eTeam

Global Cybersecurity Workforce Insights Report

Presented by

WIT
Workforce Intelligence Team

eTeam's Workforce Intelligence Team

Table of Contents

Global Trends

Cybersecurity workforce shortage

Why is There a Talent Shortage?

The cybersecurity talent shortage is driven by several factors. Rapid technological changes create a skills gap, as organizations struggle to maintain up-to-date knowledge among employees (Cybersecurity Ventures, 2023).

An aging workforce compounds this issue, with many seasoned professionals nearing retirement and insufficient succession planning to replace them (ISACA, 2023). With 58% of cybersecurity professionals having over eight years of experience, there is a significant gap in early talent recruitment (Global Cybersecurity Talent Report 2024).

Economic constraints, particularly for smaller businesses, limit the hiring of high-salary professionals (Gartner, 2023). Moreover, the demanding nature of cybersecurity roles leads to burnout and high attrition rates (Dark Reading, 2023). Addressing these factors is critical to building a robust cybersecurity workforce.

Compliance demands from regulations like GDPR and CCPA heighten the need for specialized roles, further straining the talent pool (Ponemon Institute, 2023). A lack of career pathway clarity deters younger generations, resulting in fewer new entrants into the field (CyberSeek, 2024). Gender and minority representation gaps persist, hindering diversity efforts (Women in Cybersecurity Report, 2023).

Early Talent

How Can Early Talent Help?

Early talent is crucial in closing the skills gap. According to the (ISC)² Cybersecurity Workforce Study (2024), 74% of cybersecurity professionals believe that investing in early talent is essential for long-term sustainability.

By investing in structured training and education programs, organizations can cultivate a new generation of cybersecurity professionals equipped with the latest skills and knowledge. This includes partnerships with top schools and universities for talent development, with 68% of companies reporting successful recruitment from these institutions.

Moreover, creating clear pathways for entry-level positions, alongside mentorship programs, offers not only initial employment but also opportunities for growth and specialization. These initiatives have shown that 82% of entry-level hires stay with their employers for over three years, significantly reducing the turnover rate compared to mid-career hires.

Global Trends

Emerging Threats & Addressing Them

New Threats Emerging

According to the Cyber Threat Trends Report by Cisco (2024), the most prevalent threats continue to evolve and intensify. Analyzing year-over-year data, we've observed a notable increase of approximately 20% in the frequency and sophistication of these cyber threats:

1. **Information Stealers**

   These threats, which focus on extracting sensitive data such as passwords and financial information, have surged by 22% over the past year, averaging 246 million blocks monthly. This rise can be attributed to enhanced targeting techniques and broader deployment by cybercriminals.

2. **Trojans**

   Known for their sophisticated evasion techniques, Trojans have increased in frequency by 18%, accounting for 175 million blocks. This persistent growth underscores the need for advanced detection measures as these threats continue evolving to bypass traditional security systems.

3. **Ransomware**

   Ransomware incidents, including notorious variants like Lockbit, have escalated by 25% year over year, with 154 million blocks recorded. As attackers refine their tactics and expand their reach, predictions suggest a continued upward trend, capitalizing on vulnerable systems and data-heavy environments.

4. **Remote Access Trojans (RATs) and Botnets**

   These threats, offering unauthorized control over systems and causing widespread disruptions, have shown a growth rate of 15% compared to the previous year. As reliance on connected devices expands, experts predict these threats will further proliferate, exploiting the increasing number of endpoints and IoT devices.

Overall, projections indicate that these threats will continue to rise, driven by technological advancements in adversarial tactics and the increasing digitalization of economies worldwide.

Addressing New Threats

Cybersecurity professionals are adopting a multi-layered approach to mitigate emerging threats. This includes:

DNS Security

Leveraging DNS-layer security provides accurate detection and prevention of malicious activities. Cisco's Talos intelligence, for instance, processes an average of 715 billion daily DNS requests, providing unmatched threat visibility.

Advanced Threat Intelligence

Utilizing real-time data and analytics, professionals can proactively identify and neutralize threats.

New Technologies and Coding Languages

Emerging technologies like AI and machine learning are crucial in automating threat detection and response. These technologies enhance security resilience by analyzing patterns and predicting potential breaches. Moreover, the adoption of new coding languages, such as Rust and Go, is gaining traction due to their security-centric features and memory safety.

Recommendations

- Invest in Training:
  Develop robust training programs to nurture early talent.
- Adopt Advanced Technologies:
  Leverage AI, machine learning, and DNS security for proactive threat management.
- Strengthen Partnerships:
  Collaborate with educational institutions to create a pipeline of skilled professionals.

By staying informed and agile, organizations can not only protect their digital assets but also lead in the cybersecurity domain, ensuring a secure and resilient digital future.

Predicted Expansion of Threats in the Next 3 Years

As we look ahead, the landscape of cybersecurity threats is expected to evolve significantly, driven by technological advancements and increased connectivity. Here are some anticipated trends and developments over the next three years:

Increase in AI-Driven Attacks

Artificial intelligence (AI) is not only transforming cybersecurity defenses but is also being leveraged by attackers to carry out more sophisticated and automated attacks. We can expect to see:

- **AI-Powered Malware:** Capable of adapting and modifying itself to escape detection, these threats will likely become more prevalent.
- **Deepfake Scams:** Utilization of AI to create highly convincing fake audio and video content could be used to impersonate high-profile individuals for fraudulent purposes.

Expansion of Attack Vectors

As more devices connect to the internet, the potential attack surface continues to grow:

- **IoT Vulnerabilities:** With the proliferation of Internet of Things (IoT) devices, attackers will have a larger landscape to exploit, targeting vulnerabilities in devices that may lack robust security measures.
- **Supply Chain Attacks:** These attacks will become more frequent as attackers find ways to compromise third-party vendors to infiltrate larger networks.

Emerging Threats in the Cloud Environment

As organizations move more operations to the cloud, cloud-specific threats are expected to rise:

- **Cloud Ransomware:** Attackers are likely to target cloud storage and applications, encrypting entire datasets and demanding ransom for decryption.
- **Misconfigured Systems:** With many organizations struggling to properly secure their cloud environments, improperly configured systems will pose significant risks.

Heightened Focus on Cyber Espionage

Nation-state actors will continue to engage in cyber espionage, targeting critical infrastructure and sensitive data:

- Critical Infrastructure Targeting:
  Electricity grids, water supply, and other critical infrastructure remain at risk, with attacks potentially causing widespread disruption.
- Data Exfiltration:
  Sophisticated techniques for stealing intellectual property and sensitive information will become more advanced.

Proactive Measures to Anticipate

Organizations can prepare for these expanding threats by:

- **Strengthening AI Defenses:**
  Leveraging AI and machine learning to anticipate and respond to AI-driven threats.
- **Enhancing Cloud Security:**
  Implementing strong security practices and regular audits of cloud configurations to prevent breaches.
- **Securing IoT Devices:**
  Adopting advanced security protocols for IoT devices to minimize vulnerabilities.
- **Collaborative Threat Intelligence:**
  Sharing threat intelligence across industries to stay ahead of emerging threats.

By anticipating these developments, organizations can fortify their defenses and be better equipped to safeguard their digital ecosystems against the shifting threat landscape.

For further insights and guidance on cybersecurity talent acquisition and threat management strategies, or your own custom trends report, please contact

Anthony Maggio at amaggio@eteaminc.com.

