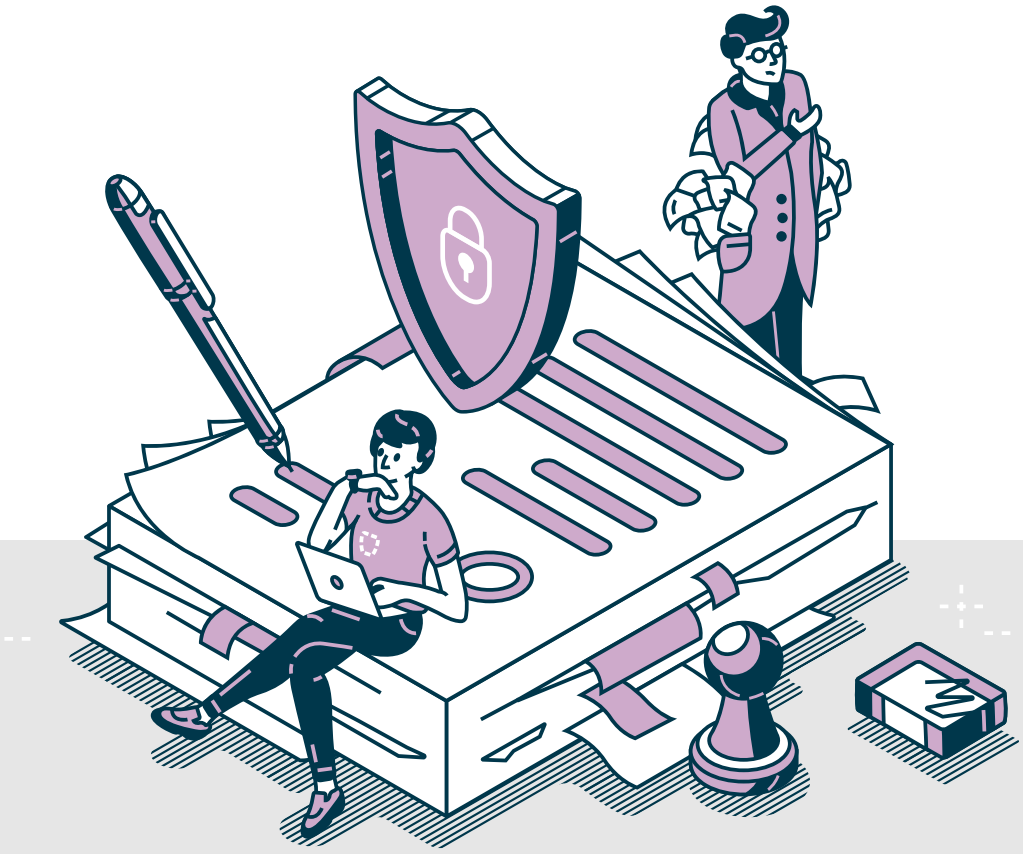
Four different strategies against **“SKILL SHORTAGE”**



In the realm of cybersecurity, an alarming predicament has emerged – a severe scarcity of skilled professionals. As technology races ahead, the demand for cyber defenders grows exponentially, yet the pool of qualified talent remains alarmingly shallow. This pressing challenge, stemming from a complex interplay of factors, casts a shadow over industries, governments, and individuals alike, underscoring the critical need for innovative solutions to bridge the widening gap between demand and availability in the cybersecurity workforce.

To address this challenge, a multi-faceted approach is crucial. Initiatives that foster interest in cybersecurity from an early age. In this race to secure our digital future, collaborative and forward-thinking measures are paramount. Only by fortifying our cyber defenses through concerted efforts can we mitigate the pressing shortage and ensure a safer digital landscape for all.

We examined the following four strategies aimed at addressing the issue of skill shortages and, ideally, building a robust talent pipeline:

1) The Employee Journey and Employer Branding
2) The Know Your Talents Approach
3) The Cross-Skilling Approach
4) Collaboration with Young Talent Programs

The Holistic Employee Journey: **A Cybersecurity Perspective**

In the dynamic world of cybersecurity, cultivating a skilled workforce is paramount. The employee journey, which includes the candidate experience, touchpoints during tenure, and the path of leavers, is crucial for visibility, retention, and shared accountability.

