CyberHubs

Cybersecurity Skills Needs Analysis report Belgium.

Co-funded by
the European Union

About CyberHubs

The European Network of Cybersecurity Skills Hubs (CyberHubs) is a 3-year project aiming to enhance the cybersecurity skills ecosystem in Europe. It will establish a network of seven Cybersecurity Skills Hubs in Belgium, Estonia, Greece, Hungary, Lithuania, Slovenia, and Spain, which will promote the development of digital skills in cybersecurity and support the development of a skilled cybersecurity workforce.

Expected results of the project include the establishment of a sustainable European Network of Cybersecurity Skills Hubs, the development of national cybersecurity skills strategies, the creation of innovative cybersecurity solutions through the Hackathon and the establishment of long-term partnerships and collaboration with the wider cybersecurity ecosystem.

Project consortium

The CyberHubs consortium brings together 21 full partners spanning 11 European Member States and 3 associated partners.

Full partners

DIGITALEUROPE | ADECCO FORMAZIONE SRL | AGORIA | AMETIC | Athens University of Economics and Business | Breyer Publico SL | Cyber Ireland | EIT Digital | GZS/CCIS | HOWEST | INFOBALT | ITL Estonia | IVSZ | Kaunas University of Technology | NUMEUM | SEPE | Solvay Brussels School of Economics and Management | Tallinn University of Technology | Universidad Internacional de La Rioja (UNIR) | Ludovika University of Public Service (NKE) | UNIVERZA V MARIBORU

Associated partners

Association of Applied Research in IT (AAVIT) | Digital Technology Skills (DTSL) | IT Ukraine

Legal Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by
the European Union

Cybersecurity Skills Needs analysis report - Belgium, 2024, final version

Deliverable D2.1: “Cybersecurity skills mismatches analysis”

Authors

- Floriane de Kerchove (Agoria)
- Jeroen Franssen (Agoria)

with support of students at the Solvay Brussels School[1] for the desk research

Editors/Reviewers

- Professor Georges Ataya (Solvay Brussels School)
- Gert-Jan Wille (Howest)
- Eric Van Cangh (Agoria)

Revision History			
Version	**Date**	**Modified by**	**Version**
0.1	27/09/2024	Floriane de Kerchove (Agoria)	Draft version
0.2	10/10/2024	Jeroen Franssen (Agoria)	Language corrections
0.3	22/10/2024	Jeroen Franssen (Agoria)	Executive summary Language corrections Layout and graph corrections
1	28/10/2024	Agoria	Final version

[1] Students at the Solvay Brussels School: Victor GOLUBOVSKIY, Adrien JAMAR, Louis LHOEST, Radost SONOVEY-ZOLA, working under the supervision of Professor Georges Ataya within the scope of Business field project courses.

Acknowledgements

We would like to sincerely thank the following experts and their organizations for their participation in the expert panels and their valued feedback in the process of the CyberTalents meetings:

Julien Haeck	Approach Cyber
Sarah Boulanger	Approach Cyber
Clément Laurens	Cresco
Carl Vastmans	Belgian Defense CyberCommand
Pascal Champagne	Cybersecurity Coalition
Maxime Lamarche	Easi
Gert-Jan Wille	Howest
Johan Galle	Howest
Bart Asnot	Microsoft
Akin Bas	Proximus
Georges Ataya	Solvay Lifelong Learning
Vanessa Lewis	Starion Group
Jasper Hooft	Toreon
Jeroen Franssen	Agoria
Saskia Van Uffelen	Agoria

Table of Contents

List of Figures

Executive Summary

Introduction

Cybersecurity has emerged as a critical field in today's rapidly evolving digital landscape. In order to meet the needs of the field, highly skilled workers are needed. However, there is a growing concern about the lack of cybersecurity professionals. Moreover, the concern is not only quantitative in nature. Stakeholders in the digital and cybersecurity ecosystem indicate there seems to be an important mismatch between skills supply and skills demand. Testimonies mention that this situation of double deficits can cause unsafe situations, unused business potential and productivity coming under pressure. In short, the deficits mean a brake on economic developments in Belgium.

Objective

The objective of this study is to identify and understand the actual and future needs for jobholders, roles and skills in the cybersecurity ecosystem in Belgium. The research team also wants to explore an instinctive mismatch between employers' demands and the offerings of training and educational entities. This analysis helps us to propose recommendations to address the shortage of cybersecurity roles and skills and will thus feed the development of a country-specific Cybersecurity Skills Strategy for Belgium.

Approach

To analyse the demand for cybersecurity roles, we collected comprehensive data from various sources, including reports, literature and labour market statistics. To further enrich our data and analysis, we conducted a questionnaire and a job vacancy analysis, and consulted an expert panel on cybersecurity roles, skills, and training. On the supply side, we catalogued post-secondary, higher education, and university-level training and education programmes. Analysing these diverse sources and findings, we were able to draw conclusions on the roles, skills, and training and education programmes for cybersecurity professionals as well as on the gap between demand and supply.

Results

The Belgian cybersecurity ecosystem is expanding rapidly. The main drivers for this expansion are the strong digitisation rate of our country, a sharp rise in cyber attacks, a growing awareness of the dangers and the implementation of European regulations. A wide variety of public and private initiatives are trying to respond to the need for diverse cybersecurity experts (at least 4,000 open vacancies) with the right competences. But a fragmented and poorly coordinated landscape results in several research sources revealing distinct quantitative and qualitative challenges.

A survey of a diverse sample of Belgian companies shows that the perceived vacancy rate for 12 selected cybersecurity roles is no less than 30%. This means that if a company has work on the shelf for 100 people, only 70 people are effectively employed. Furthermore, over the next 2 years, the demand for labour for the various cybersecurity roles is expected to grow by an average of 18%. In the 5-year term, the expectations are +63%. The most in-demand role is that of cybersecurity implementer while the greatest tension between supply and demand in the future is to be expected for cybersecurity architects, educators and auditors.

During the analysis of the required skills, the skill needs were captured in 4 categories. Almost naturally, in the vacancies examined, specialized cybersecurity skills such as incident management or cloud security were most sought after. The many mentions of the importance of soft skills were striking. While cybersecurity skills are often mentioned based on the rapidly evolving nature of the technologies, we assume that the explicit mention of soft skills indicates that traditional forms of education and training pay too little attention to them.

When analyzing a sample of the long-term training offer, it is immediately noticeable that the educational institutions theoretically cover the paths to the 12 selected roles. However, the specialized selected training courses seem to, to a certain extend, ignore the most requested role, that of cybersecurity implementer. According to the expert panel, this seems to indicate that cybersecurity as a service, which may soon be in high demand by SMEs, deserves even more attention today in the less specialized and general STEM or ICT directions.

Conclusions

In order to feed a specific Belgian strategy for cybersecurity skills, the project team, together with the experts, advocates the promotion of the theme of cybersecurity from the early use of digital devices by children.

Furthermore, promotion should also focus on women and older professionals who we believe are either underrepresented in the ecosystem or would benefit greatly from upskilling.

Good training initiatives should be able to scale up because we often found undercapacity, in particular for training courses intended for job seekers.

The existing training courses can achieve a quality injection through much closer cooperation based on concrete projects with companies.

And those same companies should invest structurally in a cybersecurity training plan for all current and future employees.

1 Introduction

1.1 Cybersecurity skills in Belgium

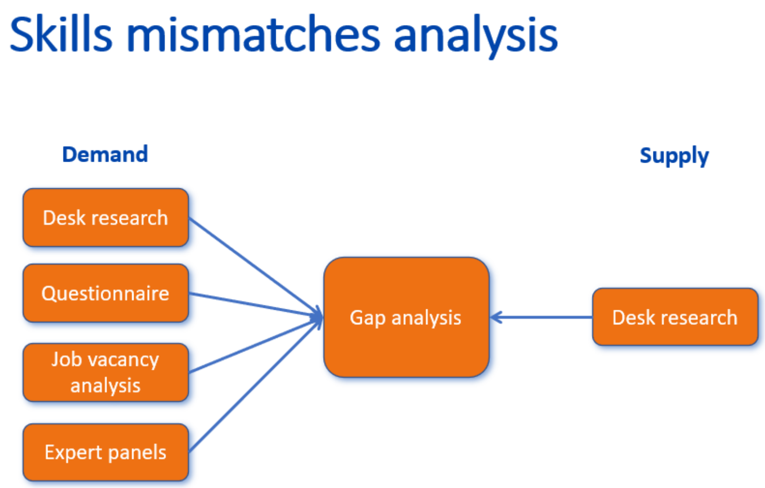
Cybersecurity has emerged as a critical field in today's rapidly evolving digital landscape. In order to meet the needs of the field, skilled workers are needed in every sector, on every level. In the ICT-sector in particular the need for highly skilled workers manifests itself in a no longer be to denied manner. However, the concern about the mismatch between the cybersecurity programme supply in training institutions and the employers' demand in the job market in all sectors seems to be growing. This report provides a detailed exploration of this issue, focusing on the specific context of Belgium, where both qualitative and quantitative analysis show that the demand for cybersecurity professionals has significantly outpaced the supply.

This report examines the current cybersecurity roles and skills landscape in Belgium, identifying gaps between the cybersecurity capabilities currently taught in educational institutions and the actual roles and skills demanded by employers. The objective is to thoroughly analyse the current demands of the cybersecurity market in Belgium and compare them to the cybersecurity skills taught by a various and representative sample of educational establishments. The aim is to highlight specific areas where these programmes do not meet the needs of the labour market and to provide recommendations.

1.2 Research approach

To analyse the demand for cybersecurity roles, we collected comprehensive data from various sources, including reports, literature and labour market statistics (61 validated sources used). To further enrich our data and analysis, we launched both a questionnaire (60 validated responses) and a job vacancy analysis (584 open vacancies analysed). Furthermore, we consulted an expert panel of 15 professionals on cybersecurity roles, skills and training. On the supply side, we catalogued post-secondary, higher education and university-level training and education programmes. All the analysed programmes have a minimum term of over 4 months.

The research team dived into five specific learning programmes which we compared with the requirements for cybersecurity roles. Based on these diverse sources and findings, we were able to draw conclusions on the demand of roles and skills on one hand, and on training and education programmes for cybersecurity professionals on the other. This allows us as well to detect and reveal the gap between demand and supply.



1.3 Reading guide

This report will be structured as follows. First, we will delve into desk research on the demand side for a series of roles needed in the field of cybersecurity. In this section we will also highlight different skills in high demand. In a next section, we will analyse the results of a questionnaire sent to a representative variety of enterprises. The different roles and skills needed in these companies will be schematised, leading us to conclusions. This section will be followed by an analysis of available job offers.

After focusing on the demand side, this report will further investigate the supply side, meaning the educational programmes and trainings. In this section, five programmes are highlighted and analysed to get a clearer view on the availability and diversity of programmes offered in Belgium.

As mentioned earlier, to gather extra qualitative insights, an expert panel was organized. The conclusions that issued out of this panel will be presented at the end of this report.

The report will be concluded with an overview of the analysed topic and recommendations aiming at making the Belgian cybersecurity ecosystem stronger and more effective.

2 Desk research (demand)

In this section we focus on analysing the demand for cybersecurity professionals in Belgium. Cybersecurity has become a central issue for businesses and the public sector in Belgium due to the increase in digital threats and the growing adoption of advanced technologies. A solid cybersecurity ecosystem is more and more considered as a 'conditio sine qua non' to make digital solutions for business, society and citizens flourish. This national and international context is creating increased demand for qualified professionals capable of protecting sensitive infrastructures and data. Government initiatives, national strategies and existing regulations, such as the NIS2 directive, are strongly influencing the demand for skills and personnel in the cybersecurity sector. The Belgian market, societal and technological context will also have a sensitive impact on the sector. By examining these initiatives, we can better understand how they are shaping the current and future cybersecurity landscape in Belgium.

We will also provide insights into cybersecurity roles and skills at both national and global levels, drawing on data from various sources, including literature, labour market reports, and databases. This will help contextualize the research presented in the following chapter.

2.1 Data collection

Several quantitative and qualitative sources were analysed to conduct desk research on the demand for cybersecurity professionals in Belgium. These sources include reports from specialized organizations on the subject at both European and Belgian levels, quantitative statistical websites, publications from specialized cybersecurity websites, official national and European websites (e.g., CCB, European Commission, EIOPA), and interviews with relevant parties (such as the CCB, Vlaio, and Cyberwal / Agence du Numérique).

Data collection in numbers	
Reports	20 reports were used for this analysis
Statistics and databases	5 quantitative sources, including statistics and databases, were used for this analysis
Publications	30 publications were used for this analysis
Websites	6 websites were used for this analysis

2.2 Overview of the national context

2.2.1 Politics and agencies

2.2.1.1 National Cybersecurity Governance and Initiatives in Belgium

In Belgium, the organization around cybersecurity is structured to ensure a coordinated and effective response to emerging digital threats (CCB, 2021). At the **national level**, the government has taken significant actions to reinforce cybersecurity resilience, including the development of a comprehensive national strategy and the establishment of key public organizations dedicated to cybersecurity.

Cybersecurity funding and promotional aspects are directed through **regions**, where each of the regions rely on crucial agencies which provide support and funding to the regional developments in cybersecurity. Examples include Cyberwal (Wallonia) and Vlaio (Flanders) which both act to connect companies and knowledge institutes, raise awareness to companies and support companies in a broad sense.

2.2.1.2 National Strategy and Guidelines

Belgium has modified its **national cybersecurity strategy** and, according to the CCB strategy documentation, it ascertains a complete and proactive system to defend an increasingly imperilled digital space (CCB, 2021; CCB, 2023d). The strategy describes that cybersecurity needs an all-inclusive approach since it is a duty shared by public authorities, private sectors, and individual citizens among others. It also sets out a vision of safe cyberspace which is open to everyone, where economic activities can take place without any fear and social prosperity flourishes. With focus on resilience of critical infrastructure, trust in digital environment enhancement and safeguarding key organizations from complex cyber-attacks, the strategy encompasses protection against various types of cyber threats.

The **guidelines** for implementing the national strategy include several main actions meant to enhance Belgium's capability towards cybersecurity (CCB, 2021; CCB, 2023d). These may involve establishing strong legal frameworks adapted for current digital threats, ensuring continuous adaptation to emerging cyber threats as well as promoting culture of awareness about cybersecurity among all stakeholders. Advanced training programmes should be developed. International cooperation is given priority through involvement with global initiatives, besides protecting own interest this also contributes towards fighting worldwide cybercrime thus raising international standards for safety on digital platforms.

Additionally, the strategy acknowledges the significant role played by **innovative technologies** (e.g.: encryption methods) **together with processes** (e.g.: secure software development practices) towards realization of these objectives (CCB, 2021). Public-private partnership is seen as vital because such alliances help pool resources necessary hence promoting robustness within the defence systems against various forms of attack originating from different quarters globally. Furthermore, there should be coordinated response (public and private sectors, at national and international levels) whenever there are incidents related to cyber space. Such measures will ensure that Belgium becomes a more secure place digitally for every person involved either directly or indirectly.

2.2.1.3 Key Actors and Public Organizations

The law and regulations establish a competent authority in Belgium which qualifies as the National Competent Centre ("NCC") for which The Centre for Cybersecurity Belgium (CCB) is responsible and qualifies as the most significant actor in the Belgian cybersecurity landscape (ECCC, 2024). It is a central authority responsible for cybersecurity, including monitoring, coordinating and overseeing implementation of cyber security policies. This organization partners with other public organizations like the Federal Police, the Public Prosecutor's Office, and the National Crisis Centre to ensure a coherent response to cyber threats. Here is a list of the **main actors sharing responsibilities and roles in the cybersecurity according to the CCB**:

- Centre for Cybersecurity Belgium (CCB): It is the main unit responsible for the coordination and implementation of the national strategy on cybersecurity. It is established by article 8 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Where Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks referred to in Chapter VII (competent authorities).
- Federal Police: This force has squads specialized in handling online crimes. These units provide necessary law enforcement powers to deal with cyber threats and offenses.
- Ministry of Justice: As far as prosecutorial duties are concerned; this ministry deals with legal frameworks surrounding cybercrimes as well as those related to legislation on cybersecurity.
- Belgian Defence: The military also has capabilities and roles in protecting critical national infrastructure and responding to significant cyber threats and attacks.
- National Crisis Centre (NCCN): Coordinating responses across various government departments during major cyber incidents or national emergencies is one of the key functions performed by this centre.
- State Security Service (VSSE): VSSE acts as a counterintelligence service at national level that covers among others terrorism, espionage activities including those originating from cyberspace.
- Federal Public Service Foreign Affairs: Among other things, this entity engages itself on international cooperation pertaining to cybersecurity vis-a-vis other countries or international organizations.
- National Security Authority (NSA or ANS): Including but not limited to defence secrets, NSA oversees measures put in place for safeguarding classified information with relevance to state sovereignty against diverse threats such as those coming from digital networks.
- Coordination Unit for Threat Analysis (OCAM): OCAM's mandate includes conducting timely assessments about threats which may include cybersecurity threats among others.
- Belgian Institute for Postal services and Telecommunications (IBPT): Regulates communications industries including aspects of cybersecurity related to telecommunications.
- Federal Public Service Economy: Deals with economic implications brought about by issues arising from safeguarding critical economic infrastructure within our borders through enhanced cybersecurity measures.
- Belgian Cybersecurity Coalition: A collaborative platform that brings together public and private sectors, academia, and research institutions across Belgium to share knowledge, develop best practices, and coordinate efforts to improve the overall cybersecurity posture of the nation.

On top of those, we can **also** mention **the following actors**:

- Cyberwal (Agence du Numérique): A cybersecurity initiative in Wallonia focused on enhancing cybersecurity measures, providing support to businesses, and fostering collaboration between academic, private, and public sectors to bolster the region's cybersecurity capabilities.
- Vlaio: The Flanders Innovation & Entrepreneurship agency, which supports businesses in Flanders, Belgium, with their cybersecurity needs through funding, guidance, and resources aimed at innovation and technological advancement.
- Agoria – Cyber Made in Belgium (CMiB): is the voice for the Belgian cybersecurity industry gathering the companies that develop and offer cybersecurity technology in Belgium.

2.2.1.4 Campaigns, Initiatives and Funding

Belgium has launched **numerous campaigns and initiatives** to sensitize its population about cybersecurity awareness and best practices enforced through it. (CCB, 2021). Examples include campaigns by Febelfin in collaboration with influencers such as Sami Farhat to promote awareness against financial fraud on the social media (Febelfin, 2024). But they also launched several awareness raising campaigns oriented towards companies such as 'preventing CEO fraud' in which cybercriminals use CEO credentials to commit fraud on the company (CCB, 2023a). Additionally, their efforts include campaigns targeting the public to educate them on various online risks and measures they can use to stay safe. They also promote training programmes and workshops specifically designed for different companies and entities (CCB, 2023b; CCB, 2023c). Another source of support comes from government grants and subsidies available for promoting cybersecurity-related activities such as research and innovation programmes (Chancellerie du Premier Ministre, 2023).

Regional agencies such as Vlaio and Agence du Numérique also have their own programmes. Among the 25 actions undertaken by Agence du Numérique/CyberWal (including training, support, funding, research projects, and studies), the "Raising Awareness of Cybersecurity 2024-2025" campaign and the "Digital Transformation of Businesses: Cyber Response Team" project stand out.

More broadly, to implement the vision and the strategic objectives of Belgium's ambitious cybersecurity strategy, significant and essential additional **investments** are necessary. This commitment by the Belgian government to allocate resources is a fundamental component of the renewed national cybersecurity strategy. It is crucial to enhance the country's cyber capabilities to arm its economy, public services, and vital organizations realistically and effectively against the increasingly numerous cyber threats.

Investments in cybersecurity also have a direct and clear economic impact. If the government can inspire and ensure trust in digital life, businesses and citizens will be more confident in investing in digital applications. This will allow boosting productivity and economic growth within the country. With this concrete investment commitment, Belgium aligns with significant initiatives taken by its neighbouring countries.

Achieving the mission of making Belgium one of the least vulnerable countries in Europe in terms of cybersecurity by 2025 is a collective effort. In addition to the Centre for Cybersecurity Belgium (CCB), other public services, intelligence and security services, the business world, Organizations of Vital Interest, the academic community, and citizens each have their own individual responsibility to achieve the ambitious objectives set.

2.2.2 Laws and regulations

It is a very dynamic and confusing Belgian regulatory framework for cybersecurity, which entails several laws and guidelines aiming at safeguarding critical infrastructure, protecting personal data, fighting cybercrime, and securing electronic communications. At a national level, there is specific legislation implementing European regulations to form a comprehensive governance structure for cybersecurity.

The **NIS2 directive** (Directive 'UE' 2022/2555), effective from 16 January 2023, replaces the NIS1 directive, aiming to secure cyberspace across Europe by imposing **security measures on key operators in various sectors**. NIS2 expands its scope to address new challenges, requiring national authorities to enhance collaboration and adopt more holistic cybersecurity approaches. NIS2 marks significant progress in protecting critical infrastructure and advancing cybersecurity across Europe.

The key changes introduced by this new Directive are as follows:

- The directive widens the scope of sectors and entities. The identified critical sectors range from energy to transport, banking, health care, water supply and digital infrastructure amongst others. A distinction is made between 'essential' and 'important' entities based on size and sector, replacing the previous 'operators of essential services' (OSE) and 'digital service providers' (DSP) classification.
- The directive increases accountability of top management.
- The directive contains other measures for risk management, notification requirements and sanctions.

NIS2 was transposed into Belgian National Law on the 17th of May 2024 (CCB, 2024b). This regulation will have the most significant impact on the cyber environment in Belgium.

The European **Cyber Resilience Act (CRA)** is a comprehensive legislative framework introduced to address the mounting **cybersecurity** challenges associated with **digital products** within the European Union (European Commission, 2022; European Commission, 2023a). This act mandates rigorous cybersecurity standards for both hardware and software products that possess digital elements and are placed on the EU market. The CRA aims to mitigate the prevalent vulnerabilities in these digital products, which often serve as gateways for cyberattacks affecting not only individual organizations but also extensive supply chains and, by extension, the internal market of the EU.

