Elevating **people**.
Elevating **business**.
Elevating **society**.

Guardians of digital trust
Cybersecurity Awareness Month

Bridging the cybersecurity talent gap

Augmenting human efforts with AI

BDO
AUDIT • ADVISORY • TAX

Bridging the cybersecurity talent gap: *Augmenting human efforts with AI*

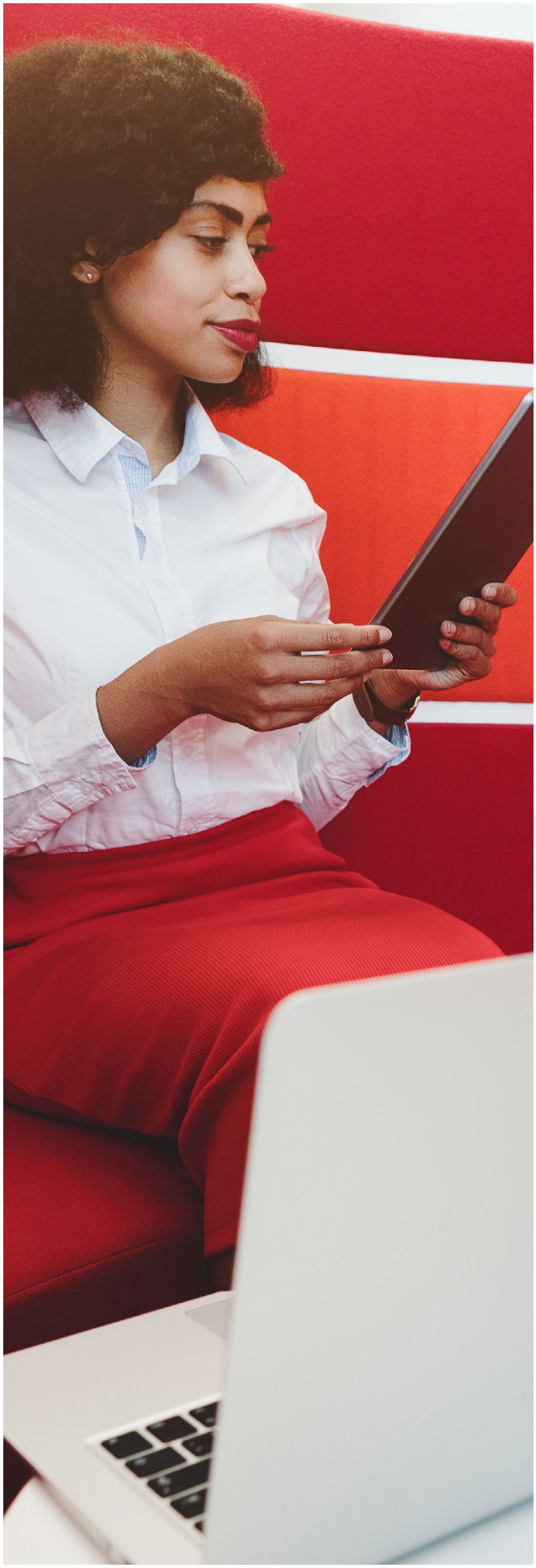
In an era where digital transformation is reshaping industries, we face a significant challenge: a growing divide between organisations which are on opposite ends of the cyber resiliency spectrum[1]. A significant contributor to this widening gap, is an increasing shortage of qualified cybersecurity professionals and as cyber threats continue to grow in volume, velocity and sophistication, organisations find it difficult to effectively secure their rapidly expanding digital footprint. The shortage in cyber talent, accelerated adoption of new technologies, and the ever-evolving threat landscape, poses a substantial risk to all organisations leveraging technology globally.

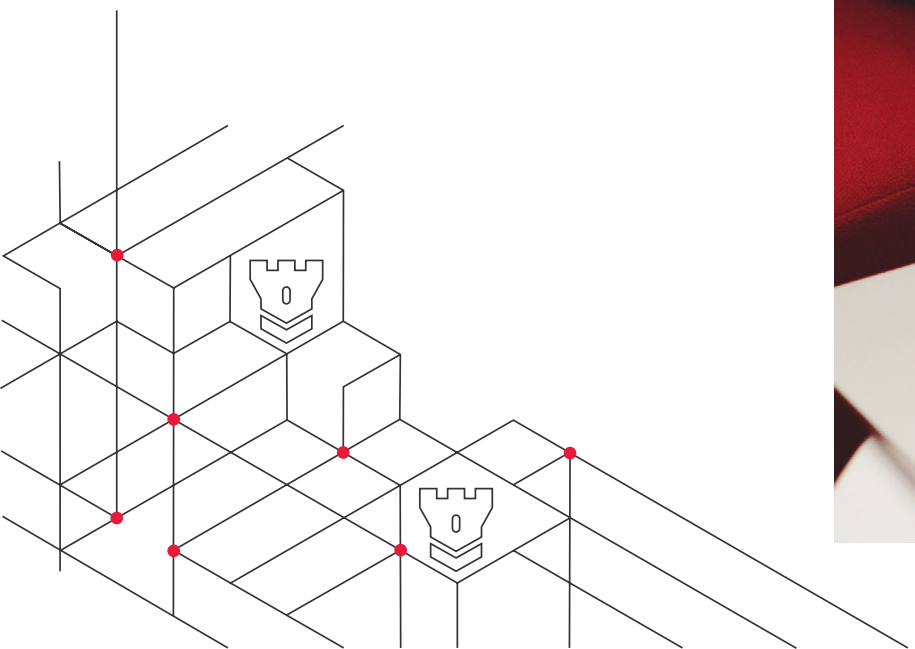
In September 2024, the International Information System Security Certification Consortium (ISC)², conducted a study which highlights the growing cybersecurity workforce gap. The study revealed a global shortfall of 4.8 million cyber professionals which are needed to secure organisations effectively. ISC² indicates the gap has grown significantly, estimating a 19% increase year over year.

