Executive Intelligence for Africa

CXO TRAIL INSIGHT

ISSUE 01 | SEPTEMBER 2025

INSIDE GITEX
Nigeria

THE CISOs
Playbook

NAIROBI
Cybersecurity Forum

+

Dapo Salami
CEO - PLATVIEW

THE CURRENCY OF TRUST

Dapo Salami on why digital trust will define Africa’s economy

UNDER THE PATRONAGE OF **HIS EXCELLENCY PRESIDENT BOLA AHMED TINUBU, GCFR**

GITEX Nigeria x Ai EVERYTHING —NIGERIA—

1 - 4 SEP 2025
ABUJA | LAGOS

FORGING THE RISE OF DIGITAL NIGERIA

GITEX NIGERIA Tech Expo & Future Economy Conference
Wed - Thurs | 3-4 Sept
Eko Hotel | LAGOS

GITEX NIGERIA Startup Festival
Wed - Thurs | 3-4 Sept
Landmark Centre | LAGOS

SUPPORTING PARTNER: FEDERAL MINISTRY OF COMMUNICATIONS, INNOVATION & DIGITAL ECONOMY

STRATEGIC PARTNER: NITDA

ENDORSED BY: LAGOS STATE GOVERNMENT

ORGANISED BY: كون KAOUN INTERNATIONAL

BE THERE! REGISTER NOW

gitexnigeria.ng #gitexnigeria

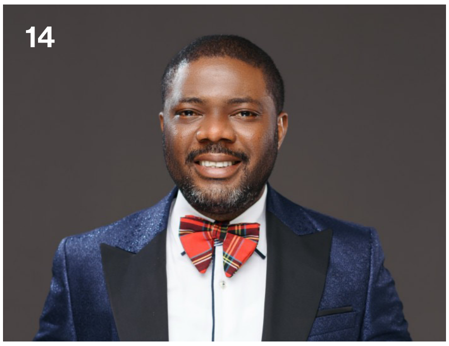
Table of contents

HIGHLIGHTS

CISOs INTERVIEW

EXCLUSIVE ARTICLES

STATISTICS



Africa's Ground breaking Initiative

Editor's note

The recent launch of AfricAI, a new joint venture dedicated to building sovereign, inclusive AI solutions for the continent, is more than just a headline; it is a powerful statement of intent. It signals that Africa is no longer just a market for technology; we are now architects and creators of our own.

This groundbreaking initiative perfectly encapsulates the dual focus of this magazine, celebrating the transformative power of AI while championing the urgent need for a robust cybersecurity posture. The recent high level cybersecurity forum in Nairobi served as a unified and urgent call to strengthen Africa's digital defenses, echoing a sentiment that cybersecurity is not a siloed issue but a shared responsibility that requires cross industry collaboration.

As we build AI for our local challenges, from healthcare to financial inclusion, we must simultaneously embed a security first mindset to ensure our digital revolution is both powerful and protected. This is the very essence of what events like GITEX Nigeria represent. As a new platform for collaboration between global tech giants and local innovators, GITEX Nigeria is a vital space for advancing this conversation. It is where we will address the critical issues of digital trust, identity security, data governance, and overall digital resilience the foundational pillars for a new economy built by us, for us.

I hope to see an increased focus on developing AI powered security solutions tailored to the specific challenges faced by African organizations, collaboration between African and international cybersecurity experts, and a commitment from African governments to invest in cybersecurity education and training.

Anabel Emekena
Editor

Publisher :
SHAHPER MEDIA

SHAHPER MEDIA LIMITED
32 Ripley Road, Berkshire, Reading
United Kingdom

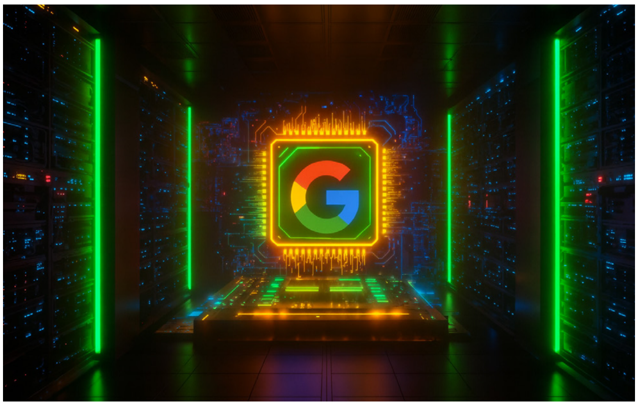
Editorial: editorial@cxotrail.com
Business & Media Relations:
hello@shahpermedia.com

Registered in England & Wales,
Company Reg. N. 15538366

Google Launches AI Mode in Search across Africa

Google has announced the launch of its new AI Mode in Search for users in Nigeria, Kenya, and South Africa, marking a significant step in the evolution of how we find and consume information online.