Prior to the implementation of the CRA, the EU faced a fragmented cybersecurity landscape marked by disparate regulations and initiatives at both the Union and national levels. This lack of uniformity led to increased legal uncertainty for manufacturers and users and imposed burdensome compliance requirements across similar product types. The CRA addresses these challenges by establishing two sets of essential requirements: product cybersecurity requirements and vulnerability handling process requirements. The adoption of the CRA is expected to significantly enhance the cybersecurity of products with digital elements by ensuring manufacturers integrate robust security features throughout the product lifecycle.

The Cyber Resilience Act is set to enter into force in the second half of 2024 and manufacturers will have to place compliant products on the Union market by 2027. All Member States will have to appoint a national market surveillance authority for its implementation. For Belgium, it should be the CCB.

Implemented on January 16, 2023, **DORA ("Digital Operational Resilience Act")** is a regulation of the European Union that represents an important milestone in the European approach to managing risks related to digital transformation in **financial services** (EIOPA, 2023). It deals with networks and critical infrastructures becoming more interconnected, as well as cyberattacks against financial institutions growing more sophisticated. The rule is part of the European Commission's strategy for digital finance which seeks to promote innovation and adoption of new technologies while ensuring stability and protecting consumers. For the first time ever in EU legislation, DORA establishes a detailed set of rules that are binding across all member countries to enhance information and communication technology (ICT) risk management capabilities uniformly throughout Europe.

There are two legal acts included within this law: one being an amendment directive aligning existing ones with provisions from DORA itself; another being these very same measures outlined directly by said regulation for financial entities' ability to withstand, respond to and recover from any significant operational disruptions caused by an ICT problem. DORA represents a shift towards operational resilience rather than focusing solely on risk prevention.

By January 17th, 2025, every single member country must have implemented these laws fully thereby making them not only mandatory but also strategic differentiators against IT/cybersecurity risk operational capabilities within given sectors of the industry as well for all financial firms considering their operational resilience.

2.2.3 Market

Expanding need for cyber resilience and government initiatives, like advancing 5G networks and increasing cybersecurity spending, are driving **market growth**. The Belgian cybersecurity industry is highly competitive with over 440 active companies active in the sector realizing an 21% production annual growth rate (Agoria, 2022). Several innovative companies are running advanced programmes to strengthen digital security and/or are helping organizations identify and mitigate cybersecurity risks. Large international companies such as IBM, Microsoft, Eviden/Atos, Thales, Orange Belgium, Naval Group and others are enriching the Belgian ecosystem. And Belgian ones are bringing their dynamic expertise in this area (e.g.: Nviso, Cresco, Toreon, Approach Cyber, Easi, Proximus, Starion Group).

The global shift towards digitization and data protection is **increasing demand** for cybersecurity skills, transforming it from an IT task to a strategic priority. In Belgium, SMEs are particularly vulnerable due to limited resources and their connections with larger companies, making cybersecurity essential to protect their operations and data. For instance, more than 31.8% of medium-sized SMEs have experienced a cybersecurity incident, with 29.7% reporting IT service unavailability (FPS Economy, 2023d). Effective cybersecurity measures such as network access controls, data backups, secure passwords, VPNs, and encryption are essential.

Belgium is experiencing a **significant demand** for cybersecurity experts, with a 16% vacancy rate, compared to 9.1% in IT and 5% across all industries (Agoria, 2022). Of the 6,450 full-time cybersecurity positions, 1,205 remain unfilled. Flanders leads with 4,210 professionals, followed by Brussels with 1,720, while Wallonia has only 520. Furthermore, as the EU capital and NATO headquarters, Brussels requires enhanced cybersecurity expertise, driving the need for more talent and training.

2.2.4 Society

Let's now focus on the demographic composition of Belgium, the education level of its population, and the degree of digitization in the country. We will also look at the digital skills of Belgians and the employment situation in the information and communication technology (ICT) sector.

2.2.4.1 Demographic composition

Belgium has a population of approximately 11.9 million inhabitants, and it is experiencing an **aging trend**. In 2023, there are 3.6 people aged 18 to 66 for every person aged 67 or older, but this ratio is projected to drop to 2.4 by 2070 (Belgian Federal Planning Bureau, 2024). Seeing the modest population growth, this shift indicates that fewer young people are entering the workforce and therefor fewer available to work as cyber expert.

2.2.4.2 Education level

In 2023, around half of 25–34-year-olds in Belgium had a higher education qualification, which is slightly lower than the previous year (53.1%). This proportion is higher among women (57.3%) than among men (42.6%). There are also regional variations, with the highest percentage of higher education graduates in Brussels (61.6%), followed by Flanders (51.6%) and Wallonia (41.5%). This means that, despite a smaller number of young people, Belgium has a relatively **high proportion of higher education graduates** among the younger generations. This is good news for cybersecurity (OECD, 2023).

In terms of the purpose of higher education studies, in 2021 most new higher education graduates (77%) obtained a bachelor's degree (or equivalent), compared with 16% who obtained a short-cycle higher education diploma and 8% who obtained a master's degree or equivalent. This indicates that bachelor's degree programmes are by far the most popular among students in Belgium (OECD,2023).

2.2.4.3 How digital is the country?

Belgium has an **advanced level of digitalisation**. This trend is encouraged by strategic initiatives such as the ‘Digital Belgium’ plan (FPS Economy, 2021) or regional plans. Belgium stands out for its adoption of advanced technologies like artificial intelligence (AI) and big data. In 2020 and 2021, 23% of Belgian companies had adopted big data technologies, compared to 14% at the EU level. Regarding cloud computing, which is efficient for storing and analysing big data, 47% of Belgian companies had adopted it, compared to 34% in the EU. The country scores above the EU average for the digitalisation of public services (4 points above the EU average) and for ‘Very high capacity network coverage’ (78% compared to 73% in the EU). *(FPS Economy, 2023a; FPS Economy, 2023b*). Despite these good results, Belgium still has some way to go to achieve the European objectives of the digital decade and catch up with the EU leaders.

An interesting macroeconomic observation on the side, is that the historically high productivity in Belgium is no longer increasing. This is different from the past and different from other European countries. There are several explanations for this waning productivity. But it does increase the need to roll out digitalisation and the associated cyber security in such a way that implementation has a demonstrably positive effect on productivity.

2.2.4.4 Digital Skills

In Belgium, there is a **shortage of ICT specialists despite a large percentage of workers specialising in ICT**:

- In 2022, Belgium had 277,500 workers specialising in ICT, representing 5.6% of total employment (4.6% in the EU). However, the distribution is uneven according to gender, with 81.3% of ICT specialists being men and only 18.7% women, a trend similar to the European average. (European Commission, 2023a).
- 15.4% of Belgian companies recruited or attempted to recruit ICT specialists in 2022, a rate higher than the European average of 9.5%. And 10.5% of the Belgian companies say they are having difficulties filling positions requiring expert ICT skills, which is well above the European average. (FPS Economy, 2023a)

Concerning the basic and advanced **digital skills**, there is **room for improvement** despite training organized by companies:

- Around 54% of the Belgian population has basic digital skills, a figure that is in line with the European average but still well short of the 80% target set for the EU's Digital Decade (FPS Economy, 2023b).
- Lower proportion of ICT graduates than the European average (2.8% compared with 4.2%),
- In 2022, 33% of Belgian companies organized training to develop their employees' ICT skills, compared with an EU average of 22.4% (Eurostat,2023). Which reflects a proactive adoption of essential digital skills in the professional environment.

These advances show the importance of having a workforce skilled in digital skills to support economic growth, but also to improve the accessibility and quality of public services through technology.

2.2.5 Technology

Belgium stands out as an **innovation leader** in Europe, with a research and development (R&D) performance that outperforms the EU average. In 2023, the country maintained a strong position in the European Innovation Index, thanks to robust public-private collaborations and significant government support for business R&D. In terms of R&D spending, the public sector in Belgium is at 101.6% of the European average, while the private sector stands at 153.5%. Belgium continues to invest heavily in cutting-edge technologies, notably through regional programmes aimed at strengthening digital security and technological innovation (BELSPO, 2021; European Commission, 2023b).

For the private sector, the **integration of advanced technologies**, such as cloud computing and artificial intelligence, has become commonplace in Belgian sectors (see previous section). Belgium is making significant progress within this framework, particularly in the deployment of 5G (despite a low level) and the development of very high-capacity networks, supported by investments in cutting-edge technologies such as artificial intelligence and quantum computing. The objectives of the EU's Digital Decade 2030 aim to make Europe an advanced digital society. There is still room for improvement for Belgium.

Focusing on cybersecurity, there are various initiatives at both federal and regional levels in Belgium, despite the absence of a well-established center of excellence. Regarding the **federal initiatives**, the Belgian government, via the Centre for Cybersecurity Belgium (CCB), is playing a central role in overseeing and coordinating the national cybersecurity strategy. (CCB, 2021) This initiative aims to position Belgium among the least vulnerable countries in Europe, underlining that technological security and innovation are priorities for the government.

In terms of international cooperation, Belgium actively participates in programmes such as DIANA (Defence Innovation Accelerator for the North Atlantic). It also contributes through initiatives such as the ECHO network, strengthening its strategic autonomy and its ability to meet current and future cybersecurity challenges (ECHO Network, 2023).

Looking at the **regional aspect**, the third pillar of the *Walloon* CyberWal programme, through the Agence du Numérique (AdN), focuses on research and innovation and is embodied by the CyberExcellence project. Organized as a consortium and fully funded by Wallonia, CyberExcellence aims to position Wallonia as a major player in cybersecurity both nationally and internationally (Digital Wallonia, 2023). *Flanders* has adopted a proactive and strategic approach to digital transformation and cybersecurity, striving to remain an attractive region for high-tech companies. The Flemish government, notably through VLAIO, is implementing ambitious plans to encourage the adoption of new technologies such as artificial intelligence (AI) and to strengthen cybersecurity within local businesses (Vlaio, 2024). Finally, *Brussels*, as a Belgian, European and international hub, is home to many European institutions, numerous technology companies and start-ups as well as academic institutions such as Université Libre de Bruxelles (ULB) and the Vrije Universiteit Brussel (VUB) (ULB, 2023; VUB, 2023). The region focuses on digital innovation through various programmes supported by the Brussels-Capital Region (hub.brussels and Innoviris). For example, hub.brussels offers specific services to help businesses adopt advanced digital technologies and strengthen their IT security (hub.brussels, 2024). Additionally, Brussels hosts numerous international events and conferences on AI and cybersecurity, reinforcing its role in digital technology in Europe.

2.3 Literature

A comprehensive search, focusing on recent scientific articles (published from 2021 onwards) or reports, aimed at understanding the cybersecurity job market and the skills required for roles in this field. We could identify very interesting international publications. But few resources related to cybersecurity are available for Belgium. For the Belgian studies, we based our work on three main publications: First socio-economic study on the cybersecurity sector in Belgium, 2022 (Agoria), État des lieux sur la Cybersécurité à Bruxelles (Evoliris) and Belgian Digital Economy Overview, 2023 (SPF Economie).

And at internation level, we used the following interesting reports on cybersecurity: Global Cybersecurity Outlook 2024 (World Economic Forum); European Cybersecurity Skills Framework Role Profiles (ENISA), State of Cybersecurity 2023 Global Update on Workforce Efforts, Resources, and Cyberoperations (ISACA); How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce – 2023 (ISC2).

2.3.1 Roles

The literature on cybersecurity roles highlights the significant and growing demand for various positions within the field. It emphasizes the importance of roles such as security analysts, architects, and incident responders, which are crucial for protecting organizations against increasing cyber threats.

Cybersecurity roles have evolved considerably over time to adapt to new threats and technologies. Once focused primarily on perimeter defence and firewall management, these roles have diversified to encompass a wider range of responsibilities, including incident management, regulatory compliance, threat intelligence and data privacy protection. What's more, with the rise of artificial intelligence and automation, new roles are emerging to harness these technologies in the context of cybersecurity.

The roles of cybersecurity are becoming increasingly important as businesses and governments rely more and more on digital technologies. Cyber-attacks have become more sophisticated and frequent, jeopardizing the confidentiality, integrity and availability of data and IT systems. As a result, organizations are recognizing the critical importance of skilled professionals to protect their digital assets, respond to incidents and maintain regulatory compliance. (Evoliris, 2017).

Despite their importance, cybersecurity roles face a number of challenges. Firstly, the shortage of cybersecurity talent is a major obstacle, with an insufficient number of qualified professionals to meet the growing demand. In addition, the growing complexity of IT environments and threats makes the task of cybersecurity professionals more difficult. They must constantly keep abreast of new technologies and emerging attack tactics to remain effective in their role. What's more, regulatory compliance and data privacy requirements impose additional challenges, requiring specialized expertise to navigate this complex and ever-changing landscape.

Our interviews with key cybersecurity stakeholders (Vlaio, Agence du Numérique Wallonne, CCB) reveal that many companies are not fully aware of the importance of cybersecurity and the various roles within it. These organizations aim to "raise awareness" about the necessity of robust cybersecurity practices. Additionally, it is evident that having a role in cybersecurity does not always require highly technical skills or advanced degrees. Often, roles remain unfilled because companies seek overly qualified candidates for tasks that do not demand such expertise. This highlights the need for a broader understanding of the diverse skill sets that can contribute to effective cybersecurity.

ENISA has identified **twelve key roles** in its **European Cybersecurity Skills Framework**, each playing a crucial role in data protection, risk management and cybersecurity incident response (ENISA, 2022b). Those 12 roles are 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; and Penetration Tester (more info in Annex 1). However, feedback coming from our interviews with the regional cybersecurity organizations in Belgium indicates that while the ECSF is a positive initiative, it has not been fully implemented in Belgium.

Companies often base job searches on security standards like ISO 27001, which may not align with specific roles, leading to confusion for job seekers.

From the strategic leadership provided by the Chief Information Security Officer (CISO) to the forensic investigation carried out by the Digital Forensics Investigator, these roles are essential to ensuring the security and resilience of IT infrastructure. Based on the Evoliris reports, three ENISA roles play a crucial role in managing risk and preserving information confidentiality: Chief Information Security Officer (CISO), Cyber Legal, Policy & Compliance Officer and Penetration tester.

A closer look at cybersecurity roles highlights their growing importance in an ever-changing digital environment. These roles, whether technical, non-technical or managerial, play a vital role in protecting data and IT systems from cyber threats. However, to meet today's complex security challenges, it is essential to promote a multidisciplinary approach to cybersecurity, incorporating not only advanced technical skills, but also a thorough understanding of the legal, regulatory and managerial aspects of information security. By investing in skills development and fostering collaboration between the various cybersecurity players, organizations can strengthen their security posture and better protect themselves against emerging threats (Evoliris, 2017).

2.3.2 Skills

To better understand the job market in the cybersecurity sector, it is important to focus not only on the roles, but also on the various skills required to work in the field.

Skills are defined as the ability to apply knowledge and use know-how to complete tasks and solve problems. Skills can be cognitive (involving the use of logical, intuitive, and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools and instruments). (Council of the European Union, 2017).

2.3.2.1 European Cybersecurity Skills Framework ECSF

The European Cybersecurity Skills Framework (ECSF) is crucial for Belgium, aiming to create a mutual understanding among individuals, employers, and educational providers across the EU. It defines the tasks, skills, and knowledge needed for cybersecurity roles, helping to address the workforce gap by guiding specialized training programmes and fostering EU-wide collaboration. The framework clarifies essential roles and skills to bridge the cybersecurity skills gap.

Skills are defined as the ability to perform tasks at a cognitive or practical level, including soft skills for interaction. Knowledge refers to applicable facts in a field. Competencies involve applying skills and knowledge to achieve results.

The ECSF framework contains a total of 73 listed skills but the most important skills that are recurring in the descriptions of the 12 roles of cybersecurity professionals are:

- Analyse and implement cybersecurity policies, certifications, standards, methodologies, and frameworks
- Assess and enhance an organization's cybersecurity posture
- Communicate, coordinate, and cooperate with internal and external stakeholders
- Conduct technical analysis and reporting
- Design systems and architectures based on security and privacy by design principles
- Develop, champion, and lead the execution of a cybersecurity strategy
- Identify and solve cybersecurity-related issues
- Implement cybersecurity recommendations and best practices
- Manage and analyse log files
- Understand, practice, and adhere to ethical requirements and standards

2.3.2.2 Workforce Framework for Cybersecurity (NICE Framework)

In addition to the ECSF, another important framework developed to address the skills gap in cybersecurity is the **Workforce Framework for Cybersecurity (NICE Framework)**, developed by the National Institute of Standards and Technology. This framework, primarily utilized in the United States but applicable globally, serves a similar purpose to the ECSF in delineating the required knowledge and skills in the cybersecurity sector. The goal of this framework is to describe and share various information about cybersecurity work using a reference taxonomy as a common language. It notably describes the different knowledge and skills required in the sector to help students understand what skills they need to develop, job seekers to showcase their skills, and employees to perform tasks. The goal is therefore strongly similar to the ECSF in wanting to improve communication to develop, identify, recruit, and retain talent in the cybersecurity sector (Petersen et al. 2020).

The NICE framework identifies over 350 skill statements that can be used in their building blocks. Here are some examples (Newhouse et al. 2017):

- S0126: Skill in using data analysis tools (e.g., Excel, STATA SAS, SPSS)
- S0231: Skill in identifying how a target communicates
- S0266: Skill in relevant programmeming languages (e.g., C++, Python, etc.)
- S0309: Skill to anticipate key target or threat activities which are likely to prompt a leadership decision

2.3.2.3 Other Frameworks

In addition to these two frameworks, which are the most important at the European and global levels and therefore are best suited to Belgium, there are also other frameworks aimed at clarifying skills in the cybersecurity field:

- the **Skills Framework for the Information Age** in its latest version, **SFIA8**, which aims to be a global reference for skills and competencies in the digital field. Therefore, it is a framework that not only covers the cybersecurity sector, but also other areas related to digital technology. Among the more than 120 skills described by the framework, there is a specific SFIA category dedicated to information and cybersecurity, comprising 58 skills necessary in the sector.
- the **CIISec Skills framework** published by the Chartered Institute of Information Security, which also allows for the description of several competencies necessary for roles related to information security and information assurance professionals in performing their roles. It is therefore not specifically dedicated to the entirety of the cybersecurity sector but also identifies certain skills necessary for various roles in information security (CIIS, 2024).

2.3.2.4 Certifications

In the field of cybersecurity, certification is of great importance as a mark of recognition of skills and as a passport to professional opportunities. However, many individuals may face obstacles in their career progression due to the lack of specific certifications, such as the SSCP (Systems Security Certified Practitioner) or their equivalents (ISC2, 2024).

Although most roles do not require all the knowledge from certain certifications, asking for them is an easy way for companies to assess the qualifications of job seekers. However, this requirement can limit motivated individuals who do not necessarily hold certifications.

The Systems Security Certified Practitioner (SSCP) certification, for example, is highly respected in the cybersecurity industry. It is offered by ISC2, a well-known and respected organization in the field of information security. SSCP certification demonstrates that an individual has the skills and knowledge required to implement, monitor and administer an IT infrastructure using information security policies and procedures. It is recognised by employers and is seen as a mark of seriousness and demonstrates a basic knowledge of cybersecurity (ISC2, 2024)

However, if we look at the numbers, it does not seem necessary to have a certification in the field to work in cybersecurity. Indeed, in Europe, 76% of employees in cybersecurity do not have formal qualifications or certified training in cybersecurity. In Belgium, this number is slightly lower, with 70% of people working in cybersecurity not having specific certifications (European Commission, 2024b).

2.4 Labour market reports and databases

Given the limited availability of reports or databases on the Belgian cybersecurity labor market, we will examine European reports to gain insights and draw connections to Belgium. We will also review the few existing Belgian reports to compare them with European observations.

From a **global perspective**, the reports used include the ISC2 2023 Cybersecurity Workforce Study, the latest Cyberskills Report from the European Commission, the Global Cybersecurity Outlook 2024 from the World Economic Forum, and the ISACA State of Cybersecurity 2023 report.

From a **local perspective**, we utilized the first comprehensive quantitative report on the current state of the cybersecurity sector in Belgium, published in November 2022 by Agoria, the Belgian federation for the technology industry. This report includes a quantitative section based on questionnaires sent to all Belgian companies working in the cybersecurity sector (Agoria, 2022). Additionally, students from the Solvay Brussels School conducted an analysis of the market sector in Belgium, incorporating 168 job offers in the country.

2.4.1 Roles

To introduce the quantitative state at the level of cybersecurity roles, it is interesting to start by analysing studies conducted on a **global scale**. The ISC2 2023 Cybersecurity Workforce Study notably gathers data at the European level, allowing us to have a first idea of the state of Belgium on this subject. This study shows that even though the cybersecurity workforce is increasing at a global scale (+8.7% in 2023), the gap widens between the number of requested individuals and the number of trained individuals available, with an increase of 12.6% year after year. The workforce gap at the European level is approximately 350,000 positions, with an increase of nearly 10 percent over the year. For Belgium, representing 1.6% of the EU population, this translates to approximately 5,600 unfilled positions (Agoria extrapolation). On the other hand, 47% of cybersecurity professionals report team cutbacks due to economic instability, including layoffs, budget cuts, and halted promotions. Even though the sector appears to be in demand (ISC2, 2023).

This workforce gap in Europe was also illustrated in the latest Cyberskills survey, in which 45% of respondents identified the difficulty of finding the right candidate as a challenge for the company when it comes to recruiting staff with the right cybersecurity skills. Additionally, 44% also identified the lack of applicants as a challenge. (European Commission, 2024b).

