Report: Understanding European Cybersecurity HR Recruitment Processes

- A collaboration between the European Cyber Security Organisation (ECSO) and the European Cybersecurity Competence Network Pilot projects

Contents

1 Introduction

This paper provides the key findings and results from the analysis around understanding how cybersecurity recruitment and overall HR processes and motivations work in Europe, based on survey responses received over the course of two months (April-May 2021). This analysis on Understanding European Cybersecurity HR Recruitment Processes in Europe is a collaboration between the Working Group (WG5) for human factors & competence building at the European Cyber Security Organisation (ECSO) (https://www.ecs-org.eu) and the Cybersecurity Competence Network (https://cybercompetencenetwork.eu).

The European Cyber Security Organisation (ECSO) is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016. ECSO was the privileged partner of the European Commission for the implementation of the Cybersecurity Public-Private Partnership (2016-2020) and aims to coordinate the development of the European Cybersecurity Ecosystem and support the protection of the European Digital Single Market, to ultimately contribute to the advancement of European digital sovereignty and strategic autonomy. Thanks to its large membership network from across Europe which includes national and regional public administrations, large companies, SMEs, research centres/academia, associations and users/operators, ECSO is in a unique position to cover the various aspects of cybersecurity R&I and industrial policy with the intention of building a comprehensive approach for strengthening the cybersecurity ecosystem in Europe. This includes various activities on education, training, skills and awareness in its WG5, where a dedicated Task Force has also been set up to help address the cybersecurity skills gap. European Human Resources for Cyber (EHR4CYBER) aims to create awareness among decision makers (private companies, regional / local administrations, national / EU administrations) about the need to develop education, training and recruitment measures, which will address the demand in the cybersecurity field. EHR4CYBER therefore focuses on activities related, but not limited to, working on a common benchmarking system in cybersecurity recruitment, fostering collaboration through the exchange of best practices, looking into the harmonisation of education and training procedures across Europe, as well as supporting the recruitment process of cybersecurity specialists.

The four pilot projects (CONCORDIA, ECHO, SPARTA and CyberSec4Europe) have been chosen to address the Horizon 2020 Cybersecurity call “Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap”. The collaboration of these four pilot project consortia of over 160 partners establishes the foundation of the European Cybersecurity Network and Competence Centre.

ECSO and ECHO spearheaded the following work, with the support of ENISA, Concordia, CyberSec4Europe, and SPARTA.

2 Understanding European Cybersecurity HR Recruitment Processes - Study by the European Cyber Security Organisation (ECSO) and the Cybersecurity Competence Network

The overall purpose of the survey was to assess how organisations in Europe currently address the recruitment of cybersecurity specialists, given the well-known shortage of cybersecurity specialists in the EU and worldwide, and provide the foundation to create a Cyber HR Toolbox. Cybersecurity is an overarching domain that starts and ends with the humans involved in the process, either working on security or being able to carry out their work relying on security hardened infrastructure. While there are many standards and best practices addressing the technologies and processes in the cybersecurity domain, the human is usually approached either as an IT/cyber professional or end-user to be trained. The HR perspective and challenges are often neglected or handled as a "traditional" HR process.

HR approaches and best practices should cover the attraction, motivation, and retention of workforce talent. Cybersecurity is not only an overarching domain, but also an interdisciplinary one, meaning it heavily builds on additional competences such as networking, coding or soft skills like communication and analytical thinking. For these reasons, HR professionals face the challenge where they either use a pre-set template to hire professionals trying to fit them into a job position, backed with industry accepted certificates, or try novel approaches with up- and re-skilling talents strongly in the domains required to turn them into a cyber specialist.

In this research, authors focused on the possible creation of an EU Cyber HR Toolbox by understanding the challenges HR professionals face, along with the practices they currently use addressing the challenges. Based on the data collected and the analysis conducted, the following recommendations are made:

1. The demand for an EU Cyber HR Toolkit is justified

- HR professionals have limited access to knowledge pools when it comes to the cyber domain
- Cybersecurity is still usually addressed as a standalone solution

2. Support the creation of an HR cyber knowledge pool

- Integration of HR topics in the broader context, rather than "just" addressing the skills gap challenge
- Sharing of best practices, approaches and lessons learned

3. There is a need for new approaches to competence building

- Cybersecurity and digital transformation challenges must be looked at in a broader context, not in silos
- Cybersecurity and digital competence building should step over the limitation of formal education and training to be integrated more into the work environment

4. There is a need for European data

- The research is based on inputs by volunteers; however, there is no accessible data on the relevant European landscape
- Research efforts should focus on the whole value-chain while a talent is being born and hired (from academia through trainings, vocational learning, self-improvement and hiring, and organisational and individual perspectives as well)

5. Integration of synergies and efforts is a must

- While cybersecurity is overarching, approaches to solving challenges are still silo based
- Academia, training providers, HR professionals, talents and workplaces should be able to cooperate to ensure that the right competences and working environments are being developed

The data for the “Understanding European Cybersecurity HR Recruitment Processes” report was gathered through an online survey, which took place from April until the end of May 2021. The survey results are presented in the following analysis.

The number of respondents were limited, given the short timeframe, which naturally affects the representativeness and validity of results. Nevertheless, the responses provide an initial overview of the situation, and the following analysis includes additional findings from roundtable discussions organised by the ECHO project and ECSO representatives. Moreover, open-ended qualitative questions of this survey provide important information about their current services and potential needs.

This analysis is completed in collaboration between five organisations / networks, and their respective authors are responsible for the content.

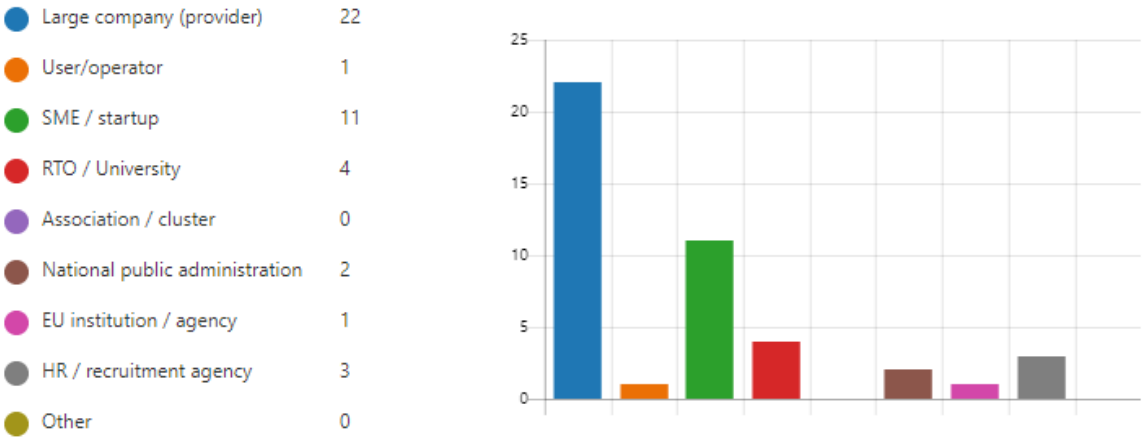
3 Analysis and Results

3.1 Background of the Respondents

The number of respondents amounted to forty-four (n=44), and their positions varied from employee to director from forty (40) different European organisations (F.

The organisations that the respondents represented were mainly medium to large size organisations (over 50 employees): 13 organisations with between 5 and 50 employees, 7 organisations between 50 to 250, and 24 organisations with more than 250 employees.
No organisations with less than five employees responded to this survey (Figure 2).