AI Mode is designed to tackle the kind of complex, multi-part questions that traditional search engines struggle with. Instead of having to break down a query into multiple keywords and sift through countless links, users can now ask nuanced, exploratory questions and receive a comprehensive, AI-powered response. Powered by a custom version of Google's latest Gemini 2.5 model, this feature uses advanced reasoning to break a single query into subtopics, simultaneously searching a multitude of queries on your behalf. The result is a richer, more detailed answer that is far more helpful.



A key highlight of this new mode is its multimodal capability. Whether you prefer to ask a question with your voice, type it out, or even upload a photo, AI Mode is designed to understand.

Google's commitment to the open web remains a core principle of this launch. The AI-powered responses are not meant to be a final destination but a starting point. They include prominent links to web sources, ensuring users can easily click through to discover more content and support the creators of the information. Data from similar features shows that these AI-powered results actually lead users to visit a greater diversity of websites and spend more time engaging with them.

With AI Mode, Google continues to expand the role of artificial intelligence in everyday information access, combining advanced reasoning capabilities with multimodal inputs to enhance user engagement and exploration across the web.

Japan Pledges $5.5B and 30,000 AI Experts for Africa at TICAD 9

At the Ninth Tokyo International Conference on African Development (TICAD 9), Japan's Prime Minister Shigeru Ishiba unveiled a new vision of partnership that moves beyond traditional aid, blending economic collaboration, technological transfer, and a push for global governance reform.

Tokyo has pledged $5.5 billion in loans, to be channeled through the African Development Bank, to support sustainable development and, crucially, help tackle Africa's debt. This the kind of affordable capital that African nations need to invest in infrastructure and technological advancement.

The commitment to train 30,000 AI experts across Africa over the next three years is a plan that directly addresses the digital skills gap and positions Japan as a key partner in empowering a new generation of African innovators. By investing in human capital, Japan is helping to build a resilient, future-proof workforce that can drive sustainable growth from within.

TICAD 9 represents a pivotal moment in Africa-Japan relations. It signals a move toward a more strategic, co-creative partnership that addresses not just the economic and technological needs of the continent, but also its rightful demand for a stronger voice on the global stage.

"Africa must have a stronger voice in shaping the decisions that affect its future. That includes long overdue reform of the Security Council, where, incredibly, Africa has no permanent member"

A Landmark Venture to Build Sovereign AI for Africa

In a significant move poised to reshape the global tech landscape, four international companies have joined forces to launch AfricAI, a new joint venture dedicated to developing and deploying enterprise-grade artificial intelligence solutions specifically for African markets. This initiative, formalized through a memorandum of understanding, marks a strategic pivot from Africa as a consumer of AI to a sovereign producer.

The founding partners are, Lakeba Group (Australia), Next Digital (Nigeria), AqlanX (UAE), and Agentic Dynamic (Netherlands), have committed to building AI that is not only secure and scalable but also deeply rooted in African realities.

The founding partners said in a joint statement. that AfricAI is not about outsourcing AI to Africa, it's about building it here, with full control over data, deployment and decision-making.

A Nigeria-First Approach with a Continental Vision

AfricAI will initially focus on Nigeria, leveraging existing national data centers and edge infrastructure to deliver impactful AI applications. The venture's first projects will prioritize sovereign AI use cases that directly address local needs, including:

Multilingual Citizen Services: AI assistants trained in local languages like Yoruba, Hausa, Igbo, and Pidgin to improve access to public services

Secure Digital Identity: AI-powered solutions for secure and seamless digital identity verification.

Document Automation: AI tools for enterprise services and public administration to automate document processing and management.

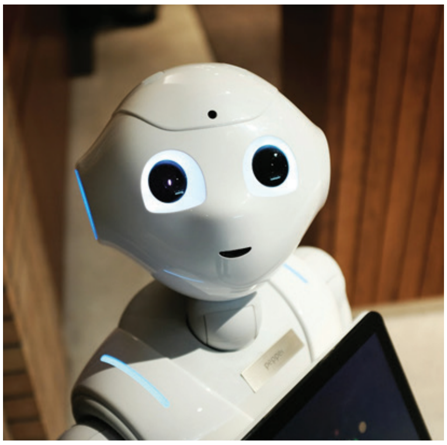
Agentic Assistants: AI applications for HR, education, and policy planning that can automate complex workflows.

