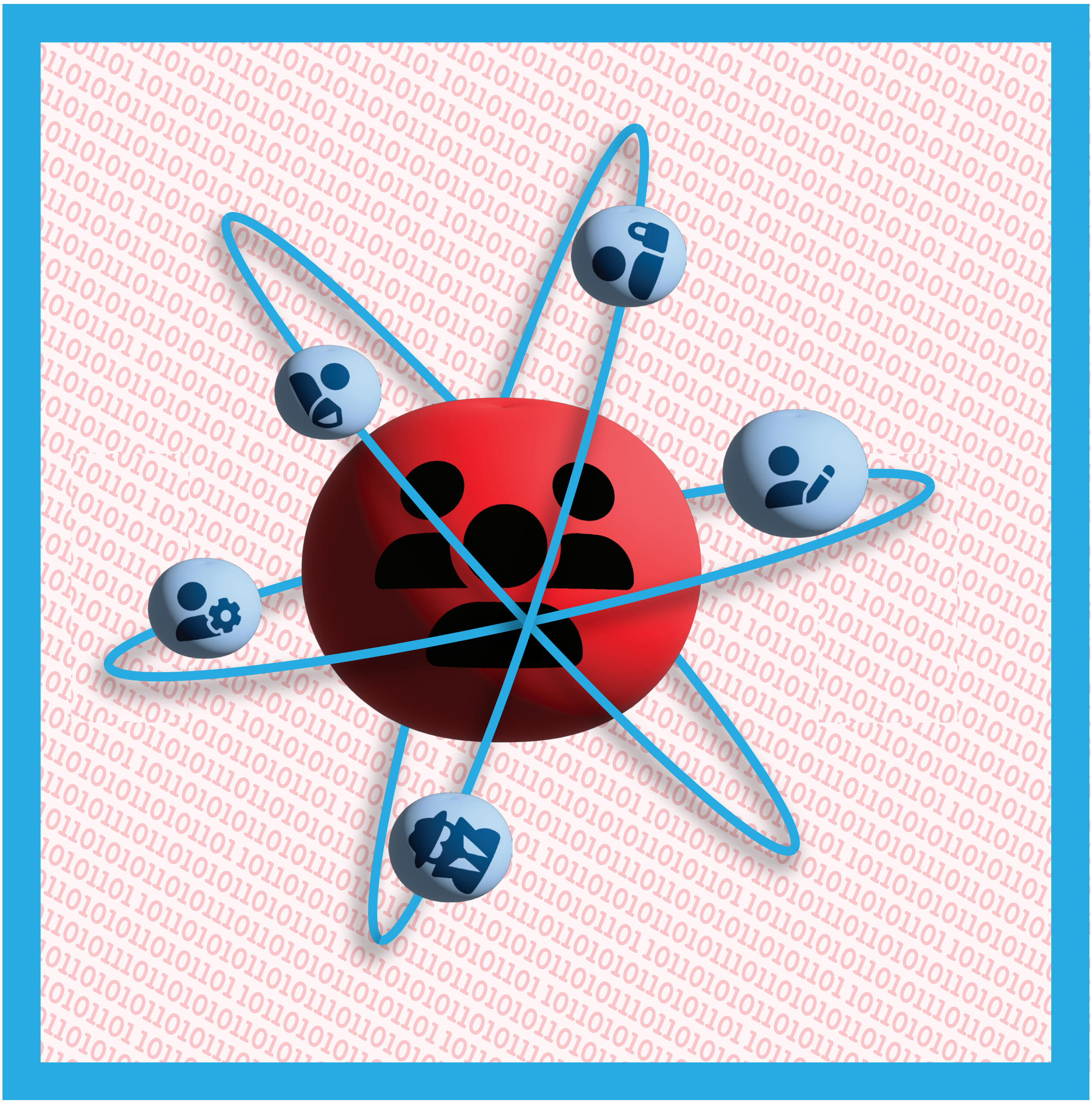
nc3.lu
National Cybersecurity
Competence Center
LUXEMBOURG

2024 Cybersecurity Workforce Study

Luxembourg's Cybersecurity Workforce Speaks out

Survey Uncovers Major Hurdles and Future Prospects



nc3
Cybersecurity
Observatory

Table of Contents

Introduction

The National Cybersecurity Competence Center have launched the Market Intelligence Observatory Platform to enhance cybersecurity market insights and to provide data that informs strategic decision-making.

This initiative includes a series of critical studies aimed at addressing the varied demands of Luxembourg's ecosystem.

The recent studies "A Comprehensive Market Study on Cybersecurity Challenges and Opportunities in Luxembourg's SME Sector" and "2023 Luxembourg Cybersecurity Ecosystem Study" provide comprehensive insights into the cybersecurity landscape, highlighting the CYBERSECURITY LUXEMBOURG initiative.The initiative aims to foster collaboration between public and private sectors by providing detailed mapping and an interactive dashboard for enhanced field visibility.

The findings from the 2023 study unveiled a dynamic ecosystem characterized by digital transformation, the Internet of Things (IoT), and new cyber threats.

82% of market participants identify human resources as a significant challenge, citing issues related to location, recruitment and retention.

77% of participants voiced concerns regarding a shortage of talent and the challenges posed by remote work.

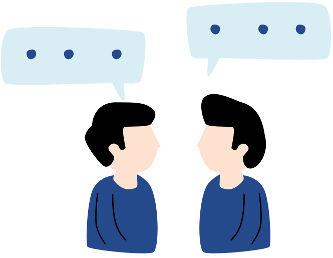
To address these pressing workforce issues, we initiated the "2024 Cybersecurity Workforce Survey" in May 2024, aiming to gather in-depth insights and develop effective solutions. The 17-week cybersecurity survey in Luxembourg drew strong participation from the community, demonstrating their dedication to the sector's advancement.

Executive Summary

Luxembourg's cybersecurity landscape is marked by a highly specialized and internationally diverse workforce, crucially supported by key industries such as Information and Communication, Financial, and Insurance sectors. The need to safeguard sensitive data and mitigate cyber risks in these regulated industries drives is a key factor driving the demand for skilled professionals.. 62.4% of cybersecurity professionals began their careers outside Luxembourg, with 51% originating from neighboring countries like France, Belgium, and Germany, highlighting significant cross-border mobility facilitated by geographic proximity and economic ties.

The field, or Ecosystem in Luxembourg attracts top talent due to its international exposure, technological advancements, and entrepreneurial opportunities, with 48% of professionals actively seeking roles in Luxembourg.

26% of professionals transitioning from diverse backgrounds into cybersecurity, fostering a rich exchange of knowledge and addressing talent gaps shows the openess of the field.



Leadership roles, including Information Security Officers, Chief Information Security Officers, and Managers, constitute 33.8% of the workforce, while specialized roles like Penetration Testers are increasingly in demand, emphasizing the shift towards proactive offensive security measures. Although 87.9% of professionals intend to stay long-term in Luxembourg, retention risks remain due to limited career growth and high housing costs. Young professionals encounter obstacles due to high experience requirements and scarce entry-level opportunities, compounded by inadequate alignment of government education initiatives with market needs.

A cultural shift towards viewing cybersecurity as a strategic priority rather than mere compliance is necessary to enhance proactive cybersecurity practices.

The lack of specialized training programs limits the development of advanced skills, such as Red Teaming, which are crucial for addressing talent shortages and future-proofing the workforce. However, the public sector's collaborative efforts within the cyber community are key in fostering a supportive environment, highlighting the importance of industry-aligned educational initiatives to strengthen the ecosystem.

About the Survey & Report

For this report, NC3 received 157 online survey responses from cybersecurity practitioners and decision-makers.
We conducted 5 in depth interviews with cybersecurity professionals working in Luxembourg. These professionals bring diverse backgrounds, enriching our insights.

This report synthesizes perspectives from Luxembourg's cybersecurity professionals, offering actionable insights for leaders, policymakers, hiring managers, and practitioners.
It identifies workforce challenges and proposes solutions to strengthen the sector.

Structure:

Insights: Key findings on workforce trends, talent gaps, and market dynamics.

Course of Action: Actionable recommendations to address challenges.

Note: Quotes reflect direct input from survey participants and interviewees.

Mapping the cybersecurity workforce in Luxembourg

Socio Economic Data: Distribution of cybersecurity workforce

In the socio-economic data section, we gathered detailed information about the respondent's size of their organizations, and sectors of activity, as classified by NACE codes, to enhance our understanding of their representation within Luxembourg's Cybersecurity workforce.

62.8% of respondents completed the survey, reflecting a strong overall engagement. This distribution highlights the overall engagement and areas where additional efforts might be needed to ensure comprehensive data collection for future surveys.

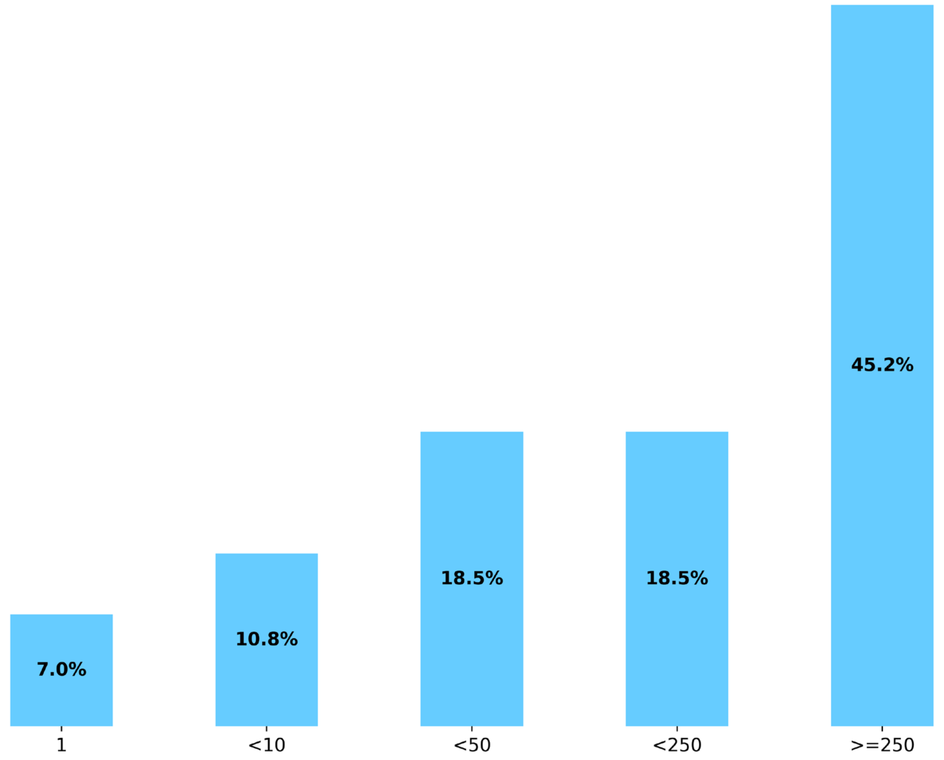


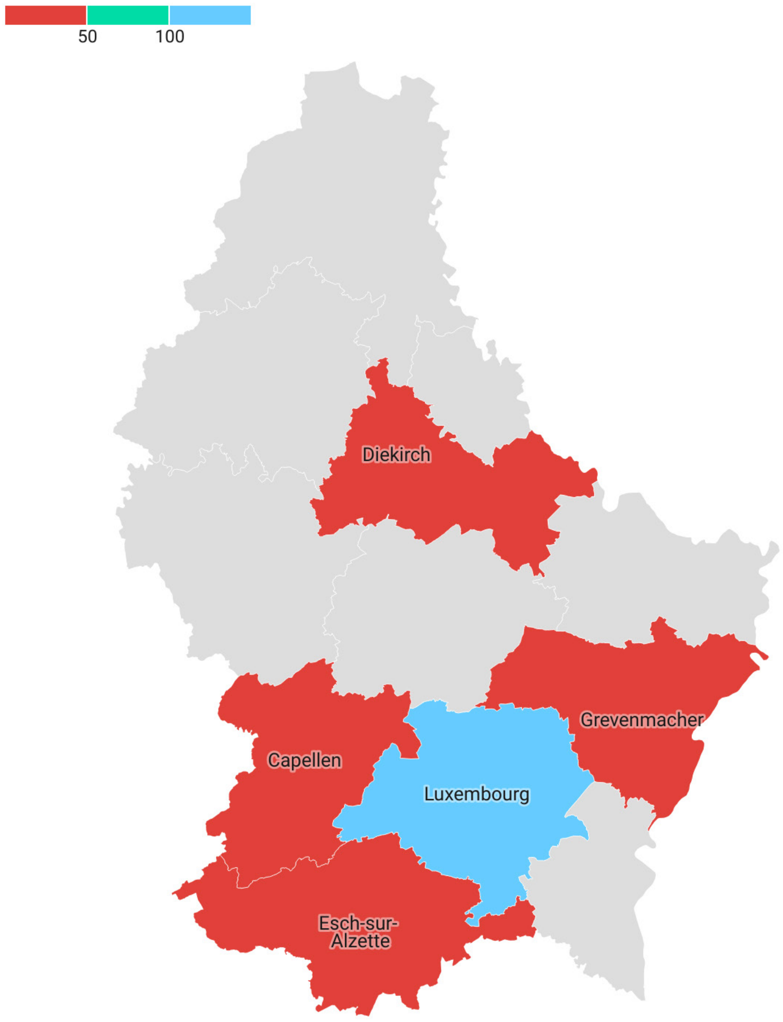
Figure 1: Distribution of respondants per company size

Survey per Company Size

Companies with 250 or more employees have the highest survey participation, with 45.2% of responses. Companies with less than 10 employees and those with 1 employee have the lowest participation, with 10 - 7 %.