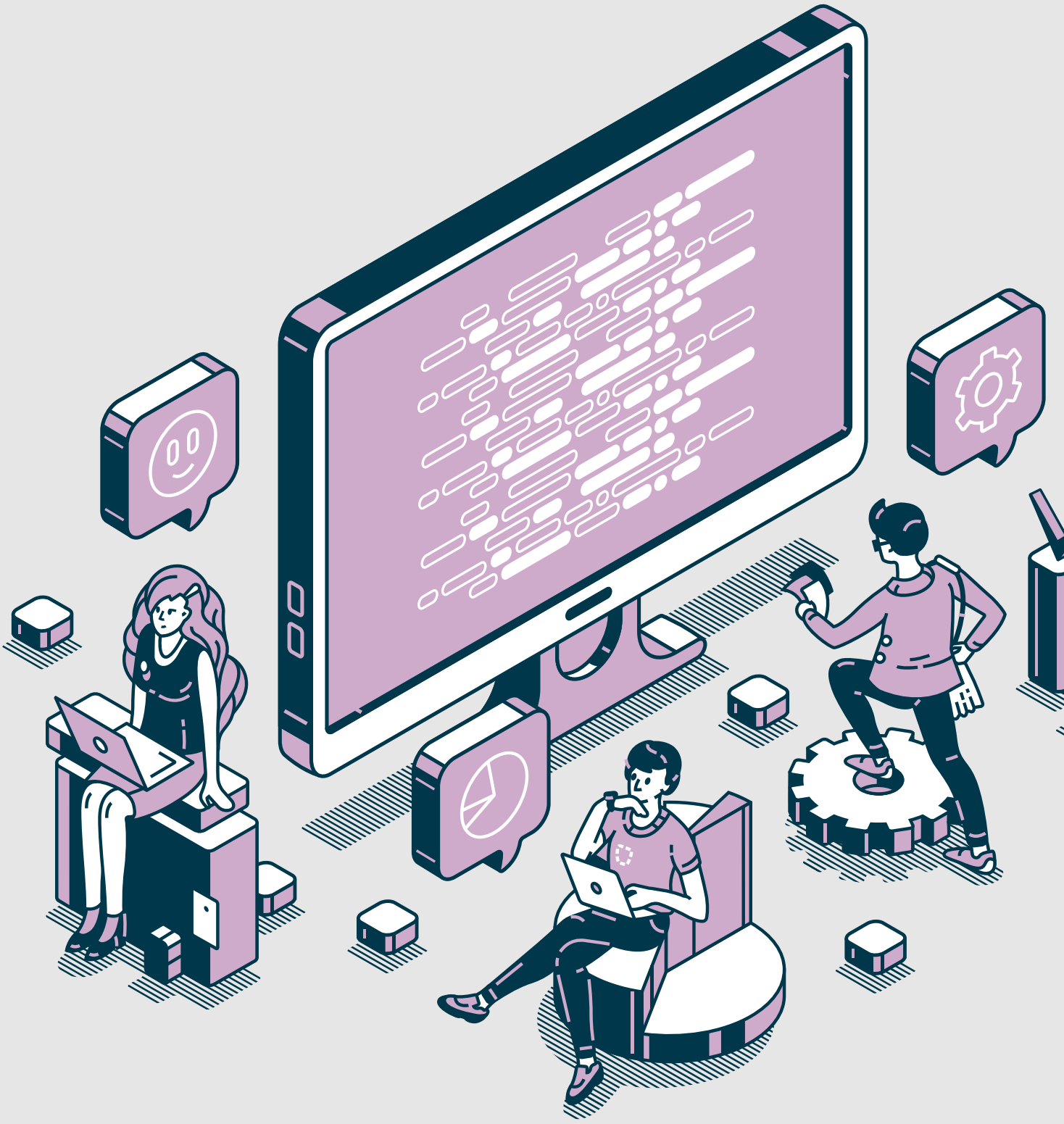
The candidate journey initiates a bond between the employee and the organization. Cybersecurity teams, with their dedication to protecting digital assets, highlight the company's commitment to a secure environment. By engaging with potential candidates, they amplify the employer brand, making it appealing to those seeking purposeful roles.

Once onboard, employees experience a series of touchpoints. Cybersecurity and HR leaders influence these moments. Regular interactions, mentorships, and ongoing training not only boost visibility but also address retention. Given the ever-changing nature of cybersecurity, continuous learning is essential. Leaders who prioritize this underscore the company's dedication to its employees' growth. By creating a nurturing atmosphere, they ensure the retention of top talent.