AfricAI has a clear long-term vision. The consortium will establish a Center of Excellence to train over 100 African AI professionals by 2026, fostering a new generation of local talent. This will lay the groundwork for future expansion into Ghana, Kenya, South Africa, and Rwanda.

Industry Leaders on the Strategic Shift

The launch has garnered strong support from its leaders, who see this as a pivotal moment for African digital independence.

Prince Malik Ado-Ibrahim, Chairman of Next Digital, emphasized the venture's role in accelerating Africa's digital sovereignty. "With AfricAI, Nigeria is setting the pace," he said. "This is about more than software; it's about exporting our intelligence, building our future on our terms, and making Africa a force in the global AI conversation."



Giuseppe Porcelli, CEO of Lakeba Group, highlighted the strategic importance of building AI infrastructure locally. "This is about building the AI infrastructure Africa deserves secure, scalable and sovereign," he noted, praising Nigeria as the "ideal launchpad" for building a truly African AI ecosystem.

AfricAI aims to position the continent as a strategic hub in the global AI landscape, ensuring that AI innovation is inclusive, ethical, and reflects the unique linguistic and cultural diversity of its people.

GITEX Nigeria

Leading Tech Brands Drive Future Digital Economy to Support Nigeria's US$1 Trillion 2030 Vision

Global tech leaders including IBM, Meta, and MTN join GITEX NIGERIA 2025, driving tech opportunities that contribute to President Bola Ahmed Tinubu's Renewed Hope Agenda across talent development & digital infrastructure

Nigeria has risen to the forefront of Africa's digital economy with a powerful ecosystem that is both homegrown and resilient – fuelled by government initiatives, global tech enterprises, and a thriving startup ecosystem; propelling Nigeria's future with tech opportunities in talent development and digital infrastructure to help achieve the goal of US$1 trillion economy by 2030.

Held under the patronage of His Excellency President Bola Ahmed Tinubu GCFR, GITEX NIGERIA premieres across Abuja and Lagos from 1-4 September 2025. It is supported by the Federal Ministry of Communications, Innovation and Digital Economy in collaboration with the National Information Technology Development Agency (NITDA). The event is endorsed by Lagos State Government, and organised by KAOUN International, the global organiser of GITEX events.,

With a burgeoning big tech landscape, international names have flocked to Nigeria and other African markets to nurture talent, support with infrastructure or provide localised solutions for existing services. Whether driven by African diaspora or the promise of opportunity, international presence is expanding, often in the form of multi-sector, public-private partnerships.

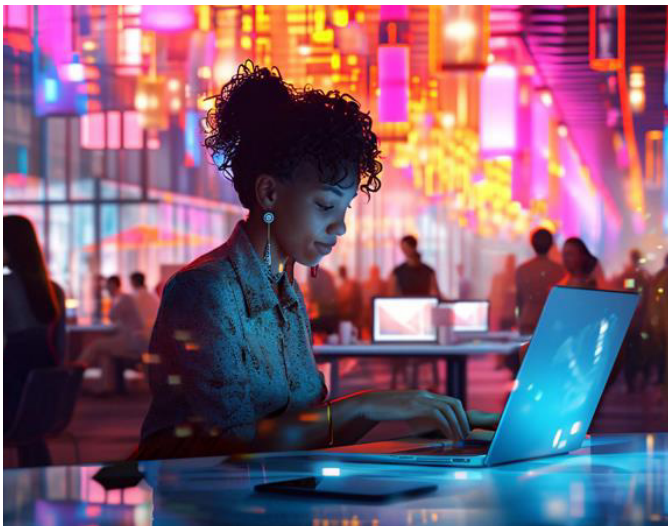
As IBM operated by MIBB affirms its presence in West Africa, it continues to build on IBM's long-standing legacy of enabling Nigeria's digital transformation. Through local engagement and ecosystem-driven growth, the focus remains on delivering impactful solutions across key sectors such as banking, telecoms, government, and education.

To capitalise on the transformative impact of GITEX NIGERIA on Lagos' startup ecosystem, the United Nations Development Programme (UNDP) will present its pan-African timbuktoo initiative at the event. The largest of its kind in the world, timbuktoo brings public and private capital together at a global scale to support and empower startups solving macro challenges facing the planet, and humanity. The event runs with support from partners AWS, Cisco, the International Finance Corporation (IFC), Kaspersky, Federal Ministry of Art, Culture, Tourism and the Creative Economy, Federal Ministry of Youth Development and Space42.

