Press Release

The Invisible War: Brazilian Expert Thiago Manzaro Serain Warns That the Global Shortage of Cybersecurity Professionals is Putting Economies at Risk

In this global shortage, a small group of professionals stands out for mastering highly specialized and technically demanding domains. Among them is Thiago Manzaro Serain, a Brazilian cybersecurity professional with advanced certification in SAP Security, a technology that underpins critical operations for governments, banks, industries, and multinational corporations.

Austin, TX, May 19, 2026 --(PR.com)-- The global digital economy is facing a dangerous paradox: cyberattacks have never been more frequent or more sophisticated, yet the number of professionals capable of defending against them has never been so small. The 2024 ISC2 Cybersecurity Workforce Study estimates that the world needs an additional 4.8 million cybersecurity specialists just to meet baseline protection requirements for governments, corporations, and critical infrastructure. The gap is now so severe that it threatens economic stability and national security across advanced economies, including the United States.

The shortage is unfolding precisely as the attack surface expands. Artificial intelligence has supercharged the offensive capabilities of criminal groups and hostile states, enabling automated, scalable, and increasingly untraceable attacks.

A perfect storm

Mass layoffs across the tech sector, particularly among network engineers, system administrators, and software developers, have pushed thousands of experienced professionals back into the job market. Many are now looking to cybersecurity as a more stable career path. But most lack hands on defensive experience, and organizations cannot afford to place high risk security roles in the hands of beginners.

The result is a labor market where degrees matter but are insufficient, certifications help but only when paired with real world experience, and experience itself has become the ultimate, and increasingly rare, differentiator.

The threat is growing faster than the defense

The escalation of the global cyber war has made the shortage even more alarming. Recent high impact attacks illustrate the destructive potential of this new battleground:

• Colonial Pipeline (U.S., 2021): a ransomware attack halted the nation’s largest fuel pipeline, triggering shortages and market disruption.
• Costa Rica (2022): the government declared a national emergency after attacks crippled ministries, tax systems, and essential services.
• MGM Resorts (U.S., 2023): hotel and casino operations were paralyzed, resulting in billions in losses and exposing vulnerabilities in the hospitality sector.
• Microsoft breach by Russia linked group (U.S., 2024): hackers accessed emails belonging to

executives and security teams, exposing strategic data and raising global concerns about digital espionage.
• ICBC – Industrial and Commercial Bank of China (U.S., 2023): the world's largest bank suffered a ransomware attack that disrupted U.S. Treasury market operations.
• HCA Healthcare (U.S., 2023): data from 11 million patients was leaked, causing nationwide disruptions to essential medical services.
• Critical infrastructure in Europe (2024–2025): coordinated attacks targeted power grids, transportation networks, and public services, underscoring systemic vulnerabilities.

Across all these incidents, one conclusion is unavoidable: there are not enough skilled professionals to identify vulnerabilities, respond to incidents, and protect complex systems.

Artificial intelligence has widened the gap even further. According to ISC2, 23% of cybersecurity teams report critical skill shortages in AI driven defense, alongside deficits in cloud security (30%), zero trust (27%), incident response (25%), and application security (24%).

The Brazilian specialist operating where few can
Amid this global shortage, a small group of professionals stands out for mastering highly specialized, technically demanding domains. Among them is Thiago Manzaro Serain, one of the few Brazilians with advanced certification in SAP Security, a technology that underpins critical operations for governments, banks, industries, and multinational corporations.

With more than 20 years of experience at global firms such as LafargeHolcim, EY, and IBM, Serain spent 16 years dedicated exclusively to Governance, Risk and Compliance (GRC) and SAP security. His work includes implementing SAP GRC Access Control and Virsa Firefighter/EAM, developing access profiles for operations across eight countries, and leading teams through critical incidents involving systems like S/4HANA, ECC, BW, CRM, and SRM. He has also overseen Big Four audits and produced strategic controls and executive level reports.

One of the most decisive moments of his career occurred during the merger of a multinational corporation, when an access management failure caused authorization issues and affected several countries. Serain led the complete restructuring of the access landscape, implemented controls and mitigations through SAP GRC, and restored the organization of access and

authorizations, preventing a violation that could have triggered significant process and compliance problems across the entire cluster.

Exclusive interview

For Serain, the digital war is already underway, and on this issue, he is unequivocal:

“The digital war happens in silence. When there aren’t enough professionals, vulnerabilities multiply, and each one can compromise a company, a government, or an entire country.”

He warns that the lack of early career professionals is one of the most dangerous trends. The ISC2 study shows that 31% of cybersecurity teams have no entry level staff, and 15% have no junior professionals at all. The base of the talent pyramid is collapsing, and there is no pipeline to replace it.

On artificial intelligence, he is blunt:

“AI allows criminals to automate global attacks. Meanwhile, training a specialist takes years. The balance is completely off.”

Serain argues that the solution requires a more practical, structured approach to talent development: home labs, bug bounty participation, open source contributions, and more entry level opportunities. He also emphasizes the need for public sector investment in critical skills.

“Cybersecurity is not a cost. It’s infrastructure. Without it, no country is safe.”

The future of the digital battlefield

Cybersecurity is no longer a technical niche; it is a geopolitical pillar. Nations that fail to invest in talent risk seeing their digital infrastructure compromised by invisible adversaries.

As Serain puts it, “In a world where the next war can begin with a single click, the future of national defense lies in specialists who can master complex systems, anticipate global risks, and act before the attack even begins.”

Contact

Karlla Marinho PR & News Agency
Karlla Marinho
407-973-8699
https://univrus.com/
✉ Contact

Online Version of Press Release

https://www.pr.com/press-release/968956