There is a noticeable gap in participation between smaller companies (less than 50 employees) and larger companies (50 or more employees), highlighting a potential area for increased outreach.

In which municipality is your head office located?



Created with Datawrapper

70%

company head offices are located in Luxembourg City.

22%

company head offices are located in Esch-sur-Alzette.

Figure 2: Distribution of respondants company head office location

Regions like Capellen (4%), Diekirch (2%), and Grevenmacher (2%) have a moderate number of head offices, reflecting a spread of business activities across these areas. These insights highlight the centralization of business activities in Luxembourg City and Esch-sur-Alzette, with a more moderate spread in other regions.

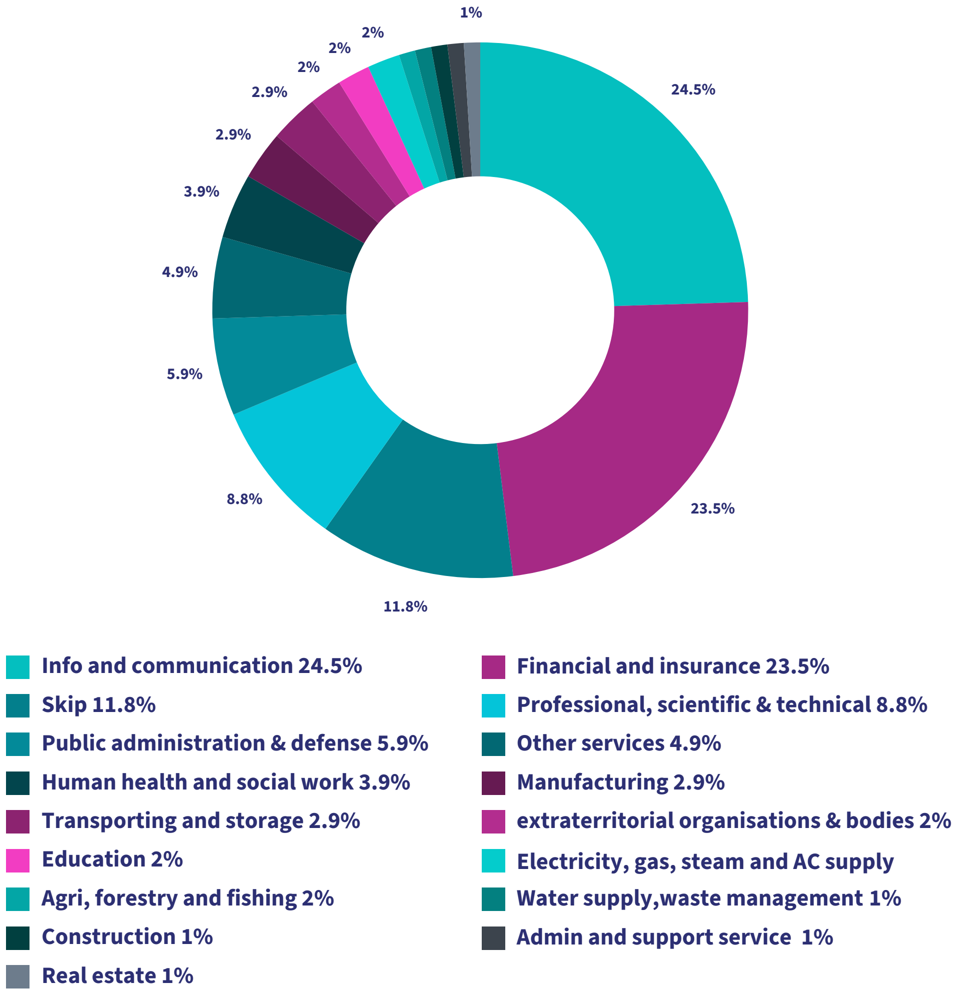


Figure 3: Distribution of respondants company's business sector as per NACE code

Business Sector

The **Information and Communication** sector leads with 25% of respondents, highlighting its strong presence in Luxembourg. **Financial and Insurance Activities** 24% and **Professional, Scientific, and Technical Activities** 9% also show significant representation in the cybersecurity landscape.

Public Administration and Defense (6%), Human Health and Social Work Activities (4.4%), and Other Services (5.1%) have moderate participation. Sectors like Agriculture, Construction, Water Supply, Real Estate, and Administrative Services each account for less than 1%, indicating lower engagement in the survey.

The faces and skills of Luxembourg's cybersecurity workforce

Regional Background: Demographics and qualifications of the cybersecurity workforce

Detailed information about the respondent's connection to Luxmbourg, education and work experience is gathered in the regional data section.

Did you grow up and/or study in Luxembourg or Greater Region?

*Greater region includes parts of four countries: Luxembourg, Germany, France, and Belgium.

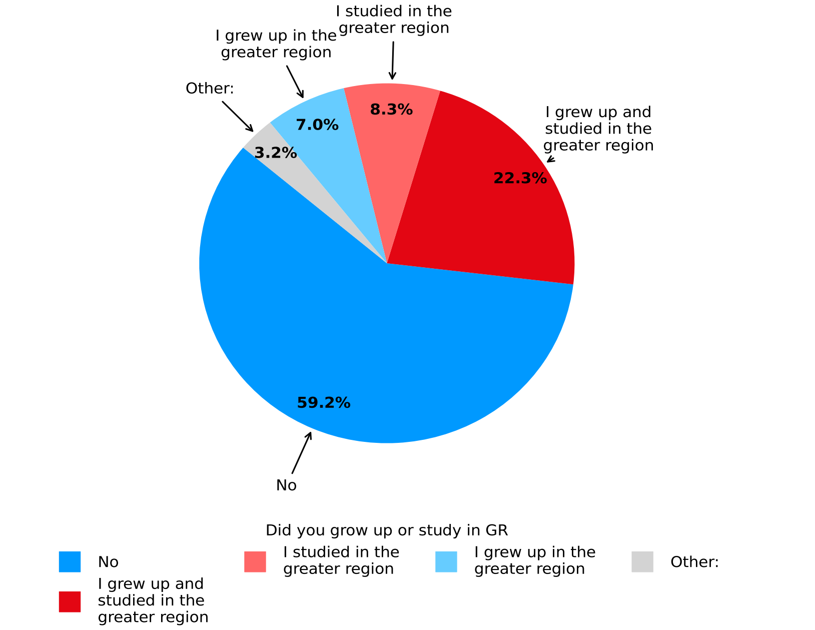


Figure 4: Distribution of respondants connection to Luxembourg & Greater Region

Most respondents neither grew up nor studied in Luxembourg or the Greater Region, reflecting a highly international workforce.

This brought more insights to understanding the respondents personal connection , cultural context, educational background and regional work experience which might be relevant for certain roles.

- **59.2% of respondents have not grown up or studied in Luxembourg or Greater region.**
- **22.3% of respondents have both grown up and studied in the Greater region.**
- **8.3% of respondents studied in the Greater region but did not grow up there.**
- **7% of respondents grew up in the Greater region but did not study there.**
- **3.2% of respondents fall into other unspecified categories.**

Insights

The Luxembourg and Greater Region is attracting students from other regions, indicating the presence of reputable educational institutions that attract non-local students.

Local residents are seeking education outside their region for various reasons, including pursuing specialized programs that are not available in their local area or simply the desire to study abroad.

Individuals are pursuing higher education and technical studies in Romania, Italy, Germany, and the UK, with the UK being the preferred destination for international studies.

There is a trend of gaining international work experience within or outside EU and returning to Luxembourg.

Many individuals, who grew up or studied in Luxembourg or the Greater Region, maintain a strong connection to the country even after studying or working abroad.

Renowned universities in the Greater Region

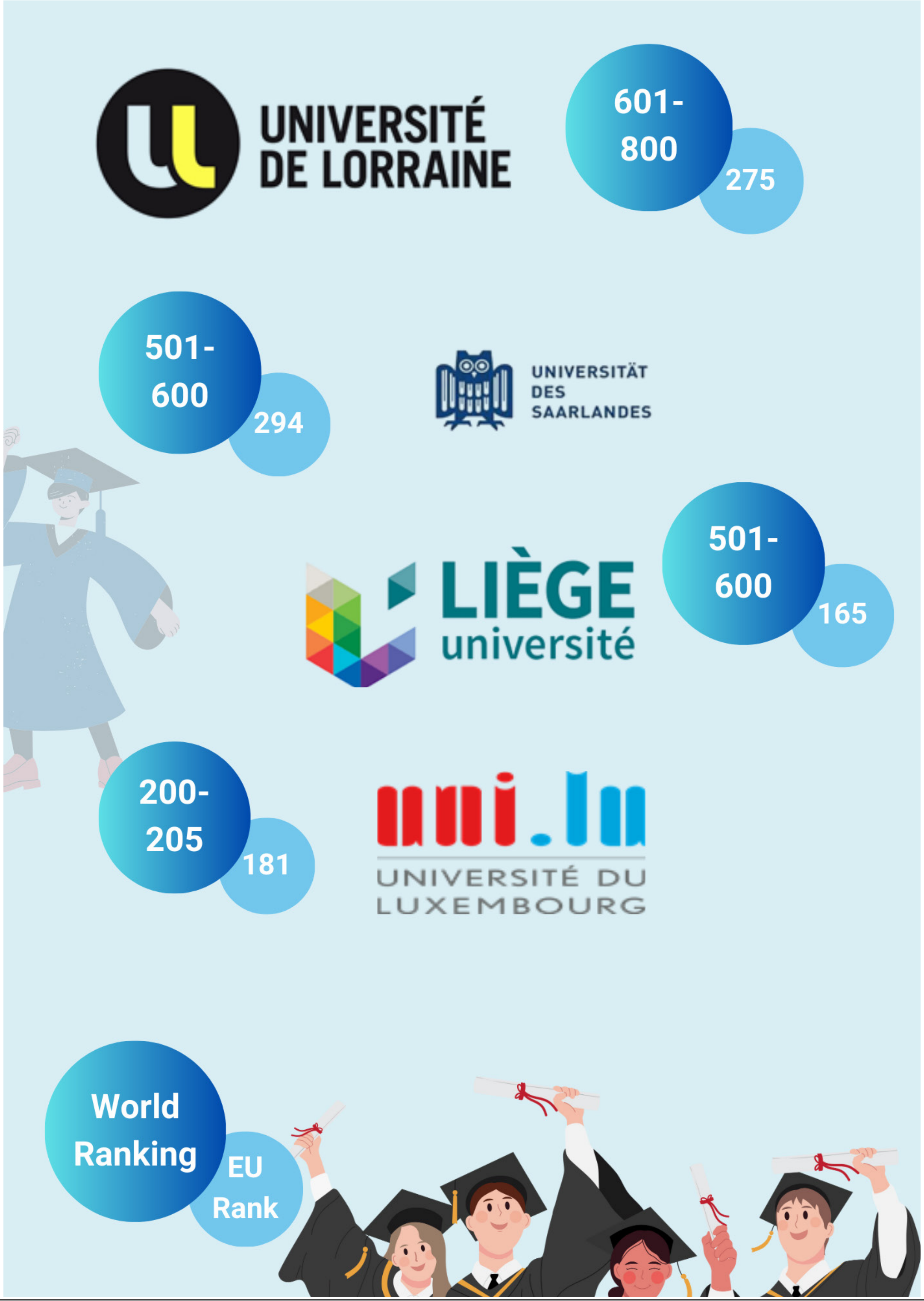


Figure 5: List of renowned universities in Greater Region

https://www.timeshighereducation.com/world-university-rankings/2024/world-ranking#!/length/25/locations/LUX/sort_by/rank/sort_order/asc/cols/stats

Diverse professional backgrounds strengthen Luxembourg’s

Career Pathways: Rich professional experiences and their contribution to Luxembourg’s cybersecurity workforce

Detailed information about respondent’s professional backgrounds, trajectories, and professional landscapes both outside and within Luxembourg is collected in the career pathways data section.