Figure 1 – Type of Organisation



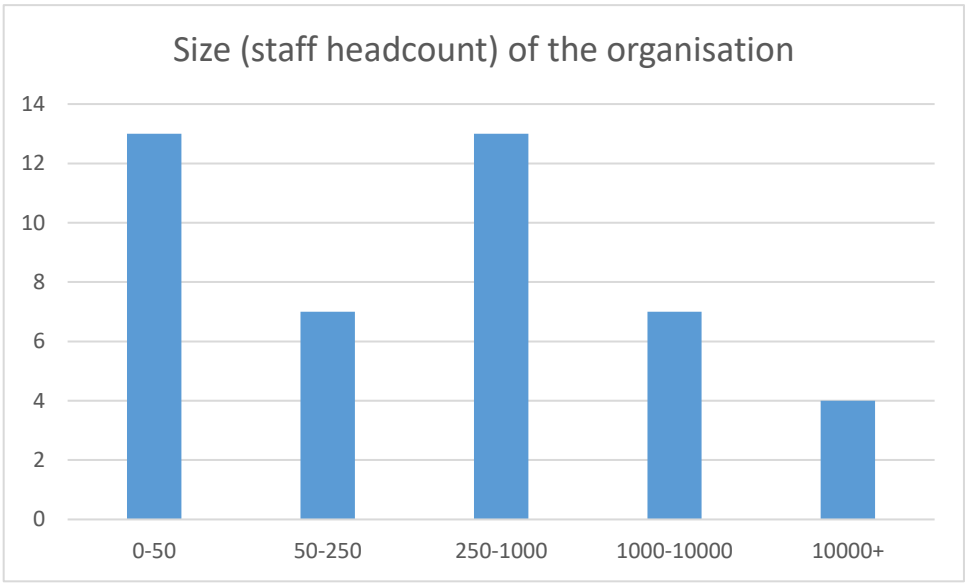


Figure 2 - Number of Employees

Most of the organisations that responded are in the IT sector: 30 vs 14 for non-IT organisations (Figure 3).

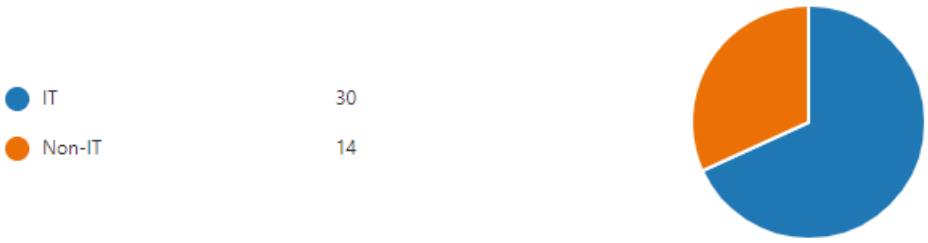


Figure 3 - Sector of the Organisation

Figure 4 demonstrates that from an economical sector perspective, the respondents were quite balanced with representation from several different sectors. The most represented sectors were Finance (6) and Telecommunications (6). 9 organisations are linked to other (not mentioned) sectors.

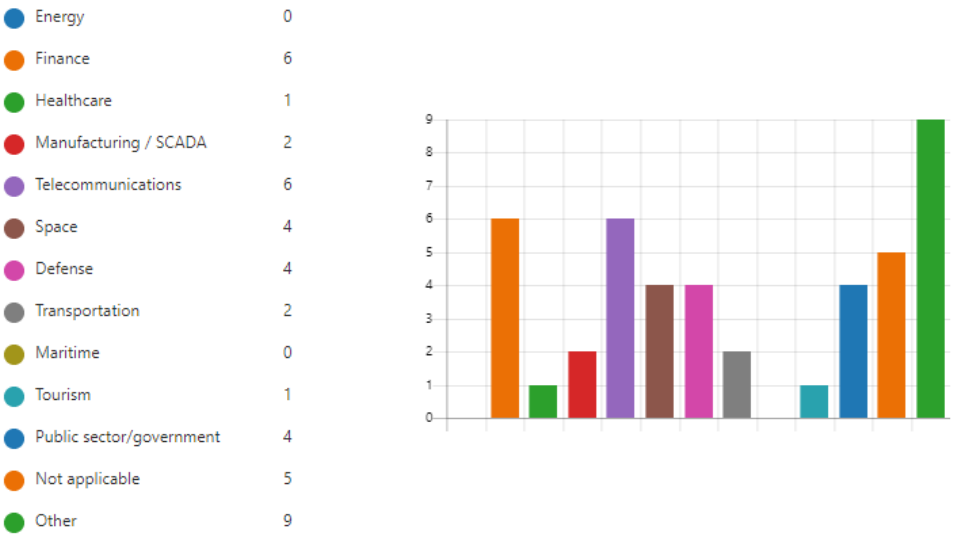


Figure 4 - Economic Sector of the Organisation

From a market segment perspective, 32 respondents included large enterprises among their main customers, while 28 deal with governmental clients. 17 of the respondents deal with SMEs (Figure 5).

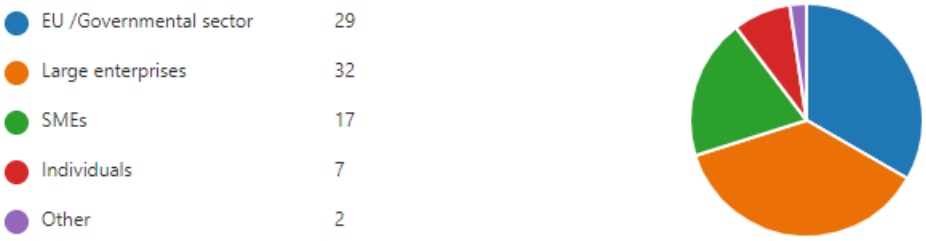


Figure 5 - Main Customers of the Organisation

Figure 6 shows the age of the respondents: 30 respondents were between 30 and 50 years old and a majority of respondents were female, as shown in Figure 7.

Figure 6 - Age of the respondents

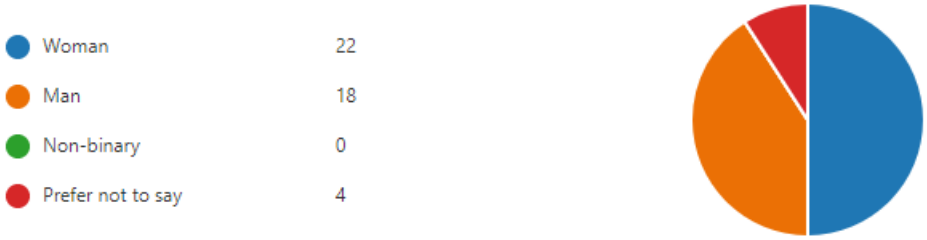


Figure 7 - Gender of the respondents

39 participants indicated that they have a master's degree, or higher.

3.2 HR expectations and practices

All respondents indicated that they have some type of dedicated cybersecurity team, 27 use an internal cybersecurity department, and others handle cybersecurity matters with an outsourced or hybrid model (Figure 8).

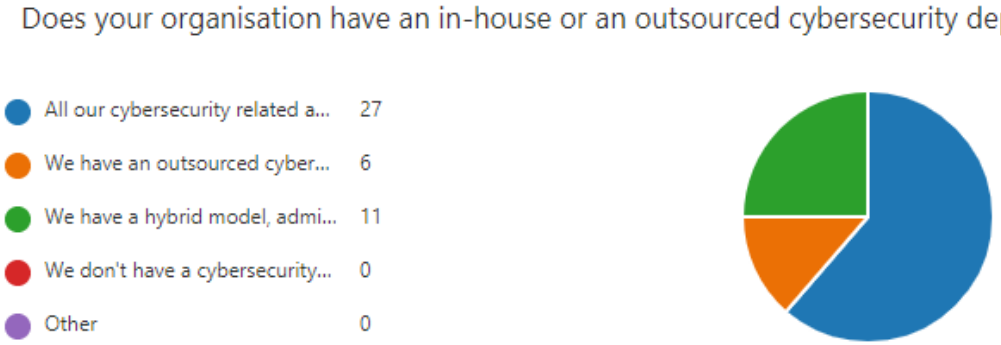


Figure 8 - Cybersecurity department

IT organisations tend to have in-house cybersecurity recruitment teams more often than non-IT organisations, as seen in Figure 9 and 10.

