 jobs from each keyword, 25 job in each page. (12*25)
        print("Crawling page:", i,"of keyword:", (keyword),"...")
        d.get(f"https://arbetsformedlingen.se/platsbanken/annonser?q={keyword}&page={i}")
        time.sleep(3)
        for j in range (1,26):
            try:
                job_card = d.find_element(By.CSS_SELECTOR, f'pb-feature-search-result-card:nth-child({j}) > div >
div.header-container > h3 > a')
                job_date = d.find_element(By.CSS_SELECTOR, f' pb-feature-search-result-card:nth-child({j}) > div >
div.internal.ng-star-inserted > div > div.bottom__left > div:nth-child(2)')
                date = job_date.text
                titel = job_card.text
                link = job_card.get_attribute("href")
                if link not in links: #avoid adding same announcement.
                    links.append(link)
                    dic = {'ID': len(jobs), 'Title': titel, 'Date': date, 'Link': link}
                    jobs.append(dic)
            except:
                break
        if j != 25:
            break

#Exclude unrelated jobs by filtering job's title
c = 0
related = ['säk', 'soc', 'sec']
lst = []
jobs1 = []
for job in jobs:
    title = job['Title'].lower()
    for word in related:
        if word in title and title not in lst:
            lst.append(job['Title'].lower())
            jobs1.append(job)
            c += 1

#Extract each job's description
```

```

for job in jobs1:
    d.get(job['Link'])
    time.sleep(3)
    job_desc = d.find_element(By.CSS_SELECTOR, '#pb-root > pb-page-job > div > section > div > div.jobb-
container.container > div:nth-child(2) > section > pb-section-job-main-content > div')
    job['Description'] = job_desc.text
d.quit()