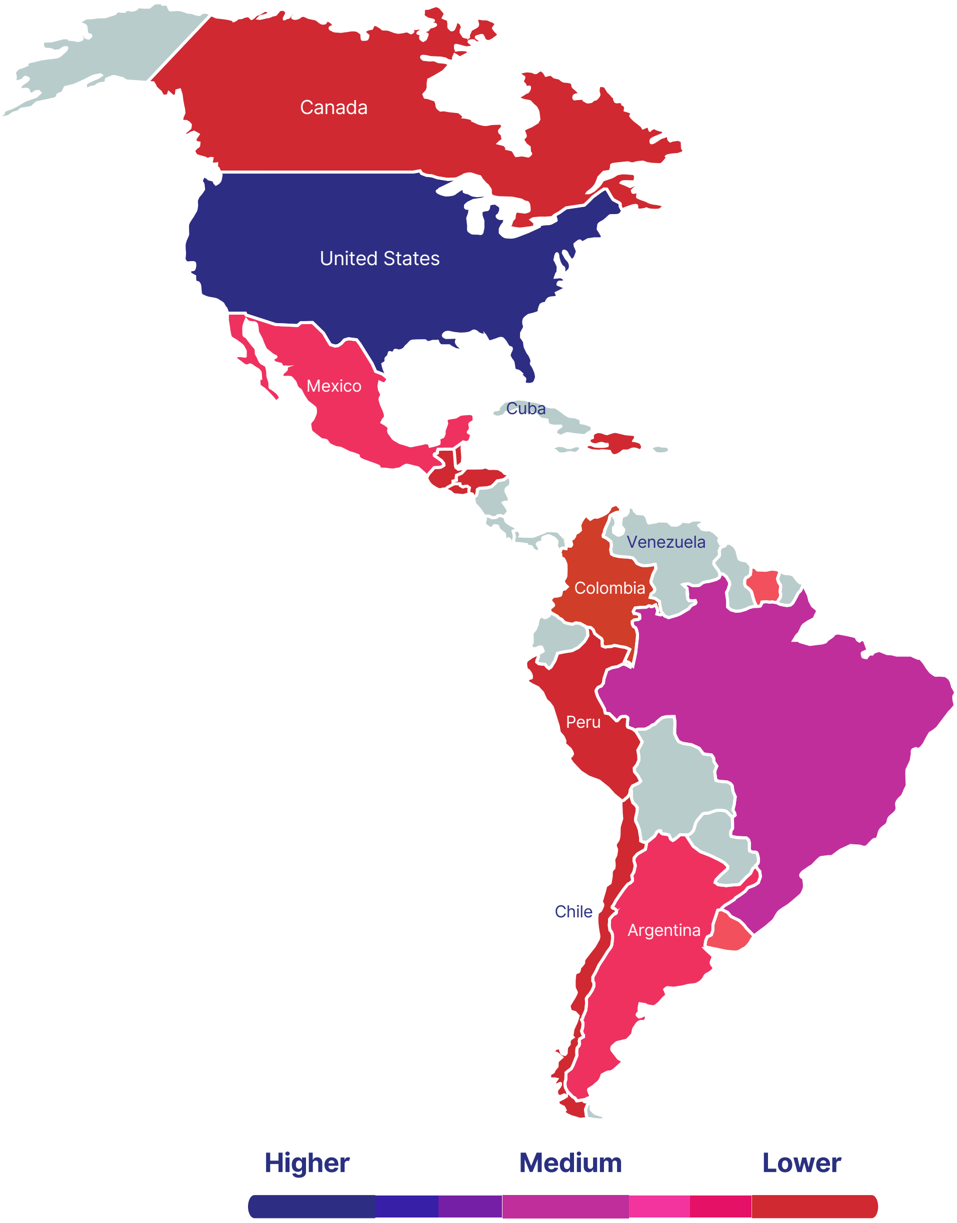
Top Locations & Costs for Cyber Security Workforces

Location	Full-Loaded Costs	SOW
United States	$196,272.78	$153.34
China	$71,291.58	$74.26
India	$27,869.20	$29.03
Philippines	$24,238.59	$25.25
Japan	$139,985.27	$109.36
Germany	$138,230.28	$107.99
Brazil	$59,337.69	$61.81
Italy	$152,966.99	$119.51
Mexico	$50,812.22	$52.93
Indonesia	$34,168.83	$35.59
France	$155,557.68	$121.53
Turkey	$31,674.40	$32.99
United Kingdom	$148,561.34	$116.06
Argentina	$107,044.85	$111.51
Netherlands	$121,102.60	$94.61
Malaysia	$48,323.35	$50.34
Spain	$97,000.30	$75.78
Romania	$33,269.36	$34.66
Canada	$155,890.12	$121.79
Austria	$121,790.93	$95.15

About this graph

Because nearly 70% of talent has 8+ year of experience, the average salaries are much higher than comparable roles. This chart includes both the fully loaded costs and SOW hourly. Fully loaded costs include all statuaries and fees, including any country-specific requirements for that labor. SOW or statement of work costs encompasses the costs of labor which the client would not directly manage the labor; instead eTeam would be responsible for paying, managing, and the overall results of the work being done. SOW includes all associated fees of managing the entire project from start to finish.

Global Spotlight – Americas



Key Insights

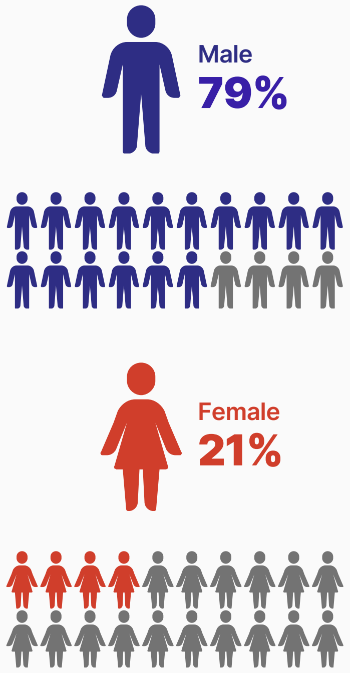
I The US is both locally and globally the home to the greatest concentration of cyber security talent. The draw back is that it is also one of the most expensive locations to employ this talent

II LATAM presents a unique opportunity for cost-effective talent. The WIT recommends diving deeper into locations like Mexico, where salaries, government/local costs, AND fees are relatively lower than the rest of LATAM

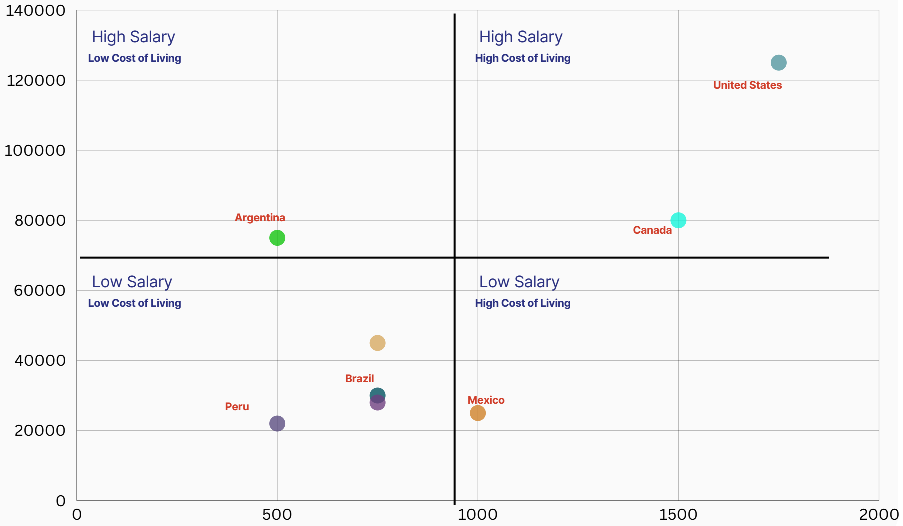
III Guatemala, Dominican Republic, and Brazil have the highest number of available candidates per role. While they cost more than Mexico, talent is more readily available