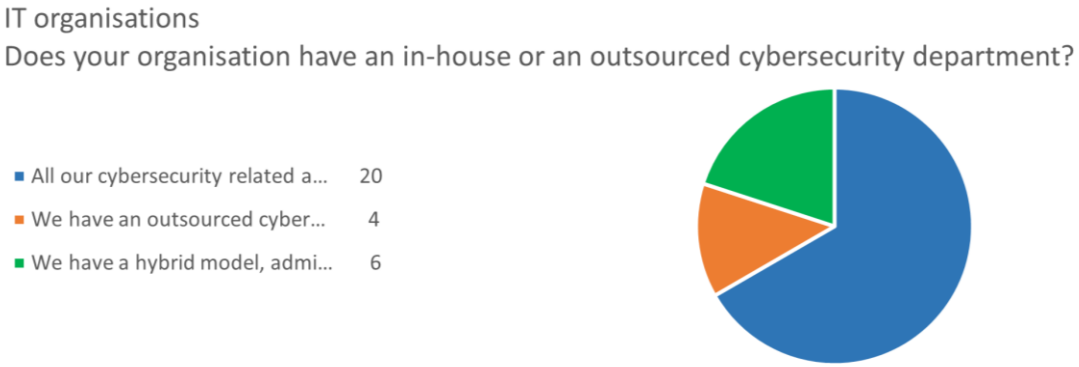


Figure 9 – Cybersecurity department for IT organisations

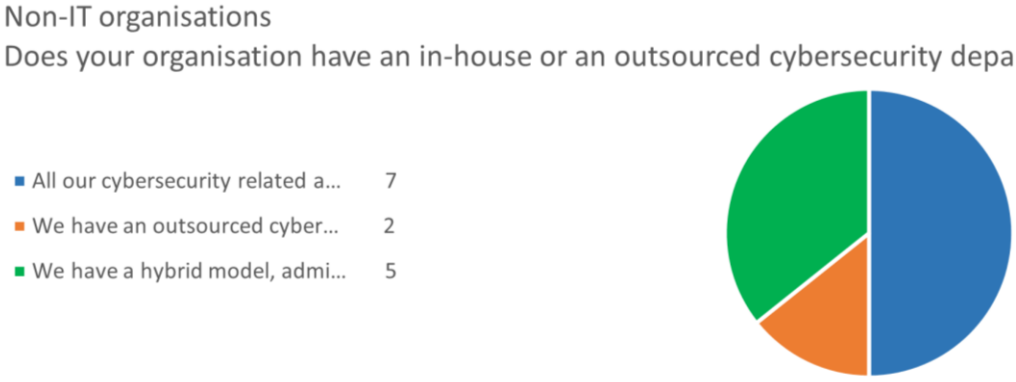


Figure 10 – Cybersecurity department for non-IT organisations

Figure 11 shows that 38 organisations have a dedicated recruitment department, with size ranging from 1 to 100 resources.

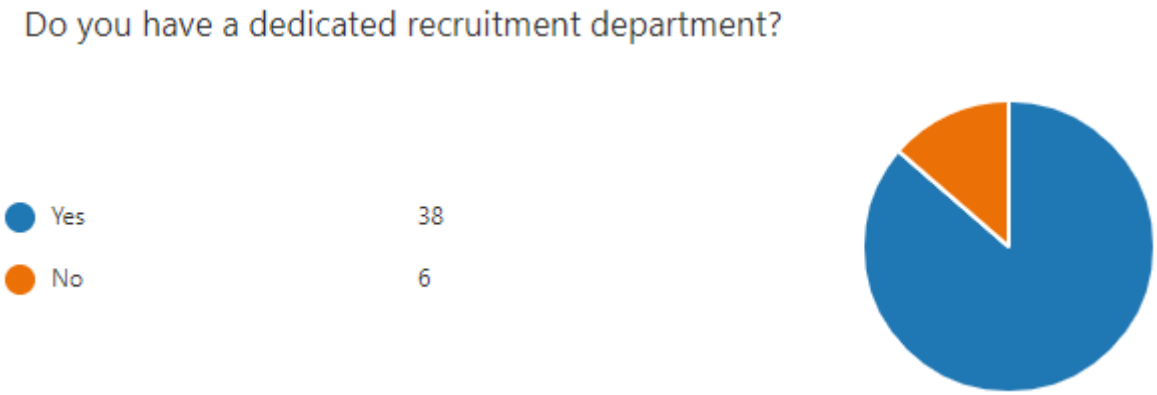


Figure 11 – Recruitment department

Of the 6 respondents who indicated that they do not have a dedicated recruitment department, 3 of them manage recruitment matters directly in-house (by management), while 2 of them use a combination of recruitment agency plus some in-house research (Figure 12).

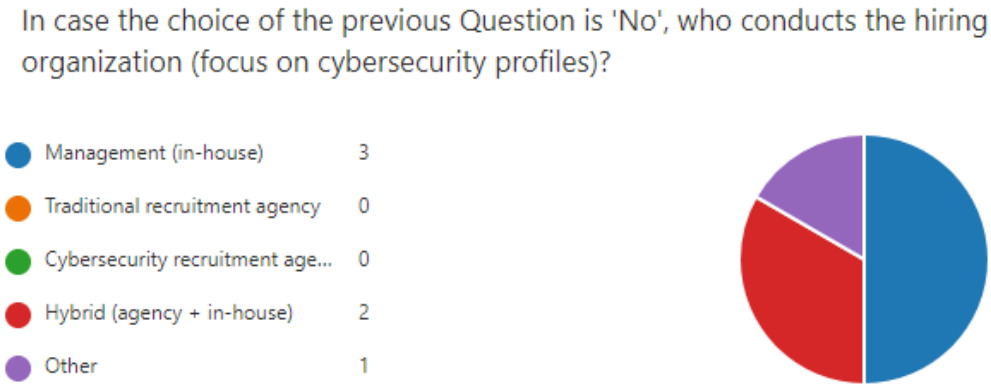


Figure 12 – Hiring process approach

The survey asked respondents to indicate which cybersecurity roles are the most sought after. Figure 13 shows that the most frequently hired roles are Security operations analysts (22), immediately followed by Software developers for cybersecurity products/solutions (21). The

survey also clearly lists a serious interest in Security architects (19) and Cybersecurity managers (19).