Did you start your career in Luxembourg?

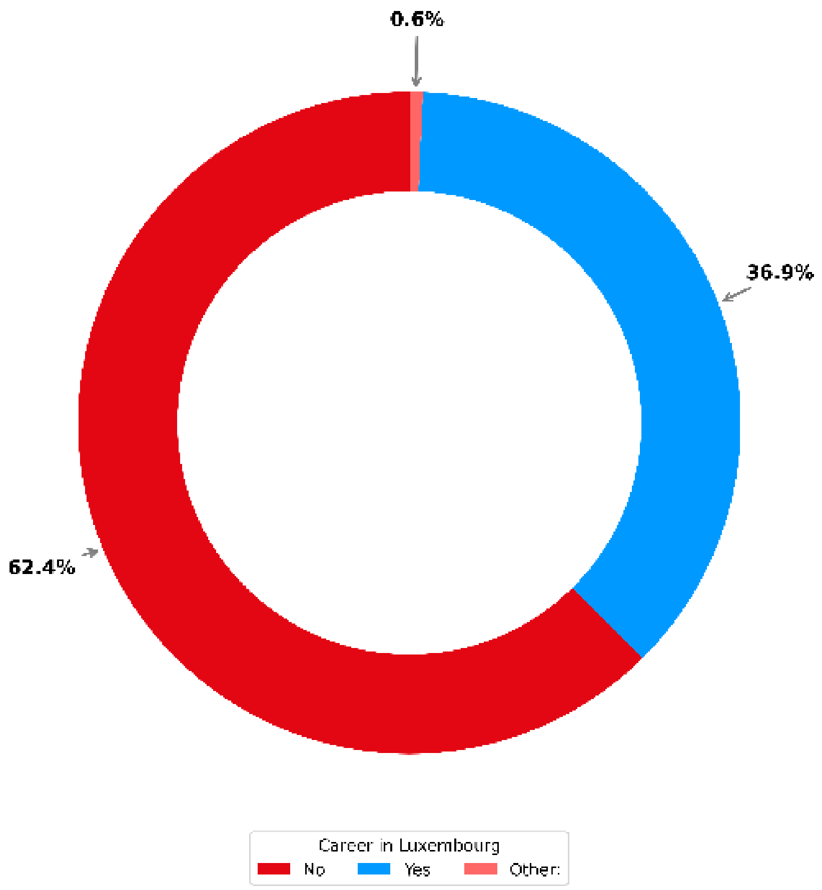


Figure 6: Distribution of respondants who started their careers in Luxembourg

62.4% respondents started their career outside Luxembourg highlighting the country's strong international

36.9 % respondents started their careers in Luxembourg, indicating that the country retains a portion of its workforce from

0.6% of respondents fall into an unspecified category, which might include unique career paths or ambiguous career

If you did not start your career in Luxembourg, please specify where you begin your professional career?

> This data clearly indicates that the majority of respondents began their careers outside of Luxembourg.

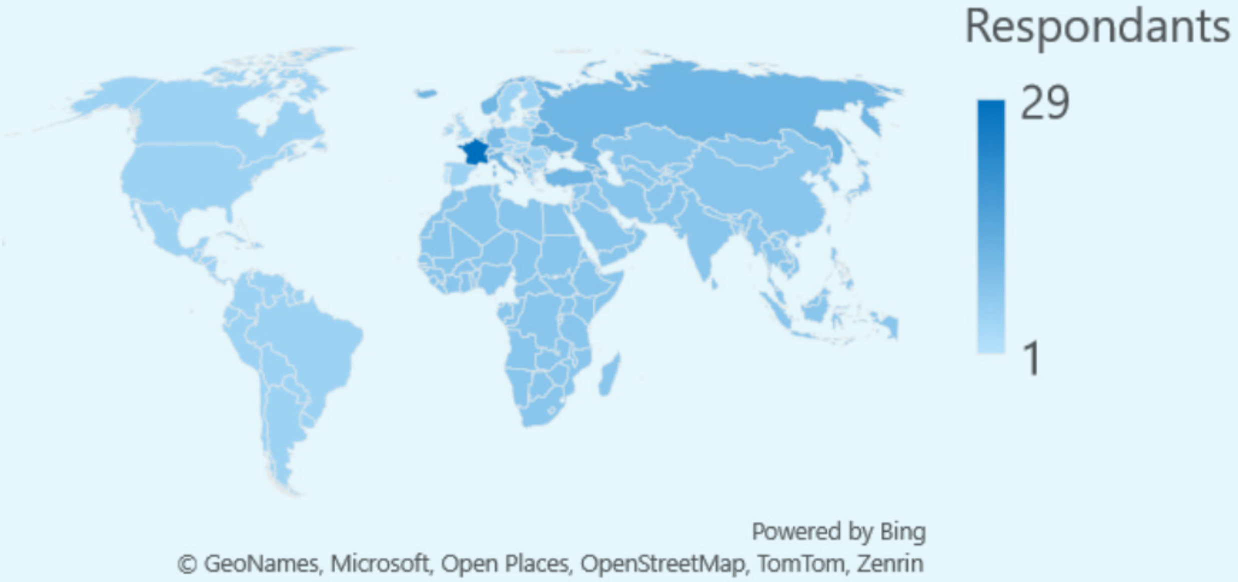
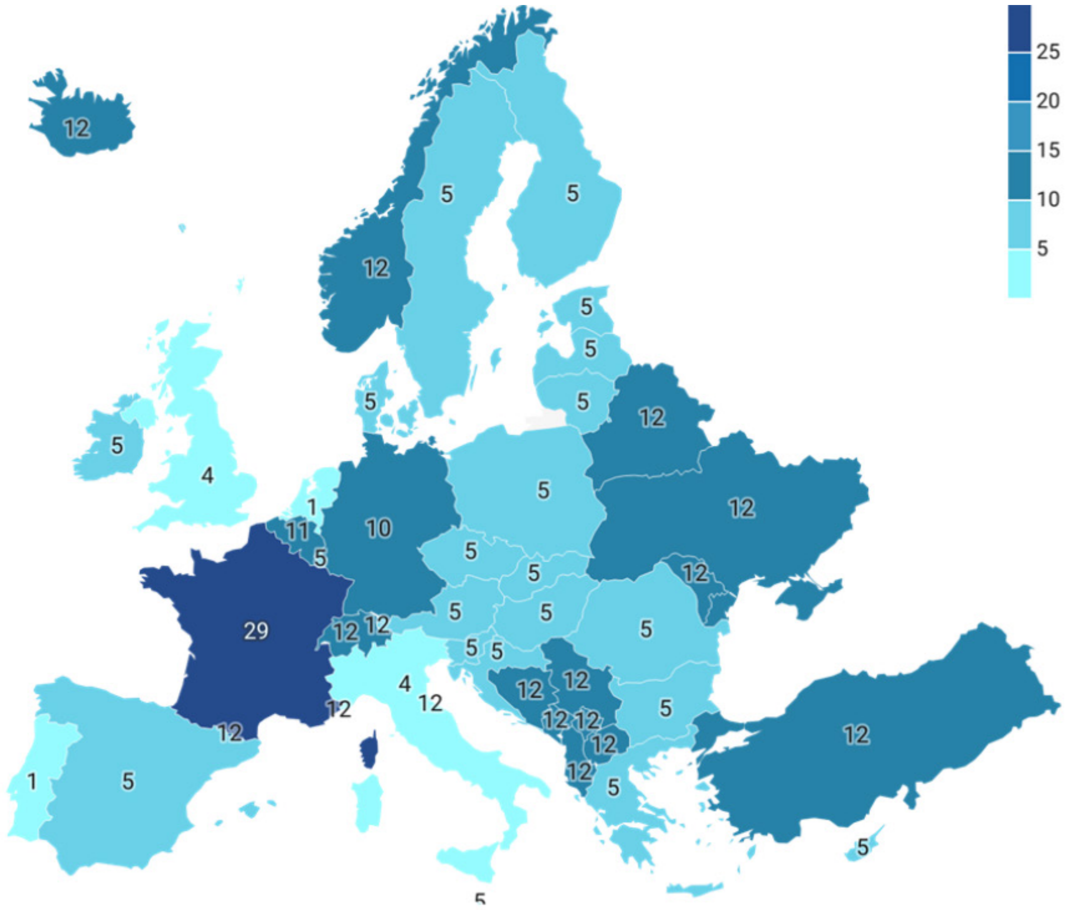

Respondants
29
1
Powered by Bing
© GeoNames, Microsoft, Open Places, OpenStreetMap, TomTom, Zenrin

Figure 7: Distribution of respondants who started their careers outside Luxembourg

8%	5%	8%
ASIA	AMERICAS and Other EU Countries	AFRICA

ZOOMING INTO EUROPE



Created with Datawrapper

Figure 8: Distribution of respondants who started their careers outside Luxembourg zoomed into Europe

30% started in France

10% started in Germany

11% started in Belgium

- **12% in other non-EU European countries.**
- **Regions such as Portugal and the Netherlands have lower representation, with only 1% of respondents, suggesting smaller populations in the surveyed context.**

What factors influenced your decision to work in Luxembourg’s cybersecurity sector?

