Research report An analysis of Cyber Security Education and the associated Job Market

Platform **Talent** voor **Technologie**

dialogic

Commissioned by

Ministerie van Economische Zaken en Klimaat

Executive summary

The Netherlands and the EU are working hard to create a society that is digitally secure. The availability of well-trained cyber security professionals is an essential condition for this. The current job market, new technological developments, as well as the intensification of cyber crime, are all factors that call for the ever-increasing need for various types of cyber security specialists[1].
The Ministry of Economic Affairs and Climate would like to have a good picture of the **current quantitative and qualitative shortages on the Dutch cyber security job market, and the expected growth and options available for improving the alignment of education with the job market** (also included as an action in the Dutch Cyber Security Strategy Action Plan 2022-2028[2]).

Platform Talent for Technology (PTvT) and Dialogic were asked to provide answers to nine research questions, which they did between September 2023 and February 2024. The questions were aimed at identifying supply and demand (job market and training opportunities). This was required to provide **evidence-based advice, including an implementation plan, on which (policy) instruments could be used in the short and long term** to reinforce the cyber security job market.

This research identified the job market and training opportunities using various data collection methods. Analysing data from various national sources resulted in the supply and demand being quantitatively represented. The data was verified and supplemented by conducting questionnaires, interviews and workshops with people from the education sector and the job market. Parties involved in Human Capital activities also contributed to the data collection and interpretation of the results.

Education

The requirements students must achieve to obtain an MBO diploma are laid down nationally in the relevant Qualification Dossier. The Minister for Education, Culture and Science is responsible for the contents of the Qualification Dossiers. It can be seen that attention has been paid in recent years to cyber security in **MBO-level training in the three ICT domain Qualification Dossiers** currently in use: ICT Support (Level 2), Software Development (Level 4) and ICT Systems & Devices (All-Round Employee Level 3 and IT Systems & Devices Expert Level 4). The **renewal of these Qualification Dossiers**, which will take effect on 1 August 2024, **has been expanded** to include what students must know and be able to do in terms of cyber security. In addition, **three MBO initiatives** were discovered that are currently in **the development phase, accreditation phase, or start-up phase** .
The focus of the MBO courses content is mainly based on **technical aspects, as well as some management and organisational aspects**. Due to the variation in how ICT courses shape education, it has not been possible to determine the exact size of the cyber security part of the course. In any case, inquiries with training managers show that **cyber security is a standard part of the ICT training at a number of MBO education institutions**, while others make more use of the possibilities offered by the **elective modules**. The total number of students in these particular courses remains approximately the same at around 23,000 students per year. Over the past few years, an average of 6,000 ICT students graduated each year.
The training directors highlight the bottlenecks and/or challenges as: [1] updating lecturers, [2] shortage of students, [3] inadequate facilities, and [4] rapid emergence of new AI themes, for example.
With the exception of ICT courses, there is little or no attention paid to cyber security in any other MBO courses. The first steps are being taken in the form of pilots within the Safety Officer training course for example.
At **Higher Education level (HBO and University)**, there are, within the Accreditation Organisation of the Netherlands and Flanders (NVAO)-accredited programmes, **10 study programmes identified that are entirely focused on cyber security (5 HBO, 5 University), 29 study programmes that offer a specialisation/elective cyber security element (18 HBO, 11 University) and 13 study programmes (6 HBO, 7 University) that have a compulsory cyber security component in their programme** (> 6 ECTS). Further, **9 Higher Education study programmes** (8 HBO, 1 University) were found that are still **in the development phase, accreditation phase, or start-up phase** .
The annual inflow of students with a relevant cyber security component in their study programme has remained fairly stable **at around 3,000 students over the last three years**. However, the **outflow of students** is **clearly increasing gradually** on an annual basis, particularly in study programmes that are entirely focused on cyber security, or for students who have chosen a cyber security specialisation/elective as part of their study programmes. HBO and University education providers **appear to have a more multi-disciplinary approach across the courses**.

1. https://www.cybersecurityraad.nl/documenten/brieven/2023/12/22/informerende-brief-van-de-cyber-security-raad-over-onderwijsversterking-en-kennisontwikkeling
2. https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

It appears little or no attention is paid to competence development in any study programmes (MBO and Higher Education) in which students can develop didactic knowledge and skills.
Various **bottlenecks** emerged during the interviews and questionnaires with teachers, professors and management, such as: [1] shortage of teachers with sufficient knowledge, [2] the content of the curriculum in which both a broad profile and specialist profiling within the cyber domain must be offered, [3] the speed at which the security world is developing in combination with the lack of ability to respond flexibly to this, [4] the image surrounding cyber security education as a technical study programme, which influences recruitment and expectation management of (potential) students and [5] the lack of resources for e.g. educational materials, hybrid learning workplaces, etc.)

We see an apparently extensive non-funded educational offer[3] (offer not subsidised by the Ministry of Education, Culture and Science and the Ministry of Economic Affairs and Climate) within **Life-Long Learning**. The training costs are borne by the person taking the training, the employer, or the benefits agency for any training at a private institute, correspondence courses or company training), of which **approximately 20% is aimed at the most requested cyber security certificates** on the job market. In addition to many providers, we see one provider with a large portfolio offers. Education is available in several forms, with hybrid forms becoming increasingly common. There are also many (often regional) activities and offers for SME entrepreneurs and citizens. Reach and impact are still difficult to estimate.
Private trainers state that people experience a **number of obstacles when it comes to cyber security retraining, additional training and further training (insufficient time from their employer, no access to training subsidies).**

Job Market

The job market demand was identified by analysing the current vacancies. This cannot cover the entire demand; it is expected that many positions are filled without a vacancy announcement.
The vacancy analysis shows **growing demand** for cyber security expertise on the job market: from approximately 8,000 in 2018 to approximately 19,000 in 2022 for both specialist cyber security profiles and a broader selection of job profiles in which cyber security forms a part. This demand **varies per province**, with a known weak-point on the **demand for intermediate and senior positions requiring HBO or University education level**. The greatest demand for cyber security expertise comes from the **government and the IT sector**, with most cyber vacancies at organisations including the Police, PWC, CGI, EY, the Tax Authorities, ING, ABN AMRO, Capgemini, KPMG and the Ministry of Defence. Organisations that have a relatively greater demand for cyber security also have a greater demand for specialist profiles.

The population of cyber security professionals can be characterised as a relatively young population with two-thirds being male and one-third female. **Immigration and labour migrants** seem to be important to the sector: approximately 5-10% of the inflow comes from foreign employees who come to work in the Netherlands. 2021 saw an **outflow** of almost 25% of the population, of which ~2% of the outflow retired and another ~2% emigrated. Approximately three quarters of those leaving the surveyed companies went to work for an organisation that falls outside the scope of this research. This does not necessarily mean they will take up another profession; they may take up the same profession or a similar profession with another employer. About 2.5% of the population switched to another company within the research population.

Across the board, a relatively **great deal of technical knowledge** is required to work in cyber security, while the required **skills and tasks to be performed** are, on the other hand, largely **non-technical** in nature. In vacancies that refer to the European Cyber Security Skills Framework (ECSF) profiles in their texts, the technical component weighs more heavily than in other types of cyber security profiles. The demand for cyber security expertise and the underlying building blocks is **growing strongly in absolute terms**, but in relative terms the **ratio between different knowledge and skill types is stable**.
15% of vacancies explicitly request a cyber security certificate. The most requested certificates are CISSP, CISM, and CISA[4]. **A certificate is often required for specialist cyber security profiles**; for example, for Chief Information Security Officer (CISO) profiles we find the demand for a certificate in 77% of the vacancies, while this is the case in 58% of the vacancies for Penetration Testers (who test computer systems and apps for security vulnerabilities).

3. unfunded education is not subsidised by the Ministry of Education, Culture and Science or the Ministry of Economic Affairs and Climate. The costs of the training are borne by the person taking the training, the employer or the benefits agency. https://www.ocwincijfers.nl/sectoren/onderwijs-algemeen/niet-bekostigd-onderwijs/deelnemers-niet-bekostigd-onderwijs
4. Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA)

Future developments

The arrival of the NIS2 directive (Network and Information Security), the Cyber Resilience Act (CRA) and the further development of AI will play a major role in the cyber security job market. The expectation is that the **NIS2 directive will increase the demand for cyber security professionals across the board**, from the ECSF profiles Chief Information Security Officers (CISO) up to Implementers, Analysts, Auditors and Pen-testers . The **CRA is expected to increase demand for cyber security professionals across the board**, with the greatest impact for the cyber integrators. As AI continues to develop and deploy, the demand for people to perform certain tasks will decrease, but new tasks will emerge at the same time and new competencies will be required. The ECSF profiles for **Penetration Tester, Cyber Threat Intelligence Specialist and Digital Forensics Investigator** offer the **greatest chance for AI to play a significant role**. Organisations marginally involved in cyber security, in which cyber security plays a relatively small role and that do not fall under the NIS2 directive and/or the CRA, will probably continue to opt for **"hybrid" functions in combination with external hiring/purchasing/organisation of cyber security expertise**.

Connection between education and the job market

The idea that education and (all) specific vacancies on the job market could match perfectly is a misconception because learning has to take place over several years and in different contexts (work environment, training, etc.). This research therefore examined the job market demand for junior positions and the subsequent connection with the training courses. In Higher Education we see **relatively too few HBO and University graduates with a specialist cyber security profile** to meet the needs of the job market. The number of Higher Education graduates with a **"substantial" cyber security component in their training is actually at the same level**. Just like the quantitative demand for **MBO cyber security junior staff: this is in line with the outflow** in the two relevant MBO-4 courses.
In terms of content, there is plenty of demand for the **"Technical" and "Management & Organisation"** competencies on the job market. We also see these building blocks in courses with a specialisation in cyber security. The **focus on "legal"** competencies is particularly evident in courses in which cyber security is **not a specialisation**. However, we do not see the **competencies reflected anywhere in "education" (e.g. teaching)** – neither in the training courses nor in vacancies at junior level.

A major challenge for the cyber security job market therefore appears to be Life-Long Learning in terms of both **attracting and retaining** (current) cyber security professionals. Account must be taken here of the difference between the position someone comes from and the position someone enters into. This difference should not be too great; there must be a "bridgeable gap". It is important to look carefully at **which backgrounds provide sufficient basis to bridge the gap**. The importance of cyber security certificates in the job market is great, especially for the more specialised cyber security profiles. These **certificates and their associated training courses are a way to bridge the gap**.
In addition, it is important to address **the aforementioned bottlenecks in education**; which will improve the quantitative and qualitative intake of regular courses, thus better meeting the demands of the job market.

Advice

The results of this research report deliver a foundation upon which advice, including an implementation proposal, will be drawn up. Several meetings held with education, the business community and collaborating partners in early 2024 determined the (policy) instruments that could be used in the short and long term to reinforce the cyber security job market. These recommendations have been bundled in a report delivered in mid-February 2024.

Table of contents

Reading guide

This report provides an overview of the approach and results of research conducted into education and the job market in terms of cyber security.
Chapter 1 describes *the background and approach to the research* and discusses the research questions posed by the Ministry of Economic Affairs and Climate. **Chapter 2** explains the *methodology of the research*, with regard to both education and the job market. Following that, **Chapter 3** explains the *results* of the research questions relating to education, while **Chapter 4** presents the *results* of the *job market analysis*. The *final conclusions* drawn from the research can read in **Chapter 5**. Finally, **Chapter 6** looks towards the future: what framework and approach should be taken from these results?

1. Background

1.1 Background

Hard work is being done to create a digitally secure society in the Netherlands and the EU. The presence of a sufficient number of well-trained cyber security professionals with expertise is an essential condition for this. The Ministry of Economic Affairs and Climate would like to have a good picture of the current quantitative and qualitative shortages on the Dutch cyber security job market and the expected growth. The Dutch Cyber Security Strategy Action Plan 2022-2028[5] includes the following actions in terms of Human Capital:

- The qualitative and quantitative shortages in the cyber security job market have been examined and recommendations made about how to address these shortages;
- Research was carried out to assess whether the initiatives for insight into ICT-wide shortages and the development of an ICT education and job market dashboard could provide sufficient insight into regional shortages of cyber security specialists.

In order to implement the above actions, the Ministry of Economic Affairs and Climate has written an extensive research proposal. The research questions focus on supply and demand (training opportunities and job market) and should lead to evidence-based advice, including an implementation plan, on the (policy) instruments that can be used in the short and long term to reduce the identified shortage on the cyber security job market. In previous years, education and the cyber security job market have been identified in several ways. This multi-disciplinary research has been supplemented and existing insights expanded by:

- focusing the research specifically on cyber security
- expanding the problem definition: what shortages are we talking about exactly?
- paying attention to specific knowledge, skills and tasks within cyber security
- paying attention to different target groups/types of organisations
- working on the development of a methodology which can also be used in the future.

This chapter discusses the following topics:

- The research questions posed by the Ministry of Economic Affairs and Climate;
- The approach as it has been divided into a research report and an advisory report;
- The approach to the provision of evidence-based advice.

1.2 Research questions

The research request from the Ministry of Economic Affairs and Climate contains nine research questions:

Offer

1. Identify the relevant Dutch education (MBO-4 up to University level) and up-skilling initiatives (e.g. mathematics, AI, data science, ICT). Build on existing initiatives such as the National Cyber Security Research Agenda (NCSRA) and the Platform Talent for Technology (PTvT);
2. Provide insight (substantiated with figures where possible) into the current inflow and outflow of training and retraining opportunities;
3. Use the results from (1) and (2) to provide insight (substantiated with figures where possible) into what type of cyber security expertise is offered and in what quantity;
4. Provide insight into the bottlenecks affecting cyber security training and retraining. Consider any factors that influence inflow and outflow.

Question

5. Provide insight (substantiated with figures where possible) into the demand for cyber security experts and the required expertise. Do this based on:
    - An overview of the vacancies registered by Dutch organisations that employ (or will employ) cyber security professionals;
    - An overview of the type of cyber security expertise required;
    - Insight into the sectoral and regional distribution of demand for cyber security expertise within the Netherlands: where does the demand come from?

5. https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

6. Make a reasoned estimate of the expected growth (present – 2028) of the demand for cyber security expertise (in terms of quantity and type of expertise). Do this based on future developments and historical growth.

Shortage

7. Provide insight (quantitatively and qualitatively) into the discrepancy between the demand for and supply of cyber security expertise. Analyse what factors cause this discrepancy. Consider, among other things, any (perceived) quality differences between different training courses and certifications.
8. Provide insight (substantiated with figures where possible) into the outflow of cyber security expertise on the Dutch job market and the reasons for this.

Advice

9. Provide evidence-based advice, including an implementation plan, on which (policy) instruments can be used in the short and long term to reduce the identified shortage in the cyber security job market. Also provide insight into which parties can/should play a role in this. Pay specific, but not exclusive, attention to:
    - The instruments of the Human Capital Agenda-ICT;
    - The public-private partnership platform dcypher;
    - Available policy instruments of the Ministry of Economic Affairs and Climate, the Ministry of Education, Culture and Science and the Ministry of Social Affairs and Employment (incl. The National Growth Fund (NGF), Action Plan for Green and Digital Jobs, The Employee Insurance Agency (UWV)).

1.3 Approach

1.3.1 Research and advisory report

In order to ultimately arrive at a supported recommendation, including an implementation proposal, the research was approached in the following manner. Figure 1 shows the flowchart of the research. The stars indicate the research questions answered in those blocks. Research and training have been used to identify the inflow and outflow in order to identify bottlenecks.

A vacancy analysis was carried out in the job market section and an answer provided to the growth demand of the cyber security job market.

Both streams provide data and input that can be used to understand the match between education and the job market. The output of this whole process is the research report.

A separate advisory report will be drawn up in addition to the research report, including an implementation proposal showing which recommendations can be implemented and by whom.

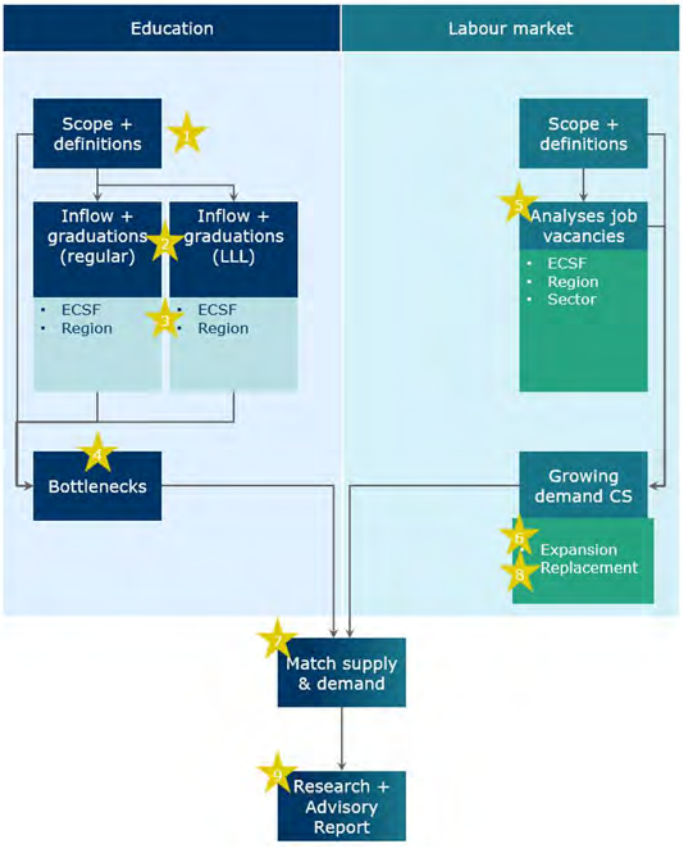


Figure 1: Research flowchart

1.3.2 Approach: a broad outline

As described above, there are two parts to this research: the research part that answers research questions 1 to 8 (and which are answered in this report) and the advisory part that answers research question 9, drawn up in early 2024 based on the results of the research part.

The relevant profession was consulted as much as possible during the research in order to arrive at supported advice based on empirical research and which ties in well with all current initiatives:

- The inputs were gathered and research results verified through interviews with representatives from education, business, sectors and relevant institutions.
- Qualitative input was collected about current training courses and vacancies from both education and the business community, as well as on future developments and expectations by distributing a number of questionnaires.
- Communications about the research were distributed and input collected through a poster presentation and a pitch at the ONE conference.
- It was possible to explain the research and approach, as well as gather a lot of input on the approach, outcomes, positioning and follow-up of the research, by joining the Cyber Security Council.
- The approach and interim results were shared at (online) workshops, where a great deal of input was collected that improved the accuracy of the research approach and interpretation of the results.

Chapter 2 describes how the research data for education and the job market was collected, how it was demarcated, and how the data was analysed.

Input for the advice and implementation part was collected by holding a workshop and a number of meetings with education and business representatives. This will be described in the advisory report.

2. Research methodology

This chapter describes the approach to making an inventory of the training courses on offer and identifying what is happening in education. The same methodology for the analysis of demand from the job market was used.
The focus of the research is on that part of the education that trains for job functions plotted in the Security Delta (HSD) Human Capital Agenda quadrant for "Occupations for Safety & Security of data and information systems".[6]
Both the data from the education and job market analyses were checked with a broad group of stakeholders and experts through workshops.

2.1 Methodology of MBO education

For MBO education, the final objectives (what students should know and be able to do at the end of the course) for the courses were coordinated with the receiving profession at a national level. This is recorded in a Qualification Dossier.
First, the Qualification Dossiers of the four ICT courses (current and from 2024) and the elective courses were assessed for their relevance to cyber security.
Training courses within Business Services and Safety were also examined for the sake of completeness.

The content of the education may vary. This is how the courses offer the necessary scope in the choice of working methods and content. To this end, a survey was conducted among ICT training directors to gain insight into how cyber security is being addressed in education.

These activities were set out in consultation and with the help of our contacts at the SBB Sector Chamber ICT and the MBO Council sector groups ICT & Creative Industry and Business Services and Safety.

Finally, we carried out desk research and searched the Katapult network for MBO education institutions with a clear cyber security profile in initial education.

2.2 Higher Education methodology

For Higher Education, colleges and universities have a lot of room to determine which courses they offer, the intended outcomes, and the content they provide. The institution writes a training plan that provides an overview of the intended learning outcomes for the entire training, the structure of the curriculum, the learning environment and the assessment methodology, and the teaching team that will provide the training. This curriculum is assessed by a panel of independent experts from the Accreditation Organisation of the Netherlands and Flanders (NVAO).

With regard to HBO education in the ICT domain, it is also relevant to mention the national framework for the final qualifications at associate degree, bachelor and professional master level. This domain description is maintained by the HBO-i foundation and established by the Association of Universities of Applied Sciences. Training courses can derive their own training profile, learning objectives and curricula from the domain description. Explicit linking of their training profile to the domain description guarantees the content and final level of the training. An IT security framework is currently being developed within the domain description to reinforce the link between education and business.

In order to identify the relevant Dutch cyber security courses at HBO and University level, a selection (using pr-eDICT) was made of all cyber security and safety-related courses and all ICT courses that had an intake in the years 2020-2022. Desk research was used to analyse and classify all these courses into three categories: [1] courses containing no cyber security, [2] courses containing some cyber security, and [3] courses that are fully focused on cyber security (viewing guide: ECSF profiles). Courses that were assessed as containing some cyber security were then further divided into the following categories: [1] programmes with a specialisation/elective cyber security component, [2] programmes with a compulsory cyber security component (more than 6 ECTS) and [3] programmes with one (elective) subject of 6 ECTS. Training courses from the first two categories were considered relevant for the purposes of this research.

The open-source Education Executive Agency (DUO) data was used to collect the inflow and outflow figures for all courses that are fully focused on cyber security and for category 2 containing some cyber security. If this data was not available (category 1 containing some cyber security courses, non-funded education, recently started courses), the inflow and outflow figures were requested from the programme director or education manager of the relevant course.

6. Figure 7: Safety and security occupations, HSD, 2018, blz 28, Human Capital Agenda Security 2023 – 2026

A survey was also conducted among the programme directors and education managers to gain insight into the current developments and trends in education, the connection and collaboration with the job market, and the bottlenecks within cyber security education.

Finally, during the process of identifying the relevant Dutch cyber security study programmes in Higher Education, interviews with representatives of education and (online) workshops identified specific cyber security study programmes that are still in the development phase, accreditation phase or start-up phase.

2.3 Methodology of Life-Long Learning (unfunded education)

A scraping of data with cyber security-related search terms via www.leeroverzicht.nl has been started. Based on the course descriptions, this resulted in 2,409 hits which were subsequently classified into 1. Fully focused on cyber security, 2. Containing some cyber security and 3. Containing no cyber security. This list also examined how many of the courses are aimed at attaining cyber security certification. This was done using automatic analysis of the training description and title, followed by a manual check for false positives. The analysis of vacancies also looked at which certificates are requested as part of a vacancy and how often.

The Regional scan for SME Digitalisation was used to build an inventory of regional, sectoral and national activities and initiatives for entrepreneurs and citizens. Within this overview, cyber security (240 hits) was selected, supplemented with activities obtained through a survey among the HCA-ICT regional contact persons.

The Katapult network map, with its overview of sustainable ICT partnerships, was reviewed for examples of ICT (re) training, specifically for cyber security.

2.4 Job market methodology

The paragraph below describes the definition of the concept of cyber security, how the European Cyber Security Skills Framework (ECSF) was used, and how the job vacancy analysis was carried out. A detailed description of the methodology is included in Appendix 1.
Cyber security is a broad concept. It concerns digital safety in the broadest sense of the word and includes technology, legislation, regulations, governance and organisation. The breadth of the concept of "cyber security" is logically also reflected in the expertise that professionals (must) have to work in this field. A clear definition of "cyber security expertise" is required in order to be able to discuss it.
Cyber security expertise in the job market can be approached at different "aggregation levels". The most direct and clear level of aggregation is the level of **job titles and profiles**. For example, there is demand for Chief Information Security Officers (CISO), Pen-testers or Cyber Incident Responders. For the purposes of this research, the European Cyber Security Skills Framework[7] formed the basis for twelve relevant (but illustrative) cyber security profiles (Figure 2).

Figure 2: The twelve job profiles within the ECSF

7. More information can be found at the ENISA website: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

The important benefits of talking about job profiles are that [1] people are usually able to imagine something about them and [2] they immediately provide a comprehensive picture in broad terms of what a person in that position does. However, there are some important disadvantages, including that [i] the contents of similar job profiles or titles can differ between or even within organisations and [ii] cyber security expertise can be required within a job profile that would generally not be classified as a cyber security profile in its own right. **Cyber expertise cannot be captured in a few functions, but can be part of a wide variety of professions on the job market**. For example, data engineers or ICT project managers must have an understanding of cyber security yet do not require a "pure" cyber security profile. It is therefore relevant to not only look at job profiles, but also to look at individual tasks, knowledge and skills at a "lower" aggregation level. The importance of "zooming in" on cyber security expertise is also emphasised by others in terms of, including for example the Security Delta (HSD) in their Human Capital Agenda[8].

Relevant tasks, knowledge and skills in cyber security have been identified in this research using the same ECSF. The twelve named functions are described in detail and structured on the basis of "Deliverables", "Main task(s)", "Key skills" and "Key knowledge". These **building blocks** can be visualised as follows (Figure 3):

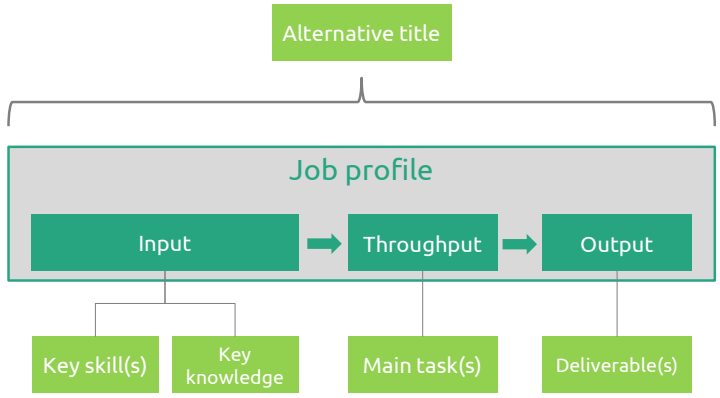


Figure 3: Building blocks for ECSF profiles

The twelve profiles correspond to 385 underlying building blocks, which corresponds to an average of 30-35 building blocks per profile. Although the twelve profiles themselves are by no means an exhaustive illustration of the cyber security job market in a broad sense, as researchers we expect the underlying 385 building blocks (deliverables, tasks, knowledge and skills) to provide a fairly complete picture of what can be understood to be cyber security expertise.

This research considers cyber expertise at the profile level, but the demand for the individual building blocks has also been investigated. These individual building blocks can then be found in the 12 (illustrative) ECSF profiles, as well as in other job profiles. Schematically, this looks like this (Figure 4):

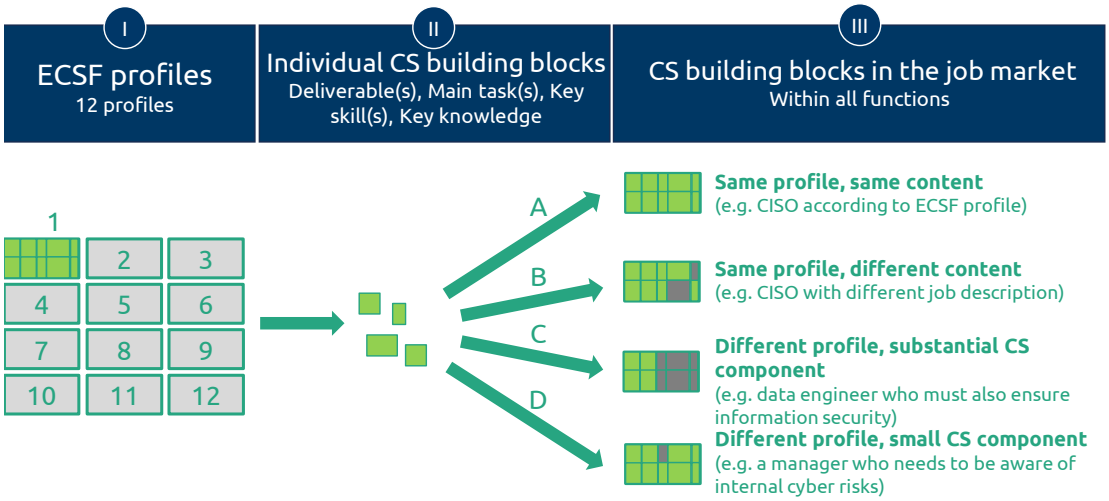


Figure 4: Cyber security building blocks in the job market

8. HSD (2023), Human Capital Agenda Security 2023 – 2026

This research therefore focuses on professions in which cyber security expertise is the main component (Types A and B in Figure 4), but also examines professions in which cyber security expertise does indeed play a role while not necessarily representing the main component (Types C and D in Figure 4).

A analysis of the vacancies on the job market to analyse the demand for cyber security expertise was carried out on vacancies from the period 2018-2022. The vacancy data comes from the company Jobdigger. The vacancy analysis follows a certain layering:

- An assessment was made of which vacancies actually require cyber security expertise. This was done by searching for a list of "generic cyber security terms". An overview of these generic terms is included in Appendix 1.
- A decision was then made to determine whether the relevant vacancy belongs to one of the twelve ECSF profiles.
- If the vacancy does not belong to one of the 12 ECSF profiles, the "cyber security level" was determined. Three categories were used for this, referring to a high cyber security level, a medium cyber security level or a low cyber security level.
- A search was also carried out in the relevant vacancies for individual tasks, knowledge and skills that are relevant to cyber security. These individual "building blocks" are based on all the building blocks named in the ECSF. This includes the 385 building blocks divided over 12 ECSF profiles.
- Two routes were used to put each building block in to practise: [1] manually creating a query that should be able to find the relevant building block in a vacancy text and [2] requesting ChatGPT to generate search terms using a separate prompt per type of building block. In the second route, approximately 20,000 search terms were manually viewed and scored on precision ("if this term is found, how likely is it that it also concerns building block X?") and recall ("how many of the building blocks on the job market are found with this search term"). After checking the two methods, it was decided that building block X was found in vacancy Y if at least one of the two methods produced a positive result.

In addition to conducting extensive analysis on job vacancies, an analysis was carried out on Statistics Netherlands microdata. The aim of this analysis was to gain insight into the outflow of cyber security professionals. This analysis was based on a list of companies (partly) active in the cyber security sector or involved in the "production" of cyber security goods and services. This list had been previously drawn up as part of the Dialogic report of 2023 called, "The economic opportunities of the cyber security sector". The people working at these companies and who are highly educated are the population of the analysis. Although these are not all cyber security professionals, cyber security professionals are not entered onto a register of cyber security professionals, so this is the second-best option to gain a general overview of the (relative) outflow.

3. Education Results

Research question 1:
Identify the relevant Dutch qualifications (MBO up to University level) and up-skilling initiatives (for example, mathematics , AI, data science, ICT). Build on existing initiatives such as the National Cyber Security Research Agenda (NCSRA) and the Platform Talent for Technology (PTvT);

In the training courses offered, it can be seen that attention has been paid to cyber security in the three MBO-level ICT Qualification Dossiers in recent years: ICT Support (Level 2), Software Development (Level 4) and ICT Systems & Devices (All-Round Employee Level 3 and IT Systems & Devices Expert Level 4). The renewal of these Qualification Dossiers, which will take effect on 1 August 2024, increases what students must know and be able to do terms of cyber security. In addition, three MBO initiatives were discovered that are in the development phase, accreditation phase or start-up phase.
At Higher Education level (HBO and University), there are, within the Accreditation Organisation of the Netherlands and Flanders (NVAO)-accredited programmes, 10 study programmes identified that are entirely focused on cyber security (5 HBO, 5 University), 29 study programmes that offer a specialisation/elective cyber security element (18 HBO, 11 University) and 13 study programmes (6 HBO, 7 University) that have a compulsory cyber security component in their programme (> 6 ECTS). In addition, 9 Higher Education study programmes (8 HBO, 1 University) that are still in the development phase, accreditation phase, or start-up phase were uncovered.
For Life-Long Learning, there is apparently an extensive non-funded educational offering, of which approximately 20% is aimed at the most sought-after cyber security certificates on the job market. In addition to many providers, we see one provider with a large portfolio offers.
Education is available in several forms, with hybrid forms becoming increasingly common. There are also many (often regional) activities and offers for SME entrepreneurs and citizens.

Research question 2:
Provide insight (substantiated with figures where possible) into the current inflow and outflow of training and retraining opportunities;

The total number of MBO ICT students remains approximately the same at around 23,000 students per year. Over the past few years, an average of 6,000 ICT students graduated each year.
The inflow of HBO and University students with a relevant cyber security component in their study programme has remained fairly stable over the past three years; around 3,000 students annually. However, the outflow of students is clearly increasing gradually on an annual basis, particularly in study programmes that are entirely focused on cyber security, or for students who have chosen a cyber security specialisation/elective component as part of their study programmes. Inflow and outflow figures for the private education market are not available for obvious reasons (competition-sensitive, privacy of participants).
The reach and impact of regional initiatives for SMEs and citizens are still difficult to estimate due to their heterogeneous nature.

Research question 3:
Use the results from (1) and (2) to provide insight (substantiated with figures where possible) into what type of cyber security expertise is offered and in what quantity;

Based on a global classification into types of expertise in technical, management & organisation, legal, research and education, the following can be seen in funded education:
The focus of MBO course content is mainly based on the technical aspects, as well as some management and organisational aspects. Due to the variation in how ICT courses shape education, it has not been possible to determine the exact size of the cyber security part of the course.
HBO and University education providers appear to have a more multi-disciplinary approach across the courses. It appears little or no attention is paid to competence development in any study programmes (MBO and Higher Education) in which students can develop didactic knowledge and skills.
Due to the large supply of training courses in the private segment, it is not feasible to plot and categorise the supply. Focus was put onto courses that lead to a cyber security certificate. Approximately 20% of all unfunded cyber security training courses focus on the most sought-after cyber security certificates on the job market.
The same applies to regional initiatives for SMEs and citizens. Overall, the offering there seems to be primarily aimed at increasing awareness and cyber resilience.

Research question 4:
Provide insight into the bottlenecks in cyber security training and retraining. Consider any factors that influence inflow and outflow.

The training directors highlighted the bottlenecks and/or challenges as: [1] updating lecturers, [2] shortage of students, [3] inadequate facilities, and [4] the rapid emergence of new AI themes, for example.
Various bottlenecks emerged during interviews and questionnaires with lecturers, professors and management of Higher Education institutions, these include: [1] shortage of teachers with sufficient knowledge, [2] the content of the curriculum in which both a broad profile and specialist profiling within the cyber domain must be offered, [3] the speed at which the security world is developing in combination with the lack of ability to respond flexibly to this, [4] the image surrounding cyber security education as a technical study programme, which influences recruitment and expectation management of (potential) students and [5] the lack of resources for e.g. educational materials, hybrid learning workplaces, etc.)
Trainers in the unfunded education segment state that the barriers include people not being given access to training subsidies for retraining, additional training and further training in cyber security, or who are not given sufficient time by employers to attend and/or complete a course.

3.1 Introduction

Cyber security education is developing rapidly. This chapter provides an overview of education and the inflow and outflow of students in and out of MBO education (Paragraph 3.3) and HBO and University education (Paragraph 3.4). Section 3.5 provides insight into the contents of these courses. Life-Long Learning is described in Paragraph 3.6; the conclusions and bottlenecks will then be addressed in Paragraph 3.7.

3.2 Framework/viewing guide

The type of training and final objectives for MBO education are both coordinated nationally. Each educational institution has room for its own interpretation of the education it provides within this framework. The description of the final objectives of all four MBO-level ICT courses was therefore examined. Training courses within Business Services were also taken into consideration.

For HBO and University education, a number of keywords were searched within the Education Executive Agency (DUO) and pre-DICT. Next, the information about training available online was examined and the training courses classified into:

- **Full cyber security study programmes**
- **Study programmes with a specialisation/choice for cyber security**
- **Study programmes with a compulsory cyber security component (> 6 EC)**
- **Courses with 1 (optional) subject of 6 EC**
- **No cyber security study programmes**

A number of cyber security and safety keywords were searched within overviews of non-funded education and public-private initiatives for the Life-Long Learning analysis.
Subsequently courses were labelled and comparable activities clustered to gain some idea of the focus of the offer. The training courses were also specifically reviewed to identify which ones offered training for cyber security certificates and how many.

3.3 MBO

3.3.1 Training offer

MBO schools offer courses at four levels. Qualification dossiers describe what the MBO students must know and must be able to do at the end of their training. The MBO training programmes and examinations are based on these requirements. Representatives from the profession and education develop Qualification Dossiers continually. The Minister for Education, Culture and Science is responsible for the contents of the Qualification Dossiers. The qualification requirements for obtaining the MBO diploma are therefore established nationally.

It is obvious that ICT training courses at MBO level have by far the most connections with cyber security compared to other MBO level training courses.
This is why these courses were examined first. The Qualification Dossiers provide a first look at the attention paid to cyber security. There are currently three Qualification Dossiers.
Table 1 describes the requirements linked to cyber security using keywords:

Current ICT Qualification Dossiers	
ICT support ICT support employee (Level 2)	Can apply security issues (such as firewall, virus scanner, WPA 2) Additional for Level 3: Provides users with guidance on security issues https://kwalificatie-mijn.s-bb.nl/

Software development Software Developer (Level 4)	Applies computer crime legislation, among other things, to software Can apply the principles of the Secure Software Development Life Cycle Can check and explain whether a software design meets security requirements https://kwalificatie-mijn.s-bb.nl/
IT systems & devices All-round IT Systems & Devices Employee (Level 3) IT Systems & Devices Expert (Level 4)	Works in accordance with applicable security guidelines Additional for Level 4: Provides security advice and improves security Responds to security incidents https://kwalificatie-mijn.s-bb.nl/

Table 1: Requirements linked to cyber security within the current MBO Qualification Dossiers

The two Level 4 courses (Software Developer and IT System & Device Expert) are most related to cyber security.

New Qualification Dossiers for ICT Support (Level 2) and Software Developer will come into effect on 1 August 2024. The ICT Support & Systems Qualification Dossier will succeed the IT Systems & Devices dossier on 1 August 2025. These new dossiers have also been reviewed.

These qualifications have been updated and cyber security given more explicit development (Table 2).
What is immediately noticeable, and also in line with expectations, is that much more attention is paid to cyber security. There is a separate profile section within the ICT system engineer course.

New ICT Qualification Dossier	
ICT support ICT Employee Level 2	Has basic knowledge of new developments in (network) security Can apply rules, agreements and procedures relating to safety and privacy https://kwalificatie-mijn.s-bb.nl/
Software development Software Developer (Level 4)	Has knowledge of security & privacy that is appropriate to his/her own field of expertise Has broad knowledge of cyber security and threats to networks and systems Has broad knowledge of legislation regarding computer crime and can work in accordance with it Follows applicable protocols and regulations regarding software safety, and demonstrates this in the design https://kwalificatie-mijn.s-bb.nl/
IT Support and Systems ICT Support Technician Level 3 ICT System Engineer Level 4	Has knowledge of simple security measures Can provide instructions to users regarding security Has knowledge about the security of information provision Works in accordance with SLAs, procedures and company agreements regarding security Demonstrates security awareness by including safety measures in information/instructions Profile section for Level 4: An important point of attention in the work of the ICT system engineer is security. This means both the security of systems and the response to cyber security attacks. Further detail is provided in the profile section. (as of March 2024)

Table 2: Requirements with a link to cyber security within the new MBO Qualification Dossiers

The ICT System Engineer Level 4 course pays the most attention to (cyber)security. This entry-level professional is trained to monitor and improve security and to respond to cyber security incidents.
In terms of the Software Development course, the young professional is primarily taught that security principles are present in all contexts of software development and that this must be taken into account in all (partial) designs.

Table 3 below contains information about how many MBO colleges offer which ICT courses. The Software Developer and Systems & Devices Expert courses have the most in common with cyber security. Almost all MBO schools offer these 2 courses.

Combination of ICT courses	Number of MBO courses
ICT Employee Level 2 Software Developer Level 4 All-round IT Systems & Devices Employee Level 3 IT Systems & Devices Expert Level 4	32
Software Developer Level 4 All-round IT Systems & Devices Employee Level 3 IT Systems & Devices Expert Level 4	5
Software Developer Level 4 All-round IT Systems & Devices Employee Level 3	1
Software Developer Level 4	2

Table 3: Which ICT courses will be offered and are offered

In addition, there are currently three MBO courses specifically focused on cyber security that are currently in the development phase, accreditation phase or start-up phase:
- MBO Rijnland: Cyber education
- Regional Training Centre ROC Aventus: Safety & Security
- Regional Training Centre ROC Mondriaan: Cyber education

In addition to the ICT courses, research was conducted into whether the Business Services and Safety course explicitly addressed cyber security knowledge and skills.
- The optional subject of Basic Cybercrime and Cyber Security has been developed as part of the Safety Officer course at Regional Training Centre ROC Aventus. Aventus is affiliated with the Centre for Safety and Digitalisation and works with East Netherlands Police to offer a one-year tailor-made training course for new police officers. The aim of this training is for students to become acquainted with the possibilities, threats and vulnerabilities of the digital world when carrying out their work and to take action if a digital incident is imminent or in progress. There is also a new qualification in development with the working title of Safety and Security. This is a qualification for a 1-year main training course (Level 4) in addition to Level 3 Safety Officer.
- In terms of legal and administrative training, the industry group is now in the process of collecting information about where training courses need to be updated from financial services companies. Topics such as sustainability and cyber security are included of course. But the work about deciding how these themes should be included in the training is still in the initial stages.

3.3.2 Inflow and outflow

The number of funded students in the school years 2017/2018 to 2022/2023 for each Qualification Dossier was examined (Table 4) to give an idea of the size of the potential HCA pool for cyber security in MBO education.

	2017-18	2018-19	2019-20	2020-21	2021-22	2022- 23
ICT Employee Level 2	2.457	2.496	2.340	2.348	2.405	2.330
Software Developer (Level 4)	8.018	8.718	9.011	9.251	9.486	9.553
All-round IT Systems & Devices Employee Level 3	4.631	4.272	3.979	3.437	3.006	2.715
IT Systems & Devices Expert Level 4	8.219	8.398	8.601	8.684	8.151	7.472
Total	23.325	23.884	23.931	23.720	23.398	22.532

Table 4: Number of funded students in school years 2017/2018 to 2022/2023 per Qualification Dossier
Source: The Education Executive Agency (DUO), processed by SBB, 7 February 2023

These numbers of ICT students across all courses result in an annual outflow of approximately 6,000 qualified MBO ICT graduates (Figure 5).

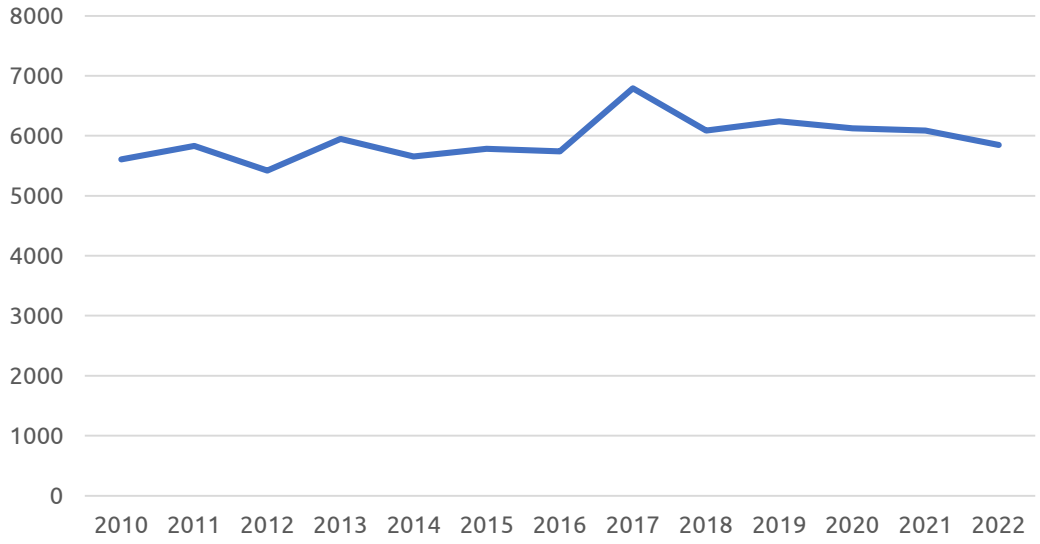


Figure 5: Annual outflow of certified funded MBO ICT graduates over time
Source: Human Capital Agenda (HCA) ICT, 2023 (generated from pr-eDICT on 18/01/2024 09:58)

Of course, these MBO graduates, including Level 4 students, will not broadly be deployable as cyber security specialists immediately after graduation. But in terms of numbers, it is of course a substantial source of cyber talent. After all, approximately 6,000 new ICT professionals who can contribute to the technical and operational aspects of cyber security and who could be placed on the path to becoming a cyber security expert are added to the job market every year.
It is therefore certainly relevant to continue monitoring the developments in these numbers of MBO students. For example, it is noticeable that there was an overall decline in the number of ICT MBO students between 2017 and 2023. It is also noteworthy to see that in the past year there has been a clear decline in IT system expert students. This is the course that most prepares for cyber security given the profile section in the new Qualification Dossier (table 4).

The number of students who take elective courses[9] that are specifically linked to cyber security was also examined. So far, this is limited to two elective modules offered within the ICT & Media Management, Smart Building and Smart Industry courses:

- The elective subject of Security in Systems and Networks 1 focuses on the preventive identification of policy deviations, vulnerabilities and threats, as well as the evaluation of the causes and risks for systems and networks. Proposals are made for security measures on this basis. This elective course will be offered by 19 MBO colleges across 34 courses to 1,004 students during the 2022-2023 academic year.

9. Source: S-BB Dashboard electives and MBO certificates. Note: this concerns the minimum number of students. Not all institutions have provided (complete) information. The dashboard does provide a representative picture, 60-70%.

- The Security in Systems and Networks 2 elective focuses on following technological developments to gain an insight into current threats and security options, comparing data from monitoring and testing, making proposals, and implementing security adjustments. This elective course will be offered by 13 MBO colleges across 20 courses to 321 students during the 2022-2023 academic year.

3.3.3 How do MBO education institutions provide ICT education?

The Qualification Dossiers ensure uniformity of the final objectives of the MBO courses. They give the MBO courses the necessary scope to fill in the educational programme.
In order to gain more insight into how cyber security education is shaped within ICT training courses, a survey was conducted among all 40 ICT training directors.
This resulted in a response from 17 participants.

Some insights from the survey are briefly summarised (supplementary tables in Appendix 2):

- When asked what grade they would give for their own cyber security efforts, more than half of the respondents gave themselves a 7 or higher. At the same time, the distribution of the scores is striking: this suggests they believe there is a considerable difference between the MBO ICT courses and the extent to which they pay sufficient attention to cyber security (Supplementary Table 4).
- Broken down by course, three out of four courses focus on cyber security (Supplementary Tables 5.1 to 5.4). Only in the ICT Support Employee Level 2 training course does 50% of the training course pay attention to cyber security.
- In the IT Systems & Devices Expert Level 4 course (Supplementary Table 5.4), attention is mainly paid to cyber security within the individual practical assignments and specific subjects and modules. In the training for software developers (Supplementary Table 5.2), attention is regularly paid to individual practical assignments and time for professional practical training.

Furthermore, desk research was conducted to identify Regional Training Centres (ROCs) that have so far focused specifically on cyber security. Currently these are:

- Regional Training Centre ROC Amsterdam: cyber security is a standard part of the ICT training courses. Students can choose the Cyber Security elective in the 2nd and 3rd year. If completed successfully, the student may officially call themselves a Cyber Security Specialist. Regional Training Centre ROC Amsterdam works intensively with large organisations such as SLTN, KPN and Hewlett Packard Enterprise. These companies contribute knowledge, expertise and teachers;
- Regional Training Centre ROC Mondriaan: cyber security is a standard part of the courses offered by the School for ICT. After completing the course, students can use practical solutions to make a company more resilient to cyber threats or progress to further education at a higher professional level. In the first year, all students receive instruction in Cisco's COPS subject and in the second year they complete a practical assignment in which a cyber security assignment is carried out within an SME;
- Regional Training Centre ROC Noorderpoort is affiliated with the Digital Craftsmanship Practorate (a practorate is a learning research community and platform of expertise in vocational education). The Practorate focuses on digital resilience as a person as well as on digital resilience in the profession. The Practorate is a follow-up to Cyber@ Work, a project in which ICT teachers embed cyber security in MBO ICT education and deploy students to reinforce the digital safety of citizens, associations, foundations and SMEs. Cyber@Work is now part of the Practorate as a knowledge circle;
- Regional Training Centre ROC Aventus participates in the in the Education and Life-Long Learning programmes of the Centre for Safety and Digitalisation. The possibility of a new substantive Level 4 training course in Safety & Digitalisation is being explored.