Global Spotlight – Americas

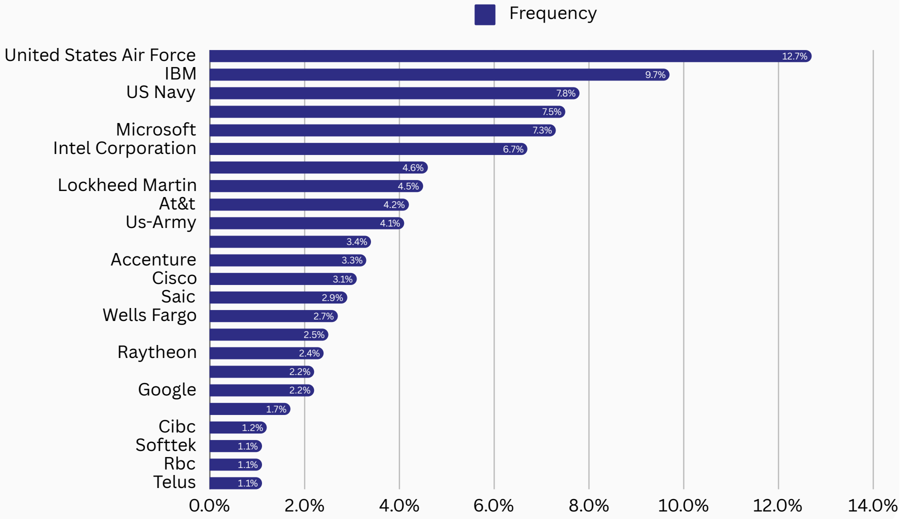
Gender Breakdown



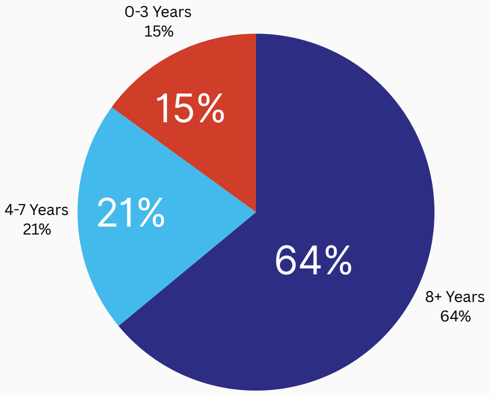
Salary Breakdown



Top Companies



Experience Breakdown

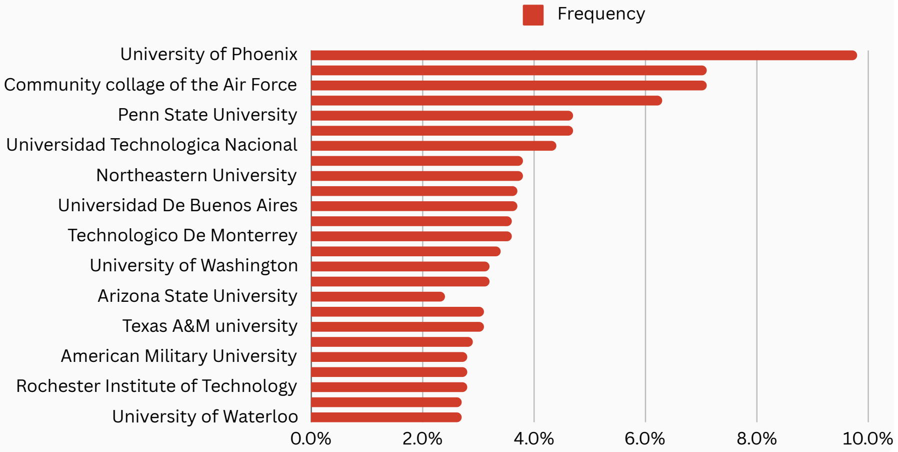


■ 8+ years

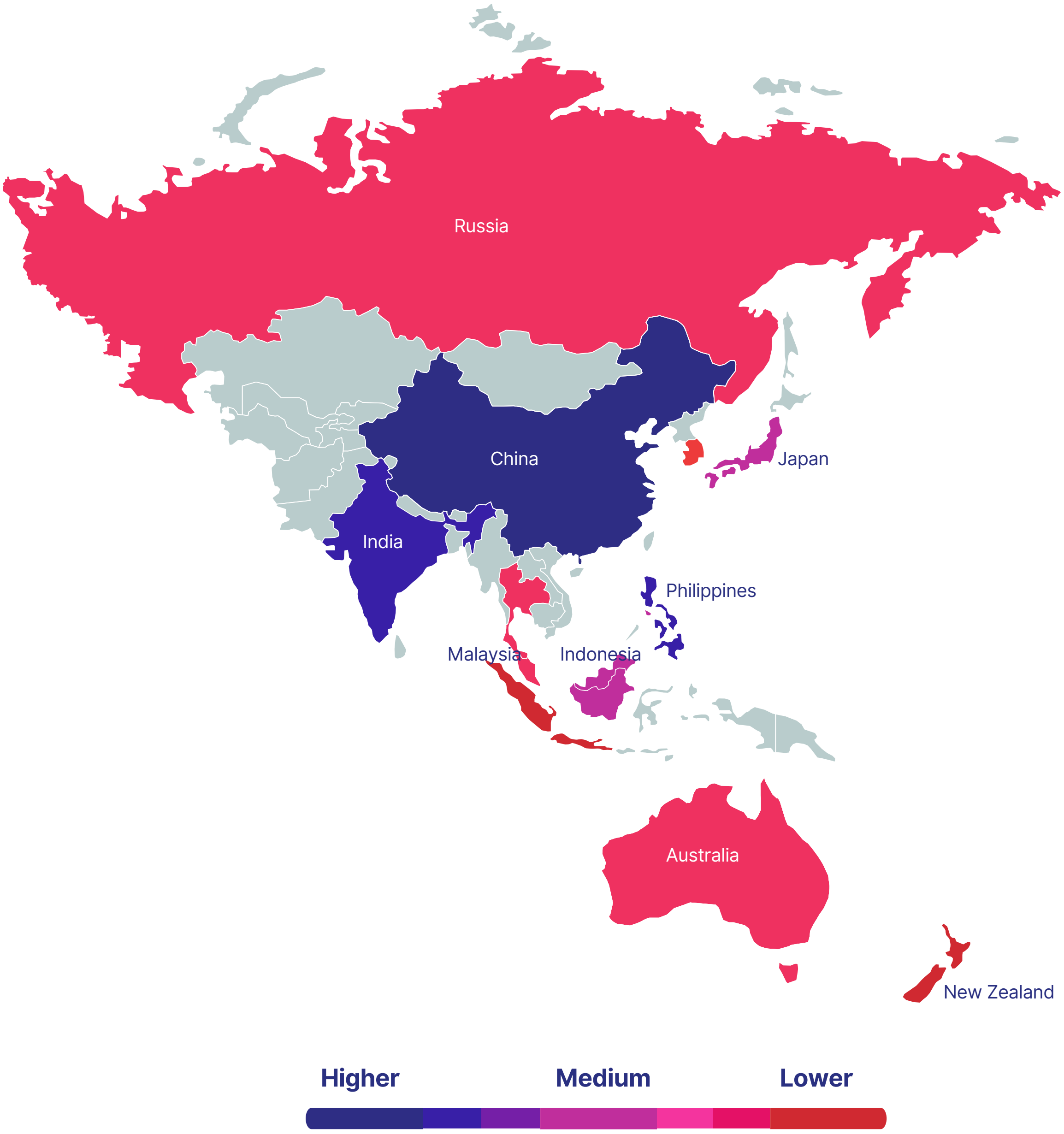
■ 4-7 years

■ 0-3 years

Top Universities



Global Spotlight – APAC



Key Insights

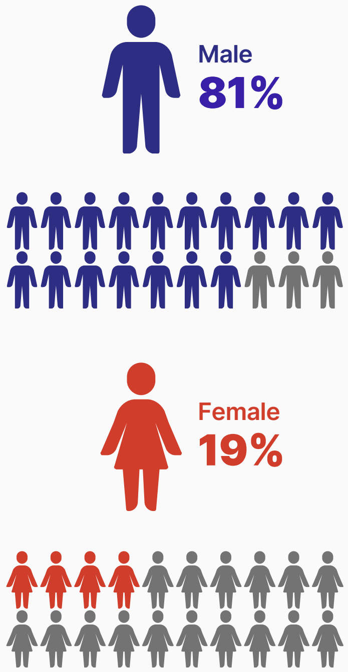
I — India has some of the lowest costs – and fees. Making it an ideal location for employing global cybersecurity talent.

II — The Philippines also present a great opportunity. While slightly more expensive than India, the number of available candidates per role is far greater, with comparable fees.