This trend can be further exacerbated by the pressure on cybersecurity experts, potentially leading to burnout or their departure from the sector. (ISACA, 2023).

At **Belgian level**, Agoria's 2022 socio-economic study, along with interviews with key stakeholders, highlights knowledge gaps, opportunities, and challenges in the sector. Belgium's cybersecurity sector is expanding rapidly, driven by technological innovation, digital transformation and the related increasing number of cyberattacks. As of 2021, Belgium had over 6,400 full-time cybersecurity employees, with 1,205 vacancies. Agoria estimates around 4,000 unfilled cybersecurity positions nationwide and across sectors, underscoring the significant talent shortage (Agoria, 2022). But there is still no standard classification for IT professionals, making it difficult to identify specific roles in the country.

Geographically, Flanders leads with 66% of Belgium's cybersecurity workforce (4,210 FTEs), followed by the Brussels-Capital Region with 27% (1,740 FTEs), and Wallonia with 7% (520 FTEs). This imbalance also affects the distribution of companies and revenue generation.

Demographically, over half of Belgian cybersecurity professionals are aged 30-50 (55%), with 35% aged 18-29, and 10% over 50, highlighting the need to attract younger talent as the workforce ages. Gender diversity remains a critical issue, with only 19% of the workforce being women. The European Commission's 2024 Cyberskills report notes that while 70% of companies value inclusion, 56% have no women in cybersecurity roles, and 31% have only one, emphasizing the persistent gender imbalance (European Commission, 2024b).

2.4.2 Skills

Although Belgium lacks a specific study on cybersecurity skill needs, global reports help understand the market gap. Such studies are essential for accurately assessing the sector's skill shortages. In 2024, 20% of leaders reported a cybersecurity skills shortage, up from 6% in 2022 (World Economic Forum, 2024).

The "State of Cybersecurity 2023" report by ISACA provides key insights at **global level**, with a focus on professionals in North America (42%) and Europe (26%) (ISACA, 2023). The survey highlights a significant gap in soft skills like communication and leadership (55% of respondents) and hard skills such as cloud computing (47%) and security controls implementation (35%). Among recent graduates, soft skills are also lacking, with hard skill gaps in security controls (54% of respondents) and networking (39%). The importance of soft skills is growing, with top global needs including communication (58%), critical thinking (54%), and problem-solving (49%).

The 5 most important hard skills for organizations at the global level today are: Identity and access management (IAM) (49%), Cloud computing (48%), Data protection (44%), Incident response (44%) and DevSecOps (36%). And the top 5 soft skills are: Communication (listening/speaking skills) (58%), Critical thinking (54%), Problem-solving (49%), Teamwork (includes collaboration and cooperation) (45%), Attention to detail (36%).

In **Belgium**, limited data exists, but a study of 168 job offers by Solvay Brussels School of Economics and Management students reveals that the top 10 soft skills sought in the cybersecurity job market include team-related skills, communication, project management, flexibility, autonomy, proactivity, Curiosity/eager to learn, pressure resistance, integrity and negotiations. These skills align closely with global trends (Choual et al., 2023).

These are relatively similar to those sought after from a global perspective but mainly demonstrate an employer's search not only for hard skills but also for soft skills.

2.5 Conclusions

The cybersecurity market and the demand for cyber experts in Belgium are expanding rapidly due to several factors: a high level of digitalization (particularly in the private sector, but also in the public sector), an increasing number of cyberattacks, and the adoption of new regulations, such as NIS2 at the EU level. Belgium also has a large number of SMEs, which are especially vulnerable due to their limited resources and connections with larger companies, making cybersecurity crucial for safeguarding their operations and data.

In response to these challenges, various public sector initiatives have been implemented to enhance cybersecurity resilience among Belgian companies and public sector entities. The Centre for Cybersecurity Belgium (CCB) plays a central role in overseeing and coordinating the national cybersecurity strategy. Additionally, regional agencies have launched initiatives to raise awareness, integrate new technologies, and support research programmes.

Belgium stands out as an innovation leader in Europe and has a high proportion of higher education graduates. Regarding ICT specialist and digital skills, there is a shortage of ICT specialists despite a large percentage of workers specialising in ICT and there is lower proportion of ICT graduates than the European average (2.8% compared with 4.2%).

As in many EU countries, Belgium is experiencing a growing demand for cybersecurity experts and a widening skills gap in this field. The number of open positions is estimated to be between 4,000 (Agoria) and 5,600 (EU source), with the vacancy rate in the cybersecurity sector significantly higher (16%) than in the IT sector (9.1%) or the overall Belgian economy (5%). This trend is exacerbated by an aging population and a gender gap in the cybersecurity sector, where only 19% of professionals are women.

There is limited literature and reports on the roles and skills required for cybersecurity experts in Belgium. International and European publications provide a much more comprehensive understanding of the sector demand. The European

Framework for Cybersecurity Roles (ECSF) by ENISA is particularly noteworthy, identifying 12 key roles essential for data protection, risk management, and cybersecurity incident response. However, this framework is not widely adopted in Belgium. Companies often base their job searches on security standards like ISO 27001 or certifications, which may not correspond to specific roles, leading to confusion among job seekers. SMEs, in particular, are not fully aware of the importance of cybersecurity or the various roles within the field.

Regarding the skills in demand for cybersecurity, various international sources can be referenced with the following conclusion:

- International frameworks are listing the demanded skills for cybersecurity (e.g.: ECSF, NICE and SFIA8).
- International studies: ISACA for example identifies the most important soft skills (e.g.: communication) and hard skills (e.g.: identity and access management) as well as the gap in soft skills (e.g.: communication and leadership) and hard skills (e.g.: cloud computing).
- Certifications schemes are also often required by employers to ensure that cybersecurity professionals possess the necessary knowledge and skills (e.g.: SSCP, ISC2).

In Belgium, a 2022 study conducted by students identified the top 10 soft skills sought in the cybersecurity job market (e.g.: teamwork, communication). They are relatively consistent with those in international studies.

3 Questionnaire

3.1 Data collection

To test the findings from the literature review against the daily practice of Belgian companies, a sample-based questionnaire was distributed. The answers allow us to further detail and nuance conclusions from the literature review. The questionnaire included questions on both cybersecurity roles, skills and the training offer.

The questionnaire was sent to 350 companies from either the digital or the manufacturing sector. It was promoted during the plenary session for the Cyber Made in Belgium community and the Cyber Talents Board meetings. It was posted on LinkedIn by Agoria, CCB and the Cybersecurity Coalition.

We received 60 responses, exceeding our target of a minimum of 50. Survey length was the main reason for drop out. Furthermore, there was no adapted version for smaller companies which might have caused a feeling of unrecognizability. Finally, most companies are not used to or not aware of the ECSF roles. For all these reasons, we believe the answers do reveal trends but they should be balanced with the available literature, the expert panel and the job vacancy analysis.

The main characteristics of the responders:
(Find more detail in Annex 2)

Size of organizations:

- 65% are large organizations (>250),
- 30% are medium (50-250)
- 5% are small (10-50) or micro (<10).

Category of organizations:

- 45% are private organizations with a need for in-house cybersecurity professionals in another sector;
- 22% are Cybersecurity organizations/providers;
- 12% are ICT organizations with a need for in-house cybersecurity professionals;
- 10% are organizations with no need for in-house cybersecurity professionals;
- 8% are public organizations with a need for in-house cybersecurity professionals.

Sector:

- 18% are active in the manufacturing sector;
- 10% in other service activities;
- 7% in information and communication;
- 7% in media;
- 7% in construction.

3.2 Results

3.2.1 Cybersecurity roles

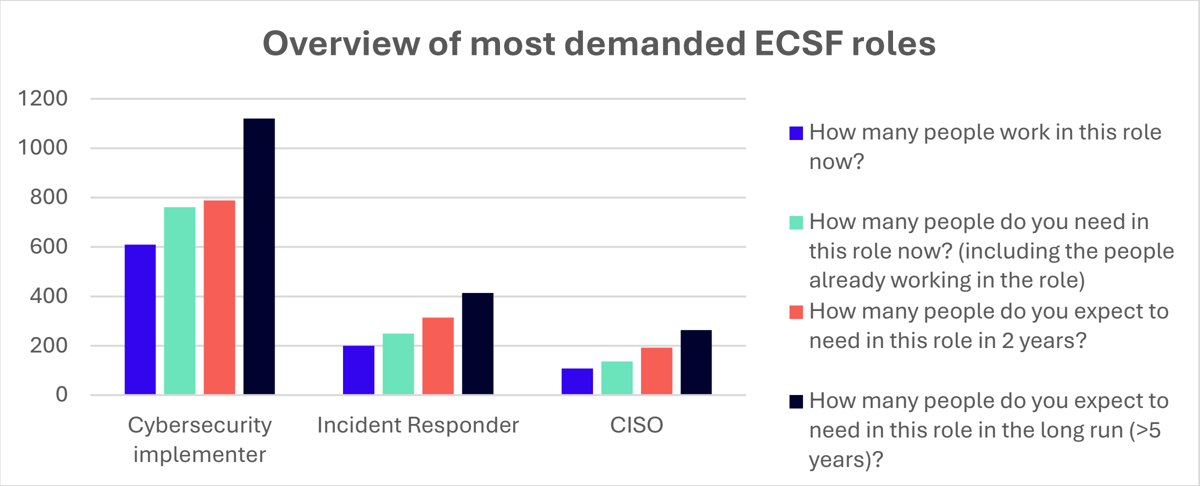


Figure 1: Overview of most demanded ECSF roles

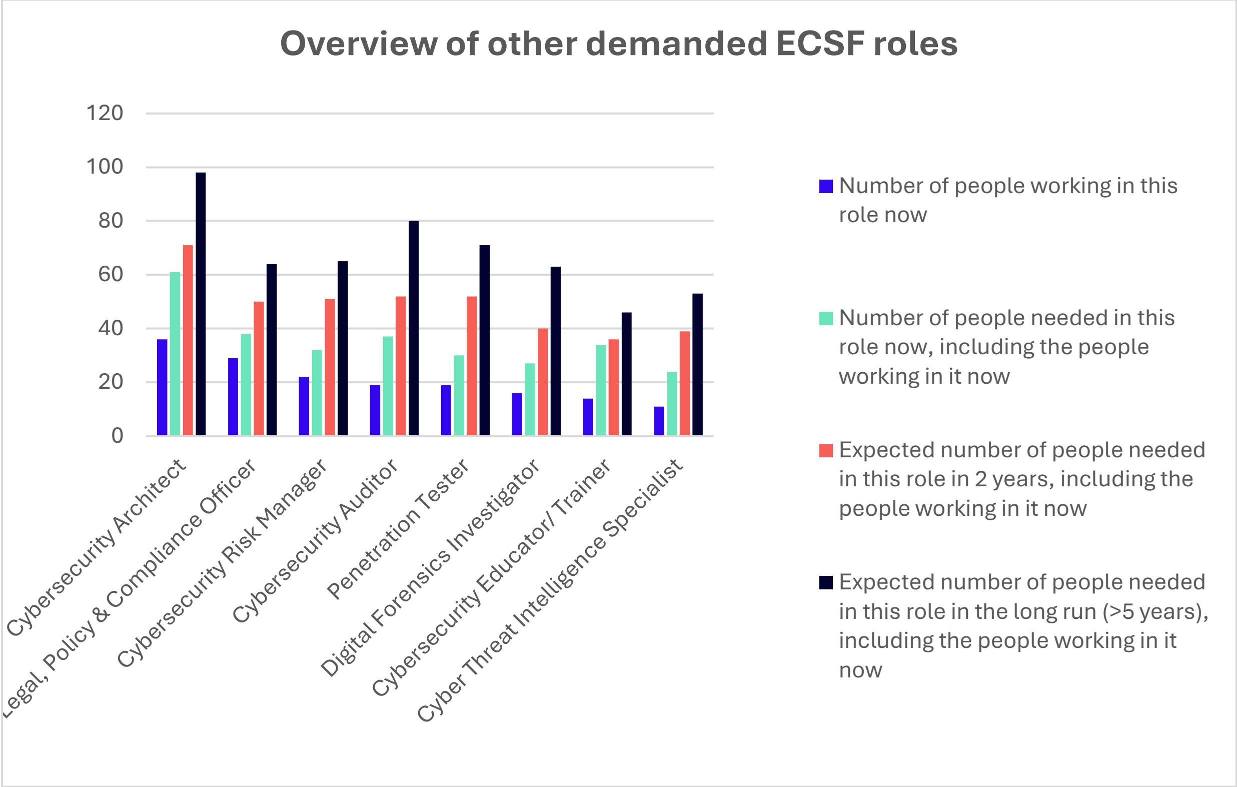


Figure 2: Overview of other demanded ECSF roles

The **ranking of most demanded roles** reflects our experience in Cybersecurity, with a very high demand for the cybersecurity implementer (56%), followed by the Incident responder (18%) and the CISO (10%). However, it is likely that some respondents selected the Implementer role as a more general term covering a series of cybersecurity experts.

For other in-demand cybersecurity roles, the cybersecurity architect is the most sought-after. This is the case especially for large companies in Belgium. However, few small companies responded to the questionnaire, and they typically answer not to require a cybersecurity architect. While roles such as Cyber Threat Intelligence Specialist and Educator/Trainer are important, they are less in demand due to their specialized nature.

We observe an average cybersecurity **vacancy rate** (% of unfilled jobs compared to the total number of jobholders needed, workers and open jobs included) of about 30%. Agoria estimated that approximately one out of six of the positions (16%) remained unfilled in 2021 in the cybersecurity sector (Agoria, 2022). The meaningful difference can be explained by the fact that firms often confuse open vacancies with the number of people they would like to employ in optimal conditions. However, the gap most probably did increase over the last years. The ISC2's cybersecurity workforce study revealed that the Global Cybersecurity Workforce Gap grew an additional 12.6% in 2023. Furthermore, the growing number of cyberattacks and the recent adoption of the NIS2 Directive are amplifying the demand for cyber experts.

Even though the total number is relatively low, the highest vacancy rates are for Cybersecurity Educators, Cyber Threat Intelligence Specialists, Cybersecurity Auditors, Cybersecurity architect and Digital Forensics Investigator. Finding good Cybersecurity educators is difficult and crucial for the future. The demand for Cybersecurity Auditors and Cybersecurity architect is increasing mostly for large entities with the NIS2 Directive.

The **increase in the demand** for cybersecurity roles in 2 years is estimated at 18% compared to the number of people needed in these roles now. Even more striking, this means +56% compared to the people working in the roles now. And the demand for cybersecurity roles in 5 years is 63% more important than the number of people needed today in these roles. Again, more outspoken, this means +116% compared to the people working in the roles now. All roles will be more demanded in 2 years and in 5 years. According to ISC2, the workforce increases in France and the Netherlands stood at respectively 14,5% and 17,1% in 2023 (ISC2, 2023). This confirms a positive trend.

3.2.2 Skills for cybersecurity professionals

The respondents were asked to evaluate the skills need for cybersecurity professionals in four categories: Cybersecurity skills, IT related skills, organization related skills and soft/transversal skills[2]The high rating given to each of them confirms the importance of all four. However, there is a more important demand for cybersecurity and soft skills/transversal skills.

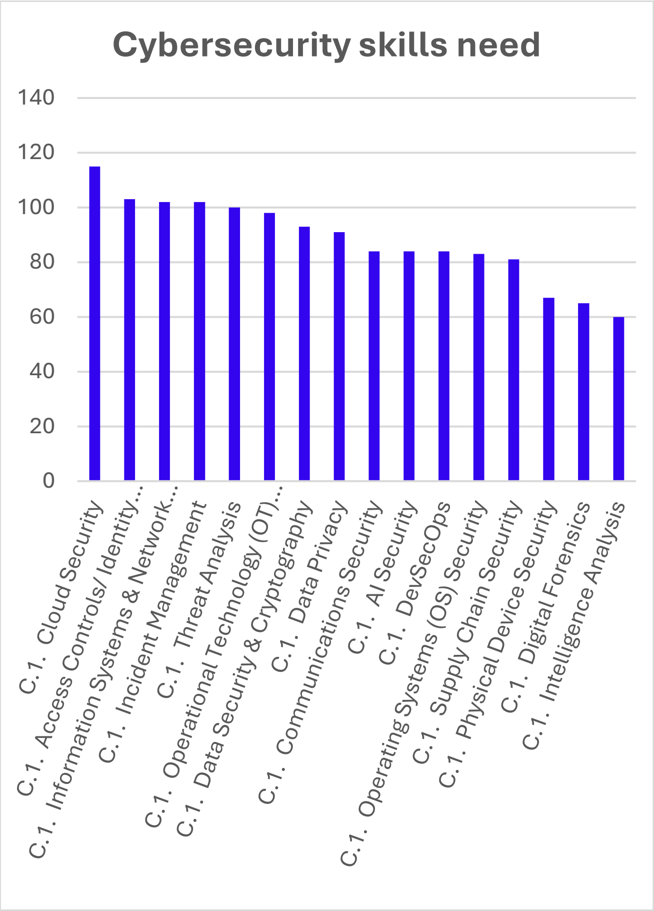


Figure 3: Cybersecurity skills need

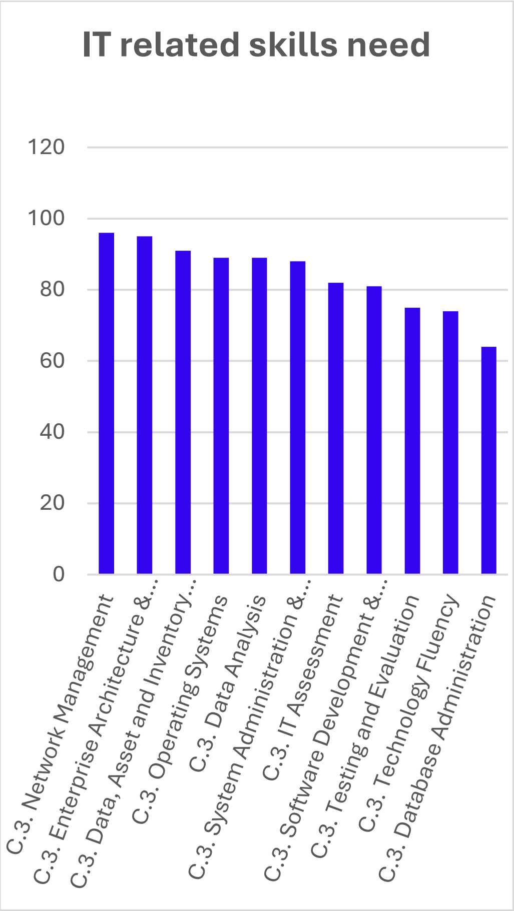


Figure 4: IT related skills need

[2] A weight has been applied to each answer to summarize and be able to benchmark the results in the graphs: Lots of need = 3, Substantial need = 2, Some need = 1, no need or not relevant = 0.

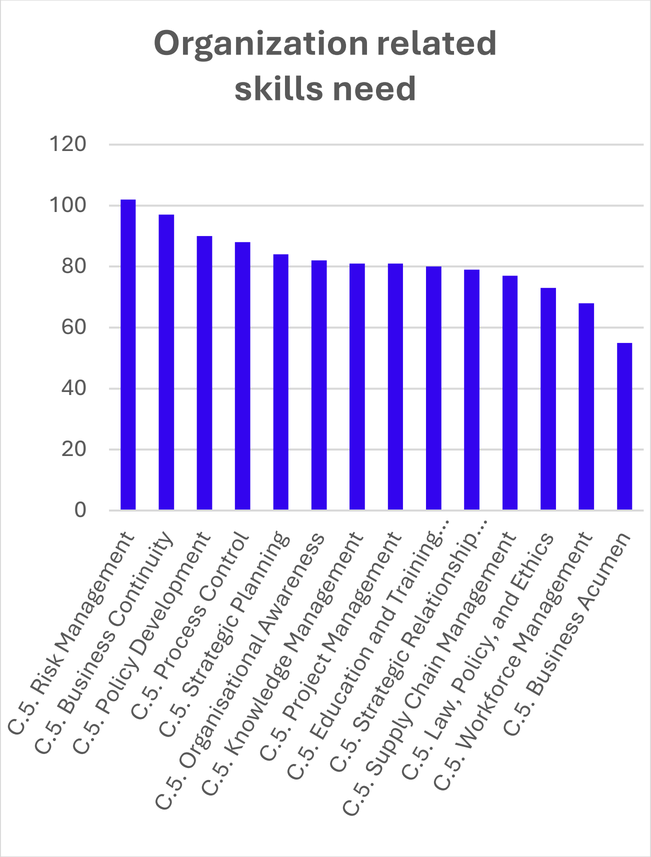


Figure 5: Organization related skills need

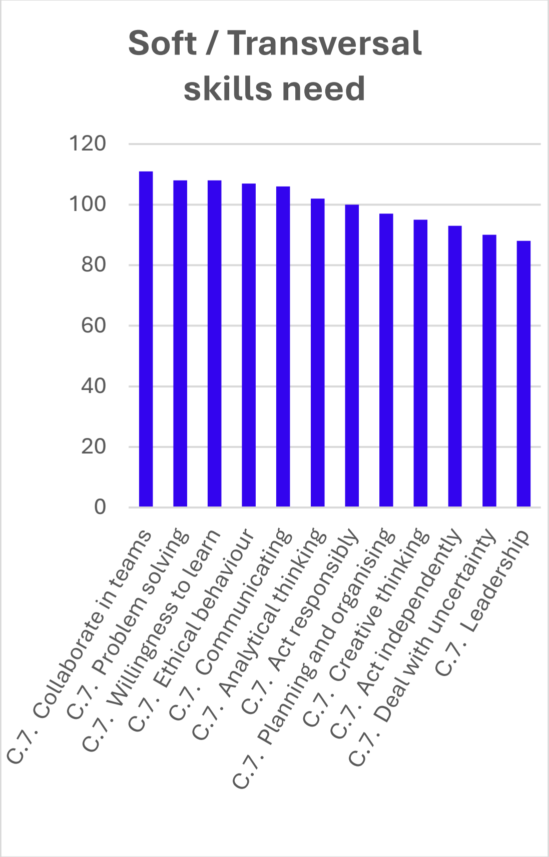


Figure 6: Soft/Transversal skills need

The three most important **cybersecurity skills** are: Cloud security (115), Access Controls/Identity Management (103) and Information Systems & Network Security/ Cyber Resiliency (102), equally with Incident Management. Some respondents added skills such as Hacking techniques, Quality control, Risk Management and Security Operation Center (SOC). Identity and access management (IAM) and Cloud computing are also the 2 most demanded skills in the ISACA study mentioned in previous chapter (ISACA, 2023).