At the moment there are three MBO courses that are still in the development phase, accreditation phase or start-up phase:

- MBO Rijnland: Cyber education
- Regional Training Centre ROC Aventus: Safety& Security
- Regional Training Centre ROC Mondriaan: Cyber education

3.3.4 What expertise does MBO train for?

An expert assessment of the classification of competencies that the job market demands was made of the types of competencies per training course on the basis of the Qualification Dossiers (Table 5).
This gives rise to the impression that MBO ICT courses are mainly aimed at technical functions within cyber security.

Course name	Share of cyber security	Technical	M&O	Legal	Research	Education
Software Developer	Some	3	0	0	0	0
IT Systems and Devices Expert	Some	3	2	0	0	0
All-round IT Systems and Devices Employee	Some	3	1	0	0	0
ICT Support Employee	Some	3	0	0	0	0

Table 5: Expert assessment of the types of competencies for each training course based on the Qualification Dossiers

3.3.5 Bottlenecks

The ICT training directors were asked what is still required to provide up-to-date cyber security education (Supplementary Table 6). In order of most frequently requested, these include professionalisation of teachers (70%), co-operation from the profession (70%), education & examination materials (almost 65%), sufficient teachers (50%) and hybrid learning workplaces (over 40%).

They were also asked which cyber security themes require more attention. Of course, this does not necessarily have to be a bottleneck, but it may highlight where a bottleneck in education may arise. The most frequently mentioned are AI (almost 80%), Data awareness (almost 60%) and Collaboration tools (50%) (Supplementary Table 7).

3.4 Higher Education

3.4.1 Training offer

Colleges and universities offer courses at HBO and University level respectively. Each educational institution determines the content of the study programmes it offers. However, the institution must write a training plan, which is assessed by a panel of independent experts from the Accreditation Organisation of the Netherlands and Flanders (NVAO).

Table 6 provides an overview of the numbers of relevant Dutch cyber security courses at HBO and University level. Within the Accreditation Organisation of the Netherlands and Flanders (NVAO)-accredited programmes, 10 study programmes have been identified that are fully focused on cyber security, 29 study programmes that offer a cyber security specialisation/elective, and 13 study programmes that have integrated a compulsory cyber security component into their programme, greater than 6 ECTS. Details about which study programmes and the educational institutions that provide them can be found in the appendix (Supplementary Tables 8 to 10). While identifying the relevant Dutch cyber security study programmes at HBO and University level, several study programmes (including three MBO initiatives) were found that are still in the development phase, accreditation phase, or start-up phase. For the sake of completeness, these study programmes have been added to the bottom of Table 6. Details about which study programmes and the educational institutions that provide them can be found in Supplementary Table 11 in Appendix 2.

Full cyber security study programmes	Aantal
HBO	5
University	5
Total	**10**
Cyber security specialisation/elective within study programme	**Aantal**
HBO	18
University	11
Total	**29**
Compulsory cyber security component > 6ECTS within study programme	**Aantal**
HBO	6
University	7
Total	**13**
Upcoming cyber security courses	**Aantal**
HBO	8
University	1
Total	**9**

Table 6: Overview of the number of relevant Dutch cyber security courses at HBO and University level

3.4.2 Inflow and outflow

The number of funded students in Higher Education in recent years was also examined. To get a sense of the size of the potential HCA pool for cyber security from Higher Education, the student inflow and outflow figures for each study programme were collected for the school years 2019/2020 to 2022/2023. Where available, this data was retrieved from the open-source Education Executive Agency (DUO) data. Figures that were not made available to the Education Executive Agency (DUO) were requested from the relevant programme directors. The figures for each course can be found in Appendix 2 (Supplementary Tables 8 to 10). The figures below show the inflow and outflow data for the entire Higher Education sector. Data broken down by HBO and University education can be found in the appendix (Supplementary Figures 2 to 7 and 8 to 13, respectively).

Figures 6 and 7 show the inflow and outflow of students respectively for all study programmes with a relevant cyber security component. These include study programmes that are fully focused on cyber security, as well as study programmes that offer a cyber security specialisation/elective and study programmes that have integrated a compulsory cyber security component into their programme (> 6 ECTS). The open-source Education Executive Agency (DUO) outflow data for the 2022/2023 academic year and the inflow data for the 2023/2024 academic year is not yet available; therefore, these school years have been omitted from the graphs for visual representation. For some cyber security specific courses, this data has been made available by the programme directors. This data can be found in Appendix 2 (Supplementary Tables 8 to 10).

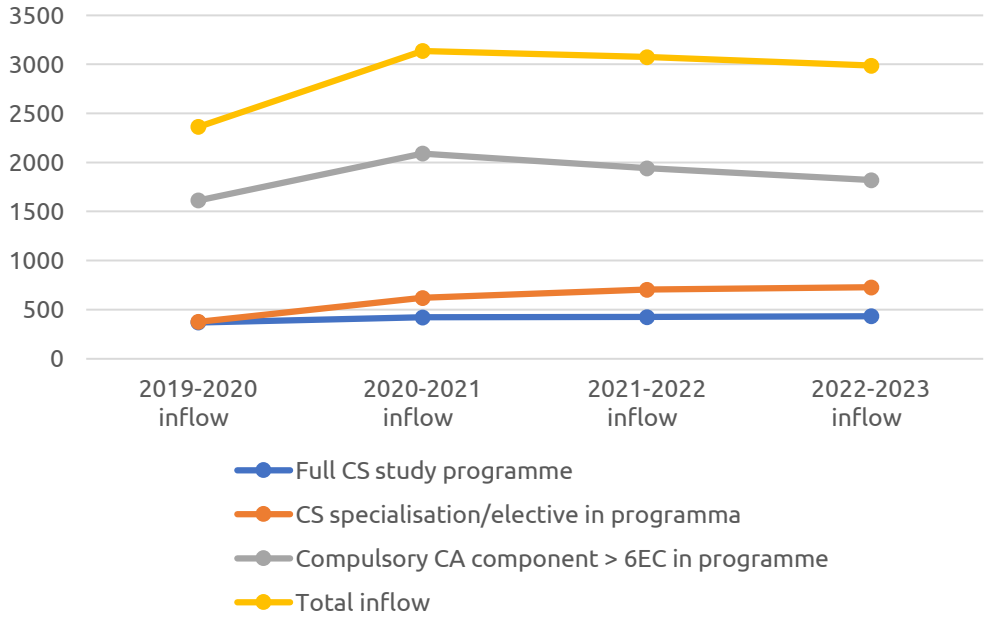


Figure 6: Student intake over time, all study programmes with a relevant cyber security component

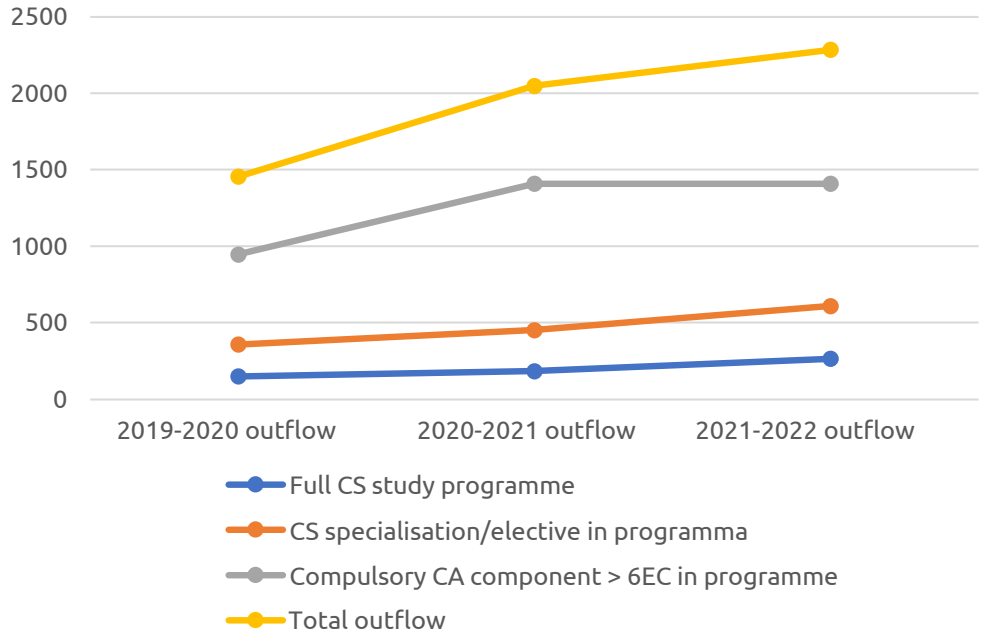


Figure 7: Student intake over time, all study programmes with a relevant cyber security component

Figures 8 and 9 show the inflow and outflow of students with a specialist cyber security focus respectively. These are students from study programmes that are fully focused on cyber security and students who have chosen to follow a cyber security specialisation/elective. Here too, the outflow data for the 2022/2023 school year and the inflow data for the 2023/2024 school year have been visually omitted from the graphs because the open-source Education Executive Agency (DUO) data for these school years is not yet available. Where available, these figures can be found in Appendix 2 (Supplementary Tables 8 to 10).

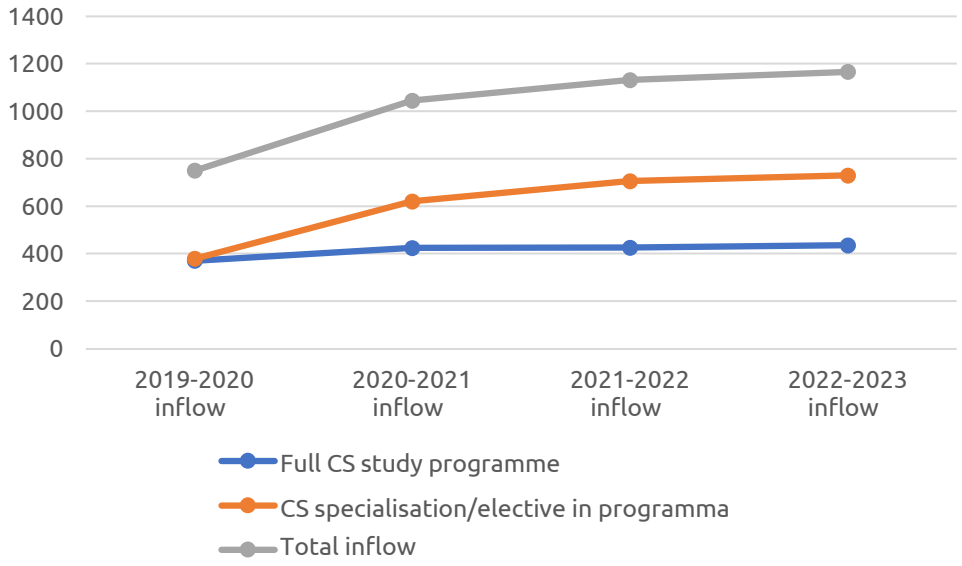


Figure 8: Progress of student intake over time, students from study programmes that are fully focused on cyber security, and students who have chosen a cyber security specialisation/elective within their study programmes

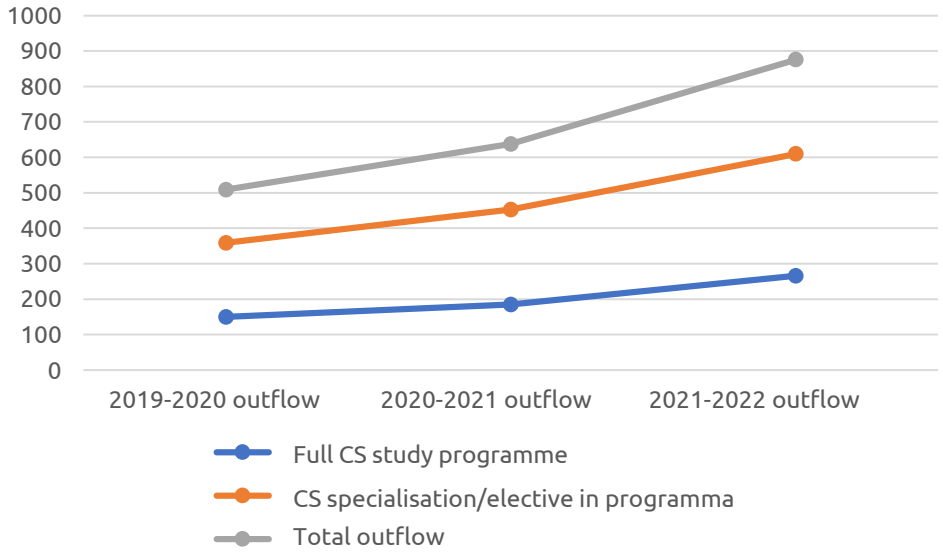


Figure 9: Progress of student intake over time, students from study programmes that are fully focused on cyber security, and students who have chosen a cyber security specialisation/elective within their study programmes

What is striking in Figures 6 and 7 is that the inflow of students with a relevant cyber security component in their study programme initially increases, but has remained fairly stable in recent years at around 3,000 students per year. However, the outflow of students is clearly increasing gradually every year. This increase mainly appears to be due to the number of students from study programmes that are fully focused on cyber security or students who have chosen to follow a cyber security specialisation/elective within their study programmes. Figures 8 and 9 confirm that both the inflow and outflow of this category of students increase over time. Given the inflow and outflow figures of approximately 70% of these courses with a cyber focus have been made available, the absolute numbers of students will be approximately 40% higher than shown in the graphs. It is expected that this will have little or no effect on the relative increase over the years.

To provide insight into the trend in the inflow/outflow ratio over the years, Figures 10 and 11 show the inflow and outflow per school year side by side.

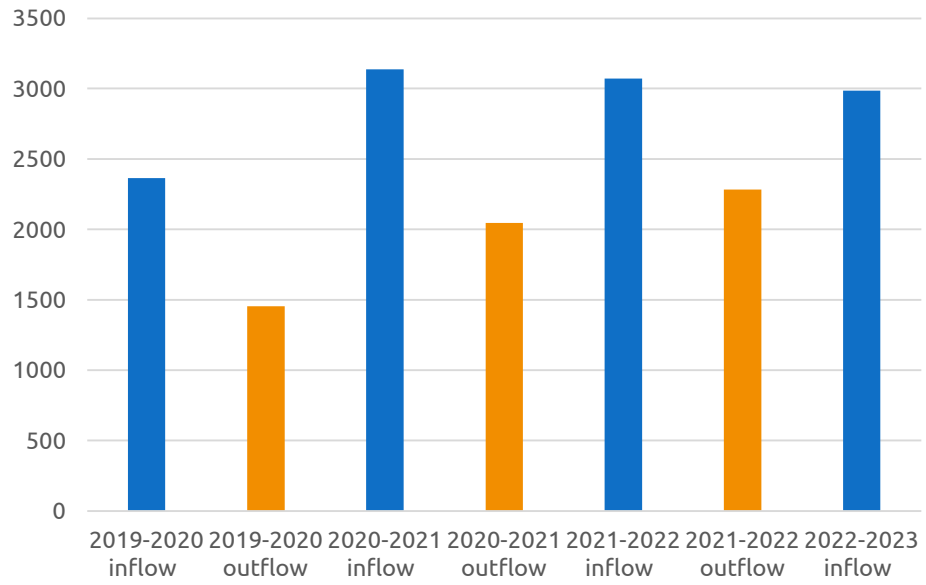


Figure 10: Inflow versus outflow for all study programmes with a relevant cyber security component

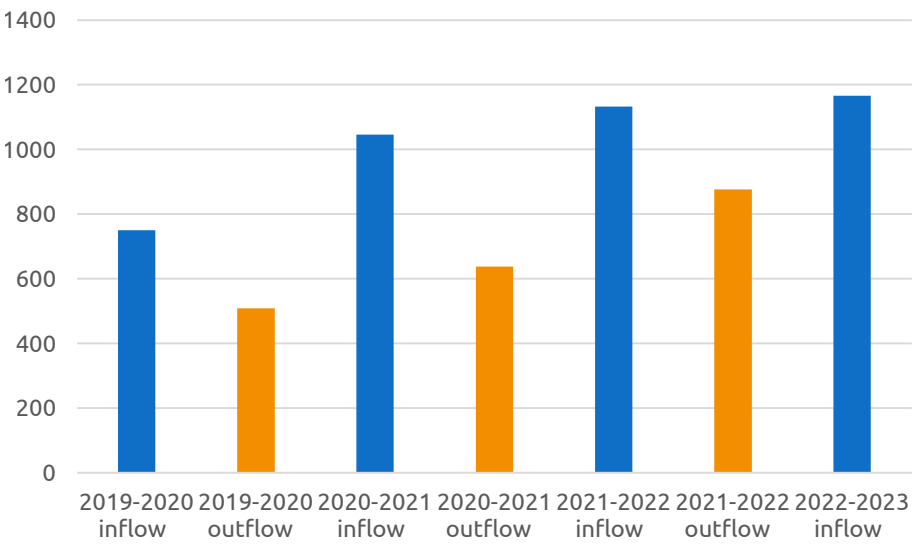


Figure 11: Inflow versus outflow of students who followed a specific cyber security course or a specific cyber security-oriented specialisation/elective.

The inflow of students is greater than the outflow of students for all school years. However, the differences gradually become smaller over time. It is likely that this decrease in the inflow/outflow ratio can be explained by the fact that most cyber security specific courses or specialisations/electives have only existed for a few years. For example, there are three specialisations/electives that only have their first student intake after the 2019-2020 school year. In addition, the Associate Degree Cyber Security of the Hogeschool van Amsterdam for example had its first inflow in 2019-2020, but has no outflow yet (Supplementary Tables 8 to 9). A study programme and/or specialisation/choice will have more inflow than outflow in the first few years. This will then catch up over time until an equilibrium is reached.

3.4.3 Survey results: developments and bottlenecks within cyber security education and actions already taken to optimise the connection to the job market

A survey was conducted among a selection of programme directors of specific cyber security courses and cyber security-oriented specialisation and elective programmes In order to gain insight into current developments/trends within cyber security education, the connection/collaboration with the job market, and the perceived bottlenecks. Twenty programme directors from thirteen different study programmes responded to the survey. The key results from the survey are summarised below:

Developments/trends in cyber security education

- Multidisciplinary approach to cyber security paying attention to both the technical and organisational elements/ policy, legislation and regulations, ethics and communication (specialist level and lay language);
- Introducing a circular policy (Adaptive Security Framework of Gartner, CSF2.0 of NIST, etc.);
- Compliance with laws and regulations (AVG, GDPR, NIS2, etc.);
- IT or security-related certificates (ISO27001, ISO7510, BIO etc.);
- Continuously updating education in view of rapidly developing focus areas: information management, cloud security, automation through AI (which will drastically change the roles of people and technology), internet of things, pen-testing, vulnerability reporting, SecDevOps, cyberspace, quantum technology, defence against advanced automated cyber attacks, thread intelligence, etc.);
- Lecturers and experts from public and private organisations, which guarantees a high quality standard;
- In general, there has been an increase in the number of cyber incidents.

Current actions for optimal connection/co-operation with the job market

- Use of guest speakers and freelance teachers from the business community;
- Internships and/or graduation projects in the profession;
- Stimulating the connection between education and job market demand by representing both education and the job market in, among other things, the training advisory council, company advisory council, other advisory bodies, representatives commission, professional field committee;
- Organisations and foundations such as Cyber Safety Nederland, Security Delta, Platform for Information Security, National Cyber Security Centre, HBO-i, Intersct, ACademic Cyber Security Society, dcypher, NEXIS;
- Cyber security events for both education and business;
- Network of teachers, alumni and their employers;
- Stakeholder events (for example an annual stakeholder dinner)

Bottlenecks in education

- Teachers:
  - Shortage of teachers with sufficient knowledge, scarce pool of experts;
  - Retaining qualified teaching staff is a challenge due to, among other things, the discrepancy between remuneration in the business community and education;
  - Learning cyber security skills requires technical hands-on courses. These are relatively hard for teachers and should be delivered in relatively small groups for optimal learning;
- Developing materials and compiling a curriculum in which quality is guaranteed across a broad profile with the teaching of very diverse skills while simultaneously offering focused and specialist profiling within the cyber domain;
- The speed at which the security world is developing combined with the lack of ability to respond flexibly to this. This is because educational units must be decided upon more than a year before implementation;
- Cyber security education is still often seen as a technical study programme. There is in sufficient recognition that cyber security education is part of all aspects of our living environment. This is important in the recruitment and expectation management of (potential) students;
- Lack of resources (lab with equipment).

3.5 Comparison of MBO and Higher Education courses content

In order to estimate the types of competencies for which a student is trained, the representation of the following competencies within the MBO and HBO courses was examined: technical, management & organisation (M&O), legal, research and education. The representation of the relevant competence is scored on a scale from 0 (no/hardly any role for the relevant competence) to 3 (the primary focus is on this competence) (Table 7).

Education type	Technical	M&O	Legal	Research	Education	Total
University	2,4	1,1	0,9	2,7	0,0	7,0
HBO	2,3	1,8	0,9	0,9	0,0	6,0
MBO	3,0	0,8	0,0	0,0	0,0	3,8
Total	2,4	1,4	0,9	1,6	0,0	6,3

Table 7: Representation of competency types within MBO and HBO courses

HBO and University education providers appear to have a more multi-disciplinary approach across the courses. The four MBO courses (Qualification Dossiers) have a strong technical focus. The teaching competence goes from strongly under-represented to absent in all study programmes. An overview of the individual MBO, HBO and University courses, scored according to their level of alignment with job market competencies, can be found in Appendix 2 (Supplementary Table 12).

3.6 Life-Long Learning

3.6.1 Training offer

For Life-Long Learning, the research team considered both non-funded education and public or public-private initiatives that focus on additional/further and retraining of all types, sizes and target groups. Initiatives that aim to generate additional (lateral) entry have also been included.

Non-funded education

Non-funded education is not subsidised by the Ministry of Education, Culture and Science or the Ministry of Economic Affairs and Climate. The costs of the training are borne by the person taking the training, the employer or the benefits agency. This private training offer is broad and diverse.

The following sources were consulted:

- www.leeroverzicht.nl

An exhaustive list of cyber security terms was used to scrape the website. This resulted in 2,409 hits, which were subsequently classified into fully focused on cyber security, containing some cyber security and containing no cyber security (Table 8).

	Fully focused on cyber security	Some focus on cyber security	No focus on cyber security	Total screened hits
Number of courses of non-funded education	1136	824	449	2409

Table 8: results from www.leeroverzicht.nl classified into fully focused, some focus and no cyber security

The list from the learning overview provides insight into the most important providers ranked according to the number of training courses etc. offered (Table 9):

#	Training provider	Quantity
1	Global Knowledge Network Netherlands bv	543
2	Icttrainingen.nl	155
3	Startel	132
4	Fast Lane Benelux B.V.	120
5	Master it Training	107
6	NCOI	104
7	Vijfhart IT-Opleidingen	92
8	@The Academy	89
9	Eduvision Opleiding & Training	69
10	CLS-trainingen	63
11	Computrain	63
12	Security Academy Opleidingen B.V.	57
13	SpiralTrain BV	30
14	Capgemini Academy	26
15	TSTC BV	23
16	LOI	16
17	IT Management Group	9
18	Xebia Academy	9
19	BTR Trainingen	7
20	Cibit Academy BV	7

Table 9: Top 20 training providers on www.leeroverzicht.nl

The number of courses offered in the form of contract education by MBO, HBO and Universities was also counted (Table 10):

	MBO and Higher Education offering in leeroverzicht.nl	
	Fully focused on cyber security	Some focus on cyber security
MBO	10	12
HBO	21	33
University	10	3

Table 10: Number of courses offered by MBO, HBO and Universities

Most of these courses require a substantial investment of time because they lead to a regular diploma (Supplementary Table 13 and 14).

Approximately 20% of all unfunded cyber security training courses focus on the most sought-after cyber security certificates on the job market. Appendix 2 contains Supplementary Table 15 with the number of courses from leeroverzicht.nl that lead to a certificate. The certificates were also scored on the extent to which they match the required job market competencies.

- *overview of Netherlands Training and Education Council (NRTO) training courses*

Not all training providers are on leeroverzicht.nl. For the sake of completeness, a quick scan was carried out of websites with training courses and education with an Netherlands Training and Education Council (NRTO) quality mark. This resulted in only a handful of courses that were not included in the learning overview. For the purposes of the analysis, this seems like a negligible number.

Public private initiatives

- *Regional scan for SME Digitalisation*

The Regional Scan for SME Digitalisation was carried out in every Dutch province at the end of 2022 and the beginning of 2023. This is a systematic inventory of regional public-private initiatives and activities aimed at the digitalisation of SMEs.
The Regional Scan was developed on the initiative of the Ministry of Economic Affairs and Climate in close collaboration with the provinces and large municipalities with the aim of:

- Gaining more insight into the ecosystems of public or public-private initiatives that
- stimulate digitalisation in SMEs;
- Identifying best practices and increasing learning capacity across regional borders;
- Stimulating greater coherence, co-operation and referral between initiatives.

The initiatives were provided with a number of labels, including the cyber security label. This selection was based on the label and was supplemented with initiatives known to the regional HCA-ICT contact persons and provides the overview presented in Table 11.

Type of activity	Quantity	Examples
Workshops & knowledge events	39	Online knowledge sessions to promote digitalisation Public knowledge café
Advice/consultancy	28	Digital support team First line advice
Network & coordinate	26	Support groups MIEC Data
Grants & financing	21	General Innovation – innovation projects Digitisation vouchers
Scans & assessments	22	AVG scan Basic Cyber Resilience Scan
Working with students	19	Vouchers blockchain projects Student advisory processes
Education for professionals	16	Lifelong Learning & Development – SME sectors Online training
Education for students	15	Cyber Serious game Hacklab.frl
Knowledge platform	12	MIEC Data Platform ICT providers
Shared facilities	10	Digitisation scan from ik ben Drenths [I come from Drenthe] Entrepreneur R&D Labs
Research and development	12	Research – Practorate for Cyber Resilience Safe Equipment
Signalling	5	Communication to SME stakeholders about acute cyber threats. Identifying training needs (via a scan for example)
Total	**225**	

Table 11: Activities for SMEs and regions, specifically cyber security:

Supplementary Table 16 is included in Appendix 2 with the list of all regional initiatives.

- *Public-private (re)training initiatives*

A search was conducted on the internet and within the Katapult network for public-private (re)training initiatives aimed at increasing the inflow into cyber security education and functions. An overview of these initiatives is shown in Table 12. The Hacklab, Cloud IT Academy and Make IT Work initiatives are listed on the HCA-ICT – network map, with Make IT Work also having the status of a working model/example initiative.

	Name	Region	Description
1	Hacklab	Friesland	The Hacklab is a safe place where young talented internet users can come to develop knowledge and skills within the cyber domain at their own level and pace. The workshop is open to digital youth, gamers, school leavers, young people on the autism spectrum and young people who miss a challenge in their current education. No prior education is required; just motivation and curiosity. The Hacklab hosts various guest lecturers who pay attention to 21st century skills in terms of IT/internet. Students are challenged with various individual and group assignments including hacking, programming, lockpicking, pen-testing, etc. Every student is different, so a mentor will help find a suitable development path as part of the workshop. The Hacklab mentors match students to potential employers if desired. This means students can gain practical experience, learn what "work" is, and, if there is a mutual click and good co-operation, get a full-fledged internship, traineeship or even a job. https://hacklab.frl/
2	Cyber security works	National	Security Delta (HSD) wants to use the www.cybersecuritywerkt.nl platform to help solve the mismatch between supply and demand for cyber security talent. The website offers plenty of opportunities for retraining and lateral entrants who want to change careers into cyber security. This is a great way to help people with an interest in cyber security (and a different background) find their way around the cyber security job market. The website contains: knowledge about cyber security, an overview of the different professions available, a test based on their work and educational background, and an overview of relevant vacancies for starters in the cyber security domain https://cybersecuritywerkt.nl/
3	Cyber Security & Cloud Cloud IT Academy	Utrecht	CITA companies offer direct employment and the opportunity to deepen and expand knowledge through the dual HBO Cyber Security & Cloud course at Hogeschool Utrecht. https://cita.academy/studenten/cyber-security-cloud/
4	Make IT Work	National	Retraining programme at HBO level with a guarantee of a job IT. One of the three retraining programmes is cyber security. The foundation for programming, databases and SQL, operating systems and networks is provided in the basic phase of this cyber security training. The student acquires fundamental knowledge and skills on a variety of cyber security topics through tutorials and practical assignments during the advanced phase. https://it-omscholing.nl/programmas/cybersecurity/
5	re_B00TCMP	National	An event set up especially for young people who have an interest and skills in IT. During re_B00TCMP they will gain more insight into working within the IT industry. This is achieved via sessions with the cyber security industry, the police and the gaming sector. They also learn more about online boundaries and the impact of cyber crime. Young people between the ages of 12 and 25 with an interest in IT gain insight into the opportunities and risks of their exceptional cyber talents through interactive workshops. https://re-b00tcmp.nl/

6	International Cyber Security Summer School	National	Security Delta (HSD) organises the International Cyber Security Summer School (ICSSS) every year in August in collaboration with the NCI Agency, Europol, Universiteit Leiden, and several Security Delta (HSD) partners. This is a multi-day event with one important goal: preparing emerging cyber security talent for a great career. Participants are students (PhD, Master) and starters/young professionals. The varied programme offers interesting lectures from top experts, perspectives from professionals in the profession, group assignments, and fun social activities such as visiting companies and going on excursions. www.summerschoolcybersecurity.org

Table 12: (Re)training and (lateral) entry initiatives specifically aimed at cyber security

3.6.2 Inflow and outflow

There is no quantitative data available on reach/number of participants who attend private education.
Some qualitative images from the trainers:

- Participants: mostly 35 years and older;
- High demand for training aimed at obtaining specific cyber security certificates;
- Decrease in demand for privacy training, increase in demand for simulations (group hacking attempt);
- Hybrid forms of learning are becoming increasingly popular;
- Customers: mainly government, banks, telecom.

In order to gain a further insight into the interest in (re)training, the Employee Insurance Agency (UWV) was approached and asked about how many people had applied for a STAP budget for cyber security training. Unfortunately, the Employee Insurance Agency (UWV) is not yet able to make these types of selections from the participants and database of training courses attended. This was the wish, but its development will not continue thanks to the discontinuation of the STAP scheme.

The researchers do not know the number of participants in the regional (SME) initiatives and it is difficult to determine.

3.6.3 What expertise?

What is the main thrust of training in non-funded education?
Certificates play an important role in the Life-Long Learning for cyber security, so this will be the focus of this section. What certificates are most in demand in the job market and how does the training market respond to the demand?

We approached the question in two ways:

- ChatGPT searches and interrogation of the Tweakers website question and answer function were used to determine the most-requested certificates. This resulted in a list of 22 certificates. The next step was to look at how often training courses for these cyber security certificates appear in www.leeroverzicht.nl. In order to bring this information to a somewhat similar level to that of government-funded education, the certificates were also scored on the types of competencies required by the job market. In total, www.leeroverzicht.nl has 240 courses offering training for one of these most requested cyber security certificates. Looking at the range of courses for certificates, 111 courses are for certificates that have a broader scope than technology/engineering, including management, organisation and legal (Supplementary Table 15).
- Secondly, the vacancy analysis looked at which certificates are requested in vacancies and how often. The top three are CISSP, CISM and CISA. This top three does not change, even if you look at the most common job descriptions (and the certificates requested for the associated vacancies). In addition, an investigation was carried out to look at how often certificates are requested for the most common jobs. For example, it appears certificates are required for 70% of the IT Security Officer and Information Security Consultant vacancies. Other jobs, such as (cyber security) consultant, appear to be less certificate-dependent (Supplementary Table 25).

3.6.4 Bottlenecks in the Life-Long Learning domain

The following statement was provided by Netherlands Training and Education Council (NRTO) members: retraining is still feasible if you have a willing employer behind you, but it is unaffordable for individual employees who do not. Structural provisions such as a system of individual learning rights are lacking. This particularly affects private IT training providers who offer opportunities to everyone; women, unemployed young people or people from socially disadvantaged backgrounds. The advantage of encouraging private IT trainers who also make a social contribution is that it creates a win-win situation and increases diversity in the professional group of cyber security specialists.
Furthermore, well-known bottlenecks in Life-Long Learning also play a role here, such as combining education with a private situation, the ongoing costs of living, holding on to certainties, and short-term thinking. Trainers also see that filling groups for cyber security training and the subsequent participation in the training after registration is problematic because employees are not released by their employers.
These bottlenecks are of course not unique to cyber security training, but they are just as relevant – despite the urgency of the subject. According to private trainers, cyber security training courses based on certificates could therefore serve as a good pilot for stimulating a learning culture or granting learning rights. In doing so, social benefits are linked to opportunities for people to develop further.

3.7 Conclusions and bottlenecks in the provision of education

In conclusion, we see the following for each type of education:

MBO

- Within MBO there is increasing attention specifically paid to cyber security in ICT courses based on the additions made to the Qualification Dossiers;
- The MBO ICT courses focus mainly on the technical aspects of cyber security;
- The number of ICT students has remained at approximately the same level in recent years, with a slight decrease in the number of students in the ICT System Engineer Level 4 course, which is the MBO course most closely linked to a cyber security career;
- A number of MBO education institutions clearly have the ambition and vision to prepare their ICT students for cyber security jobs;
- Cyber security pilots are currently taking place within the Business Services domain in the form of elective and preparatory courses in security training; of course, the question is whether these future professionals can be considered cyber security specialists;
- ICT courses report bottlenecks in realising up-to-date cyber security education, which includes a shortage of teachers, updating existing teachers and inadequate facilities. Another challenge is how to implement new themes (including AI) into the education.

Higher Education

- Within the Accreditation Organisation of the Netherlands and Flanders (NVAO)-accredited programmes, 10 study programmes have been identified that are fully focused on cyber security, 29 study programmes that offer a cyber security specialisation/elective, and 13 study programmes that have integrated a compulsory cyber security component into their programme, greater than 6 ECTS.
- The outflow of students is gradually increasing every year, especially for study programmes that are fully focused on cyber security or that have a cyber security specialisation/elective.
- Higher Education courses appear to have a more multi-disciplinary approach. However, the teaching competence is either heavily under-represented or absent in all study programmes.
- Major bottlenecks within Higher Education include a shortage of lecturers with sufficient knowledge, the content of the curriculum in which both a broad profile and specialist profiling within the cyber domain must be offered, the speed at which the security world is developing in combination with the lack of ability to offer a flexible response, and the image of cyber security education as a technical study programme, which influences the recruitment and expectation management of (potential) students and the lack of resources.
- 12 study programmes (including three MBO initiatives) were identified as still in the development, accreditation or start-up phase.

Life-Long Learning

- There is plenty of private supply, by far the largest provider with training courses containing cyber security elements is Global Network Netherlands.
- A substantial number of the courses prepare students for being awarded relevant cyber security certificates.
- Private trainers still see many obstacles in recruitment and participation for people who want to be retrained and further trained in cyber security.
- Many and diverse initiatives (public-private) are aimed at SMEs and citizens. This perhaps illustrates the point from the HCA Security Delta (HSD) 2030: there is a lack of structure and overview regarding the provision of formal and non-formal (cyber) security learning;
- The courses offered by Higher Education and MBO institutions as non-initial education often lead to regular diplomas. There may be some gains to be made here by responding to another recommendation from the HCA Security Delta (HSD): provide shorter modules and training to make them suitable for working people; after all, they are the largest talent pool for cyber security. The question is how these qualifications match job market demand considering many vacancies require specific certificates.

4. Job market results

Research question 5:

- *Clearly define (substantiated with figures where possible) how great the demand for cyber security experts is, and what expertise is required. Do this based on:*
- *An overview of the vacancies registered by Dutch organisations that employ (or will employ) cyber security professionals;*
- *An overview of the type of cyber security expertise required;*
- *Insight into the sectoral and regional distribution of demand for cyber security expertise within the Netherlands: where does the demand come from?*

The demand for cyber security expertise is growing, both for specialist cyber security profiles and for broader job profiles of which cyber security is a part. We estimate there are approximately 60,000-110,000 cyber security professionals active in the job market, of which 17,000-33,000 professionals have a specialist cyber security profile. The demand for cyber security expertise is concentrated in the provinces of Noord-Holland, Zuid-Holland and Utrecht, while the focus of the demand lies on intermediate and senior positions for which HBO or University education is required. The government and the IT sector are the two sectors with the highest demand for cyber security expertise. In addition, organisations that do relatively more with cyber security also have a greater demand for specialist profiles. The demand for cyber security professionals depends, among other things, on the role that parties have in the "cyber security value chain". For example, there is high demand for specialist cyber security profiles in the cyber security sector itself (the production of cyber security goods and services), while Cyber R&D (logically) has a high demand for Cyber Researchers.
A relatively high level of technical knowledge is required across the board to work in cyber security, but the skills required and the tasks to be performed are largely non-technical in nature. The composition of knowledge/skills/tasks appears to be quite stable as the jobs require more work experience. This implies the actual implementation of these building blocks, and the extent to which people are able to implement them, grows objectively as they develop further. Finally, 15% of the vacancies explicitly request a cyber security certificate. The most requested certificates are CISSP, CISM, and CISA.

Research question 8:
Provide insight (substantiated with figures where possible) into the outflow of cyber security expertise from the Dutch job market and the reasons for this.

The cyber security professional population is relatively young with approximately three-quarters under the age of 50. A quarter of the cyber security professionals left the cyber security sector in 2021, three-quarters of whom found a job with a company outside the survey population. Only 4% left due to retirement and emigration. The expectation is that there will be relatively little replacement demand due to retirement in the coming years.

4.1 Introduction

Cyber security is a multi-disciplinary field with many facets. It is therefore no easy matter to gain a good picture of the "cyber security job market". Various parties have tried to understand this job market in recent years.

According to the publication, "The ICT Picture" published by the Employee Insurance Agency (UWV)[10], 4,100 cyber security vacancies were advertised in 2022 (ICT Security Specialist/ICT Security Advisor). 4,738 cyber security vacancies and 11,071 ICT vacancies on pr-eDICT.nl for the year 2022 required at least one cyber security skill.

Based on figures from Statistics Netherlands, the Employee Insurance Agency (UWV) arrives at 13,000 ICT Security Specialists/ICT security consultants in terms of the number of employed cyber security professionals. The Security Delta (HSD) Human Capital Agenda estimates that in 2021, 0.4% of the working population will be cyber security professionals, which equates to ~39,000 professionals.

It is clear with such figures that it is crucial to decide on the demarcation and definition of "cyber security professional" that will be used. In many studies, cyber security seems to be approached in a fairly narrow (and often technical) sense; despite this, the interviewees spoke of its breadth and multi-disciplinary nature.

This research provides in-depth insight into the demand for cyber security expertise in the job market. What exactly is being asked for, and by whom? The foundation of the research is an extensive analysis of job vacancies, an online survey among members of Cyberveilig Nederland, and organised workshops.

This chapter is structured as follows:

- In 4.2 the **conceptual framework** will be presented and the concepts of "cyber security professional" and "cyber security expertise" examined.
- In 4.3 the **demand for cyber security professionals in general** will be addressed. This includes the number of vacancies and how they are divided into education level, work experience, region, sector and target group.
- In 4.4 the **demand for specific job profile**s will be addressed. A distinction will be made between job profiles with a large and small "cyber" component.
- In 4.5 the **demand for specific knowledge and skills** will be addressed. Here we take a deeper look at the "job profile" by reviewing the individual "building blocks" in terms of tasks, knowledge and skills that are required within vacancies on the job market.
- In 4.6 the **"outflow" and "inflow"** of cyber security professionals will be discussed. This includes looking at the outflow due to retirement and emigration and the inflow due to immigration.
- In 4.7 the **relevant developments for the future demand** for cyber security professionals will be addressed. This includes issues such as the NIS2 directive, the CRA and the use of AI.
- 4.8 finishes with the main **conclusions** we can connect to the results of this research.

4.2 Conceptual framework

4.2.1 Cyber security expertise

Cyber security is a broad concept. It concerns digital safety in the broadest sense of the word and includes technology, legislation, regulations, governance and organisation. The breadth of the concept of "cyber security" is logically also reflected in the expertise that professionals (must) have to work in this field.

Cyber security expertise in the job market can be approached at different "aggregation levels". The most direct and clear level of aggregation is the level of **job titles and profiles**. For the purposes of this research, ENISA's ECSF has been taken as the basis for twelve relevant (yet illustrative) cyber security profiles.

Cyber expertise cannot be captured in a few functions, but can be part of a wide variety of professions on the job market. It is therefore relevant to not only look at job profiles, but also to look at individual tasks, knowledge and skills at a "lower" aggregation level. **Relevant tasks, knowledge and skills** in cyber security have been identified in this research using the same ECSF. The twelve named functions are described in detail and structured on the basis of "Deliverables", "Main task(s)", "Key skills" and "Key knowledge". See also 4.2.1 for further explanation.

Although the twelve profiles themselves are by no means an exhaustive illustration of the cyber security job market in a broad sense, as researchers we expect the underlying 384 building blocks (deliverables, tasks, knowledge and skills) to provide a fairly complete picture of what can be understood to be cyber security expertise. This research considers cyber expertise at the profile level, but the demand for the individual building blocks has also been investigated. These individual building blocks can then be found in the 12 (illustrative) ECSF profiles, as well as in other job profiles. This research therefore focuses on professions in which cyber security expertise is the main component, but also examines

10. Source: Employee Insurance Agency (UWV), August 2023, based on figures from Statistics Netherlands. https://www.werk.nl/imagesdxa/factsheet_ict_tcm95-451428.pdf

professions in which cyber security expertise does indeed play a role and at the same time does not necessarily represent the main component.

4.2.2. Target groups

In this research we are not only interested in what types of expertise are required in what job profiles, we are also interested in **who has what need for cyber security expertise**. After all, there are major differences between organisations in terms of objectives and tasks, activities and the role cyber security plays.

First, the three-way division between business community, government and knowledge/educational institutions is examined. This provides more insight into the context in which cyber security expertise is required.

In addition, the roles that parties represent in the cyber security "value chain" are also examined. This uses research previously carried out for the Ministry of Economic Affairs and Climate concerning "The economic opportunities of the cyber security sector".[11] This presents a framework distinguishing between four categories (Figure 12):

A. **Cyber R&D**. These are cyber security-specific R&D activities. These results can generally be used by the cyber security sector to develop and/or improve products (goods/services).

B. **Production of cyber products and services**. This involves the (economic) activities for which cyber products/services are developed, and for which it can be stated that the output is 100% related to cyber security. ENISA has distinguished eight subcategories within this category, including hardware, consulting and managed services.

C. **Cyber integration**. This involves (economic) activities in which cyber security is integrated into a "broader" product. Examples include payment services that need to be cybersecure, vehicle braking systems that must not be hackable, or household appliances that need to be digitally protected. The output in this category is therefore partly related to cyber security and partly not.

D. **Cyber end use**. Finally, the cyber end-use category represents all (economic) activities in which "cyber security products" (100% cyber or integrated into other products) are used, but where the output no longer contains a cyber element. For example, a baker who purchases and uses a secure payment system, but actually only produces bread himself.

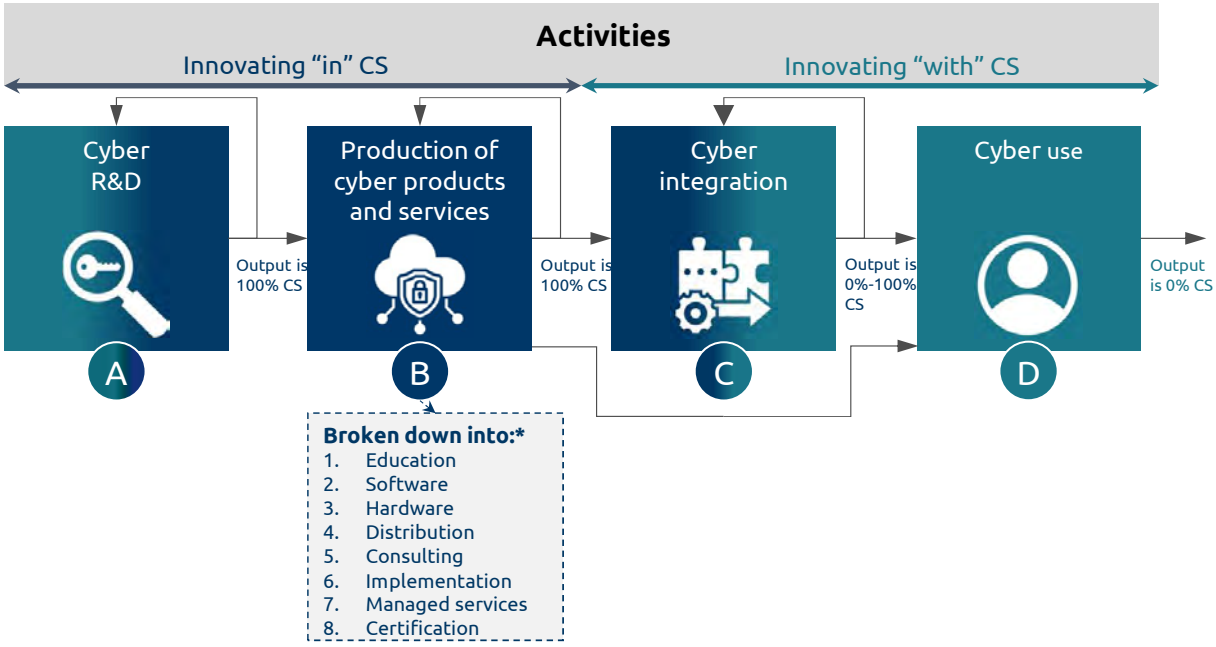


Figure 12: The cyber security sector and its value chain. Source: Dialogic (2023), The economic opportunities of the cyber security sector

11. Dialogic (2023), The economic opportunities of the cyber security sector. Can be found at: https://www.rijksoverheid.nl/documenten/rapporten/2023/04/06/de-economische-kansen-van-de-cybersecuritysector

Note that individual organisations can fulfil multiple roles. For example, a company can create cyber products and simultaneously act as an end user. In fact, virtually all organisations today can be considered end users as cyber security is important to virtually every organisation. However, cyber R&D, production and integration roles have been assigned to a more selective group of organisations. At the start of this research, it was estimated that the roles parties fulfil are also related to the type of cyber security expertise they are looking for.
Finally, there is also explicit attention for parties that require a relatively large amount of cyber security expertise on the job market (i.e. that advertise many vacancies in which cyber security expertise plays a role) versus parties that require relatively little cyber security expertise. The dynamics surrounding this theme are expected to differ between these organisations, and the expectation beforehand was that organisations that only act as a "cyber security end user" would also have less demand and a different demand.

4.3 Demand for cyber security professionals – general

4.3.1 Total

In 4.2 it is stated that cyber security expertise can be found on the job market in various ways. There are functions that could be classified as a "cyber security function", but there are also many functions in which cyber security is, to a greater or lesser extent, part of a broader range of tasks. An operational distinction has been made between these different manifestations for the analyses presented here. The job functions found in the vacancies are linked to one of the following four categories[12]:

- **ECSF**: these are job profiles that (largely) correspond to the job profiles stated in the ECSF. People who hold such a position are considered cyber security professionals.
- **Cyber Security – High**: these are job profiles that are primarily focused on cyber security, but are not directly linked to an ECSF profile. People who hold such a position are also considered cyber security professionals.
- **Cyber Security – Medium**: these are job profiles that have a broader scope than simply cyber security, but which do contain a substantial cyber security component. In this research we do not view people who hold such a position as (pure) cyber security professionals, but they must have (substantial) knowledge of cyber security.
- **Cyber Security – Low**: these are job profiles in which cyber security plays a role, but only in a marginal way. The people who hold such a position are not seen as cyber security professionals, but are involved with the topic in some way.

The number of vacancies requiring cyber security expertise has increased significantly in recent years, from approximately 8,000 in 2018 to approximately 19,000 in 2022. All of the four categories described are experiencing significant growth in demand, see Figure 13.