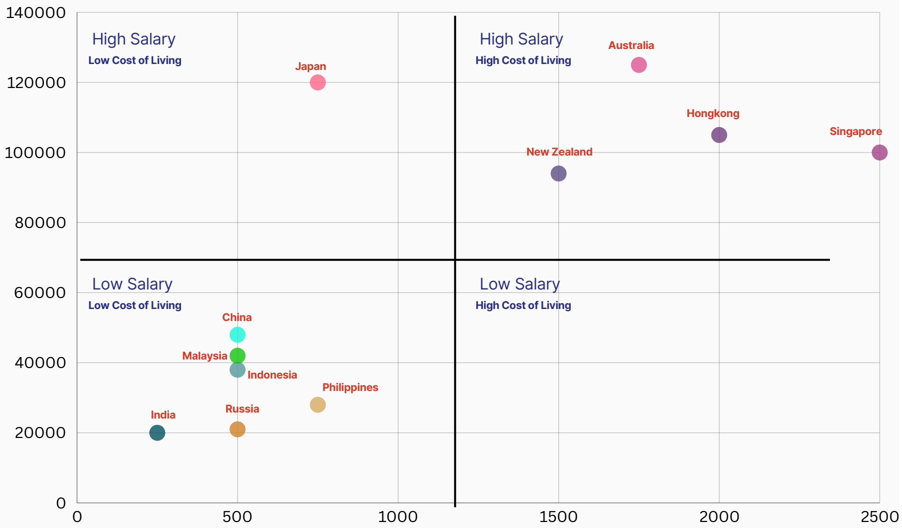
III — Japan presents an interesting opportunity. While salaries can be quite high, the lower cost of living insinuates that for the right rates, you could really find some quality, lifetime employees there.