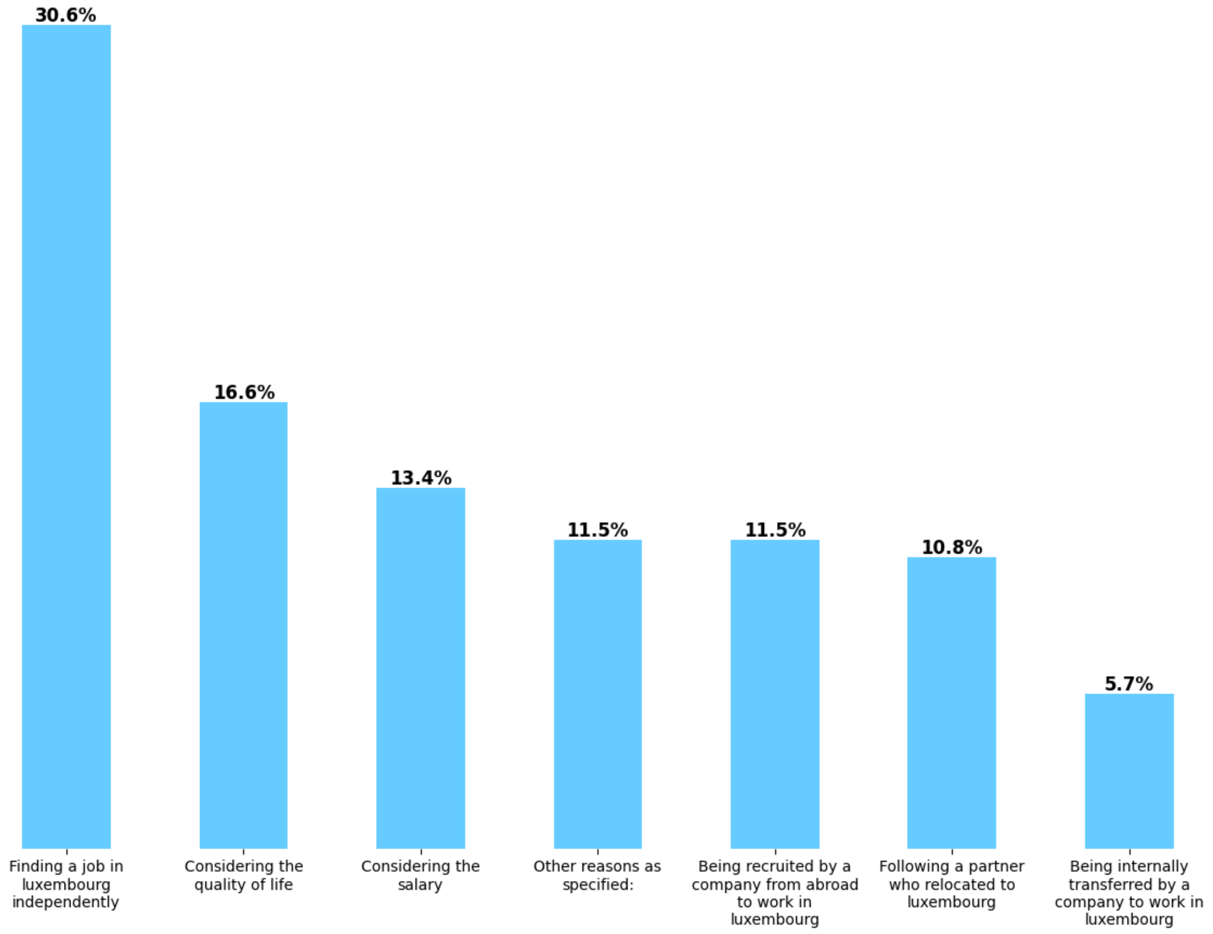


Figure 9: Key Factors Influencing the Decision to Work in Luxembourg’s Cybersecurity Sector

31% of respondents, actively seek out job opportunities in Luxembourg on their own.

This suggests a strong personal initiative and interest in the cybersecurity job market in Luxembourg.

This further reinforces Luxembourg's reputation as a prime international work destination.

Quality of life is a major consideration for 17% of respondents.

Salary is an important factor for 13% of respondents.

A small percentage 5.7% of respondents relocated due to internal company transfers, indicating that some professionals move to Luxembourg as part of their career progression.

A nearly equal percentage of respondents were either recruited by an international company or moved due to a relocating partner. This highlights Luxembourg's attractiveness to global firms and underscores the role of personal relationships in career decisions.

Luxembourg's high standard of living, safety, and excellent public services, continue to make it a highly desirable destination for professionals.

When we dig deeper into "Other reasons as specified" below are few more interesting insights:

- **Career and Skill Development**
- **Educational and Professional**

Do you have a permanent, fixed-term or freelance contract?

> The data reveals a strong preference for permanent employment, with the vast majority of respondents opting for long-term job security.

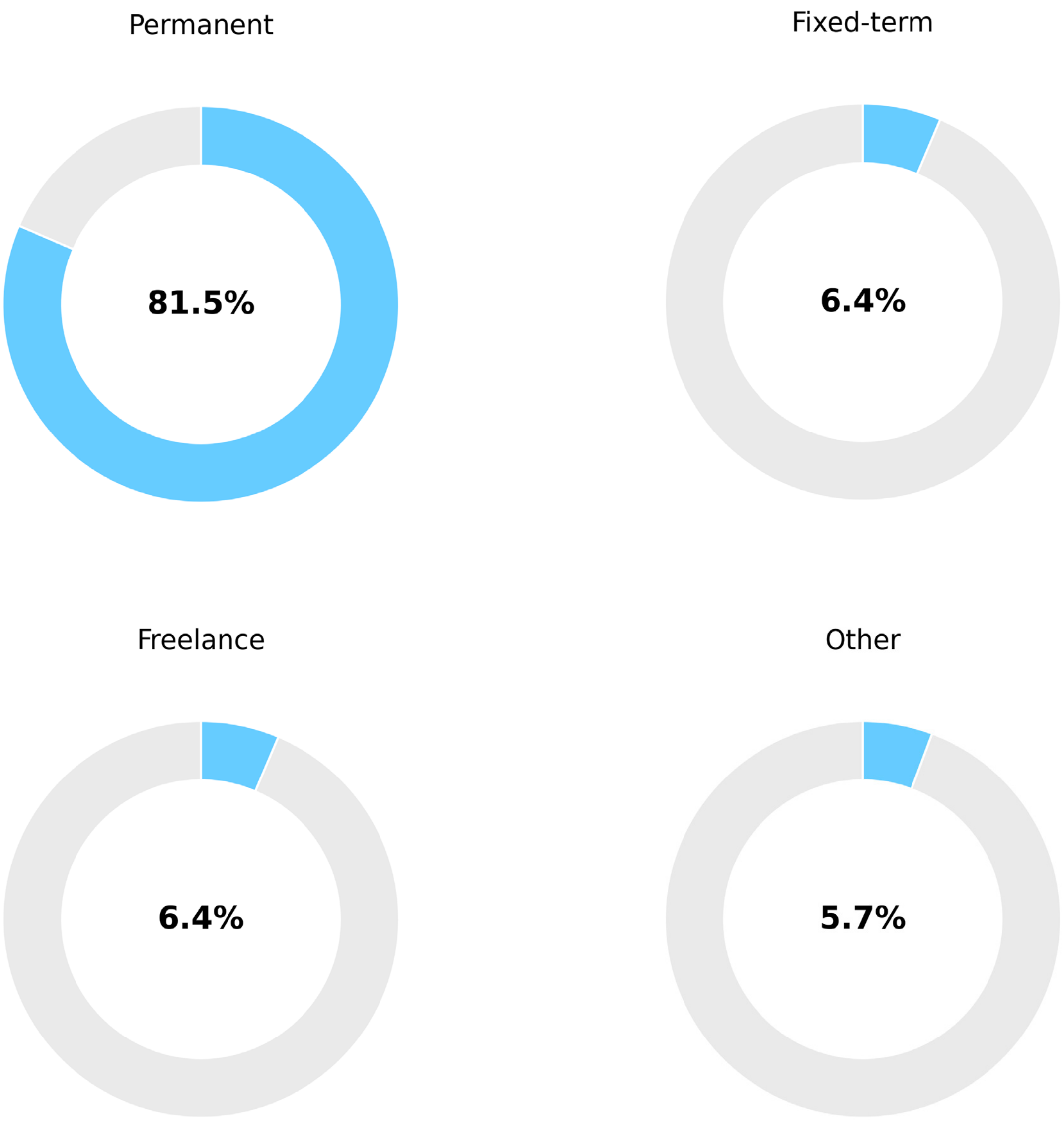


Figure 10: Distribution of Respondents by Employment Type

Luxembourg’s cybersecurity workforce distribution

42%, have completely worked in cybersecurity.

This indicates a strong presence of individuals with extensive experience in the field. These professionals work experience in Luxembourg is equal to their cybersecurity experience.

26% of respondents have moved to Luxembourg to work in cybersecurity.

What we usually observe here is that the total cybersecurity experience is more than their work experience in Luxembourg.