12. See appendix for further explanation of the methodological choices and justification

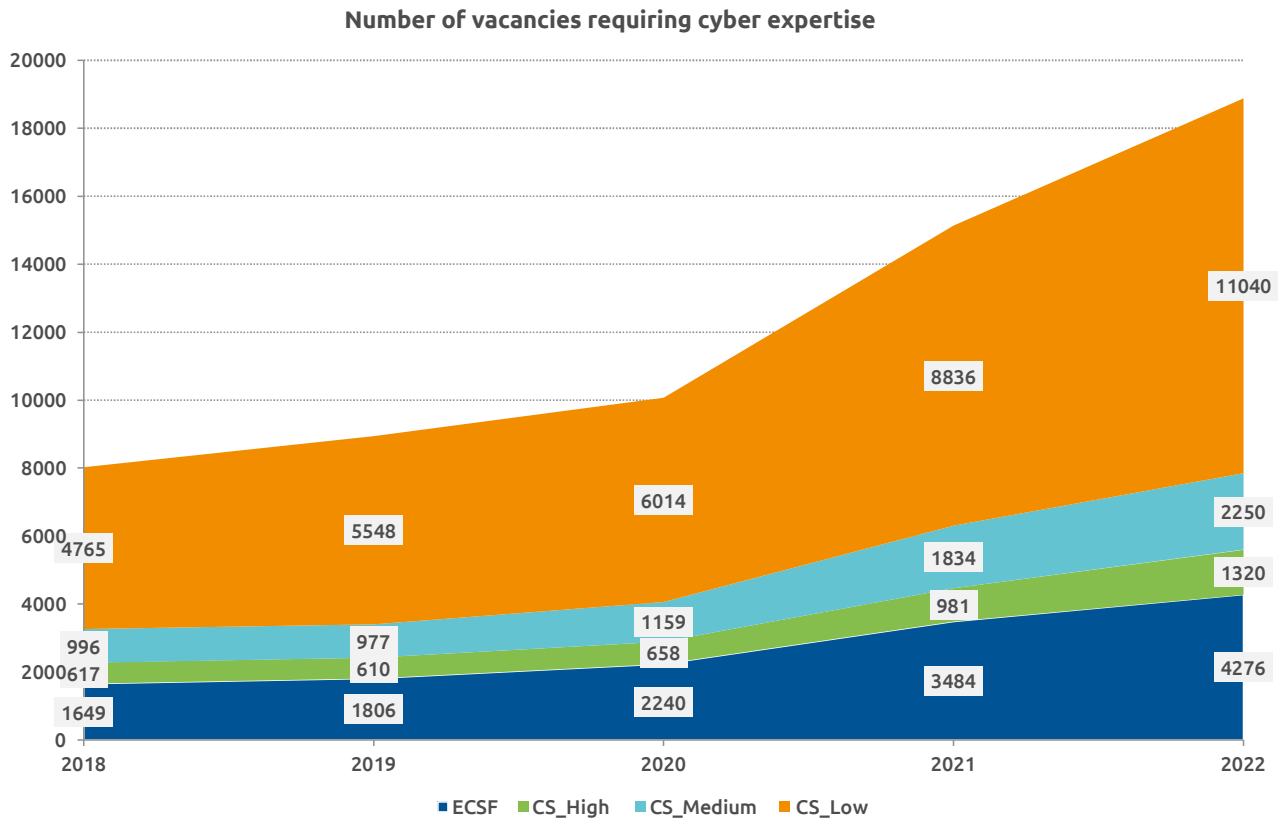


Figure 13: Number of vacancies requesting cyber security expertise. Source: Jobdigger, edited by Dialogic

The impact of using different definitions quickly becomes clear when making a distinction between different types of profiles. For example, Statistics Netherlands and pr-eDICT have taken a fairly similar approach to the concept of cyber security professional for most figures, resulting in approximately 4,000 vacancies in 2022. For the purposes of this research, a broader definition of cyber security was used, and we arrive at 4,200 – 18,900 vacancies depending on the chosen approach. We would not recommend counting the "Cyber Security – Low" category as cyber security professionals, but the category does illustrate how cyber security has a broad impact on the job market. After all, it is not only pure cyber security professionals who have to deal with it.
According to these figures, there will be ~5,600 vacancies for cyber security professionals in 2022 and another ~2,250 vacancies in which cyber security plays a substantial role (~7,850 in total).
According to the figures from "ICT in beeld" from the Employee Insurance Agency (UWV), there are 3.17 times more professionals active than the number of vacancies reported; on pr-eDICT, in the case of ICT professionals, there are 5.81 times more professionals active on the job market than the number of vacancies. If we were to use these key figures for cyber security professionals, the estimate for the total number of cyber security professionals on the job market is between 60,000-110,000 people based on this vacancy analysis (Figure 14).

	Low	**High**
	3,17	5,81

		CS professionals	
CS profile type	Vacancies	Low	High
ECSF	4276	13555	24844
CS – High	1320	4184	7669
CS – Medium	2250	7133	13073
CS – Low	11040	34997	64142
Total	**18886**	**59869**	**109728**

Figure 14: Estimated total number of cyber security professionals on the job market. Source: Jobdigger, edited by Dialogic

4.3.2 Region

The demand is not distributed evenly across the different provinces in the Netherlands. The majority of vacancies (71%) are focused in the Randstad: Noord-Holland, Zuid-Holland and Utrecht, see Figure 15. This applies to both the generic vacancies and the four separate categories.

	ECSF	CS_High	CS_Medium	CS_Low	Total
Noord-Holland	3683	1271	2095	9752	16801
Zuid-Holland	3357	1189	1790	9148	15484
Utrecht	2372	811	1549	6392	11124
Noord-Brabant	1510	337	685	3550	6082
Gelderland	1001	208	413	2313	3935
Overijssel	615	91	195	1921	2822
Limburg	334	104	163	1021	1622
Groningen	230	47	132	727	1136
Flevoland	123	30	66	392	611
Friesland	70	42	50	449	611
Drenthe	77	40	58	294	469
Zeeland	80	14	18	209	321
Unknown	3	3	2	35	43
Total	13455	4187	7216	36203	61061

Figure 15: Number of vacancies by region[13]. Source: Jobdigger, edited by Dialogic

4.3.3 Education level and work experience

Cyber vacancies largely require HBO or University education level. Of all vacancies, 91% require HBO or University education, and 98% of these are in fact in the "Cyber Security – high" category. This is consistent with the picture outlined in the interviews, which mainly concerns functions that require a high level of education.

In addition, several years of work experience are often required. As far as can be from the data, there seems to be a focus on 3+ years of work experience, see also Figure 16.

Total				
	University	HBO	MBO	Total
unknown	6665	25017	3918	**35600**
starter	260	955	191	**1406**
1-3	1048	4276	813	**6137**
3-5	1382	6466	543	**8391**
5-10	1682	6127	283	**8092**
>10	370	902	38	**1310**
Total	**11407**	**43743**	**5786**	**60936**
	19%	72%	9%	100%

ECSF				
	University	HBO	MBO	Total
unknown	1132	5813	422	**7367**
starter	31	191	14	**236**
1-3	198	906	73	**1177**
3-5	253	1895	99	**2247**
5-10	333	1803	46	**2182**
>10	46	196	2	**244**
Total	**1993**	**10804**	**656**	**13453**
	15%	80%	5%	100%

CS_High				
	University	HBO	MBO	Total
unknown	536	1794	49	**2379**
starter	22	92	2	**116**
1-3	118	300	13	**431**
3-5	158	473	8	**639**
5-10	143	357	8	**508**
>10	40	65	1	**106**
Total	**1017**	**3081**	**81**	**4179**
	24%	74%	2%	100%

13. The province in which the vacancy is posted has been deduced automatically. For some vacancies the province could not be deduced, so they are shown as unknown.

ECSF				
	University	HBO	MBO	Total
unknown	1132	5813	422	**7367**
starter	31	191	14	**236**
1-3	198	906	73	**1177**
3-5	253	1895	99	**2247**
5-10	333	1803	46	**2182**
>10	46	196	2	**244**
Total	**1993**	**10804**	**656**	**13453**
	15%	80%	5%	100%

CS_High				
	University	HBO	MBO	Total
unknown	536	1794	49	**2379**
starter	22	92	2	**116**
1-3	118	300	13	**431**
3-5	158	473	8	**639**
5-10	143	357	8	**508**
>10	40	65	1	**106**
Total	**1017**	**3081**	**81**	**4179**
	24%	74%	2%	100%

Figure 16: Number of vacancies by education level and work experience. Source: Jobdigger, edited by Dialogic

An estimate, based on the vacancy data, was also made of the type of position in terms of junior, intermediate or senior[14]. This shows, as far as is known, that approximately three quarters of the vacancies relate to intermediate and senior positions. Only a quarter relate to junior positions, which often require some work experience (Figure 17).

Total				
	University	HBO	MBO	Total
unknown	1847	8633	1793	**12273**
junior	2511	9244	1644	**13399**
intermedia	4446	17811	1533	**23790**
senior	2603	8055	816	**11474**
Total	**11407**	**43743**	**5786**	**60936**
	19%	72%	9%	100%

Figure 17: Vacancies at junior, intermediate and senior level. Source: Jobdigger, edited by Dialogic

There is often talk about "the mismatch between education and the job market". To take an honest look at the dynamics of the job market, we must talk about the possible mismatch between education and the job market for junior positions. With some exceptions, it is not realistic to move straight from college to an intermediate or senior position. It is realistic however to move from an education institution to a junior position.

Additionally, the above figures are broken down by year. They are shown in Supplementary Table 17 in Appendix 3. There will be 4,364 vacancies aimed at juniors in 2022. Of these, 1,256 are linked to a specialist cyber security profile (ECSF and "CS – High"), 537 to profiles with a substantial cyber security component ("CS – Medium") and 2,571 to profiles with a small cyber security component ("CS – Low"). When studying the link between regular education and the job market, it may be more logical to look at this question from the job market perspective. When looking at progression and development in the job market, refresher training, further training and Life-Long Learning, it is particularly useful to also look at intermediate and senior positions. Note that the numbers for junior, intermediate and senior positions will be underestimates as there is still a group of "unknowns" who in practice must fall into one of these categories.

4.3.4 Sector

Top 10 sectors with cyber vacancies. Source: Jobdigger, edited by Dialogic

#	SBI-2	Sector_name	2018	2019	2020	2021	2022	Total
1	84	Public administration, government services and compulsory social security	857	1152	1503	1743	2570	7825
2	62	Activities for the provision of ICT-based services	927	1054	1409	1541	2196	7127
3	69	Legal services, accountancy, tax advice and administration	550	621	544	1240	1658	4613
4	70	Holdings (non-financial), group services within own group and management consultancy	795	792	593	973	1079	4232
5	46	Wholesale and trade mediation (not including cars and motorcycles)	425	490	732	1337	805	3789
6	64	Financial institutions (excluding insurance and pension funds)	489	628	513	776	1040	3446
7	85	Education	344	351	385	572	716	2368
8	80	Security and detection	197	327	372	524	463	1883
9	86	Healthcare	312	318	285	461	475	1851
10	78	Employment agencies, temporary employment agencies and personnel management	95	121	211	613	603	1643

Figure 18: Top 10 sectors with cyber vacancies. Source: Jobdigger, edited by Dialogic

14. This is a label assigned by data supplier Jobdigger based on the available information.

Distinguishing between the share of cyber security in the profile and the associated four categories, it is noticeable that the IT sector stands out when it comes to the specific demand for ECSF profiles (Figure 19).

#	SBI-2	Sector_name	ECSF	CS_High	CS_Medium	CS_Low	Total
1	84	Public administration, government services and compulsory social security	1178	845	1082	4720	7825
2	62	Activities for the provision of ICT-based services	1895	308	788	4136	7127
3	69	Legal services, accountancy, tax advice and administration	792	645	797	2379	4613
4	70	Holdings (non-financial), group services within own group and management consultancy	776	412	583	2461	4232
5	46	Wholesale and trade mediation (not including cars and motorcycles)	717	208	352	2512	3789
6	64	Financial institutions (excluding insurance and pension funds)	913	163	419	1951	3446
7	85	Education	493	201	234	1440	2368
8	80	Security and detection	354	168	312	1049	1883
9	86	Healthcare	371	133	199	1148	1851
10	78	Employment agencies, temporary employment agencies and personnel management	204	70	125	1244	1643

Figure 19: Top 10 sectors with cyber vacancies, broken down by category. Source: Jobdigger, edited by Dialogic

4.3.5 Organisations

The vacancy data identified approximately 6,200 organisations in the Netherlands that posted at least one cyber vacancy during the period 2018-2022. The Top 100 organisations account for 42% of the vacancies, which means the job market for cyber security professionals has been quite concentrated in recent years. Figure 20[15] shows the top 50.

15. When creating this figure, the name of the organisation that posted the vacancy was aggregated. This means both the Ministry of Defence and the Central Government appear in the table.

#	Organisation	2018	2019	2020	2021	2022	Total CS vacancies	2019-2022
1	Police	119	425	484	314	717	2059	48%
2	PWC	105	88	87	355	623	1258	616%
3	CGI	9	146	250	267	530	1202	112%
4	EY	63	125	99	329	476	1092	381%
5	The Tax Authorities	47	134	197	238	319	935	62%
6	ING	119	174	126	195	244	858	94%
7	ABN AMRO	141	113	120	164	232	770	93%
8	Capgemini	77	62	49	223	166	577	239%
9	KPMG	77	94	56	115	234	576	318%
10	Ministry of Defence	91	28	158	103	182	562	15%
11	Philips	11	13	149	149	143	465	-4%
12	Rohde & Schwarz Benelux			50	396		446	-100%
13	Rabobank	52	99	70	79	134	434	91%
14	Fox-IT	74	112	57	141	12	396	-79%
15	Employee Insurance Agency (UWV)	37	46	55	97	151	386	175%
16	Atos			24	47	314	385	1208%
17	Alliander	85	41	47	85	113	371	140%
18	ASML	43	44	81	81	105	354	30%
19	Stichting Cyber Security Academy The Hague	152	89	38	32	37	348	-3%
20	Thales Group	80	37	107	88	35	347	-67%
21	Macee	63	184	68	21	1	337	-99%
22	The Water Authority	39	45	55	81	105	325	91%
23	Irdeto	11	15	47	127	119	319	153%
24	Sogeti Nederland	49	123	56	15	52	295	-7%
25	De Nederlandsche Bank	44	58	45	71	76	294	69%
26	Thales Nederland	116	30	108	17	15	286	-86%
27	Accenture	39	11	17	99	119	285	600%
28	Dutch government	48	45	1	62	125	281	12400%
29	TNO	55	25	25	82	91	278	264%
30	PwC Accountants	89	152	15			256	-100%
31	Deloitte Legal	48		103	103	1	255	-99%
32	Secura	31	19	72	83	46	251	-36%
33	NS	15	22	39	48	123	247	215%
34	Kader Group			1	62	170	233	16900%
35	Levy				75	151	226	
36	Amsterdam municipality	29	28	61	55	46	219	-25%
37	The Public Prosecution Service	36	33	25	47	72	213	188%
38	Modis		1	30	173	9	213	-70%
39	Deloitte	72	16	30	66	25	209	-17%
40	the Volksbank	26	29	39	57	53	204	36%
41	Witteveen+Bos Consulting engineers	52	45	40	29	34	200	-15%
42	SAP Nederland	7		29	153	3	192	-90%
43	PLUSIT			7	91	93	191	1229%
44	DHL		29	33	41	81	184	145%
45	Mazars	5	33	18	31	94	181	422%
46	KPN	22	96	26	15	18	177	-31%
47	TM Software Europe	57	21	35	32	17	162	-51%
48	Orange Cyberdefence			51	56	50	157	-2%
49	Northwave	6	12	35	64	36	153	3%
50	Centric	32	17	41	37	25	152	-39%

Figure 20: Top 50 organisations – number of cyber vacancies. Source: Jobdigger, edited by Dialogic

This top 50 includes government (e.g. Police, Tax Authorities, Ministry of Defence and Central Government), the business community (e.g. PWC, CGI, Fox-IT, ING and ASML) and a knowledge institution (TNO). Despite all having a high demand for cyber security expertise, the type of profile sought may differ, see Figure 21.

#	Organisation	ECSF	CS_High	CS_Medium	CS_Low	Total CS vacancies
1	Police	291	228	369	1171	2059
2	PWC	190	208	266	594	1258
3	CGI	359	50	26	767	1202
4	EY	152	160	181	599	1092
5	The Tax Authorities	149	52	118	616	935
6	ING	221	45	115	477	858
7	ABN AMRO	219	21	89	441	770
8	Capgemini	116	102	91	268	577
9	KPMG	93	90	70	323	576
10	Ministry of Defence	55	86	72	349	562
11	Philips	135	50	71	209	465
12	Rohde & Schwarz Benelux	24	1	34	387	446
13	Rabobank	105	22	62	245	434
14	Fox-IT	88	74	73	161	396
15	Employee Insurance Agency (UWV)	53	11	32	290	386
16	Atos	46	5	25	309	385
17	Alliander	132	15	44	180	371
18	ASML	171	9	32	142	354
19	Stichting Cyber Security Academy The Hague	123	43	55	127	348
20	Thales Group	87	5	21	234	347
21	Macee	80	16	29	212	337
22	The Water Authority	34	22	50	219	325
23	Irdeto	37	6	37	239	319
24	Sogeti Nederland	51	30	29	185	295
25	De Nederlandsche Bank	76	11	26	181	294
26	Thales Nederland	73	11	27	175	286
27	Accenture	95	41	45	104	285
28	Dutch government	58	70	48	105	281
29	TNO	98	20	67	93	278
30	PwC Accountants	30	26	31	169	256
31	Deloitte Legal	26	49	38	142	255
32	Secura	114	8	45	84	251
33	NS	88	13	11	135	247
34	Kader Group	10	6	5	212	233
35	Levy	39	2	9	176	226
36	Amsterdam municipality	46	4	27	142	219
37	The Public Prosecution Service	7	15	24	167	213
38	Modis	2		2	209	213
39	Deloitte	39	30	43	97	209
40	the Volksbank	54	13	34	103	204
41	Witteveen+Bos Consulting engineers	9	18	3	170	200
42	SAP Nederland	67	7	27	91	192
43	PLUSIT	46	15	16	114	191
44	DHL	10		2	172	184
45	Mazars	135		2	44	181
46	KPN	65	6	17	89	177
47	TM Software Europe	59	17	33	53	162
48	Orange Cyberdefence	46	47	31	33	157
49	Northwave	40	8	49	56	153
50	Centric	52	16	41	43	152

Figure 21: Top 50 organisations – number of cyber vacancies by category. Source: Jobdigger, edited by Dialogic

These results show that the emphasis differs greatly between organisations. For example, CGI and ASML have a relatively high demand for ECSF profiles, while the Employee Insurance Agency (UWV) and Atos include cyber security in the periphery of the broader functions.

4.3.6 Target groups

As described in 4.2.2, we are also interested in those who have a demand for cyber security expertise. To this end, we can look at the roles within the cyber security value chain and check whether the party belongs to the government, the business community or educational/knowledge institutions. The Top 100 organisations were examined and an estimation of the category to which they (primarily) belong was made. This roughly provides the following picture (Figure 22):

Based on Top 100 organisations

Category	ECSF	CS_High	CS_Medium	CS_Low	Total
Cyber R&D (n=4)	198	32	83	252	565
Cyber production (n=31)	1833	1074	1384	4535	8826
Cyber integration (n=50)	2954	635	1299	7246	12134
Business lives (n=71)	4199	1438	2259	10063	17959
Government (n=22)	1229	612	926	4134	6901
Education/KI (n=5)	229	33	94	302	658
Government (n=2)	156	45	55	171	427
Cyber end-use (everyone)	6174	2206	3462	15325	27167

Figure 22: Number of vacancies by target group based on the Top 100 organisations. Source: Jobdigger, edited by Dialogic

Based on primary focus, the cyber R&D category appears to be by far the smallest. This is also in line with the previous research "The economic opportunities of the cyber security sector". These numbers may be an underestimation as there may be several organisations that play some (small) part in cyber R&D, but in any case this seems to be the smallest category. In the Top 100 we see many parties (also) being active as cyber producers or cyber integrators. Almost 80% of the ECSF profiles in this population are requested by parties that are (also) active as producers or integrators. This is consistent with the picture that emerges from the research interviews: most demand for pure cyber security profiles is limited to end users only (with the exception of the CISO function).

Another way to compare the organisations within the data is to look at how many cyber security vacancies that organisations have posted, see Figure 23. This also shows that organisations that do more with cyber security relatively also have a greater demand for specialist profiles. And vice versa: organisations that post relatively few cyber security vacancies often ask for people with a broader/different profile, for which cyber security is only a part. Only 22% of the vacancies from organisations with <=3 cyber security vacancies relate to ECSF profiles or job profiles with a large share of cyber security.

Number of vacancies in the organisation	Total	ECSF	CS_High	CS_Medium	CS_Low
>50	30751	6817	2491	3952	17491
11-50	14727	3279	940	1732	8776
4-10	8146	1883	407	804	5052
<=3	6209	1115	270	600	4224
Unknown	1228	361	79	128	660
Total	**61061**	**13455**	**4187**	**7216**	**36203**

Number of vacancies in the organisation	Total	ECSF	CS_High	CS_Medium	CS_Low
>50	100%	22%	8%	13%	57%
11-50	100%	22%	6%	12%	60%
4-10	100%	23%	5%	10%	62%
<=3	100%	18%	4%	10%	68%
Unknown	100%	29%	6%	10%	54%
Total	**100%**	**22%**	**7%**	**12%**	**59%**

Figure 23: Demand for cyber security profile types and the number of cyber security vacancies that organisations post. Source: Jobdigger, edited by Dialogic

4.4 Demand for specific job profiles

In 4.3 the general demand for cyber security expertise is described. This section takes a closer look at specific job profiles that are in demand.

4.4.1 Total

Research was conducted within the vacancies to determine where cyber expertise is required. Job titles, as used by Jobdigger, are then linked to the four category types (ECSF, High, Medium, Low). The link to ECSF profiles was made by linking the mentioned job titles in the vacancy data to an ECSF profile, if applicable. The labels used by Jobdigger have been left intact for those job title labels belonging to the "CS – High", "CS – Medium" and "CS – Low" categories. This leads to the most requested job profiles/titles, as shown in Figure 24.

Based on these results we see the following:

- The (C)ISO and the Cyber Security Implementer are by far the most requested profiles within the ECSF profiles.
- A lot of cyber security consultants/advisors, privacy experts and cyber security managers can be seen within the "CS – High" category.
- A lot of consultants/advisors and managers who cover a broader field in addition to cyber security (often IT in the broad sense) can be seen within the "CS – Medium" category.
- Technical ICT-oriented professions of which cyber security represents a (small) share can be mainly seen within the "CS – Low" category.

#	ECSF profile	Number of vacancies
1	ECSF – CISO	3649
2	ECSF – Cyber Security Implementer	3619
3	ECSF – Cyber Threat Intelligence Specialist	1626
4	ECSF – Cyber Security Architect	1382
5	ECSF – Cyber Security Risk Manager	823
6	ECSF – Cyber Security Auditor	557
7	ECSF – Penetration Tester	520
8	ECSF – Cyber Security Researcher	489
9	ECSF – Cyber Legal, Policy & Compliance Officer	275
10	ECSF – Cyber Incident Responder	246
11	ECSF – Digital Forensics Investigator	154
12	ECSF – Cyber Security Educator	115
	Total	13455

#	Job title – CS-high	Number of vacancies
1	Cyber Security Consultant	301
2	Officer (data protection)	296
3	Information Security Advisor	254
4	Cyber Security Consultant	99
5	Information Security Consultant	58
6	Business Consultant Security	55
7	Researcher	47
8	Information Security & Privacy Advisor	39
9	Manager Cyber Security	37
10	Cyber Security Advisor	36
11	Privacy Manager	34
12	Privacy & Information Security Advisor	34
13	Security Advisor	32
14	Cyber Security	31
15	Cyber Security Expert	30
16	Traineeship Cyber Security	29
17	Information Security Coordinator	28
18	Identity & Management Architect	27
19	Public Private Partnership Account Manager	26
20	Cyber Security Project Manager	24
	Other	2670
	Total	4187

#	Job Title – CS Agent	Number of vacancies
1	Privacy Officer	467
2	Security Consultant	329
3	Consultant	298
4	Advisor	216
5	Manager	160
6	Analyst	131
7	Privacy Consultant	124
8	Digital Specialist	119
9	Security Manager	103
10	Security Talent	89
11	Business Development Manager	75
12	Risk Manager	72
13	Traineeship	69
14	Web developer	69
15	IT Security Manager	69
16	Privacy Advisor	67
17	IT Risk Manager	67
18	Cloud Security Consultant	67
19	Sales Manager	66
20	Privacy Lawyer	62
	Other	4497
	Total	7216

#	Job Title – CS-low	Number of vacancies
1	System Administrator	449
2	Auditor	358
3	Functional Manager	248
4	Account Manager	226
5	Project manager	213
6	Courier	198
7	Software Engineer	190
8	Information manager	188
9	Network administrator	167
10	Engineer	166
11	Developer	158
12	Architect	149
13	Data Engineer	147
14	Traineeship Information Management Governme	146
15	Product Owner	142
16	Business Analyst	135
17	Compliance Officer	127
18	Project Leader	123
19	Software Developer	113
20	Technical Application Manager	108
	Other	32452
	Total	36203

Figure 24: Most requested job titles by category. Source: Jobdigger, edited by Dialogic

4.4.2 Region

In 4.3.2 the regional distribution of cyber security vacancies is shown: a large proportion of the vacancies are posted in the Randstad. The three provinces of Noord-Holland, Zuid-Holland and Utrecht also appear to be relatively more specialised in terms of cyber security. This picture is reflected in the job profiles in demand in the region. **The Top 20 job profiles of the top provinces also contain more cyber security specialist functions** (ECSF and "Cyber Security – High") than the provinces where fewer cyber security vacancies have been advertised, see Supplementary Table 18 in Appendix 3.

4.4.3 Education level and work experience

The demand, linked to work experience and education level, was also examined by job profile. The Top 20 requested job profiles were printed out for each combination of MBO, HBO and University on the one hand, and junior, intermediate and senior on the other. This corresponds to (3 x 3 =) 9 combinations/tables. Details of the job profiles per combination of requested education level and work experience are included in Supplementary Table 19 in Appendix 3.

The tables clearly show that, in general, different types of professionals are required based on the education levels. We see relatively many job profiles with a low cyber security content at the MBO level, while there are many job profiles with an IT character for which cyber security is a component. In addition, the ECSF profiles for which an MBO education level is sometimes required are mainly technical in nature. This picture is also in line with the overall findings; MBO graduates often have a specific technical focus.

The functions at HBO and University level are relatively comparable. There are some differences to be found. The researcher profile is therefore something for which (logically) a university education is primarily required.

An important finding is that the ECSF profiles offer sufficient opportunities to start as a junior. A junior will not start working as a senior supervisor immediately, but will be able to take on parts of the CISO package, after which they will develop as an ISO (with a specific range of tasks) into a "full" CISO. There also seem to be opportunities for growth in profiles such as Implementer, where it is possible to take on a specific role at the start and learn more and more through experience at work.

4.4.4 Sector

The cyber security profiles in demand on the job market are also related to the sectors in which the organisations operate. After all, the goals, tasks and activities of organisations create the need for certain knowledge and expertise among people in order to be able to properly perform the required tasks. To illustrate how different sectors require different profiles, the Top 20 job profiles for the four sectors in which demand for cyber security expertise is greatest are shown below (Figure 25).

Certain profiles are in high demand in all these sectors, such as the ECSF profiles CISO, Cyber Threat Intelligence Specialist, Cyber Security Implementer, Cyber Security Risk Manager and Cyber Security Architect. Other profiles are particularly sought after in certain sectors; a Pen-tester is particularly sought after in IT and business services, while Privacy Officers are particularly sought after within government.

#1. 84 – Public administration, government services and social care.

#	Job profile	Type	Number of vacancies
1	ECSF – CISO	ECSF	460
2	ECSF – Cyber Threat Intelligence Specialist	ECSF	222
3	ECSF – Cyber Security Implementer	ECSF	142
4	ECSF – Cyber Security Risk Manager	ECSF	127
5	Privacy Officer	CS_Mediun	125
6	Digital Specialist	CS_Mediun	119
7	ECSF – Cyber Security Architect	ECSF	108
8	Officer	CS_High	85
9	Functional Manager	CS_Low	71
10	ECSF – Cyber Security Auditor	ECSF	66
11	Information Security Advisor	CS_High	62
12	Information manager	CS_Low	55
13	Advisor	CS_Mediun	55
14	Auditor	CS_Low	40
15	System Administrator	CS_Low	35
16	Privacy Advisor	CS_Mediun	34
17	Officer	CS_Low	32
18	Lawyer	CS_Low	32
19	Information Advisor	CS_Low	32
20	ICT Manager	CS_Low	32

#2. 62 – IT service activities

#	Job profile	Type	Number of vacancies
1	ECSF – Cyber Security Implementer	ECSF	682
2	ECSF – CISO	ECSF	425
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	242
4	ECSF – Cyber Security Architect	ECSF	174
5	ECSF – Penetration Tester	ECSF	174
6	Security Consultant	CS_Medium	132
7	ECSF – Cyber Security Risk Manager	ECSF	110
8	Cyber Security Consultant	CS_High	74
9	Account Manager	CS_Low	67
10	Consultant	CS_Medium	58
11	System Administrator	CS_Low	52
12	Technical Application Manager	CS_Low	45
13	PHP Developer	CS_Low	35
14	Service desk Employee	CS_Low	33
15	Access Management Consultant	CS_Low	33
16	Project manager	CS_Low	32
17	Engineer	CS_Low	32
18	Developer	CS_Low	31
19	Cloud Consultant	CS_Low	30
20	Backend Developer	CS_Low	30

#3. 69 – Legal services, accountancy, tax advice and administration

#	Job profile	Type	Number of vacancies
1	ECSF – Cyber Security Auditor	ECSF	199
2	ECSF – Cyber Threat Intelligence Specialist	ECSF	128
3	ECSF – Cyber Security Implementer	ECSF	88
4	ECSF – CISO	ECSF	87
5	ECSF – Penetration Tester	ECSF	78
6	Auditor	CS_Low	76
7	ECSF – Cyber Security Architect	ECSF	70
8	Cyber Security Consultant	CS_High	69
9	ECSF – Digital Forensics Investigator	ECSF	65
10	Consultant	CS_Mediun	59
11	Sales & Marketing Intern	CS_Low	52
12	Manager	CS_Mediun	43
13	Cyber Security Consultant	CS_High	38
14	ECSF – Cyber Incident Responder	ECSF	37
15	Business Management Consultant	CS_Mediun	37
16	Actuarial & Quantitative Consultant	CS_Low	31
17	Associate	CS_Low	31
18	Work student & Quantitative Consulting	CS_Low	30
19	Advisor	CS_Mediun	29
20	Actuarial & Consulting Student Assistant	CS_Low	27

70 – Holdings (not finance), group services internal and management adv

#	Job profile	Type	Number of vacancies
1	ECSF – Cyber Security Implementer	ECSF	184
2	ECSF – CISO	ECSF	150
3	ECSF – Cyber Security Architect	ECSF	133
4	ECSF – Cyber Threat Intelligence Specialist	ECSF	105
5	Information Security Advisor	CS_High	58
6	Web developer	CS_Medium	55
7	Advisor	CS_Medium	55
8	ECSF – Cyber Security Risk Manager	ECSF	54
9	Cyber Security Consultant	CS_High	52
10	ECSF – Cyber Security Auditor	ECSF	44
11	System Administrator	CS_Low	39
12	Consultant	CS_Medium	39
13	Privacy Consultant	CS_Medium	37
14	Consultant IT Assurance	CS_Low	36
15	Consultant IT Assurance	CS_Low	35
16	Cloud Security Consultant	CS_Medium	32
17	Cyber Security Consultant	CS_High	31
18	ECSF - Cyber LPC Officer	ECSF	29
19	ECSF – Cyber Incident Responder	ECSF	29
20	Security Consultant	CS_Medium	28

Figure 25: Top 20 job profiles per sector. Source: Jobdigger, edited by Dialogic

4.4.5 Organisations

The aggregated figures on the cyber security job market are in a sense abstract; they include "totals", entire sectors, and vacancies at a certain education level. In reality, these are aggregates of all the individual manifestations of the need for cyber security expertise. These are individual organisations that, in individual cases, require people who can perform certain tasks and bring with them certain knowledge and skills. These underlying actual case studies in practice become clearer when we zoom in on individual organisations.

Figure 26 shows the job profiles (with a cyber component) requested by the four organisations with high demand for cyber security expertise (Police, CGI, Tax Authorities and ABN AMRO) on the job market. Although a number of generic ECSF profiles are requested by all, it quickly becomes apparent that different organisations require different job profiles. The police are in need of investigators, team leads and generalists for tactical investigation. The demand for IT professionals at CGI with some cyber security expertise can also be seen. For an organisation such as the Tax Authorities, profiles such as financial investigator and tax investigator also emerge. Company-specific profiles at ABN AMRO such as the ABN IT Talent Programme and Global IT Talent programme, are emerging, as well as functions such as the Transaction Monitoring Specialist.

Police

#	Job profile	Type	Number
1	Digital Specialist	CS_Mediun	119
2	ECSF – Cyber Threat Intelligence Specialist	ECSF	112
3	ECSF – Cyber Security Implementer	ECSF	59
4	ECSF – Cyber Security Architect	ECSF	54
5	ECSF – Cyber Security Risk Manager	ECSF	40
6	Public Private Partnership Account Manager	CS_High	26
7	Investigator	CS_Low	20
8	Developer	CS_Low	19
9	Team leader	CS_Low	17
10	Analyst	CS_Mediun	17
11	General Tactical Investigation	CS_Mediun	17
12	Operational Specialist	CS_Low	16
13	Delivery Manager Oracle Linux	CS_Low	15
14	Intake & Service Employee	CS_Low	14
15	User support	CS_Low	14
16	Specialist Open Source Intelligence	CS_Low	13
17	Tester	CS_Low	13
18	Financial Investigator	CS_Mediun	13
19	Privacy Advisor	CS_Mediun	13
20	Digital Cybercrime Coordinator	CS_High	13

CGI

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	163
2	ECSF – Cyber Security Architect	ECSF	59
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	44
4	ECSF – CISO	ECSF	42
5	Technical Application Manager	CS_Low	38
6	ECSF – Cyber Security Risk Manager	ECSF	37
7	Cyber Security Consultant	CS_High	27
8	Test automation engineer	CS_Low	26
9	Outsystems Developer	CS_Low	24
10	Java Software Engineer	CS_Low	22
11	Business Information Analyst	CS_Low	21
12	Director Consulting Service	CS_Low	19
13	Experienced Java Software Engineer	CS_Low	18
14	Filenet Consultant	CS_Low	16
15	Oracle Database Administrator DBA	CS_Low	15
16	Digital Workplace Engineer	CS_Low	13
17	Engineer	CS_Low	12
18	Project manager	CS_Low	12
19	MES Service Engineer	CS_Low	12
20	MES Business Consultant	CS_Low	12

The Tax Authorities

#	Job profile	Type	Number
1	ECSF – Cyber Security Auditor	ECSF	46
2	ECSF – Cyber Security Implementer	ECSF	35
3	ECSF – CISO	ECSF	22
4	Information Security Advisor	CS_High	19
5	ECSF – Cyber Threat Intelligence Specialist	ECSF	17
6	ECSF – Cyber Security Risk Manager	ECSF	17
7	Analyst	CS_Mediun	12
8	Financial Investigator	CS_Mediun	12
9	Forensic IT Investigator	CS_Low	11
10	Tax Investigator	CS_Low	11
11	Tactical Investigator	CS_Mediun	10
12	Team Leader	CS_Low	9
13	Investigator	CS_Low	9
14	Business advisor	CS_Low	9
15	Information Management Advisor	CS_Low	8
16	Business advisor	CS_Mediun	8
17	Integrated Security Advisor	CS_Mediun	8
18	Advisor	CS_Mediun	8
19	Audit Traineeship	CS_Low	8
20	Privacy & Data Coordinator	CS_Mediun	7

ABN AMRO

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	82
2	ECSF – CISO	ECSF	68
3	ECSF – Cyber Security Auditor	ECSF	31
4	ECSF – Cyber Threat Intelligence Specialist	ECSF	22
5	ABN IT Talent Programme	CS_Low	17
6	Compliance Advisor	CS_Low	16
7	Global IT Talent Programme	CS_Low	10
8	ECSF – Cyber Security Architect	ECSF	10
9	Artificial Intelligence Translator	CS_Low	10
10	Analyst	CS_Mediur	10
11	IT Project Manager	CS_Low	9
12	Business Architect	CS_Low	9
13	Model Innovation & Project	CS_Low	9
14	Transaction Monitoring Specialist	CS_Low	8
15	Security Case Developer Application	CS_Low	8
16	Career guide	CS_Mediur	7
17	Administrative Clerk	CS_Low	7
18	ABN AMRO	CS_Mediur	7
19	Business Process Expert Security	CS_High	7
20	Innovation & projects Model Validator	CS_Low	7

Figure 26: Four organisations and their Top 20 profiles. Source: Jobdigger, edited by Dialogic

4.4.6 Target groups

The different target groups, as addressed in 4.2.2., have different dynamics, which is also reflected in the demand for different job profiles. The Top 100 organisations were examined and a (rough) estimate made of which target group they (primarily) fall into. This is shown in Supplementary Table 20 in Appendix 3.

Not surprisingly, there is a relatively high demand for researchers within “cyber R&D”. There appears to be a high demand for specialist cyber security profiles within the cyber security sector itself (producers of cyber security goods/ services) and integrators, including highly technical profiles.

As mentioned earlier, the parties that do a relatively large amount of cyber security work and have a high demand for cyber security professionals are also the parties that request specialist profiles relatively often. These results support that picture.

4.5 Demand for specific tasks, knowledge and skills

This section explores the concept of cyber security expertise at a deeper level. The step is now made from job profile level to individual tasks, knowledge and skills. These "building blocks" form the basis for what the cyber security professional must know, be able to do and then, actually do. See also 4.2.1 for further explanation. See Appendix 1 for a methodological justification.

4.5.1 Total

The ECSF profiles consist of a number of components, including deliverables, main tasks, key skills and key knowledge. Certain building blocks can be explicitly found in many vacancies. Of course, not every vacancy has an equal level of detail, and sometimes the language cannot (easily) be recognised automatically, but it is possible to analyse in general how often certain building blocks occur. Individual building blocks of cyber security knowledge and cyber security skills (Figure 27) can be found in 79-85% of the vacancies.

Type of building block	Number of vacancies	% vacancies
Deliverable	33006	54%
Key knowledge	51966	85%
Key skills	48279	79%
Main tasks	40783	67%

Figure 27: Overview of the building blocks discovered. Source: Jobdigger, edited by Dialogic

The analysis uncovered the Top 20 per type of building block. Figure 28 shows the Top 20 **tasks**. It can be seen immediately that the top 3 consists of tasks related to the "Management & Organisation" category. This involves developing and maintaining collaborative relationships with both external and internal stakeholders. Other tasks often explicitly identified working within legal frameworks, proposing new cyber security processes & procedures, and assessing and dealing with cyber security risks.

The results also show (again) that cyber security is anything but a purely "technical" domain, a view that is sometimes held within the Netherlands. There is certainly a need for the performance of technically-oriented tasks, but the main thrust of a large part of the associated tasks lies in management and organisation, legislation and regulations, and research/analysis.

#	Main task(s)	Category	% vacancies	Number of vacancies
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	40,7%	24860
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36,7%	22439
3	Collaborate with other teams and colleagues	Man. & Org.	31,4%	19178
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	25,1%	15331
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	3,2%	1933
6	Enforce and advocate organisation's data privacy and protection program	Legal	3,1%	1870
7	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1,8%	1112
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1,6%	997
9	Deploy penetration testing tools and penetration test programs	Technical	1,6%	952
10	Design and propose a secure architecture to implement the organisation's strategy	Technical	1,4%	863
11	Manage legal aspects of information security responsibilities and third-party relations	Legal	1,3%	776
12	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	1,3%	776
13	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	1,1%	700
14	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1,1%	657
15	Assist in designing, implementing, auditing and compliance testing activities in order to ensure cyber security and privacy compliance	Man. & Org.	0,7%	439
16	Conduct research, innovation and development work in cyber security-related topics	Research	0,6%	357
17	Identify, analyse and assess technical and organisational cyber security vulnerabilities	Research	0,5%	333
18	Identify and document compliance gaps	Research	0,5%	309
19	Ensure compliance with and provide legal advice and guidance about data privacy and data protection standards, laws and regulations	Legal	0,5%	294
20	Contribute to the development of the organisation's cyber security strategy, policy and procedures	Man. & Org.	0,5%	285

Figure 28: Top 20 "Main tasks" discovered. Source: Jobdigger, edited by Dialogic

Looking at the **skills** required, a largely similar picture emerges. Many non-technical skills are required for communication, management and organisation. At the same time, many technical skills can be seen in the Top 20 (Figure 29). The fact that tasks and skills do not have a 1 to 1 relationship is not surprising; after all, multiple skills may be required to perform a certain task, and multiple tasks may be performed based on the same skill. In technical terms, this suggests a "many-to-many relationship" (m:m).

#	Key skill(s)	Category	% vacancies	Number of vacancies
1	Motivate and encourage people	Man. & Org.	44,0%	26863
2	Identify, analyse and correlate cyber security events	Research	41,9%	25562
3	Collaborate with other team members and colleagues	Man. & Org.	31,4%	19182
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	31,2%	19074
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	9,9%	6016
6	Develop codes, scripts and programs	Technical	5,9%	3619
7	Develop code, scripts and programs	Technical	5,9%	3619
8	Think creatively and outside the box	Research	4,1%	2484
9	Identify and select appropriate pedagogical approaches for the intended audience	Research	2,6%	1577
10	Work under pressure	Man. & Org.	2,3%	1383
11	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	2,0%	1240
12	Conduct ethical hacking	Technical	2,0%	1225
13	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	1,9%	1132
14	Identify and exploit vulnerabilities	Technical	1,8%	1100
15	Assess the security and performance of solutions	Technical	1,6%	984
16	Design systems and architectures based on security and privacy by design and by defaults cyber security principles	Technical	1,4%	861
17	Perform social engineering	Technical	1,3%	818
18	Review codes assess their security	Technical	1,3%	788
19	Conduct technical analysis and reporting	Technical	1,2%	731
20	Carry out working-life practices of the data protection and privacy issues involved in the implementation of the organisational processes, finance and business strategy	Legal	0,7%	456

Figure 29: Top 20 "Key Skills" discovered. Source: Jobdigger, edited by Dialogic

Finally, there are many technical **knowledge elements** in the Top 20 knowledge subjects (Figure 30). There are also other knowledge subjects, such as knowledge of management practices and certain procedures, but the technical component seems to predominate in terms of knowledge. These findings together broadly suggest that working in cyber security requires a substantial knowledge base, but that many tasks performed by cyber security professionals are not necessarily (solely) technical in nature. It underlines the multi-disciplinary nature of cyber security, as well as the importance of "technical" knowledge. This finding in relation to different types of cyber security profiles will be looked at more closely later in this paragraph.

#	Key knowledge	Category	% vacancies	Number of vacancies
1	Cyber security standards, methodologies and frameworks	Technical	45,8%	27983
2	Cyber security controls and solutions	Technical	43,1%	26336
3	Cyber threats	Technical	35,9%	21906
4	Cyber security related laws, regulations and legislations	Legal	34,7%	21199
5	Management practices	Man. & Org.	30,3%	18481
6	Cyber security procedures	Man. & Org.	30,0%	18296
7	Cyber security risks	Technical	28,2%	17243
8	Cyber security recommendations and best practices	Man. & Org.	26,5%	16151
9	Cyber security policies	Man. & Org.	21,6%	13167
10	Cyber security-related technologies	Technical	13,9%	8458
11	Multi-disciplinary aspect of cyber security	Man. & Org.	10,4%	6356
12	Secure Operation Centres (SOCs) operation	Technical	6,8%	4134
13	Cyber security-related research, development and innovation (RDI)	Research	5,8%	3554
14	Auditing-related certification	Technical	5,7%	3476
15	Risk management standards, methodologies and frameworks	Man. & Org.	4,7%	2859
16	Penetration testing procedures	Technical	4,1%	2478
17	Cyber security attack procedures	Technical	3,5%	2122
18	Computer networks security	Technical	2,8%	1699
19	Operating networks security	Technical	2,7%	1658
20	Computer programming	Technical	2,7%	1658

Figure 30: Top 20 "Key knowledge" discovered. Source: Jobdigger, edited by Dialogic

Looking at the demand for different "types of building blocks" over time, it can be seen that the demand for these building blocks increases in absolute terms across the board, but that the relative ratio remains virtually the same over time (Figure 31). The field therefore "does not appear to be changing in terms of composition". Approximately one third of the building blocks relate to the "Management & Organisation" category, approximately 30% to technology, approximately 20% to legislation & regulations and approximately 20% to research.

Number of vacancies with type of building block	2018	2019	2020	2021	2022	Total
Legal	4.151	4.472	4.976	7.677	10.328	**31.604**
Management & Organisation	6.891	7.702	8.631	13.506	16.728	**53.458**
Education	304	261	344	624	807	**2.340**
Research	3.986	4.380	5.021	8.068	9.746	**31.201**
Technical	6.054	6.840	7.558	11.752	14.758	**46.962**
Total	**21.386**	**23.655**	**26.530**	**41.627**	**52.367**	**165.565**

Number of vacancies with type of building block	2018	2019	2020	2021	2022	Total
Legal	19%	19%	19%	18%	20%	**19%**
Management & Organisation	32%	33%	33%	32%	32%	**32%**
Education	1%	1%	1%	1%	2%	**1%**
Research	19%	19%	19%	19%	19%	**19%**
Technical	28%	29%	28%	28%	28%	**28%**

Figure 31: Development of demand for "types of building blocks" over time. Source: Jobdigger, edited by Dialogic

The various tasks, skills and knowledge have also been broken down into types of cyber security professional, see the figures below. It is important to note that this is limited to the most common cyber security building blocks (for example, the ECSF framework). For example, a developer might also be asked to be proficient in JavaScript or PHP; a financial analyst may also need to have some knowledge of financial flows. These building blocks were not considered in this research. The research explicitly focused on identifying cyber security-relevant building blocks in the various job functions.

It can be seen that there are quite a few similarities based on the breakdown into the four categories of cyber security functions (ECSF, CS – High, CS – Medium, CS – Low). In terms of tasks and skills, the common denominators include collaboration with internal and external stakeholders and the ability to identify and assess cyber risks. In terms of knowledge, there is often a demand for technical know-how about risks and threats, standards, methodologies and frameworks. Cyber security technical skills seem to be requested relatively more often within the ECSF profiles, for example for ethical hacking and dissecting technical systems. On the other hand, there seems to be more demand for more "generic" IT skills within the profiles with a low cyber security content, for example: programming and dealing with OS and servers. This is also in line with the different types of functions found in the different categories (Supplementary Tables 21 to 24).

Certificates

A specific building block that attracted plenty of interest during the research interviews and workshops are the certificates required by the job market. The Netherlands Training and Education Council (NRTO), among others, noted that certificates are relatively important in the job market for cyber security professionals.

One or more certificates are explicitly requested or mentioned in 9,387 vacancies (15%). The most requested certificates are the Certified Information Systems Security Professional (CISSP), the Certified Information Security Manager (CISM), and the Certified Information Systems Auditor (CISA), see Figure 32.

#	Certificate	% vacancies	Number of vacancies
1	CISSP	11,2%	6821
2	CISM	8,1%	4925
3	CISA	5,6%	3417
4	CIPP	2,8%	1713
5	CEH	2,1%	1301
6	CCSP	1,6%	999
7	OSCP	1,6%	950
8	CRISC	1,3%	785
9	CIPM	1,2%	762
10	GIAC	0,6%	342

#	Certificate	% vacancies	Number of vacancies
11	GCIH	0,4%	253
12	CSSLP	0,4%	230
13	OSCE	0,3%	204
14	SSCP	0,2%	150
15	GSEC	0,2%	141
16	GCIA	0,2%	105
17	GCFA	0,2%	103
18	CFE	0,2%	97
19	ECSA	0,1%	52
20	GWAPT	0,1%	45

Figure 32: Top 20 most requested certificates. Source: Jobdigger, edited by Dialogic

This relative ranking largely holds true for the different types of vacancies for cyber security professionals. However, in line with expectations, most certificates are requested for cyber security functions with an ECSF profile, see Figure 33.