The journey also considers **departing employees**. Cybersecurity heads can foster goodwill by conducting insightful exit interviews. This comprehensive approach to exits emphasizes genuine care for the individual and enhances the employer brand. Departing employees who feel appreciated become brand champions, enhancing the company's reputation.

The synergy between cybersecurity teams, leaders, and HR is essential in shaping the employee journey. It's a collective effort to improve visibility and retention. Cybersecurity teams highlight the company's security commitment, while leaders promote growth. Recognizing their combined impact, the cybersecurity sector can craft a strong company narrative, attracting and retaining top talent.

In summary, the employee journey is a blend of visibility and retention. Cybersecurity teams and leaders craft a compelling narrative that appeals to those pursuing a significant career in cybersecurity.



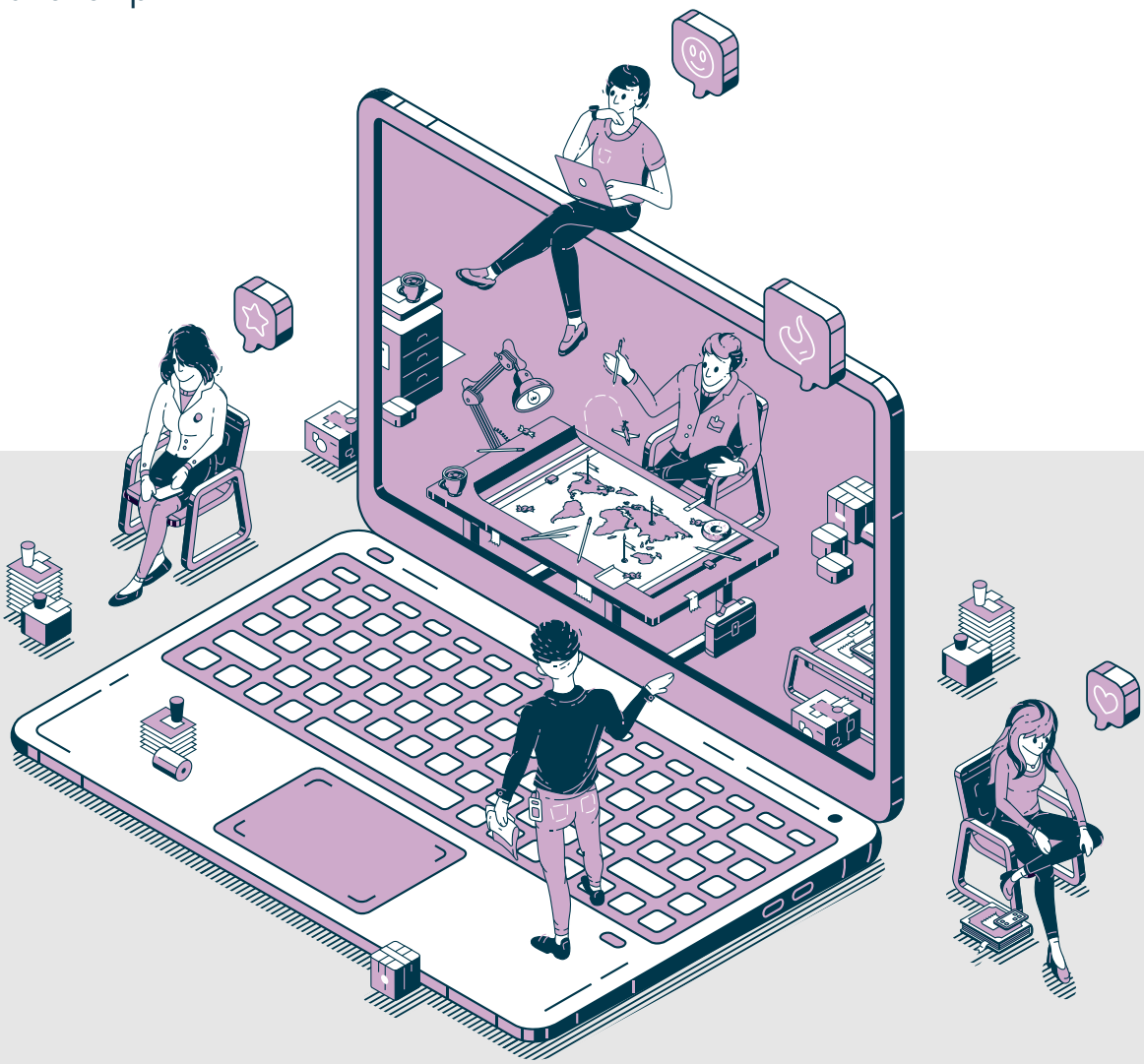
The “Know Your Talents” Approach:
Nurturing Cybersecurity Excellence