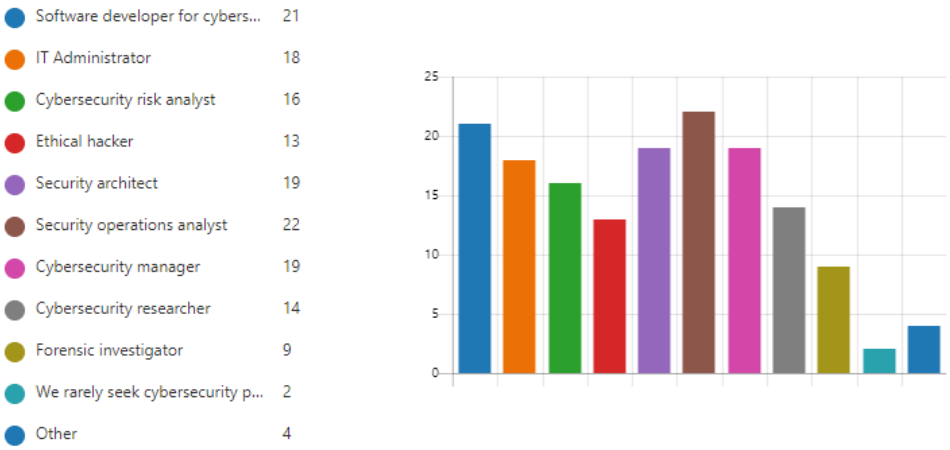


Figure 13 – Cybersecurity Roles Most Frequently Sought

In terms of planned hiring numbers, all organisations are planning to hire at least 1 cybersecurity specialist within the next 12 months (from 1 to 150). About half of the organisations plan to hire in between 1 and 10 cybersecurity professionals.

When hiring IT specialists, it is clear that most of the organisations give cybersecurity a specific focus: 15 of them actually consider cybersecurity experience as a prerequisite to hire any IT specialist (Figure 14).

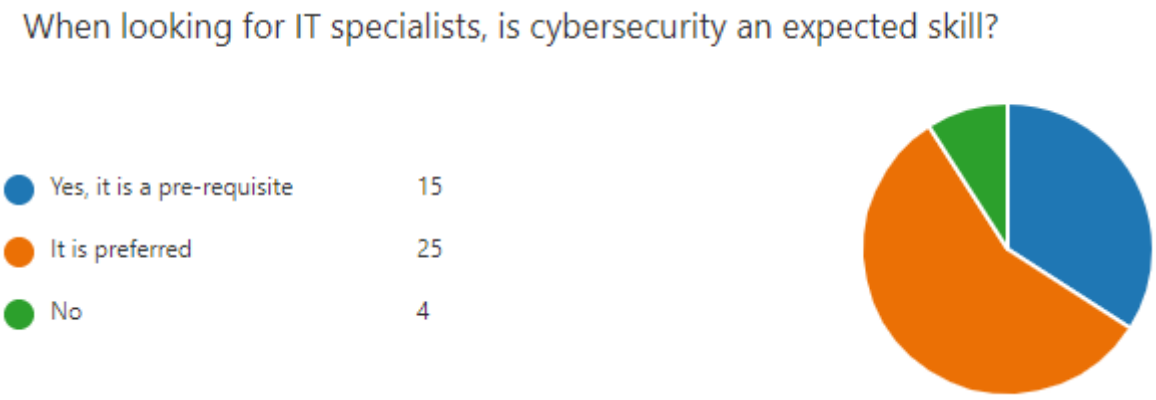


Figure 14 – Cybersecurity as a Skill for IT Specialists

Comparing Figures 15 and 16 indicates that when hiring IT specialists, IT organisations require cybersecurity skills twice as often than non-IT organisations

Figure 15 – Cybersecurity as a Skill for IT Specialists in IT Organisations

Figure 16 – Cybersecurity as a Skill for IT Specialists in Non-IT Organisations

Most of the respondents (34) said that that they usually search for cybersecurity specialists from within the EU while 9 respondents indicated that they also search for specialists worldwide, as is seen in Figure 17.

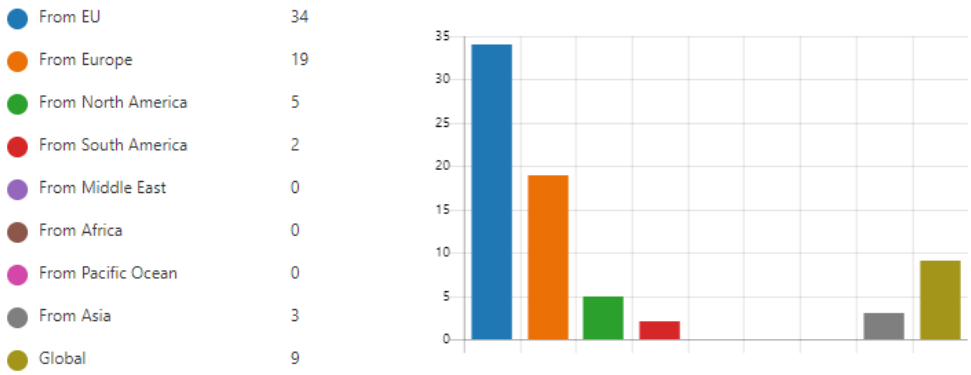


Figure 17 – Cybersecurity Specialists Recruitment Zones

Figure 18 demonstrates the majority of the respondents indicated that they create individual job descriptions when creating new cybersecurity positions. One respondent stated that they use the NIST framework as the industry best practice when creating a job description for cybersecurity profiles.

Figure 18 – Cybersecurity Position Specification

As seen in Figure 19, similar considerations can be made for the definition of the job title. 25 respondents adhere to their internal structure while 6 respondents are using existing standards and taxonomies. Among them, NICE and the European Skills, Competences, Qualifications and Occupations (ESCO) classification are the most used.

This is interesting considering that ENISA is currently developing a European cybersecurity skills framework. It appears that the time is ripe for such a framework as it should allow European stakeholders to apply a classification and framework to job profiles that fits the needs of the European job market. It would be interesting to take stock of the application of ENISA's framework once it has been out for a year or so (at the time of writing, the framework is still under development).

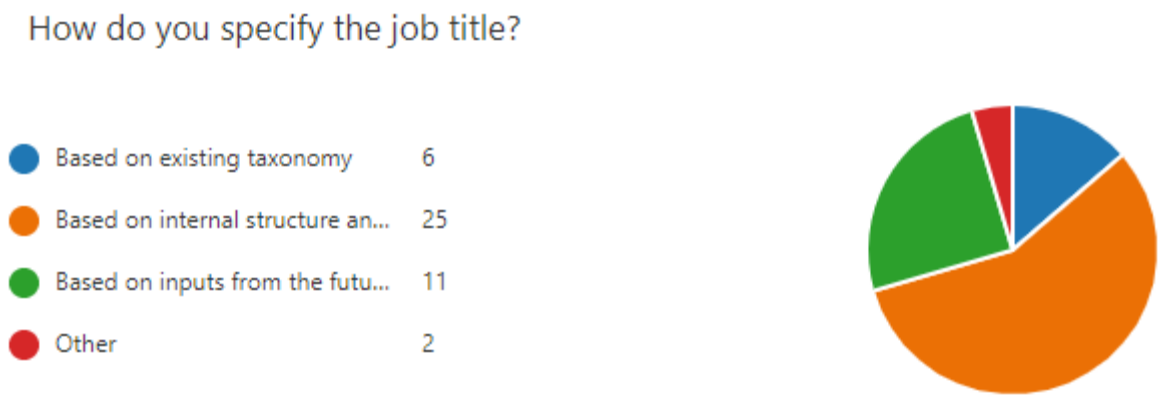


Figure 19 – Cybersecurity Job Title Definition

Figure 20 shows that 31 participants consider certifications relevant when selecting candidates but they still prefer candidates with stronger working experience. However, 9 respondents do not consider candidates without the minimum education/certification requirements.