#	Job Title – E	% vacancies	Number of vacancies
1	CISSP	25,6%	3440
2	CISM	17,0%	2290
3	CISA	10,6%	1422
4	CEH	5,4%	729
5	OSCP	4,2%	568
6	CCSP	3,6%	491
7	CRISC	2,9%	385
8	CIPP	2,8%	376
9	GIAC	1,8%	238
10	GCIH	1,7%	235

#	Job title – C	% vacancies	Number of vacancies
1	CISSP	27,3%	1145
2	CISM	22,9%	960
3	CISA	14,4%	603
4	CIPP	9,0%	377
5	CEH	6,1%	256
6	CRISC	3,6%	149
7	OSCP	3,2%	136
8	CIPM	3,2%	132
9	CCSP	2,1%	89
10	OSCE	1,0%	42

#	Job Title – C	% vacancies	Number of vacancies
1	CISSP	2,9%	1065
2	CISM	2,1%	751
3	CISA	2,0%	708
4	CIPP	0,8%	286
5	CCSP	0,5%	199
6	CIPM	0,4%	160
7	CRISC	0,4%	144
8	CEH	0,3%	106
9	OSCP	0,3%	106
10	SSCP	0,1%	41

#	Job Title – C	% vacancies	Number of vacancies
1	CISSP	15,5%	1121
2	CISM	12,1%	873
3	CIPP	9,0%	649
4	CISA	8,4%	606
5	CIPM	4,7%	340
6	CEH	2,7%	198
7	CCSP	2,6%	190
8	OSCP	2,0%	143
9	CRISC	1,3%	92
10	GIAC	0,6%	44

Figure 33: Certificates by category in cyber security vacancies. Source: Jobdigger, edited by

For many functions, a cyber security certificate is explicitly requested most of the time. This happens less often in other functions. For the Top 25 functions that explicitly request a cyber security certificate, the Access Management Consultant, CISO and Security Advisor are asked for a certificate relatively often, see Figure 34. Additionally, the specific certificates requested for the 10 functions in which the most certificates are requested have been identified, see Supplementary Table 25. Some certificates such as the CISSP are in high demand everywhere. Other certificates are more specific, such as the CISSP-ISSAP for the Cyber Security Architect, or the Offensive Security Certified Professional (OSCP) for the Penetration Tester.

#	Job title	Number of vacancies	Total number of vacancies	% vacancies in this position
1	ECSF – CISO	2051	2649	77%
2	ECSF – Cyber Threat Intelligence Specialist	609	1627	37%
3	ECSF – Cyber Security Implementer	428	3619	12%
4	ECSF – Cyber Security Architect	375	1382	27%
5	ECSF – Penetration Tester	302	520	58%
6	ECSF – Cyber Security Risk Manager	272	823	33%
7	Privacy Officer	198	467	42%
8	ECSF – Cyber Security Auditor	173	557	31%
9	Security Consultant	172	329	52%
10	Cyber Security Consultant	161	301	53%
11	Auditor	125	358	35%
12	Information Security Advisor	111	254	44%
13	ECSF – Cyber Incident Responder	91	246	37%
14	Consultant	73	298	24%
15	ECSF – Cyber Legal, Policy & Compliance Officer	71	275	26%
16	Cyber Security Consultant	67	99	68%
17	Officer	66	296	22%
18	Privacy Consultant	63	124	51%
19	Manager	48	160	30%
20	IT Security Manager	45	69	65%
21	Privacy Lawyer	43	62	69%
22	Information Security Consultant	40	58	69%
23	Security Advisor	34	44	77%
24	Access Management Consultant	32	34	94%
25	Analyst	30	131	23%

Figure 34: Top 25 job profiles that explicitly require a cyber security certificate. Source: Jobdigger, edited by Dialogic

4.5.2 Region

The different building blocks have also been broken down by region, see Figure 35. The distribution over the building blocks largely follows the same distribution as the vacancies. There are some deviations, such as the fact that a relatively high number of educational building blocks can be found in Noord Brabant and Zuid Holland. The individual tasks, knowledge and skills required follow the general demand of the regions. See Supplementary Table 26 for an overview.

Absolute

Province	Legal	Man. & Org.	Education	Research	Technical	Total
Drenthe	279	433	25	235	354	**1326**
Flevoland	331	554	35	297	482	**1699**
Friesland	353	521	31	266	416	**1587**
Gelderland	2181	3451	99	1970	3042	**10743**
Groningen	607	1007	30	553	886	**3083**
Limburg	863	1358	57	801	1274	**4353**
Noord-Brabant	3113	5365	345	2990	4784	**16597**
Noord-Holland	7769	14544	576	8727	12589	**44205**
Overijssel	1408	2475	56	1340	2368	**7647**
Utrecht	5731	9780	390	5892	8443	**30236**
Zeeland	161	248	20	159	234	**822**
Zuid-Holland	8786	13687	671	7954	12063	**43161**
Unknown	22	35	5	17	27	**106**
Total	**31325**	**53025**	**2315**	**30966**	**46608**	**164239**

Relatively

Province	Legal	Man. & Org.	Education	Research	Technical	Total
Drenthe	1%	1%	1%	1%	1%	**1%**
Flevoland	1%	1%	2%	1%	1%	**1%**
Friesland	1%	1%	1%	1%	1%	**1%**
Gelderland	7%	7%	4%	6%	7%	**7%**
Groningen	2%	2%	1%	2%	2%	**2%**
Limburg	3%	3%	2%	3%	3%	**3%**
Noord-Brabant	10%	10%	15%	10%	10%	**10%**
Noord-Holland	25%	27%	25%	28%	27%	**27%**
Overijssel	4%	5%	2%	4%	5%	**5%**
Utrecht	18%	18%	17%	19%	18%	**18%**
Zeeland	1%	0%	1%	1%	1%	**1%**
Zuid-Holland	28%	26%	29%	26%	26%	**26%**
Unknown	0%	0%	0%	0%	0%	**0%**

Figure 35: Types of building blocks per province. Source: Jobdigger, edited by Dialogic

4.5.3 Education level and work experience

The building blocks have also been broken down into vacancies based on the required level of education and work experience, and this can be seen in Supplementary Table 27. This shows which building blocks are in high demand per function category. The required building blocks are quite comparable due to the varying degrees of work experience. There are also many similarities between the educational levels, apart from a number of nuanced differences. This suggests the required knowledge and skills are comparable at a certain conceptual level across different levels of education and work experience, and that the difference lies mainly in the way they are implemented. To illustrate: being able to work well together plays a role from the start, but the way in which this manifests itself, and the people with whom you have to (be able to) work, changes as a person moves into a more senior position. The level within a building block thus seems to vary, while the importance of the building blocks seems to be quite stable.[16]

16. Part of this may also have a methodological explanation. Some building blocks are more likely to be explicitly mentioned in a vacancy than other building blocks.

4.5.4 Sector

The most frequently discovered building blocks for the 5 sectors in which the most cyber security vacancies were found can be seen in Supplementary Table 28. In broad terms there are many similarities, but there are differences in nuance too. There seems to be relatively more emphasis on building blocks relating to Management & Organisation and Legal within the government. There is, unsurprisingly, more emphasis on technical skills within the IT sector.

4.5.5 Organisations

The requested building blocks can also be viewed at the level of individual organisations. Three examples are provided below: TNO, Secura and ABN AMRO (Figure 36). A relatively high number of building blocks can be found within the functions of TNO regarding Management & Organisation in the Top 10, while for Secura, there is a relatively high number of building blocks regarding technology in the Top 10.

Organisation name	**Category**
TNO	Knowledge institution Cyber R&D

#	Top 10 Cs job profiles	Vacancies 2018-2022
1	Crypto Specialist	22
2	Cyber Security Specialist	18
3	Cyber Security Researcher	17
4	Cyber Security Scientist	14
5	Security Talent	12
6	Crypto Researcher	12
7	Start function	10
8	Researcher	6
9	System Simulation Engineer	5
10	Cyber Security Researcher	5
	Other	*157*
	Total	**278**

	starter	unknown	1-3	3-5	5-10	>10	Total
Univers	6	171	12	11	7	3	**210**
HBO		45	1	10	3		**59**
MBO	3	6					**9**
Total	**9**	**222**	**13**	**21**	**10**	**3**	**278**

	2018	2019	2020	2021	2022	Total
Total	55	25	25	82	91	**278**

	Full-time	Full-time,Part-time	unknown	Part-time	Total
Total	134	6	68	70	**278**

#	Top 10 CS competencies	Type	Category	Vacancies 2018-2022
1	Develop relationships with cyber security-related authorities and communitie	Main task(s)	Man. & Org.	151
	Motivate and encourage people	Key skill(s)	Man. & Org.	151
3	Cyber security controls and solutions	Key knowledge	Technical	142
4	Cooperate and share information with authorities and professional groups	Main task(s)	Man. & Org.	139
5	Management practices	Key knowledge	Man. & Org.	132
6	Collaborate with other team members and colleagues	Key skill(s)	Man. & Org.	117
	Collaborate with other teams and colleagues	Main task(s)	Man. & Org.	117
8	Cyber security recommendations and best practices	Key knowledge	Man. & Org.	98
9	Cyber threats	Key knowledge	Technical	94
10	Cyber security procedures	Key knowledge	Man. & Org.	90
	Total			**278**

Organisation name
Secura

Category
Company
Cyber production

#	Top 10 Cs job profiles	Vacancies 2018-2022
1	Information Security Consultant	19
2	IOT Security Expert	18
3	Auditor	14
4	Technical Security Specialist	13
5	Penetration Tester	12
6	Cloud Security Specialist	11
7	Consultant Security Awareness	10
8	Principal Security Expert	9
9	Information and Security Consultant	7
10	Ethical Hacker	7
	Other	*131*
	Total	**251**

	starter	unknown	1-3	3-5	5-10	Total
University		28	3	7	1	**39**
HBO	12	94	5	41	54	**206**
MBO		4	2			**6**
Total	**12**	**126**	**10**	**48**	**55**	**251**

	2018	2019	2020	2021	2022	Total
Total	31	19	72	83	46	**251**

	Full-time	Full-time,Part-time	unknown	Part-time	Total
Total	12	5	175	59	**251**

#	Top 10 CS competencies	Type	Category	Vacancies 2018-2022
1	Motivate and encourage people	Key skill(s)	Man. & Org.	141
2	Cyber security risks	Key knowledge	Technical	113
3	Identify, analyse and correlate cyber security events	Key skill(s)	Research	104
4	Cyber security standards, methodologies and frameworks	Key knowledge	Technical	103
	Cyber threats	Key knowledge	Technical	103
6	Cyber security-related technologies	Key knowledge	Technical	89
7	Multi-disciplinary aspect of cyber security	Key knowledge	Man. & Org.	84
	Work on operating systems, servers, clouds and relevant infrastructures	Key skill(s)	Technical	84
9	Cyber security controls and solutions	Key knowledge	Technical	77
10	Cyber threat actors	Key knowledge	Technical	69
	Total			**251**

Organisation name
ABN AMRO

Category
Company
Cyber integration

#	Top 10 Cs job profiles	Vacancies 2018-2022
1	IT Development Engineer	22
2	Technical IT-Auditor	20
3	Business Information Security Officer	17
4	ABN IT Talent Programme	17
5	Information Security Officer	17
6	Compliance Advisor	16
7	Information Security Expert	11
8	Artificial Intelligence Translator	10
9	Analyst	10
10	Global IT Talent Programme	10
	Other	*620*
	Total	**770**

	starter	unknown	5-10	3-5	1-3	>10	Total
Univers	12	83	123	11	17	20	**266**
HBO	38	230	136	54	11	6	**475**
MBO	7	20				1	**28**
Pre-University		1					**1**
Total	**57**	**334**	**259**	**65**	**28**	**27**	**770**

	2018	2019	2020	2021	2022	Total
Total	141	113	120	164	232	**770**

	Full-time	Full-time,Part-time	unknown	Part-time	Total
Total	230	23	239	278	**770**

#	Top 10 CS competencies	Type	Category	Vacancies 2018-2022
1	Cyber security controls and solutions	Key knowledge	Technical	263
2	Cyber threats	Key knowledge	Technical	257
3	Develop relationships with cyber security-related authorities and communitie	Main task(s)	Man. & Org.	256
4	Identify, analyse and correlate cyber security events	Key skill(s)	Research	244
5	Cyber security risks	Key knowledge	Technical	227
6	Work on operating systems, servers, clouds and relevant infrastructures	Key skill(s)	Technical	224
7	Cyber security standards, methodologies and frameworks	Key knowledge	Technical	210
8	Motivate and encourage people	Key skill(s)	Man. & Org.	179
9	Cooperate and share information with authorities and professional groups	Main task(s)	Man. & Org.	162
	Develop relationships with cyber security-related authorities and communitie	Main task(s)	Man. & Org.	162
	Total			**770**

Figure 36: Examples of building blocks in individual organisations. Source: Jobdigger, edited by Dialogic

4.5.6 Target groups

Finally, the building blocks have also been split across the mentioned target groups, in this case based on the Top 100 organisations that have been labelled manually (see Supplementary Table 29). (A relatively high number of technical building blocks are found in cyber production and integration within the "cyber security value chain". The technical building blocks are also found relatively more in the business community when compared to government. Across the board, non-technical skills, including true soft skills, are important for performing these professions.

4.6 Outflow and inflow

For the purposes of this research, we noticed that the growing demand on the cyber security job market is mainly associated with the so-called "expansion demand": the demand resulting from additional cyber security work on the job market. Although this expansion demand is also highly relevant for the cyber security job market, there is also a so-called "replacement demand": the demand resulting from an outflow of labour. There can be many reasons for this outflow; for example, switching to another (type of) profession, retiring, emigrating abroad or unexpectedly becoming ill or incapacitated for work. There was a particular interest at the start of this research in understanding how many cyber security professionals retire and/or emigrate abroad, this was to gain an idea of what cyber security expertise the Netherlands is "losing".

Investigating this is no trivial matter and presents many challenges. The biggest challenge is that there is no registration of "cyber security professionals" in the Netherlands. Existing occupational classifications are unsuitable for gaining good insight into these professionals[17]. This requires an indirect estimation of the people who are likely to be active as cyber security professionals.

In previous research into the "economic opportunities of the cyber security sector", a list of companies that form part of the cyber security sector was drawn up. This specifically concerns companies that are (also) active as producers of cyber security products (goods/services), see Category B in Figure 12. The people working within these companies have a relatively higher probability of being cyber security professionals. In addition, the vacancy analysis shows that the majority of cyber security positions require HBO or University education level. **The analyses presented in this section will therefore be based on individuals who [1] have completed HBO or University education and who [2] are employed in companies that are (also) active as producers of cyber security goods and services**. It should be noted that [i] many of these companies also engage in non-cyber security activities and [ii] there are also non-cyber security professionals active within cyber security companies. While this is not a watertight approach, given the current information it is a pragmatic way to gain some insight into the dynamics of the job market for cyber security professionals. Outflow and Inflow figures were identified based on the data available within the Statistics Netherlands microdata environment. The results presented here relate to 2021; less detailed data are available for 2022. The figures can be used to estimate the expected orders of magnitude of inflow and outflow of cyber security professionals in relative terms. *The absolute numbers laid out here do not equal the number of cyber security professionals.*

17. In the Employee Insurance Agency (UWV) publication "ICT in beeld" (August 2023), a custom assignment appears to have been given to Statistics Netherlands, in which Statistics Netherlands probably edited the source data of the Enquête Beroepsbevolking (EBB) [Labour Force Survey] specifically. This information was not available for use in this report. It may be interesting in the future to explore whether the raw data from the EBB can be used to gain more insight into cyber professionals. A broader scope could/should also be used than is used currently in order to do more justice to the full range of the "cyber security professional" concept.

Results

The results of the analysis are summarised in two infographics, see Figure 37.
The following conclusions from the analysis can be drawn:

Current population

- **The population of cyber security professionals is relatively young**. About three quarters of the population is under 50 years of age. The expectation is that there will be relatively little replacement demand due to retirement in the coming years.
- **Men are relatively "over-represented"**. Two out of three professionals in the population are male. A third are female.

Outflow

- There was an outflow of almost 25% of the population in 2021.
- **A small part of the population (0.4%) retired** (~2% of those leaving).
- **A small part of the population (0.4%) emigrated**. (~2% of those leaving).
- About three quarters of those who leave go on to work for an organisation outside the research population[18]. This does not necessarily mean they will take up another profession; they may take up the same profession or a similar profession with another employer.
- About 2.5% of the population switched to another company within the research population.

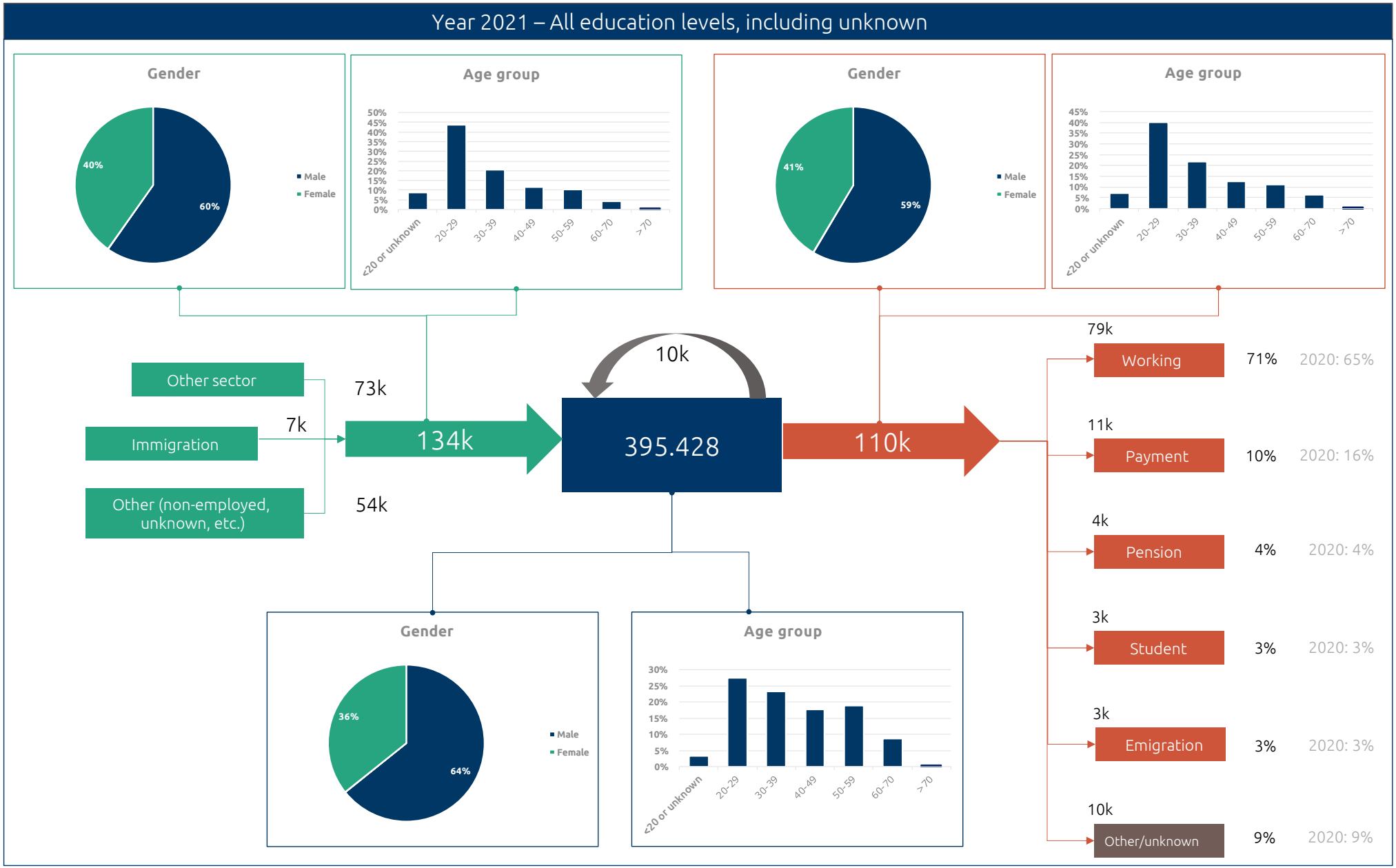
Inflow

- **Immigration and migrant workers appear to be important for the sector**. About 5-10% of the inflow is attributable to immigration. This is in line with what we see in the ICT top sector. Even ~15% of the inflow comes from immigration. There too, ~3% of the total stock can be attributed to immigration in the year in question.
    - It is usually the case for immigrants that the level of education is not included in Dutch registrations. This makes it difficult to identify the educational level for this target group. What is known is that ~7,000 immigrants entered this population in 2021, of which 570 are known to be highly educated. For the other ~6,500 it is unknown.

General

- **The inflow and outflow figures fluctuate over the years**. This can be due to several reasons. Although this cannot be directly calculated from the figures, and this has not been investigated further for the purposes of this research, it is conceivable that the situation regarding COVID-19 had an impact on this.

18. The current research population only concerns organisations in the cyber R&D, cyber producers and cyber integration categories, as described in Figure 12: The cyber security sector and its value chain. Source: Dialogic (2023), The economic opportunities of the cyber security sector. For more information about the creation of this research population: https://www.rijksoverheid.nl/documenten/rapporten/2023/04/06/de-economische-kansen-van-de-cybersecuritysector


Year 2021 – All education levels, including unknown
Gender
40%
60%
Male
Female
Age group
50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
<20 or unknown
20-29
30-39
40-49
50-59
60-70
>70
Gender
41%
59%
Male
Female
Age group
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%
<20 or unknown
20-29
30-39
40-49
50-59
60-70
>70
Other sector
73k
Immigration
7k
Other (non-employed, unknown, etc.)
54k
134k
10k
395.428
110k
79k
Working
71%
2020: 65%
11k
Payment
10%
2020: 16%
4k
Pension
4%
2020: 4%
3k
Student
3%
2020: 3%
3k
Emigration
3%
2020: 3%
10k
Other/unknown
9%
2020: 9%
Gender
36%
64%
Male
Female
Age group
30%
25%
20%
15%
10%
5%
0%
<20 or unknown
20-29
30-39
40-49
50-59
60-70
>70

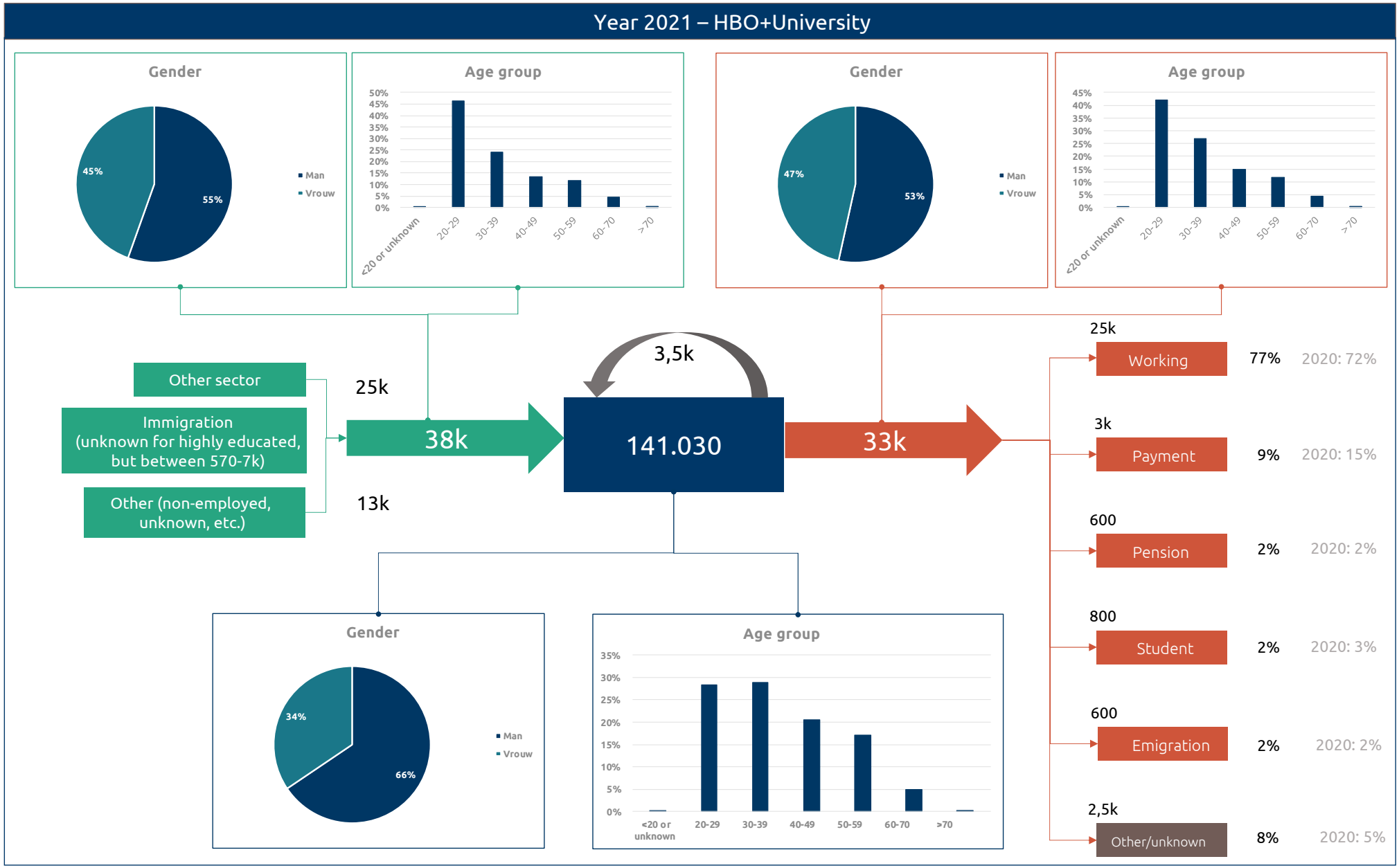


Figure 37: Outflow and inflow based on a population of companies that are (also) active in the cyber security sector. Source: Statistics Netherlands-microdata, processed by Dialogic

4.7 Relevant developments

For the purposes of this research, stakeholders were asked about which developments they consider important to meet the demand for cyber security expertise. The most frequently mentioned developments are:

1. The introduction of the NIS2 directive;
2. The introduction of the CRA;
3. Use of AI;
4. The way in which organisations organise their required cyber security expertise (in-house and/or externally).

This section describes the developments and explains the impact that the demand for cyber security expertise will have, to the extent possible based on the collected input, empiricism and substantiation.

4.7.1 NIS2

NIS2, the Network and Information Security directive, is the successor to the NIS directive.[19] The European version has been published and is currently being translated into Dutch law. The aim of the directive is to "increase the cyber security and resilience of essential services in EU Member States". This new directive expands the scope to include more sectors while mandating stricter security standards and reporting requirements. The guideline applies to organisations that [1] are active in certain sectors and [2] can be classified as an "essential" or "important" entity. A full explanation can be found on the NCTV website.[20] Parties that fall within this new directive have a *duty of care* and a *reporting obligation* and will be *supervised*.

This new legislation can be generally considered as a motivating factor to answering the question, "What should be done about cyber security?". The impact of the NIS2 directive on the demand for cyber security expertise in organisations is expected to differ between the organisations. On the one hand, there are a number of organisations already doing plenty in terms of cyber security, and therefore the introduction of the NIS2 directive does not require (or only requires minor) additional efforts within their own organisation. Of note though is the fact that large parties must also ensure cyber security within the chain. For example, if a large manufacturing company has a large number of SME suppliers, they must come up to standard as well. If the suppliers are unable to organise this themselves, support may be required from major parties within the value chain or ecosystem. So, even if one party has its internal affairs in order, this does not mean they will not experience any consequences from the NIS2 directive.

On the other hand, there is an expectation that some organisations will have to make an extra effort. The expectation is that organisations that currently only take on the role of "cyber end user", and not the role of cyber R&D, cyber production or cyber integrator, may face a relatively new challenge. Those parties that are more specialised with cyber security will have a higher level of cyber security maturity and generally have a good understanding of what is going on and what is required. This does not mean it will be easy for them; however, the relatively greater inexperience of "pure cyber security end users" with cyber security means their transition (due to the NIS2 directive) may be greater.

According to the interviewees, working on cyber security often seems to follow the process of first appointing one or more people who already have an overview and thus, who understand what needs to be done. These could be, for example, information managers, cyber security managers or CISOs. Once they know exactly what needs to be done, there is still the question of implementation. The "execution of the plan" thus naturally follows the "drafting of the plan". The expectation is that the NIS2 directive will provide an impetus for organisations to formulate a strategy and plan, and that this will also translate into a greater demand for professionals for the implementation. This implementation can also take on different job profiles, from the Pen-tester to the Cyber Security Implementer, Cyber Incident Responder and the System Administrator.
Comments were also made about how the new legislation also requires activity to support the compliance, supervision and enforcement. The expectation is that this will lead to greater need for professionals, to deal with auditing tasks for example.

Therefore, the expectation is that the NIS2 directive, with its duty of care, reporting obligation and supervision, will increase the demand for cyber security professionals. The follow-up question to this is: how will the requested expertise be organised within the economy. To what extent will organisations bring cyber security expertise onto the staff, or will they choose to organise this externally by hiring and purchasing and/or through partnerships? This point is discussed further in 4.7.4.

19. More information can be found at https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/
20. https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen/wat-zijn-de-sectoren-en-criteria-die-bepalen-of-een-organisatie-onder-de-nis2-richtlijn-valt

4.7.2 CRA

In addition to the NIS2 directive, the arrival of the Cyber Resilience Act (CRA) is a relevant development for the demand for cyber security expertise. The CRA ensures digital products placed on the (European) market meet strict cyber security requirements. The main points of the CRA can be found on digitaleoverheid.nl[21]:

- *"Only digital products that meet the strictest security requirements will be released onto the market.*
- *Manufacturers are required to provide free safety updates throughout the life-cycle of their products, as well as to report digital vulnerabilities and incidents.*
- *Non-commercial open source software is exempt.*
- *Manufacturers will be given sufficient time to implement the rules."*

The European Union states that the legislation should come into force at the beginning of 2024. In addition: *"Manufacturers will have to apply the rules 36 months after they come into force"*.[22] This law will therefore play a role over the coming years. In terms of the conceptual cyber security value chain model used in this report, this law will focus on the "integrators". On the one hand, stricter requirements may apply to parties that already act as cyber integrators. On the other hand, some parties will be forced to act as cyber integrators, despite not (sufficiently) doing so at present.

The obligations imposed by the CRA could impact the entire cyber security value chain. Those parties that function solely as cyber end users are expected to experience little impact on their own demand for cyber security professionals as a result of the CRA. However, those parties involved in integration, as well as production and R&D, will have to invest more in cyber security across the board to get everything in order and keep it that way.
The obligations imposed by the CRA will require manufacturers to comply with the law at a more strategic level and adapt their strategies and plans accordingly. This requires, for example, cyber security professionals with an integrated view of business operations and the integration of cyber security within them. At a more tactical and operational level, manufacturers will also need to adapt their products to meet the requirements. This in turn requires, among other things, more people who can also technically design and implement cyber security. The result of this is greater demand for cyber security professionals in the broadest sense of the word, including cyber security architects and implementers. This legislation also increases the demand for compliance, supervision and enforcement professionals. This could include, among other things, more auditors and legal & compliance officers.

4.7.3 Use of AI

One of the most frequently reported developments is the rise and use of Artificial Intelligence, also known as "AI". The term AI is interpreted differently by different people, but the basic definition used for this report is (computer) systems that in some sense exhibit a form of (human) intelligence. In other words, the computer can [1] perform tasks that humans currently perform and/or can [2] perform new tasks humans cannot perform.

Three main reasons for the rapid development of AI are:

1. **Information gathering**. More data (AI "input") is being created that AI must learn and work on. More (usable) data also means more opportunities to extract value from that data.
2. **Information processing**. Information processing is becoming increasingly powerful, both in terms of hardware (more powerful computers, faster processors, better working memory, etc.) and software (better algorithms capable of performing more complex tasks).
3. **Accessibility**. Powerful AI models are becoming increasingly accessible to a wider audience. For example, centrally hosted models (current common models are GPT-4 or DALL-E) can be easily used, and they can usually be easily integrated into broader work processes via an API.

The opportunities and risks of AI are not limited to one single sector; the cyber security domain is also being confronted with opportunities and risks. Looking at job market opportunities, there appear to be a number of cyber security tasks in which AI can play a role. **At its core, AI has always been about information processing**. This means tasks in which information processing is central and, without AI, the information processing skills would normally have to be assigned to people (or not assigned at all).
The researchers looked at the various tasks and skills and categorised them into whether they involve the type of information processing in which AI could play a role (perhaps only in theory for the time being). The results are shown in Figure 38. The analysis appears to show a lot of potential for the use of AI, especially in the relatively technically-oriented ECSF profiles. This includes the Penetration Tester, Cyber Threat Intelligence Specialist, Digital Forensics Investigator and the Cyber Incident Responder.

21. https://www.digitaleoverheid.nl/nieuws/overeenstemming-eu-landen-over-cyber-resilience-act/
22. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

		Key skills – potential AI			Main tasks – potential AI			Skills + tasks – potential AI		
#	ECSF profile	None/few	Substantial	% substantial	None/few	Substantial	% substantial	None/few	Substantial	% substantial
1	Penetration Tester	3	8	73%	3	5	63%	6	13	68%
2	Cyber Threat Intelligence Specialist	3	7	70%	7	5	42%	10	12	55%
3	Digital Forensics Investigator	3	2	40%	3	3	50%	6	5	45%
4	Cyber Incident Responder	4	2	33%	6	5	45%	10	7	41%
5	Cyber Security Implementer	5	2	29%	7	3	30%	12	5	29%
6	Cyber Security Risk Manager	6		0%	4	4	50%	10	4	29%
7	Cyber Security Architect	9	1	10%	8	4	33%	17	5	23%
8	Cyber Security Auditor	5	3	38%	11	1	8%	16	4	20%
9	Cyber Security Researcher	4	3	43%	12	0	0%	16	3	16%
10	Cyber Legal, Policy & Compliance Officer	8		0%	11	1	8%	19	1	5%
11	Chief Information Security Officer (CISO)	15	1	6%	14	0	0%	29	1	3%
12	Cyber Security Educator	9		0%	8	0	0%	17	0	0%
	Total ECSF	**74**	**29**	**28%**	**94**	**31**	**25%**	**168**	**60**	**26%**

Figure 38: Potential of AI for the different ECSF profiles. Source: Dialogic

It is therefore conceivable that parts of the work of these job profiles will be carried out by (or with) AI in the future. In part, this means certain tasks may disappear, but also that new tasks will emerge (e.g. developing and managing the AI) and new competencies will be required (e.g. being able to deal with software in which AI is integrated in a smart way). Broadly speaking, when there is demand for a sufficient number of new tasks and specialisms, this often creates a new job profile on the job market. For example, AI engineers are now in demand in the high-tech industry, and privacy officers have become commonplace (partly due to the introduction of the GDPR); these are functions that did not exist a few years ago. The (further) rise of "AI Cyber Experts" is therefore not unthinkable, regardless of what this group of professionals will be called.

On the one hand, AI will undoubtedly reduce the demand for certain tasks, knowledge and skills (meaning we can do more with fewer people), but at the same time it will also lead to new tasks and require new knowledge and skills.

The tasks and skills laid out in the ECSF that will probably lend themselves relatively well to support or implementation by AI are also regularly requested in vacancies explicitly. Figure 39 provides an overview of this.

#	Building blocks	Number of vacancies	% vacancies
	Main tasks		
1	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	1112	1,8%
2	Design and propose a secure architecture to implement the organisation's strategy	863	1,4%
3	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	657	1,1%
4	Identify, analyse and assess technical and organisational cyber security vulnerabilities	333	0,5%
5	Identify and document compliance gaps	309	0,5%
6	Identify and assess cyber security-related threats and vulnerabilities of ICT systems	136	0,2%
7	Identify, recover, extract, document and analyse digital evidence	82	0,1%
8	Identify, analyse, mitigate and communicate cyber security incidents	67	0,1%
9	Identify, monitor and assess the Tactics, Techniques and Procedures (TTPs) used by cyber threat actors by analysing open-source and proprietary data, information and intelligence	43	0,1%
10	Identification of threat landscape including attackers' profiles and estimation of attacks' potential	42	0,1%
	Key skill(s)		
1	Identify, analyse and correlate cyber security events	25562	41,9%
2	Develop codes, scripts and programs	3619	5,9%
3	Develop code, scripts and programs	3619	5,9%
4	Conduct ethical hacking	1225	2,0%
5	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	1131	1,9%
6	Identify and exploit vulnerabilities	1100	1,8%
7	Assess the security and performance of solutions	984	1,6%
8	Perform social engineering	818	1,3%
9	Review codes assess their security	788	1,3%
10	Conduct technical analysis and reporting	731	1,2%

Figure 39: Demand for tasks and skills in which AI could play a role. Source: Jobdigger, edited by Dialogic

AI will not only impact the way cyber security professionals can do their work via an "internal" route, it will also impact what cyber security professionals need or want to protect us via an "external" route. A well-known example is AI and the rise of deep fakes, which have made crimes such as defamation and identity fraud possible in new ways. AI can also lead to more digital systems being connected and working together intelligently, which for example increases the risks of failure, makes certain systems a greater target, and can also increase the demand for cyber security. These are just a few examples, but they illustrate how AI is impacting both the world at large, and specifically the work that cyber security professionals do.

4.7.4 'Make or buy'

A relevant development mentioned several times in this research is the consideration organisations will have to give to the organisation of the necessary cyber security expertise [1] in-house or [2] externally, for example through purchasing or partnerships. This could be viewed as a "make or buy" decision.
There are many situations in which, for example, an FG or CISO works for multiple organisations, or where arrangements within municipalities to ensure specialist functions are filled that may exceed the maturity and needs of individual organisations. In other words, assuming there is growing demand for cyber security expertise in the future, the next question is: in which organisations will this demand manifest itself and how. Should every organisation have its own cyber security expertise in-house and if so, what expertise do they need exactly?

Statistics Netherlands used the Cyber Security Monitor (2022) to ask companies how they carry out their ICT safety activities. The results can be found in Figure 40. The results show that small organisations with up to nine people do most themselves, or state that it is not relevant to them. For larger organisations, the general rule is that approximately 20% arrange everything themselves, and the remaining 80% either outsource it entirely or do it in collaboration with external parties. In addition, the larger the organisation, the more often it is carried out in collaboration with external parties. An important explanation is that the complexity and risks for large organisations are increasing, and (even) more specialist knowledge, skills and products are required to stay secure when operating digitally.

The vacancy data also shows that very often, many parties with little involvement in the development of cyber (R&D, production, integration) and that often deal with the subject as cyber end users actually outsource their cyber security to professionals with a broader profile. For example, this could include “generic” IT professionals who also manage cyber security. The question is whether future developments will lead to this group of organisations bringing more specialist cyber security profiles in-house, or whether they will continue to work with their own “hybrid” professionals and/or arrange this with external parties. In general terms, the research shows that these organisations must first be aware of the role cyber security plays in the organisation, and that hiring someone who has the overview is simply the first step. This person can then estimate what needs to be hired/purchased externally and/or what needs to be done internally to meet the organisation’s cyber security goals.

The conclusion of this report is that, based on the information collected, we expect:

- Organisations that are marginally involved with the subject, in which cyber security plays a relatively small role and that do not fall under the NIS2 directive and/or CRA, will probably continue to opt for the “hybrid” functions in combination with external hiring/purchasing.
- Organisations that are marginally involved with the subject, but will fall under the NIS2 directive and/or CRA, will more than likely employ at least one specialist cyber security profile. Of note is that many of the parties that fall under the legislation already employ such professionals, and there is no good view of which organisation groups currently have little or no cyber security expertise in-house, but that will need it in the future.

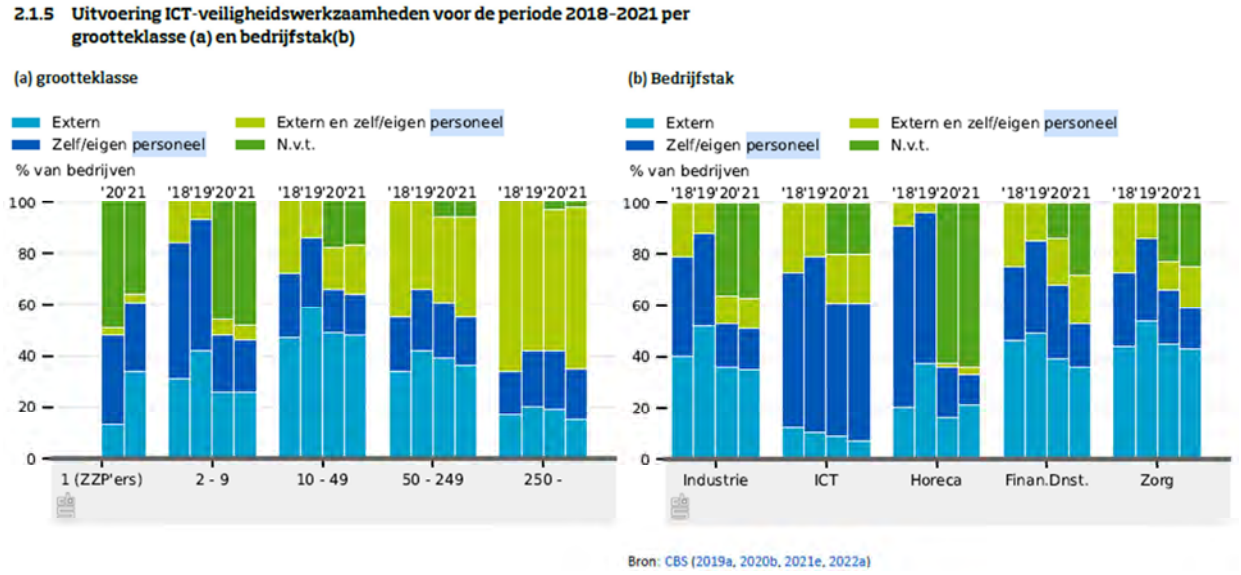


Figure 40: Ways in which companies carry out their ICT safety activities. Source: Statistics Netherlands, Cyber security monitor 2022.

4.8 Conclusions

The following conclusions are based on the job market findings:

Demand for cyber security professionals – general

1. [4.3.1] **The demand for cyber security expertise is growing**, both in the specialist cyber security profiles and the broader job profiles containing some cyber security.
2. [4.3.1] We estimate there to be approximately **60,000-110,000 cyber security professionals active on the job market**, of which 17,000-33,000 are professionals with a specialist cyber security profile.
3. [4.3.2] The **demand for cyber security expertise is concentrated in the Randstad** (Noord-Holland, Zuid-Holland, Utrecht).
4. [4.3.3] The focus of the demand is on **intermediate and senior positions for which MBO or University education** is required.
5. [4.3.4] The **government and the IT sector** are the two sectors with the highest demand for cyber security expertise.
6. [4.3.5] The **ten organisations** with the most cyber vacancies are the Police, PWC, CGI, EY, Tax Authorities, ING, ABN AMRO, Capgemini, KPMG and the Ministry of Defence.
7. [4.3.6] **Organisations that are relatively more involved with cyber security also have a greater demand for specialist profiles**. A large part of the demand for specialist cyber security professionals lies with parties that, in addition to the role of cyber end user, also have the role of producer and/or integrator.

Demand for cyber security professionals – job profiles

8. [4.4.1] **The most requested job profiles** for each type of cyber security profile are:
   a. **ECSF**. [1] CISO, [2] Cyber Security Implementer and [3] Cyber Threat Intelligence Specialist
   b. **"Cyber Security – High"**. [1] Cyber Security Consultant, [2] Data Protection Officer and [3] Information Security Advisor
   c. **"Cyber Security – Medium"**. [1] Privacy Officer, [2] Security Consultant and [3] Consultant
   d. **"Cyber Security – Low"**. [1] System Administrator, [2] Auditor, [3] Functional Manager
9. [4.4.2] **The top provinces have more specialist cyber security profiles** in the top 20 job profiles than the provinces where fewer cyber vacancies have been advertised.
10. [4.4.3] **For many cyber security profiles there are opportunities to start working in junior positions**, albeit with a more focused range of tasks and fewer responsibilities.
11. [4.4.4] **Different sectors have different ways in which cyber security expertise manifests itself.** For example, demand in the IT sector is for broader IT functions that include cyber security, while demand in the government is for advisors with a broader profile that includes cyber security.
12. [4.4.5] **It only becomes really clear at the organisational level what the specific demand is in specific contexts**. Ultimately, the job market is a sum of individual functions at individual organisations. More focus is required to really understand the demand at a more granular level.
13. [4.4.6] **The demand for cyber security professionals differs between parties with a different role in the "cyber security value chain"**. For example, there is high demand for specialist cyber security profiles in the cyber security sector itself (the production of cyber security goods and services), while Cyber R&D (logically) has a high demand for Cyber Researchers.

Demand for cyber security professionals – tasks, knowledge and skills

14. [4.5.1] Across the board, relatively **more technical knowledge** is required to be active in cyber security, but the **required skills and tasks** to be performed are largely **non-technical** in nature. The technical component weighs more heavily in ECSF profiles than in other types of cyber security profiles.
15. [4.5.1] The demand for cyber security expertise and the underlying building blocks is **growing strongly in absolute terms**; but in relative terms, the **ratio between different knowledge and skill types is stable**.
16. [4.5.1] **15% of the vacancies explicitly request a cyber security certificate**. The most requested certificates are CISSP, CISM, and CISA.
17. [4.5.1] **A certificate is often required for specialist cyber security profiles**; for example, 77% of CISO profile vacancies require a certificate and 58% of the Pen-tester vacancies require a certificate.
18. [4.5.3] **The composition of the building blocks appears to be quite stable** as the functions require more work experience. This implies the actual implementation of these building blocks, and the extent to which people are able to implement them, grows objectively as they develop further.

Inflow and outflow

19. [4.6] **The population of cyber security professionals is relatively young**. About three quarters of the population is under 50 years of age. The expectation is that there will be relatively little replacement demand due to retirement in the coming years.
20. [4.6] **Men are relatively "over-represented"**. Two out of three professionals are male. A third are female.
21. [4.6] **0.4% of the population retired** (~2% of the outflow).
22. [4.6] **0.4% of the population emigrated** (~2% of the outflow).
23. [4.6] **Immigration/migrant workers appear to be important to the sector**. ~5-10% of the inflow is attributable to immigration.

Relevant developments

24. [4.7.1] The expectation is that the **duty of care, reporting obligation and supervision required by the NIS2 directive will generally increase the demand for cyber security professionals across the board**.
25. [4.7.2] The expectation is that **the CRA will increase the demand for cyber security professionals across the board, with the greatest impact likely to be on cyber integrators**.
26. [4.7.3] With the further **development and deployment of AI, the demand for people to perform certain tasks will decrease**, but **new tasks will arise** and **new competencies** will be required. There is the greatest potential for AI to perform/support parts of the work of the Penetration Tester, Cyber Threat Intelligence Specialist and the Digital Forensics Investigator within the ECSF profiles.
27. [4.7.4] **Organisations that are marginally involved with cyber security, in which cyber security plays a relatively small role**, and that do not fall under the NIS2 directive and/or CRA, will probably continue to opt for the **"hybrid" functions in combination with external hiring/purchasing/organisation** of cyber security expertise.

5. Connection between education and the job market

Research question 6:
Provide insight (quantitatively and qualitatively) into the discrepancy between the demand for and supply of cyber security expertise. Analyse what factors cause this discrepancy. Consider, among other things, (perceived) quality differences between different courses and certification .

The idea that education and (all) specific vacancies on the job market could match perfectly is a misconception because learning has to take place over several years and in different contexts (work environment, training, etc.). This research therefore examined the job market demand for junior positions and the subsequent connection with the training courses.
In Higher Education we see relatively too few HBO and University graduates with a specialist cyber security profile to meet the needs of the job market. However, the number of HBO and University graduates who had a "substantial" cyber security component in their training is aligned with demand. Just like the quantitative demand for MBO cyber security junior staff: this is in line with the outflow in the two relevant MBO-4 courses.
In terms of content, there is plenty of demand for the "Technical" and "Management & Organisation" competencies on the job market. We also see these building blocks in courses with a specialisation in cyber security. The focus on "legal" competencies is particularly evident in courses in which cyber security is not a specialisation. However, we do not see the competencies reflected anywhere in "education" (e.g. teaching) – neither in the training courses nor in vacancies at junior level.

A major challenge for the cyber security job market therefore appears to lie in Life-Long Learning, both in attracting and retaining (current) cyber security professionals.

Account must be taken here of the difference between the position someone comes from and the position someone enters into. This difference should not be too great; there must be a "bridgeable gap". It is important to look carefully at which backgrounds provide sufficient basis to bridge the gap.
Certificates can play a role here: the importance of certificates on the cyber security job market is great, especially for the more specialised cyber security profiles. These certificates and their associated training courses are a way to bridge the gap.
In addition, it is important to address the aforementioned bottlenecks in education; which will improve the quantitative and qualitative intake of regular courses, thus better meeting the demands of the job market.

5.1 Connection between education and the job market

There is often talk about "the mismatch between education and the job market". Looking at what happens in practice, the two concepts of "education" and "job market" need to be specified in more detail so a meaningful statement about the connection between the two can be made. Looking at **regular** education, it is better to look at mainly **junior positions** on the job market; after all, it is unrealistic for a recent graduate to hold an intermediate or senior position, with some exceptions. When reviewing **intermediate and senior positions**, it is more realistic to avoid looking at regular education, but rather at **Life-Long Learning** (refresher training, learning on the job, private trainers, etc.).