Vishnu Taimni, General Manager of IBM operated by MIBB said: "Nigeria is a strategic priority for IBM operated by MIBB, anchored in decades of trusted partnerships across public and private sectors. As the country accelerates its digital agenda, GITEX NIGERIA offers a valuable opportunity to deepen collaboration and reaffirm our commitment to co-creating technologies that empower industries and communities for the future."

H.E. Babajide Sanwo-Olu, Governor of Lagos State Federal Republic of Nigeria, said: "Lagos is and continues to be a city that facilitates progress. As we collectively build our city into the preferred destination for innovation and digital solutions, GITEX NIGERIA's shared ambition will place Lagos at the heart of Africa's digital future

The GITEX NIGERIA programme then transitions to Lagos, headlining across two locations from 3-4 September. The Eko Hotel Convention Centre hosts the GITEX NIGERIA Tech Expo & Future Economy Conference, while the Landmark Centre welcomes the GITEX NIGERIA Startup Festival. Combined, it will be West Africa's largest gathering of technology visionaries, industry leaders, and decision-makers overseeing digital transformation of non-tech sectors.



> "GITEX NIGERIA is more than an event, it is the cornerstone for Africa's digital renaissance and a catalyst for developing world class AI infrastructure"

Dapo Salami

CEO - PLATVIEW

Dapo Salami on Driving Cybersecurity and Digital Resilience Trust in Africa

COVER STORY

> "At the end of the day, Africa does not just need cybersecurity, it needs cyber resilience built for its context."

QI: Can you share details about Platview Technologies' journey and how your participation in industry events like GITEX Nigeria has influenced your company's strategy?

Platview Technologies was founded to help businesses across Africa strengthen their cybersecurity posture in an increasingly digital world. Over the years, we have built strong alliances with global leaders like Thales and Imperva, becoming a Platinum Partner which further consolidates our strategy in ensuring digital trust across the continent.

This year, we also launched Fraudspect, an AI-powered fraud detection platform designed to protect businesses in real time. These milestones have positioned Platview Technologies as a trusted cybersecurity innovator, enabling African businesses to grow with confidence. Looking ahead, our focus remains on driving innovation, securing Africa's digital transformation, and providing solutions that empower businesses to thrive in a connected world.

Participating in GITEX Nigeria is an unmissable opportunity for us as a leading cybersecurity company committed to protecting Africa's digital future. As the premier hub for innovation,

GITEX Nigeria brings together visionary leaders, tech disruptors, and industry experts shaping the next wave of digital transformation across the continent. This provides the platform to showcase our advanced security offerings and reinforce our role in building a safer, smarter digital Africa.

> "That was when it became clear that cybersecurity isn't just a wishful necessity; it's the foundation of digital trust and business continuity."

Q2: Your company's mission is to safeguard businesses and build consumer trust. From a leadership perspective, how do you define and measure "digital trust" for your clients, and how do you ensure your solutions genuinely contribute to it?

At Platview Technologies, we define digital trust as the confidence businesses and consumers have that their data, transactions, and digital interactions remain secure, private, and reliable. It is not just about deploying cybersecurity tools, it is about enabling businesses to operate fearlessly in the digital economy.

From a leadership perspective, digital trust has three pillars for us:

- **Security** - Ensuring systems are resilient against cyber threats and fraud.
- **Transparency** - Giving clients visibility into risks, compliance, and how their data is being protected.
- **Reliability** - Ensuring that our solutions perform consistently, so business operations and customer experiences are never compromised.

We measure digital trust by looking at outcomes, not just implementations. For example:

- Reduction in fraud attempts and successful breaches for our clients.
- Faster compliance audits and regulatory clearances due to stronger data protection.
- Improved customer retention and adoption rates when consumers feel safe transacting digitally.

To ensure our solutions truly contribute, we follow two key approaches:

- **Continuous Innovation** - Our AI-powered platform, Fraudspect provides real-time fraud detection and adaptive defenses, and our new digital risk/cyber threat intelligence solution, ReconX which focuses on safeguarding businesses online with real-time actionable intelligence.
- Partnerships with Global Leaders - Such as Thales and Imperva enabling us to integrate world-class security frameworks tailored to Africa's digital growth.

Ultimately, digital trust is measured when our clients' customers can confidently click 'Pay Now', 'Transfer Fund', share sensitive information, or engage online without hesitation. That confidence is the real currency of the digital economy, and our mission is to safeguard it.

Q3: Thinking strategically about the services you offer, which industries do you primarily serve, and what market gap did you identify that led to your unique value-added solutions?

Our services primarily serve highly regulated and transaction-heavy industries such as financial services, telecommunications, government, and critical infrastructures. These are sectors where trust, compliance, and resilience are absolutely non-negotiable.