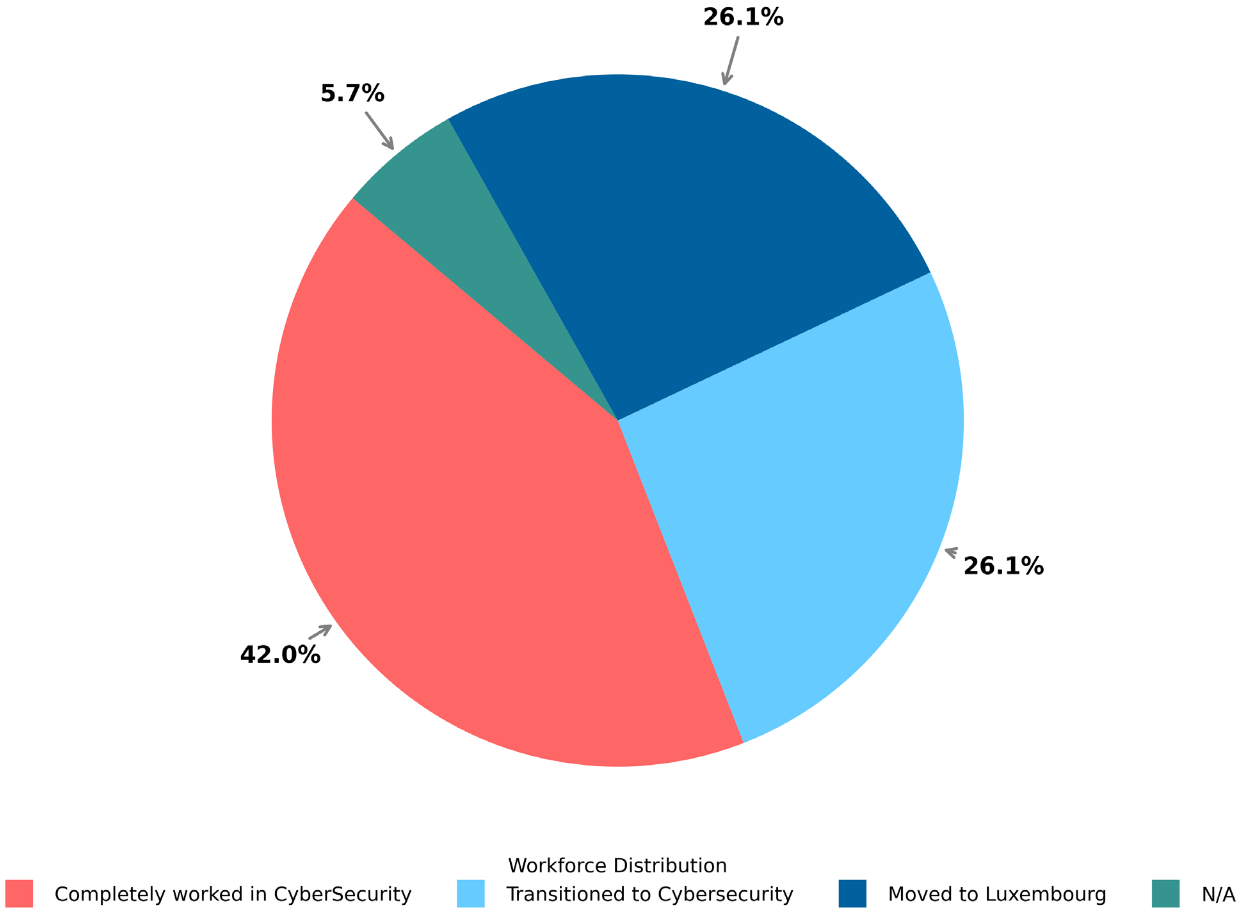


Figure 11: Luxembourg workforce distribution

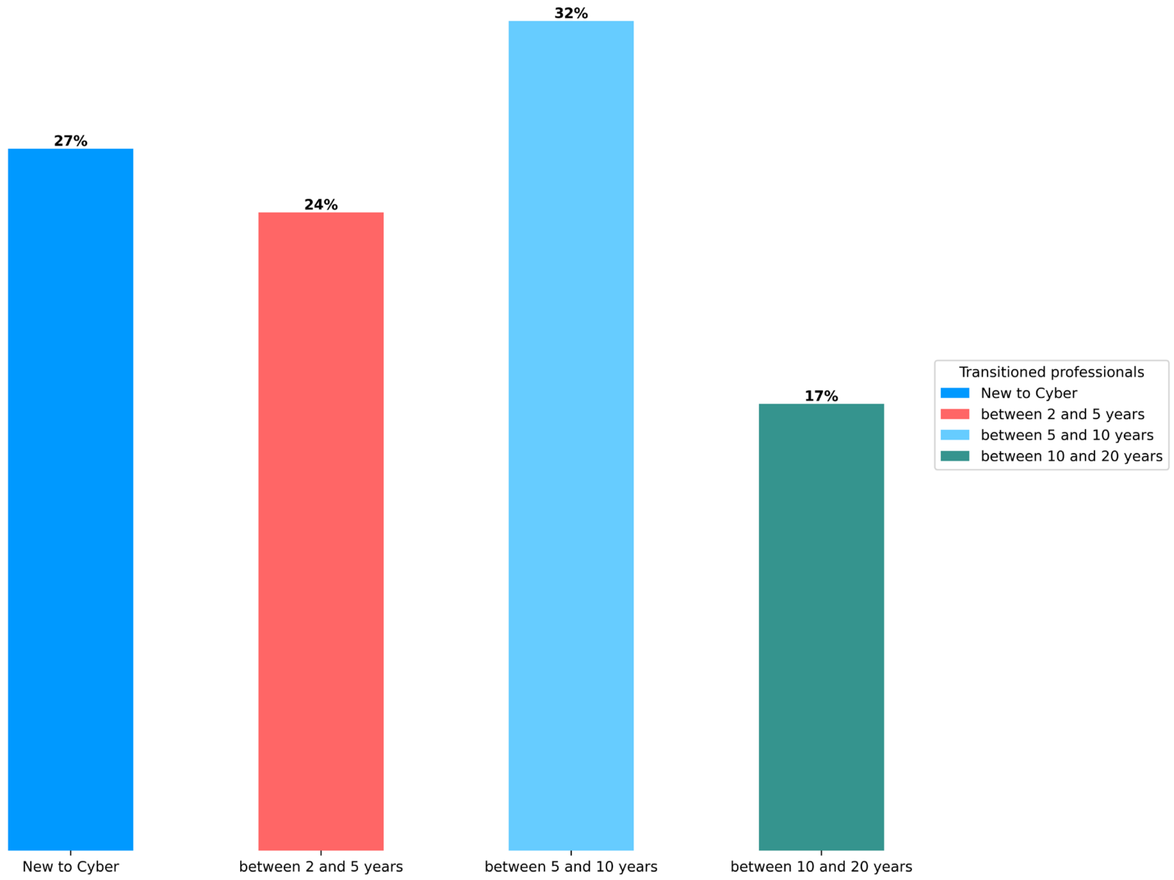


Figure 12: Distribution of professionals who have transitioned to cybersecurity

26% of respondents have transitioned to cybersecurity.

with 32% of respondents having between 5 and 10 years of experience before the shift. This suggests that a considerable number of individuals have made a career shift into the cybersecurity domain at mid career.

We also observe that

- 27% of respondents have newly transitioned to cybersecurity have < 2 years of experience.
- 24% of respondents between 2 and 5 years of experience.

This analysis is based on the respondants country of work where they began their career.

- **The highest number of professionals are from France across nearly all experience levels, particularly in the "5 to 10 years" and "10 to 20 years" categories..**
- **A significant number of professionals are from Belgium, particularly in the "More than 20 years" category**
- **A few professionals are from other EU and Non-EU European countries, dispersed across different experience levels.**
- **Relatively fewer professionals are from Africa, the Americas, and Asia, with the majority having experience ranging between 2 and 20 years.**
- **A smaller but notable presence of professionals from United Kingdom, Italy, and Netherlands have, having between 2 and 20 years of experience.**
- The high number of entries in the "No Data" category suggests that there the data was not provided bu the respondent. Addressing these gaps could provide a more comprehensive understanding of the cybersecurity workforce.

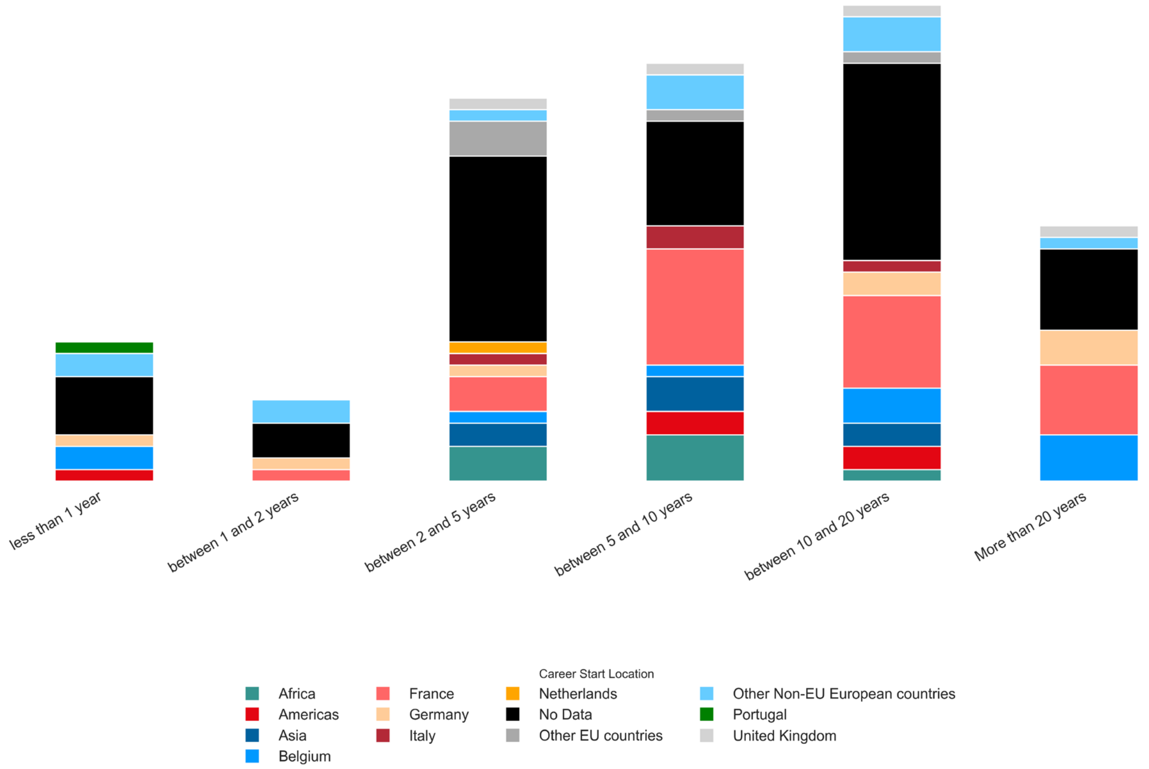


Figure 13: Distribution of Cybersecurity Experience of Respondents who moved to Luxembourg based on the country of first work

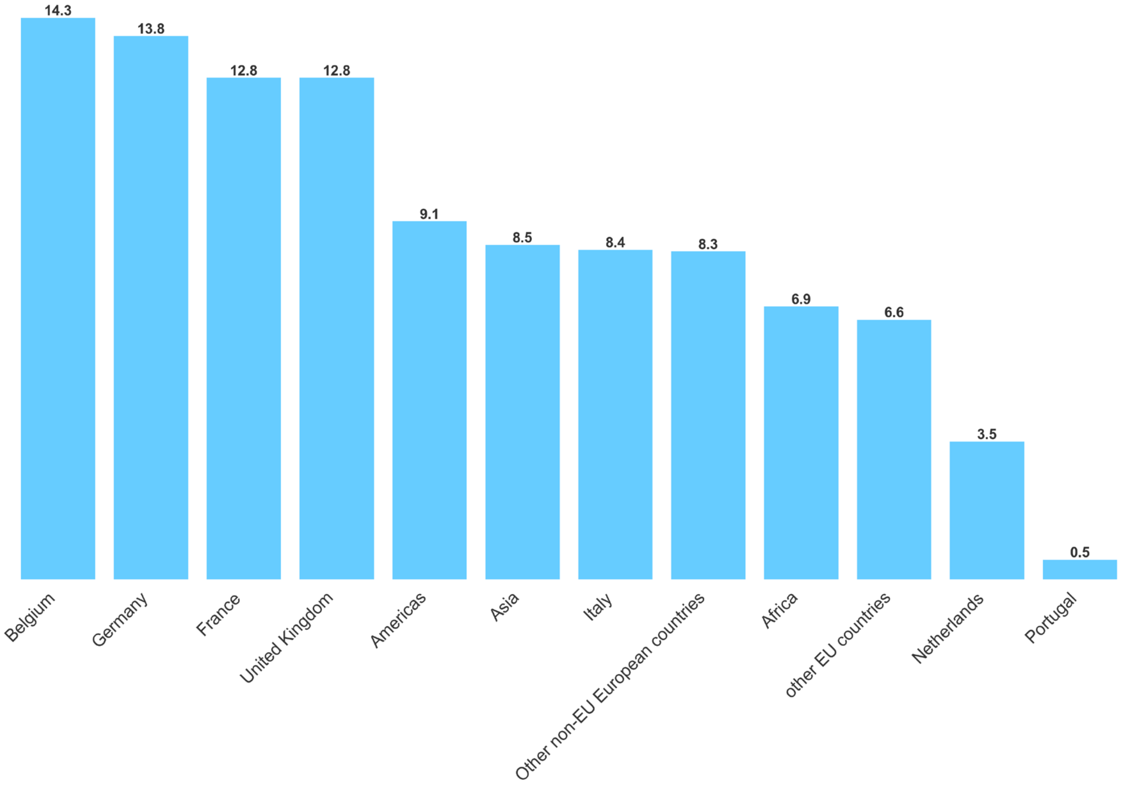


Figure 14: Average cybersecurity experience categorized by the country where respondents' professional careers initiated.

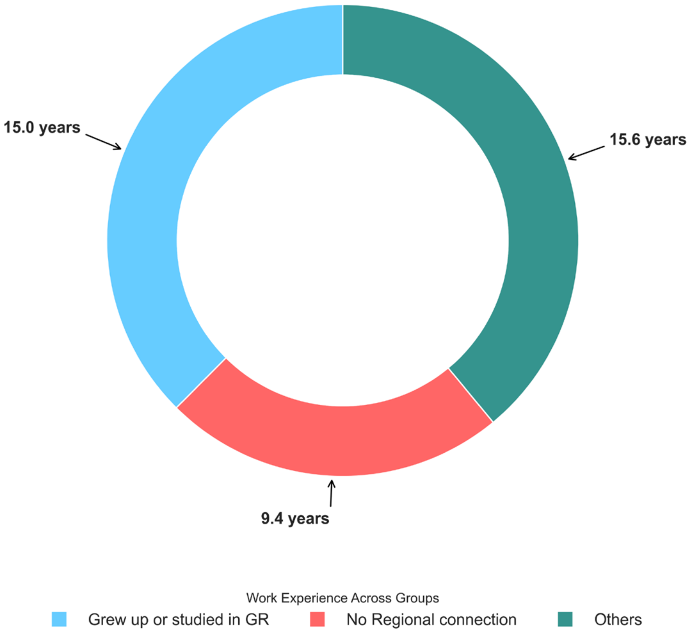


Figure 15: Average work experience categorized by respondents connection to Luxembourg

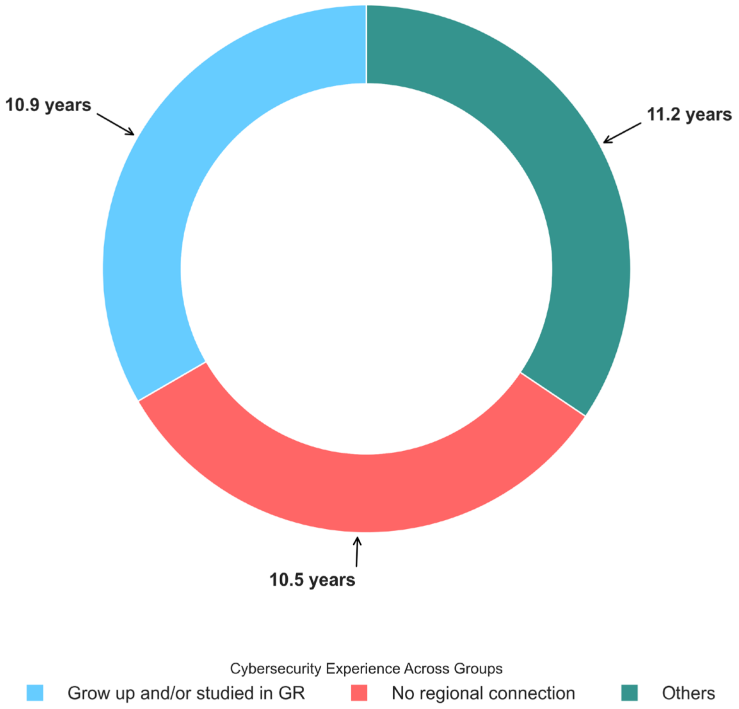


Figure 16: Average cybersecurity experience categorized by the respondents connection to Luxembourg

> Despite varying overall work experience, all groups have similar levels of average cybersecurity experience, highlighting a strong focus and specialization in this area across the board.