The relationship between regular education on the one hand and vacancies on the job market on the other are reviewed below. First, a number of preliminary comments:

- Vacancies
  - **Vacancies are a proxy for demand in the job market, but vacancies do not equal demand**. Vacancies are one, albeit common, manifestation of demand. Organisations can also hire people without posting a vacancy (e.g. interns who are offered an employment contract after completing their internship).
  - **The vacancy data used here is extensive, but not 100% comprehensive**. The Jobdigger data provider collects vacancies from many sources (job platforms, individual websites of organisations), but they cannot identify all vacancies in the Netherlands (e.g. offline vacancies on notice boards).
  - **Vacancy figures do not in themselves take into account "throughput"**. In theory, it is possible for two professionals to swap jobs every week. This would mean that if two vacancies were posted every week, two professionals could fill 104 vacancies every year. Although this is an extreme and unlikely example, it does illustrate that a vacancy cannot simply be equated with the (permanent) demand for one professional.
- Education

  The number of degrees awarded is not equal to the number of people awarded with a degree; this is because one person can obtain multiple degrees. The numbers for graduates are added together for the identified courses. This does not take into account the fact that one person can follow multiple courses. For example, someone with a bachelor's degree can still follow a master's degree, or a person with a Level 4 MBO education can still follow HBO education. Because the number of the education courses completed for graduates is at least 1, and the number of diplomas obtained is not equal to the number of graduates, the number of people that have completed at least one relevant cyber education course may be overestimated.
- Relationship between education and the job market
  - **The analysis presented below does not look at [1] the (lateral) entry from the job market and the [2] inflow via labour migration**. This means that if there is a "gap" between what regular education "delivers" and what the job market demands, it may be that the difference is filled by these two sources.

5.2 Regular education & junior functions

A quantitative picture of the relationship between demand from the job market and supply from regular education is shown below. This is followed by some qualitative reflections.

Quantitative image

Starting points

The following principles were used to identify the connection between (regular) education and the job market (junior functions):

- Vacancies
  - All the cyber security vacancies classified as "junior positions" in the year 2022 were reviewed.
  - Looking at junior positions, it can reasonably be expected that these are positions that a (recently) graduated jobseeker can apply for. The "junior phase" usually lasts more than one year. The "junior phase" often last three years. In this case, it might be fairer to divide the total demand for junior positions by 3 in order to match it to the annual outflow from education.
  - The level of education, focused on HBO and University education, is used because the majority of the demand for cyber security expertise is concentrated here.
  - The type of cyber security profile (ECSF, CS – High, CS – Medium, CS – Low) were used
- Education
  - All cyber security courses that [1] focus fully on cyber security, [2] partly focus on cyber security through a specialisation, or [3] partly focus on cyber security through a compulsory component of >6 EC were reviewed.
  - The outflow (and inflow) in 2022, which corresponds to the academic year 2021-2022 was reviewed.

Connection between regular education and junior positions on the job market – HBO and University education
The relationship between education and the job market at HBO and University level can be broadly summarised by the following Figure 41:

:Job market and HBO and University education 2022

Vacancies		Outflow Education		Inflow Education	
Full CS		**Full CS**		**Full CS**	
Vacancies ECSF	845				
Vacancies CS - Hoog	295				
Vacancies full CS	1140	Graduates full CS	266	Inflow full CS	426
Partial CS		**Partial CS**		**Partial CS**	
Vacancies CS - Middle	481	Graduates partial CS (specialisation)	610	Inflow partial CS (specialisation)	706
Vacancies CS - Low	2116	Graduates partial CS (component)	1409	Inflow partial CS (component)	1940
Vacancies partial CS	2597	Graduates total	2019	Inflow total	2646
CS - total		**CS - total**		**CS - total**	
Vacancies total	**3737**	**Graduates total**	**2285**	**Inflow total**	**3072**

Figure 41: job market and HBO and University education 2022

The demand for **specialist cyber security profiles** was 1,140 vacancies, with 845 being linked to an ECSF profile. Looking at the outflow from education that specialises fully in cyber security, there were only 266 graduates in 2022, assuming each diploma corresponds to one person. If the demand covered ~3 years of junior positions, and part of the vacancies therefore also applied to professionals who are already active in the job market (for 1 or 2 years), the annual demand would be ~380 (1/3 of 1140). It can therefore be seen that there is more demand from the job market than what education currently delivers. Thankfully, the inflow in 2022 is 426, and the inflow into education does follow job market growth. **However, based on these figures it does appear that education is lagging behind, and that more attention is required for the entry into and completion of these courses**. As mentioned earlier, the job market can also meet demand through inflow from the job market and labour migration, so the "mismatch" **estimated above does not necessarily mean demand is not being met**.

For vacancies related to **"containing some cyber security"**, demand is 481 (CS – Medium) and 2,116 (CS – Low) on the job market in 2022. This are 2,597 vacancies in total. Again, if these vacancies were to cover a three-year period, this would equate to ~865 vacancies per year. In 2022, education produced 2,019 graduates (610 with a specialisation in cyber security and 1,409 with a compulsory cyber security component > 6 EC). In general, this would suggest **that education should be able to keep pace with job market demand**. The inflow for these courses is also increasing; growth that we are also seeing on the job market.

Although there is some uncertainty surrounding the figures laid out above, it is possible to state that **relatively too few graduates with a specialist cyber security profile are being delivered, but that the number of graduates with a "substantial" cyber security component in their training is at the right level**. If graduates with a "partial cyber security education" were to also apply for specialist cyber security profiles, there could again be a shortage of graduates in that category. In order to meet the expected (greater) demand in the future, more outflow from both specialist training courses and "hybrid" training courses seems desirable.

MBO
Approximately 6,000 MBO students graduate from the 4 MBO courses in question every year. The Software Developer and IT Systems & Devices Expert courses have the largest share of cyber security in their training. This means they have the best chance of matching the vacancy requirements. Since there are no outflow figures for every course, but the ratio of these courses compared to the other 2 Qualification Dossiers in 2022 is known, the estimation is that approximately 75% of the outflow comes from these courses.
It seems plausible that the **quantitative demand for MBO cyber security junior staff (733) can be met by the outflow in MBO (75% of the total outflow = 4500)**.

Qualitative picture: heterogeneity in the specialist profiles

A distinction has been made above between specialist cyber security profiles and partial cyber security profiles in order to maintain an overview. However, there is still heterogeneity in the specialist profiles. The demand for "types" of competencies linked to the various specialist ECSF profiles in 2022 is set out below. All building blocks (tasks, knowledge and skills) within the described ECSF profiles are provided with a "type", whereby an estimate of the primary type to which a building block belongs (Figure 42) has been made.

This is not exact mathematics, and the percentages do have some flexibility, but the estimate does give a rough idea of a different focus within the various profiles.

	2022 - Junior - vacancies				Building Blocks					
ECSF-profile	WO	HBO	MBO	Total	Legal	M&O	Education	Research	Technical	Total
Cybersecurity Researcher	33	6	0	39	8%	20%	4%	56%	12%	100%
Digital Forensics Investigator	9	7	0	16	4%	12%	0%	15%	69%	100%
Cyber Threat Intelligence Specialist	6	83	15	104	3%	30%	0%	11%	57%	100%
Penetration Tester	4	71	1	76	0%	15%	0%	9%	76%	100%
Cybersecurity Risk Manager	1	61	11	73	0%	38%	0%	8%	54%	100%
Cybersecurity Educator	0	2	0	2	4%	15%	63%	7%	11%	100%
Cyber Incident Responder	0	13	1	14	6%	25%	0%	3%	66%	100%
Cyber Legal, Policy & Compliance Officer	2	15	0	17	56%	33%	4%	4%	4%	100%
CISO	28	167	9	204	5%	86%	2%	2%	5%	100%
Cybersecurity Architect	4	51	2	57	5%	24%	0%	0%	71%	100%
Cybersecurity Implementer	22	225	66	313	0%	17%	0%	0%	83%	100%
Cybersecurity Auditor	9	26	1	36	7%	23%	0%	0%	70%	100%
Total	118	727	106	951	8%	30%	5%	9%	48%	100%
CS - High	52	243	10	305	-	-	-	-	-	-
CS - Middle	93	388	56	537	-	-	-	-	-	-
CS - Low	388	1728	455	2571	-	-	-	-	-	-
Total	651	3086	627	4364						

Figure 42: Building blocks within the junior vacancies 2022

We see that some profiles, such as the Cyber Security Implementer and the Penetration Tester, rely more on technical knowledge and skills. Other functions, such as the CISO and the Cyber Risk Manager, have a greater reliance on knowledge and skills in terms of Management & Organisation.

The extent to which these building blocks are addressed varies across the different courses. For the full cyber security training courses, it has been assumed for convenience that they should reasonably be able to apply for the junior position of all ECSF profiles and that the missing knowledge can be acquired while in the position. This will not apply in all cases of course.

All “partly cyber security courses” are labelled based on the amount of attention paid to the five types of competencies: 0 (no attention), 1 (some attention), 2 (substantial attention), or 3 (primary focus). An overview of the number of graduates who received at least substantial attention (i.e. score 2 or 3) for the type of competence within the training (Figure 43) can be seen below:

	2021-2022					
	Total		Hbo		Wo	
	Outflow	Inflow	Outflow	Inflow	Outflow	Inflow
1 Full CS	266	426	43	94	223	332
2. Partial CS - specialisation	610	706	389	387	221	319
- substantial attention for 'Technical' (>=2)	421	443	354	352	67	91
- substantial attention for 'M&O' (>=2)	240	312	86	84	154	228
- substantial attention for 'Legal' (>=2)	35	35	35	35	0	0
- substantial attention for 'Research' (>=2)	221	319	0	0	221	319
- substantial attention for 'Education' (>=2)	0	0	0	0	0	0
3. Partial CS - Compulsory component of >6 EC	1409	1940	785	1079	624	861
- substantial attention for 'Technical' (>=2)	514	742	140	164	374	578
- substantial attention for 'M&O' (>=2)	924	1206	730	983	194	223
- substantial attention for 'Legal' (>=2)	619	784	369	501	250	283
- substantial attention for 'Research' (>=2)	541	704	0	0	541	704
- substantial attention for 'Education' (>=2)	0	0	0	0	0	0

Figure 43: Inflow and outflow per category of cyber security training (full – specialisation – mandatory component)

There is plenty of job market demand for “Technical” and “Management & Organisation” competencies. It is the same for courses with a cyber security specialisation. The focus on “legal” is mainly found in courses in which cyber security is not a specialisation, while the focus on “teaching” competencies is not found anywhere. In principle, there appears to be no job market demand for “Cyber Educators” at the junior level, so this does not seem to be a problem at all. Educating and training other people in cyber security is therefore a competence that people only seem to develop once they enter the job market.

A general point of attention is the extent to which one can still be relatively easily retrained in a junior position after completing a training course. If the gap is too large, the organisation in question can no longer hire the graduate. This qualitative mismatch is difficult to capture in vacancy numbers and graduate numbers.

5.3 Intermediate/senior functions

Outflow from regular education cannot be used for intermediate and senior positions. This category in particular needs a review of such aspects as learning-on-the-job, autonomous learning, and private training and retraining.

For these functions, professionals who are already active on the job market and who have a sufficient basis to enter the relevant intermediate or senior position need to be reviewed. For intermediate professionals, these will often be juniors “within the same profile” (vertical development) or lateral entrants who have already developed well in some of the required competencies. The same generally applies to senior positions, with inflow/through flow from intermediate positions with a comparable profile or lateral entrants (e.g. good managers who want to shift their focus to the cyber security domain).

It is particularly important to pay attention to development paths for the intermediate and senior level cyber security job market. From which position can someone enter the intermediate or senior position in question? The difference between the position someone comes from and the position someone will go into cannot be too large; there must be a “bridgeable gap”. The “gap” between two functions depends on the knowledge and skills (and required personality) across the board.

For illustration, a simplified example will be used using the CISO profile, which involves two components: [1] management skills and [2] (technical) cyber security knowledge. The following scenarios could occur in this simplified example:

- If someone masters both components, the person immediately qualifies.
- If someone is missing both components, the gap will be too big.
- If someone has knowledge about cyber security, but no/insufficient management skills, the question now becomes whether they can learn/develop the management skills. This will come naturally for some, for others it can be developed, and for some this will never be a competence they become good at.
- If someone does not have the required cyber security knowledge, but does have sufficient management skills, the question now is whether they can acquire sufficient cyber security knowledge in the foreseeable future to fulfil the position successfully. Chapter 4 described how much of a CISO's job and skill set is non-technical in nature. Choosing who might be suitable for the transition will probably depend on how big the "gap" is.

This principle of bridgeable gaps can also be projected onto cyber security professions. The visualisation below, in which two professions are connected with a line when the gap can be bridged (Figure 44), is for ICT professions in a generic sense. When zooming in on the profiles, it quickly becomes clear that not all professions A can be transferred to professions B. If the inflow for a specific cyber security profile at intermediate or senior level needs to be increased, it is important to look carefully at which backgrounds provide a sufficient basis to bridge the gap.

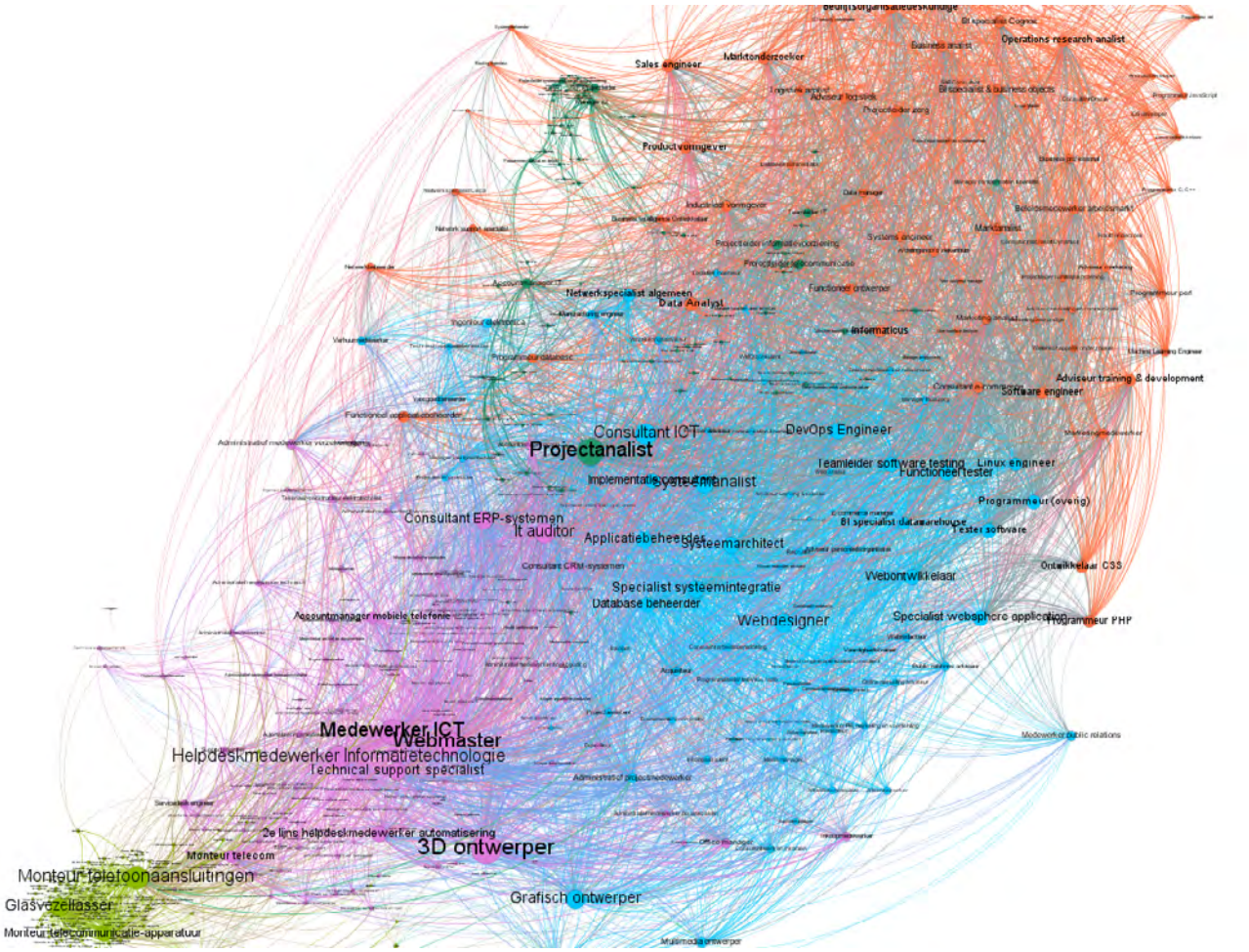


Figure 44: Transition professions, calculated from the destination profession (an ICT profession). Source: pr-eDICT, data provided by CentERdata. Edited by Dialogic

As described in Chapter 3, there is a wide range of Life-Long Learnings. The importance of certificates in the cyber security job market is great, especially for the more specialised cyber security profiles. These certificates and their associated training courses are a way to bridge the gap.

5.4 Conclusion

The following conclusions have been drawn:

Starter functions:

- For many functions there is a gap between what is required and how people emerge from the "training benches". There are many non-entry level positions. This gap needs to be bridged. **The idea that education and (all) the actual vacancies on the job market could match perfectly is a misconception**; this is because additional learning is required over several years and in different contexts.
- There are **relatively too few HBO and University graduates with a specialist cyber security profile**.
- The number of Higher Education graduates with a **"substantial" cyber security component in their training is actually at the same level**.
- The quantitative demand for **MBO cyber security junior personnel is at the same level as the outflow** in the two relevant MBO Level 4 courses.
- There is plenty of job market demand for **"Technical" and "Management & Organisation" competencies**. We also see these building blocks in courses with a specialisation in cyber security.
- The **focus on "legal"** is mainly found in courses where **cyber security is not a specialisation**.
- The focus on **"teaching" competencies is not reflected anywhere**, not in the training courses or the junior level vacancies.

Intermediate/senior positions:

- It is always a requirement to send people with a good foundation into the job market, but a **major issue for cyber security seems to lie mainly in Life-Long Learning**.
- The difference between the position someone comes from and the position someone wants to move into cannot be too great; there must be a "bridgeable gap". It is important to look carefully at **which backgrounds provide sufficient basis to bridge the gap**.
- The importance of cyber security certificates in the job market is great, especially for the more specialised cyber security profiles. These **certificates and their associated training courses are a way to bridge the gap**.

5.5 Points of attention for further consideration

Answering research questions 1 to 8 provides insight into the supply and demand side of the cyber security job market. The following factors, among others, play a role in the advice:

Education

- The regional differences in job market demand are large: how does this affect the training offer? Will this be taken into account and if so how?
- There is a demand for different profile types: from the hybrid/multi-disciplinary profile to the cyber specialist profile. How does this demand relate to the current and future range of courses? How can educational institutions deal with this?

Job Market

- Companies that are unaware of the (future) risks currently have no demand. This could represent a large latency in the demand. There is a difference between need and demand.
- There is a chain dependency on suppliers; this means large companies have a responsibility to get smaller companies on board.
- Many of the vacancies come from large companies – smaller companies do not seem to be fully aware of this yet, have fewer requirements, and those requirements are different. Often this will involve hybrid functions. How do we ensure there are many people in the job market with a broader scope?
- The regional differences in the job market create a concentrated question: what do the regional differences mean for the policy instruments to be deployed?

International:

- Labour migration: 5-15% of the inflow comes from migrant workers. What policy instruments can be used in a scenario with high/low labour migration?

- This question also applies to cyber security training: what policy instruments can be used in a scenario with a high/ low labour migration?

Future developments:

- The expected consequences of the arrival of the NIS2 directive on the job market are addressed in Chapter 4. The implications of this new legislation are still unknown at the organisational level. The size of this expected growth is difficult to estimate: how can this be dealt with?

Connection education – junior function:

- How can students be prepared for a junior position in cyber security, e.g.:
  a. by participating in specific task responsibilities after the training, such as an implementer;
  b. Setting up traineeships;
  c. Include more work-based learning in education so students can develop additional skills that are not necessarily technical in nature, but are more related to being able to collaborate, linking content to the organisational context, etc.;
  d. Include the most requested certificates in regular education.

6. Finally, how have we developed the advice?

6.1 Introduction

This report provides a wealth of input, which in turn provides a deeper insight into the extent to which education and the job market are aligned in terms of cyber security and the movements seen in the job market. This information provides a good overview of the current situation, as well as for the past 5 years; it is therefore an important starting point for further policy advice. This chapter provides a preview of the development of the advice and the accompanying implementation plan.

6.2 Approach and conceptual framework for advice

These results inform stakeholders from education, business, and parties involved in Human Capital activities during their discussions held in several meetings in January 2024 about the (policy) instruments that can be used, in what way they should be implemented, and by whom.

The conceptual framework shown below (Figure 45), which provides an image of the entire education-job market chain, was used for this. The most crucial points to pay attention to are:

A. Inflow and outflow of cyber security education: what can we do to get more students interested in a cyber security education and then provide them with the right skills and knowledge so they are trained in such a way that their skills match the demand for junior positions on the job market?
B. Retraining and refresher training for cyber security “entry-level roles”: What can we do to retrain recent graduates from non-cyber-related education to make them available for a cyber role? Which educational background offers the best chance of success?
C. Horizontal development towards cyber security professionals: how can we retrain and up-skill intermediate and senior professionals in a non-cyber function to a cyber function? For which functions is this most promising and what is required to achieve it?
D. Vertical development of cyber security professionals: how can we ensure linear flow up the chain from junior to intermediate to senior positions so professionals can grow?
E. Retaining cyber security graduates and cyber security professionals: what is required to minimise outflow and retain professionals in the cyber security job market?
F. Labour migration: how many cyber professionals come to work in the Netherlands from abroad? How many Dutch cyber professionals leave the Netherlands to work abroad? What can and do we want to do about the relatively large international influx into the cyber security job market?
G. Attention to cyber security among non-cyber security professionals: how much attention is paid to cyber security by non-cyber security professionals? Can we increase this, and what does that mean for the entire job market chain?

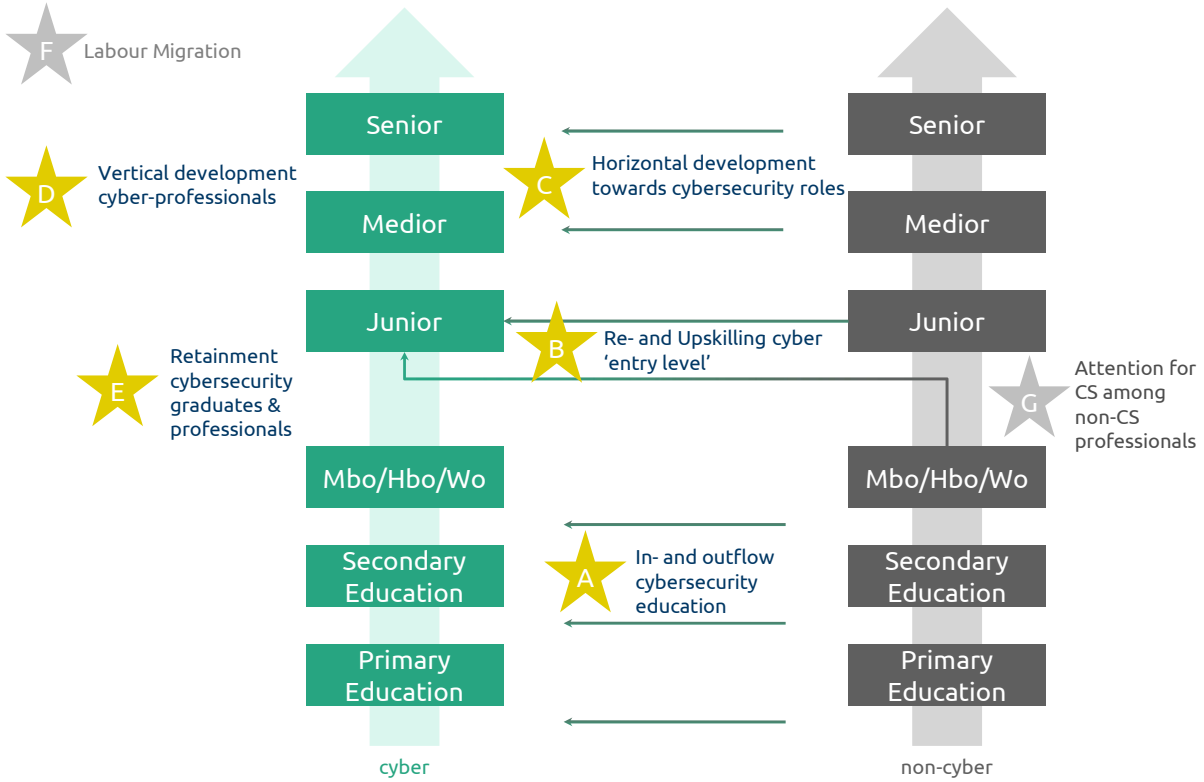


Figure 45: Conceptual framework that provides an image of the total education-job market chain

During the next phase of this research, the crucial points laid out above are discussed with various stakeholders to determine the (policy) instruments that can be used, based on the answers to research questions 1 to 8.
For a detailed approach and development of the advice, including implementation, please refer to the second part of this research: the advice report.

Contact information

Platform Talent for Technology contact person:
Marion Sieh
m.sieh@ptvt.nl

Dialogic contact person:
Arthur Vankan
vankan@dialogic.nl

Postal address:
Platform Talent for Technology
Postbus 76
2501 CB Den Haag

Visiting address:
Oranjebuitensingel 6 (4th floor)
2511 VE Den Haag

Appendices

Appendix 1. Methodological justification of the job market

This appendix explains the methodological choices for identifying the "cyber security job market" sector.

Identifying cyber security vacancies

The searched vacancies were purchased from Jobdigger. The analysis of the "cyber security job market" is based on ICT sector vacancies as defined in pr-edict and vacancies outside the ICT sector. Looking beyond the ICT sector is also necessary because the cyber security sector has a strong multi-disciplinary character. This means it is likely that cyber security functions will also be in demand in other sectors.

The presence of the cyber security-related terms shown in Supplementary Table 1 was used to search through the vacancies. The vacancies were then randomly reviewed to determine how many cyber security-related terms must appear in a vacancy before it can be considered a cyber security vacancy. During this search, it turned out that relevant cyber security vacancies sometimes contained only one cyber security-related term. A vacancy is therefore included in the analysis if it contains at least one cyber security-related term. Increasing the threshold is likely to lead to more true positive vacancies being removed than false positive vacancies being removed, which will only decrease the quality of the sample. The choice was therefore made to include a (slight) overestimation of the number of cyber security vacancies.

Cyber security-related terms
Cyber
Information Security
Information security
Netwerkbeveiliging
Netwerk security
Network security
Cloud security
cloudbeveiliging
IT-security
IT-security
Databeveiliging
Data security
Digitale veiligheid
Digitale beveiliging
Digitale crim

Supplementary Table 1: Cyber security-related terms for identifying cyber security vacancies

Identification of job profiles

The (slight) overestimation of the number of cyber security vacancies was countered by classifying the vacancies against the degree of cyber security relevance per job profile. This means the job titles were cleaned up and re-aggregated into (where possible) an ECSF profile. The operationalisation described in Supplementary Table 2 was used for this. A job title containing the terms in the right column has been upgraded to the ECSF profile in the left column.

ECSF profile	Mapping of job titles
Chief Information Security Officer (CISO)	security & officer or functionaris & informat or informat & security or functionaris & beveiliging or ciso or chief information security
Penetration Tester	security & tester or pen-tester or penetration or ethical hacker
Cyber Security Implementer	security & implement or security & engineer or cyber & engineer or IT & engineer or system & engineer or devops & engineer or cloud & engineer or network & engineer or netwerk & engineer or solution & engineer
Cyber Security Researcher	onderzoeker & security or onderzoeker & cyber or research & security or phd or postdoc or post doc
Cyber Security Risk Manager	risk manager & security or risk manager & informat or security & analist or informat & analist or security & assessor
Cyber Security Architect	solution & architect or data & architect or security & architect or infra & architect or IT & architect
Cyber Legal, Policy & Compliance Officer	compliance & risk or compliance & security or compliance & analist or GRC or protection & officer or policy & officer or IT & beleid or beveiliging & beleid or functionaris & bescherming
Digital Forensics Investigator	forensic
Cyber Incident Responder	incident & response or cyber & defense or crisis & manage or siem & engineer or incident & security
Cyber Security Auditor	audit & security or audit & IT
Cyber Security Educator	security & trainer or docent & security or security & awareness
Cyber Threat Intelligence Specialist	cyber & threat or threat & analyst or cyber & intelligence or cyber & threat or cyber & specialist or security & specialist

Supplementary Table 2: Mapping of job titles to ECSF profiles

For each job title not linked to an ECSF profile, the degree of cyber security relevance was determined by looking at the number of cyber security-related terms per vacancy. A manual inspection was used to develop the following categorisation:

- High cyber security relevance: Job titles with an average of 6 or more cyber security-related terms per vacancy.
- Moderate cyber security relevance: Job titles with an average of between 3 and 5.9 cyber security-related terms per vacancy.
- Low cyber security relevance: Job titles with an average of less than 3 cyber security-related terms per vacancy.

This categorisation was used in the breakdowns to provide a fair representation of the vacancy sample.

Identification of specific knowledge and skills

After identifying the cyber security vacancies and categorising the job titles, a search was carried out on the vacancies for the presence of specific tasks, skills and knowledge from within the cyber security domain. These "building blocks" are defined for each profile in the ECSF. The extent to which the building blocks are relevant and for which functions was quantified for each building block. The definition of these search terms was operationalised via two routes, see Supplementary Figure 1.

Supplementary Figure 1: Putting tasks, skills and knowledge into practise

For route 1, the search terms were created by intelligently querying ChatGPT. Questions were formulated for each building block category (Deliverables, Main task(s), Key skill(s) and Key knowledge) and ChatGPT provided search terms as suggestions. Information about the building block was automatically provided for these questions, and ChatGPT generated relevant search terms for each building block. These search terms were automatically translated into Dutch by ChatGPT. Because the sample contains both English and Dutch vacancies, it is important to operationalise the search terms in both languages. This resulted in a set of approximately 20,000 search terms. These terms were manually reviewed for precision. Precision indicates a degree of certainty. When a search term found in a vacancy has high precision for a building block, it can be certain that the building block is actually present in the vacancy. This therefore demonstrates how specific a search term is. Only search terms with high precision were used for the analysis. By using high precision search terms, the number of false positives was minimised.
In route 2, search terms were manually created in the form of queries. A query is a combination of related terms. The idea behind this is that a combination of terms can signal the presence of a building block. This involves a combination of terms; therefore, fewer specific terms can be used compared to route 1. Tabel 3 shows the operationalisation of the queries in this research. At least one term for each building block is entered into the first set of search terms (set A); the other sets are optional. The **search terms within a set** have an OR relationship; the **sets** have an AND relationship with each other. Using Tabel 3 we can work out an example. According to the this method, Building Block A can be considered as being present in a vacancy when Term 2, Term 3 and Term 4 can be found in a vacancy. However, this building block is also present when Term 1, Term 3 and Term 5 are present in a vacancy. The point is that at least one term per (completed) set is present in the vacancy.

Table 3 Operationalisation manual queries	Set A	Set B	Set C	Set D	Specific cyber security term
Building Block A	Term 1, Term 2	Term 3	Term 4, Term 5		
Building Block B	Term 6				Term 7

Supplementary Table 3: Operationalisation manual queries

Finally, the results of both routes were combined. If a building block is present in the vacancy according to at least one of the two routes, it is included as such in the analysis.

Appendix 2. Tables related to education

Tables related to MBO in Paragraph 3.3

Tables related to the results of the survey among ICT training managers

grade	number of respondents
1	
2	
3	2
4	
5	3
6	1
7	2
8	
9	3
10	3

(N= 14)

Supplementary Table 4: What grade do you give for the commitment to cyber security within your own ICT training courses?

	Never		Occasionally		Regularly		Frequently		Always		Total	Weighted average
Guest lectures	20,00%	2	50,00%	5	20,00%	2	0,00%	0	10,00%	1	10	2,3
Group assignments	30,00%	3	30,00%	3	20,00%	2	10,00%	1	10,00%	1	10	2,4
Individual practical assignments	20,00%	2	0,00%	0	40,00%	4	10,00%	1	30,00%	3	10	3,3
Specific subjects/ modules	30,00%	3	20,00%	2	10,00%	1	20,00%	2	20,00%	2	10	2,8
BPV	20,00%	2	30,00%	3	30,00%	3	10,00%	1	10,00%	1	10	2,6
Other	33,33%	3	33,33%	3	33,33%	3	0,00%	0	0,00%	0	9	2

Supplementary Table 5.1: ICT Support Level 2 Employee: To what extent is or can cyber security be a topic?

	Never		Occasionally		Regularly		Frequently		Always		Total	Weighted average
Guest lectures	20,00%	3	46,67%	7	26,67%	4	0,00%	0	6,67%	1	15	2,27
Group assignments	20,00%	3	26,67%	4	20,00%	3	20,00%	3	13,33%	2	15	2,8
Individual practical assignments	13,33%	2	20,00%	3	6,67%	1	40,00%	6	20,00%	3	15	3,33
Specific subjects/ modules	13,33%	2	20,00%	3	26,67%	4	13,33%	2	26,67%	4	15	3,2
BPV	6,67%	1	33,33%	5	40,00%	6	0,00%	0	20,00%	3	15	2,93
Other	46,67%	7	20,00%	3	13,33%	2	6,67%	1	13,33%	2	15	2,2

Supplementary Table 5.2: Software Developer Level 4: To what extent is or can cyber security be a topic?

	Never		Occasionally		Regularly		Frequently		Always		Total	Weighted average
Guest lectures	8,33%	1	58,33%	7	16,67%	2	8,33%	1	8,33%	1	12	2,5
Group assignments	0,00%	0	41,67%	5	25,00%	3	8,33%	1	25,00%	3	12	3,17
Individual practical assignments	0,00%	0	25,00%	3	16,67%	2	25,00%	3	33,33%	4	12	3,67
Specific subjects/ modules	8,33%	1	16,67%	2	33,33%	4	0,00%	0	41,67%	5	12	3,5
BPV	8,33%	1	33,33%	4	25,00%	3	0,00%	0	33,33%	4	12	3,17
Other	50,00%	5	30,00%	3	0,00%	0	0,00%	0	20,00%	2	10	2,1

Supplementary Table 5.3: All-round IT System & Device Level 4: To what extent is or can cyber security be a topic?

	Never		Occasionally		Regularly		Frequently		Always		Total	Weighted average
Guest lectures	7,14%	1	64,29%	9	14,29%	2	7,14%	1	7,14%	1	14	2,43
Group assignments	0,00%	0	28,57%	4	28,57%	4	21,43%	3	21,43%	3	14	3,36
Individual practical assignments	0,00%	0	14,29%	2	7,14%	1	50,00%	7	28,57%	4	14	3,93
Specific subjects/ modules	0,00%	0	14,29%	2	21,43%	3	14,29%	2	50,00%	7	14	4
BPV	0,00%	0	35,71%	5	28,57%	4	7,14%	1	28,57%	4	14	3,29
Other	22,22%	2	44,44%	4	11,11%	1	0,00%	0	22,22%	2	9	2,56

Supplementary Table 5.4: IT System & Device Expert Level 4: To what extent is or can cyber security be a topic?

Answer choices	Reactions	
Sufficient teachers	50,00%	7
Professionalisation of teachers	71,43%	10
Teaching and examination material	64,29%	9
Hybrid learning workplaces	42,86%	6
Cooperation from the profession, e.g. through guest lectures, company visits, practical assignments	71,43%	10
Other (please explain)	14,29%	2
Total number of respondents: 14		

Supplementary Table 6: What do you (still) need in order to be able to provide up-to-date cyber security education? (multiple answers possible)

	Certainly requires more attention		Already gets enough attention		N/A		Total	Weighted average
Security of networks and systems, users, software and devices	28,57%	4	64,29%	9	7,14%	1	14	1,69
Data awareness	57,14%	8	35,71%	5	7,14%	1	14	1,38
BI	78,57%	11	7,14%	1	14,29%	2	14	1,08
Cloud	28,57%	4	64,29%	9	7,14%	1	14	1,69
Collaboration tooling	50,00%	7	35,71%	5	14,29%	2	14	1,42
Privacy	35,71%	5	57,14%	8	7,14%	1	14	1,62
Soft skills (collaboration, ethical and honest behaviour, dealing with pressure, etc.)	28,57%	4	64,29%	9	7,14%	1	14	1,69
Total number of respondents: 14								

Supplementary Table 7: Can you state whether the cyber security themes below should receive more attention in your training courses in the future?

Higher Education tables – Paragraph 3.4

	2019-2020 inflow	2019-2020 outflow	2020-2021 inflow	2020-2021 outflow	2021-2022 inflow	2021-2022 outflow	2022-2023 inflow	2022-2023 outflow	2023-2024 inflow
De Haagse Hogeschool	**10**	**10**	**10**	**10**	**12**	**7**	**11**		**14**
m Cyber Security Engineering (post-initiele master)	10	10	10	10	12	7	11		14
Hogeschool INHOLLAND									**40**
Ad Cybersecurity part-time									16
Ad Cybersecurity full-time									24
Hogeschool Utrecht									
Ad Cybersecurity									
Hogeschool van Amsterdam	**51**	**0**	**80**	**19**	**82**	**36**	**90**		
Ad Cybersecurity	51	0	80	19	82	36	90		
NHL Stenden Hogeschool									
Ad Cyber Safety & Security									
Universiteit Leiden	**261**	**83**	**298**	**123**	**280**	**193**	**284**	**217**	**257**
b Security Studies	237	65	281	107	265	174	269	207	249
m Cyber Security (post-initiele master)	24	18	17	16	15	19	15	10	8
Universiteit Maastricht									
m Advanced Master in Privacy, Cybersecurity, Data Management and Leadership (post-initiele master)									
Universiteit van Amsterdam	**44**	**47**	**26**	**26**	**34**	**25**	**38**		
m Security and Network Engineering part-time	13	18	5	7	14	5	10		
m Security and Network Engineering full-time	31	29	21	19	20	20	28		
Vrije Universiteit Amsterdam	**5**	**10**	**10**	**7**	**18**	**5**	**13**		
m Computer Security	5	10	10	7	18	5	13		
Total	**371**	**150**	**424**	**185**	**426**	**266**	**436**	**217**	**311**

Supplementary Table 9: Overview of Higher Education study programmes with a cyber security specialisation or elective

	2019-2020 inflow	2019-2020 outflow	2020-2021 inflow	2020-2021 outflow	2021-2022 inflow	2021-2022 outflow	2022-2023 inflow	2022-2023 outflow	2023-2024 inflow
Chr. Hogeschool Windesheim	**59**	**59**	**76**	**76**	**68**	**68**	**60**	**60**	
Infrastructure Design and Security (b HBO ICT)	59	59	76	76	68	68	60	60	
De Haagse Hogeschool									
Information Security Management (b HBO ICT)									
Erasmus Universiteit Rotterdam					**49**	**49**	**49**	**49**	
Data Privacy and Cyber Security (m business information management)					49	49	49	49	
Fontys Hogescholen	**58**	**58**	**57**	**57**	**66**	**66**	**177**	**72**	**78**
ICT & Infrastructure (Associate Degree ICT)	0	0	0	0	0	0	64	0	14
ICT & Cyber Security (b HBO ICT)	58	58	57	57	66	66	113	72	64
Hanzehogeschool Groningen									
Software Engineering (b HBO ICT)									
Hogeschool INHOLLAND	**25**	**25**	**29**	**29**	**20**	**20**	**24**	**18**	**6**
Security (b computer science)	25	25	29	29	20	20	9	9	
Information Security Officer (b Safety & Security Management)							15	9	6
Hogeschool Rotterdam	**35**	**35**	**35**	**35**	**35**	**35**	**35**	**35**	**35**
Privacy, Security, Risk (B Business IT & Management)	35	35	35	35	35	35	35	35	35
Hogeschool Utrecht	**39**	**39**	**40**	**40**	**47**	**47**	**9**	**9**	
Cyber Security & Cloud (b HBO ICT)	39	39	40	40	47	47	9	9	
Information Security (b Safety & Security Management)									
Hogeschool van Amsterdam	**26**	**26**	**50**	**50**	**47**	**47**	**66**	**66**	
Cyber Security (b HBO ICT)	26	26	50	50	47	47	66	66	
Hogeschool van Arnhem en Nijmegen	**47**	**32**	**58**	**40**	**49**	**51**	**49**	**32**	

Infrastructure & Security Management (b HBO ICT)	47	32	58	40	49	51	49	32	
NHL Stenden Hogeschool									
Certified Ethical Hacking (b (technical) computer science)									
Secure Programming (b (technical) computer science)									
Hack@Sea (b (technical) computer science)									
Radboud Universiteit Nijmegen									
Cyber security (b computer science)									
Cyber Security (m computer science)									
Cyber Security and AI (m computer science)									
Security or Privacy Office (m information sciences)									
Saxion Hogeschool									
Infrastructure (b HBO ICT)									
Cyber Security (not related to one specific programme)									
Techn. Universiteit Eindhoven	**83**	**64**	**87**	**65**	**88**	**64**	**69**	**22**	
Information Security Technology (m computer science and engineering)	23	10	29	12	27	20	25	22	
Cyber-Physical systems (m embedded systems)	60	54	58	53	61	44	44		
Technische Universiteit Delft									
Cyber Security (m computer science)									
Universiteit Leiden	**0**	**0**	**184**	**54**	**179**	**105**	**171**	**89**	
Cyber Security (m Crisis and Security Management)	0	0	184	54	179	105	171	89	
Universiteit Twente									
Cyber Security (m computer science)									

Vrije Universiteit Amsterdam	**7**	**21**	**5**	**7**	**3**	**3**			
Security (m computer science (joint degree))	7	21	5	7	3	3			
Zuyd Hogeschool					**55**	**55**	**21**	21	45
Cyber Security (b HBO ICT)					55	55	21	21	45
Total	**379**	**359**	**621**	**453**	**706**	**610**	**730**	**473**	**164**

Supplementary Table 9: Overview of Higher Education study programmes with a cyber security specialisation or elective

	2019-2020 inflow	2019-2020 outflow	2020-2021 inflow	2020-2021 outflow	2021-2022 inflow	2021-2022 outflow	2022-2023 inflow	2022-2023 outflow	2023-2024 inflow
Avans Hogeschool	**89**	**60**	**97**	**82**	**68**	**85**	**82**		
b business it & management part-time	22	13	21	31	18	20	19		
b Business IT & Management full-time	67	47	76	51	50	65	63		
De Haagse Hogeschool	**298**	**119**	**284**	**146**	**282**	**136**	**248**		
b Safety & Security Management part-time	24	13	24	26	32	11	25		
b Safety & Security Management dual	141	64	142	71	112	76	103		
b Safety & Security Management full-time	133	42	118	49	138	49	120		
Hogeschool INHOLLAND			**405**	**330**	**350**	**290**	**310**	**230**	**250**
B Safety & Security Management			405	330	350	290	310	230	250
NHL Stenden Hogeschool	**273**	**162**	**307**	**161**	**247**	**134**	**251**		
b HBO ICT part-time	26	10	13	5	18	5	12		
b HBO ICT full-time	98	44	112	61	78	50	81		
b Safety & Security Management part-time	0	10	13	0	12	5	23		
b Safety & Security Management full-time	149	98	169	95	139	74	135		
Radboud Universiteit Nijmegen	**164**	**62**	**141**	**52**	**134**	**69**	**183**		
b computer science	164	62	141	52	134	69	183		
Rijksuniversiteit Groningen	**90**	**78**	**112**	**106**	**88**	**98**	**54**		
m it-law part-time	20	20	10	20	10	20	0		
m IT Law full-time	70	58	102	86	78	78	54		
Saxion Hogeschool	**181**	**98**	**203**	**128**	**132**	**140**	**120**		
b Safety & Security Management part-time	21	14	20	18	19	10	14		
b Safety & Security Management full-time	160	84	183	110	113	130	106		
Technische Universiteit Delft	**192**	**149**	**225**	**165**	**259**	**180**	**263**		

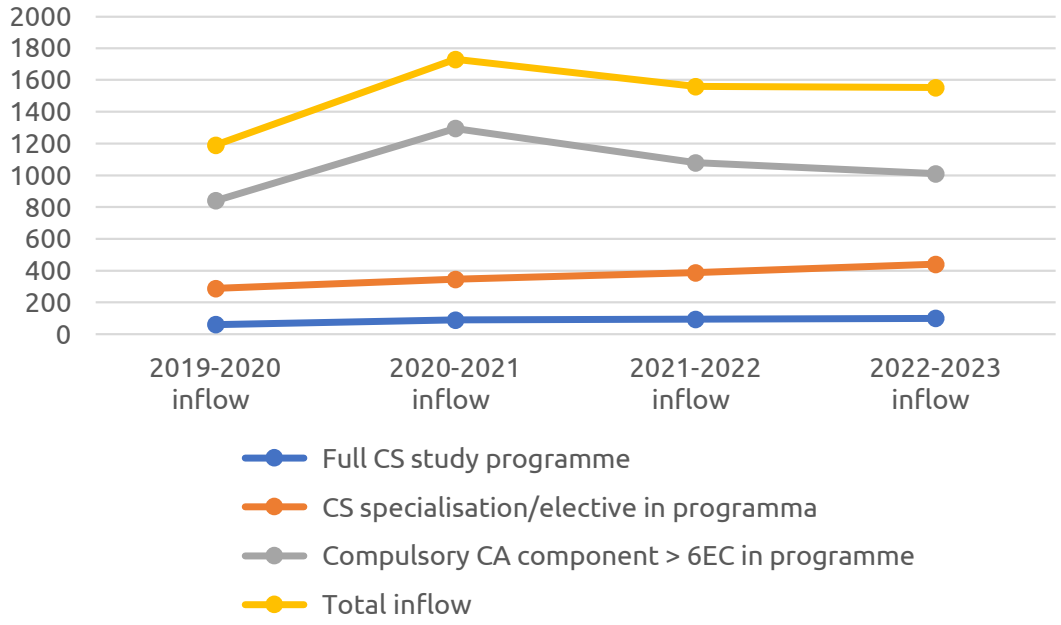
m Computer Science	192	149	225	165	259	180	263		
Tilburg University	**108**	**92**	**100**	**102**	**137**	**97**	**140**		
m Law and Technology	108	92	100	102	137	97	140		
Universiteit Leiden	**219**	**127**	**218**	**137**	**243**	**180**	**168**	**38**	**56**
b Computer Science full-time	141	68	149	70	157	83	108		
Law and Digital Technologies (Advanced Master Programme)	38	33	34	31	58	55	40	38	56
m ICT in Business and the Public Sector	40	26	35	36	28	42	20		
Total	**1576**	**914**	**2058**	**1378**	**1882**	**1354**	**1779**	**230**	**250**

Supplementary Table 10: Overview of Higher Education study programmes with a compulsory cyber security component (>6 ECTS)

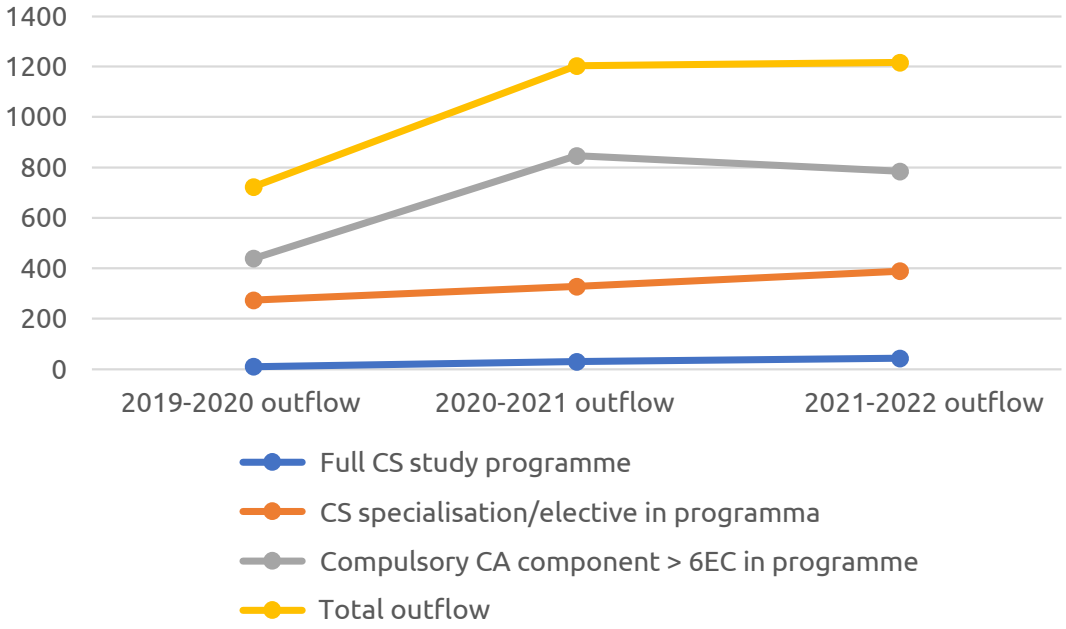
Upcoming courses
Avans Hogeschool
AI & Security learning community
De Haagse Hogeschool
Associate Degree Cyber Security
B cyber engineering
Hogeschool Leiden
M Digital Forensics
Hogeschool Utrecht
Associate Degree Cyber Security
B Digital Security
M Digital Security
MBO Rijnland
Cyber education
NHL Stenden Hogeschool
Associate Degree Cyber Safety & Security
Regional Training Centre ROC Aventus
Safety& Security
Regional Training Centre ROC Mondriaan
Cyber education
Universiteit Leiden
B Cyber Security and Cyber Governance/Cybercrime & Cyber Security

Supplementary Table 11: Overview of courses still in the development phase, accreditation phase or start-up phase.