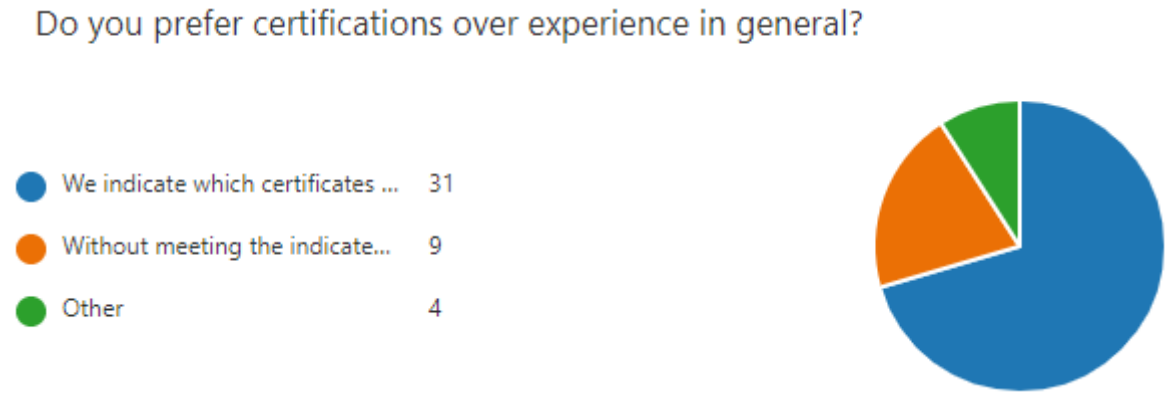


Figure 20 – Certification over Experience

The choice which education/certifications are needed are generally (in 30 cases) driven by the manager hiring for the position (Figure 21).

Figure 21 – Selecting Relevant Certifications for a Vacancy

Figure 22 shows that from an education perspective, 25 participants noted that experience is most relevant, while generally holding a BSc or a Master's degree is an advantage (during the selection process), and 13 respondents highlighted that at least a BSc is generally necessary for any cybersecurity position.

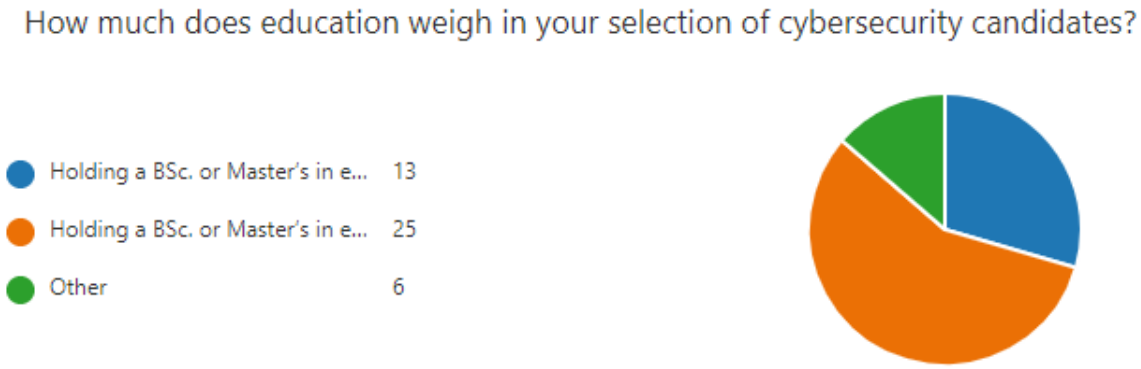


Figure 22 – Weight of Education on Cybersecurity Candidate Selection

From a candidate assessment perspective, most of the participants (24) conduct practical skills assessment during the interviews. However, 2 respondents do not perform hands-on assessment of the candidates (as a deliberate choice), while 18 adopt this approach only in some cases. When experience is more relevant than education, indications are that tasks and challenges are performed 60% of the time (Figure 23).

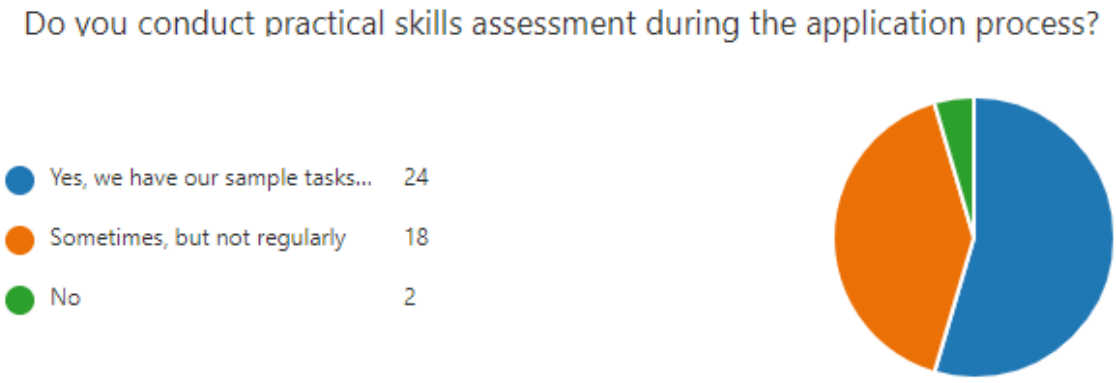


Figure 23 – Using Skills Assessment during Application Process

To determine the salaries for cybersecurity candidates we can observe a variety of approaches. 10 organisations refer to internal remuneration schemes, while 9 make offers proportional to the candidate's experience. 17 respondents indicated that they leverage a combination of factors to assess the salaries (Figure 24).

Figure 24 – Setting the Salary Level for Cybersecurity Professionals

Figure 25 shows how there is an interesting variety on how candidates are found by organisations searching for cybersecurity specialists. Social media and company websites are leading the category (36) but many organisations also leverage on their internal network (33) and personal recommendation (26).

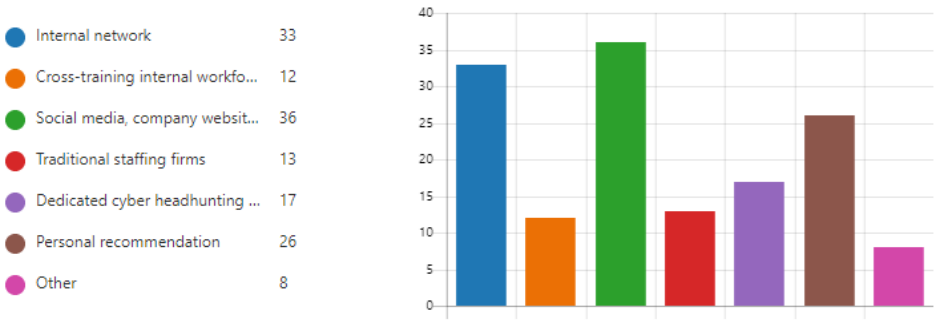


Figure 25 – How to Find Cybersecurity Candidates

The retention of cybersecurity experts seems to be an important problem for the respondents. Various measures are put in place to retain cybersecurity professionals. Offering trainings and involving the cybersecurity experts in innovative activities and projects seem among the most used means to retain experts, as demonstrated in Figure 26.