For **IT-related skills**, the most needed skills are Network Management (96), Enterprise Architecture and Infrastructure Design (95) and Data, Asset and Inventory Management (91).

The respondents rated the following **Organization-related skills** the highest: Risk Management (102), Business Continuity (97) and Policy Development (90).

Soft/transversal skills are deemed highly important. The top three skills are: Collaborate in teams (111), Problem solving (108) and Willingness to learn (108). Ethical behavior and Communication follow closely (107 and 106, respectively). This underscores the significance of soft skills as highlighted in the literature in the previous chapter.

3.2.3 Training of cybersecurity professionals

All main reasons for having to **train personnel in cybersecurity roles** are quite important for the respondents (from 34 to 82% of the respondents consider there is a need for training of personnel in cybersecurity roles). The most important driver is that New (technological) developments ask for new skills (82%). The second most mentioned reason is the lack of a right skillset for job starters (46%). This figure naturally formes a strong basis to urge training providers to come up with a more contemporary and agile offering. Other reasons mentioned are : New business processes requiring new skills (42%); The organization switching infrastructure (38%); and Clients asking for specific skills (34%).

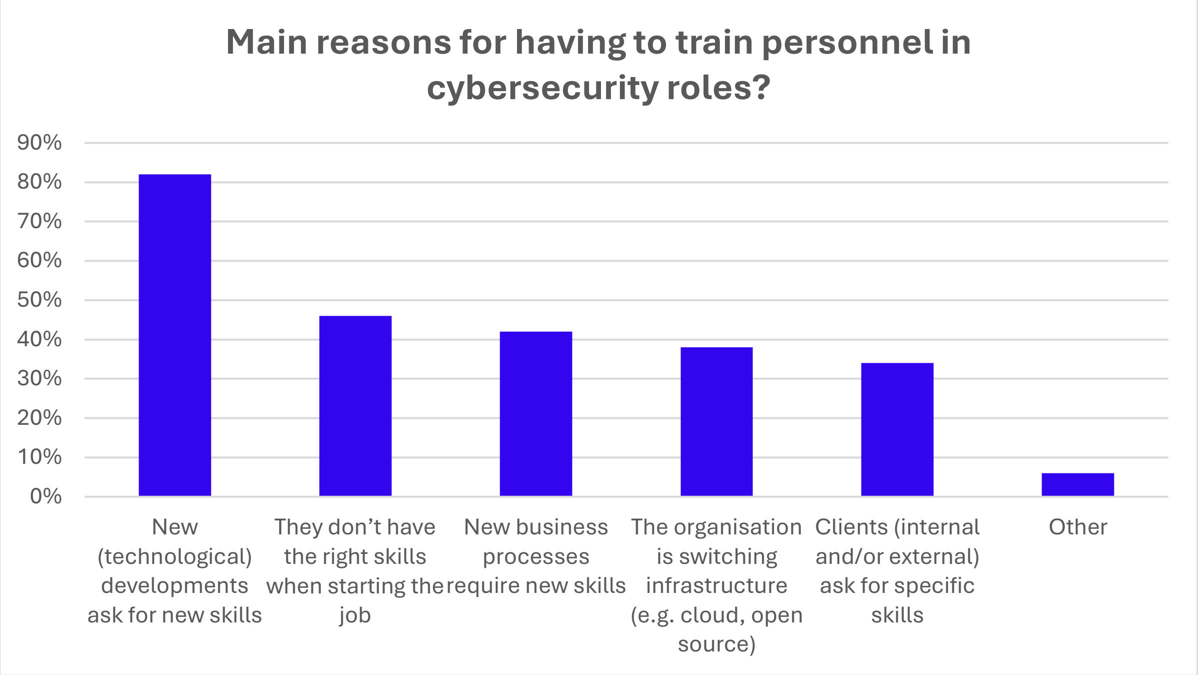


Figure 7: Main reasons for the need to train workers in cybersecurity roles

61% of respondents consider that there is **no backlog in the training** of their staff in cybersecurity roles. This relatively high percentage is in line with the European figures quoted above concerning the high proportion of Belgian companies that organized training to develop their employees' ICT skills (see 2.2.4.4. Digital skills). Some of them have their own academy.

For the remaining 39%, the first reason by far that there is indeed a backlog in training personnel in cybersecurity roles, is that the workers don't have time for training (74%). The lack of time can be explained by the growing cyber threats and market, the very fast evolution of technology and the increasing workforce gap for cybersecurity experts. This gap might also be further exacerbated by the pressure on cybersecurity experts, potentially leading to burnout or their departure from the sector (ISACA, 2023). The other reasons for a backlog are training is too expensive (39%); the organization does not have time to organize training (39%); and the organization does not have people to train them (22%).

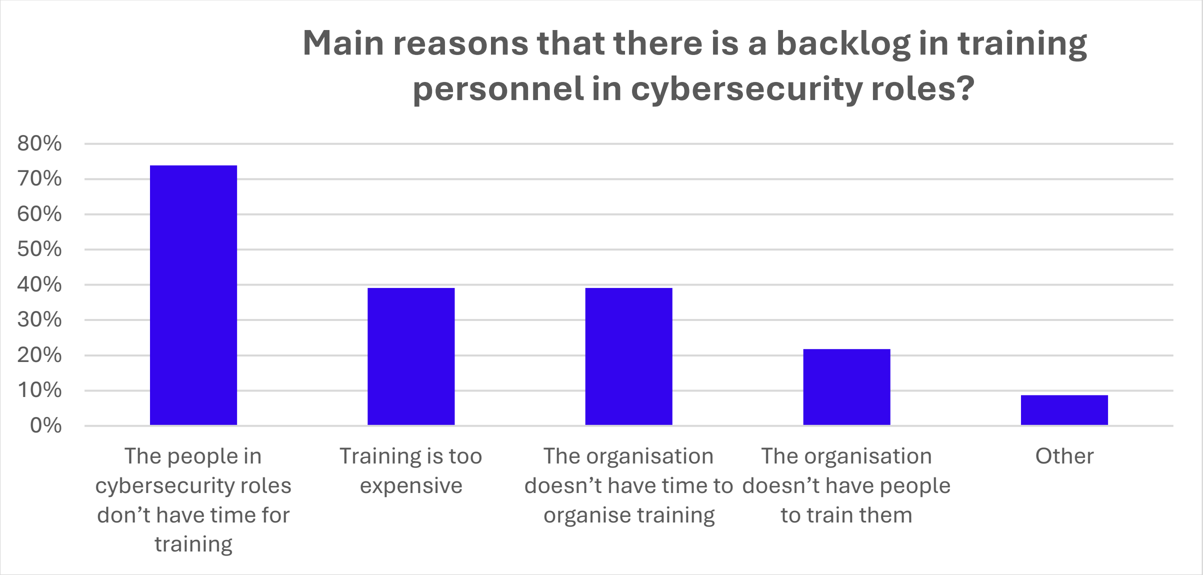


Figure 8: Main reasons for a backlog in training workers in cybersecurity roles

'On the job coaching and training' is the first **training strategy** for personnel in cybersecurity (very important or important for almost 90% of the respondents). It is followed by 'Upskill own ICT personnel' (82%) and 'Hire people and train them' (75%). The least relevant training strategy is 'Reskill own non-ICT personnel' (not relevant or some importance for 41% of the respondents). Given the shortage of cybersecurity experts, training non-ICT staff working in an area of interest (e.g. banking) could be a way of working worth exploring. It is crucial for organizations to develop a comprehensive global upskilling strategy and a plan to align with their identified business requirements, using the various strategies outlined in the graph below.

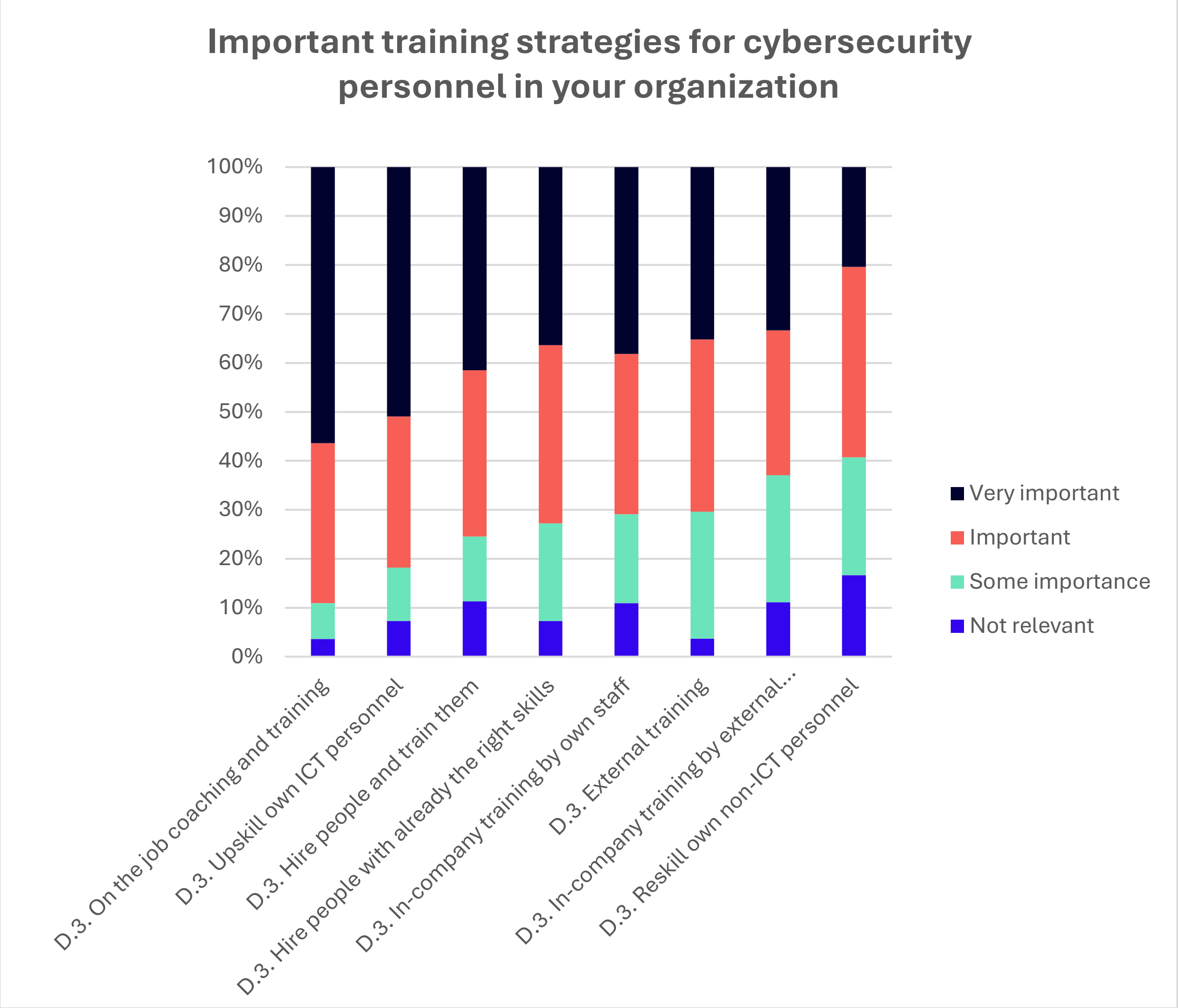


Figure 9: Training strategies for cybersecurity staff in your organization

When hiring for a cybersecurity role, the most important qualification is having Formal professional education relevant for the role (very important or important for 77% of respondents), followed by Bachelor/master degree relevant for the role (61%) and Formal certification relevant for the role (59%). The less important qualifications are Bachelor/master degree in any field (not relevant or some importance for 66%) and Formal professional education in any field (56%). It is quite logical, organizations prefer hiring qualified professionals than having to train them. However, some organizations are moving towards more creative solutions when hiring professionals in other fields. It might be beneficial to expand the hiring funnel to attract a larger pool of candidates.

In Belgium in general, based on labour market shortages, it is trending that diplomas are losing some importance while the more flexible and competency-linked micro-credentials seem to be gaining importance.

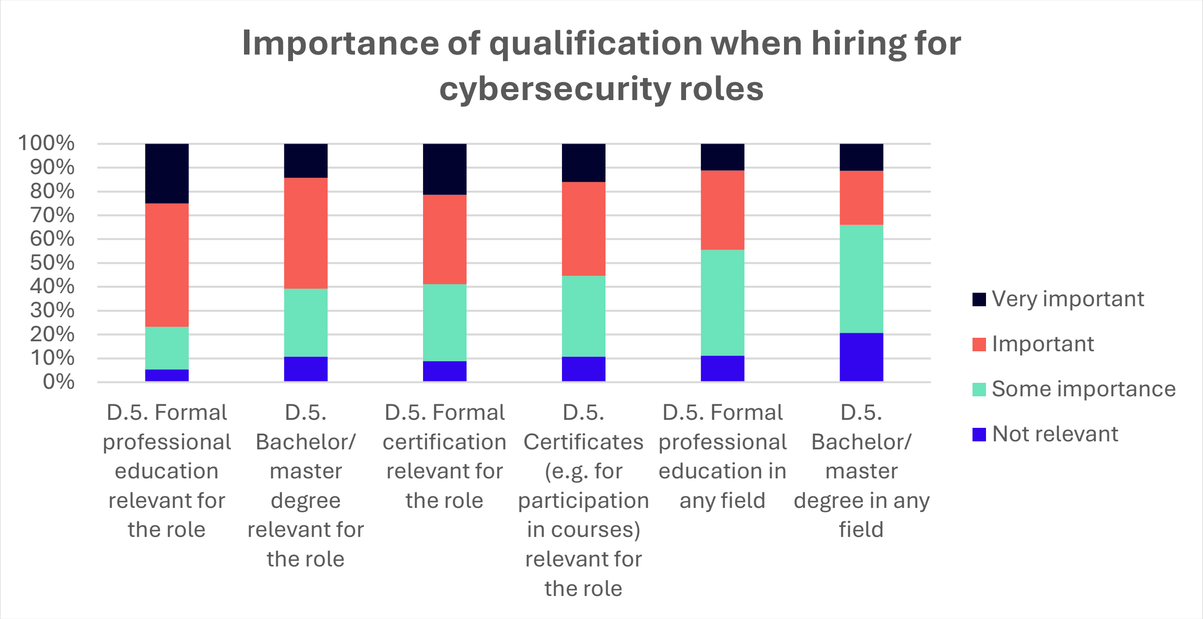


Figure 10: Importance of qualification when hiring for cybersecurity roles

3.3 Conclusions

The most demanded cybersecurity **role** is the Cybersecurity Implementer (56% of roles), followed by the Incident Responder (18%) and the Chief Information Security Officer (CISO, 10%). In 2024, there is a vacancy rate of about 30%. The difference compared to the 2021 Agoria estimation of 16% can be explained by a demand increase gap and by a traditional overestimation when conducting surveys on open vacancies in ideal circumstances. Even though the total number of demand for the role is relatively low, the highest vacancy rates are for Cybersecurity educators, Cyber Threat Intelligence Specialists, and Cybersecurity Auditors. The demand for cybersecurity roles is estimated to increase by 18% over the next two years compared to the current need, and by 56% in the next 5 years. The demand is growing at a fast pace for all roles.

The highest demand for **skills per category** is seen in Cybersecurity skills, followed by Soft/transversal skills. IT and organization related skills are also considered important. The most needed Cybersecurity skills are Cloud security and Access controls/Identity Management while the most demanded Soft/transversal skills are the ability to Collaborate in teams and Problem solving.

The primary reason for having to **train personnel** in cybersecurity roles is that New (technological) developments ask for new skills (82%). This is not surprising given the fast evolution of threats and technologies in cybersecurity. The second reason is the lack of right skills of the people starting the job (46%). Additionally, 61% of respondents believe there is no backlog in training personnel for cybersecurity roles. This relatively high percentage aligns with European figures indicating a high proportion of Belgian companies that have organized training to develop their employees' ICT skills. The main reason for any training backlog is that people don't have time for training. Regarding training strategies, 'on-the-job coaching and training' is considered the most important by respondents. It is crucial to develop a comprehensive global upskilling strategy for organizations.

4 Job vacancy analysis

In this section, we present the results of our job vacancy analysis, based on data collected from various job boards. This report has been prepared in collaboration with Abodoo (www.abodoo.com).

4.1 Data collection

The job boards that were used to collect the job vacancies are: Glassdoor, Himalayas, Indeed, Infosec, Jobat and LinkedIn. In total, 584 cybersecurity job vacancies could be found for Belgium. 84% could be linked to an Enisa cybersecurity role. The data collection was done in June 2024.

4.2 Results

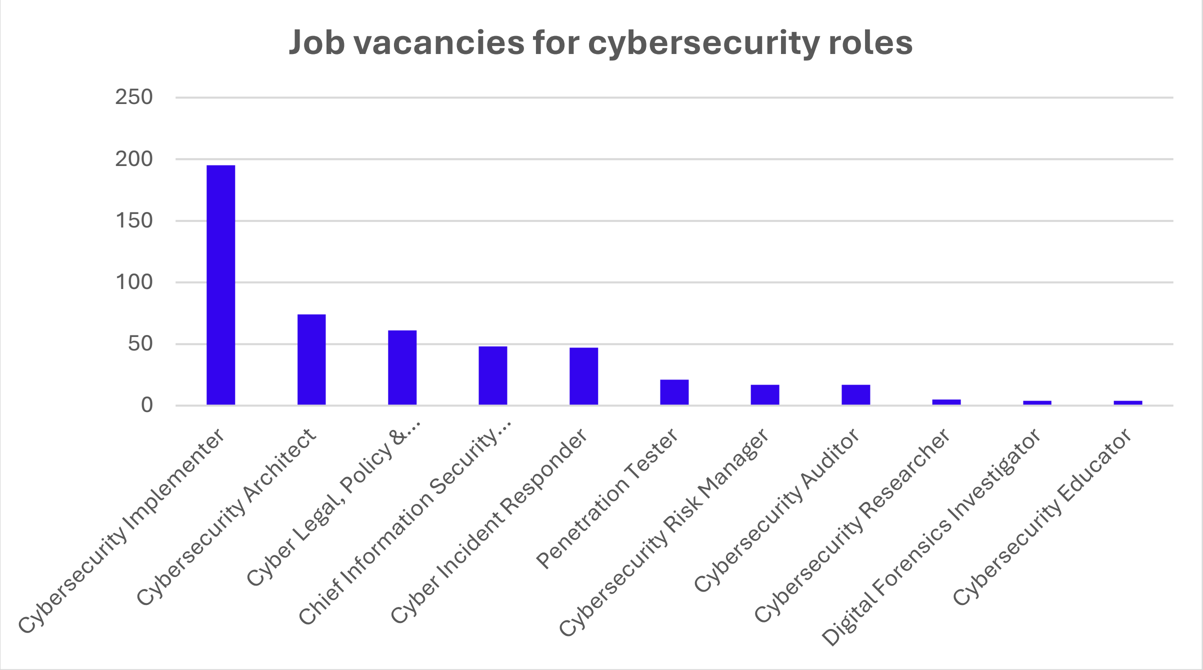


Figure 11: Job vacancies for cybersecurity roles

As goes for the questionnaire, the **role** in highest demand is by far the Cybersecurity Implementer (40%). The top five roles remain the same (questionnaire: Cybersecurity Implementer, Incident Responder, CISO, Cybersecurity architect and Cyber Legal, Policy & Compliance officer), but appear in a different order. The Cybersecurity architect and the Cyber legal, policy and compliance officer are in 2nd and 3rd position. Similarly, the 3 least demanded roles (questionnaire: Digital Forensic investigator, Cybersecurity Educator/Trainer and Cyber Threat Intelligence specialist) are also the same, though their order varies.

For the **skills**, the most demanded category is Cybersecurity skills followed by Transversal/Soft skills. But the mix of the 4 categories stands as IT related skills and Organizational skills are also very well represented. This result shows the same pattern as in the questionnaire.

The most demanded skills for each category are as follows:

	Table 1 Most demanded skills per category		
	Cybersecurity skills		**Transversal/Soft skills**
1	Incident management (291)	1	Communicating (295)
2	Access controls Identity management (214)	2	Problem solving Dealing with problems (257)
3	Information systems and network security (205)	3	Team work Collaborating in team & networks (210)
4	Data security and cryptography (176)	4	Leadership Leading others (164)
5	Threat analysis (172)	5	Analytical thinking Processing information (147)
	IT related skills		**Organizational skills**
1	Data analysis (202)	1	Project management (261)
2	System administration and integration (190)	2	Risk management (180)
3	Network management (178)	3	Strategic planning (107)
4	Operating systems (154)	4	Policy development (105)
5	Enterprise architecture, infrastructure design (125)	5	Process control (87)

The ranking aligns closely with the questionnaire but shows some differences. These differences could be attributed to the high representation of both the manufacturing and ICT sectors in the questionnaire, as well as a discrepancy between the perceived importance of skills (as indicated in the questionnaire) and the skills actually listed in job offers.

The top five cybersecurity skills align with the top seven in the questionnaire. Although cloud security, which is ranked first in the questionnaire, is not in the top five skills of the job vacancy analysis, it closely follows with 125 occurrences. Operational Technology (OT) related security (6th in the questionnaire) is rather specific to the manufacturing sector, reflecting the respondents' sector.