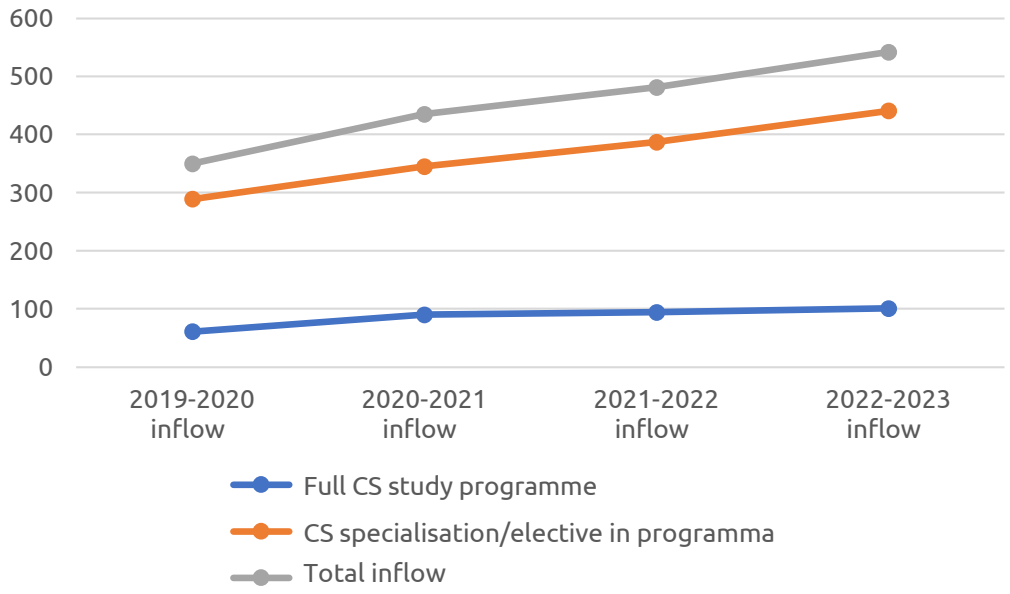
Inflow and outflow data for funded HBO Education



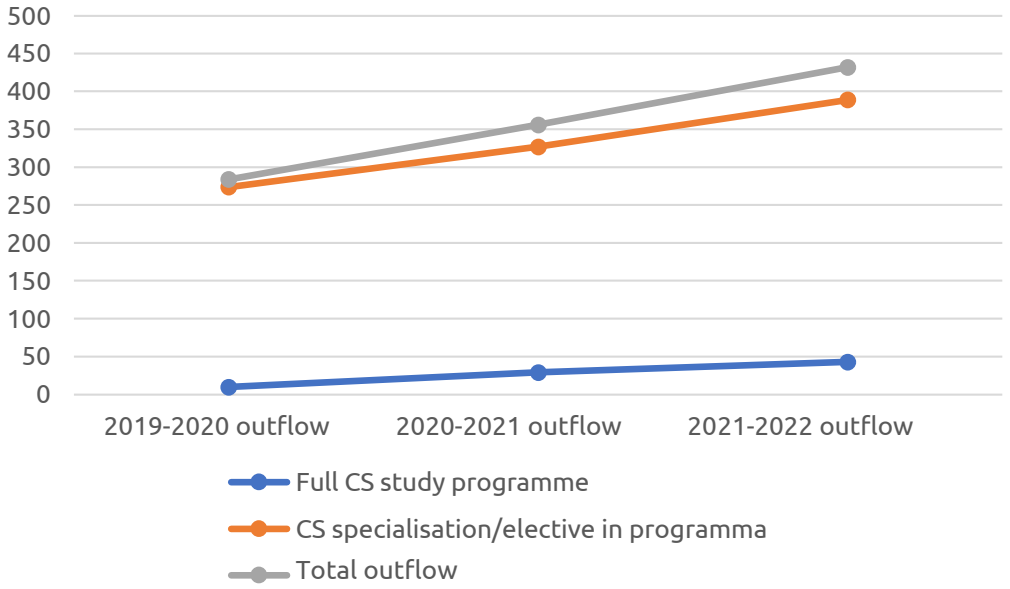
Supplementary Figure 2: Student intake over time, all HBO study programmes with a relevant cyber security component



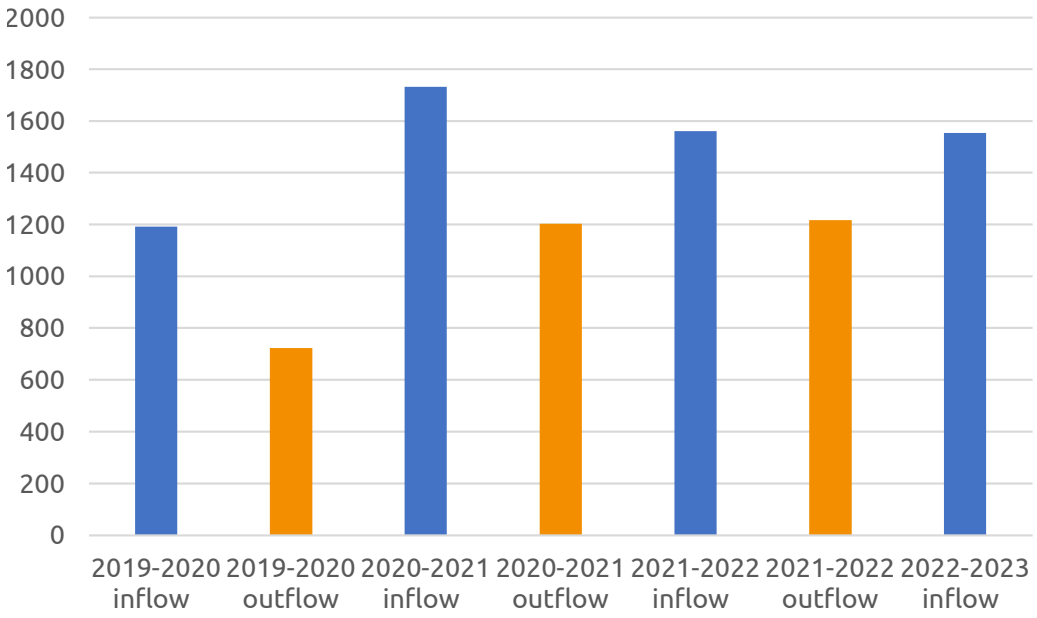
Supplementary Figure 3: Student intake over time, all HBO study programmes with a relevant cyber security component



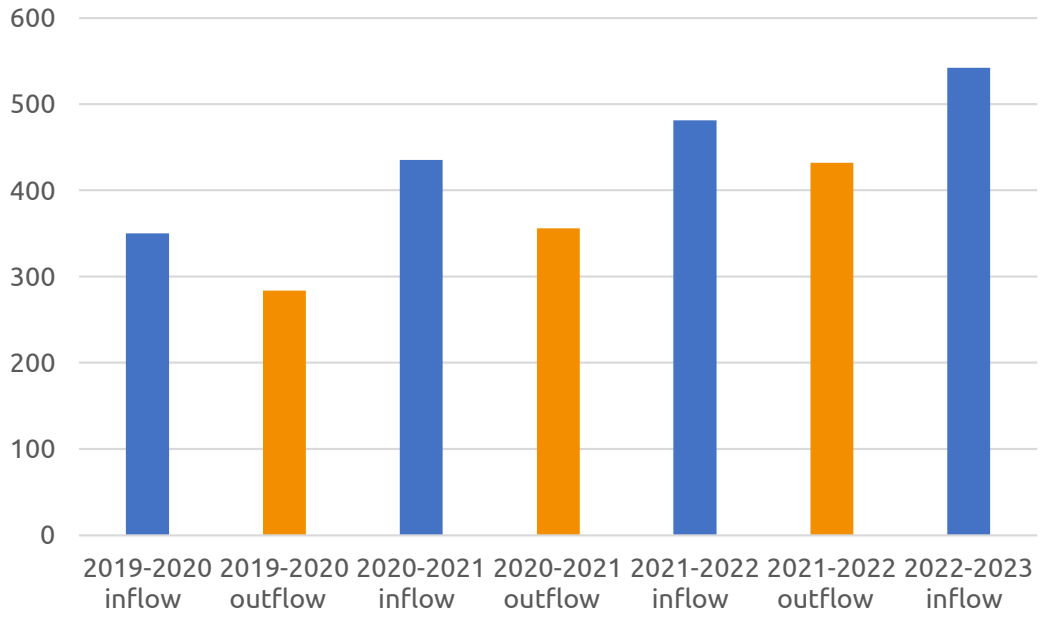
Supplementary Figure 4: Progress of student intake over time, students from HBO study programmes that are fully focused on cyber security and students who have chosen a cyber security specialisation/elective as part of their study programme



Supplementary Figure 5: Progress of student intake over time, students from HBO study programmes that are fully focused on cyber security and students who have chosen a cyber security specialisation/elective as part of their study programme

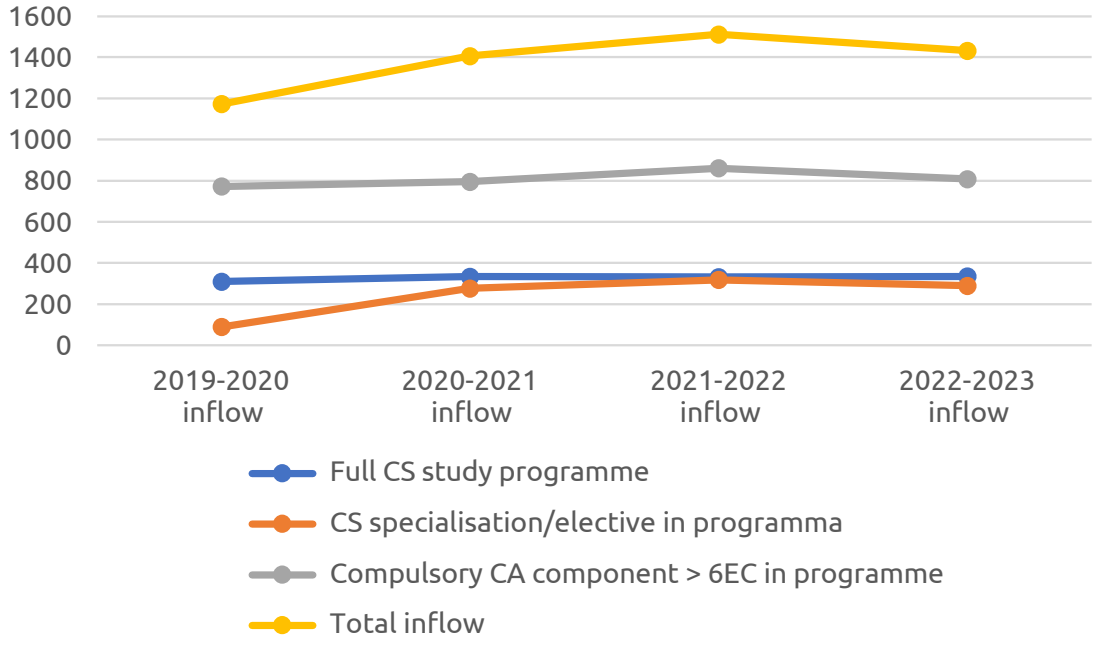


Supplementary Figure 6: Inflow versus outflow for all HBO study programmes with a relevant cyber security component

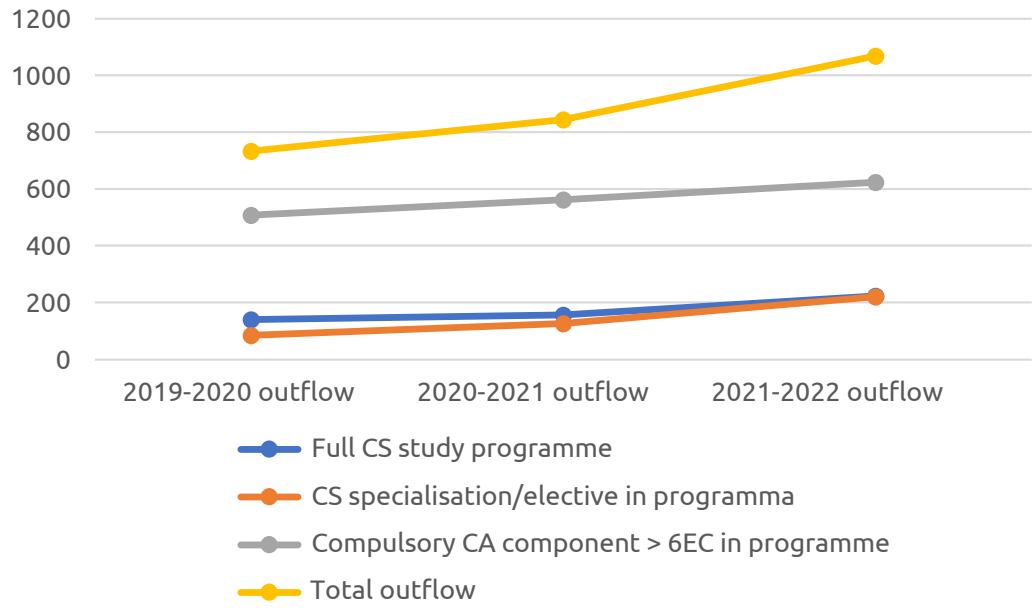


Supplementary Figure 7: Inflow versus outflow of university students who have followed a specific cyber security programme or a specific cyber security specialisation/elective.

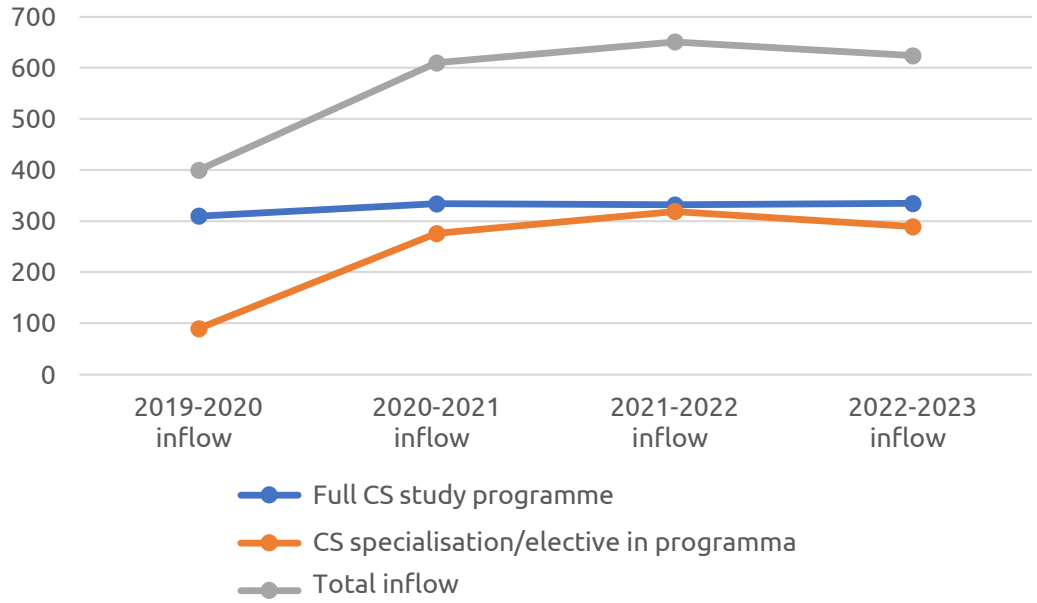
Inflow and outflow of funded University Education



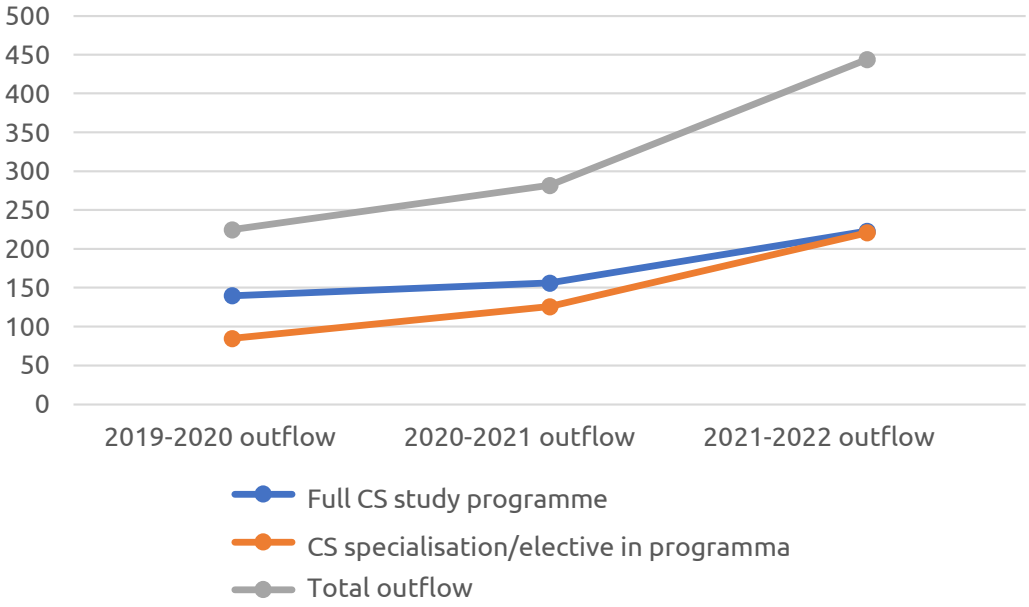
Supplementary Figure 8: Student intake over time, all University study programmes with a relevant cyber security component



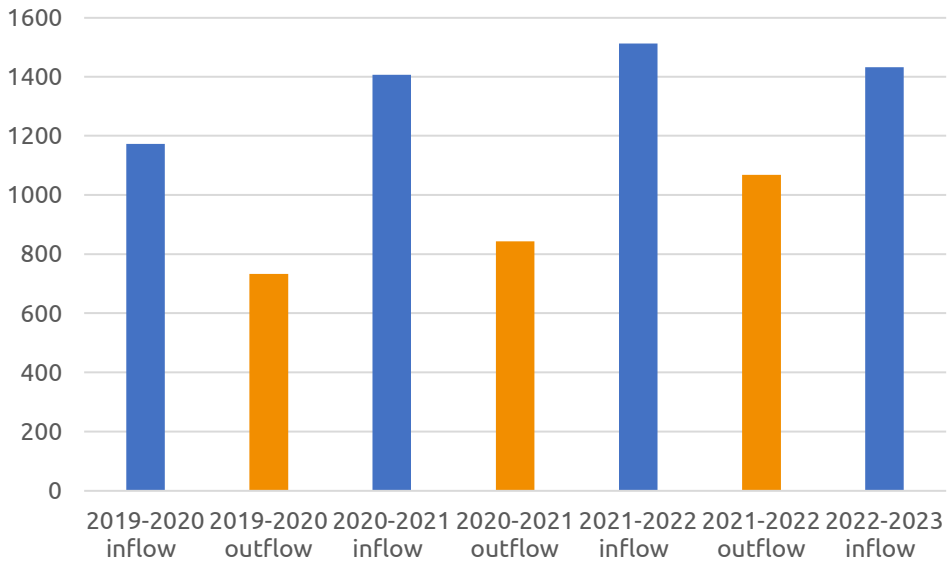
Supplementary Figure 9: Student intake over time, all University study programmes with a relevant cyber security component



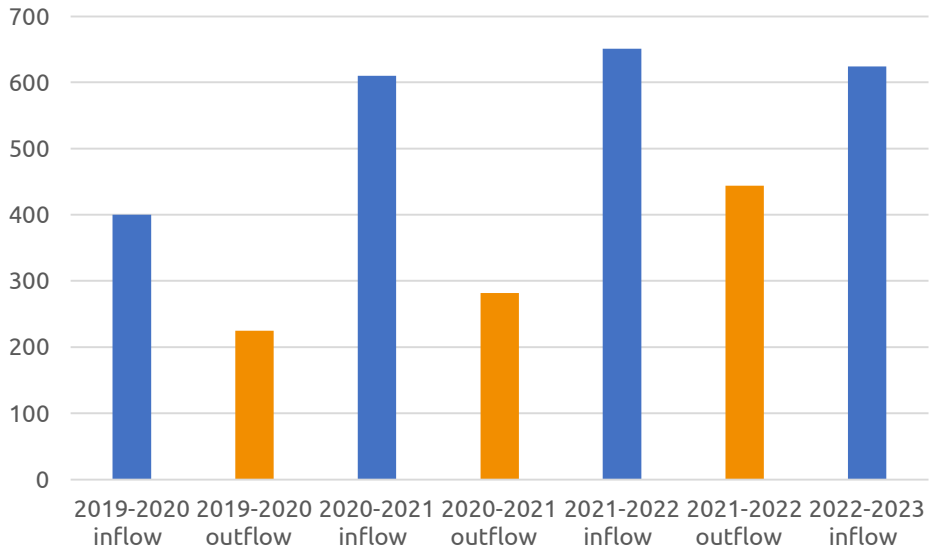
Supplementary Figure 10: Progress of student intake over time, students from University study programmes that are fully focused on cyber security and students who have chosen a cyber security specialisation/elective as part of their study programme



Supplementary Figure 11: Progress of student intake over time, students from University study programmes that are fully focused on cyber security and students who have chosen a cyber security specialisation/elective as part of their study programme



Supplementary Figure 12: Inflow versus outflow for all University study programmes with a relevant cyber security component



Supplementary Figure 13: Inflow versus outflow of university students who have followed a specific cyber security programme or a specific cyber security specialisation/elective.

Tables comparing the content of MBO and Higher Education courses in Paragraph 3.5

Education type	Setting	Current training course code	Course name	Share_ cyber security	Technical	M&O	Legal	Research	Education
MBO	MBO – generic	25604	Software Developer	Some	3	0	0	0	0
MBO	MBO – generic	25606	IT Systems and Devices Expert	Some	3	2	0	0	0
MBO	MBO – generic	25605	All-round IT Systems and Devices Employee	Some	3	1	0	0	0
MBO	MBO – generic	25607	ICT Support Employee	Some	3	0	0	0	0
University	Universiteit Leiden	75120	M Cyber Security (Post Master)	Full	3	3	3	2	0
University	Universiteit Maastricht	75150	M Advanced Master in Privacy, Cyber Security, Data Management and Leadership (Post Master)	Full	3	3	3	2	0
HBO	De Haagse Hogeschool	70207	M Cyber Security Engineering (Post Master)	Full	3	1	1	1	0
HBO	Hogeschool van Amsterdam	80156	Associate Degree Cyber Security	Full	3	1	0	1	0
University	Universiteit Leiden	59320	B Security Studies	Full	1	3	1	2	0
University	Universiteit Leiden	60417	M Crisis and Security Management	Some	1	3	1	2	0
University	Universiteit van Amsterdam	60227	M Security and Network Engineering full-time	Full	3	0	0	2	0
University	Universiteit van Amsterdam	60227	M Security and Network Engineering part-time	Full	3	0	0	2	0
University	Vrije Universiteit Amsterdam	60802	M Computer Security	Full	3	0	0	2	0
HBO	Saxion Hogeschool	39268	B Safety & Security Management full-time	Some	1	3	1	1	0

HBO	Saxion Hogeschool	39268	B Safety & Security Management part-time	Some	1	3	1	1	0
HBO	Hogeschool Utrecht	39268	B Safety & Security Management	Some	1	3	2	1	0
HBO	Hogeschool INHOLLAND	39268	B Safety & Security Management	Some	1	3	2	1	0
HBO	Hogeschool INHOLLAND	39268	B Safety & Security Management	Some	1	3	2	1	0
HBO	De Haagse Hogeschool	39268	B Safety & Security Management full-time	Some	1	3	1	1	0
HBO	De Haagse Hogeschool	39268	B Safety & Security Management part-time	Some	1	3	1	1	0
HBO	De Haagse Hogeschool	39268	B Safety & Security Management dual	Some	1	3	1	1	0
HBO	NHL Stenden Hogeschool	39268	B Safety & Security Management full-time	Some	1	3	2	1	0
HBO	NHL Stenden Hogeschool	39268	B Safety & Security Management part-time	Some	1	3	2	1	0
HBO	NHL Stenden Hogeschool	80185	Associate Degree Cyber Safety & Security	Full	3	3	1	1	0
HBO	Hogeschool INHOLLAND	80156	Associate Degree Cyber Security full-time	Full	3	2	3	1	0
HBO	Hogeschool INHOLLAND	80156	Associate Degree Cyber Security part-time	Full	3	2	3	1	0
HBO	Hogeschool Utrecht		Associate Degree Cyber Security	Full	3	2	1	1	0
HBO	Chr. Hogeschool Windesheim	30020	b HBO ICT	Some	3	0	0	1	0
HBO	Avans Hogeschool	39118	b Business IT & Management full-time	Some	2	3	0	1	0

HBO	Hogeschool Rotterdam	39118	b business it & management	Some	1	3	3	1	0
HBO	Saxion Hogeschool	30020	b HBO ICT	Some	3	0	0	1	0
HBO	Hanzehogeschool Groningen	30020	b HBO ICT	Some	3	2	1	1	1
HBO	Hogeschool Utrecht	30020	b HBO ICT	Some	3	1	0	1	0
HBO	Zuyd Hogeschool	30020	b HBO ICT	Some	3	1	0	0	0
HBO	Hs van Arnhem en Nijmegen	30020	b HBO ICT	Some	3	2	1	1	0
HBO	Hs van Arnhem en Nijmegen	34131	b embedded systems engineering full-time	Some	3	0	0	0	0
HBO	Hogeschool INHOLLAND	34479	b computer science	Some	3	1	1	1	0
HBO	De Haagse Hogeschool	30020	b HBO ICT	Some	3	2	1	1	0
HBO	Hogeschool van Amsterdam	30020	b HBO ICT	Some	3	1	0	1	0
HBO	Fontys Hogescholen	30020	b HBO ICT	Some	3	1	1	1	0
HBO	Fontys Hogescholen	34479	b computer science	Some	3	1	0	1	0
HBO	Fontys Hogescholen	80083	Associate Degree AD-ICT	Some	3	0	0	1	0
HBO	NHL Stenden Hogeschool	30020	b HBO ICT full-time	Some	3	1	0	1	0
HBO	NHL Stenden Hogeschool	34475	b technical computer science	Some	3	0	0	1	0
HBO	NHL Stenden Hogeschool	34479	b computer science	Some	3	0	0	1	0
University	Universiteit Leiden	56978	b Computer Science full-time	Some	3	0	0	1	0
University	Universiteit Leiden	60205	m ICT in Business and the Public Sector	Some	2	3	1	3	0
University	Rijksuniversiteit Groningen	60620	m IT Law full-time	Some	1	1	3	3	0
University	Erasmus Universiteit Rotterdam	60453	m business information management	Some	1	3	1	3	0
University	Technische Universiteit Delft	60300	m Computer Science	Some	3	1	0	3	0
University	Techn. Universiteit Eindhoven	60331	m embedded systems	Some	3	0	0	3	0

University	Techn. Universiteit Eindhoven	60438	m computer science and engineering	Some	3	0	0	3	0
University	Universiteit Twente	60300	m Computer Science	Some	3	0	0	3	0
University	Universiteit Twente	60331	m embedded systems	Some	3	0	0	3	0
University	Maastricht University	50300	b data science and artificial intelligence	Some	3	1	0	3	0
University	Vrije Universiteit Amsterdam	65014	m computer science (joint degree)	Some	3	0	0	3	0
University	Radboud Universiteit Nijmegen	59326	b computer science	Some	3	0	0	3	0
University	Radboud Universiteit Nijmegen	59326	b computer science	Some	3	0	0	3	0
University	Radboud Universiteit Nijmegen	60255	m information sciences	Some	3	1	1	3	0
University	Radboud Universiteit Nijmegen	60364	m computer science	Some	3	0	0	3	0
University	Radboud Universiteit Nijmegen	60364	m computer science	Some	3	0	0	3	0
University	Tilburg University	60069	M Law and Technology	Some	1	3	3	3	0
University	Universiteit Leiden	?	Law and Digital Technologies (Advanced Master Programme)	Some	1	2	3	3	0
University	Rijksuniversiteit Groningen	60620	M IT law	Some	1	1	3	3	0

Supplementary Table 12: MBO and Higher Education, scored according to the degree of connection with job market competencies

Life-Long Learning tables for Paragraph 3.6

Name of training course	Institute	Duration/extent
Business IT & Management	Avans Hogeschool	240 EC
Computer Science	Universiteit Twente	120 EC
Computer Science and Engineering	Eindhoven University of Technology	120 EC
Computing Science	Radboud University	180 EC
Computing Science	Radboud University	120 EC
Criminology	Universiteit Leiden	180 EC
Crisis and Security Management	Universiteit Leiden	60 EC
Engineering Systems	HAN University of Applied Sciences	90 EC
Engineering Systems	HAN_ University of Applied Sciences	36 months
Engineering Systems	HAN_ University of Applied Sciences	18 months
Engineering Systems – Cyber-Physical Systems	HAN_ University of Applied Sciences	18 months
Engineering Systems – Cyber-Physical Systems	HAN_ University of Applied Sciences	18 months
HBO ICT	Fontys Hogeschool	240 EC
HBO ICT	Hanzehogeschool Groningen	240 EC
HBO ICT	Hogeschool Utrecht	240 EC
HBO ICT	Hogeschool van Amsterdam	240 EC
HBO ICT	HZ University of Applied Sciences	240 EC
HBO ICT	Windesheim	240 EC
Industrial and Applied Mathematics	Eindhoven University of Technology	120 EC
Computer science	Hogeschool Leiden	240 EC
Computer science	NHL Stenden	240 EC
Computer science	NHL Stenden Hogeschool	48 months
Computer science	NHL Stenden Hogeschool	48 months
Safety & Security Management	Avans Hogeschool	240 EC
Safety & Security Management	Avans Hogeschool	240 EC
Safety & Security Management	NHL Stenden	240 EC
Safety & Security Management	NHL Stenden Hogeschool	48 months
Safety & Security Management	Saxion	240 EC
Safety & Security Management	Saxion	240 EC
Safety & Security Management	Hogeschool Utrecht	240 EC
International Trends and Threats in Safety and Security	Saxion Hogeschool	10 weeks
Introduction to ICT	Deltion College	1 day
IT Audit Compliance & Advisory (ITACA)	VU Vrije universiteit Amsterdam	129 days
IT law	Rijksuniversiteit Groningen	60 EC
Master Computer Science	Open university	Study duration not known
Master Digital Forensics	Hogeschool Leiden	60 EC
Master Military Strategic Studies	Faculteit Militaire Wetenschappen	Study duration not known
Master Software Engineering	Open university	Study duration not known

Privacy, Law & Security	Hogeschool Utrecht*	0 hours
Safety & Security Management (English variant)	De Haagse Hogeschool	240 EC
Security Management	Hogeschool Utrecht	Study duration not known
Security Management	Hogeschool Utrecht*	0 hours
Security Management	Saxion	240 EC
Security Studies	Universiteit Leiden	180 EC
Software Developer MBO 4 BBL	Regional Training Centre ROC Friese Poort Volwassenenonderwijs [Adult education]	4 years
Software Developer MBO 4 BOL	Regional Training Centre ROC Friese Poort Volwassenenonderwijs [Adult education]	4 years
Strategic View on Data Analytics	Erasmus Universiteit Rotterdam	4 months
Technical Computer Science	NHL Stenden	240 EC
Technical Computer Science	NHL Stenden Hogeschool	48 months

Supplementary Table 13: Life-Long Learning, MBO and Higher Education – containing some cyber security

Name of training course	Institute	Duration/extent
Advanced Business Analytics & (Big) Data Governance	VU - Vrije Universiteit Amsterdam	6 weeks
Advanced Master in Privacy, Cyber Security and Data Management	Maastricht University	Study duration not known
Bachelor cyber security	Avans+	2 years
Basic Training for Security in Systems and Networks	Koning Willem I College	21 hours
Be Cyber Secure	Saxion Hogeschool	10 weeks
Computer Security	Vrije Universiteit Amsterdam	120 EC
Cyber Safety & Security	NHL Stenden	120 EC
Cyber Safety & Security	NHL Stenden	120 EC
Cyber Safety and Security	NHL Stenden Hogeschool	24 months
Cyber Security	Hogeschool van Amsterdam	120 EC
Cyber Security	Technische Universiteit Delft	0 days
Cyber Security	Universiteit Leiden	Study duration not known
Cyber Security & Ethics	Hogeschool Utrecht	Study duration not known
Cyber Security & Ethics	Hogeschool Utrecht*	0 hours
Cyber Security Awareness	Deltion College	2 weeks
Cyber Security Engineering	De Haagse Hogeschool	Study duration not known
Cyber Security Engineering	De Haagse Hogeschool	Study duration not known
Cyber Security Engineering	De Haagse Hogeschool	Study duration not known
Cyber Security Fundamentals	Hbo Drechtsteden (Da Vinci HBO Drechtsteden)	5 months
Cyber Security	Hogeschool Inholland	120 EC
Cyber Security for Managers and Executives: Taking the Lead	Technische Universiteit Delft	6 weeks

Cyber Security Specialist	ICT College (Regional Training Centre ROC Midden Nederland)	36 months
Cyber Security Specialist	ICT College (Regional Training Centre ROC Midden Nederland)	36 months
Cyber Security Specialist	Tech Campus (Regional Training Centre ROC Midden Nederland)	36 months
Cyber Security Specialist	Tech Campus (Regional Training Centre ROC Midden Nederland)	36 months
Ethical Hacking	Hanzehogeschool Groningen (Hanzehs van Groningen)	Study duration not known
Expert IT systems and devices, Security	MBO Rijnland MBO College Technology & ICT (MBO Rijnland)	3 years
Expert IT systems and security	ICT College (Regional Training Centre ROC Midden Nederland)	36 months
Expert IT systems and security	Media, ICT & Design College (Regional Training Centre ROC Midden Nederland)	36 months
Expert IT systems and security	Tech Campus (Regional Training Centre ROC Midden Nederland)	36 months
Hardware Security: Physical Attacks	Universiteit van Amsterdam	2 days
Information Security	Hanzehogeschool Groningen (Hanzehs van Groningen)	Study duration not known
Information Security	Saxion Hogeschool	10 weeks
Information Security and Privacy Legislation in Practice (DPO) – Day	Bestuursacademie Nederland	2 days
Information Security Management	De Haagse Hogeschool	240 EC
Master Course Cybercrime, Cyber Security & Risk Management	Universiteit Twente	6 months
Masterclass Risks of Digitisation, Cybercrime, Prevention & Security	Universiteit Twente	4 days
Post-HBO Cyber Security Management	De Haagse Hogeschool	240 hours
Security and Network Engineering	Universiteit van Amsterdam	Study duration not known
Security and Safety Standardisation	HAN_ University of Applied Sciences	4 hours
The fundamentals of information security	Saxion Hogeschool	10 weeks

Supplementary Table 14: Life-Long Learning, MBO and Higher Education: full cyber security

Index	Volledige naam certificaat	Afkorting	Aantal	Beschrijving	Tech-nisch	M&O	Legal	Onder-zoek	Onder-wijs
1	Certified Information Systems Security Professional	CISSP	47	Dit certificaat wordt aangeboden door (ISC)² en is bedoeld voor ervaren informatiebeveiligingsprofessionals. Het behandelt een breed scala aan beveiligingstopics en is zeer gewaardeerd in de branche. Certificaten die hier nog onder vallen zijn: CISSP-ISSMP, CISSP-ISSAP.	3	2	2	0	0
2	Certified Ethical Hacker	CEH	31	De CEH-certificering, aangeboden door EC-Council, richt zich op ethisch hacken en penetratietesten. Het leert professionals hoe ze kwetsbaarheden kunnen identificeren en beveiliging kunnen verbeteren.	3	0	0	0	0
3	Certified Information Security Manager	CISM	33	Dit certificaat is ook van (ISC)² en is gericht op informatiebeveiligingsbeheer. Het richt zich op beveiligingsstrategie en governance.	2	3	2	0	0
4	Certified Information Systems Auditor	CISA	14	Ook aangeboden door ISACA, is CISA gericht op audit, controle en zekerheid van informatiesystemen. Het is waardevol voor professionals die betrokken zijn bij auditwerkzaamheden.	2	3	2	1	0
5	CompTIA Security+	CompTIA Security+	23	Dit is een toegankelijk certificaat dat de basisbeginselen van cybersecurity behandelt. Het is geschikt voor beginners en is vaak de eerste stap voor mensen die een carrière in cybersecurity willen beginnen.	3	0	0	0	0
6	Certified Cloud Security Professional	CCSP	21	Deze certificering is gericht op cloud-beveiliging en wordt aangeboden door (ISC)². Het is geschikt voor professionals die werken met cloudtechnologieën.	3	0	1	0	0
7	Certified Information Security Technician	CIST	0	Dit is een certificering die wordt aangeboden door CompTIA en is bedoeld voor technische professionals die werken aan de uitvoering van beveiligingsmaatregelen en technologieën.	2	3	0	0	0
8	Certified Information Privacy Professional	CIPP	10	Aangeboden door de International Association of Privacy Professionals (IAPP), zijn er verschillende CIPP-certificeringen beschikbaar, zoals CIPP/E (Europese privacy), CIPP/US (Amerikaanse privacy), en anderen, gericht op privacywetgeving en -beleid.	1	0	3	0	0
9	Certified Secure Software Lifecycle Professional	CSSLP	4	Ook van (ISC)², is deze certificering gericht op beveiliging gedurende de volledige levenscyclus van softwareontwikkeling en is geschikt voor beveiligingsprofessionals die betrokken zijn bij softwareontwikkeling.	3	0	1	0	0
10	Certified in Risk and Information Systems Control	CRISC	11	Aangeboden door ISACA, is CRISC gericht op beveiligingsrisicobeheer en -controle, en is bedoeld voor professionals die betrokken zijn bij risicobeheer op het gebied van in-formatiebeveiliging.	3	2	1	0	0
11	Certified Information Forensics Investigator	CIFI	9	Dit certificaat richt zich op forensische onderzoeken en wordt aangeboden door het International Association of Forensic and Security Metrology (IAFSM).	3	0	3	0	0

12	Certified Wireless Security Professional	CWSP	3	Dit certificaat richt zich op draadloze netwerkbeveiliging en wordt aangeboden door CWNP. Het is ideaal voor professionals die betrokken zijn bij het beveiligen van draadloze netwerken.	3	0	0	0	0
13	Certified Blockchain Security Professional	CBSP	4	Dit certificaat is gericht op blockchain-beveiliging en wordt aangeboden door Blockchain Training Alliance. Het is geschikt voor professionals die werken met blockchain-technologieën.	3	0	0	0	0
14	Certified IoT Security Practitioner	CIoTSP	0	Dit certificaat is gericht op beveiliging van het Internet of Things (IoT) en wordt aangeboden door CertNexus. Het behandelt de beveiligingsuitdagingen in verband met IoT-apparaten en -netwerken.	3	0	0	0	0
15	Certified Cloud Professional	CCP	5	Dit certificaat wordt aangeboden door Cloud Security Alliance en is gericht op verschillende aspecten van cloudbeveiliging, waaronder cloudarchitectuur en -beheer.	3	0	0	0	0
16	Certified Network Defender	CND	9	Gericht op netwerkbeveiliging en -verdediging.	3	0	0	0	0
17	Certified Cloud Security Specialist	CCSS	0	Voor beveiligingsspecialisten die werken met de cloud.	3	0	0	0	0
18	Offensive Security Certified Professional	OSCP	5	Concentreert zich op praktische penetratietestvaardigheden.	3	0	0	0	0
19	Certified Wireless Analysis Professional	CWAP	0	Gericht op diepgaande analyse van draadloze netwerken.	3	0	0	0	0
20	Certified Incident Response Handler	CIRH	0	Voor gespecialiseerde incidentresponsvaardigheden.	3	0	0	0	0
21	Certified Information Systems Security Officer	CISSO	5	Gericht op beveiligingsbeheer en -beleid.	3	0	0	0	0
22	Certified Cloud Security Knowledge	CCSK	6	Gericht op cloudbeveiligingskennis en -praktijken.	3	1	1	0	0

Supplementary Table 15: Cyber security certificates: number of courses from leeroverzicht.nl that train for this certificate and scored on the extent to which the certificate matches job market competencies

Provincie	Initiatief	Activiteit ID	Activiteit naam	Activiteit type	Startdatum activiteit	Eind-datum	Vestigingsplaats / geografie
Zuid-Holland	Cybernetwerk Drechtsteden	25	IT security manager	Advice/consultancy	1 January 2020		Drechtsteden
Zuid-Holland	MKB Deal Leiden	162	Coaching	Advice/consultancy	1 September 2021		Leiden
Noord-Holland	SPOT035	538	Permanent source of information for all steps you want to take in terms of digitalisation	Advice/consultancy	1 January 2021		Hilversum/Gooi & Vechtstreek
Noord-Holland	Cupola XS	568	Advies door expert	Advice/consultancy	3 January 2022		Haarlem
National	Smart Industry	605	Programma Data Delen	Advice/consultancy	5 February 2018		Zoetermeer
Noord-Holland	Data Science Alkmaar	521	Data Science Alkmaar is a platform for innovation in which the triple helix gains a good view of the developments concerning Big Data and Artificial Intelligence in order to use these for the benefit of regional economic growth and development.	Knowledge platform	1 January 2013		Alkmaar/Working area Province NH
Noord-Holland	SPOT035	536	Workshops, webinars, courses and knowledge sessions, personal consultation interviews, plan of action, coaching and guidance.	Knowledge platform	1 January 2021		Hilversum/Gooi & Vechtstreek
Noord-Holland	Purmervalley	545	Inspire, inform and connect. Ambition to inspire and interest young people in education and a job in ICT and technology. Optimal connection between business and education.	Knowledge platform	1 January 2017		Purmerend/ Zaanstreek waterland/West Friesland
National	Mijn Digitale Zaak	587	Platform ICT providers	Knowledge platform			Utrecht
National	Digital Trust Centre	589	Knowledge, information and advice via the website	Knowledge platform	8 June 2018		The Hague
National	Nederland Digitaal	593	Nederland Digitaal website	Knowledge platform	1 July 2018		The Hague
National	Dutch Blockchain Coalition (DBC)	595	DBC Knowledge Base	Knowledge platform	1 March 2017		to be confirmed
Zuid-Holland	EDIH	7	Access to financing	Networking & coordination	1 June 2023		MRDH
Zuid-Holland	EDIH	9	Innovation ecosystem and networks	Networking & coordination	1 June 2023		MRDH
Zuid-Holland	The Hague Security Delta	51	Bringing parties together for projects	Networking & coordination	1 January 2013		The Hague
Zuid-Holland	The Hague Security Delta	52	Support in finding financing	Networking & coordination	1 January 2013		The Hague

Zuid-Holland	The Hague Security Delta	53	Help solve the mismatch between supply and demand for security talent.	Networking & coordination	1 January 2013		The Hague
Zuid-Holland	Cyberweerbaarheidscentrum [Cyber Resilience Centre] Greenport	75	Bringing parties together for mutual consultation	Networking & coordination	1 October 2022		Zuid-Holland
Zuid-Holland	FERM Rotterdam	79	Network app	Networking & coordination	1 January 2017		Port of Rotterdam
Zuid-Holland	Human Capital Cyber Security (working title)	151	Interactive tool for Cyber Security SMEs	Networking & coordination	yet to start		Zuid-Holland
Noord-Holland	TechConnect	519	The aim is to increase equal opportunities in the tech job market and make tech training and jobs accessible to everyone. Women, people from socially disadvantaged neighbourhoods and home-grown SMEs are trained as programmers, data analysts, “growth hackers”, UX designers or tech managers.	Education for professionals	1 January 2019		Amsterdam/ Working area MRA
Noord-Holland	Cupola XS	571	Development needs & training	Education for professionals	3 January 2022		Haarlem
Noord-Holland	Smart Makers Academy	573	Skills-oriented training (metro line)	Education for professionals	1 January 2021		Haarlem
Noord-Holland	3D Makers Zone	501	Skills programme	Education for students	17 April 2014		Haarlem
Noord-Holland	Digital Society School	520	Company/foundation that supports students, professionals and organisations to become digital transformation leaders.	Education for students	1 January 2018		Amsterdam/ work area greater Amsterdam. Trainees/students come from all over the world.
Noord-Holland	House of Digital	533	Created from RIF demand	Education for students	1 June 2018		Amsterdam/mra
Noord-Holland	De Digital Accountant	542	Investigate how SME accounting firms can navigate the jungle of software tools in order to efficiently use digitalisation and data analysis for their clients and their own business operations.	Education for students	1 April 2020	1 October 2022	Amsterdam
Noord-Holland	Purmervalley	543	Inspire, inform and connect. Ambition to inspire and interest young people in education and a job in ICT and technology. Optimal connection between business and education.	Education for students	1 January 2017		Purmerend/ Zaanstreek waterland/West Friesland

Noord-Holland	De Digital Accountant	541	Investigate how SME accounting firms can navigate the jungle of software tools in order to efficiently use digitalisation and data analysis for their clients and their own business operations.	Research and development	1 April 2020	1 October 2022	Amsterdam
Zuid-Holland	Cybernetwerk Drechtsteden	24	Conducting your own scans	Scans & assessments	1 January 2020		Drechtsteden
Zuid-Holland	Cybernetwerk Drechtsteden	26	Cyberscan	Scans & assessments	1 January 2020		Drechtsteden
Zuid-Holland	Cyber network ZHE	57	Safety scans	Scans & assessments	1 January 2020		Oud-Beijerland
Zuid-Holland	Cyberweerbaarheidscentrum [Cyber Resilience Centre] Greenport	73	Baseline measurement & toolbox	Scans & assessments	1 October 2022		Zuid-Holland
Zuid-Holland	FERM Rotterdam	81	Paid scan	Scans & assessments	1 January 2017		Port of Rotterdam
Noord-Holland	ROMInwest	535	Innovating: ROM InWest helps to bring propositions to the market faster.	Scans & assessments	1 October 2021		Haarlem/Noord Holland
National	Mijn Digitale Zaak	585	Digitisation scan of KVK	Scans & assessments			Utrecht
National	Digital Trust Centre	588	Basic Cyber Resilience Scan	Scans & assessments	14 November 2019		The Hague
Zuid-Holland	FERM Rotterdam	80	Vouchers	Grants & financing	1 January 2017		Port of Rotterdam
Zuid-Holland	MKB010NEXT	176	Vouchers (corona)	Grants & financing	1 January 2020		Rotterdam
Noord-Holland	MKB Innovatie Topsectoren (MIT) Haalbaarheid	524	Promoting sustainable innovations in SMEs in order to contribute to a sustainable, innovative and entrepreneurial economy. subsidy for carrying out a feasibility project. This project consists of conducting a feasibility research or a combination of a feasibility research with industrial research and/or experimental development.	Grants & financing	1 January 2015		Provincie NH
Noord-Holland	MKB Innovatie Topsectoren (MIT) R&D	525	Promoting sustainable innovations in SMEs in order to contribute to a sustainable, innovative and entrepreneurial economy. Grant for carrying out a Research & Development collaboration project consisting of industrial research or experimental development or both together.	Grants & financing	1 January 2015		Provincie NH
Noord-Holland	Innovatiefonds NH	527	This fund makes convertible loans available for proving new concepts and ideas: Proof-of-Concept.	Grants & financing	1 August 2018		Provincie NH

Noord-Holland	ROMInwest	534	Investments: ROM InWest stimulates technology and innovation and allows it to grow further through investments. ROM InWest manages two funds for this purpose: the SME fund of €60 million and the Transition Fund with a target capital of €100 million	Grants & financing	1 October 2021		Haarlem/Noord Holland
National	Mijn Digitale Zaak	586	Digitisation subsidy	Grants & financing	21 June 2022		The Hague
National	Cyber resilience subsidy	591	Cyber resilience subsidy	Grants & financing	21 February 2019		The Hague
European	Digital Europe Programme	619	Digital Europe Programme	Grants & financing	29 April 2021		Brussels
Zuid-Holland	MKB Digiwerkplaats Haaglanden	153	Advisory targets for students and entrepreneurs	Working with students	1 February 2020		Haaglanden
Zuid-Holland	Dutch Innovation Factory	155	TechTalent: students work on entrepreneurs' (innovative) issues by completing challenges	Working with students	1 September 2019		Zoetermeer
Zuid-Holland	Digiwerkplaats Rijnmond	165	Advice to student about targets	Working with students	1 September 2021		Rotterdam
Noord-Holland	MKB Digital Workspace	518	Students solve companies' digitalisation questions.	Working with students	1 October 2019		Amsterdam/ Working area MRA
Noord-Holland	Cupola XS	569	Assignments by students	Working with students	3 January 2022		Haarlem
Zuid-Holland	EDIH	5	Information services	Workshops & knowledge events	1 June 2023		MRDH
Zuid-Holland	EDIH	6	Test before invest	Workshops & knowledge events	1 June 2023		MRDH
Zuid-Holland	Cybernetwerk Drechtsteden	23	Information sessions	Workshops & knowledge events	1 January 2020		Drechtsteden
Zuid-Holland	The Hague Security Delta	50	Increase knowledge	Workshops & knowledge events	1 January 2013		The Hague
Zuid-Holland	Cyber network ZHE	54	Knowledge meetings	Workshops & knowledge events	1 January 2020		Oud-Beijerland
Zuid-Holland	Cyber network ZHE	55	Webinars	Workshops & knowledge events	1 January 2020		Oud-Beijerland
Zuid-Holland	Cyberweerbaarheidscentrum [Cyber Resilience Centre] Greenport	74	Q&As, cyber café, awareness sessions and information dissemination	Workshops & knowledge events	1 October 2022		Zuid-Holland

Zuid-Holland	FERM Rotterdam	82	Public knowledge café	Workshops & knowledge events	1 January 2017		Port of Rotterdam
Zuid-Holland	FERM Rotterdam	83	Closed knowledge sessions	Workshops & knowledge events	1 January 2017		Port of Rotterdam
Zuid-Holland	MKB Digicafe	152	Online knowledge sessions to promote digitalisation	Workshops & knowledge events	1 April 2021		Zuid-Holland
Zuid-Holland	MKB Digiwerkplaats Haaglanden	154	Knowledge sessions/roadmaps for SMEs	Workshops & knowledge events	1 February 2020		Haaglanden
Zuid-Holland	Mijn digitale werkplaats Drechtsteden	167	Knowledge sessions (thematic table with expert companies, municipalities & province)	Workshops & knowledge events	1 September 2020		Dordrecht
Zuid-Holland	MKB010NEXT	175	Webinars, Sessions, Workshops	Workshops & knowledge events	1 January 2020		Rotterdam
Noord-Holland	3D Makers Zone	498	Inspiration session	Workshops & knowledge events	17 April 2014		Haarlem
Noord-Holland	SPOT035	537	Permanent source of information for all steps you want to take in terms of digitalisation	Workshops & knowledge events	1 January 2021		Hilversum/Gooi & Vechtstreek
Noord-Holland	Purmervalley	544	Inspire, inform and connect. Ambition to inspire and interest young people in education and a job in ICT and technology. Optimal connection between business and education.	Workshops & knowledge events	1 January 2017		Purmerend/ Zaanstreek waterland/West Friesland
Noord-Holland	Cupola XS	570	Masterclasses	Workshops & knowledge events	1 November 2021		Haarlem
Utrecht	Cybernetwork Utrecht		Website for referrals for entrepreneurs. Events are organised with partners (for example PVO) from this website: https://www.cybernetwerkutrecht.nl/				
Workshops & knowledge events			Municipality of Utrecht				
Utrecht	Ondernemer centraal		Business point where entrepreneurs can go with, for example, questions about digitalisation	Grants & financing			Municipality of Utrecht
Utrecht	Lectoraat Cybersecurity HU		Conducts practical research into cyber security at the request of companies/industry organisations	Research and development			Hogeschool Utrecht

Utrecht	Resilience training for entrepreneurs		PVO organises free cyber resilience workshops at the request of business associations, industrial estates or other entrepreneur associations.	Workshops & knowledge events			Midden Nederland
Utrecht	Cyber Chief Amersfoort		Regional Training Centre ROC Midden Nederland students conduct a digital scan of a company and provide tailor-made advice. This is done free of charge and under the professional guidance from cyber security professionals.	Working with students			Amersfoort
Flevoland	Cyber Chief Dronten		Regional Training Centre ROC Friese Poort students conduct a digital scan of a company and provide tailor-made advice. This is done free of charge and under the professional guidance from cyber security professionals.	Working with students			Dronten
Overijssel	WinSecure – You win, we secure!		Delivering IT security services and setting up a security community to increase online safety in the Zwolle region. Conducted by Hogeschool Windesheim students	Working with students			Zwolle
Overijssel	Cyber Security Awareness Course by Deltion		Course for SME entrepreneurs/employees to reduce risks to the crucial digital infrastructure. How to improve the safety of the website and devices, for example.				
	Workshops & knowledge events			Overijssel			
Overijssel	Cyber Aware Course for insiders by ITPH Academy		Training is intended for everyone, both business and private, to increase digital resilience	Workshops & knowledge events			Overijssel
Utrecht	Business Circle Entrepreneurial Veenendaal		Cyber monitor	Scans & assessments			Veenendaal
Flevoland	Veilig Ondernemen Flevoland		Organise cyber security knowledge sessions.	Workshops & knowledge events			Flevoland

Flevoland	MKB Schakelteam Flevoland		The advisors from the MKB Schakelteam support and advise SME companies on six themes: strategy, organisation, financing, marketing, personnel and implementation. Refer to them for cyber security issues.	Scans & assessments			Flevoland
Flevoland	EDIH Digital Hub Noordwest		Entrepreneurs can gain quick access to testing facilities, knowledge institutions, experts from the partner network and financing and internationalisation opportunities through their regional EDIH. The aim of this is to accelerate the digitalisation transition in the industry, healthcare and agri-food sectors.	Networking & coordination			Flevoland

Supplementaire Table 16: Regioscan digitalisering mkb - alle regionale initiatieven.