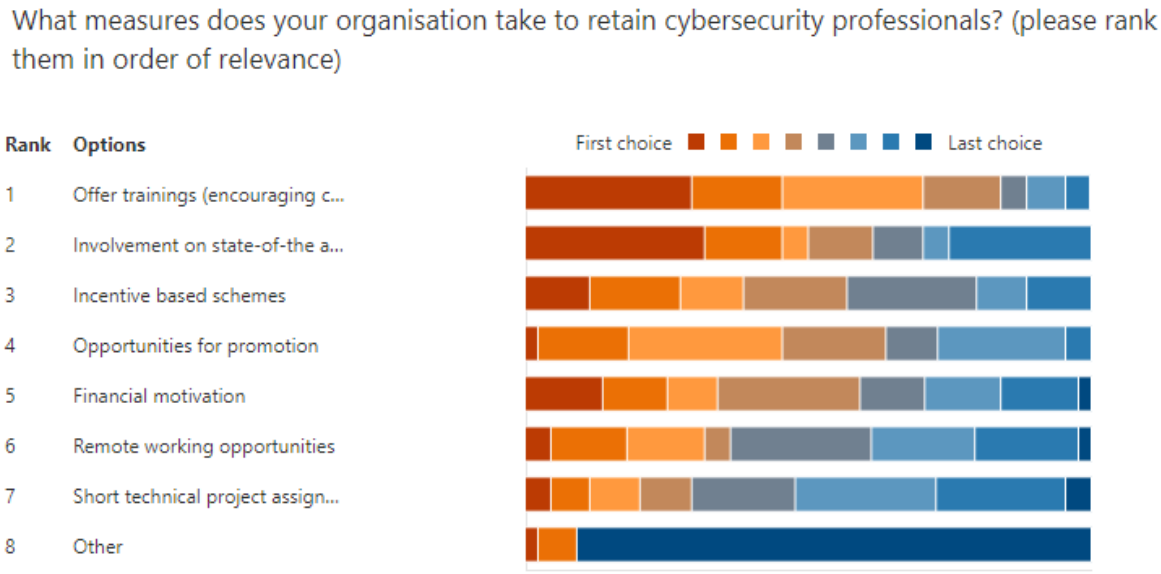


Figure 26 – How to Retain Cybersecurity Experts

Organisations seem to be investing in the education of their cybersecurity professionals: 39 of the respondents indicated that they offer at least one (paid) training per year (Figure 27). Trainings are mainly provided via external organisations but 14 respondents indicated that they are delivered in-house (Figure 28).

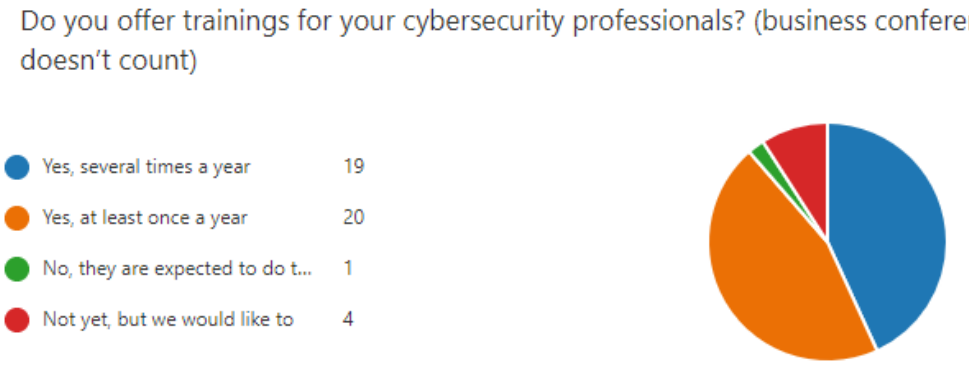


Figure 27 – Training Programmes for Cybersecurity Experts

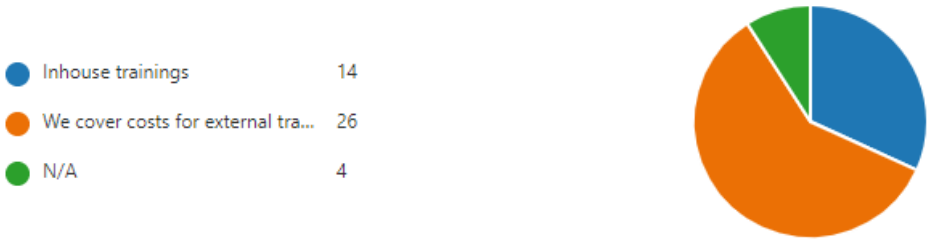


Figure 28 – How Training Programmes are Offered

It is interesting to understand how much time, on average, these organisations need to fill their cybersecurity positions. While no one states that they are able to fill the positions in one to two weeks, the majority indicates up to six months for the recruitment process, which is considerably slower than in order knowledge domains. Seven respondents stated that they have difficulties with filling their cybersecurity positions. While this would appear a low number, it still indicates that some support from HR is still needed to better reach the right candidates. Out of those 7 respondents, 5 are large companies. Large companies also represent the majority of organisations who fill positions in over 6 months (Figure 29).

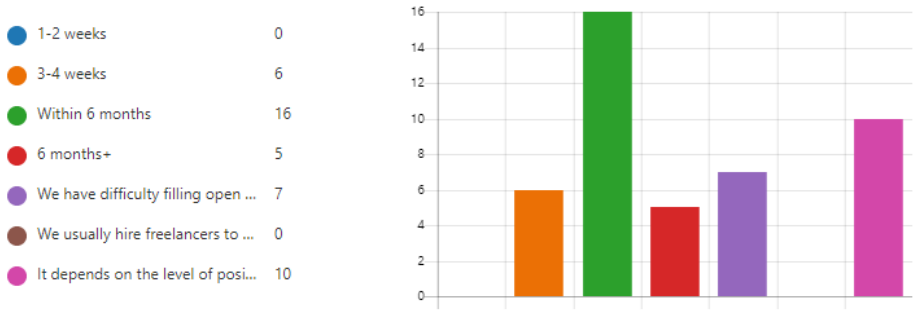


Figure 29 – Time to Fill a Cybersecurity Position

On average, organisations screen 10 to 15 CVs (with related interviews) before selecting a candidate.

In comparison with more 'classical' IT positions, there are several differences between organisations in terms of remuneration matters: 12 organisations roughly offer the same salary, while 24 of them confirm that they generally pay a higher salary (10% to 30% more than IT specialists). No organisation indicated that they pay a cybersecurity specialist less than an equivalent IT specialist (Figure 30).

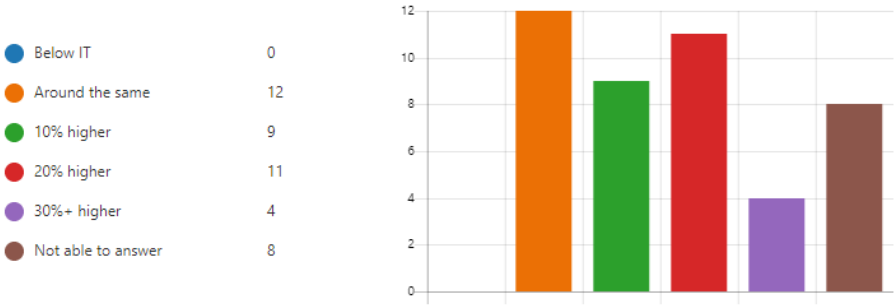


Figure 30 – Cybersecurity Expert Salaries in Comparison with IT Specialists

When salaries are 30%+ higher than average, all the organisations indicted that they fill open cybersecurity positions within 6 months, while three out of four fill them in within 3-4 week (Figure 31).