Global Spotlight – APAC

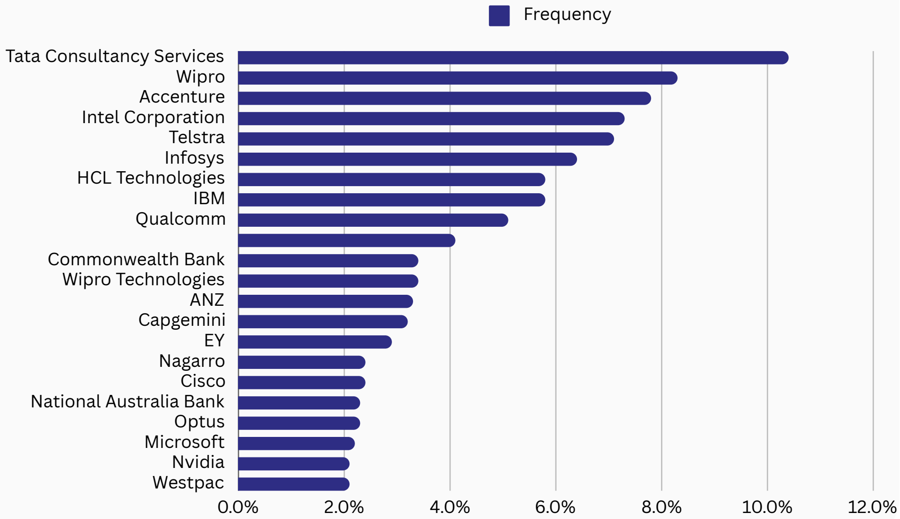
Gender Breakdown



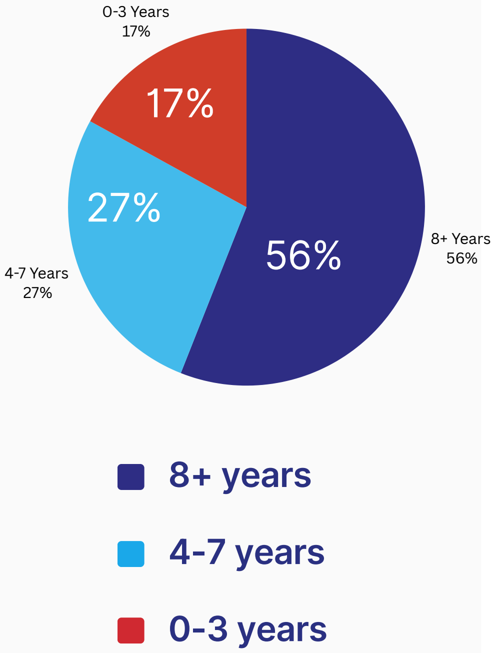
Salary Breakdown



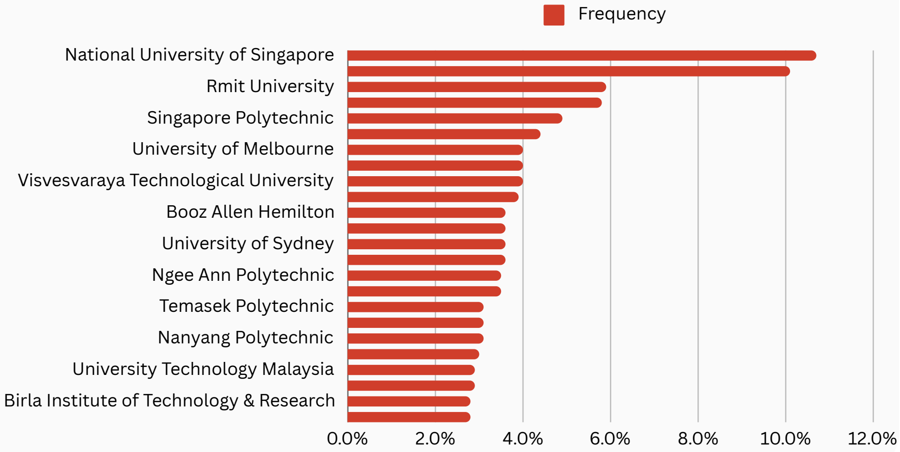
Top Companies



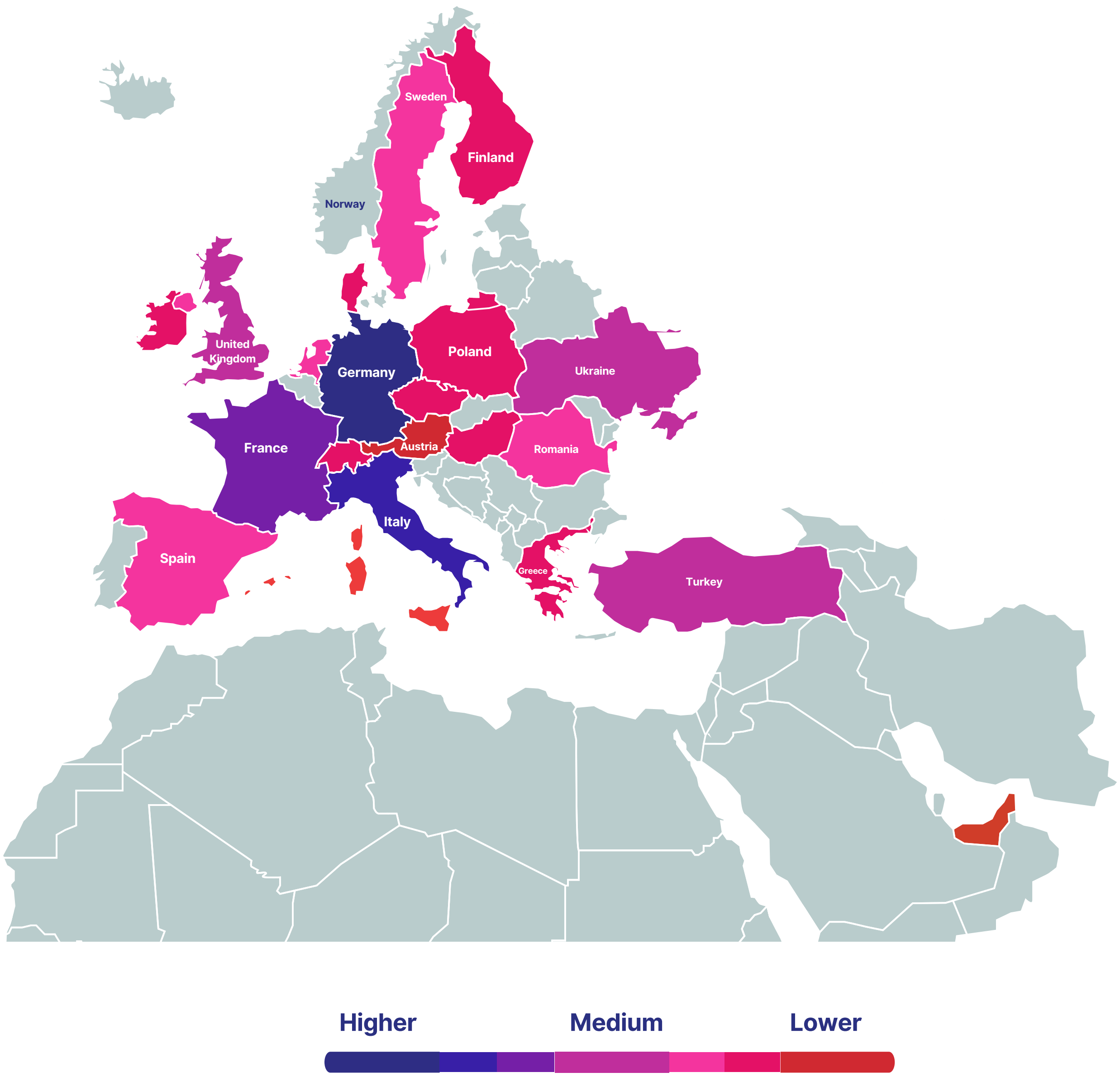
Experience Breakdown



Top Universities



Global Spotlight – EMEA



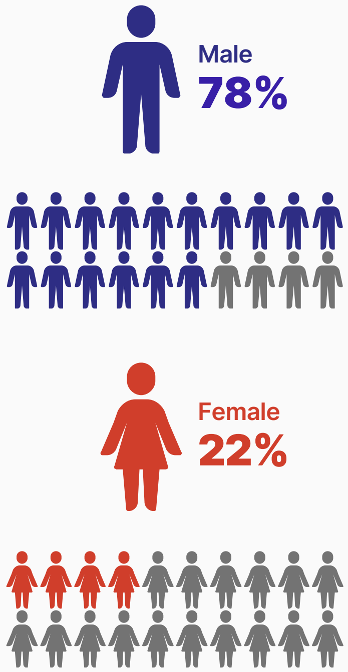
Key Insights

I Turkey and Ukraine have a great deal of candidates per role available, as well as very competitive pricing. While not as cost efficient as LATAM or APAC, both locations present an ideal location for EMEA talent.

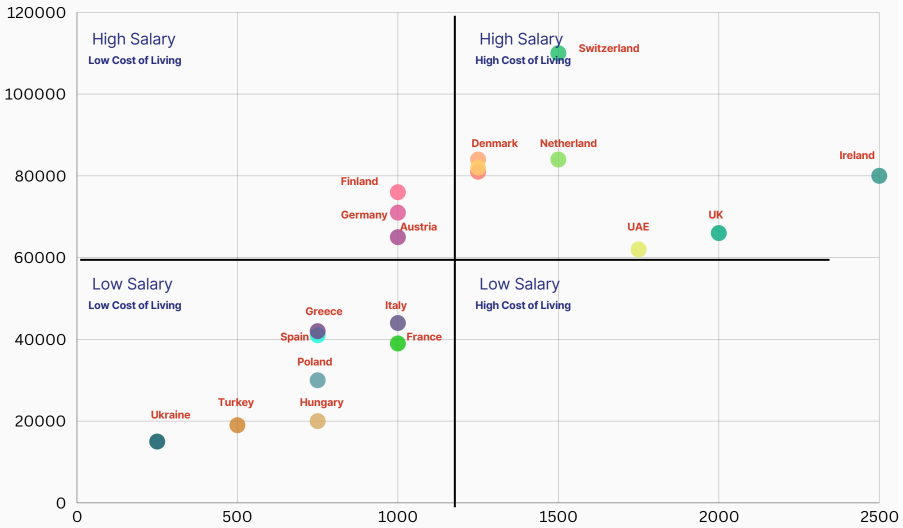
II Switzerland has several factors making it one of the most expensive locations for cyber talent globally. A large talent shortage and strong demand in the area drives up rates. There is also a huge financial sector in the country further driving up the need for talent. This hints that for financial companies seek top-talent, Switzerland is a strong contender.