For transversal/soft skills, the results are quite similar to those in the questionnaire. However, the importance of communication and leadership is even more emphasized in the job vacancy analysis. Problem-solving and teamwork are also in the top three.

The top five IT-related skills are nearly the same as in the questionnaire. Data analysis ranks first here. The Organizational skills are also quite similar, except for Project management, which is only in eighth position in the questionnaire.

4.3 Conclusions

Nearly 600 cybersecurity job vacancies could be collected on job boards. The results of the job vacancy analysis are quite in line with the answers of the questionnaire regarding the demanded roles and skills.

The top five roles are:

- Cybersecurity implementer
- Cybersecurity architect
- Cyber legal, policy and compliance officer
- CISO
- Cyber incident responder

The role in highest demand is by far the Cybersecurity Implementer as we also saw in the questionnaire.

The demanded skills are also quite similar to the ones in the questionnaire. Higher importance is granted to Cybersecurity and Transversal/Soft skills. The differences are:

- Cybersecurity skills: Incident management is the most demanded skill, where in the questionnaire Cloud security came up as number one
- Transversal/Soft skills: Communication is considered even more important than in the results of the questionnaire (1st)
- Organizational skills: Project management ranks much higher (1st vs 8th)
- IT related skills: Data analysis is more important (1st)

5 Desk research (supply)

Most educational programmes of longer than 6 months, related to the cybersecurity sector in Belgium have been listed to provide an overview from the supply side. We first explain how data were collected and then present the observations that can be drawn from the programmes. We present the results of the analysis of five important programmes in Belgium compared to the ECSF/ENISA roles.

5.1 Data collection

Multiple sources were used to compile a comprehensive list of cybersecurity related programmes currently available in Belgium. These include specialized databases, websites of colleges and universities, and the websites of organizations responsible for employment and training in the three regions of Belgium[3]. The selected training programmes fall into the VET EQF 5 to VET EQF 8 categories, encompassing several months-long training programmes, bachelor's and master's degrees at higher education institutions and universities, as well as post-master's programmes. Detailed information was collected from the dedicated websites of each programme. For the most important learning programmes (+/-30), we sent mail communication to the providers to ask for additional information, including the number of learners who completed the programmeme and the total capacity of learners. We received answers from almost 2/3 of them. Finally, to better understand the content of these programmes as well as the roles they can lead to, we analysed five representative major programmes offered in Belgium, at both bachelor and master level.
(Find more details in annex 3)

Next to the examined sample, in Belgium, we also have a wide variety of short trainings in Cybersecurity. However, given the fast evolution of this offer and the scope of this study, we didn't go into detail by collecting information on these short trainings.

After our thorough research on cybersecurity training programmes, we have identified 61 long-term programmes (>6 months) offered by both traditional educational institutions and private organizations. Characteristics of these programmes:

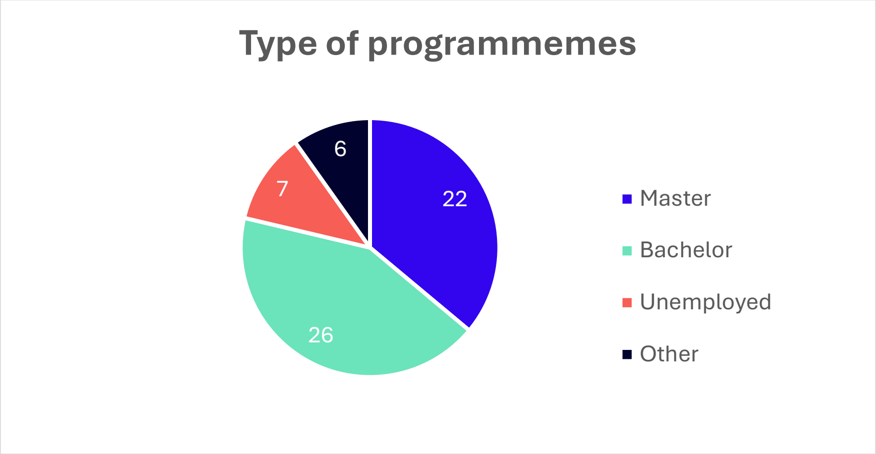


Figure 12: Type of programmes

[3] The databases used included the ENISA Cyberhead database, cybersecurity training programmes listed by the Centre for Cybersecurity Belgium, and the training programmes compiled by students from the Solvay Brussels School in a 2023 report on the cybersecurity education landscape in Belgium (ENISA, 2024; CCB, 2024c). Additionally, region-specific organizations were consulted, such as Forem, the Walloon office for vocational training and employment, the Vlaamse AI Academie database, which is the Flemish organization for technology and artificial intelligence sector training, and finally, Bruxelles Formation for the Brussels-Capital region.

5.2 Results

5.2.1 Overview & characteristics of the cybersecurity learning programmes

Regarding the **61 learning programmes**, 22 are master's level courses (EQF7) and 26 bachelor's level (EQF6). Seven programmes have been developed for unemployed people (EQF4/5). The six remaining programmes are offered by private or public institutions and are open for anyone with the required entry-level skills (EQF4/5).

The programmes are distributed as follows at regional level:

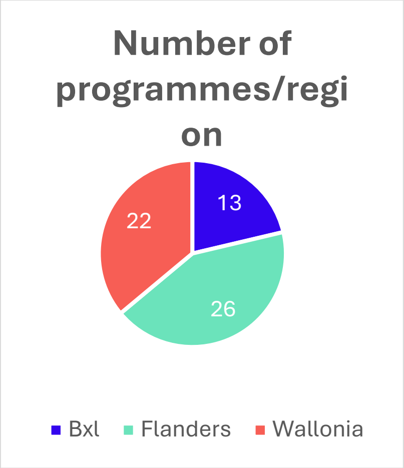


Figure 13
Number of programmes per region

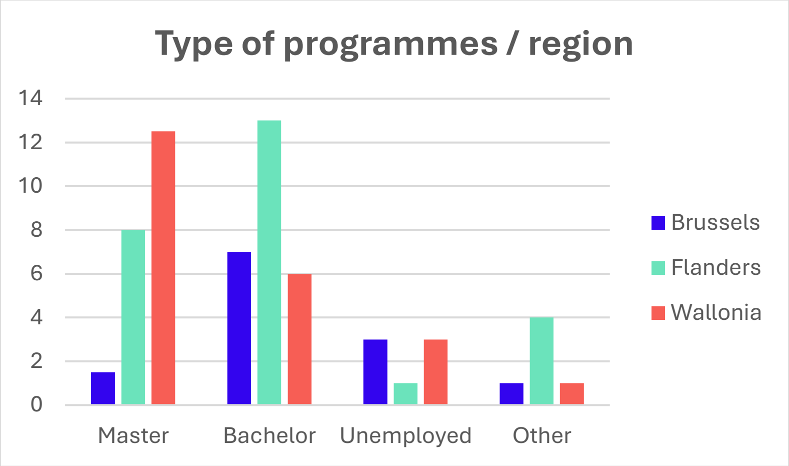
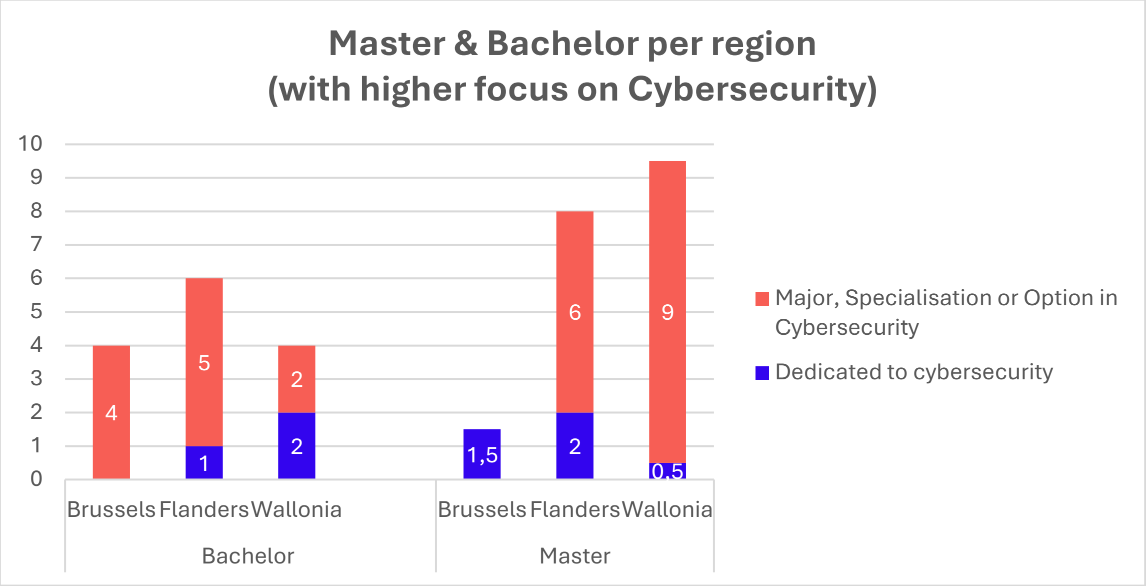


Figure 14
Type of programmeme per region

For the **Masters and Bachelor programmes**, 3 bachelors, 2 masters and 2 executive masters are fully dedicated to cybersecurity. They are well balanced across the Belgian regions. 25 programmes propose a Major, a specialisation or option in cybersecurity or a security related domain (e.g. ICT security & networks) while 16 programmes tackle cybersecurity but not as a specific priority in the whole of the programmeme (1 or 2 courses).

The regional breakout for the Master and Bachelor degree with a specific focus on Cybersecurity (32 in total):



Remark: one Master is taught in Brussels and Wallonia (RMA, ULB & co), explaining why you find 1,5 and 0,5 in the graph.

Figure 15: Master and Bachelor per region

We can highlight the following additional information:

4 masters are dedicated to cybersecurity: 2 in Flanders and 2 in Wallonia/Brussels, including 2 Executive masters aiming for a professional's target group (Brussels and Antwerp)

It is also worth mentioning that bachelor's and EQF 5 level courses are mostly taught in the language of the respective region. On the other hand, for master level courses, English is the most common used language of instruction, promoting an international scope and openness to global perspectives in cybersecurity.

Leading institutions such as KU Leuven and UC Louvain stand out for the specialized excellence level of their Master's offerings in cybersecurity, providing opportunities to specialize in specific areas such as cryptography, network security, and risk management.

One notable programme, collaborative and interregional, involves Belgian Defence as well as various Walloon and Brussels institutions, testifying to the cooperation between the civilian and military sectors in strengthening cybersecurity skills.

Learning programmes for unemployed have also been developed by regional employment agencies, often in close collaboration with partners (e.g.: Becode, Cefora, EPHEC). These programmes generally take between 6 and 12 months and include a working experience. The average number of participants lays between 10 and 15 for a group. We identified 3 programmes in Wallonia, 3 in Brussels (including 1 of the Flemish Working Agency VDAB) and 1 in Flanders.

To finish: the six **remaining programmes**, referred to as 'Other,' range from 6 months to 2 years in duration. They are offered by private or public institutions such as IFAPME, Syntra, and Centrum voor Avondonderwijs, and are open to anyone with the required entry-level skills (EQF4/5). Four progammes take place in Flanders, 1 in Brussels and 1 in Wallonia. These programmes are available as evening courses or workplace learning ('alternance'). Generally, they target individuals who are currently employed or wish to gain workplace skills. Data on shorter trainings have not been collected.

Regarding the **number of learners** who completed the programme, for Bachelor and Master degrees, the range goes from 3 learners (newly created major in Cybersecurity) to 119 learners (Master dedicated to Cybersecurity). In most cases, the programmes have no limit for the number of possible learners and could accept more students (except for the Executive Masters for example). Several training institutions reported an increase in the number of registrations (e.g.: “A noter que nous sommes en croissance constante.”; “it is expected that the number of students will organically increase in the coming years.”).

Regional employment agencies launched new training programmes for unemployed last year. Usually, groups can accommodate about 12 participants. For the programmes that have already started, according to the regional employment agencies, there are much more people interested than places available.

We can see a positive dynamic for the **creation of new training programmes**. UGent for instance set up a new Major in Cybersecurity (master’s in data science engineering) last year. Howest has transformed its ‘cybersecurity major’ into a bachelor's degree dedicated to cybersecurity this year (starting in September 2024). On French speaking side, Henallux together with HELHa is working on a project of “Master en Gouvernance de la Cybersécurité en Alternance” applying a dual learning method which involves companies in the educational process. Regional employment agencies recently launched new cybersecurity programmes. For instance, VDAB is starting 4 new training programmes, including two that are now open. Bruxelles Formation and Digitalcity.brussels completed a first training early 2024.

5.2.2 Five programmes and the ECSF roles

The results show that there are numerous programmes in Belgium for training in cybersecurity roles. To better understand the content of these programmes as well as the roles they can lead to, we analysed five major programmes offered in Belgium. We selected two EQF 6 programmes (bachelor's level) and three EQF 7 programmes (master's level, inclusive one Executive master). The purpose of this section is to briefly explain what these programmes consist of, their characteristics, and finally, to identify the different roles according to the ECSF framework of ENISA that can result from these programmes.

5.2.2.1 HELMo - Bachelier Informatique orientation Sécurité des systèmes

The Haute École Libre Mosane offers a bachelor's degree in computer science focused on system security, addressing organizational, technical, and legal aspects related to cybersecurity. The programme spans three years and includes courses totalling 180 ECTS credits. It is a practice-based education with technical projects covering various technologies. The skills developed are related to programmeming languages, computer system security, technological advancements, identifying system weaknesses, and vulnerability audits. A 15-week internship in Belgium or abroad must be completed in a company chosen by the student. (HELMo, 2024)

Institutions	HELMo, Haute Ecole Libre Mosane
Location	Liège
Duration	3 years
Work placement	15 weeks in a company
Language	French

HELMo's Bachelor of Cybersecurity programme prepares students primarily for the following roles:

Cyber Incident Responder	The Cyber Incident Responder role: trains students to identify and respond effectively to cybersecurity incidents. They learn to analyse attacks, coordinate the operational response, and restore systems securely.
Cybersecurity Architect	Cybersecurity architect
Cybersecurity Risk Manager	Cybersecurity Risk Manager: training focused on cybersecurity risk management, where students learn to identify, assess and mitigate risks associated with information and system security.
01010 11101 00101 Penetration Tester	Penetration tester

5.2.2.2 Howest – Bachelor in Cybersecurity

Howest University of Applied Sciences offers a bachelor’s degree in Cybersecurity. The goal of this programme is to train cybersecurity experts who are ready for a cybersecurity profession and who combine the attacker mindset, the defender mindset, the ethical mindset as well as the organizational mindset. It is an EQF Level 6 programme of 180 ECTS, which means it is a bachelor's degree designed to launch a career in cybersecurity.

The first year focuses more on computer science and fundamentals, including programmeming, scripting, web, networking, and IT law. The second year is intended to explore in depth offensive aspects and most of the defensive areas, as well as security management and threat modelling. Finally, the last year elaborates on specialized domains such as industrial and IOT security, incident response, threat intelligence, cryptography, cybersecurity of and with AI as well as practical applications in the field, including a security audit in a real organization, an internship and communication.

The Howest Bachelor explicitly uses the ENISA CSF roles model to validate the completeness of their curriculum by maintaining a traceability matrix of where in the programme the skills and competences listed in the model are covered precisely. The following roles are fully covered: Cyber Incident Responder, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Educator, Cybersecurity Implementer, Digital Forensics Investigator and Penetration Tester.

Institution	Howest University of Applied Sciences
Location	Bruges Station Campus - Building J
Duration	3 years, 20-24 hours per week
Work placement	Real assignments, internship
Language	Dutch & English

Howest's Bachelor in Cybersecurity mainly prepares you for the following roles (top 5):

Penetration Tester	Penetration Tester: This programme equips students with the skills needed to perform penetration testing, where they assess the security of computer systems by simulating attacks, essential for the Penetration Tester role.
Cyber Incident Responder	Cyber Incident Responder: Training includes modules on security incident response, preparing students to effectively identify, analyze and resolve security incidents, crucial skills for a Cyber Incident Responder.
Cybersecurity Implementer	Cybersecurity Implementer: this programmeme includes courses that lead to the Cybersecurity implementer role.
Cybersecurity Architect	Cybersecurity Architect: this programmeme includes courses that lead to the Cybersecurity architect role.
Digital Forensics Investigator	Digital Forensics Investigator: The programme also offers training in Digital Forensics, preparing students to conduct forensic analysis after security incidents. This role involves the recovery and analysis of digital data to understand how a security breach occurred and to identify the perpetrators, aligning well with the needs of a Digital Forensics Investigator.

5.2.2.3 KU Leuven - Master of Cybersecurity

KU Leuven offers an advanced master's programme in Cybersecurity. This EQF 7 programme, consisting of 60 ECTS, is primarily aimed at master's students with a background in electrical engineering, computer science, or mathematics who have an interest in the field of cybersecurity. The goal of this programme is to enhance students' skills in the legal, commercial, and operational aspects of cybersecurity. The programme addresses five main areas: cryptography, privacy, hardware security, secure software, and system security. The first semester covers these topics, and then four of them are selected for more in-depth study. The second semester focuses on specializing in two themes, along with a common legal course for all students. (KU Leuven, 2024)

Institution	Katholieke Universiteit Leuven
Location	Leuven
Duration	1 year
Thesis/Research	Research seminars and master's thesis
Language	English

The Master in Cybersecurity at the University of Leuven prepares students in priority for these roles:

Penetration Tester	Penetration Tester: KU Leuven's programme teaches cryptography and network security, preparing students to assess the security of computer systems by simulating attacks, a key skill for penetration testers.
Cybersecurity Architect	Cybersecurity Architect: The programme includes specialized courses in secure system design and digital platform security, equipping students with the skills needed to design and develop robust security architectures.
Cybersecurity Researcher	Cybersecurity Researcher: The programme's coverage of advanced cryptography and privacy techniques positions students well for cybersecurity research roles, where they can develop new methods and technologies to improve computer security.
Cybersecurity Educator	Cybersecurity Educator: According to the programmeme manager, the programmeme can also lead to the Cybersecurity educator role.

5.2.2.4 ULB, ERM, HEB, HELB, UCL, UNamur - Master in Cybersecurity

Four universities and two colleges together offer a special master's programme in cybersecurity. The institutions participating in the programme are the 'Ecole Royale Militaire', Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Haute Ecole de Bruxelles, Haute Ecole Libre de Bruxelles. This two-year programme, representing 120 ECTS credits for the entire master's degree, is accessible to students holding a bachelor's degree in computer science or engineering, as well as IT professionals and individuals seeking a second master's degree.

The programme covers various topics in cybersecurity, including cryptography, systems and networks, legal and ethical issues, human rights, security management, and software engineering. The first year is intended to provide a common foundation of knowledge, and the second year focuses on more advanced topics. Students can choose between courses focused on system design and analysis or corporate strategy and must complete a mandatory long-term internship of approximately 12 weeks. (ULB, 2024)

Institutions	Ecole Royale Militaire, Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Haute Ecole de Bruxelles, Haute Ecole Libre de Bruxelles
Location	Brussels (ULB/ERM/HEB/HELB), Louvain (UCL), Namur (UNamur)
Duration	2 years
Workplace placement	Internship in year 2
Language	English (90%), French (10%)

Here are the four main roles prepared by this programme, which is offered at the various universities.

Penetration Tester	Penetration Tester: Students acquire the skills needed to identify and exploit system vulnerabilities, in order to improve their security through rigorous penetration testing.
Cybersecurity Auditor	Cybersecurity Auditor: The programme prepares students to carry out security audits, assessing systems and policies to ensure compliance with standards and regulations.
Cyber Incident Responder	Cyber Incident Responder: This role involves preparation to identify and manage responses to security incidents, developing effective strategies to detect, contain and resolve intrusions.
Digital Forensics Investigator	Digital Forensics Investigator: Students learn to retrieve and analyze post-incident digital data, essential for understanding how and why a security breach occurred, preparing them for the role of Digital Forensics Investigator.

5.2.2.5 Solvay Brussels School - Exec. Master in Cybersecurity Management

The Executive Master in Cybersecurity Management is a programme offered at the Université Libre de Bruxelles, specifically within the Solvay Brussels School of Economics and Management. It is an EQF Level 8 programme, which means it is a post-master's programme primarily aimed at professionals who want to develop their skills and knowledge in the field of cybersecurity. The programme runs from January to December, with sessions held 2 to 3 days per month, including group projects. The prerequisites for the programme are at least 5 years of experience and involvement in managerial decision-making related to digital or cybersecurity activities. (Solvay Lifelong Learning, 2024).

Institution	ULB, Solvay Brussels School of Economics and Management
Location	Brussels, ULB Solbosch campus
Duration	1 year, 2-3 days per month
Work placement	For professionals
Language	English

Solvay's Executive Master in Cybersecurity Management course mainly prepares you for the following roles:

Chief Information Security Officer (CISO)	Chief Information Security Officer (CISO): The programme offers a comprehensive module on information security leadership, preparing participants to oversee the organization's IT security strategy, including governance, risk management and incident response.
Cyber Incident Responder	Cyber Incident Responder: The Security Operations module trains participants in incident management, giving them the skills to identify, analyse and respond effectively to security incidents.
Cyber Legal, Policy and Compliance Officer	Cyber Legal, Policy & Compliance Officer: Through discussions on governance, risk, compliance and certification, the programme prepares participants to manage the legal and compliance aspects of security initiatives.
Cybersecurity Architect	Cybersecurity Architect: The programme includes a specific module on security architecture, preparing participants to design and develop robust security infrastructures to protect data and resources.
Cybersecurity Risk Manager	Cybersecurity Risk Manager: Training covers cybersecurity risk management, enabling participants to develop strategies for identifying, assessing and managing risks associated with information security.