Luxembourg's cybersecurity sector thrives on international talent, reinforcing its status as a global cybersecurity hub. Even though individuals start their careers in different countries, they bring well-developed cybersecurity expertise when they move to Luxembourg.

Did you start your career in the same field as the one in which you are working now?

The data shows that a significant number of individuals have shifted careers in the field of cybersecurity, with 56.7% of professionals transitioning to different fields.

This highlights the fluid nature of career paths in the field, with many starting in IT or software development before specializing in cybersecurity due to a growing interest in security and new challenges.

- **42% of cybersecurity professionals remain in their initial roles, indicating fulfilling career paths with advancement opportunities.**
- **The small percentage of professionals experiencing minimal deviations suggests evolving responsibilities due to fast-paced technology.**
- **The data emphasizes the need for adaptability and lifelong learning in cybersecurity to protect digital assets.**

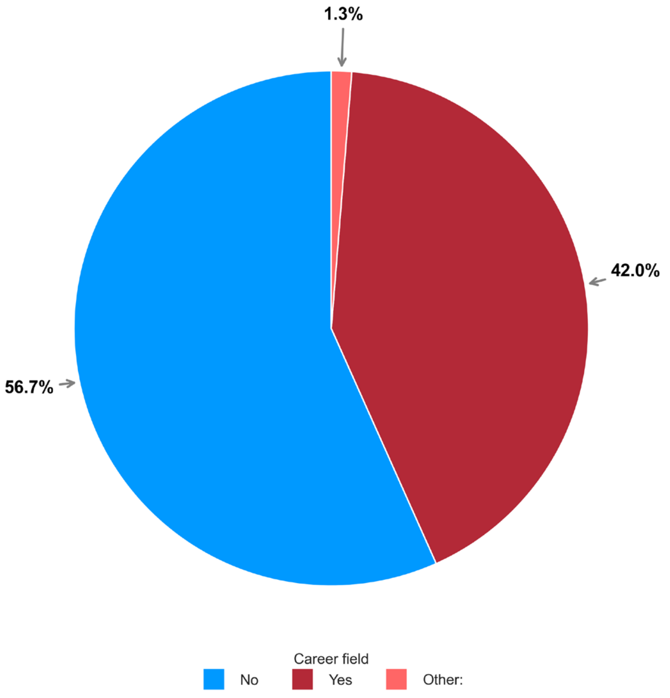


Figure 17: Career Transition Trends Among Respondents

What is your current role? We have used ENISAs ECSF (European Cybersecurity Skills Framework).

The role of ISO, Manager and CISO is the most common, making up about 33.8% of the workforce.

The "Other" category is significant at 20.4%, suggesting a wide variety of job titles that are not captured by the standard categories. Specialized Roles like Penetration Tester, Ethical Hacker, and Cybersecurity Risk Officer each make up 8.3%. Less Common Roles: Roles such as Cybersecurity Educator and Cyber Threat Intelligence Specialist Cybersecurity Researcher, r Research and Development (R&D) Officer, Digital Forensics Investigator, are less common, each making up less than 2% of the respondents.

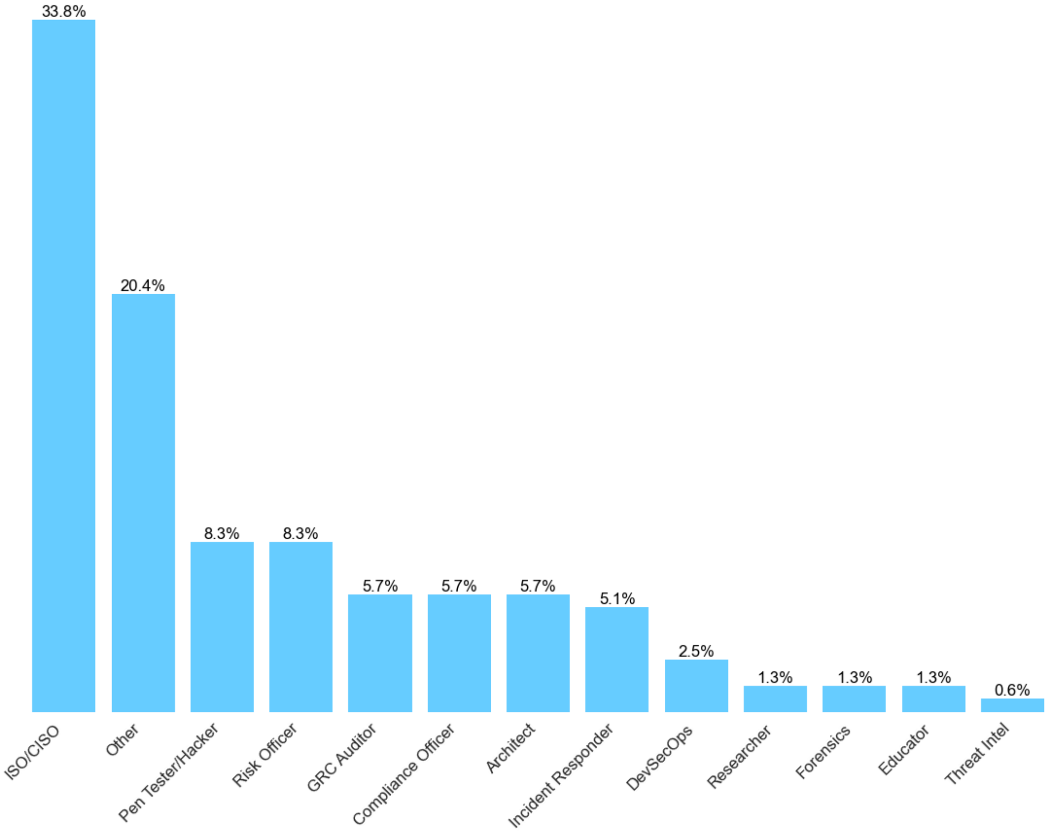


Figure 18: Cybersecurity workforce composition by Current Job Role

The experience distribution for Information Security Officers(ISO) or Chief Information security officer (CISOs) is diverse, with 19.1% having over ten years of experience, 4.5% having less than five years, and 10.2% having 5 to 10 years of experience.

Respondents’ future cybersecurity career goals reflect the evolving nature of the workforce, emphasizing

> **These findings illustrate a workforce rich in seasoned professionals, indicating robust expertise and depth in the cybersecurity field, while also suggesting opportunities for growth and mentorship for those newer to the industry.**

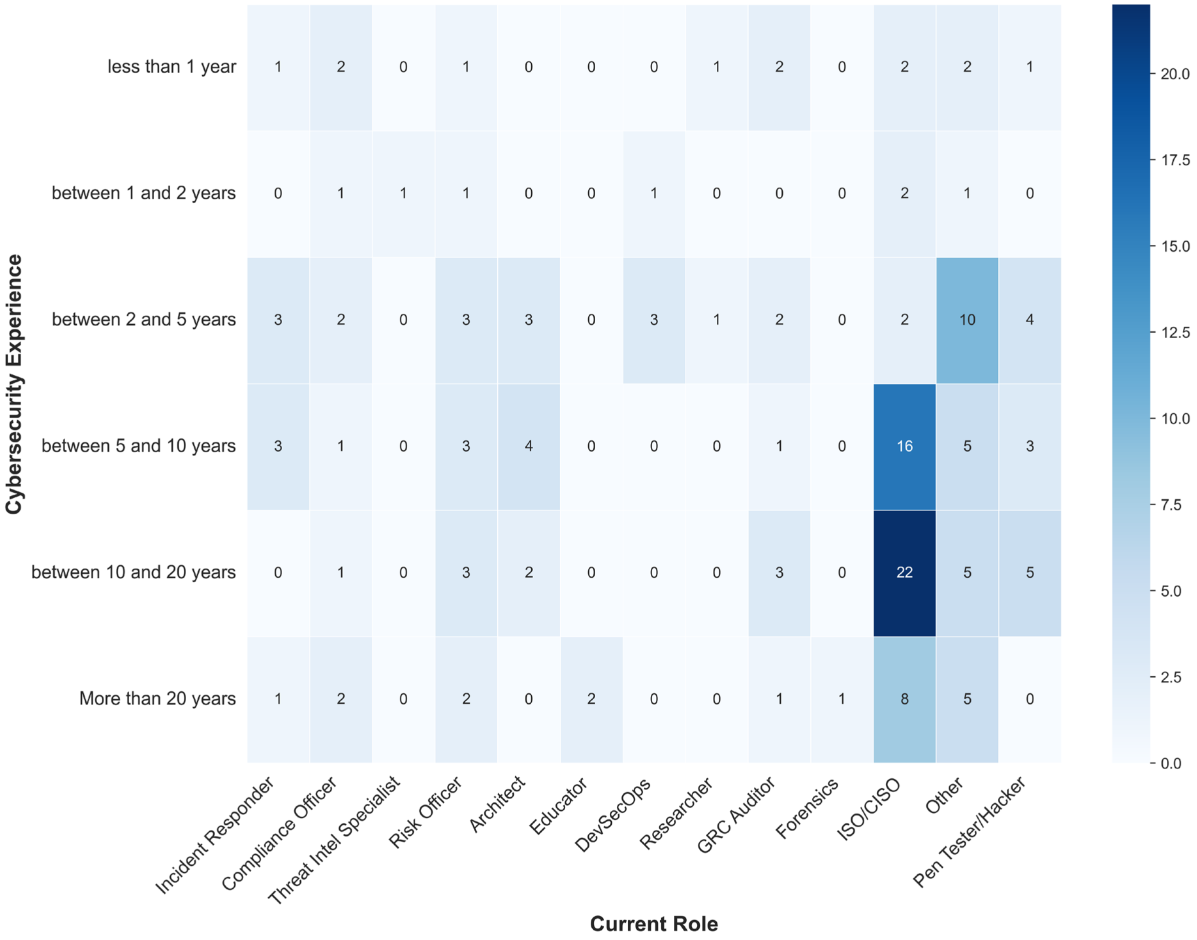


Figure 19: Distribution of cybersecurity experience across current role of the cybersecurity workforce

Insights

Luxembourg attracts 62.4% of cybersecurity professionals from abroad, mainly from France, Belgium, Germany, and some non-EU regions.

49% have worked in Luxembourg for over 5 years, and 78% of those with 5+ years in Luxembourg have 10–20 years of cybersecurity expertise.

56.7% transitioned from IT or other fields, while 42% have always worked in cybersecurity, often with 10–20 years of experience.

Management roles (33.8%) are growing, while technical roles like penetration testers, GRC auditors, and threat intelligence analysts remain critical.