Global Spotlight – EMEA

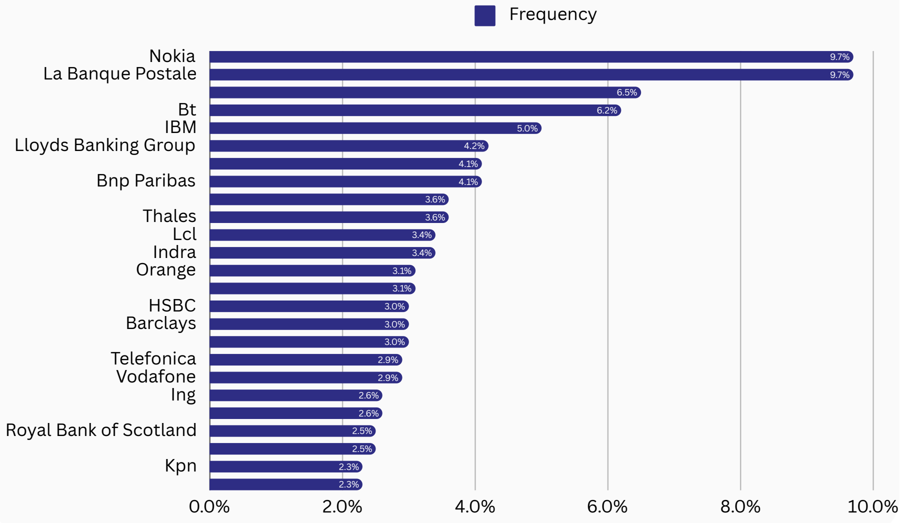
Gender Breakdown



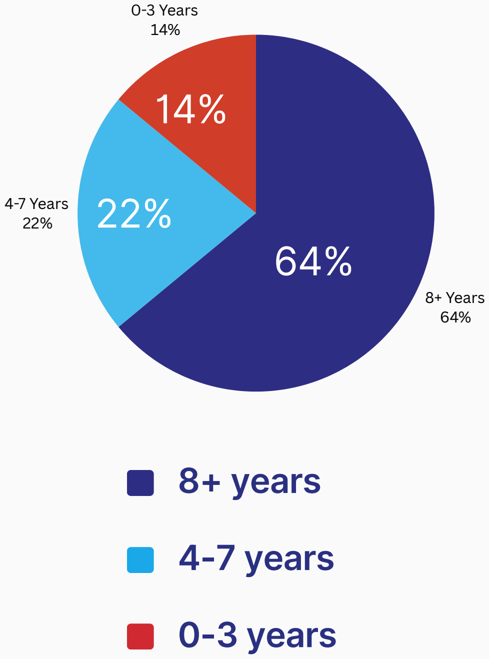
Salary Breakdown



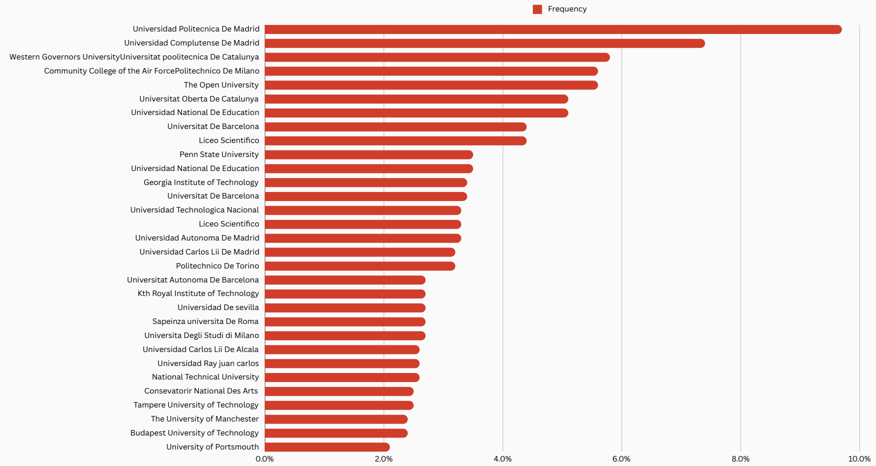
Top Companies



Experience Breakdown



Top Universities

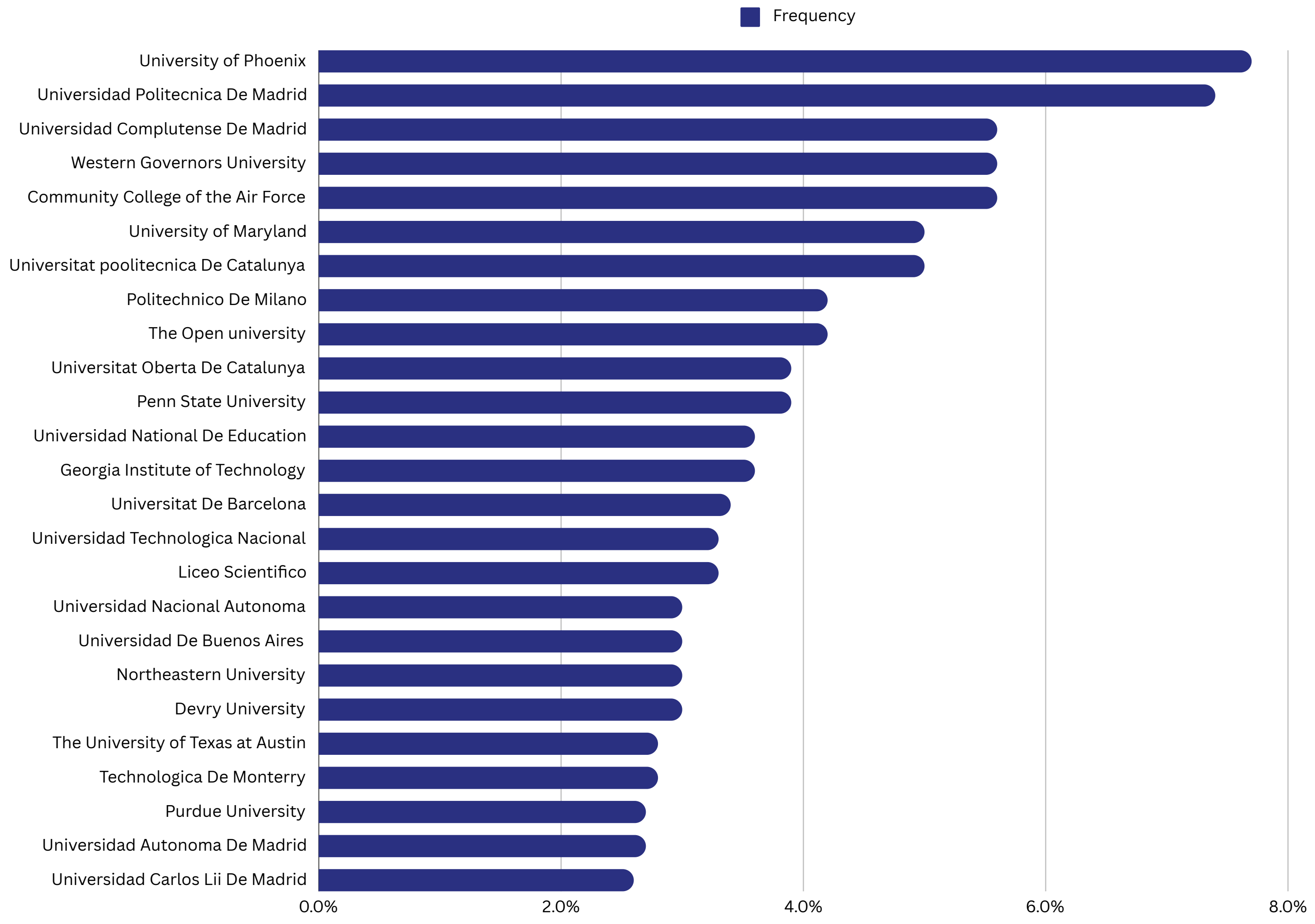


Global Trends

Early Talent Highlights

The cybersecurity landscape is constantly evolving, with new threats emerging daily. By nurturing young talent, we ensure a steady influx of fresh perspectives and innovative solutions to tackle these challenges. Early exposure to cybersecurity principles and practices helps build a strong foundation, enabling young engineers to develop critical thinking and problem-solving skills essential for the field.

Top Universities Globally for Cyber Talent



Additionally, the demand for cybersecurity professionals far exceeds the supply, making it vital to cultivate talent early to bridge this gap. Investing in early talent development also fosters a culture of continuous learning and adaptability, which is essential in a field where staying updated with the latest technologies and threats is paramount. Ultimately, by prioritizing the growth of young cybersecurity engineers, we not only enhance the security of our digital infrastructure but also empower the next generation to lead and innovate in this critical domain.

In-Demand Cybersecurity Skills

And Why You Should Base Your Hiring for Them

With more organizations moving operations to the cloud, expertise in securing cloud environments, understanding cloud architecture, and risk management in cloud settings are critical.

- Threat Intelligence Analysis:
  The ability to gather, analyze, and interpret threat data to anticipate and mitigate potential cyber attacks is increasingly important.
- Penetration Testing:
  Skills in simulating attacks to test the defenses of IT systems are vital for identifying vulnerabilities and enhancing security measures.
- Incident Response:
  Proficiency in quickly responding to and managing security breaches to minimize impact and prevent future incidents is essential.
- Network Security:
  Expertise in designing and implementing secure network architectures to protect against intrusions and data loss is in high demand.
- Security Automation:
  As threats become more sophisticated, the ability to use automation tools for threat detection and response enhances efficiency and effectiveness.

Importance of Skills-Based Hiring

Skills-based hiring emphasizes specific abilities and competencies over traditional credentials. This approach is crucial in the fast-paced field of cybersecurity for several reasons:

- **Addressing Talent Gaps:**
  By focusing on skills, organizations can tap into a broader talent pool, including non-traditional candidates who may not have formal degrees but possess the necessary technical expertise.
- **Adaptable Workforce:**
  A skills-focused approach ensures that the workforce is adaptable and capable of keeping up with rapidly evolving technologies and threats.
- **Cost-Effectiveness:**
  Skills-based hiring can be more cost-effective, reducing reliance on costly certifications and allowing employers to train new hires in specific areas needed for their roles.

Future Outlook

As cybersecurity threats become more sophisticated, the importance of skills-based hiring will continue to grow:

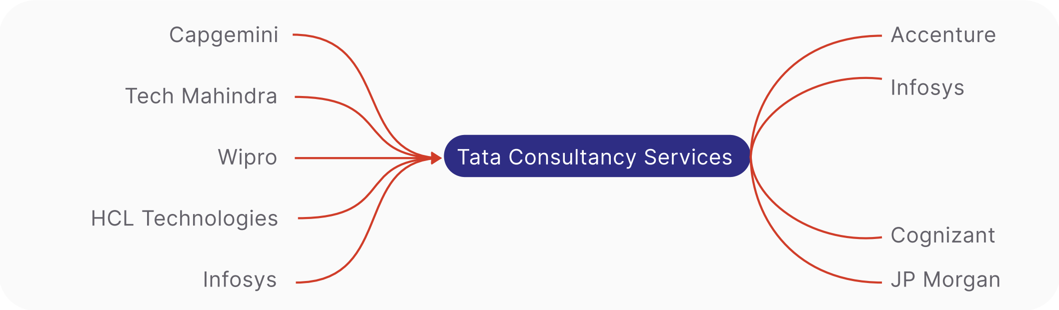
- **Agility and Innovation:** Organizations will benefit from an agile workforce that can innovate and adapt to new challenges, with employees who are constantly upgrading their skillsets.
- **Diversity and Inclusion:** Skills-based hiring can lead to a more diverse workforce by valuing varied experiences and perspectives, essential for tackling complex cybersecurity challenges.
- **Sustainable Talent Development:** Focusing on skills provides a pathway for continuous learning and development, ensuring a sustainable talent pipeline that can evolve with technological advancements.

In conclusion, prioritizing skills-based hiring now and in the future is essential for building a resilient and capable cybersecurity workforce, adequately prepared to defend against an ever-changing threat landscape.