5.2.2.6 Comparison of five programmes linked to the ECSF roles

Table 2: Comparison of five programmes linked to the ECSF roles

	HELMO	Howest	KU Leuven	ULB	Solvay
CS Implementer		x			
Incident responder	x	x		x	x
CISO					x
CS Architect	x	x	x		x
Compliance officer					x
CS Risk manager	x				x
CS Auditor				x	
Penetration tester	x	x	x	x	
CS Researcher			x		
Digital forensics investigator		x		x	
CS Educator / Trainer		x	x		
Cyber Threat Intelligence Specialist			x	x	x

All roles are covered. For the Cybersecurity implementer, the most demanded role, there is only one training leading to this role. The main tasks of the Cybersecurity Implementer are typically handled by an IT expert, overseen by a CISO or CIO. However, the standard training for an IT expert is in Applied Computer Science, not in a dedicated cybersecurity programme. Therefore, it is crucial that all Applied Computer Science programmes include mandatory cybersecurity courses.

5.3 Conclusions

In conclusion, our extensive literature search and our contacts with training institutions about the supply of cybersecurity training programmes in Belgium has revealed a rich landscape of educational opportunities:

- A wide range of EQF classification levels, spread across different regions and offered in several languages enabling a broad spectrum of educational and professional needs to be met.
- A broad range of Masters and Bachelors dedicated to Cybersecurity or with cybersecurity Major, Specialisation or Options in Cybersecurity in the 3 regions, including some high-level programmes and a large choice of training options.
- A positive dynamic with new training programmes for students and for unemployed, and an increasing number of registrations.
- The analysis of five major programmes has shown that these courses are structured to cover almost all of the 12 roles defined in ENISA's ECSF competency framework, illustrating the comprehensiveness of the cybersecurity training available. This coverage ensures that graduates are well prepared to take on a range of essential cybersecurity roles.

However, there is still room for improvement:

- Master's and bachelor's degrees could welcome more students and should attract more women.
- Each university/higher education could have a cybersecurity major, specialisation or option and all IT-related master's and bachelor's degrees should have courses in Cybersecurity (today some of them still have few or no course in this domain).
- New training programmes for unemployed could be launched (more people interested than places available).
- The reskilling training avenue should be explored further (see ‘Other’ category and Executive masters). More data could be collected on long and short trainings to identify the possible gaps (e.g.: only one programme in ‘Other’ for the Walloon Region). And workers should be encouraged to reskill in cybersecurity.
- We don’t have a deep understanding of the quality of all learning programmes. It requires a deeper analysis. However, from the expert panel or contact with the industry and based on the good practices of the 5 analysed programmes, we can identify three areas for quality improvement for many programmes: better adapt the programmes to the last cybersecurity evolution (train the trainer) and the needed roles and skills, work more closely with the field (e.g.: stage, workplace learningg/alternance, lecturers, etc.) and teach soft skills (communication, etc.).

By continuing to develop and refine these training pathways, Belgium is ensuring a strong defence against cyber threats and a secure digital future for all sectors of society.

6 Expert panel

6.1 Data collection

An expert panel was convened a first time in June. The initial results of the study were shared for feedback during a meeting with cyber talent stakeholders in September.

For the expert panel, participants were invited via e-mail to participate in a two-hours online session on the 25th of June. The invitation was sent to a total of 14 entities representing higher education, enterprises, defence and Agoria. In the end 11 participants were selected with different backgrounds and functions ranging from HR to a more business background (find more info in Acknowledgments): higher education in cybersecurity (2), public entities linked to cybersecurity (2), the cybersecurity industry (6) and a senior expert in education and labour market (1). Also the two managers of the CyberHubs project at Agoria were present in the meeting. Floriane de Kerchove (Senior Advisor Advocacy Digital) and Eric Van Cangh (Senior Business Group Leader Cybersecurity) both acted as the moderators and coordinators of the meeting.

The participants shared their views about cybersecurity roles, skills and training & education needs in the short run (next 2 years) and the long run (> 5 years). To facilitate the discussion, the participants were asked to fill in a form and evaluate the demand for the 12 ECSF/ENISA cybersecurity roles and the cybersecurity skills needed for each profile (see annex 4). We gave the possibility to choose the following answers: *Low/Medium/High and Shrinking/Stable/Growing*. For the training & education section, we held an open debate.

The meeting with the cyber talent stakeholders took place on September 24th. This group consisted of representatives from companies or institutions active in cybersecurity (8), training entities (1), and Agoria (4). They validated or nuanced the main results of the analysis, and their remarks were integrated into the report.

6.2 Results

6.2.1 Cybersecurity roles

All participants agree that the demand for most of the roles will be classified as medium to high and will be stable or expand in the **next two years**. There is a direct link both with the implementation of NIS2 and other regulations such as DORA and with a growing number of cyberattacks.

The panel also highlights the significant differences between large companies and SMEs. SMEs have different needs, budgets and expectations compared to larger enterprises. Therefor the panel thinks it is important to distinguish these two. For example, an SME is unlikely to hire a Cybersecurity Architect or a CISO, as these roles are rather not suited to their size. Instead, small companies will increasingly work with Managed Security Service Providers (MSSPs) and will not have internal cybersecurity experts.

"There is a big difference between big companies and SMEs. For a Cybersecurity architect or a CISO for example. And you have a lot of SMEs in Belgium. Small companies will not hire a CISO for instance, it is much too expensive. They will work with an MSSP."

During the CyberTalents meeting, participants emphasized that the primary challenge consists in finding senior-level cybersecurity professionals.

Focusing on the various roles, we can summarize the result of the survey and the discussion in the expert panel about the demand for cybersecurity roles in the next 2 years as follows:

- Roles, highest in demand and growth (> 7/10)
  CISO, Cyber Incident responder, Cybersecurity Risk manager, Cybersecurity auditor
- The increasing need for internal and external cybersecurity auditors is fully related to the need for certification and to NIS2
- For the CISO role, there was a discussion about the evolution in the next 2 years and > 5 years: medium demand now and growth > 5 years because of NIS or high demand now and stable > 5years? Panelist state that this will probably depend on the size of the organization and the sector the organization belongs to.
- Cybersecurity researcher: the need for this less demanded role is considered as medium and stable in the next 2 years.
- Cybersecurity architect and Digital forensic investigator: the demand for this profile is estimated as 'medium' (important role but not necessary in all companies) and is growing or stable. A Cybersecurity architect is again a role suitable for big companies and less for SMEs.

Overall, the panelists believe that the long run demand trend (> 5 years) should be a bit more stable due to the fact that NIS2 will already be implemented. They do however think that this demand would still be medium to high for most roles. It is expected that the demand of larger organizations stabilises over time but that the smaller enterprises need to catch up and thus still have a growing demand in the long run. It can explain the different evolution perceptions of the participants.

"We are implementing in two phases: larger companies will likely stabilize within five years, while smaller companies will catch up."

The impact of AI was also an important topic during the debates. A participant suggested that AI could possibly reduce the necessity of recurrent cybersecurity activities (e.g.: compliance officer, cyber incident responder). Others agree that AI will have an impact but that it will not reduce the need for those roles and that impacted activities (for the compliance officer for example) will be embedded within the business (e.g.: HRM, purchase will have control over their processes including compliance activities and legal concerns).

"Perhaps - or should I say probably - in five years, AI could significantly assist with specific recurrent cybersecurity activities. We need to take that into account."

Deep diving into the evolution of the various roles in the long run, the conclusions are:

- The demand for six roles should remain relatively high (> 7/10 respondents): CISO, Cyber Incident Responder, Cybersecurity risk manager, Cybersecurity auditor, Cybersecurity educator and Cybersecurity implementer.
- Even though the panelist expect a more stable situation in > 5 years, a majority of the participants think that the demand will grow for the following roles: Cyber legal and compliance officer, Cyber threat intelligence specialist, Cybersecurity risk manager, Cybersecurity auditor
- The Cybersecurity risk manager and the cybersecurity auditor will also be in high demand. The Cybersecurity risk manager is the foundation of a cybersecurity strategy. In the long run, this role should be a 'commodity' and should be integrated in the business section of all companies.
- The outlook for the next two years is quite similar to that of the next five years for 2 profiles: Cybersecurity researcher and Penetration tester. For the cybersecurity researcher, the demand is expected to remain mainly low to medium and stable. For the Penetration tester, it remains medium or high and stable or a slight growth.
- Cybersecurity architect: medium to high demand and more stable in 5 years than on short notice. This role is more suitable for large companies that should already have this role in place in 5 years. It should be integrated in the enterprise architect job.
- Digital Forensics Investigator: the demand is expected to remain mostly medium and very stable in the long run.

6.2.2 Skills for cybersecurity professionals

Identifying the skills in a form is challenging for participants, especially companies, and is difficult to accomplish in a short amount of time. Therefore, the results can only provide a global view on skills.

Both technical and soft skills are considered very important over the **next two years**. Regarding soft skills, communication (for all profiles except Digital Forensic Investigator and Pen Tester) and stress resistance (especially for CISO and Cyber Incident Responder) are mentioned most often. Soft skills, such as communication and learning capacity, are key for cybersecurity roles and are becoming increasingly important. Companies participating in the panel emphasize that having only technical skills is not sufficient.

Some participants noted that while generalization of roles can be useful, the required skills vary significantly depending on the domain in which professionals work. For example, the skills needed for a Pen Tester will differ based on whether they are working in network security, mobile security, Microsoft environments, Linux environments, etc. This variability makes it difficult to precisely define the skills for each role.

According to participants, the main innovation trends that will impact cybersecurity skills over the **next five years** include AI, quantum computing, native cloud, and confidential High Performance Computing (HPC). Governance is also highlighted as an important factor by one participant. Anotherr participant emphasises that part of cybersecurity expertise will become a ‘commodity’. It will or should be integrated into other professionals’ tasks (e.g.: manager).

> *"The main technology trends that will change the content of the jobs in the future are AI, post-quantum and native cloud. Confidential HPC could also have an important impact."*

The new hard skills identified for each role are as follows:

- CISO: Native cloud risk management, AI
- Cyber incident responder: automation, native cloud incident response, advanced technology facing
- Cyber compliance officer : AI legal
- Cyber Threat Intelligence specialist : machine learning
- CS Risk manager: architecture, Security by design
- CS architect: native cloud security
- CS educator: new technologies/controls/threats/education models
- CS implementer: business links
- Pen Tester: native cloud, post quantum, AI

Regarding soft skills, participants believe they will become increasingly important in the long run, with communication being a key example.

6.2.3 Training of cybersecurity professionals

The main findings of the expert panel for the training of cybersecurity professionals in the **next 2 years** are as follows:

- Reskilling: Training individuals already working in a specific sector for a cybersecurity job can sometimes be more effective than hiring a cybersecurity expert. These individuals tend to stay with the company longer, whereas cybersecurity experts may change jobs more frequently. For example, initiatives in the banking and insurance sector (e.g., partnership between Febelfin and Solvay) have shown success.

> *The best way to find and keep people is to reskill people working in a specific sector, such as the insurance sector, and train them in Cybersecurity.*

- Learning methods: Project-based learning, skills-based learning on the spot, knowledge sharing, and interdisciplinary collaboration are crucial. Sometimes, you learn more by exchanging experiences with peers than through formal training. Creating a community of CISOs to share knowledge, for example, would be beneficial.

- Communication skills: It is not enough to have highly technical people; soft skills are also essential. When hiring, soft skills are a critical criterion. Fifteen years ago, there was a preference for technically proficient candidates; today, we prioritize candidates with a good attitude and basic skills, knowing that technical training will be provided. Many companies organize training sessions to teach communication skills to their cybersecurity experts. These skills should also be included in cybersecurity education programmes and embedded inside every training topic.

> *Training in communication skills is crucial for the success of cybersecurity professionals. While we have many technically proficient individuals, the ability to explain their work to others is essential. Without this skill, even the most knowledgeable person is as ineffective as a book lying on a desk.*

- Lifelong learning: Internal training and certifications are vital for keeping skills updated in a rapidly evolving environment and for providing career growth opportunities for cybersecurity professionals.
- Partnerships/Collaboration: Some organizations launch initiatives with partners. For example, the Defence sector establishes partnerships through the Royal Military Academy (RMA) or presents Cyber Defence to students.
- Importance of real environments to attract students: Howest organizes Hackathons and 'Capture the Flag' initiatives and has an OT demonstrator. A key element in attracting students to thebachelor's programme is the promise of hands-on experience, fully hackable in their second year.
- Diversity: the percentage of women in cybersecurity is very low. The training and education institutions as well as the professional actors should work on attracting more women in the sector.

In the **long run (>5 years)**, soft skills, especially communication skills, will become increasingly important. As work becomes more virtual (e.g., decentralized autonomous organizations, generative AI), the real human added value lies in communication, face-to-face interaction, complementarity, and pedagogical capacity. Educational institutions should place a greater emphasis on integrating these communication skills into their programmes.

> *Currently, the focus is 90% on hard skills and 10% on soft skills. I believe educational institutions should aim for a 50-50 balance. This shift would give people a better chance for a brighter career and enable them to perform their jobs more effectively.*

6.3 Conclusions

All participants agree that the demand for most of the **roles** will be classified as medium to high and will be stable or expand in the next two years. This is the direct consequence of the implementation of NIS2 and other regulations such as DORA, as well as of the growing number of cyberattacks. The roles with the highest 'high' and 'growing' votes are the CISO, Cyber Incident responder, Cybersecurity Risk manager and Cybersecurity auditor. The participants also highlight the significant differences between large companies and SMEs. Small companies will not hire a CISO for example, they will work with a MSSP.

Participants believe that the long run demand trend (>5 years) should be a bit more stable due to the fact that NIS2 will already be implemented. However, the demand for certain roles, such as Cybersecurity Risk Manager and Cybersecurity Auditor, remains high and continues to grow. It is also expected that the demand of larger organizations stabilises over time but that the smaller enterprises need to catch up. Last, AI could significantly assist with specific recurrent cybersecurity activities but will not reduce the demand for these roles.

Both technical and soft **skills** will be very important in the next 2 years. Soft skills, such as communication, stress resistance and learning capacity, are key for cybersecurity roles and are becoming increasingly important.

In the long run (>5 years), key technologies that will have an impact on skills include AI, quantum computing, native cloud, and confidential High-Performance Computing (HPC). In addition, the participants believe that soft skills will become increasingly important, with communication being a key example.

Regarding **training** of cybersecurity professionals, the participants highlight the importance of reskilling, adapted learning methods (project-based learning, knowledge sharing, etc.), communication skills (embedded in every training topic), lifelong learning, partnerships, real environment to attract students and more women in the sector. Soft skills, especially communication skills, will become increasingly important in the long term. Education institutions should integrate more soft skills into their programmes.

7 Conclusions

The objective of this study was to identify the roles and skills needed in the cybersecurity ecosystem in Belgium and to explore the mismatch between employers' demands and the offerings of training and education entities. This analysis also aimed to propose recommendations to address the shortage of cybersecurity jobholders and skills.

Cybersecurity is becoming increasingly crucial for both private and public entities in Belgium. They are confronted with a growing number of cyberattacks and new regulations, such as NIS2. Furthermore, Belgium has an advanced and increasing level of digitalization. One of the key challenges to remain cyber resilient is the shortage of cybersecurity professionals.

No specific reports or data about cybersecurity roles and skills are available for Belgium. The only significant sources are international reports such as ISC2 2023 and ISACA 2023, and the Agoria socio-economic study on the cybersecurity sector in Belgium (2022). This makes this current report highly relevant, as it provides a more accurate view of the cybersecurity roles, skills, and education & training programmes in Belgium. The used framework is based on the twelve ECSF roles developed by ENISA.

Below are the main conclusions of the analysis, which are based on desk research, a questionnaire, and a job vacancy analysis for the skills needed. The training and education programmes (supply side) were also examined through desk research. Additionally, an expert panel contributed to developing a qualitative approach to understanding the skills needed and the training and education landscape. We will conclude with recommendations to address the challenge of the shortage of cybersecurity professionals.

7.1 Cybersecurity roles

The five most important roles in cybersecurity, both for current professionals and job vacancies, are Cybersecurity Implementer, Cyber Incident Responder, CISO, Cybersecurity Architect, and Cyber Legal, Policy & Compliance Officer. These roles represent 91% and 82% of the roles in the questionnaire and job vacancy analysis, respectively. The ranking differs between those currently working in these roles and the job vacancies.

The average difference between people needed and those currently employed for these roles is about 30%. This is quite significant. Demand for all these roles is expected to grow in the future. The number of required positions is projected to increase by 18% over the next two years and by 63% in more than five years. This trend is confirmed by the expert panel.

However, it is important to distinguish large companies and SMEs. We anticipate a two-phase implementation: large companies will need more cybersecurity professionals to comply with NIS2 within the next few years and will stabilize in five years, while smaller companies will catch up in five years. Small companies are more likely to work with Managed Security Service Providers (MSSPs).

Focusing on the 5 most demanded roles, we can highlight the following:

- Cybersecurity Implementer: This is the most demanded role. 58% of people are working in this position according to the questionnaire and 40% in the job vacancy analysis. For this rol we note a vacancy rate of 25%. For the cybersecurity implemeter, we expect to see medium but below average growth in the next 2 years and quite high growth in > 5 years, probably caused by a predicted growing maturity of SMEs.
- Cyber Incident Responder: the second most common role, with 18% of people currently working in this position and a below-average vacancy rate. It ranks slightly lower in job vacancies (10%, 5th position). This role remains highly demanded, with above-average growth expected in the next 2 years and moderate growth or stabilization in more than 5 years.

- CISO (Chief Information Security Officer): This role is third in the questionnaire (10%) and fourth in job vacancies (12%). It has an above-average growth outlook for the next 2 years, likely due to the impact of NIS2 regulations on large companies. The trend is also positive in > 5 years. Nevertheless some experts think this growth might slow down.

- Cybersecurity Architect: Although only 3% of people currently work in this role (4th position), the demand is much higher, with a vacancy rate of 69% and job vacancies representing 15%. Future demand for this role is expected to grow at an average rate, with a slight slowdown in growth over the next 5 years. As goes for the CISO, this role is especially demanded by large companies.

- Cyber Legal, Policy & Compliance Officer: This role is expected to see increased demand over the next 2 years, with only 3% of current cybersecurity professionals working in this area and a vacancy gap of 31%. It accounts for 12% of job vacancies, likely due to the impact of NIS2 regulations. Demand for this role is projected to continue growing beyond 5 years, albeit at a slower pace.

Even though the total number is relatively low, the highest difference between people needed and working in a role is for Cybersecurity educators, Cyber Threat Intelligence Specialists, Cybersecurity Auditors, Cybersecurity architect and Digital Forensics Investigators.

7.2 Skills for cybersecurity professionals

The most quoted category of skills is Cybersecurity, followed by Transversal/Soft skills. IT-related skills and Organizational skills are also often mentioned. This pattern is consistent in both the questionnaire and job vacancy analysis.

The top five cybersecurity skills in the job vacancy analysis are: Incident management, Access controls (Identity management), Information systems and network security, Data security and cryptography, and Threat analysis. The respondents to the questionnaire give a 1st ranking importance to Cloud security and a 6th position for Operational Technology (OT) security (more relevant to the manufacturing sector, reflecting the respondents' profiles).

For transversal/soft skills, Teamwork, Problem solving, and Communication are very important. Willingness to learn and Ethical behaviour rank also high for current professionals, while Communication and Leadership are more important in the job vacancies. Communication skills (including presentation, communication with colleagues, crisis communication) are expected to only gain importance in the future (2 and 5 years).

In the top five most important Organizational skills, we found: Risk management, Policy development, Process control, and Strategic planning. Business continuity is more important in the questionnaire. Project management ranks first in job vacancies, indicating a possible trend towards increased importance for project based ways of working.

Lastly, the top 6 IT related skills are : Network management, Enterprise architecture & infrastructure design, Data, asset and inventory management, Operating systems, Data analysis and System administration and integration (with varying rankings depending on the source).

The innovation trends that should have an impact on skills in the future are: AI, post-quantum, native cloud and confidential HPC. Somes activities should also be more and more embedded within the business (e.g.: HRM, purchase).

7.3 Education and training of cybersecurity professionals

Our conclusion is based on the answers of the questionnaire about training in their organization, on our desk research on training and education programmes in cybersecurity and on the expert panel discussion.

The primary reason for having to **train personnel** in cybersecurity roles is that New (technological) developments ask for new skills (82%). This is not surprising given the fast evolution of threats and technologies in cybersecurity. The second and third reasons are respectively the Lack of right skills of the people starting the job (46%) and New business processed requiring new skills. Additionally, 61% of the respondents state there is no backlog in training personnel for cybersecurity roles. This relatively high percentage aligns with European figures indicating a high proportion of Belgian companies that have organized training to develop their employees' ICT skills. The main reason for any training backlog is that people don't have time for training. Regarding training strategies, 'on-the-job coaching and training' is considered the most important by respondents. It is crucial to develop a comprehensive global upskilling strategy for organizations.

Our analysis of **cybersecurity training and education programmes** in Belgium has revealed a rich landscape of educational opportunities:

- A wide range of EQF classification levels, spread across different regions and offered in several languages enabling a broad spectrum of educational and professional needs to be met.
- A broad range of Masters and Bachelors dedicated to Cybersecurity or with cybersecurity Major, Specialisation or Options in Cybersecurity in the 3 regions, including some high level programmes and a large choice of training options.
- A positive dynamic with new training programmes for students and for unemployed, and an increasing number of registrations.
- The analysis of five major programmes has shown that these courses are structured to cover all of the 12 roles defined in ENISA's ECSF competency framework, illustrating the comprehensiveness of the cybersecurity trainings available.