[1] Discover our second article in the series: the growing divide between cyber resilient and non-cyber resilient organisations

> "The ISC² Cybersecurity Workforce Study highlights a concerning perception among cybersecurity professionals. After two years of declining investment in hiring and professional development opportunities, organisations are now facing significant skills and staffing shortages – an issue that professionals warn is heightening overall risk," said ISC2 Executive Vice President of Corporate Affairs Andy Woolnough.
>
> "At a time when global instability and emerging technologies like AI are rapidly increasing the threat landscape, investment in skills development and the next generation of the cyber workforce is more crucial than ever. This will enable cybersecurity professionals to meet these challenges and keep our critical assets secure."

The deficit in cyber talent is a result of a shortage of quality training and education, lack of investment into staff by organisations, budget challenges, and often difficulty in retaining skilled staff. Adding to the complexity is the challenging role of cybersecurity professionals, who often battle tight budgets which slow progress, high volumes of requests, and constant demands across the business. The outlook appears grim, and if not corrected will lead to long term consequences for businesses and organisations of all sizes. There are two areas where we must focus. The first and most obvious, is developing the talent we already have in our organisations, getting them the experience and capability they need to help us defend our assets. We need to focus on continuous skills development, as well as equally focus on retention of these individuals in the field. The second is leveraging the newer and more advanced technology capability to support these individuals with keeping pace with the increased volume, by focusing their attention on complex/high-value tasks while leveraging technology to address menial/low-value functions. As we struggle with the talent shortage, modern solutions like artificial intelligence (AI) and automation are emerging as key enablers to close this gap and protect our critical systems.





The scale of the cyber talent shortage

The current cybersecurity skills gap is a complex problem to solve as at its core, the issue is the pace of technological change. Industry 4.0 has provided us new ways of working, collaborating, and automation we never thought possible. With every evolution of the technology landscape, exponentially more new attack vectors emerge as attackers seek weaknesses in systems and employ sophisticated tactics to gain access to these ever changing and continuously sprawling technology estates. The constant evolution requires a cybersecurity workforce who are skilled in traditional foundational security principles, while are also able to remain nimble enough to adapt to new technologies and to modern methods of protecting those capabilities.

The speed of business and technological evolution makes it difficult for cyber professionals to keep pace, especially in this market where a shortage of talent is prevalent and attackers are multiple steps ahead. This is where the continued drive to educate, provide continuous learning for professionals in the field on modern methods, and a focus on recruiting talent with both academic and hands-on experience is key.

AI: *A force multiplier for cyber defence*

Advancements in technology is also fuelling opportunity for cyber defence teams. As an opportunity to combat this talent shortage, artificial intelligence and automation offer the opportunity for a more sustainable and efficient cybersecurity program. AI won't replace human expertise, but it can be leveraged as an effective capability to augment human efforts, enable humans to keep pace, and enable organisations to do more with fewer resources.

AI and machine learning with large language models analyse large quantities of data at a high rate of speed, with the ability to find patterns, and flag risks in near real time. This surfaces those highest risks to human resources so they can focus on more complex investigation activities. Traditional rule-based cybersecurity tools rely on static signatures, often binary logic, and almost always create noise and distractions for cybersecurity professionals. AI systems can learn from data, patterns, and these systems adapt to elevate those signals which are most relevant for humans to analyse. Whether used to identify new and unusual patterns of behaviour, mapping behaviours to known bad actor techniques, or identifying unknown behaviour which mimics behaviours most common with a cyber-attack, these technologies significantly enhance an organisation's ability to respond to emerging threats. Threats of this nature would otherwise go unnoticed by conventional systems, helping cybersecurity staff get to root cause faster and mitigate threats almost in an expedited manner, with fewer human resources.

The benefit of having AI handle repetitive, data-heavy tasks is an effective way to get more done with the same resources, but the most significant value is in how AI will augment and compliment human expertise. AI cannot replace the years of experience, institutional and contextual knowledge cybersecurity professionals provide. However, a collaboration between human intelligence and artificial intelligence will result in a far more resilient cyber defence strategy and a more resilient organisation.