Competitive Insights

It’s important to note that globally, the top employers for cybersecurity talent skew heavily to the American military-industrial complex. When the military is excluded, we get a better understanding of the bigger picture. This section will highlight the top 8 employers of Cybersecurity Enginees, as well as which companies they hire from and which companies they lose their talent to. Ideally this information should be shared with your recruitment and HR teams to understand WHERE the top talent is working

Hiring Talent From



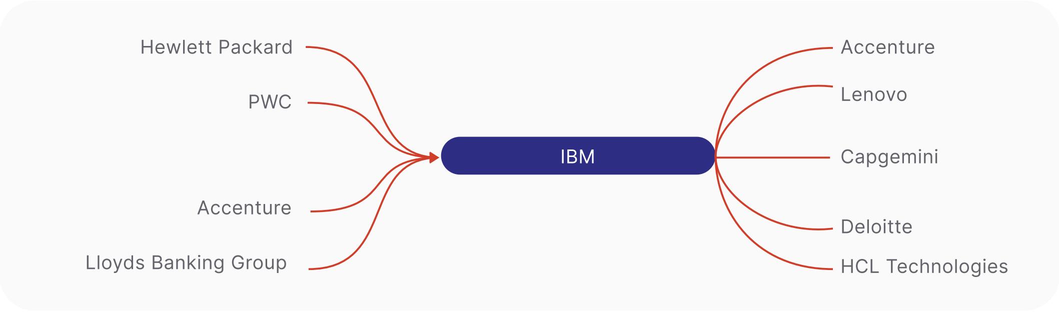
Capgemini
Tech Mahindra
Wipro
HCL Technologies
Infosys

Tata Consultancy Services

Accenture
Infosys
Cognizant
JP Morgan

Losing Talent to

Hiring Talent From



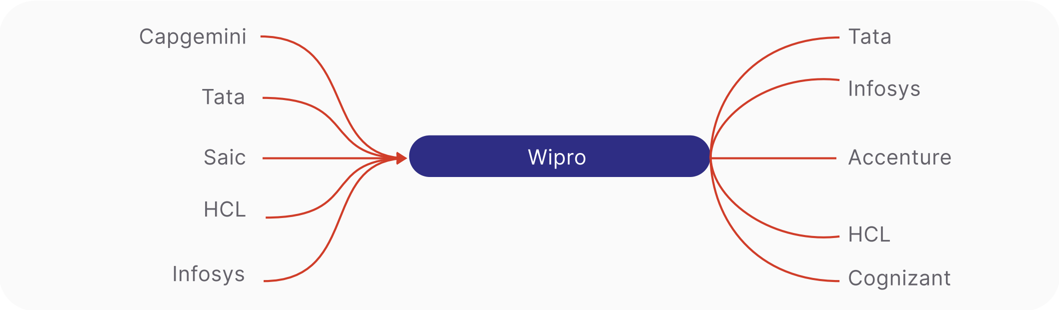
Hewlett Packard
PWC
Accenture
Lloyds Banking Group

IBM

Accenture
Lenovo
Capgemini
Deloitte
HCL Technologies

Losing Talent to

Hiring Talent From



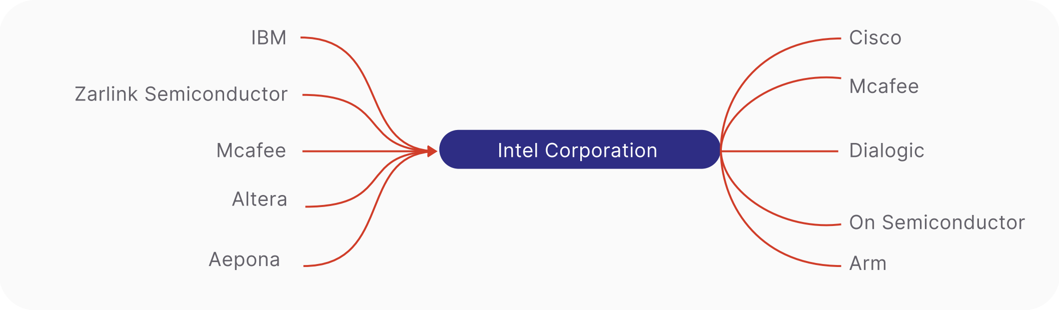
Capgemini
Tata
Saic
HCL
Infosys

Wipro

Tata
Infosys
Accenture
HCL
Cognizant

Losing Talent to

Hiring Talent From



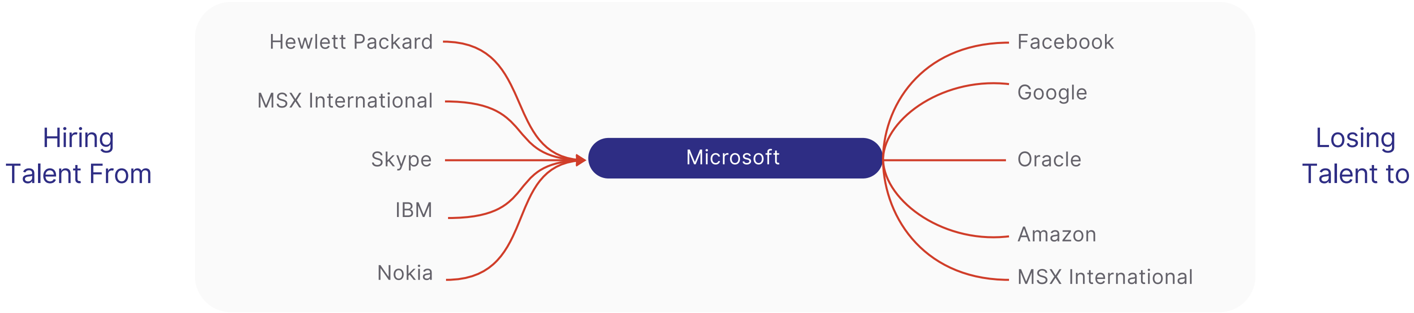
IBM
Zarlink Semiconductor
Mcafee
Altera
Aepona