However, this analysis and the exchange with the expert panel highlight several possible improvements:

- Masters and Bachelors degrees could welcome more students and should attract more women.
- Masters and Bachelors degrees and other training courses best maximise interaction with companies offering work on projects as part of the pathways as this appears to be the best guarantee of soft/transversal skills development.
- Each university or higher education institution could offer a cybersecurity major, specialization, or option. All IT-related Master's and Bachelor's degrees should include courses in cybersecurity, as some currently have few or none.
- New training programmes for the unemployed could be launched (more people interested than places available).
- The reskilling training avenue should be further developed.
- The quality of the programmes should be improved by better adapting them to latest developments in cybersecurity (train the trainer) and the needed roles and skills, working more closely with the field (e.g., project-based learning, internships, workplace learning/alternance), and teaching soft skills more (esp. communication).

7.4 Recommendations

Based on the skills need analysis, four main recommendations have been identified:

1) Promote cybersecurity studies and trainings

- Start working on cybersecurity awareness in primary school at the same moment kids and youngsters start using digital devices
- Include specific cybersecurity courses in all STEM/Digital classes at secondary school
- Organize more awareness raising campaign, inclusive for women and elderly professionals

2) More cybersecurity trainings and courses

- A cybersecurity specialization in all IT related masters and bachelors
- A cybersecurity course in all other programmes (e.g.: management, law, …)
- Scale up of the cybersecurity training programmes for unemployed

3) Improve the quality of cybersecurity training and education programmes

- Better adapt the programmes to the last cybersecurity evolution (e.g.: train the trainer) and to the needed roles and skills
- Organize all trainings by design in a dual way. Encourage educational institutions and companies to work together on real life projects, allowing not only technical knowledge but also soft / transversal skills to be trained
- Include time for knowledge exchange between teachers and company operational experts in this dual way of organizing education
- Set up an Excellence centre for Cybersecurity to improve quality, share expertise and increase the number of high-level trainers

4) Invest more in reskilling and upskilling for the company's staff

- Adopt a cybersecurity training strategy and plan in each organization
- Reskill workers with less relevant roles to cybersecurity related roles based on structured programme with external partners
- Broaden the hiring funnel

8 References

- Agoria. (2022). First socio-economic study on the cybersecurity sector in Belgium https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
- Agoria. (2023). Thales Belgium. Agoria Connect. https://www.agoriaconnect.be/fr/fournisseur/thales-belgium
- Awati, R., & Pratt, M. K. (2023). ICT (information and communications technology or technologies). TechTarget. https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies
- BELSPO. (2021). Belgian Report on Science, Technology and Innovation (BRISTI) 2021 https://meri.belspo.be/site/docs/publications/BRISTI_2021%20FR.pdf
- CCB. (2021). Cybersecurity Strategy Belgium 2.0 2021-2025. Centre For Cybersecurity Belgium https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
- CCB. (2023a). La fraude au CEO : mieux vaut prévenir que payer. https://ccb.belgium.be/fr/document/la-fraude-au-ceo-mieux-vaut-pr%C3%A9venir-que-payer
- CCB. (2023b). Événement de partage des connaissances ECCC. https://ccb.belgium.be/fr/actualit%C3%A9/ev%C3%A9nement-de-partage-des-connaissances-eccc
- CCB. (2023c). Sensibiliser à la cybersécurité sur le lieu de travail : Découvrez cette série de 10. https://ccb.belgium.be/fr/actualit%C3%A9/sensibiliser-%C3%A0-la-cybers%C3%A9curit%C3%A9-sur-le-lieu-de-travail-d%C3%A9couvrez-cette-s%C3%A9rie-de-10
- CCB. (2023d). Annual Report 2023. https://ccb.belgium.be/en/news/annual-report-2023
- CCB. (2024). The NIS2 law, Supervision and Sanctions NIS2: Supervision | Centre for Cybersecurity Belgium
- CCB. (2024b). PUBLICATION OF THE NIS2 LAW IN THE BELGIAN OFFICIAL JOURNAL Publication of the NIS2 law in the Belgian Official Journal | Centre for Cybersecurity Belgium
- CCB. (2024c). ICT SECURITY EDUCATION IN BELGIUM https://ccb.belgium.be/en/ict-security-education-belgium
- Chancellerie du Premier Ministre. (2023). Centre pour la Cybersécurité Belgique. https://chancellerie.be/fr/centre-cybersecurite-belgique
- Choual S., Hamouchi H., Uyar E., Valentin L. (2023). Analysis of the cybersecurity education landscape in Belgium: Alignment between the skills taught by teaching entities and the skills sought by employers.
- CIIS. (2024). Skills Framework. https://www.ciisec.org/frameworks/skills-framework/
- CWF. (2024). Increasing Diversity Within the Cybersecurity Workforce WF. CyberWayFinder. https://www.cyberwayfinder.com/
- Digital Wallonia. (2024). CyberWal by Digital Wallonia. https://www.digitalwallonia.be/cyberwal/#actions
- Doucet, B. (2022). Première radiographie socio-économique du secteur belge de la cybersécurité. Regional-IT. https://www.regional-it.be/2022/11/18/premiere-radiographie-socio-economique-du-secteur-belge-de-la-cybersecurite/
- ECCC. (2024) - European Cybersecurity Competence Centre and Network. Belgium NCC. https://cybersecurity-centre.europa.eu/belgium-ncc_en

- ECHO Network. (2023). Welcome to ECHO. https://echonetwork.eu/welcome-to-echo/
- EIOPA. (2023). Digital Operational Resilience Act (DORA). https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
- ENISA. (2022a). European Cybersecurity Skills Framework (ECSF) - User Manual. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf
- ENISA. (2022b). European Cybersecurity Skills Framework Role Profiles. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles
- ENISA. (2024). CYBERHEAD - Cybersecurity Higher Education Database. ENISA. https://www.enisa.europa.eu/topics/education/cyberhead
- Europass. (2024). Description of the eight EQF levels. https://europass.europa.eu/fr/description-eight-eqf-levels
- European Commission. (2022). Cyber Resilience Act. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
- European Commission. (2023a). EU Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- European Commission. (2023b). European Innovation Scoreboard. https://research-and-innovation.ec.europa.eu/statistics/performance-indicators/european-innovation-scoreboard_en
- European Commission. (2024a). European e-Competence Framework (e-CF). https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf
- European Commission. (2024b). Cyberskills. https://europa.eu/eurobarometer/surveys/detail/3176
- European Parliament. (2023). The NIS2 Directive: A high common level of cybersecurity in the EU https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
- Eurostat. (2023a). Digital skills training in enterprises. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade?
- Eurostat. (2023b). ICT specialists in the workforce. https://ec.europa.eu/eurostat

- Eurostat. (2023b). ICT specialists in the workforce. https://ec.europa.eu/eurostat

- Evoliris. (2017). État des lieux sur la Cybersécurité à Bruxelles. https://digitalcity.brussels//sites/default/files/2020-07/Cyberse%cc%81curite%cc%81%20-%20rapport%20de%20veille%202017FR.pdf
- Febelfin. (2024). Gagner de l'argent rapidement avec Sami Farhat : c'est une illusion. https://febelfin.be/fr/presse/fraude-et-securite/gagner-de-l-argent-rapidement-avec-sami-farhat-c-est-une-illusion
- FPS Economy. (2023a). Belgian Digital Economy Overview, Edition 2023. https://economie.fgov.be/fr/publications/belgian-digital-economy
- FPS Economy. (2023b). Digital Decade 2030 Report: Annex Belgium. https://economie.fgov.be/fr/file/7467299/download?token=5laXYJx1
- FPS Economy. (2023c). Digital Decade 2030. Service Public Fédéral Économie. https://economie.fgov.be/fr/themes/line/les-tic-en-belgique/barometre-de-la-societe-de/digital-decade-2030

- FPS Economy. (2023d). La cybersécurité au sein des PME belges https://economie.fgov.be/fr/themes/entreprises/pme-et-independants-en/digitalisation-des-pme/la-cybersecurite-au-sein-de
- GuardSquare. (2024). Mobile Application Security Solutions. https://www.guardsquare.com
- HELMo. (2024). Bachelier Informatique sécurité systèmes cybersécurité HELMo Liège. https://www.helmo.be/fr/formations/secsy182-informatique-orientation-securite-des-systemes-cybersecurite
- Howest. (2024). Bachelor in Cybersecurity. https://www.howest.be/nl/opleidingen/bachelor/cybersecurity
- hub.brussels. (2024). Digital transformation: advice for businesses. https://hub.brussels/en/services/digital-transformation-advice-businesses/
- ISACA. (2023). State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources, and Cyberoperations. https://www.isaca.org/resources/reports/state-of-cybersecurity-2023
- ISACA. (2023). Cybersecurity and Burnout: The Cybersecurity Professional's Silent Enemy. Cybersecurity and Burnout: The Cybersecurity Professional's Silent Enemy (isaca.org)
- ISC2. (2023). How the Economy, Skills Gap, and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. https://mysecuritymarketplace.com/reports/how-the-economy-skills-gap-and-artificial-intelligence-are-challenging-the-global-cybersecurity-workforce-2023/
- ISC2. (2024). IT Security Certification | SSCP - Systems Security Certified Practitioner | ISC2. https://www.isc2.org/certifications/sscp
- ISO. (2013). ISO/CEI 27001 :2013, Technologies de l'information—Techniques de sécurité—Systèmes de management de la sécurité de l'information—Exigences. https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27001:ed-2:v1:fr
- KU Leuven. (2024). Master of Cybersecurity. https://www.kuleuven.be/programmes/master-cybersecurity
- Mordor Intelligence (2023). Belgium Cybersecurity Market. https://www.mordorintelligence.com/industry-reports/belgium-cybersecurity-market
- Nemeroff, B. (2024). Soft skills 101: definition + 50 examples. Handshake. https://joinhandshake.com/blog/students/soft-skills-examples/
- Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST special publication, 800(2017), 181. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
- OECD. (2023). Education at a Glance 2023: OECD Indicators. https://www.oecd.org/education/education-at-a-glance/
- Petersen, R., Santos, D., Smith, M., & Witte, G. (2020). Workforce framework for cybersecurity (NICE framework) (No. NIST Special Publication (SP) 800-181 Rev. 1 (Withdrawn)). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
- Schellman. (2024). An Update on EU Cybersecurity: NIS2, EU Cybersecurity Schemes, and the Cyber Resilience Act https://www.schellman.com/blog/cybersecurity/update-on-eu-cybersecurity-november-2023

- Schmitt, S. (2022, April 29). Naval Group opens new counter-mine warfare, cyber labs in Brussels. Defense News. https://www.defensenews.com/global/europe/2022/04/29/naval-group-opens-new-counter-mine-warfare-cyber-labs-in-brussels/?
- Service Public Fédéral Économie. (2021). Digital Belgium : L'agenda numérique pour la Belgique. https://economie.fgov.be/fr/themes/line/strategie-pour-un-marche/digital-belgium-lagenda
- SFIA. (2024). SFIA as an informative resource for the NIST Cybersecurity framework. https://sfia-online.org/en/tools-and-resources/sfia-views/sfia-view-information-cyber-security/sfia-as-an-informative-resource-for-the-nist-cybersecurity-framework
- Solvay Lifelong Learning. (2024). Executive Master in Cybersecurity Management | https://exed.solvay.edu/en/executive-education/digital-transformation-and-governance/executive-master-in-cybersecurity-management
- Statbel. (2023a). Pyramide des âges. https://statbel.fgov.be/fr/figures/pyramide-des-ages
- Statista (2023a). Cybersecurity Market in Belgium: Revenue. https://www.statista.com/outlook/tmo/cybersecurity/belgium#revenue
- Statista (2023b). Cybersecurity Report. https://www.statista.com/study/124902/cybersecurity-report/
- Sweepatic. (2024). External Attack Surface Management Platform. https://www.sweepatic.com/easm-platform
- ULB. (2023). Master en sécurité des systèmes informatiques. https://www.ulb.be/fr/programmeme/2023-ma-secu
- ULB. (2024). Master in CyberSecurity. https://masterincybersecurity.ulb.ac.be/
- UNESCO. (2023). Digital skills critical for jobs and social inclusion. https://www.unesco.org/en/articles/digital-skills-critical-jobs-and-social-inclusion
- Vlaio. (2024). Een op drie Vlaamse bedrijven gebruikt artificiële intelligentie. https://www.vlaio.be/nl/nieuws/een-op-drie-vlaamse-bedrijven-gebruikt-artificiele-intelligentie#:~: .
- VUB. (2023). Computational Design and Software Languages Lab. https://cdsl.research.vub.be/
- Women4cyber. (2024). Women4cyber – European Cybersecurity Organization. https://women4cyber.eu/
- World Economic Forum. (2024). Global Cybersecurity Outlook 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
- European Commission. (2024c). *Eurobarometer Survey 3176* https://europa.eu/eurobarometer/surveys/detail/3176

9 Annexes

9.1 Annex 1: ENISA – European Cybersecurity Skills Framework Roles Profiles

The ECSF role profiles document lists the 12 typical cybersecurity professional role profiles along with their identified titles, missions, tasks, skills, knowledge, competences. The main purpose of this framework is to create a common understanding between individuals, employers and providers of learning programmes across EU Member States, making it a valuable tool to bridge the gap between the cybersecurity professional workplace and learning environments. The full report can be downloaded here.

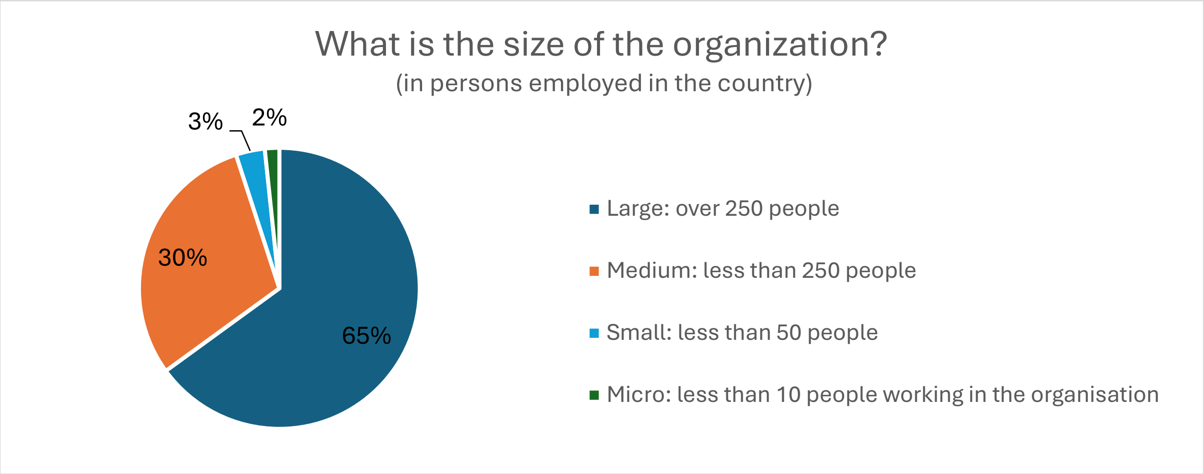
ECSF Role Profile	Description
Cybersecurity Implementer	The cybersecurity implementer/expert **develops, implements, maintains, monitors, upgrades and tests cybersecurity solutions** (systems, assets, software, controls and services) on infrastructures and products and provides cybersecurity-related support to users and customers. *Alternative names: Cybersecurity Developer, Cybersecurity Engineer, Information Security Implementer, Cybersecurity Solutions Expert, Development, Security & Operations (DevSecOps) Engineer*
Chief Information Security Officer (CISO)	The (chief) information security officer/ manager **manages** an organization's cybersecurity strategy and its implementation to ensure that digital systems, services and assets are adequately secure and protected. *Alternative names: Cybersecurity Programmeme Director, Information Security Officer (ISO), Head of Information Security*
Cyber Incident Responder	The incident responder **analyses, evaluates and mitigates** the impact of cybersecurity incidents and **handles incidents** during cyber-attacks, assuring the continued operations of ICT systems. *Alternative names: Cyber Incident Handler, Cyber Crisis Expert, Incident Response Engineer, Security Operations Center (SOC) Analyst, Cyber Fighter /Defender, Security Operation Analyst (SOC Analyst), Cybersecurity SIEM Manager*
Cyber Legal, Policy and Compliance Officer	The cyber compliance officer **oversees and assures compliance** with cybersecurity- and data-related standards, legal and regulatory frameworks and policies in line with the organization's strategy and legal requirements. *Alternative names: Data Protection Officer (DPO), Data Compliance Officer, Privacy Protection Officer, Cyber Legal Advisor, Information Governance Officer, Cybersecurity Legal Officer, IT/ICT Compliance Manager, Governance Risk Compliance (GRC) Consultant, Cyber Law Consultant.*

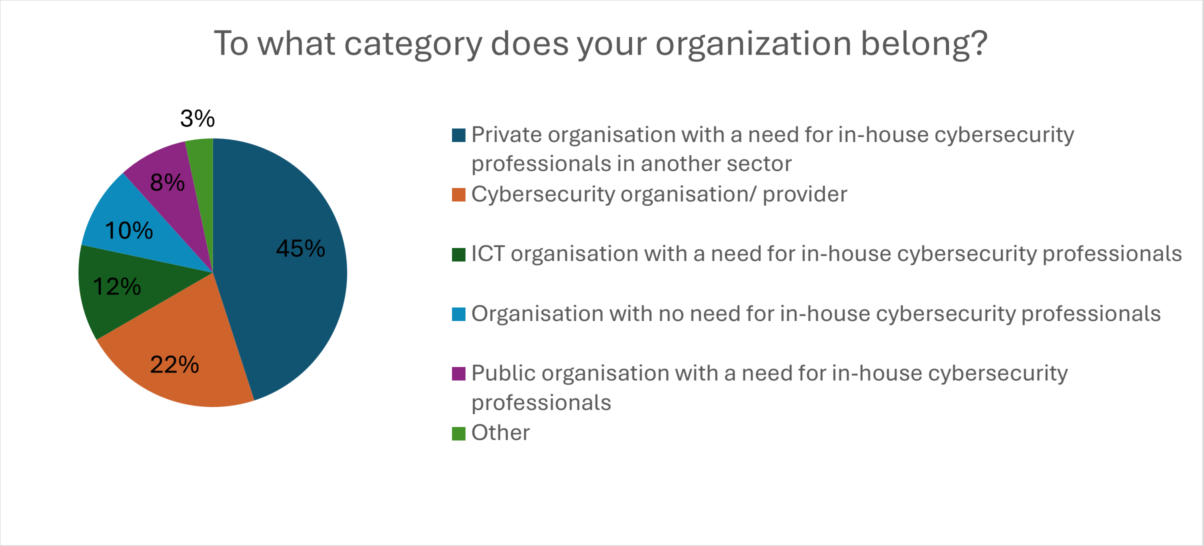
Cybersecurity Architect	The cybersecurity architect **plans and designs solutions** based on security-by-design and privacy-by-design principles. Creates and continuously improves architectural models and cybersecurity controls and coordinates secure development. *Alternative names: Cybersecurity Solutions Architect, Cybersecurity Designer, Data Security Architect.*
Cyber Threat Intelligence Specialist	The cyber threat intelligence specialist **collects, processes and analyses cyber threat data** and information and produces actionable intelligence reports and disseminates them to stakeholders. *Alternative names: Cyber Intelligence Analyst, Cyber Threat Modeller*
Cybersecurity Auditor	The cybersecurity auditor **performs cybersecurity audits** - evaluates, tests and verifies cybersecurity-related ICT products and services, functions and policies ensuring compliance with guidelines, standards and regulations. *Alternative names: Information Security Auditor (IT or Legal Auditor), Governance Risk Compliance (GRC) Auditor, Cybersecurity Audit Manager, Cybersecurity Procedures and Processes Auditor, Information Security Risk and Compliance Auditor, Data Protection Assessment Analyst.*
Cybersecurity Educator	The cybersecurity educator **designs, develops and conducts awareness, training and educational programmes** in cybersecurity and data protection-related topics. *Alternative names: Cybersecurity Awareness Specialist, Cybersecurity Trainer, Faculty in Cybersecurity (Professor, Lecturer).*
Cybersecurity Researcher	The cybersecurity researcher **conducts fundamental/basic and applied research** and facilitates innovation in the cybersecurity domain. *Alternative names: Cybersecurity Research Engineer, Chief Research Officer (CRO) in cybersecurity, Senior Research Officer in cybersecurity, Research and Development (R&D) Officer in cybersecurity, Scientific Staff in cybersecurity, Research and Innovation Officer /Expert in cybersecurity, Research Fellow in cybersecurity*
Digital Forensics Investigator	The digital forensics investigator provides **analysis, reconstruction and interpretation of digital evidence** in a cybercriminal investigation. *Alternative names: Digital Forensics Analyst, Cybersecurity & Forensic Specialist, Computer Forensics Consultant*