Course of Actions

Talent Acquisition & Skill Diversification

Recruit Beyond Certifications

Highlight Non-Traditional Pathways

Career Visibility & Role Democratization

Showcase Success Stories

Educate about lesser-known roles

Integration & Inclusion

Language & Cultural Training

Cultural Exchange Initiatives

Community Building & Mentorship

Create Cross-Cultural Networks

Host Inclusive Events

Retention & Growth

Career Development Programs

Flexible Retention Strategies

These conclusions reflect the evolving nature of the cybersecurity workforce, with a strong emphasis on leadership roles and a diverse range of specialized positions. This strategy not only strengthens cybersecurity capabilities but also reinforces Luxembourg's reputation as an inclusive, forward-thinking hub for global professionals

Securing the future of Luxembourg's cybersecurity workforce

Opportunities and Challenges: Luxembourg Cybersecurity workforce's stability, growth, and satisfaction

Detailed information about respondent's long term commitment, market opportunities, and perception of Luxembourg's cybersecurity ecosystem is collected in the opportunities and challenges section.

Do you intend to stay in Luxembourg for more than 5 years, or do you plan to stay after the completion of your fixed term contract if it extends beyond this period?

Majority of respondents 87.9% **intend to stay in Luxembourg for more than 5 years or after their fixed-term contract ends.**

The main motivations to stay in Luxembourg are the fact that the respondent lives in the country, and the cybersecurity teams are smaller, which leads to working on a wider range of missions bringing visibility.

Fewer respondents only 8.3% of respondents do not plan to stay in Luxembourg beyond the 5-year mark or after their contract.

Younger professionals are more interested in the international environment. It's more complicated for them to see Luxembourg as a home but more as a career step.

3.8% respondents have other views.

Lack of Certain Specialized Roles: There is a perceived lack of open positions in cybersecurity research and specialized roles like pentesting and red team jobs. This scarcity makes it difficult for individuals to find relevant opportunities in Luxembourg.

> **When you focus on Reverse Engineering, Malware Analysis / Antivirus, Exploit dev. you have no opportunities.**
>
> **-Cybersecurity Professional**

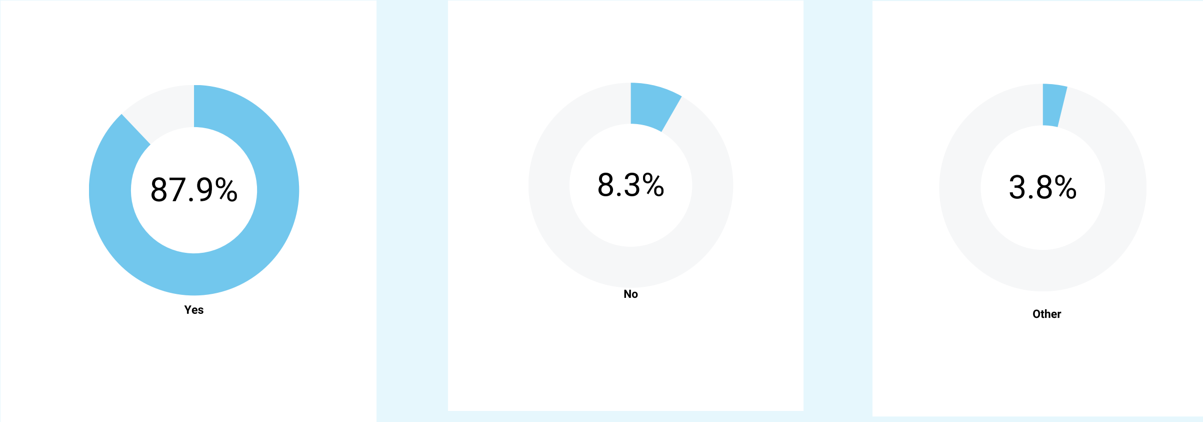


Figure 20: Distribution of respondants intentions for Long-Term Stay in Luxembourg

Top 3 reasons you would consider leaving

19%

desire for better career advancement opportunities.

17%

say high housing costs are a major concern.

14%

desire remote work policy.

- **Employees are looking for roles that offer growth and development, and a lack of such opportunities can drive them to seek employment elsewhere.**
- **The cost of living, particularly housing, is a critical factor influencing employees decisions to stay or leave.**
- **Importance of flexible work arrangements in retaining employees, especially in the post-pandemic era.**

What might be the main reasons you would consider leaving?

Other than the Top 3

- 11.1% of respondents said for better compensation.
- 8.3% of respondents would consider leaving due to family or personal reasons or commuting time. It’s surprising that both reasons have an equal number of respondents, showing that personal life and commuting challenges impact job decisions and satisfaction.
- 5.6% would consider leaving post Retirement. Retirement plans influence decisions for 2 respondents.
- 2.8% would consider leaving because of Cultural or Environmental Fit or Career Change.

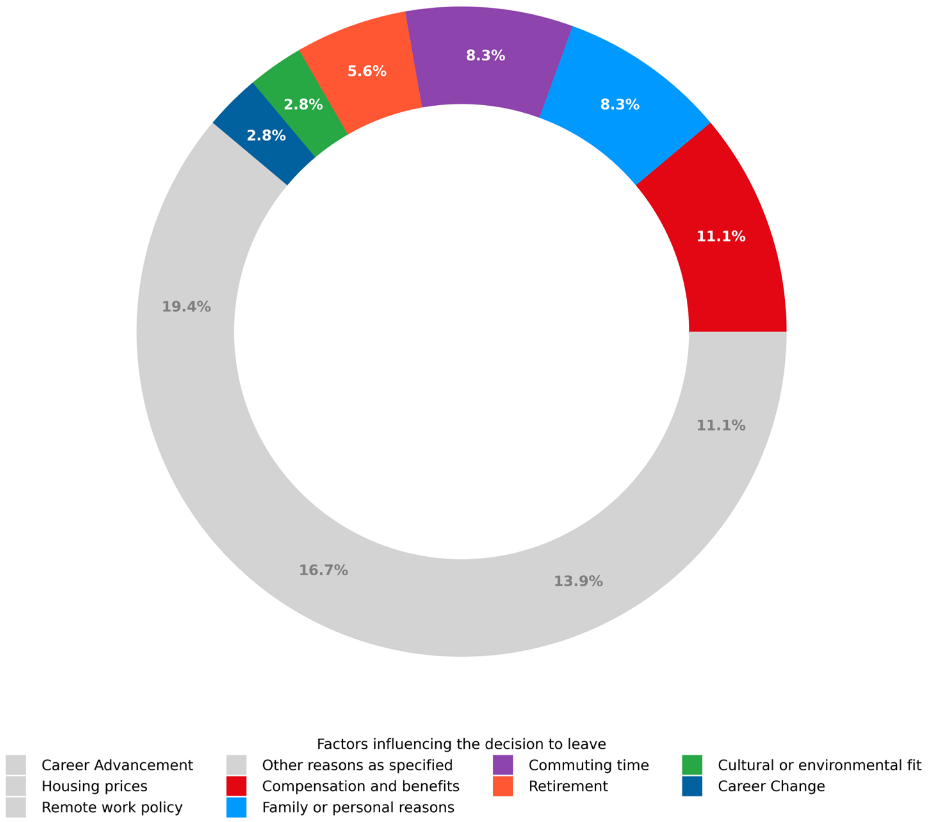


Figure 21: Distribution of respondants factors Influencing decision to leave Luxembourg other than the top 3

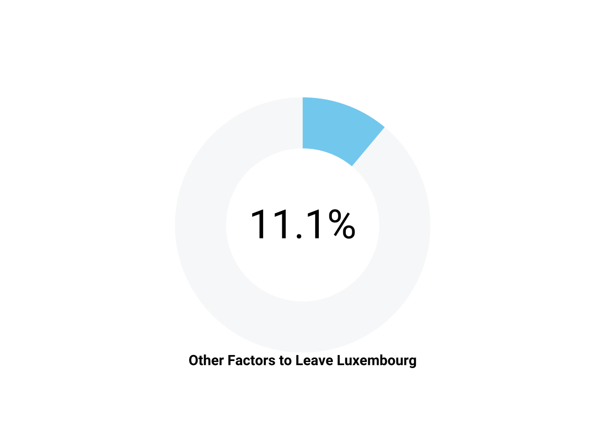


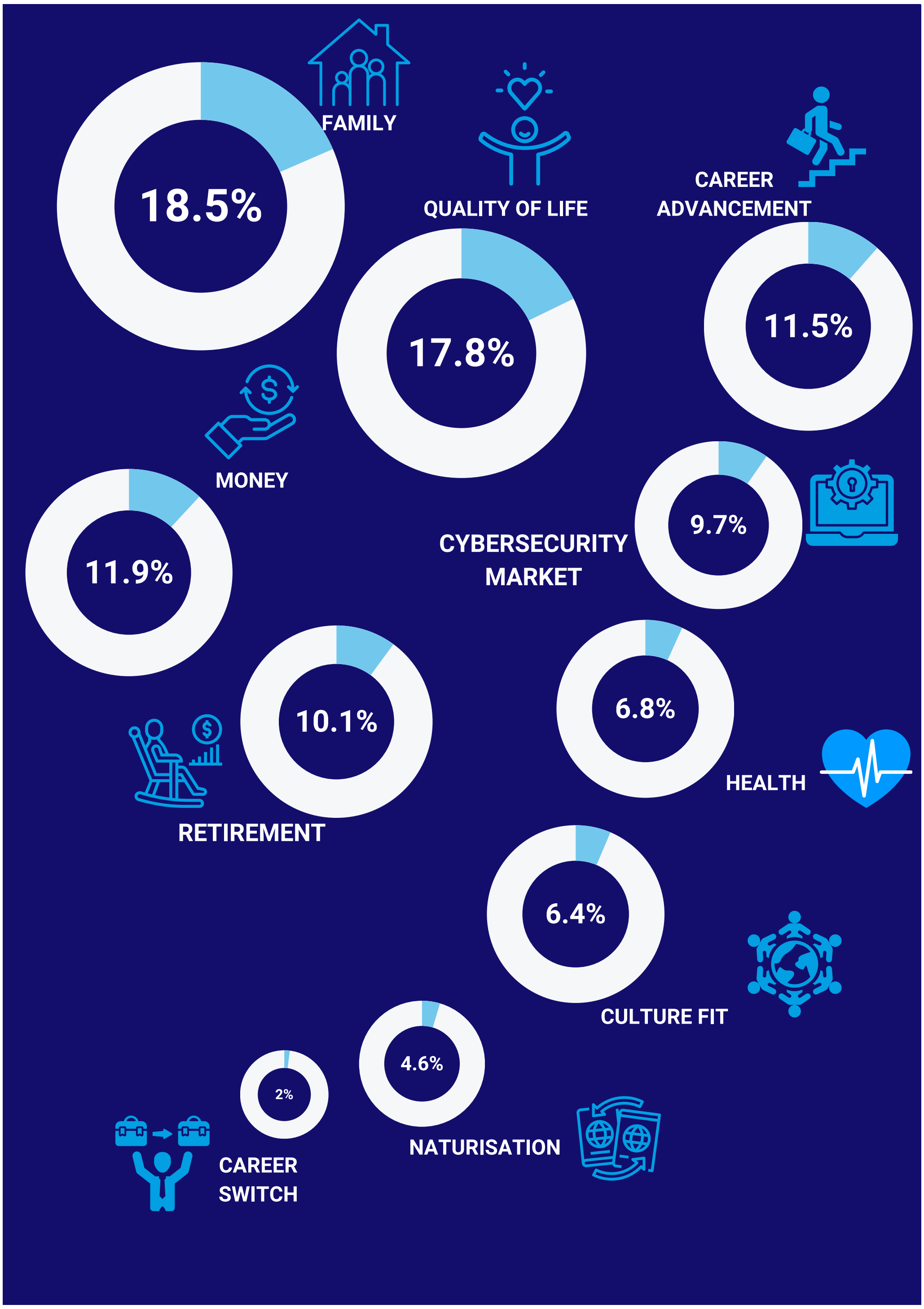
Figure 22: Distribution of respondants factors Influencing decision to leave Luxembourg focusing on Other reasons

> **Luxembourgish salaries arent the best, but professionals come to Luxembourg for the opportunity.**
> -CISO Luxembourg

Reasons for Relocating to Other Countries for Cybersecurity Jobs in Luxembourg

- **Schooling system: Potential reason for relocation.**
- **Higher salary: Private sector cybersecurity roles in neighboring countries are better compensated.**
- **Cost of living: Lower prices for services or goods in neighboring countries.**
- **Niche Roles: Limited market due to outsourcing of niche roles like red teaming.**
- **Language Requirements & Certifications: Importance of French in cybersecurity, especially in the service sector.**
- **Specific Roles: Recruitment efforts predominantly focus on candidates with specific profiles, particularly those proficient in French and experienced in Risk Management within the financial sector.**

Top 3 reasons you would consider staying



These insights suggest that personal and professional factors both play crucial roles in respondents decisions to stay in their current roles or locations.