In the competitive landscape of talent acquisition, the “Know Your Talents” strategy stands out, emphasizing the importance of cultivating enduring relationships with potential candidates, both pre and post their entry into the job market. Recognizing the surging demand for cybersecurity experts, this approach transcends traditional recruitment, melding networking, adaptability, and proactive community engagement.

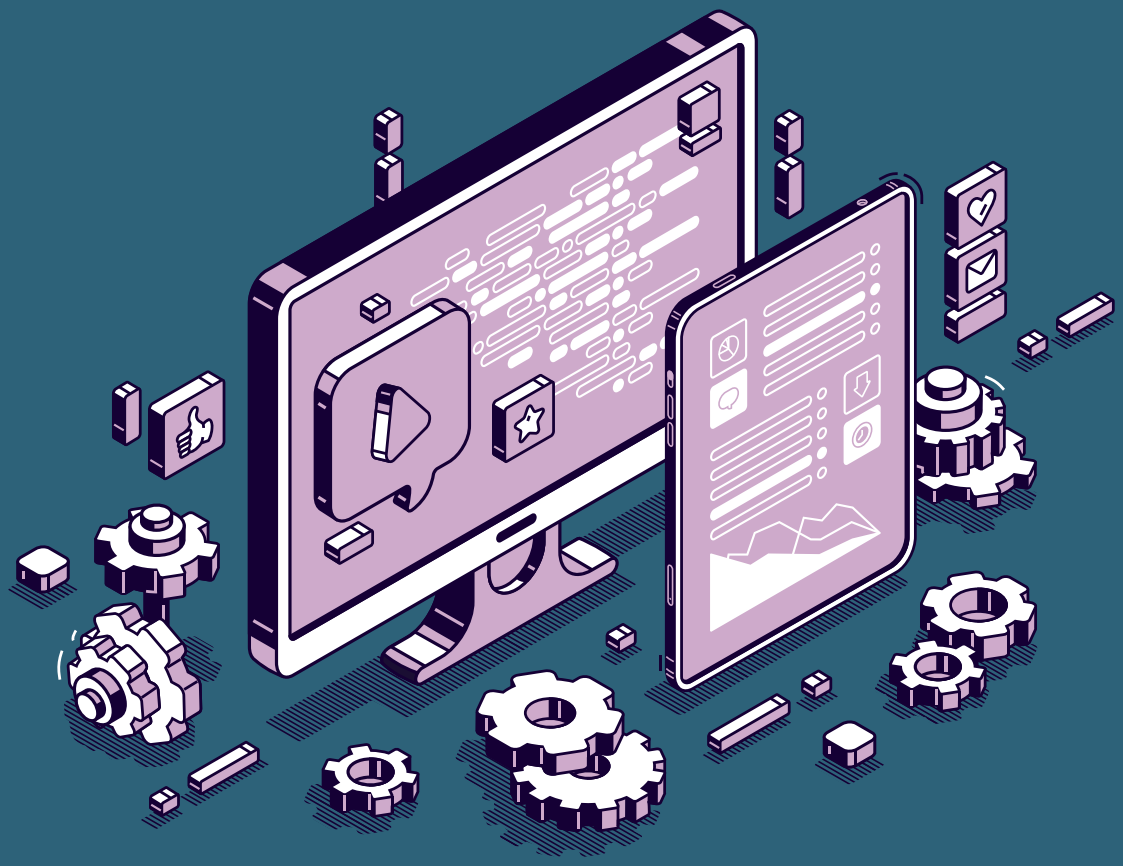
For companies to truly stand out to top-tier professionals, they must not solely rely on conventional hiring methods. The “Know Your Talents” philosophy champions a proactive and sustained engagement. It’s not just about filling vacancies; it’s about embedding oneself in the cybersecurity community, understanding its nuances, and identifying rising stars early on.