Appendix 3. Tables related to the job market

Junior	2018	2019	2020	2021	2022	Total
ECSF	271	394	419	618	951	2653
University	66	63	67	136	118	450
HBO	188	305	334	454	727	2008
MBO	17	26	18	28	106	195
CS_High	146	138	159	208	305	956
University	34	40	41	67	52	234
HBO	112	96	115	137	243	703
MBO		2	3	4	10	19
CS_Medium	193	241	278	373	537	1622
University	59	38	39	84	93	313
HBO	129	187	214	259	388	1177
MBO	5	16	25	30	56	132
CS_Low	977	1465	1296	1859	2571	8168
University	209	272	269	376	388	1514
HBO	589	933	850	1256	1728	5356
MBO	179	260	177	227	455	1298
Total	**1587**	**2238**	**2152**	**3058**	**4364**	**13399**

Intermediate	2018	2019	2020	2021	2022	Total
ECSF	721	715	1009	1534	1857	5836
University	126	108	127	214	197	772
HBO	553	577	838	1289	1568	4825
MBO	42	30	44	31	92	239
CS_High	217	212	258	386	545	1618
University	69	60	69	94	115	407
HBO	145	150	184	287	417	1183
MBO	3	2	5	5	13	28
CS_Medium	375	342	496	773	887	2873
University	106	66	102	176	188	638
HBO	258	259	375	577	675	2144
MBO	11	17	19	20	24	91
CS_Low	1681	2019	2345	3361	4057	13463
University	373	453	426	695	682	2629
HBO	1110	1401	1691	2412	3045	9659
MBO	198	165	228	254	330	1175
Total	**2994**	**3288**	**4108**	**6054**	**7346**	**23790**

Senior	2018	2019	2020	2021	2022	Total
ECSF	297	341	376	712	880	2606
University	65	74	64	124	116	443
HBO	229	253	300	568	698	2048
MBO	3	14	12	20	66	115
CS_High	133	132	122	221	275	883
University	43	33	46	69	55	246
HBO	87	99	70	149	215	620
MBO	3		6	3	5	17
CS_Medium	224	227	166	398	468	1483
University	65	41	34	97	107	344
HBO	155	181	129	291	327	1083
MBO	4	5	3	10	34	56
CS_Low	968	813	909	1666	2146	6502
University	268	206	238	433	425	1570
HBO	615	538	574	1114	1463	4304
MBO	85	69	97	119	258	628
Total	**1622**	**1513**	**1573**	**2997**	**3769**	**11474**

Unknown	2018	2019	2020	2021	2022	Total
ECSF	359	355	436	620	588	2358
University	65	46	50	91	76	328
HBO	280	288	363	518	474	1923
MBO	14	21	23	11	38	107
CS_High	120	128	118	166	190	722
University	30	19	19	34	28	130
HBO	89	105	94	131	156	575
MBO	1	4	5	1	6	17
CS_Medium	203	165	218	285	356	1227
University	40	39	37	47	49	212
HBO	147	117	170	219	272	925
MBO	16	9	11	19	35	90
CS_Low	1122	1235	1449	1929	2231	7966
University	188	172	218	323	276	1177
HBO	721	764	927	1282	1516	5210
MBO	213	299	304	324	439	1579
Total	**1804**	**1883**	**2221**	**3000**	**3365**	**12273**

Supplementary Table 17: Vacancies by education level, work experience and year. Source: Jobdigger, edited by Dialogic

1. Noord-Holland

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	1035
2	ECSF – CISO	ECSF	885
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	502
4	ECSF – Cyber Security Architect	ECSF	430
5	ECSF – Cyber Security Auditor	ECSF	198
6	ECSF – Cyber Security Risk Manager	ECSF	187
7	Cyber Security Consultant	CS_High	160
8	ECSF – Penetration Tester	ECSF	130
9	Consultant	CS_Mediun	115
10	Auditor	CS_Low	108
11	System Administrator	CS_Low	93
12	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	89
13	Privacy Officer	CS_Mediun	83
14	Security Consultant	CS_Mediun	79
15	Manager	CS_Mediun	78
16	ECSF – Digital Forensics Investigator	ECSF	73
17	ECSF – Cyber Incident Responder	ECSF	71
18	Software Engineer	CS_Low	65
19	Officer (data protection)	CS_High	60
20	ECSF – Cyber Security Researcher	#VERW!	59

2. Zuid-Holland

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	950
2	ECSF – CISO	ECSF	893
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	296
4	ECSF – Cyber Security Architect	ECSF	289
5	ECSF – Cyber Security Risk Manager	ECSF	252
6	ECSF – Cyber Security Researcher	ECSF	188
7	ECSF – Penetration Tester	ECSF	152
8	ECSF – Cyber Security Auditor	ECSF	136
9	Privacy Officer	CS_Mediun	107
10	Functional Manager	CS_Low	97
11	System Administrator	CS_Low	90
12	Security Consultant	CS_Mediun	78
13	Information Security Advisor	CS_High	76
14	Project manager	CS_Low	69
15	Officer	CS_High	67
16	Auditor	CS_Low	67
17	Consultant	CS_Mediun	63
18	Advisor	CS_Mediun	59
19	ECSF – Digital Forensics Investigator	ECSF	57
20	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	56

3. Utrecht

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	723
2	ECSF – Cyber Security Implementer	ECSF	566
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	331
4	ECSF – Cyber Security Architect	ECSF	238
5	ECSF – Cyber Security Risk Manager	ECSF	188
6	ECSF – Penetration Tester	ECSF	112
7	Privacy Officer	CS_Mediun	103
8	Traineeship Programme	CS_Low	86
9	ECSF – Cyber Security Auditor	ECSF	74
10	Security Consultant	CS_Mediun	71
11	Auditor	CS_Low	66
12	Cyber Security Consultant	CS_High	62
13	System Administrator	CS_Low	60
14	ECSF – Cyber Incident Responder	ECSF	60
15	Web developer	CS_Mediun	59
16	Information Security Advisor	CS_High	59
17	Account Manager	CS_Low	55
18	Information manager	CS_Low	48
19	Project manager	CS_Low	45
20	Consultant	CS_Mediun	45

4. Noord-Brabant

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	404
2	ECSF – Cyber Security Implementer	ECSF	324
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	239
4	ECSF – Cyber Security Architect	ECSF	139
5	ECSF – Cyber Security Researcher	ECSF	114
6	System Administrator	CS_Low	96
7	ECSF – Cyber Security Risk Manager	ECSF	65
8	ECSF – Cyber Security Auditor	ECSF	65
9	ECSF – Penetration Tester	ECSF	62
10	Privacy Officer	CS_Mediun	56
11	Security Consultant	CS_Mediun	49
12	Auditor	CS_Low	45
13	Advisor	CS_Mediun	44
14	Courier	CS_Low	43
15	ECSF – Cyber Incident Responder	ECSF	43
16	Information Security Advisor	CS_High	43
17	Officer	CS_High	36
18	Consultant	CS_Mediun	35
19	Network administrator	CS_Low	30
20	ECSF – Cyber Security Educator	ECSF	29

5. Gelderland

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	304
2	ECSF – Cyber Security Implementer	ECSF	224
3	ECSF – Cyber Security Architect	ECSF	171
4	ECSF – Cyber Threat Intelligence Specialist	ECSF	113
5	ECSF – Cyber Security Risk Manager	ECSF	63
6	ECSF – Cyber Security Auditor	ECSF	49
7	System Administrator	CS_Low	48
8	Auditor	CS_Low	41
9	Privacy Officer	CS_Mediun	37
10	Security Consultant	CS_Mediun	32
11	Officer	CS_High	30
12	ECSF – Penetration Tester	ECSF	27
13	Information manager	CS_Low	23
14	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	23
15	Traineeship Information Management Governmen	CS_Low	21
16	Consultant	CS_Mediun	21
17	Architect	CS_Low	21
18	Information Security Advisor	CS_High	19
19	Courier	CS_Low	17
20	Account Manager	CS_Low	17

6. Overijssel

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	288
2	ECSF – CISO	ECSF	144
3	ECSF – Cyber Security Researcher	ECSF	42
4	ECSF – Cyber Threat Intelligence Specialist	ECSF	42
5	ECSF – Cyber Security Architect	ECSF	37
6	Industrial Automation Technician	CS_Low	33
7	Software Engineer	CS_Low	27
8	ECSF – Cyber Security Risk Manager	ECSF	27
9	System Administrator	CS_Low	26
10	Officer	CS_High	26
11	Smart Industrial Automation Advisor	CS_Low	24
12	Privacy Officer	CS_Mediun	23
13	Information Security Advisor	CS_High	21
14	Machine Safety Advisor	CS_Low	20
15	Cloud Architect	CS_Low	20
16	Information manager	CS_Low	18
17	Upcoming Technical Installation Specialist	CS_Low	18
18	Intermediate Safety Expert	CS_Low	16
19	Digital Trust Advisor	CS_Low	16
20	System Architect	CS_Low	15

7. Limburg

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	114
2	ECSF – CISO	ECSF	103
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	29
4	ECSF – Cyber Security Architect	ECSF	28
5	Courier	CS_Low	27
6	Privacy Officer	CS_Mediun	24
7	Auditor	CS_Low	18
8	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	18
9	ECSF – Cyber Security Risk Manager	ECSF	17
10	Officer	CS_High	17
11	Traineeship Information Management Governmen	CS_Low	16
12	System Administrator	CS_Low	13
13	Project Leader	CS_Low	13
14	ECSF – Digital Forensics Investigator	ECSF	13
15	Software Project Manager	CS_Low	12
16	Functional Manager	CS_Low	12
17	Policy Officer	CS_Low	12
18	Integration Specialist	CS_Low	12
19	Sales Manager	CS_Mediun	11
20	Secondary Technical Employee	CS_Low	10

8. Groningen

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	62
2	ECSF – Cyber Security Implementer	ECSF	51
3	ECSF – Cyber Security Researcher	ECSF	38
4	ECSF – Cyber Threat Intelligence Specialist	ECSF	36
5	Crypto Specialist	CS_Mediun	16
6	Software Developer	CS_Low	16
7	ECSF – Cyber Security Auditor	ECSF	13
8	Traineeship Information Management Governmen	CS_Low	12
9	Functional Manager	CS_Low	12
10	ECSF – Cyber Security Architect	ECSF	10
11	Microsoft Server Specialist	CS_Low	10
12	ECSF – Penetration Tester	ECSF	10
13	Compliance Advisor	CS_Mediun	9
14	ECSF – Cyber Security Risk Manager	ECSF	8
15	Lawyer	CS_Low	8
16	Information Security Advisor	CS_High	8
17	Advisor	CS_Mediun	8
18	Crypto Researcher	CS_Low	7
19	Privacy Officer	CS_Mediun	7
20	Integrated Security Coordinator	CS_High	7

9. Flevoland

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	33
2	ECSF – Cyber Security Implementer	ECSF	23
3	ECSF – Penetration Tester	ECSF	20
4	ECSF – Cyber Threat Intelligence Specialist	ECSF	19
5	Protection Automation Control Engineer	CS_Low	10
6	ECSF – Cyber Incident Responder	ECSF	9
7	Sales Manager	CS_Mediun	8
8	Privacy Officer	CS_Mediun	7
9	Cloud Infrastructure Specialist	CS_Low	7
10	ECSF – Cyber Security Educator	ECSF	7
11	Advisor	CS_Mediun	6
12	Product Owner	CS_Low	6
13	System Administrator	CS_Low	6
14	Consultant	CS_Mediun	5
15	ICT Project Manager	CS_Low	5
16	Audio & Video Engineer	CS_Low	5
17	Software Engineer	CS_Low	5
18	Information Management Advisor	CS_Low	5
19	Inspire Programmer	CS_Low	5
20	Account Manager High	CS_Low	5

10. Friesland

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	42
2	Officer	CS_High	13
3	Privacy Officer	CS_Mediun	13
4	Lecturer in Safety & Security Management	CS_Low	11
5	Network administrator	CS_Low	10
6	ECSF – Cyber Security Implementer	ECSF	10
7	Technician in Energy Technology	CS_Low	9
8	Software Engineer	CS_Low	7
9	Product Manager	CS_Mediun	7
10	System Administrator	CS_Low	7
11	C# Delphi Software Engineer	CS_Low	7
12	IT Security Professor	CS_High	6
13	Public Order Safety Policy Officer	CS_Low	6
14	Data Analyst	CS_Low	6
15	.NET Software Developer	CS_Low	6
16	Project coordinator	CS_Low	5
17	Data Engineer	CS_Low	5
18	ICT Manager	CS_Low	5
19	Operational Technology Technician	CS_Low	5
20	R&D Engineer	CS_Low	4

11. Drenthe

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	33
2	ECSF – Cyber Threat Intelligence Specialist	ECSF	13
3	Driver	CS_Low	13
4	ECSF – Cyber Security Implementer	ECSF	10
5	Security Manager	CS_Mediun	9
6	ECSF – Cyber Security Architect	ECSF	8
7	Technical Cmdb Manager	CS_Low	7
8	Secondary Technical Employee	CS_Low	7
9	Information Security Advisor	CS_High	6
10	System Administrator	CS_Low	6
11	Privacy Officer	CS_Mediun	6
12	ECSF – Cyber Security Risk Manager	ECSF	6
13	Information manager	CS_Low	5
14	Call Centre Agent Dutch	CS_Low	5
15	Project manager	CS_Low	5
16	Officer	CS_High	5
17	ICT Lead	CS_Low	5
18	Java Developer	CS_Low	5
19	Advisor	CS_Mediun	4
20	Business Manager	CS_Low	4

12. Zeeland

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	24
2	ECSF – Cyber Security Architect	ECSF	23
3	ECSF – CISO	ECSF	21
4	ICT Technician Specialisation IT	CS_Low	20
5	Functional Manager	CS_Low	9
6	Traineeship Information Management Governmen	CS_Low	9
7	Network administrator	CS_Low	8
8	Simulation Based Project Engineer	CS_Low	7
9	ECSF – Cyber Threat Intelligence Specialist	ECSF	6
10	Process Automation Engineer	CS_Low	5
11	Officer	CS_High	5
12	ICT System Specialist Cloud	CS_Low	4
13	Policy Officer	CS_Low	4
14	Information Security & Privacy Advisor	CS_High	4
15	Advisor	CS_Mediun	4
16	System/Application Administrator	CS_Low	4
17	ECSF – Cyber Security Risk Manager	ECSF	4
18	Engineer/Specialist Telecom	CS_Low	4
19	Planner	CS_Low	3
20	Policy Officer Information Provision ICT	CS_Low	3

Supplementary Table 18: The Top 20 job profiles by region. Source: Jobdigger, edited by Dialogic

Junior – WO			
#	Job profile	Type	Number
1	ECSF – Cyber Security Researcher	ECSF	97
2	ECSF – CISO	ECSF	84
3	ECSF – Cyber Security Implementer	ECSF	69
4	ECSF – Cyber Security Auditor	ECSF	64
5	ECSF – Cyber Threat Intelligence Specialist	ECSF	50
6	Sales & Marketing Intern	CS_Low	32
7	Consultant	CS_Mediun	32
8	ECSF – Penetration Tester	ECSF	23
9	Traineeship	CS_Mediun	21
10	Crypto Specialist	CS_Mediun	21
11	ECSF – Cyber Security Architect	ECSF	21
12	Trainee	CS_Low	20
13	Lawyer	CS_Low	20
14	ECSF – Digital Forensics Investigator	ECSF	20
15	Officer	CS_Low	19
16	Consultant IT Assurance	CS_Low	18
17	Privacy Officer	CS_Mediun	17
18	IT Risk Mitigation Manager	CS_High	17
19	Associate	CS_Low	17
20	Digital Assurance Traineeship	CS_Low	16

Junior – HBO			
#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	572
2	ECSF – CISO	ECSF	456
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	262
4	ECSF – Cyber Security Risk Manager	ECSF	175
5	ECSF – Penetration Tester	ECSF	174
6	ECSF – Cyber Security Architect	ECSF	112
7	Consultant	CS_Mediun	91
8	ECSF – Cyber Security Auditor	ECSF	90
9	Traineeship Information Management Government	CS_Low	86
10	Traineeship Programme	CS_Low	84
11	Auditor	CS_Low	78
12	Privacy Officer	CS_Mediun	72
13	Cyber Security Consultant	CS_High	70
14	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	58
15	Account Manager	CS_Low	53
16	System Administrator	CS_Low	49
17	Digital Specialist	CS_Mediun	46
18	Information Security Advisor	CS_High	46
19	Traineeship	CS_Mediun	44
20	Engineer	CS_Low	44

Junior – MBO			
#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	115
2	System Administrator	CS_Low	52
3	Courier	CS_Low	43
4	Operations employee	CS_Low	31
5	ECSF – Cyber Threat Intelligence Specialist	ECSF	30
6	Support Engineer	CS_Low	27
7	Service desk Employee	CS_Low	21
8	Administrative Clerk	CS_Low	21
9	ECSF – CISO	ECSF	21
10	ECSF – Cyber Security Risk Manager	ECSF	20
11	Network administrator	CS_Low	17
12	Account Manager	CS_Low	17
13	Operations employee	CS_Low	16
14	IT Support Employee	CS_Low	16
15	Commercial employee	CS_Low	16
16	Driver	CS_Low	15
17	Management assistant	CS_Low	13
18	ICT Employee	CS_Low	12
19	ICT Specialist	CS_Low	12
20	Information Specialist Change Manager	CS_Low	12

Intermediate – WO			
#	Job profile	Type	Number
1	ECSF – CISO	ECSF	292
2	ECSF – Cyber Security Implementer	ECSF	123
3	ECSF – Cyber Security Architect	ECSF	119
4	Officer	CS_High	64
5	ECSF – Cyber Threat Intelligence Specialist	ECSF	60
6	ECSF – Cyber Security Auditor	ECSF	58
7	ECSF – Cyber Security Researcher	ECSF	51
8	Auditor	CS_Low	49
9	Cyber Security Consultant	CS_High	46
10	Privacy Officer	CS_Mediun	41
11	Manager	CS_Mediun	35
12	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	31
13	Compliance Officer	CS_Low	31
14	IT Risk Manager	CS_Mediun	30
15	Information manager	CS_Low	28
16	Product Consultant	CS_Low	27
17	Consultant	CS_Mediun	22
18	Enterprise Architect	CS_Low	21
19	Engineer	CS_Low	21
20	Data Scientist	CS_Low	18

Intermediate – HBO			
#	Job profile	Type	Number
1	ECSF – CISO	ECSF	1377
2	ECSF – Cyber Security Implementer	ECSF	1299
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	615
4	ECSF – Cyber Security Architect	ECSF	594
5	ECSF – Cyber Security Risk Manager	ECSF	330
6	ECSF – Penetration Tester	ECSF	178
7	ECSF – Cyber Security Auditor	ECSF	148
8	Security Consultant	CS_Mediun	137
9	Functional Manager	CS_Low	115
10	Privacy Officer	CS_Mediun	108
11	ECSF – Cyber Incident Responder	ECSF	104
12	System Administrator	CS_Low	99
13	Auditor	CS_Low	98
14	Cyber Security Consultant	CS_High	89
15	Information Security Advisor	CS_High	87
16	Account Manager	CS_Low	83
17	Project manager	CS_Low	77
18	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	76
19	Architect	CS_Low	71
20	Information manager	CS_Low	70

Intermediate – MBO			
#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	146
2	System Administrator	CS_Low	99
3	ECSF – CISO	ECSF	40
4	Network administrator	CS_Low	39
5	ECSF – Cyber Threat Intelligence Specialist	ECSF	29
6	Technician in Energy Technology	CS_Low	22
7	ICT Technician Specialisation IT	CS_Low	18
8	Intermediate Safety Expert	CS_Low	17
9	Support Engineer	CS_Low	17
10	Service Desk Employee ICT	CS_Low	14
11	ICT Specialist	CS_Low	14
12	ECSF – Cyber Security Risk Manager	ECSF	14
13	Energy Technology Technician	CS_Low	13
14	ICT Employee	CS_Low	13
15	Security Consultant	CS_Mediun	12
16	Support employee	CS_Low	12
17	Technical Application Manager	CS_Low	11
18	Service desk Employee	CS_Low	11
19	Workplace manager	CS_Low	11
20	Office Manager	CS_Low	10

Senior – WO			
#	Job profile	Type	Number
1	ECSF – CISO	ECSF	130
2	ECSF – Cyber Security Researcher	ECSF	89
3	ECSF – Cyber Security Architect	ECSF	62
4	ECSF – Cyber Security Implementer	ECSF	55
5	ECSF – Cyber Security Auditor	ECSF	45
6	Auditor	CS_Low	44
7	Privacy Lawyer	CS_Mediun	41
8	Justice & Safety Manager	CS_Low	22
9	ECSF – Cyber Threat Intelligence Specialist	ECSF	22
10	Privacy Officer	CS_Mediun	21
11	Officer	CS_High	21
12	Financial Risk Management Consultant	CS_Low	20
13	Associate & Financial Consulting	CS_Low	20
14	Work student & Quantitative Consulting	CS_Low	19
15	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	18
16	Project manager	CS_Low	17
17	Consultant/Manager	CS_Low	17
18	Sales & Marketing Intern	CS_Low	16
19	Operational & Value Consultant	CS_Low	16
20	Cyber Security Consultant	CS_High	15

Senior– HBO			
#	Job profile	Type	Number
1	ECSF – CISO	ECSF	550
2	ECSF – Cyber Security Implementer	ECSF	496
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	296
4	ECSF – Cyber Security Architect	ECSF	273
5	ECSF – Cyber Security Risk Manager	ECSF	136
6	Privacy Officer	CS_Mediun	96
7	ECSF – Cyber Security Auditor	ECSF	86
8	ECSF – Penetration Tester	ECSF	67
9	Security Consultant	CS_Mediun	64
10	Traineeship Information Management Government	CS_Low	60
11	ECSF – Cyber Incident Responder	ECSF	51
12	Consultant	CS_Mediun	48
13	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	43
14	System Administrator	CS_Low	41
15	Account Manager	CS_Low	41
16	Officer	CS_High	38
17	Product Owner	CS_Low	37
18	Project manager	CS_Low	35
19	Cyber Security Consultant	CS_High	35
20	Advisor	CS_Mediun	32

Senior – MBO			
#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	65
2	Secondary Technical Employee	CS_Low	25
3	ECSF – CISO	ECSF	20
4	Support Engineer	CS_Low	18
5	System Administrator	CS_Low	17
6	Network administrator	CS_Low	13
7	ECSF – Cyber Security Auditor	ECSF	11
8	Investigator	CS_Low	8
9	ECSF – Cyber Threat Intelligence Specialist	ECSF	8
10	Administrative Clerk	CS_Low	8
11	General Tactical Investigation	CS_Mediun	8
12	Workplace manager	CS_Low	8
13	Hosting Engineer PaaS	CS_Low	7
14	Planner	CS_Low	7
15	BRP Specialist	CS_Low	7
16	ICT Employee	CS_Low	6
17	Tactical Investigator	CS_Mediun	6
18	Infrastructure Platform Specialist	CS_Low	6
19	IT Service Desk employee	CS_Low	6
20	Technician	CS_Low	5

Supplementary Table 19: The Top 20 job profiles by experience category and education level. Source: Jobdigger, edited by Dialogic

Based on the Top 100 organisations

Cyber R&D

#	Job profile	Type	Number
1	ECSF – Cyber Security Researcher	ECSF	100
2	ECSF – Cyber Threat Intelligence Specialist	ECSF	33
3	ECSF – Cyber Security Implementer	ECSF	26
4	Crypto Specialist	CS_Mediun	22
5	ECSF – Cyber Security Educator	ECSF	20
6	Crypto Researcher	CS_Low	12
7	Security Talent	CS_Mediun	12
8	Candidates	CS_Low	10
9	Start function	CS_Mediun	10
10	Software Engineer Lecturer	CS_Low	7
11	ECSF – CISO	ECSF	7
12	Coach High School ICT Lecturer	CS_Low	6
13	Researcher	CS_High	6
14	Outstanding Pdeng Candidate	CS_Low	6
15	ECSF – Cyber Security Risk Manager	ECSF	6
16	Research	CS_Low	6
17	Cyber Workforce Developer	CS_Mediun	4
18	Cyber Security Project Leader	CS_High	4
19	Safe Society Project Leader	CS_Low	4
20	Cyber Security Lector	CS_Mediun	4

Cyber production

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	464
2	ECSF – Cyber Threat Intelligence Specialist	ECSF	317
3	ECSF – Cyber Security Architect	ECSF	254
4	ECSF – CISO	ECSF	233
5	ECSF – Penetration Tester	ECSF	181
6	Cyber Security Consultant	CS_High	170
7	ECSF – Cyber Security Risk Manager	ECSF	152
8	ECSF – Cyber Incident Responder	ECSF	100
9	ECSF – Digital Forensics Investigator	ECSF	93
10	Consultant	CS_Mediun	90
11	ECSF – Cyber Security Auditor	ECSF	73
12	Cyber Security Consultant	CS_High	73
13	Project manager	CS_Low	60
14	Web developer	CS_Mediun	55
15	Cloud Security Consultant	CS_Mediun	54
16	Privacy Consultant	CS_Mediun	51
17	Manager	CS_Mediun	51
18	Account Manager	CS_Low	44
19	Technical Application Manager	CS_Low	43
20	Security Consultant	CS_Mediun	43

Cyber integration

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	904
2	ECSF – CISO	ECSF	646
3	ECSF – Cyber Security Architect	ECSF	447
4	ECSF – Cyber Threat Intelligence Specialist	ECSF	440
5	ECSF – Cyber Security Auditor	ECSF	258
6	ECSF – Cyber Security Risk Manager	ECSF	172
7	Courier	CS_Low	132
8	Auditor	CS_Low	106
9	ECSF – Penetration Tester	ECSF	91
10	Traineeship Programme	CS_Low	85
11	Privacy Officer	CS_Mediun	82
12	Software Engineer	CS_Low	72
13	ECSF – Cyber Incident Responder	ECSF	69
14	Product Owner	CS_Low	51
15	Engineer	CS_Low	51
16	Analyst	CS_Mediun	48
17	Business Analyst	CS_Low	45
18	Information Security Advisor	CS_High	44
19	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	43
20	Security Manager	CS_Mediun	36

Educational/knowledge institutions

#	Job profile	Type	Number
1	ECSF – Cyber Security Researcher	ECSF	100
2	ECSF – Cyber Security Educator	ECSF	35
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	34
4	ECSF – Cyber Security Implementer	ECSF	26
5	Crypto Specialist	CS_Mediun	22
6	ECSF – CISO	ECSF	18
7	Crypto Researcher	CS_Low	12
8	Security Talent	CS_Mediun	12
9	Information manager	CS_Low	11
10	Start function	CS_Mediun	10
11	Candidates	CS_Low	10
12	Functional Manager	CS_Low	9
13	Software Engineer	CS_Low	7
14	Software Engineer Lecturer	CS_Low	7
15	ECSF – Cyber Security Risk Manager	ECSF	7
16	Privacy Officer	CS_Mediun	6
17	Outstanding Pdeng Candidate	CS_Low	6
18	Research	CS_Low	6
19	Coach High School ICT Lecturer	CS_Low	6
20	Researcher	CS_High	6

Business lives

#	Job profile	Type	Number
1	ECSF – Cyber Security Implementer	ECSF	1379
2	ECSF – CISO	ECSF	690
3	ECSF – Cyber Threat Intelligence Specialist	ECSF	658
4	ECSF – Cyber Security Architect	ECSF	572
5	ECSF – Cyber Security Auditor	ECSF	285
6	ECSF – Penetration Tester	ECSF	269
7	ECSF – Cyber Security Risk Manager	ECSF	256
8	Cyber Security Consultant	CS_High	217
9	ECSF – Cyber Incident Responder	ECSF	158
10	Traineeship Information Management Governmen	CS_Low	146
11	Auditor	CS_Low	139
12	Courier	CS_Low	132
13	Consultant	CS_Mediun	125
14	ECSF – Digital Forensics Investigator	ECSF	95
15	Project manager	CS_Low	90
16	Traineeship Programme	CS_Low	85
17	ECSF – Cyber Legal, Policy & Compliance Officer	ECSF	78
18	Security Consultant	CS_Mediun	77
19	Software Engineer	CS_Low	74
20	Cyber Security Consultant	CS_High	74

Government

#	Job profile	Type	Number
1	ECSF – CISO	ECSF	282
2	ECSF – Cyber Threat Intelligence Specialist	ECSF	269
3	ECSF – Cyber Security Architect	ECSF	260
4	ECSF – Cyber Security Implementer	ECSF	199
5	ECSF – Cyber Security Risk Manager	ECSF	131
6	Digital Specialist	CS_Mediun	119
7	ECSF – Cyber Security Auditor	ECSF	107
8	Privacy Officer	CS_Mediun	43
9	Information Security Advisor	CS_High	41
10	Analyst	CS_Mediun	40
11	Advisor	CS_Mediun	38
12	Auditor	CS_Low	35
13	Security Manager	CS_Mediun	31
14	Investigator	CS_Low	29
15	Officer	CS_Low	29
16	ICT Manager	CS_Low	28
17	Functional Manager	CS_Low	27
18	Public Private Partnership Account Manager	CS_High	26
19	Air Force ICT Officer	CS_Low	25
20	Financial Investigator	CS_Mediun	25

Supplementary Table 20: Demand for job profiles (based on the Top 100 organisations). Source: Jobdigger, edited by Dialogic

#	ECSF profile	Category	% vacancies	Number of vacancies
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	57,6%	7746
2	Cyber threats	Technical	52,1%	7004
3	Cyber security controls and solutions	Technical	51,4%	6912
4	Cyber security risks	Technical	43,6%	5866
5	Cyber security related laws, regulations and legislations	Legal	40,3%	5425
6	Cyber security procedures	Man. & Org.	33,3%	4481
7	Cyber security recommendations and best practices	Man. & Org.	30,2%	4057
8	Management practices	Man. & Org.	27,8%	3746
9	Cyber security-related technologies	Technical	26,8%	3606
10	Cyber security policies	Man. & Org.	24,3%	3276
	Key skill(s)			
1	Identify, analyse and correlate cyber security events	Research	51,6%	6949
2	Work on operating systems, servers, clouds and relevant infrastructures	Technical	45,5%	6117
3	Motivate and encourage people	Man. & Org.	44,3%	5964
4	Collaborate with other team members and colleagues	Man. & Org.	28,1%	3787
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	9,7%	1302
6	Develop codes, scripts and programs	Technical	7,2%	966
7	Develop code, scripts and programs	Technical	7,2%	966
8	Identify and exploit vulnerabilities	Technical	4,7%	635
9	Conduct ethical hacking	Technical	4,4%	587
10	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	3,9%	520
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	41,4%	5568
2	Cooperate and share information with authorities and professional groups	Man. & Org.	31,7%	4270
3	Collaborate with other teams and colleagues	Man. & Org.	28,1%	3787
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	21,2%	2854
5	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	4,4%	586
6	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	3,9%	519
7	Design and propose a secure architecture to implement the organisation's strategy	Technical	3,2%	426
8	Enforce and advocate organisation's data privacy and protection program	Legal	2,9%	394
9	Deploy penetration testing tools and penetration test programs	Technical	2,9%	385
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	2,4%	320

Supplementary Table 21: Top 10 tasks, skills and knowledge for ECSF profiles. Source: Jobdigger, edited by Dialogic

#	Job title – CS-high	Category	% vacancies	Number of vacancies
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	66,0%	2763
2	Cyber threats	Technical	62,1%	2599
3	Cyber security risks	Technical	51,8%	2167
4	Cyber security related laws, regulations and legislations	Legal	49,2%	2061
5	Cyber security controls and solutions	Technical	45,0%	1885
6	Cyber security recommendations and best practices	Man. & Org.	42,6%	1785
7	Cyber security procedures	Man. & Org.	40,7%	1706
8	Management practices	Man. & Org.	36,8%	1540
9	Cyber security policies	Man. & Org.	35,5%	1485
10	Cyber security-related technologies	Technical	17,6%	736
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	57,1%	2392
2	Identify, analyse and correlate cyber security events	Research	56,0%	2345
3	Collaborate with other team members and colleagues	Man. & Org.	38,0%	1593
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	27,2%	1138
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	7,9%	331
6	Think creatively and outside the box	Research	4,2%	174
7	Conduct ethical hacking	Technical	4,2%	174
8	Identify and select appropriate pedagogical approaches for the intended audience	Research	3,5%	148
9	Identify and exploit vulnerabilities	Technical	3,5%	146
10	Design systems and architectures based on security and privacy by design and by defaults cyber security principles	Technical	3,4%	141
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	53,7%	2247
2	Cooperate and share information with authorities and professional groups	Man. & Org.	39,4%	1648
3	Collaborate with other teams and colleagues	Man. & Org.	38,0%	1593
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	27,8%	1165
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	5,1%	214
6	Enforce and advocate organisation's data privacy and protection program	Legal	5,0%	208
7	Manage legal aspects of information security responsibilities and third-party relations	Legal	3,3%	139
8	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	3,2%	136
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	3,0%	125
10	Design and propose a secure architecture to implement the organisation's strategy	Technical	3,0%	125

Supplementary Table 22: Top 10 tasks, skills and knowledge for profiles with a high cyber security content. Source: Jobdigger, edited by Dialogic

#	Job Title – CS Agent	Category	% vacancies	Number of vacancies
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	53,5%	3863
2	Cyber threats	Technical	48,1%	3474
3	Cyber security controls and solutions	Technical	44,6%	3217
4	Cyber security related laws, regulations and legislations	Legal	44,4%	3202
5	Cyber security risks	Technical	41,8%	3015
6	Cyber security recommendations and best practices	Man. & Org.	33,7%	2434
7	Cyber security procedures	Man. & Org.	33,7%	2433
8	Management practices	Man. & Org.	30,0%	2165
9	Cyber security policies	Man. & Org.	25,2%	1818
10	Cyber security-related technologies	Technical	16,9%	1219
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	49,5%	3573
2	Identify, analyse and correlate cyber security events	Research	48,3%	3488
3	Collaborate with other team members and colleagues	Man. & Org.	34,7%	2501
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	29,3%	2112
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10,0%	722
6	Develop code, scripts and programs	Technical	5,0%	361
7	Develop codes, scripts and programs	Technical	5,0%	361
8	Think creatively and outside the box	Research	4,2%	303
9	Conduct ethical hacking	Technical	3,6%	262
10	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	3,3%	236
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	48,0%	3465
2	Cooperate and share information with authorities and professional groups	Man. & Org.	37,8%	2730
3	Collaborate with other teams and colleagues	Man. & Org.	34,7%	2501
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	25,2%	1822
5	Enforce and advocate organisation's data privacy and protection program	Legal	5,2%	378
6	Manage legal aspects of information security responsibilities and third-party relations	Legal	4,4%	315
7	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	4,4%	314
8	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	4,0%	288
9	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	2,7%	195
10	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	2,6%	187

Supplementary Table 23: Top 10 tasks, skills and knowledge for profiles with a substantial cyber security content. Source: Jobdigger, edited by Dialogic

#	Job Title – CS-low	Category	% vacancies	Number of vacancies
	Key knowledge			
1	Cyber security controls and solutions	Technical	39,6%	14322
2	Cyber security standards, methodologies and frameworks	Technical	37,6%	13611
3	Management practices	Man. & Org.	30,5%	11030
4	Cyber security related laws, regulations and legislations	Legal	29,0%	10511
5	Cyber security procedures	Man. & Org.	26,7%	9676
6	Cyber threats	Technical	24,4%	8829
7	Cyber security recommendations and best practices	Man. & Org.	21,8%	7875
8	Cyber security policies	Man. & Org.	18,2%	6588
9	Cyber security risks	Technical	17,1%	6195
10	Multi-disciplinary aspect of cyber security	Man. & Org.	8,3%	2998
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	41,3%	14934
2	Identify, analyse and correlate cyber security events	Research	35,3%	12780
3	Collaborate with other team members and colleagues	Man. & Org.	31,2%	11301
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	26,8%	9707
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10,1%	3661
6	Develop codes, scripts and programs	Technical	6,0%	2161
7	Develop code, scripts and programs	Technical	6,0%	2161
8	Think creatively and outside the box	Research	4,3%	1539
9	Identify and select appropriate pedagogical approaches for the intended audience	Research	2,7%	973
10	Work under pressure	Man. & Org.	2,3%	827
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	38,1%	13791
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	37,5%	13580
3	Collaborate with other teams and colleagues	Man. & Org.	31,2%	11297
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	26,2%	9490
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	3,1%	1128
6	Enforce and advocate organisation's data privacy and protection program	Legal	2,5%	890
7	Deploy penetration testing tools and penetration test programs	Technical	1,2%	436
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	0,7%	237
9	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	0,6%	201
10	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	0,5%	194

Supplementary Table 24: Top 10 tasks, skills and knowledge for profiles with a low cyber security content. Source: Jobdigger

1. ECSF – CISO

#	Certificate	Number of vacancies
1	CISSP	1799
2	CISM	1537
3	CISA	875
4	CIPP	290
5	CRISC	253
6	CCSP	201
7	CEH	144
8	CIPM	111
9	GIAC	48
10	OSCP	47

Manager

#	Certificate	Number of vacancies
1	CISSP	217
2	CEH	128
3	CISM	87
4	CISA	60
5	GCIH	82
6	OSCP	50
7	GSEC	33
8	GIAC	28
9	GCIA	21
10	CCSP	20

2. ECSF – Cyber Threat Intelligence

#	Certificate	Number of vacancies
1	CISSP	454
2	CISM	246
3	CEH	166
4	CISA	157
5	OSCP	80
6	CCSP	78
7	GIAC	69
8	GCIH	63
9	CRISC	27
10	SSCP	27

7. Privacy Officer

#	Certificate	Number of vacancies
1	CIPP	199
2	CIPM	119
3	CISSP	14
4	CISM	6
5	CDPSE	5
6	CISA	5

3. ECSF – Cyber Security

#	Certificate	Number of vacancies
1	CISSP	334
2	CISM	126
3	CEH	113
4	OSCP	65
5	CSSLP	52
6	CISA	44
7	CCSP	35
8	SSCP	35
9	GIAC	28
10	GCIH	24

8. ECSF – Cyber Security Auditor

#	Certificate	Number of vacancies
1	CISA	132
2	CISSP	110
3	CISM	39
4	CCSP	34
5	CEH	20
6	CRISC	18
7	CSSLP	11
8	OSCP	4

4. ECSF – Cyber Security Architect

#	Certificate	Number of vacanc
1	CISSP	366
2	CISM	145
3	CCSP	99
4	CISA	75
5	CEH	42
6	CRISC	35
7	OSCP	24
8	GIAC	15
9	CISSP-ISSAP	15
10	CHFI	12

9. Security Consultant

#	Certificate	Number of vacanc
1	CISSP	154
2	CISM	111
3	CISA	62
4	CEH	35
5	CCSP	23
6	CIPP	18
7	OSCP	18
8	SSCP	4
9	CRISC	4
10	CSSLP	4

5. ECSF – Penetration Tester

#	Certificate	Number of vacanc
1	OSCP	278
2	CISSP	81
3	OSCE	81
4	CEH	62
5	CISA	30
6	GIAC	21
7	GWAPT	15
8	CISM	12
9	CSSLP	10
10	ECSA	9

10. Cyber Security Consultant

#	Certificate	Number of vacanc
1	CISSP	150
2	CISM	128
3	CISA	88
4	CIPP	48
5	CRISC	30
6	CEH	22
7	OSCP	20
8	CCSP	13
9	CIPM	6
10	OSCE	4

Supplementary Table 25: Top 10 requested certificates for the 10 functions that require the most certificates. Source: Jobdigger, edited by Dialogic

1. Noord-Holland

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	40%	6803
2	Cooperate and share information with authorities and professional groups	Man. & Org.	32%	5369
3	Collaborate with other teams and colleagues	Man. & Org.	26%	4291
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	21%	3585
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	5%	809
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	551
7	Design and propose a secure architecture to implement the organisation's strategy	Technical	3%	459
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	3%	458
9	Deploy penetration testing tools and penetration test programs	Technical	2%	414
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	2%	288
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	44%	7356
2	Identify, analyse and correlate cyber security events	Research	41%	6894
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	32%	5447
4	Collaborate with other team members and colleagues	Man. & Org.	26%	4291
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	13%	2167
6	Develop code, scripts and programs	Technical	7%	1187
7	Develop codes, scripts and programs	Technical	7%	1187
8	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	4%	694
9	Think creatively and outside the box	Research	3%	532
10	Identify and select appropriate pedagogical approaches for the intended audience	Research	3%	431
	Key knowledge			
1	Cyber security controls and solutions	Technical	43%	7285
2	Cyber security standards, methodologies and frameworks	Technical	41%	6812
3	Cyber threats	Technical	37%	6197
4	Management practices	Man. & Org.	37%	6152
5	Cyber security risks	Technical	30%	5100
6	Cyber security related laws, regulations and legislations	Legal	30%	4975
7	Cyber security procedures	Man. & Org.	25%	4224
8	Cyber security recommendations and best practices	Man. & Org.	23%	3891
9	Cyber security-related technologies	Technical	18%	3016
10	Cyber security policies	Man. & Org.	16%	2658

2. Zuid-Holland

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	43%	6707
2	Cooperate and share information with authorities and professional groups	Man. & Org.	39%	6104
3	Collaborate with other teams and colleagues	Man. & Org.	34%	5293
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	28%	4379
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	422
6	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2%	367
7	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	256
8	Deploy penetration testing tools and penetration test programs	Technical	1%	218
9	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1%	190
10	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	181
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	44%	6775
2	Identify, analyse and correlate cyber security events	Research	44%	6736
3	Collaborate with other team members and colleagues	Man. & Org.	34%	5296
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	30%	4622
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8%	1198
6	Develop code, scripts and programs	Technical	5%	801
7	Develop codes, scripts and programs	Technical	5%	801
8	Think creatively and outside the box	Research	5%	789
9	Work under pressure	Man. & Org.	3%	424
10	Identify and select appropriate pedagogical approaches for the intended audience	Research	2%	336
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	48%	7395
2	Cyber security controls and solutions	Technical	42%	6511
3	Cyber security related laws, regulations and legislations	Legal	39%	6029
4	Cyber threats	Technical	36%	5622
5	Cyber security procedures	Man. & Org.	34%	5226
6	Management practices	Man. & Org.	29%	4415
7	Cyber security risks	Technical	28%	4371
8	Cyber security recommendations and best practices	Man. & Org.	27%	4242
9	Cyber security policies	Man. & Org.	25%	3861
10	Cyber security-related technologies	Technical	13%	1965