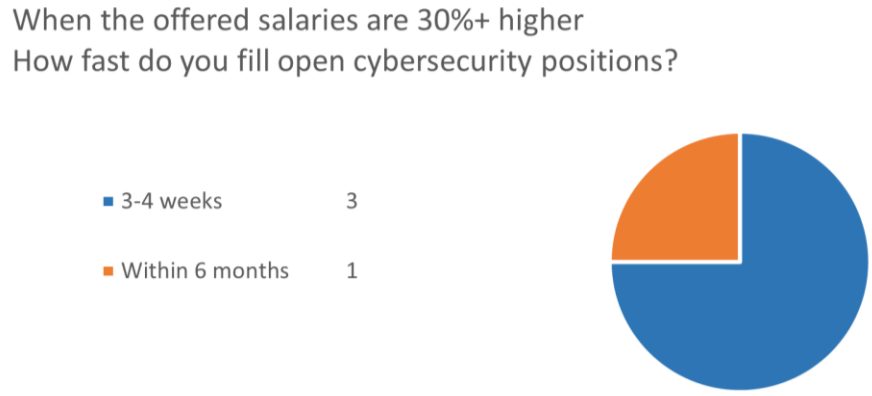


Figure 31 – Time to Fill a Cybersecurity Position with Salaries 30%+ Higher than Average

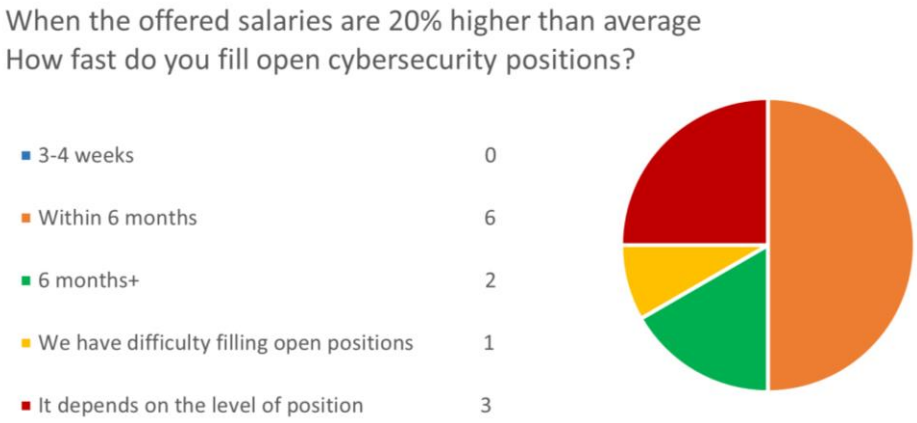


Figure 32 – Time to Fill a Cybersecurity Position with Salaries 20% Higher than Average

A comparison of Figures 33 and 34 shows that the speed at which cybersecurity positions are filled depends on the years of experience required for junior positions. When junior positions do not require experience, organisations do not experience difficulties hiring but when junior positions require experience, organisation find more difficulties hiring and the average time to fill positions increases.

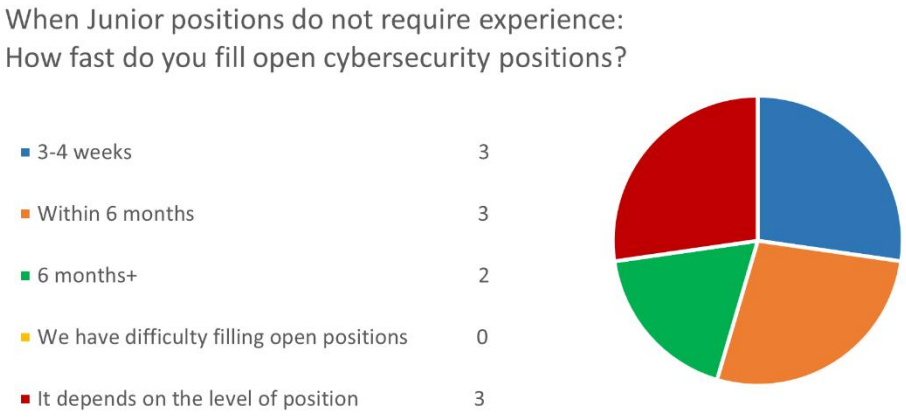


Figure 33 – Time to Fill a Cybersecurity Position when Junior Positions do not Require Experience

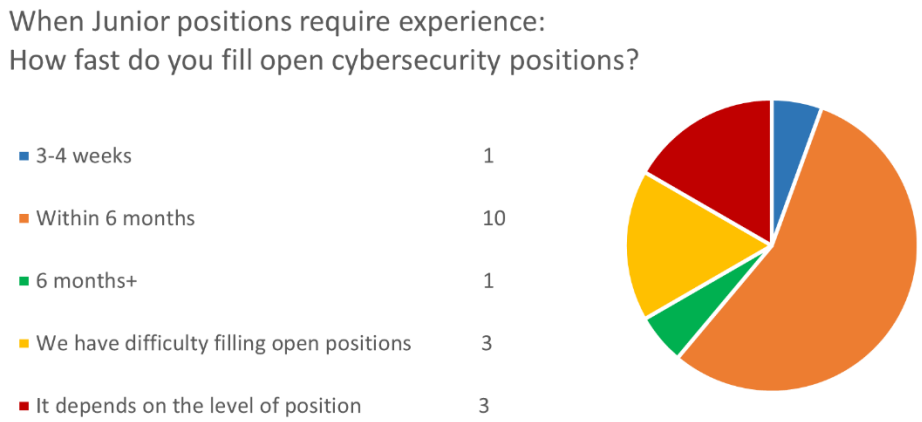


Figure 34 – Time to Fill a Cybersecurity Position when Junior Positions Require Experience

Among the most appreciated certifications, CISSP leads with 31 respondents indicating this as their preferred certification. However, CISM (22 preferences), OSCP (19 preferences) and GIAC (18 preferences) also seem of significant interest for the organisations (Figure 35).

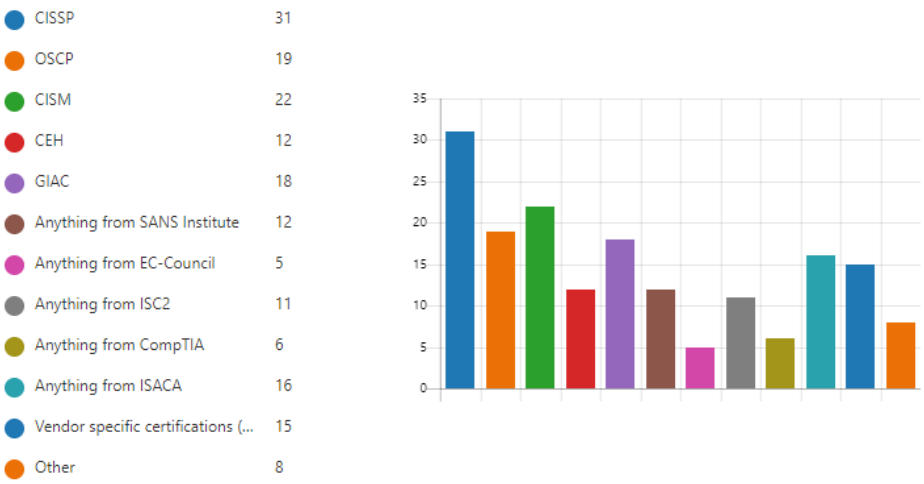


Figure 35 – Most Endorsed Cybersecurity Certifications

From a candidate evaluation perspective, most organisations adopt multi-stage interview processes (from 3 to 4 interviews, on average). Several organisations ask candidates to perform tests and sustain extensive technical question sessions. 6 organisations consider it necessary that at least one interview is conducted in physical presence of the candidate.

The last question of the questionnaire refers to the biggest issues when trying to recruit cybersecurity professionals. The main (by far) notified issue is the general lack, worldwide, of cybersecurity specialists while the demand is constantly growing. This leads to a very competitive market from an organisation's perspective, as they are forced to cope with high salary demands from candidates. In addition, several organisations highlight the complexity of hiring experts for a domain that they do not master. As a growing trend, respondents indicated that several candidates, despite lacking significant cybersecurity skills, still enrich their CV with cybersecurity concepts and keywords.