While partnering with talent agencies can enhance reach, it’s equally vital for executives and organizations to be active community participants. Feeling the community’s pulse, attending events, and fostering genuine connections can position a company as a preferred destination for the industry’s best.

Adopting the “Know Your Talents” approach demands more than a recruitment strategy shift; it calls for a cultural evolution. Organizations must be agile, fostering an environment that not only attracts but also nurtures and retains top talent, ensuring a symbiotic, long-term relationship.



Fostering Cybersecurity Talent through **Cross-Skill and Up-Skill Approaches**



In the rapidly evolving landscape of cybersecurity, the acquisition and retention of top talent necessitate a departure from conventional skill-centric paradigms. While specialized expertise remains crucial, the multifaceted demands of the field underscore the indispensability of cross-skilling and up-skilling initiatives. Cybersecurity professionals are not confined to siloed technical roles; rather, a diverse skill set that encompasses understanding business dynamics, database management, coding, network proficiency, and even insights into human behavior is imperative.

The conventional view of cybersecurity as a realm solely defined by technical prowess is evolving. Professionals are required to operate within an intricate web of business intricacies, technological intricacies, and the intricate psychology of potential threat actors. The efficacy of defense mechanisms relies on comprehensive knowledge of the organization's operations, which highlights the significance of cross-skilling. A cybersecurity expert well-versed in database management and network administration, for instance, can better comprehend and counter the nuanced tactics employed by cybercriminals.

Furthermore, the dynamic nature of cyber threats necessitates perpetual adaptation. Up-skilling, therefore, becomes an ongoing journey. Proficiency in programming languages not only bolsters an individual's technical acumen but also empowers them to develop innovative solutions that preempt emerging threats. Understanding human behavior and motivations can enhance the creation of robust social engineering countermeasures, bridging the gap between technological defenses and human vulnerabilities.

Collaboration with Young Talent Programs: **A Gateway to Cybersecurity Excellence**

In the quest for cybersecurity supremacy, pioneering organizations are not just seeking seasoned experts but are also turning their attention to young potential talents, especially those in their first apprenticeship. By partnering with youth talent programs, these organizations are revolutionizing the way future defenders of the digital realm are identified and nurtured. These initiatives, often embedded within school programs, act as crucibles for budding talents, guiding them through the challenges of youth, helping them forge their characters, and channeling their potential towards the complex world of cyber resilience.

What sets these programs apart is their holistic approach. Instead of traditional training models that focus solely on company-specific needs, these initiatives prioritize the overall growth of the individual. By identifying and cultivating talents at this early educational stage, they not only lay the groundwork for a diverse skill set but also help these young minds grow into the cybersecurity role. Participants are molded with a blend of technical skills, business understanding, ethical considerations, coding expertise, and the psychology behind cyber threats. The result? A new generation of professionals whose abilities go beyond the conventional boundaries of cybersecurity.

This partnership between organizations and youth talent programs is mutually beneficial. Companies gain fresh perspectives, innovative techniques, and a pool of potential that's eager to learn. In return, these young apprentices receive invaluable real-world experience, mentorship, and a fast-tracked path into cybersecurity. By assisting them in mastering the challenges of youth, organizations can bind these talents to their company, ensuring loyalty and dedication.

In the broader picture of digital defense, this collaboration with young talent programs is a game-changer. It's a strategy fueled by innovation, passion, and a vision for a cyber-resilient future. By investing in these young minds, organizations are not only bolstering their defenses but also building a legacy of expertise, ensuring the safety of the digital realm for the next generation.

Cyber Circle, located in Switzerland, is a project that connects CISOs (Chief Information Security Officers) with researchers. This collaborative community meets every two months for an evening of valuable discussions and activities centered around their roles. The focus is on providing insights, facilitating cross-industry learning, enabling external peer networking, and conducting practical workshops. The ultimate goal is to establish improved cybersecurity principles, including human-centered security, within companies.

Join Cyber Circle and become part of a friendly community shaping the future of cybersecurity!

Circle hosts:
Milena Thalmann, White Rabbit Communications
Stefan von Rohr, Peer Consult
Peter Kosel, cyberunity

Based on Cyber Circle Season 1, Zürich, January 2023