3. Utrecht

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	40%	4500
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	39%	4317
3	Collaborate with other teams and colleagues	Man. & Org.	36%	3963
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	26%	2883
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	3%	281
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	259
7	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	186
8	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	2%	177
9	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	2%	177
10	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	154
	Key skill(s)			
1	Identify, analyse and correlate cyber security events	Research	43%	4765
2	Motivate and encourage people	Man. & Org.	43%	4734
3	Collaborate with other team members and colleagues	Man. & Org.	36%	3963
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	30%	3383
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10%	1131
6	Think creatively and outside the box	Research	6%	696
7	Develop codes, scripts and programs	Technical	6%	630
8	Develop code, scripts and programs	Technical	6%	630
9	Identify and select appropriate pedagogical approaches for the intended audience	Research	3%	340
10	Conduct ethical hacking	Man. & Org.	3%	284
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	49%	5428
2	Cyber security controls and solutions	Technical	41%	4547
3	Cyber threats	Technical	39%	4306
4	Cyber security related laws, regulations and legislations	Legal	35%	3922
5	Cyber security risks	Technical	30%	3373
6	Cyber security procedures	Man. & Org.	30%	3372
7	Cyber security recommendations and best practices	Man. & Org.	28%	3159
8	Management practices	Man. & Org.	26%	2889
9	Cyber security policies	Man. & Org.	22%	2400
10	Cyber security-related technologies	Technical	12%	1371

4. Noord-Brabant

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	41%	2472
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	2173
3	Collaborate with other teams and colleagues	Man. & Org.	28%	1690
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	24%	1470
5	Enforce and advocate organisation's data privacy and protection program	Legal	5%	288
6	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	4%	243
7	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	4%	226
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	141
9	Conduct research, innovation and development work in cyber security-related topics	Research	2%	141
10	Deploy penetration testing tools and penetration test programs	Technical	2%	114
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	46%	2788
2	Identify, analyse and correlate cyber security events	Research	38%	2336
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	33%	2035
4	Collaborate with other team members and colleagues	Man. & Org.	28%	1690
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	11%	695
6	Develop codes, scripts and programs	Technical	7%	409
7	Develop code, scripts and programs	Technical	7%	409
8	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	4%	258
9	Identify and exploit vulnerabilities	Technical	3%	177
10	Identify and select appropriate pedagogical approaches for the intended audience	Research	2%	141
	Key knowledge			
1	Cyber security controls and solutions	Technical	49%	2951
2	Cyber security standards, methodologies and frameworks	Technical	44%	2687
3	Cyber security related laws, regulations and legislations	Legal	33%	2025
4	Cyber threats	Technical	32%	1919
5	Management practices	Man. & Org.	30%	1809
6	Cyber security procedures	Man. & Org.	29%	1779
7	Cyber security recommendations and best practices	Man. & Org.	26%	1604
8	Cyber security risks	Technical	22%	1368
9	Cyber security policies	Man. & Org.	18%	1121
10	Cyber security-related technologies	Technical	16%	985

5. Gelderland

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	42%	1666
2	Cooperate and share information with authorities and professional groups	Man. & Org.	35%	1390
3	Collaborate with other teams and colleagues	Man. & Org.	32%	1253
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	25%	980
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	114
6	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2%	85
7	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	58
8	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	1%	46
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	43
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1%	39
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	45%	1783
2	Identify, analyse and correlate cyber security events	Research	44%	1746
3	Collaborate with other team members and colleagues	Man. & Org.	32%	1253
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	30%	1182
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	209
6	Develop code, scripts and programs	Technical	5%	181
7	Develop codes, scripts and programs	Technical	5%	181
8	Identify and select appropriate pedagogical approaches for the intended audience	Research	4%	150
9	Think creatively and outside the box	Research	2%	82
10	Work under pressure	Man. & Org.	2%	78
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	50%	1962
2	Cyber security controls and solutions	Technical	42%	1650
3	Cyber security related laws, regulations and legislations	Legal	40%	1585
4	Cyber threats	Technical	39%	1522
5	Cyber security procedures	Man. & Org.	35%	1367
6	Cyber security risks	Technical	31%	1237
7	Cyber security recommendations and best practices	Man. & Org.	29%	1138
8	Cyber security policies	Man. & Org.	28%	1115
9	Management practices	Man. & Org.	27%	1053
10	Cyber security-related technologies	Technical	13%	530

6. Overijssel

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	40%	1139
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	1015
3	Collaborate with other teams and colleagues	Man. & Org.	34%	969
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	26%	721
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	3%	72
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	52
7	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	1%	30
8	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	26
9	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1%	20
10	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	20
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	47%	1322
2	Identify, analyse and correlate cyber security events	Research	42%	1183
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	37%	1036
4	Collaborate with other team members and colleagues	Man. & Org.	34%	969
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10%	270
6	Develop codes, scripts and programs	Technical	6%	169
7	Develop code, scripts and programs	Technical	6%	169
8	Identify and select appropriate pedagogical approaches for the intended audience	Research	2%	61
9	Conduct ethical hacking	Technical	1%	42
10	Think creatively and outside the box	Research	1%	40
	Key knowledge			
1	Cyber security controls and solutions	Technical	56%	1575
2	Cyber security standards, methodologies and frameworks	Technical	47%	1340
3	Cyber security related laws, regulations and legislations	Legal	31%	864
4	Cyber threats	Technical	30%	834
5	Cyber security recommendations and best practices	Man. & Org.	27%	773
6	Management practices	Man. & Org.	27%	763
7	Cyber security risks	Technical	24%	664
8	Cyber security procedures	Man. & Org.	23%	651
9	Cyber security policies	Man. & Org.	22%	611
10	Multi-disciplinary aspect of cyber security	Man. & Org.	17%	474

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	37%	598
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	582
3	Collaborate with other teams and colleagues	Man. & Org.	34%	550
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	27%	431
5	Enforce and advocate organisation's data privacy and protection program	Legal	6%	95
6	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Legal	4%	57
7	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	2%	40
8	Manage legal aspects of information security responsibilities and third-party relations	Legal	2%	36
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	32
10	Deploy penetration testing tools and penetration test programs	Technical	2%	27
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	42%	678
2	Identify, analyse and correlate cyber security events	Research	37%	607
3	Collaborate with other team members and colleagues	Man. & Org.	34%	550
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	29%	472
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	7%	116
6	Think creatively and outside the box	Research	7%	108
7	Develop codes, scripts and programs	Technical	5%	85
8	Develop code, scripts and programs	Technical	5%	85
9	Work under pressure	Man. & Org.	3%	55
10	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	2%	37
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	49%	801
2	Cyber security controls and solutions	Technical	41%	672
3	Cyber security related laws, regulations and legislations	Legal	34%	549
4	Cyber security procedures	Man. & Org.	33%	542
5	Cyber threats	Technical	30%	483
6	Cyber security recommendations and best practices	Man. & Org.	28%	454
7	Management practices	Man. & Org.	27%	445
8	Cyber security policies	Man. & Org.	26%	420
9	Cyber security risks	Technical	21%	345
10	Multi-disciplinary aspect of cyber security	Man. & Org.	9%	148

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	41%	469
2	Collaborate with other teams and colleagues	Man. & Org.	37%	416
3	Develop relationships with cyber security-related authorities and communities	Man. & Org.	37%	415
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	26%	298
5	Manage legal aspects of information security responsibilities and third-party relations	Legal	2%	19
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	19
7	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	1%	14
8	Deploy penetration testing tools and penetration test programs	Technical	1%	13
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	12
10	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	1%	11
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	47%	535
2	Identify, analyse and correlate cyber security events	Research	44%	496
3	Collaborate with other team members and colleagues	Man. & Org.	37%	417
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	31%	353
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	62
6	Develop codes, scripts and programs	Technical	4%	51
7	Develop code, scripts and programs	Technical	4%	51
8	Think creatively and outside the box	Research	4%	42
9	Design systems and architectures based on security and privacy by design and by defaults cyber security principles	Technical	3%	32
10	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	2%	20
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	53%	598
2	Cyber security related laws, regulations and legislations	Legal	39%	442
3	Cyber security controls and solutions	Technical	37%	420
4	Cyber threats	Technical	34%	390
5	Cyber security procedures	Man. & Org.	33%	375
6	Cyber security policies	Man. & Org.	33%	370
7	Cyber security recommendations and best practices	Man. & Org.	30%	339
8	Management practices	Man. & Org.	28%	317
9	Cyber security risks	Technical	25%	286
10	Multi-disciplinary aspect of cyber security	Man. & Org.	8%	87

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	39%	239
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	36%	221
3	Collaborate with other teams and colleagues	Man. & Org.	35%	211
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	27%	166
5	Manage legal aspects of information security responsibilities and third-party relations	Legal	3%	19
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	16
7	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	2%	14
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	10
9	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2%	10
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1%	9
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	45%	277
2	Identify, analyse and correlate cyber security events	Research	40%	242
3	Collaborate with other team members and colleagues	Man. & Org.	35%	211
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	33%	200
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	12%	74
6	Develop codes, scripts and programs	Technical	7%	41
7	Develop code, scripts and programs	Technical	7%	41
8	Think creatively and outside the box	Research	6%	35
9	Conduct ethical hacking	Technical	4%	26
10	Identify and select appropriate pedagogical approaches for the intended audience	Research	4%	23
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	46%	284
2	Cyber security procedures	Man. & Org.	42%	256
3	Cyber security controls and solutions	Technical	42%	255
4	Cyber security related laws, regulations and legislations	Legal	38%	233
5	Cyber threats	Technical	38%	230
6	Management practices	Man. & Org.	35%	211
7	Cyber security risks	Technical	30%	181
8	Cyber security recommendations and best practices	Man. & Org.	27%	165
9	Cyber security policies	Man. & Org.	25%	155
10	Cyber security-related technologies	Technical	10%	62

10. Friesland

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	42%	259
2	Collaborate with other teams and colleagues	Man. & Org.	39%	236
3	Develop relationships with cyber security-related authorities and communities	Man. & Org.	36%	217
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	31%	191
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	21
6	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2%	15
7	Design and propose a secure architecture to implement the organisation's strategy	Technical	2%	12
8	Assist in designing, implementing, auditing and compliance testing activities in order to ensure cyber security and privacy compliance	Man. & Org.	2%	10
9	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	9
10	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	1%	7
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	42%	259
2	Collaborate with other team members and colleagues	Man. & Org.	39%	236
3	Identify, analyse and correlate cyber security events	Research	35%	216
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	19%	118
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8%	47
6	Develop codes, scripts and programs	Technical	4%	22
7	Develop code, scripts and programs	Technical	4%	22
8	Think creatively and outside the box	Research	3%	18
9	Identify and select appropriate pedagogical approaches for the intended audience	Research	3%	18
10	Work under pressure	Man. & Org.	3%	16
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	45%	272
2	Cyber security related laws, regulations and legislations	Legal	40%	245
3	Cyber security procedures	Man. & Org.	33%	200
4	Cyber security controls and solutions	Technical	32%	198
5	Management practices	Man. & Org.	32%	194
6	Cyber security policies	Man. & Org.	29%	179
7	Cyber security recommendations and best practices	Man. & Org.	26%	159
8	Cyber threats	Technical	25%	150
9	Cyber security risks	Technical	19%	118
10	Multi-disciplinary aspect of cyber security	Man. & Org.	8%	49

11. Drenthe

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	43%	202
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	43%	202
3	Collaborate with other teams and colleagues	Man. & Org.	37%	173
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	29%	136
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	13
6	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	7
7	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	1%	5
8	Ensure the senior management approves the cyber security risks of the organisation	Man. & Org.	1%	4
9	Assist in cyber security-related capacity building including awareness, theoretical training, practical training, testing, mentoring, supervising and sharing	Education	1%	4
10	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	4
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	48%	224
2	Identify, analyse and correlate cyber security events	Research	44%	208
3	Collaborate with other team members and colleagues	Man. & Org.	37%	173
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	28%	133
5	Identify and select appropriate pedagogical approaches for the intended audience	Research	6%	27
6	Develop codes, scripts and programs	Technical	4%	21
7	Develop code, scripts and programs	Technical	4%	21
8	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	4%	21
9	Design systems and architectures based on security and privacy by design and by defaults cyber security principles	Technical	3%	14
10	Work under pressure	Man. & Org.	3%	12
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	56%	261
2	Cyber security related laws, regulations and legislations	Legal	45%	211
3	Cyber security procedures	Man. & Org.	39%	183
4	Cyber security controls and solutions	Technical	39%	182
5	Cyber security policies	Man. & Org.	38%	178
6	Cyber threats	Technical	35%	163
7	Cyber security recommendations and best practices	Man. & Org.	33%	156
8	Management practices	Man. & Org.	32%	150
9	Cyber security risks	Technical	27%	127
10	Risk management standards, methodologies and frameworks	Man. & Org.	8%	39

12. Zeeland

#	Building blocks	Category	% vacancies	Number of vacancies
	Main tasks			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	116
2	Collaborate with other teams and colleagues	Man. & Org.	36%	115
3	Develop relationships with cyber security-related authorities and communities	Man. & Org.	27%	88
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	25%	80
5	Enforce and advocate organisation's data privacy and protection program	Legal	5%	17
6	Manage legal aspects of information security responsibilities and third-party relations	Legal	4%	12
7	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	2%	8
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	7
9	Deploy penetration testing tools and penetration test programs	Technical	1%	4
10	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	1%	2
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	38%	122
2	Identify, analyse and correlate cyber security events	Research	38%	121
3	Collaborate with other team members and colleagues	Man. & Org.	36%	115
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	27%	87
5	Think creatively and outside the box	Research	9%	28
6	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	17
7	Develop code, scripts and programs	Technical	4%	13
8	Develop codes, scripts and programs	Technical	4%	13
9	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	3%	10
10	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	3%	9
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	42%	135
2	Cyber security procedures	Man. & Org.	33%	107
3	Cyber security related laws, regulations and legislations	Legal	33%	106
4	Cyber security policies	Man. & Org.	29%	93
5	Cyber threats	Technical	26%	83
6	Cyber security controls and solutions	Technical	25%	80
7	Management practices	Man. & Org.	23%	73
8	Cyber security risks	Technical	21%	69
9	Cyber security recommendations and best practices	Man. & Org.	20%	65
10	Cyber security-related technologies	Technical	13%	43

Supplementary Table 26: Individual tasks, knowledge and skills required in the regions

Junior – MBO

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	30%	490
2	Collaborate with other teams and colleagues	Man. & Org.	26%	429
3	Develop relationships with cyber security-related authorities and communities	Man. & Org.	26%	425
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	19%	309
5	Enforce and advocate organisation's data privacy and protection program	Legal	2%	25
6	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	10
7	Deploy penetration testing tools and penetration test programs	Technical	1%	10
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1%	9
9	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1%	9
10	Identify and assess cyber security-related threats and vulnerabilities of ICT systems	Research	0%	8
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	41%	677
2	Work on operating systems, servers, clouds and relevant infrastructures	Technical	31%	503
3	Identify, analyse and correlate cyber security events	Research	29%	472
4	Collaborate with other team members and colleagues	Man. & Org.	26%	429
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	88
6	Think creatively and outside the box	Research	5%	76
7	Work under pressure	Man. & Org.	4%	69
8	Develop code, scripts and programs	Technical	4%	61
9	Develop codes, scripts and programs	Technical	4%	61
10	Identify and select appropriate pedagogical approaches for the intended audience	Research	2%	36
	Key knowledge			
1	Cyber security controls and solutions	Technical	38%	622
2	Management practices	Man. & Org.	31%	505
3	Cyber security standards, methodologies and frameworks	Technical	29%	482
4	Cyber threats	Technical	29%	475
5	Cyber security related laws, regulations and legislations	Legal	24%	389
6	Cyber security procedures	Man. & Org.	23%	378
7	Cyber security risks	Technical	17%	280
8	Cyber security recommendations and best practices	Man. & Org.	15%	246
9	Cyber security policies	Man. & Org.	11%	183
10	Cyber security-related technologies	Technical	10%	163

Junior – HBO

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	35%	3257
2	Cooperate and share information with authorities and professional groups	Man. & Org.	34%	3188
3	Collaborate with other teams and colleagues	Man. & Org.	30%	2782
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	24%	2194
5	Enforce and advocate organisation's data privacy and protection program	Legal	3%	234
6	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2%	206
7	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	2%	167
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	123
9	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1%	119
10	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	114
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	44%	4086
2	Identify, analyse and correlate cyber security events	Research	43%	3929
3	Collaborate with other team members and colleagues	Man. & Org.	30%	2782
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	30%	2745
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8%	757
6	Develop code, scripts and programs	Technical	8%	715
7	Develop codes, scripts and programs	Technical	8%	715
8	Think creatively and outside the box	Research	4%	362
9	Conduct ethical hacking	Technical	3%	271
10	Work under pressure	Man. & Org.	3%	241
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	44%	4085
2	Cyber security controls and solutions	Technical	43%	3940
3	Cyber threats	Technical	36%	3299
4	Cyber security related laws, regulations and legislations	Legal	33%	3062
5	Management practices	Man. & Org.	29%	2690
6	Cyber security risks	Technical	28%	2574
7	Cyber security procedures	Man. & Org.	28%	2563
8	Cyber security recommendations and best practices	Man. & Org.	26%	2435
9	Cyber security policies	Man. & Org.	20%	1806
10	Cyber security-related technologies	Technical	14%	1253

Junior – WO

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	48%	1200
2	Cooperate and share information with authorities and professional groups	Man. & Org.	45%	1141
3	Collaborate with other teams and colleagues	Man. & Org.	39%	991
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	30%	750
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2%	54
6	Enforce and advocate organisation's data privacy and protection program	Legal	2%	49
7	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	2%	42
8	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	2%	39
9	Deploy penetration testing tools and penetration test programs	Technical	1%	35
10	Manage legal aspects of information security responsibilities and third-party relations	Legal	1%	29
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	54%	1365
2	Identify, analyse and correlate cyber security events	Research	48%	1200
3	Collaborate with other team members and colleagues	Man. & Org.	39%	991
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	25%	635
5	Develop code, scripts and programs	Technical	10%	242
6	Develop codes, scripts and programs	Technical	10%	242
7	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	9%	223
8	Think creatively and outside the box	Research	3%	87
9	Work under pressure	Man. & Org.	3%	64
10	Conduct ethical hacking	Technical	2%	61
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	44%	1116
2	Cyber security controls and solutions	Technical	40%	1014
3	Management practices	Man. & Org.	37%	928
4	Cyber security related laws, regulations and legislations	Legal	36%	895
5	Cyber security recommendations and best practices	Man. & Org.	35%	890
6	Cyber threats	Technical	35%	875
7	Cyber security procedures	Man. & Org.	31%	772
8	Cyber security risks	Technical	28%	713
9	Cyber security policies	Man. & Org.	24%	593
10	Multi-disciplinary aspect of cyber security	Man. & Org.	15%	385

Intermediate – MBO

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	28%	429
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	26%	392
3	Collaborate with other teams and colleagues	Man. & Org.	24%	373
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	20%	308
5	Enforce and advocate organisation's data privacy and protection program	Legal	2%	25
6	Deploy penetration testing tools and penetration test programs	Technical	1%	20
7	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	18
8	Contribute to the development of the organisation's cyber security strategy, policy and procedures	Man. & Org.	1%	9
9	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	1%	9
10	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1%	8
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	40%	617
2	Work on operating systems, servers, clouds and relevant infrastructures	Technical	37%	561
3	Identify, analyse and correlate cyber security events	Research	26%	400
4	Collaborate with other team members and colleagues	Man. & Org.	24%	373
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	5%	79
6	Think creatively and outside the box	Research	3%	48
7	Develop codes, scripts and programs	Technical	3%	40
8	Develop code, scripts and programs	Technical	3%	40
9	Work under pressure	Man. & Org.	2%	36
10	Identify and select appropriate pedagogical approaches for the intended audience	Research	2%	36
	Key knowledge			
1	Cyber security controls and solutions	Technical	40%	608
2	Cyber security standards, methodologies and frameworks	Technical	36%	552
3	Cyber threats	Technical	30%	465
4	Management practices	Man. & Org.	30%	464
5	Cyber security procedures	Man. & Org.	29%	443
6	Cyber security related laws, regulations and legislations	Legal	26%	398
7	Cyber security recommendations and best practices	Man. & Org.	18%	270
8	Cyber security risks	Technical	16%	245
9	Cyber security policies	Man. & Org.	16%	241
10	Cyber security-related technologies	Technical	13%	195

Intermediate – HBO

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	43%	7637
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	6348
3	Collaborate with other teams and colleagues	Man. & Org.	30%	5342
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	24%	4349
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	4%	672
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	590
7	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	3%	551
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	368
9	Design and propose a secure architecture to implement the organisation's strategy	Technical	2%	353
10	Deploy penetration testing tools and penetration test programs	Technical	2%	321
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	43%	7656
2	Identify, analyse and correlate cyber security events	Research	43%	7586
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	36%	6491
4	Collaborate with other team members and colleagues	Man. & Org.	30%	5343
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	10%	1726
6	Develop code, scripts and programs	Technical	6%	1152
7	Develop codes, scripts and programs	Technical	6%	1152
8	Think creatively and outside the box	Research	4%	701
9	Identify and select appropriate pedagogical approaches for the intended audience	Research	3%	507
10	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	3%	489
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	51%	9084
2	Cyber security controls and solutions	Technical	48%	8605
3	Cyber threats	Technical	39%	6979
4	Cyber security related laws, regulations and legislations	Legal	36%	6375
5	Cyber security procedures	Man. & Org.	32%	5637
6	Cyber security risks	Technical	31%	5608
7	Management practices	Man. & Org.	31%	5457
8	Cyber security recommendations and best practices	Man. & Org.	27%	4797
9	Cyber security policies	Man. & Org.	21%	3764
10	Cyber security-related technologies	Technical	17%	3048

Intermediate – WO

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	52%	2301
2	Cooperate and share information with authorities and professional groups	Man. & Org.	47%	2081
3	Collaborate with other teams and colleagues	Man. & Org.	41%	1818
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	34%	1505
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	5%	218
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	152
7	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	2%	96
8	Deploy penetration testing tools and penetration test programs	Technical	2%	89
9	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	2%	88
10	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	86
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	52%	2314
2	Identify, analyse and correlate cyber security events	Research	49%	2161
3	Collaborate with other team members and colleagues	Man. & Org.	41%	1818
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	28%	1234
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	14%	617
6	Develop code, scripts and programs	Technical	6%	245
7	Develop codes, scripts and programs	Technical	6%	245
8	Identify and select appropriate pedagogical approaches for the intended audience	Research	3%	155
9	Think creatively and outside the box	Research	3%	149
10	Work under pressure	Man. & Org.	3%	128
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	56%	2471
2	Cyber security related laws, regulations and legislations	Legal	44%	1976
3	Cyber security controls and solutions	Technical	44%	1952
4	Cyber threats	Technical	40%	1767
5	Cyber security recommendations and best practices	Man. & Org.	37%	1644
6	Management practices	Man. & Org.	36%	1597
7	Cyber security procedures	Man. & Org.	36%	1585
8	Cyber security risks	Technical	36%	1581
9	Cyber security policies	Man. & Org.	32%	1430
10	Multi-disciplinary aspect of cyber security	Man. & Org.	12%	539

Senior – MBO				
#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	295
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	35%	288
3	Collaborate with other teams and colleagues	Man. & Org.	35%	282
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	23%	191
5	Deploy penetration testing tools and penetration test programs	Technical	4%	29
6	Enforce and advocate organisation's data privacy and protection program	Legal	1%	11
7	Identify and assess cyber security-related threats and vulnerabilities of ICT systems	Research	1%	10
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1%	10
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1%	7
10	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	0%	4
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	46%	377
2	Identify, analyse and correlate cyber security events	Research	37%	302
3	Collaborate with other team members and colleagues	Man. & Org.	35%	282
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	33%	266
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	7%	54
6	Work under pressure	Man. & Org.	6%	47
7	Think creatively and outside the box	Research	4%	30
8	Assess the security and performance of solutions	Technical	4%	29
9	Develop codes, scripts and programs	Technical	3%	22
10	Develop code, scripts and programs	Technical	3%	22
	Key knowledge			
1	Cyber security controls and solutions	Technical	43%	351
2	Cyber security standards, methodologies and frameworks	Technical	34%	279
3	Cyber security related laws, regulations and legislations	Legal	33%	270
4	Cyber threats	Technical	32%	258
5	Management practices	Man. & Org.	31%	256
6	Cyber security procedures	Man. & Org.	30%	245
7	Cyber security risks	Technical	16%	132
8	Cyber security recommendations and best practices	Man. & Org.	15%	121
9	Cyber security-related technologies	Technical	10%	83
10	Cyber security policies	Man. & Org.	10%	78

Senior – HBO				
#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	44%	3568
2	Cooperate and share information with authorities and professional groups	Man. & Org.	36%	2867
3	Collaborate with other teams and colleagues	Man. & Org.	30%	2399
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	25%	1988
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	5%	420
6	Enforce and advocate organisation's data privacy and protection program	Legal	4%	344
7	Design and propose a secure architecture to implement the organisation's strategy	Technical	2%	196
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	2%	169
9	Deploy penetration testing tools and penetration test programs	Technical	2%	168
10	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	167
	Key skill(s)			
1	Identify, analyse and correlate cyber security events	Research	45%	3600
2	Motivate and encourage people	Man. & Org.	44%	3536
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	33%	2645
4	Collaborate with other team members and colleagues	Man. & Org.	30%	2399
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	13%	1045
6	Think creatively and outside the box	Research	5%	381
7	Develop codes, scripts and programs	Technical	4%	348
8	Develop code, scripts and programs	Technical	4%	348
9	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	4%	286
10	Conduct ethical hacking	Technical	3%	221
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	46%	3717
2	Cyber security controls and solutions	Technical	46%	3681
3	Cyber threats	Technical	39%	3179
4	Cyber security related laws, regulations and legislations	Legal	35%	2847
5	Cyber security risks	Technical	32%	2583
6	Management practices	Man. & Org.	32%	2544
7	Cyber security procedures	Man. & Org.	29%	2316
8	Cyber security recommendations and best practices	Man. & Org.	28%	2231
9	Cyber security policies	Man. & Org.	21%	1681
10	Cyber security-related technologies	Technical	17%	1378

Senior – WO				
#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	54%	1398
2	Cooperate and share information with authorities and professional groups	Man. & Org.	46%	1197
3	Collaborate with other teams and colleagues	Man. & Org.	39%	1006
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	33%	846
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	4%	109
6	Enforce and advocate organisation's data privacy and protection program	Legal	3%	77
7	Design and propose a secure architecture to implement the organisation's strategy	Technical	2%	49
8	Deploy penetration testing tools and penetration test programs	Technical	2%	47
9	Manage legal aspects of information security responsibilities and third-party relations	Legal	2%	46
10	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	2%	44
	Key skill(s)			
1	Identify, analyse and correlate cyber security events	Research	51%	1326
2	Motivate and encourage people	Man. & Org.	51%	1320
3	Collaborate with other team members and colleagues	Man. & Org.	39%	1009
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	22%	572
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	13%	334
6	Develop code, scripts and programs	Technical	4%	116
7	Develop codes, scripts and programs	Technical	4%	116
8	Think creatively and outside the box	Research	3%	86
9	Design systems and architectures based on security and privacy by design and by defaults cyber security principles	Technical	3%	78
10	Identify and select appropriate pedagogical approaches for the intended audience	Research	3%	75
	Key knowledge			
1	Cyber security standards, methodologies and frameworks	Technical	48%	1254
2	Cyber security related laws, regulations and legislations	Legal	43%	1127
3	Management practices	Man. & Org.	40%	1042
4	Cyber threats	Technical	38%	984
5	Cyber security controls and solutions	Technical	36%	944
6	Cyber security risks	Technical	34%	888
7	Cyber security procedures	Man. & Org.	33%	854
8	Cyber security recommendations and best practices	Man. & Org.	31%	804
9	Cyber security policies	Man. & Org.	30%	782
10	Multi-disciplinary aspect of cyber security	Man. & Org.	16%	415

Supplementary Table 27: Individual tasks, knowledge and skills broken down by vacancies, based on the level of education requested and work experience

SBI 46 – Wholesale and commercial intermediation (not in cars and motorcycles)

#	Building blocks	Category	Number
	Main task(s)		
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	1422
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1220
3	Collaborate with other teams and colleagues	Man. & Org.	1022
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	588
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	205
6	Enforce and advocate organisation's data privacy and protection program	Legal	199
7	Conduct research, innovation and development work in cyber security-related topics	Research	113
8	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	81
9	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	73
10	Deploy penetration testing tools and penetration test programs	Technical	68
	Key skill(s)		
1	Work on operating systems, servers, clouds and relevant infrastructures	Technical	1406
2	Motivate and encourage people	Man. & Org.	1378
3	Identify, analyse and correlate cyber security events	Research	1255
4	Collaborate with other team members and colleagues	Man. & Org.	1022
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	883
6	Think creatively and outside the box	Research	508
7	Develop codes, scripts and programs	Technical	224
8	Develop code, scripts and programs	Technical	224
9	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	164
10	Identify and exploit vulnerabilities	Technical	105
	Key knowledge		
1	Cyber security controls and solutions	Technical	2164
2	Cyber security standards, methodologies and frameworks	Technical	1388
3	Management practices	Man. & Org.	1035
4	Cyber security related laws, regulations and legislations	Legal	1031
5	Cyber threats	Technical	912
6	Cyber security-related research, development and innovation (RDI)	Research	766
7	Cyber security recommendations and best practices	Man. & Org.	748
8	Cyber security procedures	Man. & Org.	715
9	Cyber security risks	Technical	643
10	Cyber security-related technologies	Technical	590

SBI 62 – Information technology service activities

#	Building blocks	Category	Number
	Main task(s)		
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	2589
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1607
3	Collaborate with other teams and colleagues	Man. & Org.	1424
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	1089
5	Enforce and advocate organisation's data privacy and protection program	Legal	181
6	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	151
7	Deploy penetration testing tools and penetration test programs	Technical	124
8	Assist in designing, implementing, auditing and compliance testing activities in order to ensure cyber security and privacy compliance	Man. & Org.	110
9	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	101
10	Design and propose a secure architecture to implement the organisation's strategy	Technical	72
	Key skill(s)		
1	Work on operating systems, servers, clouds and relevant infrastructures	Technical	2933
2	Motivate and encourage people	Man. & Org.	2486
3	Identify, analyse and correlate cyber security events	Research	2418
4	Collaborate with other team members and colleagues	Man. & Org.	1424
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	561
6	Develop codes, scripts and programs	Technical	479
7	Develop code, scripts and programs	Technical	479
8	Think creatively and outside the box	Research	331
9	Conduct ethical hacking	Technical	312
10	Identify and exploit vulnerabilities	Technical	177
	Key knowledge		
1	Cyber security controls and solutions	Technical	3502
2	Cyber security standards, methodologies and frameworks	Technical	3154
3	Cyber threats	Technical	2412
4	Cyber security procedures	Man. & Org.	1937
5	Management practices	Man. & Org.	1906
6	Cyber security related laws, regulations and legislations	Legal	1890
7	Cyber security risks	Technical	1852
8	Cyber security recommendations and best practices	Man. & Org.	1393
9	Cyber security-related technologies	Technical	1355
10	Multi-disciplinary aspect of cyber security	Man. & Org.	775

SBI 84 – Public administration, government services and compulsory social security

#	Building blocks	Category	Number
	Main task(s)		
1	Cooperate and share information with authorities and professional groups	Man. & Org.	4581
2	Collaborate with other teams and colleagues	Man. & Org.	4401
3	Develop relationships with cyber security-related authorities and communities	Man. & Org.	3998
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	3486
5	Enforce and advocate organisation's data privacy and protection program	Legal	266
6	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	169
7	Manage legal aspects of information security responsibilities and third-party relations	Legal	167
8	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	121
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	31
10	Ensure the organisation's resiliency to cyber incidents	Man. & Org.	24
	Key skill(s)		
1	Collaborate with other team members and colleagues	Man. & Org.	4401
2	Identify, analyse and correlate cyber security events	Research	4400
3	Motivate and encourage people	Man. & Org.	4233
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	2222
5	Work under pressure	Man. & Org.	447
6	Identify and select appropriate pedagogical approaches for the intended audience	Research	374
7	Develop code, scripts and programs	Technical	263
8	Develop codes, scripts and programs	Technical	263
9	Think creatively and outside the box	Research	159
10	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	150
	Key knowledge		
1	Cyber security standards, methodologies and frameworks	Technical	4858
2	Cyber security procedures	Man. & Org.	4445
3	Cyber security related laws, regulations and legislations	Legal	3944
4	Cyber threats	Technical	3641
5	Cyber security policies	Man. & Org.	3376
6	Cyber security recommendations and best practices	Man. & Org.	3077
7	Cyber security controls and solutions	Technical	2781
8	Cyber security risks	Technical	2652
9	Management practices	Man. & Org.	1973
10	Multi-disciplinary aspect of cyber security	Man. & Org.	787

SBI 69 – Legal services, accountancy, tax advice and administration

#	Building blocks	Category	Number
	Main task(s)		
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	1752
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1189
3	Collaborate with other teams and colleagues	Man. & Org.	894
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	739
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	454
6	Design and propose a secure architecture to implement the organisation's strategy	Technical	259
7	Enforce and advocate organisation's data privacy and protection program	Legal	164
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	98
9	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	86
10	Assist in designing, implementing, auditing and compliance testing activities in order to ensure cyber security and privacy compliance	Man. & Org.	86
	Key skill(s)		
1	Motivate and encourage people	Man. & Org.	2654
2	Identify, analyse and correlate cyber security events	Research	2162
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	1085
4	Collaborate with other team members and colleagues	Man. & Org.	894
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	512
6	Develop code, scripts and programs	Technical	359
7	Develop codes, scripts and programs	Technical	359
8	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	343
9	Conduct ethical hacking	Technical	205
10	Think creatively and outside the box	Research	151
	Key knowledge		
1	Management practices	Man. & Org.	2709
2	Cyber security controls and solutions	Technical	1864
3	Cyber threats	Technical	1813
4	Cyber security standards, methodologies and frameworks	Technical	1734
5	Cyber security risks	Technical	1630
6	Cyber security related laws, regulations and legislations	Legal	1435
7	Cyber security recommendations and best practices	Man. & Org.	1288
8	Cyber security procedures	Man. & Org.	1119
9	Multi-disciplinary aspect of cyber security	Man. & Org.	902
10	Cyber security-related technologies	Technical	876

SBI 70 – Holdings (non-financial), group services within own group and management consultancy

#	Building blocks	Category	Number
	Main task(s)		
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	1538
2	Cooperate and share information with authorities and professional groups	Man. & Org.	1190
3	Collaborate with other teams and colleagues	Man. & Org.	913
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	787
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	164
6	Enforce and advocate organisation's data privacy and protection program	Legal	127
7	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	70
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	67
9	Design and propose a secure architecture to implement the organisation's strategy	Technical	66
10	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	57
	Key skill(s)		
1	Motivate and encourage people	Man. & Org.	1762
2	Identify, analyse and correlate cyber security events	Research	1392
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	1300
4	Collaborate with other team members and colleagues	Man. & Org.	913
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	315
6	Develop code, scripts and programs	Technical	285
7	Develop codes, scripts and programs	Technical	285
8	Conduct ethical hacking	Technical	130
9	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	94
10	Think creatively and outside the box	Research	87
	Key knowledge		
1	Cyber security controls and solutions	Technical	1735
2	Cyber security standards, methodologies and frameworks	Technical	1725
3	Cyber security related laws, regulations and legislations	Legal	1341
4	Management practices	Man. & Org.	1287
5	Cyber threats	Technical	1223
6	Cyber security recommendations and best practices	Man. & Org.	1152
7	Cyber security risks	Technical	976
8	Cyber security procedures	Man. & Org.	840
9	Cyber security policies	Man. & Org.	646
10	Cyber security-related technologies	Technical	534

Supplementary Table 28: Top building blocks per sector. Source: Jobdigger, edited by Dialogic

Cyber R&D

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	59,6%	337
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	45,0%	254
3	Collaborate with other teams and colleagues	Man. & Org.	40,9%	231
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	30,6%	173
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2,5%	14
6	Secure resources to implement the cyber security strategy	Man. & Org.	1,9%	11
7	Review, plan and allocate appropriate cyber security resources	Man. & Org.	1,9%	11
8	Deploy penetration testing tools and penetration test programs	Technical	1,4%	8
9	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1,4%	8
10	Produce architectural documentation and specifications	Technical	1,1%	6
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	56,5%	319
2	Collaborate with other team members and colleagues	Man. & Org.	40,9%	231
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	36,6%	207
4	Identify, analyse and correlate cyber security events	Research	31,5%	178
5	Develop codes, scripts and programs	Technical	19,1%	108
6	Develop code, scripts and programs	Technical	19,1%	108
7	Identify and select appropriate pedagogical approaches for the intended audience	Research	9,2%	52
8	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8,7%	49
9	Manage and analyse log files	Technical	3,5%	20
10	Think creatively and outside the box	Research	2,5%	14
	Key knowledge			
1	Management practices	Man. & Org.	0,2%	1
2	Cyber security controls and solutions	Technical	0,4%	2
3	Cyber security procedures	Man. & Org.	0,5%	3
4	Cyber threats	Technical	0,7%	4
5	Cyber security recommendations and best practices	Man. & Org.	0,9%	5
6	Cyber security standards, methodologies and frameworks	Technical	1,1%	6
7	Cyber security related laws, regulations and legislations	Legal	1,2%	7
8	Pedagogical standards, methodologies and frameworks	Education	1,4%	8
9	Cyber security risks	Technical	1,6%	9
10	Cyber security policies	Man. & Org.	1,8%	10

Cyber integration

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	41,8%	5053
2	Cooperate and share information with authorities and professional groups	Man. & Org.	41,2%	4982
3	Collaborate with other teams and colleagues	Man. & Org.	34,5%	4169
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	26,0%	3151
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	3,8%	461
6	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	3,4%	407
7	Enforce and advocate organisation's data privacy and protection program	Legal	2,8%	333
8	Deploy penetration testing tools and penetration test programs	Technical	2,3%	274
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	1,9%	232
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1,8%	216
	Key skill(s)			
1	Identify, analyse and correlate cyber security events	Research	43,6%	5273
2	Motivate and encourage people	Man. & Org.	38,8%	4690
3	Collaborate with other team members and colleagues	Man. & Org.	34,5%	4169
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	30,4%	3680
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	17,3%	2098
6	Develop codes, scripts and programs	Technical	7,1%	864
7	Develop code, scripts and programs	Technical	7,1%	864
8	Think creatively and outside the box	Research	6,4%	777
9	Decompose and analyse systems to develop security and privacy requirements and identify effective solutions	Technical	3,1%	373
10	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	2,6%	319
	Key knowledge			
1	Cyber security controls and solutions	Technical	43,7%	5288
2	Cyber security standards, methodologies and frameworks	Technical	42,5%	5143
3	Cyber threats	Technical	34,7%	4199
4	Cyber security related laws, regulations and legislations	Legal	31,5%	3811
5	Cyber security procedures	Man. & Org.	29,5%	3566
6	Management practices	Man. & Org.	28,4%	3432
7	Cyber security risks	Technical	28,3%	3427
8	Cyber security recommendations and best practices	Man. & Org.	23,9%	2885
9	Cyber security policies	Man. & Org.	16,6%	2007
10	Cyber security-related technologies	Technical	15,7%	1905

Cyber production

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	41,5%	3580
2	Cooperate and share information with authorities and professional groups	Man. & Org.	24,9%	2147
3	Collaborate with other teams and colleagues	Man. & Org.	19,4%	1669
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	16,3%	1401
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	6,1%	525
6	Design and propose a secure architecture to implement the organisation's strategy	Technical	3,7%	323
7	Enforce and advocate organisation's data privacy and protection program	Legal	2,8%	238
8	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	1,6%	140
9	Deploy penetration testing tools and penetration test programs	Technical	1,6%	139
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1,6%	135
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	47,4%	4084
2	Identify, analyse and correlate cyber security events	Research	41,4%	3567
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	35,5%	3056
4	Collaborate with other team members and colleagues	Man. & Org.	19,4%	1669
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	9,1%	784
6	Think creatively and outside the box	Research	7,7%	666
7	Develop codes, scripts and programs	Technical	6,9%	596
8	Develop code, scripts and programs	Technical	6,9%	596
9	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	4,9%	420
10	Conduct ethical hacking	Technical	4,8%	415
	Key knowledge			
1	Cyber security controls and solutions	Technical	50,4%	4345
2	Management practices	Man. & Org.	42,6%	3672
3	Cyber threats	Technical	41,1%	3541
4	Cyber security standards, methodologies and frameworks	Technical	38,2%	3291
5	Cyber security risks	Technical	34,2%	2947
6	Cyber security related laws, regulations and legislations	Legal	29,1%	2509
7	Cyber security procedures	Man. & Org.	27,9%	2409
8	Cyber security recommendations and best practices	Man. & Org.	23,4%	2018
9	Cyber security-related technologies	Technical	19,0%	1642
10	Multi-disciplinary aspect of cyber security	Man. & Org.	19,0%	1639

Business lives

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	41,0%	7251
2	Cooperate and share information with authorities and professional groups	Man. & Org.	29,0%	5128
3	Collaborate with other teams and colleagues	Man. & Org.	23,5%	4163
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	18,1%	3206
5	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	5,5%	967
6	Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy	Technical	3,3%	585
7	Enforce and advocate organisation's data privacy and protection program	Legal	3,0%	528
8	Deploy penetration testing tools and penetration test programs	Technical	2,7%	481
9	Design and propose a secure architecture to implement the organisation's strategy	Technical	2,6%	466
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1,8%	326
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	41,2%	7300
2	Identify, analyse and correlate cyber security events	Research	40,2%	7111
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	33,6%	5953
4	Collaborate with other team members and colleagues	Man. & Org.	23,5%	4163
5	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	16,3%	2885
6	Think creatively and outside the box	Research	7,6%	1337
7	Develop codes, scripts and programs	Technical	7,5%	1336
8	Develop code, scripts and programs	Technical	7,5%	1336
9	Anticipate required changes to the organisation's information security strategy and formulate new plans	Man. & Org.	4,1%	730
10	Conduct ethical hacking	Technical	3,1%	557
	Key knowledge			
1	Cyber security controls and solutions	Technical	49,9%	8839
2	Cyber security standards, methodologies and frameworks	Technical	39,3%	6950
3	Cyber threats	Technical	35,9%	6360
4	Management practices	Man. & Org.	35,5%	6282
5	Cyber security risks	Technical	29,6%	5235
6	Cyber security related laws, regulations and legislations	Legal	26,1%	4615
7	Cyber security procedures	Man. & Org.	23,4%	4151
8	Cyber security recommendations and best practices	Man. & Org.	22,6%	4001
9	Cyber security-related technologies	Technical	19,5%	3447
10	Multi-disciplinary aspect of cyber security	Man. & Org.	15,5%	2751

Government

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	57,8%	3981
2	Collaborate with other teams and colleagues	Man. & Org.	53,2%	3666
3	Develop relationships with cyber security-related authorities and communities	Man. & Org.	46,3%	3188
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	42,4%	2918
5	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	1,5%	104
6	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	1,1%	75
7	Enforce and advocate organisation's data privacy and protection program	Legal	1,0%	68
8	Manage legal aspects of information security responsibilities and third-party relations	Legal	0,8%	55
9	Develop and propose staff awareness training to achieve compliance and foster a culture of data protection within the organization	Education	0,5%	36
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	0,4%	30
	Key skill(s)			
1	Identify, analyse and correlate cyber security events	Research	58,1%	4004
2	Collaborate with other team members and colleagues	Man. & Org.	53,2%	3666
3	Motivate and encourage people	Man. & Org.	52,1%	3586
4	Work on operating systems, servers, clouds and relevant infrastructures	Technical	30,6%	2110
5	Work under pressure	Man. & Org.	5,7%	391
6	Develop code, scripts and programs	Technical	5,2%	356
7	Develop codes, scripts and programs	Technical	5,2%	356
8	Identify and select appropriate pedagogical approaches for the intended audience	Research	4,4%	306
9	Think creatively and outside the box	Research	3,6%	246
10	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	2,1%	147
	Key knowledge			
1	Cyber security procedures	Man. & Org.	57,3%	3947
2	Cyber security standards, methodologies and frameworks	Technical	55,3%	3810
3	Cyber threats	Technical	46,0%	3166
4	Cyber security related laws, regulations and legislations	Legal	42,0%	2893
5	Cyber security controls and solutions	Technical	35,5%	2446
6	Cyber security risks	Technical	34,3%	2360
7	Cyber security policies	Man. & Org.	32,9%	2264
8	Cyber security recommendations and best practices	Man. & Org.	32,5%	2239
9	Management practices	Man. & Org.	22,8%	1571
10	Multi-disciplinary aspect of cyber security	Man. & Org.	12,0%	824

Educational/knowledge institutions

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Cooperate and share information with authorities and professional groups	Man. & Org.	62,3%	410
2	Develop relationships with cyber security-related authorities and communities	Man. & Org.	46,5%	306
3	Collaborate with other teams and colleagues	Man. & Org.	43,2%	284
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	36,6%	241
5	Develop organisation's cyber security architecture to address security and privacy requirements	Technical	2,9%	19
6	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	2,1%	14
7	Review, plan and allocate appropriate cyber security resources	Man. & Org.	1,7%	11
8	Secure resources to implement the cyber security strategy	Man. & Org.	1,7%	11
9	Deploy penetration testing tools and penetration test programs	Technical	1,2%	8
10	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1,2%	8
	Key skill(s)			
1	Motivate and encourage people	Man. & Org.	54,1%	356
2	Collaborate with other team members and colleagues	Man. & Org.	43,2%	284
3	Work on operating systems, servers, clouds and relevant infrastructures	Technical	32,7%	215
4	Identify, analyse and correlate cyber security events	Research	31,9%	210
5	Develop codes, scripts and programs	Technical	17,3%	114
6	Develop code, scripts and programs	Technical	17,3%	114
7	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	8,1%	53
8	Identify and select appropriate pedagogical approaches for the intended audience	Research	7,9%	52
9	Think creatively and outside the box	Research	3,3%	22
10	Manage and analyse log files	Technical	3,0%	20
	Key knowledge			
1	Management practices	Man. & Org.	40,4%	266
2	Cyber security controls and solutions	Technical	38,8%	255
3	Cyber security procedures	Man. & Org.	33,0%	217
4	Cyber threats	Technical	31,5%	207
5	Cyber security recommendations and best practices	Man. & Org.	28,3%	186
6	Cyber security standards, methodologies and frameworks	Technical	26,3%	173
7	Cyber security related laws, regulations and legislations	Legal	25,1%	165
8	Pedagogical standards, methodologies and frameworks	Education	21,4%	141
9	Cyber security risks	Technical	19,6%	129
10	Cyber security policies	Man. & Org.	18,5%	122

Other

#	Building blocks	Category	% vacancies	Number of vacancies
	Main task(s)			
1	Develop relationships with cyber security-related authorities and communities	Man. & Org.	34,0%	145
2	Cooperate and share information with authorities and professional groups	Man. & Org.	29,3%	125
3	Collaborate with other teams and colleagues	Man. & Org.	26,5%	113
4	Cooperate with key personnel for reporting of security incidents according to applicable legal framework	Legal	17,8%	76
5	Assist in designing, implementing, auditing and compliance testing activities in order to ensure cyber security and privacy compliance	Man. & Org.	5,6%	24
6	Implement threat intelligence collection, analysis and production of actionable intelligence and dissemination to security stakeholders	Technical	1,9%	8
7	Design and propose a secure architecture to implement the organisation's strategy	Technical	1,2%	5
8	Conduct privacy impact assessments and develop, maintain, communicate and train upon the privacy policies, procedures	Legal	0,9%	4
9	Develop an organisation's cyber security risk management strategy	Man. & Org.	0,7%	3
10	Identify cross-sectoral cyber security achievements and apply them in a different context or propose innovative approaches and solutions	Research	0,7%	3
	Key skill(s)			
1	Work on operating systems, servers, clouds and relevant infrastructures	Technical	34,0%	145
2	Identify, analyse and correlate cyber security events	Research	33,5%	143
3	Motivate and encourage people	Man. & Org.	28,6%	122
4	Collaborate with other team members and colleagues	Man. & Org.	26,5%	113
5	Develop code, scripts and programs	Technical	14,1%	60
6	Develop codes, scripts and programs	Technical	14,1%	60
7	Conduct ethical hacking	Technical	11,9%	51
8	Work under pressure	Man. & Org.	6,8%	29
9	Communicate, coordinate and cooperate with internal and external stakeholders	Man. & Org.	6,1%	26
10	Conduct technical analysis and reporting	Technical	5,6%	24
	Key knowledge			
1	Cyber threats	Technical	42,6%	182
2	Cyber security standards, methodologies and frameworks	Technical	39,8%	170
3	Cyber security controls and solutions	Technical	37,5%	160
4	Cyber security risks	Technical	33,0%	141
5	Cyber security related laws, regulations and legislations	Legal	27,9%	119
6	Management practices	Man. & Org.	24,1%	103
7	Cyber security procedures	Man. & Org.	23,0%	98
8	Cyber security recommendations and best practices	Man. & Org.	21,5%	92
9	Cyber security-related technologies	Technical	17,6%	75
10	Cyber security policies	Man. & Org.	16,4%	70

Supplementary Table 29: Building blocks per target group, based on the Top 100 organisations. Source: Jobdigger, edited by Dialogic