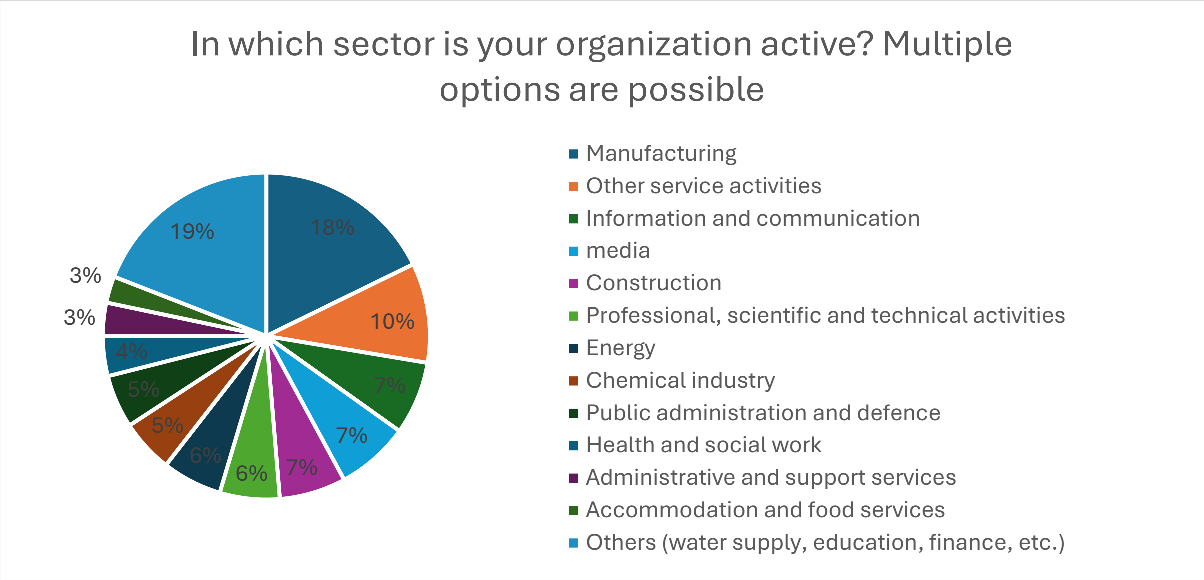
Penetration Tester	The penetration tester **assesses the effectiveness of security controls**, reveals and utilise cybersecurity vulnerabilities, assessing their criticality if exploited by threat actors. *Alternative names: Pentester, Ethical Hacker, Vulnerability Analyst, Cybersecurity Tester, Offensive Cybersecurity Expert, Defensive Cybersecurity Expert, Red Team Expert, Red Teamer*
Cybersecurity Risk Manager	The cybersecurity Risk Manager manages the **organization's cybersecurity-related risks aligned to the organization's strategy**. Develop, maintain and communicate the risk management processes and reports. *Alternative names: Information Security Risk Analyst, Cybersecurity Risk Assurance Consultant, Cybersecurity Risk Assessor, Cybersecurity Impact Analyst, Cyber Risk Manager*

European Union Agency for Cybersecurity (ENISA)(2022). European Cybersecurity Skills Framework (ECSF). Available at: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles<Annexes could be results you want to show or other additional information>

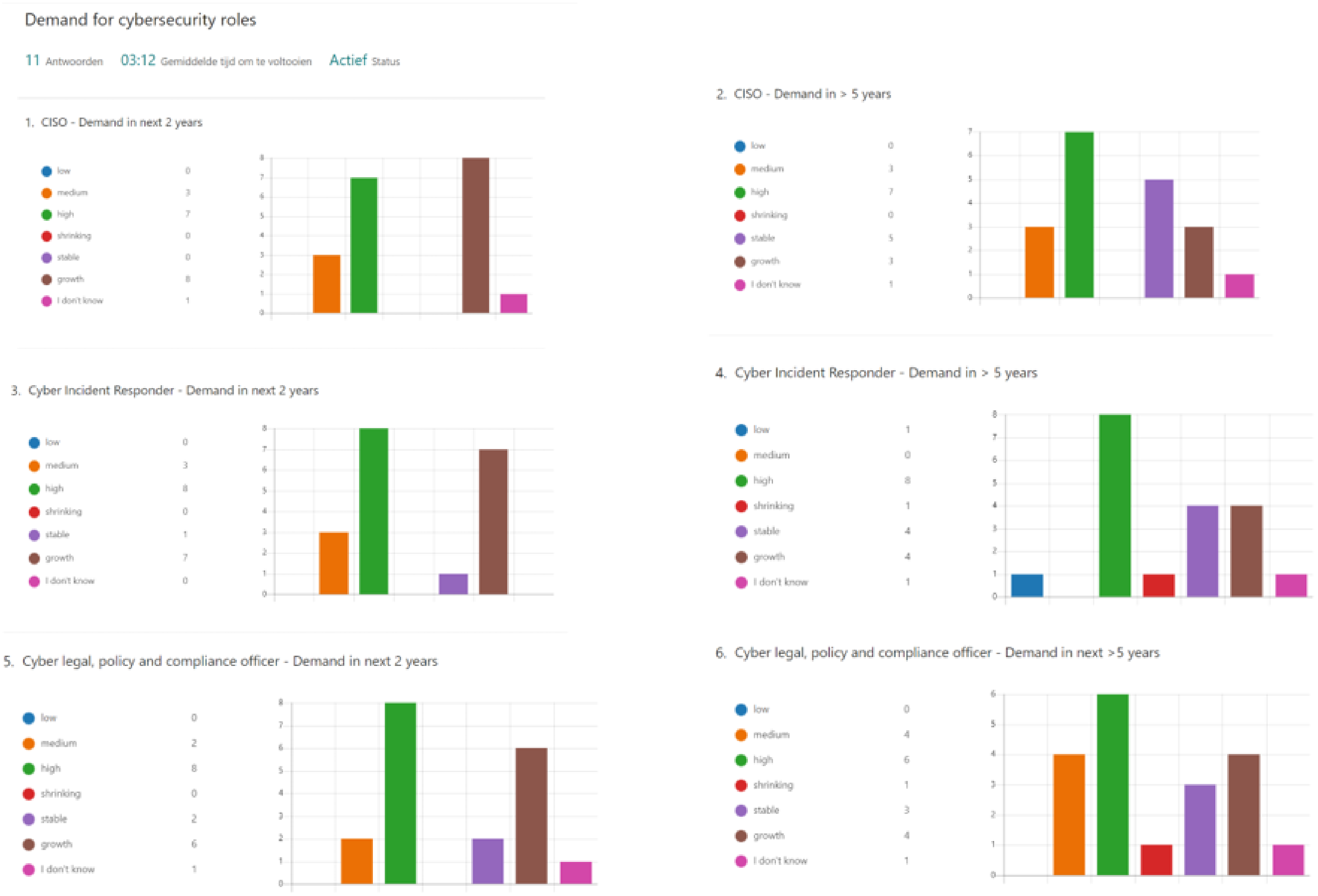
9.2 Annex 2: Questionnaire


What is the size of the organization?
(in persons employed in the country)


To what category does your organization belong?


In which sector is your organization active? Multiple options are possible

9.3 Annex 3: Expert panel – Demand for 12 ECSF/ENISA roles



Demand for cybersecurity roles

11 Antwoorden 03:12 Gemiddelde tijd om te voltooien Actief Status

1. CISO - Demand in next 2 years

● low	0
● medium	3
● high	7
● shrinking	0
● stable	0
● growth	8
● I don't know	1

2. CISO - Demand in > 5 years

● low	0
● medium	3
● high	7
● shrinking	0
● stable	5
● growth	3
● I don't know	1

3. Cyber Incident Responder - Demand in next 2 years

● low	0
● medium	3
● high	8
● shrinking	0
● stable	1
● growth	7
● I don't know	0

4. Cyber Incident Responder - Demand in > 5 years

● low	1
● medium	0
● high	8
● shrinking	1
● stable	4
● growth	4
● I don't know	1

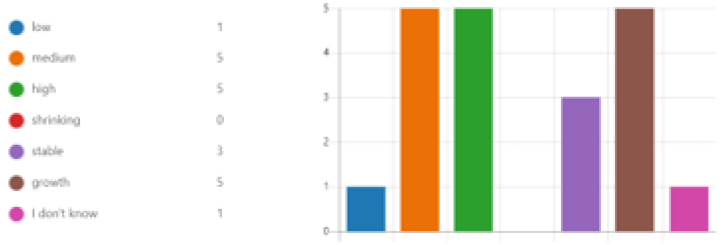
5. Cyber legal, policy and compliance officer - Demand in next 2 years

● low	0
● medium	2
● high	8
● shrinking	0
● stable	2
● growth	6
● I don't know	1

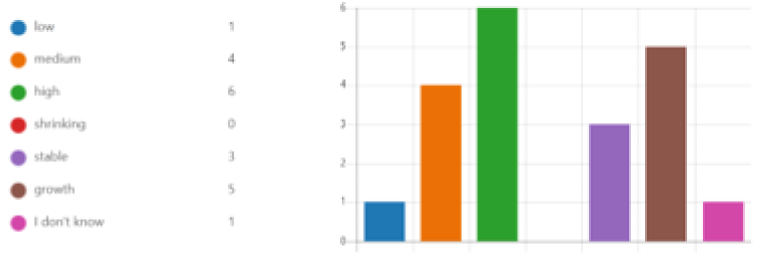
6. Cyber legal, policy and compliance officer - Demand in next >5 years

● low	0
● medium	4
● high	6
● shrinking	1
● stable	3
● growth	4
● I don't know	1

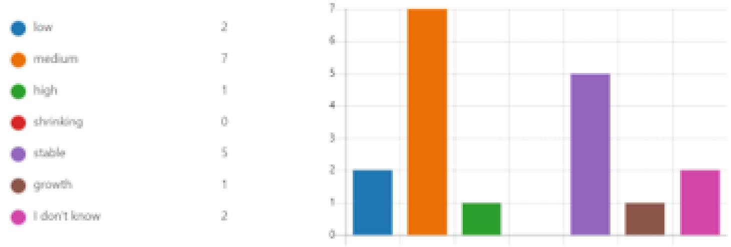
7. Cyber Threat Intelligence specialist - Demand in next 2 years



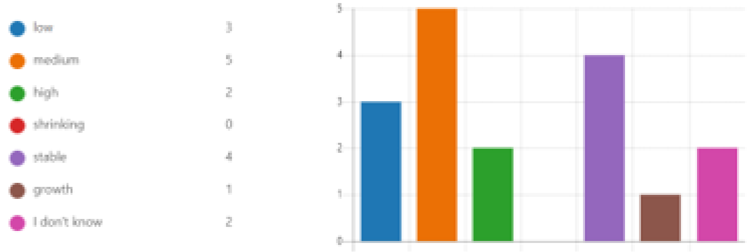
8. Cyber Threat Intelligence specialist - Demand in > 5 years



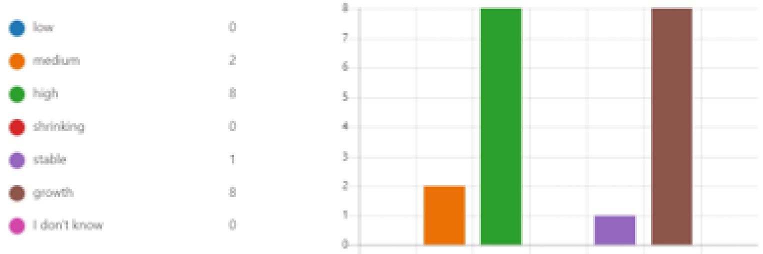
9. Cybersecurity Researcher - Demand in next 2 years



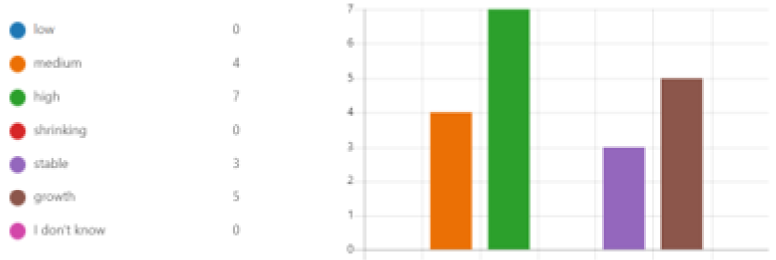
10. Cybersecurity Researcher - Demand in > 5 years



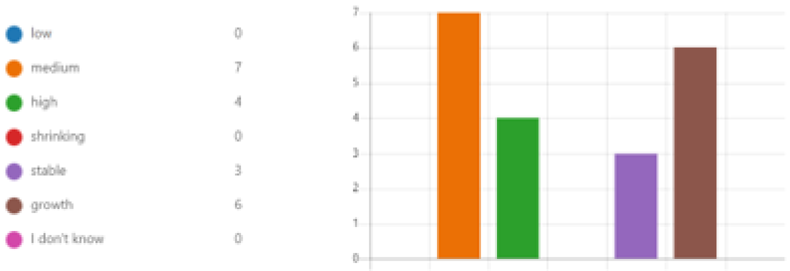
11. Cybersecurity Risk manager - Demand in next 2 years



12. Cybersecurity Risk manager - Demand in >5 years

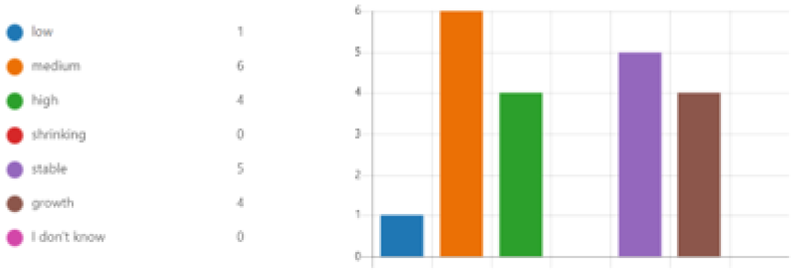


13. Cybersecurity Architect - Demand in next 2 years



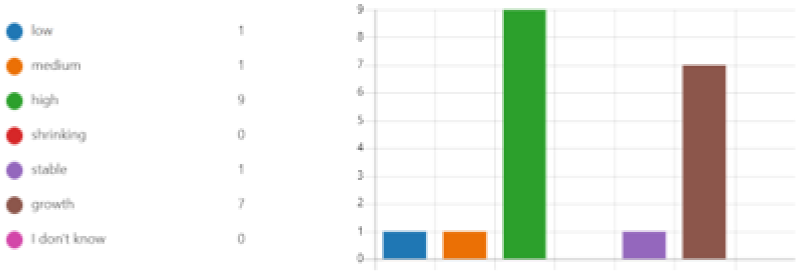
●	low	0
●	medium	7
●	high	4
●	shrinking	0
●	stable	3
●	growth	6
●	I don't know	0

14. Cybersecurity Architect - Demand in >5 years



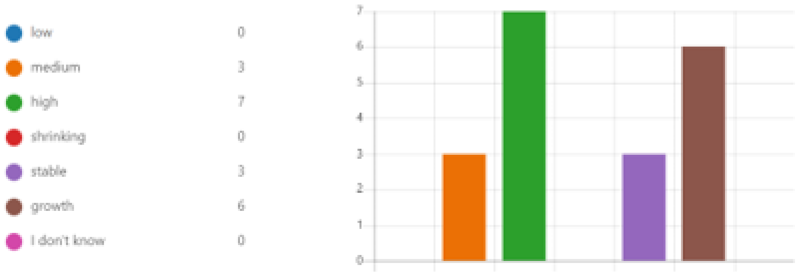
●	low	1
●	medium	6
●	high	4
●	shrinking	0
●	stable	5
●	growth	4
●	I don't know	0

15. Cybersecurity auditor - Demand in next 2 years



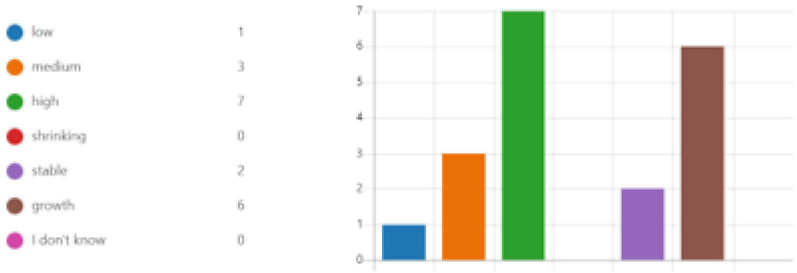
●	low	1
●	medium	1
●	high	9
●	shrinking	0
●	stable	1
●	growth	7
●	I don't know	0

16. Cybersecurity auditor - Demand in >5 years



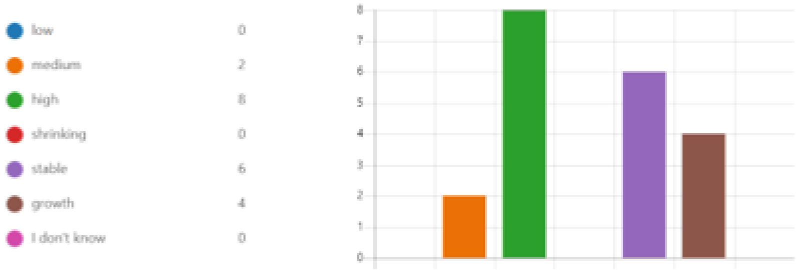
●	low	0
●	medium	3
●	high	7
●	shrinking	0
●	stable	3
●	growth	6
●	I don't know	0

17. CYbersecurity educator - Demand in next 2 years



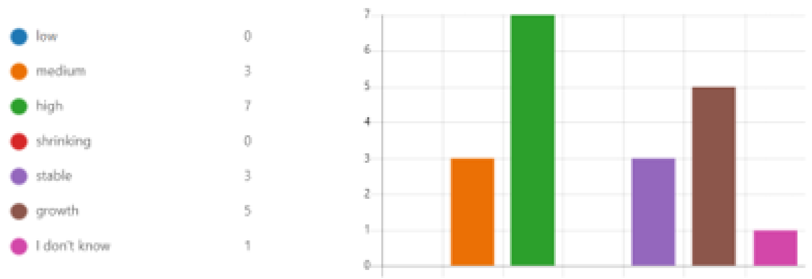
●	low	1
●	medium	3
●	high	7
●	shrinking	0
●	stable	2
●	growth	6
●	I don't know	0

18. Cybersecurity educator - Demand in >5 years



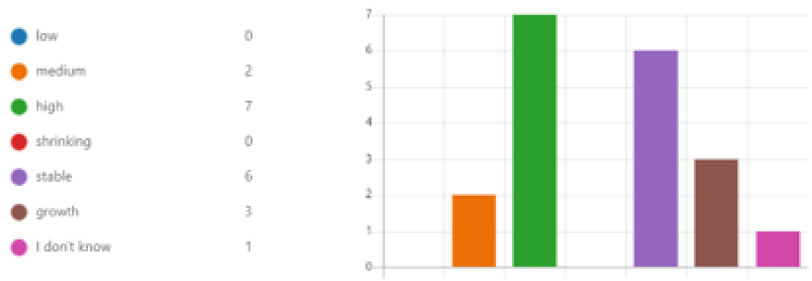
●	low	0
●	medium	2
●	high	8
●	shrinking	0
●	stable	6
●	growth	4
●	I don't know	0

19. Cybersecurity implementer - Demand in next 2 years



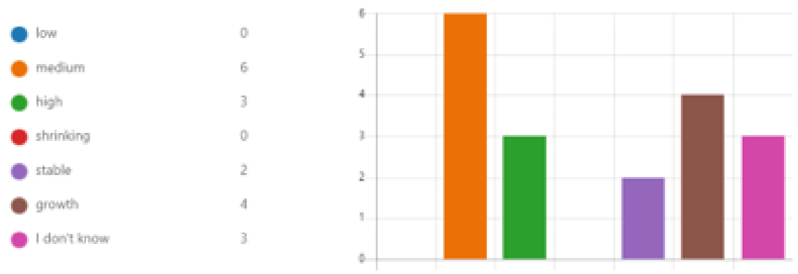
● low	0
● medium	3
● high	7
● shrinking	0
● stable	3
● growth	5
● I don't know	1

20. Cybersecurity implementer - Demand in >5 years



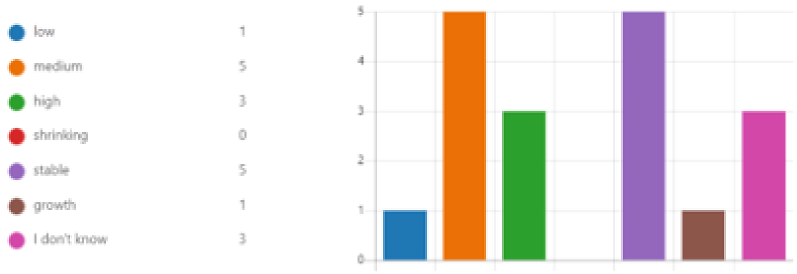
● low	0
● medium	2
● high	7
● shrinking	0
● stable	6
● growth	3
● I don't know	1

21. Digital Forensics Investigator - Demand in next 2 years



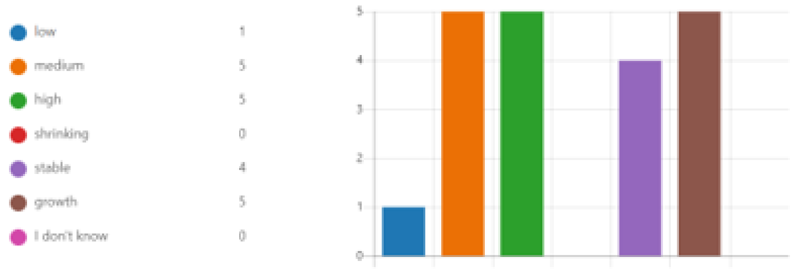
● low	0
● medium	6
● high	3
● shrinking	0
● stable	2
● growth	4
● I don't know	3

22. Digital Forensics Investigator - Demand in >5 years



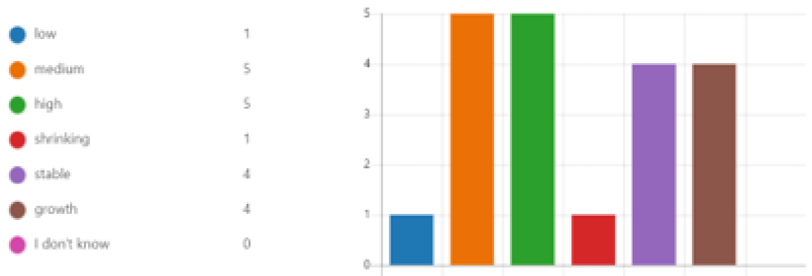
● low	1
● medium	5
● high	3
● shrinking	0
● stable	5
● growth	1
● I don't know	3

23. Penetration tester - Demand in next 2 years



● low	1
● medium	5
● high	5
● shrinking	0
● stable	4
● growth	5
● I don't know	0

24. Penetration tester - Demand in >5 years



● low	1
● medium	5
● high	5
● shrinking	1
● stable	4
● growth	4
● I don't know	0

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by
the European Union