

The quantum leap

Safwan Akram, Country Manager for KSA at Help AG, and Luca Collacciani, Head of EMEA and APAC at SandboxAQ, explore how quantum computing and large quantitative models are poised to disrupt the cybersecurity landscape in Saudi Arabia and the wider Middle East.

Let's start with this partnership between Help AG and SandboxAQ. How do you complement each other's strengths?

Safwan: When it comes to partnerships in the cybersecurity space, it's not about selling everything and anything. That's not how successful businesses scale. Yes, you can sell 100 transactional deals from 100 different vendors every year, but what you'll quickly realise is that to scale to a sizable market, you need focus.

And the reason you need focus with partners like SandboxAQ is that the client wants a trusted partner. At Help AG, we are that trusted partner for many strategic clients. Why? Because we have people who understand the technology, who can speak the language, and who can go into the technical details. We then bring in our vendor partners as trusted advisors who can dive even deeper and translate that technical insight into business value.

In our RFP and tendering processes, we follow a very rigorous system. We may bring in a vendor for a specific need today, but because of the trust, credibility, and technical proficiency we demonstrate, we know we can cross-sell and up-sell with them on second and third projects.

Ultimately, sustainability and scalability come from having strategic vendor partners and SandboxAQ is one of those partners for us.

Luca: So, SandboxAQ, as you know, is a Google spin-off headquartered in California. And whenever we look at a new market, we always evaluate the landscape and identify the most reliable partners in the region. With Help AG, we saw a company that has been in this business for a long time. They are a proven enterprise player, and they understand the local market exceptionally well: the regulations, the customer expectations, and the trust dynamics that matter here.

They have established strong, long-standing relationships with many customers in the region, and that complements our offering perfectly. We provide the SaaS solution, but they provide all the services, integration, and the wrapper around it. They bring trust, and more importantly, they have the skills and capability to support customers locally, and that's exactly what we need.

How would you assess Saudi Arabia's readiness in post-quantum cybersecurity?

Luca: So, as you know, I'm responsible for EMEA and Asia Pacific, and the Middle East is actually where we're seeing the strongest traction across both regions. I've been genuinely impressed by how forward-looking this part of the world is—especially the UAE and Saudi Arabia.

Just recently, for example, we saw new cybersecurity regulations being



Safwan Akram
Country Manager for KSA
Help AG

introduced in the UAE, and what stood out to me is how open the region is to innovation. Unlike many mature markets, countries here are not burdened by decades of technical debt. They are building infrastructure at extraordinary speed, which allows them to innovate faster and adopt advanced technologies with far fewer constraints.

This ability to move quickly means the region is not just keeping up with global trends—it's often looking further ahead and



shaping what the future will look like. From my perspective, that creates an incredible opportunity. I've rarely seen a region so committed to forward-thinking growth and technological advancement, and it's truly exciting to be part of that journey.

Saudi Arabia has been investing aggressively in AI, sovereign cloud, and other advanced technologies. Do you think the country can also become a global leader in post-quantum cybersecurity?

Safwan: Of course. The Kingdom is heavily focused on future-proofing its infrastructure, its data, and its national capabilities. Much of the investment we're seeing today is directed toward technologies that may not be everyday threats right now, post-quantum being a good example, but will become critical within the next three to five years. We know this shift is coming, and Saudi Arabia is positioning itself early to lead in this space.

The foundation is already being built. The country has invested significantly in the necessary infrastructure and is rapidly developing local talent to match that pace. From a regulatory perspective, we're seeing the government introduce mandates that support long-term resilience. Yes, there are challenges,

such as the global scarcity of cybersecurity and quantum-skilled professionals, but there is also significant momentum.

Across sectors, including academia, there is a strong push to close the talent gap. Universities are partnering closely with industry to accelerate skills development and create pathways for Saudi nationals to become leaders in post-quantum security, AI, and other forward-looking technologies. The strategy is clear: build the talent, build the infrastructure, and build the future now.

Luca, could you explain what LQM is and how it differs from traditional AI models?

As you know, SandboxAQ is a global leader in large quantitative models. And the reason for that is simple: we believe that large language models (LLMs) cannot scale in certain mission-critical domains.

LLMs fundamentally operate on probability, they are predicting the next likely word. Large quantitative models, on the other hand, are built on the laws of physics, chemistry, mathematics, and even biology. They have inherent guardrails because they model the real world, not just linguistic patterns.

This distinction matters enormously in cybersecurity. In security, you cannot afford a model that "guesses" and gets it wrong. A single

incorrect assumption can be disastrous. When you need to determine whether a specific cipher or certificate is breakable or whether it will be vulnerable by 2027; you need absolute certainty, not probabilistic guesswork.

And that's why quantitative models are so powerful in this space: they create mathematically verifiable predictions, not creative approximations. This level of precision is essential for protecting systems against emerging threats, including post-quantum risks.

What are some of the the steps enterprises, especially in Saudi Arabia, should take now to start preparing early for what's coming?

Safwan: What we're seeing today is that many organizations are going back to the basics: hardening their infrastructure and addressing the gaps they may have overlooked. It's no longer just compliance-driven; it's quality-driven. They are revisiting zero trust architectures, reassessing their overall security design, and ensuring proper defense-in-depth strategies are in place.

This foundation will be essential as they begin thinking about AI security, and all the emerging risks associated with LLMs, risks that technologies like LQM are now helping to mitigate.