Intel Corporation

Cisco
Mcafee
Dialogic
On Semiconductor
Arm

Losing Talent to

Competitive Insights



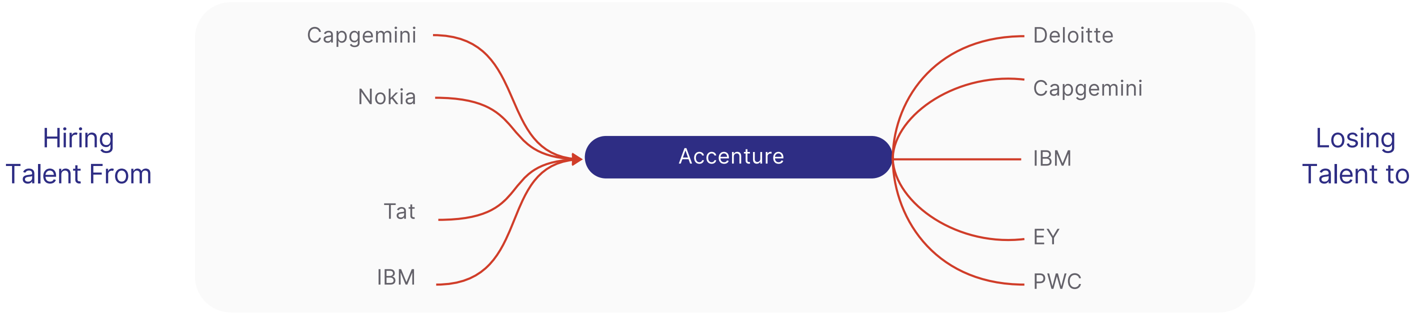
Hiring Talent From

Hewlett Packard
MSX International
Skype
IBM
Nokia

Microsoft

Losing Talent to

Facebook
Google
Oracle
Amazon
MSX International



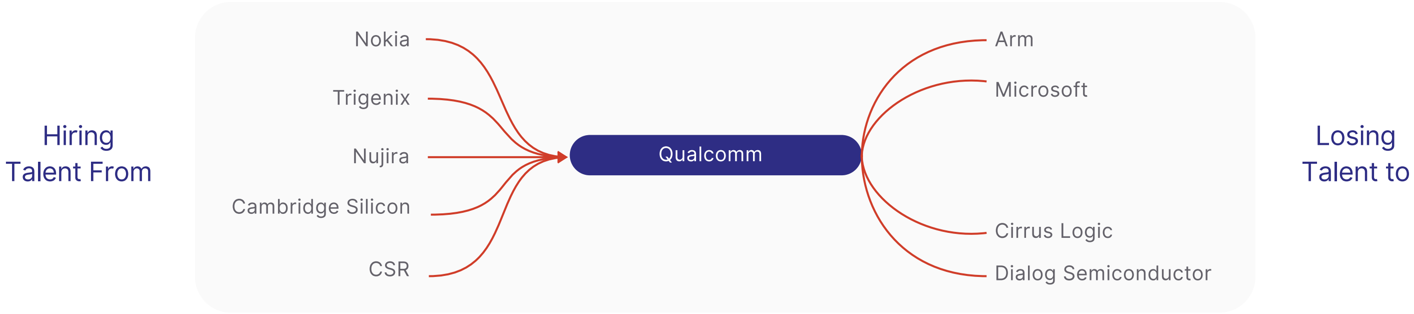
Hiring Talent From

Capgemini
Nokia
Tat
IBM

Accenture

Losing Talent to

Deloitte
Capgemini
IBM
EY
PWC



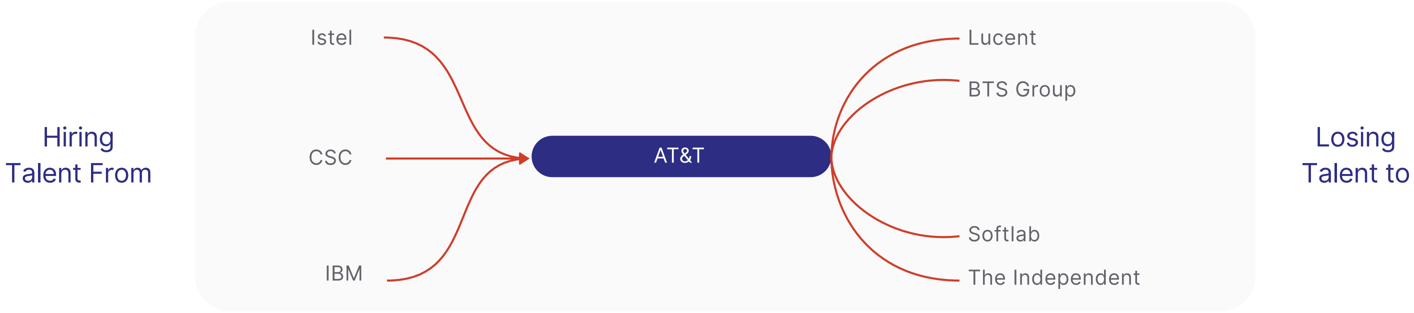
Hiring Talent From

Nokia
Trigenix
Nujira
Cambridge Silicon
CSR

Qualcomm

Losing Talent to

Arm
Microsoft
Cirrus Logic
Dialog Semiconductor



Hiring Talent From

Istel
CSC
IBM

AT&T

Losing Talent to

Lucent
BTS Group
Softlab
The Independent

Summary & Contact US

About eTeam Inc.

eTeam is a 25-year talent solutions leader that works with 75% of Fortune 500 companies. With operations in over 150 countries, we specialize in providing contingent workforce management, direct hire, AOR/EOR solutions, IC compliance, SOW solutions and global payroll services backed by our in-house technology platforms. As a certified Minority Business Enterprise, diversity is central to our culture, reflected in our leadership, our employee workforce, and our SHeTeam initiative.

Right Talent, Right Fit, and Impeccable Time to Fill

Contingent Workforce Management:
Manage your temporary and project-based workforce with precision no matter the size of your organization. From startups to enterprise-level businesses, we tailor our solutions to meet your unique requirements.

Direct Hiring:
We help you source and onboard the right talent across 150+ geographies with our High5 pre-vetted talent communities.

AOR/EOR Solutions:
Our experts aid you in avoiding international hiring risk by handling all HR-related tasks, including onboarding, paying, and administering benefits like advance pay.

IC Compliance:
eTeam's experts stay abreast of legislative updates to ensure your payroll is consistently in line with local regulations and global independent contractor laws.

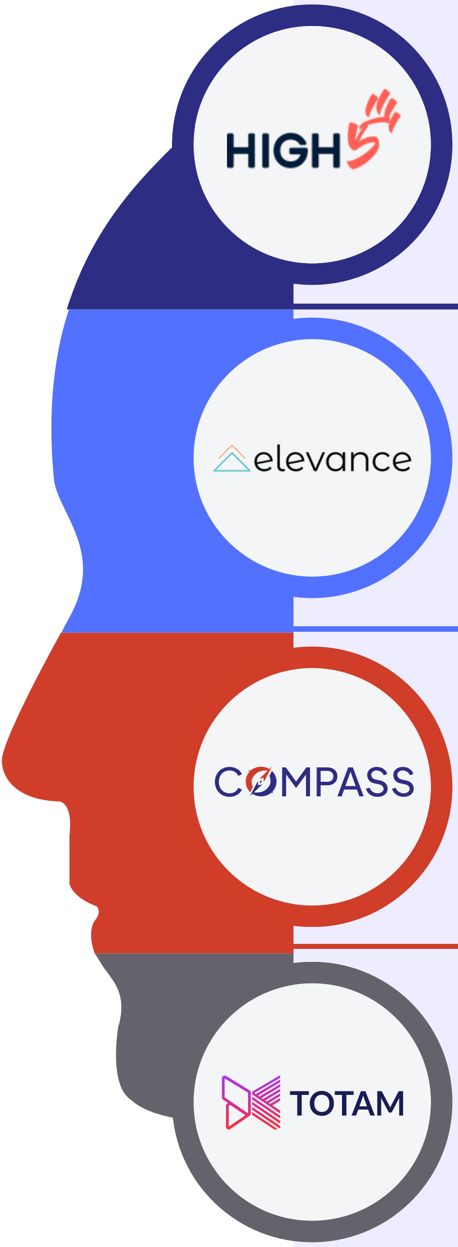
SOW Solutions:
We guide you to reallocate rogue spend into your non-employee workforce programs while improving deliverable-based SOW projects, mitigating risk, and driving savings.

Global Payroll Services:
Our payroll services cover a multitude of countries, accommodating diverse regulatory environments and efficiency in payroll processing across geographies.

eTeam xTend:
Empower you existing contingent workforce program to globally expand. Works with both internal programs and MSPs.

Embedded Recruitment:
Elements, eTeam’s strategic partner, provides embedded talent acquisition, a new breed of RPO for advanced recruiting and global expansion.

Our Suite of Innovative Technology Platforms



High5: An innovative digital talent platform that brings together people, processes, and technology to deliver dynamic staffing and talent solutions.

Elevance: An all-in-one independent contractor compliance platform that updates itself in real-time on current case law. Built on the decision-making patterns of judges and regulators.

Compass: eTeam's self-service global EOR platform for clients' on-demand needs around workforce management, reporting, and employee/contracting onboarding.

TOTAM: eTeam's strategic partner, a powerful VMS & FMS platform that provides a truly holistic view of all existing workforce employees without spending on software integration. Any type of talent, any type of engagement, anywhere in the world.

About our Workforce Intelligence Team (W.I.T.)

Workforce Industry Insights, Global Talent Trends, and Complete Analysis.

This report has been created by the Workforce Intelligence Team at eTeam Inc. Our expert workforce insights team uses a variety of first-hand research techniques, tools and proprietary data to help you understand more about the talent trends and opportunities within your target market and geographical regions.

Our projects span from conducting salary benchmarking for individual vacancies to performing multi-region competitor analysis and providing location-specific workforce strategies. We provide customized reporting on talent market trends to help you tackle global challenges with solution-oriented datapoints.

WIT

Workforce Intelligence Team

To find out more about how eTeam's Workforce Intelligence Team can support your talent acquisition strategy or to inquire about your own custom report, please reach out to **amaggio@eteamin.com.**