Opportunities for efficiencies with AI

There are many areas in the Cyber capability stack where AI services can be leveraged to supplement the skills provided by human staff. Below are examples of AI services which can be considered:

Threat Detection

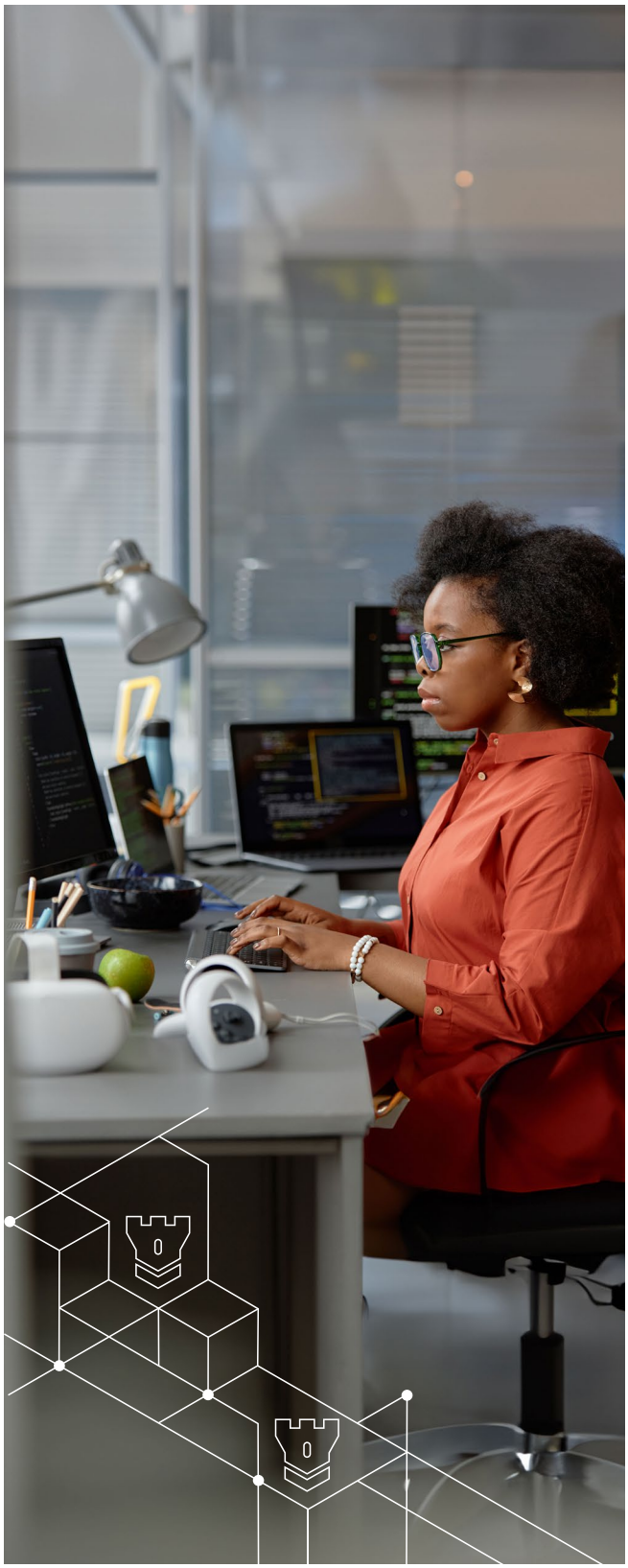
AI can monitor network activity with incredible efficiency and accuracy, using heuristics and machine learning to find advanced cyber threats and identify abnormal traffic patterns. These AI powered services can take on the "heavy lifting" from network analysis and forensics, allowing for near real-time threat detection and empowering security analysts with meaningful correlated data.

Vulnerability Management

VM platforms powered by AI can be leveraged to provide enriched data and reports, allowing for an accurate view of the organisation's security posture. These tools leverage capabilities to actually test the exploitability of vulnerabilities, allowing the organisation to prioritise remediation efforts based on actual risk, with compensating controls taken into consideration.

Incident Response

AI powered IR tools can handle the initial phases of incident response through the automatic identification and containment of identified threats. Leveraging a unified security ecosystem can allow an AI IR platform to leverage various control capabilities within the technology stack to thwart cyber-attacks. This reduces the time required to respond to threats and allows cybersecurity teams more bandwidth to focus on remediation activities.



Conclusion: *Closing the gap with collaboration*

The global cybersecurity talent shortage is a concerning challenge which threatens the sustainability of our digital ecosystems. Leveraging AI, automation, and modern education techniques, we will be successful at strengthening our cyber talent, as well as augmenting our existing workforce to enable organisations to scale their security efforts more efficiently.

While AI can help significantly by taking on routine tasks, human resources will always be needed to provide context, creativity, and strategic thinking. Together, this will bridge the divide.

Gilchrist Mushwana

Advisory Director: **Cyber Security**
GMushwana@bdo.co.za

Elevating **people.**
Elevating **business.**
Elevating **society.**

BDO
AUDIT • ADVISORY • TAX