4 Conclusion

The challenges and issues faced by stakeholders in hiring and retaining cybersecurity professionals and building strong teams of cyber-defenders are many, complex and interconnected. The expectations and attitudes of the employers sometimes exceed the real qualification and proficiency levels of the graduates and there are very limited options for HR professionals to assess this. In the end, the discrepancy between the expectations and the actual cybersecurity competence landscape along with the capabilities of (candidate) employees challenges the capabilities of the HR department, as it cannot complement the process as professionally and effectively as in the case of other professional domains. A more intensive collaboration between industry and academia, not only in the identification and definition of the requirements and objectives, but also joint investments in internship programs, equipment of practical laboratories, work-based learning, tools for hands-on learning, etc. is very necessary and urgent. These investments shall focus not just on the cybersecurity specific competence building, but also contribute to the HR professionals' better understanding and cyber workforce related situational awareness. There is an urgent need to overstep the biases of the cybersecurity skills shortage and focus on addressing the challenge by providing overarching solutions. Defining the ecosystem and stakeholders is still an ongoing process and while a lot of work has been done in the domain, the ecosystem and an effective collaboration mechanism still needs to established.

ANNEX Survey Questions

Understanding European Cybersecurity HR Recruitment Processes

Corporate survey

After the generic information part, the survey focuses on the HR expectations and understanding the current HR practices (for IT and non-IT sectors) in Europe.

Organisational and personal profile questions:

- **Category of organisation**
  - Large company (provider)
  - User/operator
  - SME / startup
  - RTO / university
  - Association / cluster
  - National public administration
  - EU institution/agency
  - HR / recruitment agency
  - Other (specify)
- **Size (staff headcount) of the organisation (local branch/office where applicable)**
  - Open field answer
- **Country**
  - Choose your country (drop-down menu)
- **Sector** (IT / non-IT)
  - IT
    - In case that the sector is IT, choose among IT, IT security, cybersecurity
  - Non-IT
- **Economic sector**
  - Energy
  - Finance
  - Healthcare
  - Manufacturing / SCADA
  - Telco
  - Other (specify)
  - Not applicable

- **Your age**
  - 18-30

  - 30-40
  - 40-50
  - 50+
  - Don't wish to say
- **Your gender**
  - Female
  - Male
  - Don't wish to say
- **Your position within the organisation**
  - HR / recruitment responsible
  - Management
  - Other (please specify)
- **Your level of studies**
  - Bachelor
  - Master's
  - PhD
  - Other (specify)
- **Your main qualification**
  - IT
  - Non-IT

HR expectations and practices questions:

Does your organisation have an in-house or an outsourced cybersecurity department?

- All our cybersecurity related administration and development tasks are provided by the in-house team
- We have an outsourced cybersecurity department
- We have a hybrid model, administration and maintenance are in-house, specialised tasks are outsourced (please describe those tasks)
- Other: (please provide details)

Do you have a dedicated recruitment department?

- If yes, how big (staff headcount)?
  - Open field answer
- If not, who conducts the hiring process for your organisation?
  - Management (in-house)
  - Traditional recruitment agency
  - Cybersecurity recruitment agency
  - Hybrid (agency + in-house)

Your main customers are (multi-choice):

- EU/ governmental sector
- Large enterprises
- SMEs
- Individuals

What cybersecurity roles do you hire most frequently? (multi-choice)

- Software developer for cybersecurity projects
- IT Administrator
- Cybersecurity risk analyst
- Ethical hacker
- Security architect
- Security operations analyst
- Cybersecurity manager
- Cybersecurity researcher
- Forensic investigator
- Other (specify)
- We rarely seek cybersecurity professionals

When looking for IT specialists, is cybersecurity an expected skill?

- Yes, it is a pre-requisite
- It is preferred
- No

According to your estimate, how many cybersecurity professionals are you planning to recruit in the next 12 months?

- Open field answer

From which locations do you seek cybersecurity professionals? (multi-choice)

- In the EU
- In Europe
- USA
- Middle East
- Asia
- Global
- I only recruit professionals from inside my own country

How do you specify the position?

- Using a generic template for job description available online
- Creating an individual job description
- Following industry best practice descriptions and creating a template from that. If so, please specify which best practice source you are using

How do you specify the job title?

- Based on existing taxonomy (if yes, please specify which one)
- Based on internal structure and activities
- Based on inputs from the future team lead/direct line manager

Do you prefer certifications over experience in general?

- We indicate which certificates we find important, but experience is more important
- Without meeting the indicated level of education and certifications we don't even call the prospect
- Other (please explain):

How do you choose among certifications required to fill the vacancy?

- Based on the input from future team lead/direct line manager
- Based on sample job position templates available on the internet
- We don't list certifications
- Based on personal experiences with those certifications

How much does education weigh in your selection of cybersecurity candidates?

- Having a Bsc. or master's in engineering, computer science or related discipline is a must
- Having a Bsc. or master's in engineering, computer science or related discipline is an advantage but experience is more important
- Other (please specify):

Do you conduct practical skills assessment during the application process?

- Yes, we have our sample tasks and challenges (please provide more details)
- Sometimes, but not regularly
- No
    - If no, is that a deliberate choice or due to lack of time/resources?
    - Would an external practical assessment be valuable?

How do you set the salary level for cybersecurity professionals?

- According to the candidate's experience (incl. professional certifications)
- According to internal remuneration practices
- Derived from the available budget
- Offering a competitive wage to attract the best talents
- A combination of the above

How do you find candidates? (multi-choice)

- Internal network
- Cross-training internal workforce
- Social media, company website, specialised platforms
- Traditional staffing firms
- Dedicated cyber headhunting services

- Personal recommendation

What measures does your organisation take to retain cybersecurity professionals? (please rank them in order of relevance)

- Offer trainings (encouraging continuous professional development)
- Incentive based schemes
- Opportunities for promotion
- Financial motivation
- Short technical project assignments, gaming actions, etc.
- Remote working opportunities
- Other (specify)

Do you offer trainings for your cybersecurity professionals? (business conference attendance doesn't count)

- Yes, several times a year
- Yes, at least once a year
- No, they are expected to do their own personal development
- Not yet, but we would like to

If so, how do you offer trainings opportunities to your personnel?

- Inhouse trainings
- We cover costs for external trainings

How fast do you fill open cybersecurity positions?

- 1-2 weeks
- 3-4 weeks
- Within 6 months
- 6 months+
- We have difficulty filling open positions
- We usually hire freelancers to fill positions faster
- It depends on the level of position (please provide details)

How many CVs do you receive or interviews do you conduct on average before finding the right candidate?

- Open field answer

Compared to similar IT positions (eg senior IT expert and senior cybersecurity expert) what is the level of offered salaries for cybersecurity professionals?

- Below IT
- Around the same
- 10% higher
- 20% higher

- 30%+ higher

How many years of experience do you require, on average, for the following non managerial cybersecurity positions? (multi-choice)

- For junior positions no previous experience is required.
- For junior positions we require typically less than a year of experience (but it is required to have)
- For senior positions we require 3+ years (eg analysts)
- For senior positions we require 3+ years (eg pentesters)
- For senior positions we require 3+ years (eg engineers)
- For senior positions we require 5+ years (eg analysts)
- For senior positions we require 5+ years (eg pentesters)
- For senior positions we require 5+ years (eg engineers)
- For senior positions we require 7+ years (eg analysts)
- For senior positions we require 7+ years (eg pentesters)
- For senior positions we require 7+ years (eg engineers)
- Open field:

Which cybersecurity trainings and certifications are endorsed by your organisation? (multi-choice)

- CISSP
- OSCP
- CISM
- CEH
- GIAC
- Anything from SANS Institute
- Anything from EC-Council
- Anything from ISC2
- Anything from CompTIA
- Vendor specific certifications (CISCO certified, MS certified, etc)
- Other (please specify):

How do you evaluate the candidates according to the required profile?

Free comment input field

What are the biggest issues for you while trying to hire new cybersecurity professionals?

Free comment input field

We are happy to hear your comments and views. If you wish you can leave a comment here.

Free comment input field