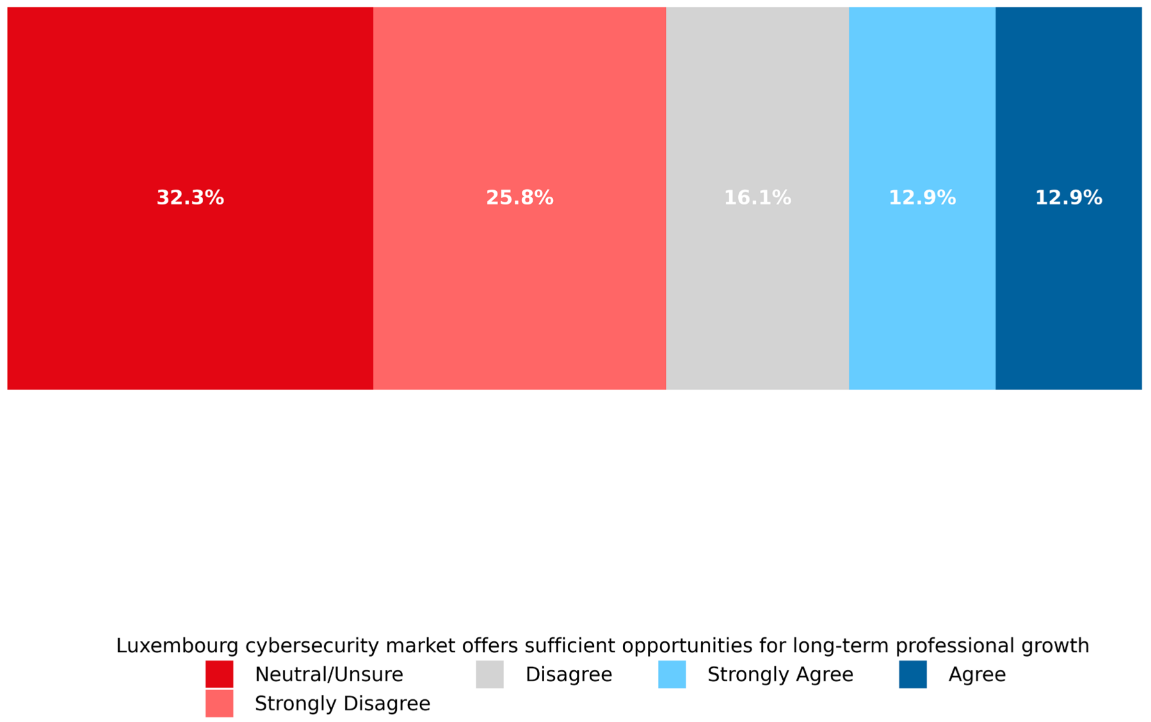


Figure 23: Perceptions of Long-Term Career Growth in Luxembourg's Cybersecurity Market

Do you think the Luxembourg cybersecurity market offers sufficient opportunities for long-term professional growth?

- Majority of respondents 32.3% are neutral/unsure about whether the market offers sufficient opportunities for long term professional growth. This indicates a significant level of uncertainty or lack of clear perception among the participants.
- A combined total of 49.1% of respondents (25.8% strongly disagree and 16.1% disagree) do not believe that the market provides adequate opportunities for long-term growth. This suggests a notable level of dissatisfaction.
- Only 25.8% of respondents (12.9% strongly agree and 12.9% agree) feel that the market does offer sufficient opportunities for long-term professional growth.

Cybersecurity: Compliance Necessity or Business Catalyst?

> The insights reflect a trend where compliance is a primary driver, but there is growing recognition of cybersecurity's strategic importance.

- **38.7% view cybersecurity primarily as a compliance obligation.**
- **32.3% see cybersecurity as both a compliance obligation and a business enabler.**
- **19.4% view cybersecurity solely as a business enabler.**
- **9.7% have other views, which could include unique or less common perspectives on the role of cybersecurity in an organization.**

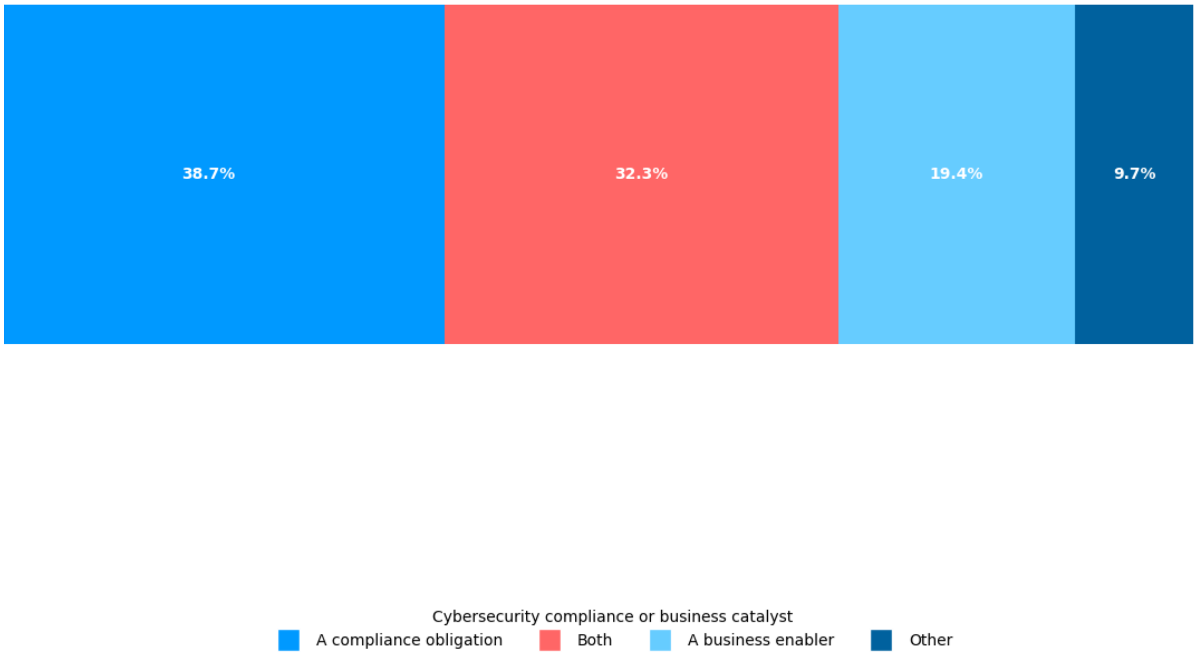


Figure 24: Distribution of respondants views on Cybersecurity

Insights

Cost of Living & Remote Work: High housing prices and inflexible remote work policies drive professionals to consider relocation.

Market Limitations: Specialized cybersecurity talent struggles to find roles in Luxembourg's compact market, leading professionals to pursue opportunities in larger ecosystems.

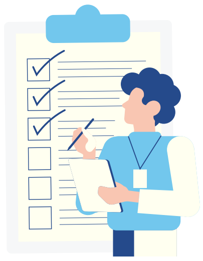
Limited opportunities for upward mobility in Luxembourg's small market push skilled workers to seek growth abroad.

Lack of awareness among employees increases security risks.

Strategic Perception Gaps: Some companies see cybersecurity as compliance rather than a strategic asset.

Rigid language requirements in consulting/ service sectors limit international talent and limit diversity.

Course of Action



To shift the perception of cybersecurity from a mere compliance obligation to a **strategic business enabler**

Employee Training & Awareness

Leadership Commitment

Integrate Cybersecurity into **Business Strategy** Highlight Success Stories with cybersecurity as business catalyst

Robust **job support** for career growth

Addressing the job market challenges

Cybersecurity: Talent Shortage? A Growing Global Concern – What About Luxembourg?

Market Trends: Cybersecurity Talent Shortage?

The increasing frequency and sophisticated cyberattacks have heightened the demand for skilled ONLY experienced professionals.

Which elements, such as evolving market trends, actions taken by private organizations, or specific policies implemented by the government, are significantly affecting the cybersecurity talent gap in Luxembourg?

38.7% of our respondents shared their views on this.

- The Luxembourg ecosystem, proximity to public authorities and private-sector professionals is a key asset.
- While government initiatives support education and training, more focus is needed on upskilling and job placement.
- Employers favor candidates with cross-domain experience, making it tough for fresh graduates and career changers. Many companies seek skilled professionals but at low costs with unrealistic experience expectations.
- Few courses are available for professionals in niche areas like penetration testing and reverse engineering
- High experience requirements and a lack of real entry-level roles hinder young professionals from entering cybersecurity.
- Long commutes, limited remote work options, and administrative burdens reduce job appeal for young talent.
- Lengthy work permit processing times often result in abandoned hires, influenced by international administrative relations.

> “Luxembourg’s cybersecurity job market is split between infrastructure and development roles. Job fairs show more data processing professionals than cybersecurity specialists. Companies prioritize standard IT profiles, outsourcing complex projects—mainly to the Netherlands and Belgium—due to the market’s limited size, reducing local role diversity.
>
> -Cybersecurity Professional

Course of Action

Early Education

Incentivize **Hiring Freshers or Transitioning Resources**

Expand opportunities for internships, apprenticeships, mentorship.

Value and **Incorporate fresh perspectives** and the enegy

Don’t look for Unicorns, Skills First Approach

Re-Skilling and Upskilling

Develop Quality Specialized trainings

Adopt remote working

Take risk and make a hard choice

Conclusion

The 2024 Cybersecurity Workforce Survey for Luxembourg highlights challenges and opportunities in the country's evolving cybersecurity landscape. Luxembourg's status as a regional employment hub attracts a diverse, international workforce, but issues like transportation difficulties for cross-border workers and high housing costs are diminishing its attractiveness, as reflected in its declining Global Talent Competitiveness Index.

The new generation of workers increasingly values work-life balance over salary, leading to a divide in the workforce between those who can afford to live in Luxembourg and those who face long commutes and housing challenges.

> **To sustain growth, leadership must integrate cybersecurity into its core business strategies, foster a culture of collaboration, and provide clear career pathways with ongoing learning opportunities.**

This includes focusing on emerging technologies, such as AI and cybersecurity threats, to equip professionals with the necessary skills to stay ahead of industry trends.

Addressing talent shortages requires focusing on fresh graduates, non-traditional candidates, and high-quality reskilling programs. Embracing skills over unrealistic experience requirements will broaden the talent pool, while early education initiatives and strategic mentorship can help cultivate a future cybersecurity workforce. Additionally, creating a supportive ecosystem with recognition programs, innovative project involvement, and cross-functional collaboration will keep professionals engaged and motivated. Flexible work arrangements and language training will further improve work-life balance and communication within a diverse workforce.

By focusing on these priorities, Luxembourg can position itself as a global leader in cybersecurity, attracting, developing, and retaining a dynamic, inclusive workforce ready to tackle the challenges of the future.

Methodology

Research methodology:

1. Reviewed existing literature and data sources as a foundation for the study.

2. Applied a **PEST** (Political, Economic, Sociological, and Technological) matrix to explore external factors affecting cybersecurity workforce in Luxembourg.

3. Generated research hypotheses and formulated them into survey questions.

4. Administered an online survey in to collect first hand data from cybersecurity professionals working in Luxembourg and gather new market statistics.

5. Conducted in-depth interviews with Cybersecurity leaders, managers and professionals for detailed insights related to the survey.

6. Received peer and expert reviews from the Luxembourg House of Cybersecurity.

nc3
Cybersecurity
Observatory

Published by the Luxembourg House of Cybersecurity
April 2025