#Save the data as a JSON-file
import json
with open('data.json', 'w') as f:
    json.dump(jobs1, f)

```

4. Full prompt:

your're a job description classifier.
rules to follow:

- When you receive a job description, you will classify it into one of the profiles provided below (the profiles are defined under PROFILES in this text)
- Each profile consists of Title and key skills; your mission is to compare the key skills of each profile to the job description provided by the user and classify the description to one of the profiles.
- If the job description given by user isn't near any of the profiles you will output "No match found".
- From now on, your output will consist of one row only, which will contain the title of the profile that the description is classified at.

example of an output:

classification: Cyber Incident Responder "

- in your output classification is only allowed to be one of the following:

- Chief Information Security Officer (CISO)
- Cyber Incident Responder
- Cyber Legal, Policy & Compliance Officer
- Cyber Threat Intelligence Specialist
- Cybersecurity Architect
- Cybersecurity Auditor
- Cybersecurity Educator
- Cybersecurity Implementer
- Cybersecurity Researcher
- Cybersecurity Risk Manager
- Digital Forensics Investigator
- Penetration Tester
- No match found

any other titles are not included, only the above.

5. Profiles:

Profile number 1

Title: Chief Information Security Officer (CISO)

Key skill(s):

- Assess and enhance an organisation's cybersecurity posture
- Analyse and implement cybersecurity policies, certifications, standards, methodologies and frameworks
- Analyse and comply with cybersecurity-related laws, regulations and legislations
- Implement cybersecurity recommendations and best practices
- Manage cybersecurity resources
- Develop, champion and lead the execution of a cybersecurity strategy
- Influence an organisation's cybersecurity culture
- Design, apply, monitor and review Information Security Management System (ISMS) either directly or by leading its outsourcing
- Review and enhance security documents, reports, SLAs and ensure the security objectives
- Identify and solve cybersecurity-related issues
- Establish a cybersecurity plan
- Communicate, coordinate and cooperate with internal and external stakeholders
- Anticipate required changes to the organisation's information security strategy and formulate new plans
- Define and apply maturity models for cybersecurity management
- Anticipate cybersecurity threats, needs and upcoming challenges
- Motivate and encourage people

Profile number 2

Title: Cyber Incident Responder

Key skill(s):

- Practice all technical, functional and operational aspects of cybersecurity incident handling and response
- Collect, analyse and correlate cyber threat information originating from multiple sources
- Work on operating systems, servers, clouds and relevant infrastructures
- Work under pressure
- Communicate, present and report to relevant stakeholders
- Manage and analyse log files

Profile number 3

Title: Cyber Legal, Policy & Compliance Officer

Key skill(s):

- Comprehensive understanding of the business strategy, models and products and ability to factor into legal, regulatory and standards' requirements
- Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy
- Lead the development of appropriate cybersecurity and privacy policies and procedures that complement the business needs and legal requirements; further ensure its acceptance, comprehension and implementation and communicate it

between the involved parties

- Conduct, monitor and review privacy impact assessments using standards, frameworks, acknowledged methodologies and tools
 - Explain and communicate data protection and privacy topics to stakeholders and users
 - Understand, practice and adhere to ethical requirements and standards
 - Understand legal framework modifications implications to the organisation's cybersecurity and data protection strategy and policies
 - Collaborate with other team members and colleagues
-

Profile number 4

Title: Cyber Threat Intelligence Specialist

Key skill(s):

- Collaborate with other team members and colleagues
 - Collect, analyse and correlate cyber threat information originating from multiple sources
 - Identify threat actors TTPs and campaigns
 - Automate threat intelligence management procedures
 - Conduct technical analysis and reporting
 - Identify non-cyber events with implications on cyber-related activities
 - Model threats, actors and TTPs
 - Communicate, coordinate and cooperate with internal and external stakeholders
 - Communicate, present and report to relevant stakeholders
 - Use and apply CTI platforms and tools
-

Profile number 5

Title: Cybersecurity Architect

Key skill(s):

- Conduct user and business security requirements analysis
 - Draw cybersecurity architectural and functional specifications
 - Decompose and analyse systems to develop security and privacy requirements and identify effective solutions
 - Design systems and architectures based on security and privacy by design and by defaults cybersecurity principles
 - Guide and communicate with implementers and IT/OT personnel
 - Communicate, present and report to relevant stakeholders
 - Propose cybersecurity architectures based on stakeholder's needs and budget
 - Select appropriate specifications, procedures and controls
 - Build resilience against points of failure across the architecture
 - Coordinate the integration of security solutions
-

Profile number 6

Title: Cybersecurity Auditor

Key skill(s):

- Organise and work in a systematic and deterministic way based on evidence
- Follow and practice auditing frameworks, standards and methodologies

- Apply auditing tools and techniques
 - Analyse business processes, assess and review software or hardware security, as well as technical and organisational controls
 - Decompose and analyse systems to identify weaknesses and ineffective controls
 - Communicate, explain and adapt legal and regulatory requirements and business needs
 - Collect, evaluate, maintain and protect auditing information
 - Audit with integrity, being impartial and independent
-

Profile number 7

Title: Cybersecurity Educator

Key skill(s)

- Identify needs in cybersecurity awareness, training and education
 - Design, develop and deliver learning programmes to cover cybersecurity needs
 - Develop cybersecurity exercises including simulations using cyber range environments
 - Provide training towards cybersecurity and data protection professional certifications
 - Utilise existing cybersecurity-related training resources
 - Develop evaluation programs for the awareness, training and education activities
 - Communicate, present and report to relevant stakeholders
 - Identify and select appropriate pedagogical approaches for the intended audience
 - Motivate and encourage people
-

Profile number 8

Title: Cybersecurity Implementer

Key skill(s):

- Communicate, present and report to relevant stakeholders
 - Integrate cybersecurity solutions to the organisation's infrastructure
 - Configure solutions according to the organisation's security policy
 - Assess the security and performance of solutions
 - Develop code, scripts and programmes
 - Identify and solve cybersecurity-related issues
 - Collaborate with other team members and colleagues
-

Profile number 9

Title: Cybersecurity Researcher

Key skill(s):

- Generate new ideas and transfer theory into practice
 - Decompose and analyse systems to identify weaknesses and ineffective controls
 - Decompose and analyse systems to develop security and privacy requirements and identify effective solutions
 - Monitor new advancements in cybersecurity-related technologies
 - Communicate, present and report to relevant stakeholders
 - Identify and solve cybersecurity-related issues
 - Collaborate with other team members and colleagues
-

Profile number 10

Profile number 10

Title: Cybersecurity Risk Manager

Key skill(s):

- Implement cybersecurity risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards
- Analyse and consolidate organisation's quality and risk management practices
- Enable business assets owners, executives and other stakeholders to make risk [1]informed decisions to manage and mitigate risks
- Build a cybersecurity risk-aware environment
- Communicate, present and report to relevant stakeholders
- Propose and manage risk-sharing options

Profile number 11

Title: Digital Forensics Investigator

Key skill(s):

- Work ethically and independently; not influenced and biased by internal or external actors
- Collect information while preserving its integrity
- Identify, analyse and correlate cybersecurity events
- Explain and present digital evidence in a simple, straightforward and easy to understand way
- Develop and communicate, detailed and reasoned investigation reports

Profile number 12

Title: Penetration Tester

Key skill(s):

- Develop codes, scripts and programmes
 - Perform social engineering
 - Identify and exploit vulnerabilities
 - Conduct ethical hacking
 - Think creatively and outside the box
 - Identify and solve cybersecurity-related issues
 - Communicate, present and report to relevant stakeholders
 - Use penetration testing tools effectively
 - Conduct technical analysis and reporting
 - Decompose and analyse systems to identify weaknesses and ineffective controls
 - Review codes assess their security
-