The market gap we identified was twofold:

Fragmented Security Solutions - Many organizations had point tools that didn't integrate well, leaving blind spots in fraud detection, compliance, and data protection.

Africa-Specific Challenges – Most global solutions often were not tailored to the unique cyber risks, fraud patterns, regulatory requirements, and digital adoption realities across the African markets. The same applies to the duo of Digital Risk Protection and Cyber Threat Intelligence. With nascent infrastructure across Africa, there is a need for an agile approach to effectively address these challenges.

Our value-add lies in bridging this gap by delivering integrated, all-in-one platforms like Fraudspect for real-time fraud detection, leveraging identity verification as key value proposition, ReconX for digital risk protection, while also leveraging platinum partnerships with Thales and Imperva to offer enterprise-grade data protection tailored for local needs.

▶ Building Trust, Driving Innovation:

In essence, we do not just build or integrate cybersecurity products, we provide end-to-end digital trust solutions that empower organizations to innovate confidently and scale securely in Africa's fast-growing digital economy.

Q4: The African market presents unique challenges and opportunities in cybersecurity. What specific regional risks or trends do you believe require the most attention, and how is Platview Technologies uniquely positioned to address them?

Africa's digital economy is growing rapidly, but with this growth comes a unique set of cybersecurity risks that demand focused attention. The top three we have identified are:

- Rapid digital adoption without matching security maturity - As mobile

We launched Fraudspect & ReconX

▶ Our AI-powered platform, Fraudspect provides real-time fraud detection and adaptive defenses.

▶ New digital risk/cyber threat intelligence solution, ReconX which focuses on safeguarding businesses online with real-time actionable intelligence.

banking, fintech, and e-commerce scale, attackers exploit weak identity verification, insufficient data protection and fraud controls.

- Regulatory and compliance gaps - Uneven cybersecurity regulations across Africa's markets make it difficult for organizations to consistently meet global, regional, or national standards. Yet, they are still targets for cross-border threats.

- Rise of sophisticated fraud and social engineering - From AI-generated attacks to insider threats, cybercriminals are tailoring attacks to Africa's unique financial and telecom ecosystems.

Platview Technologies is uniquely positioned to address these challenges through:

- AI-driven solutions like Fraudspect which provide real-time fraud detection and adaptive identity verification that align with local transaction patterns.

- Leadership in Enterprise Data Protection service, giving businesses access to enterprise-grade data protection, encryption, tokenization and application security previously out of reach.

- Localized expertise by understanding Africa's regulatory landscape and designing solutions that can help clients achieve compliance while still enabling innovation.

At the end of the day, Africa does not just need cybersecurity, it needs cyber resilience built for its context. That is the gap we are filling.

Q5: You've been a prominent figure in the cybersecurity and digital solutions space. Can you walk us through a pivotal moment in your career that fundamentally shaped your perspective on the industry?

The business of digital trust comes with a daily inherent challenge that require unique problem-solving skills. One pivotal moment for me was witnessing how a client's data breach didn't just expose vulnerabilities, it completely eroded customer confidence and stalled their growth. That was when it became clear that cybersecurity isn't just a wishful necessity; it's the foundation of digital trust and business continuity.

That moment fundamentally shaped our vision at Platview Technologies. It drove us to build and provide solutions that do not just block threats, but also empower organizations to innovate confidently comply seamlessly, and scale securely. Every product we have launched, from Fraudspect, to ReconX, to our Enterprise Data Security Service is tied back to that mission: helping Africa's businesses grow by making trust their strongest competitive advantage."

Q6: You recently launched "Fraudspect," a fraud prevention system that leverages AI and machine learning. How do you ensure that your product roadmap stays ahead of the rapidly evolving threats faced by businesses, especially in the financial sector?

Fraudspect was designed with the understanding that fraud patterns evolve faster than traditional systems can adapt. To stay ahead, our product roadmap is built around three core principles:

Adaptive Intelligence - Fraudspect continuously learns from new fraud patterns. It evolves in real time rather than relying solely on static rules. Considering the new wave of fraud proliferation, synthetic identity fraud is on the rise, and we are helping organizations nib this in the bud with the identity verification which is a pillar of value in the Fraudspect service offering.

- **Collaborative Intelligence** – Through our newly launched ReconX platform, we can aggregate and capture regional cyber risk trends unique to African markets, ensuring the platform reflects real-world threats. Contextualization is a new paradigm in fraud prevention. With Fraudspect and the embedded layer of intelligence from smart signals, we can detect the specific identity (human, service account, agentic AI, etc) behind every transaction.

- **Continuous Innovation** - Our roadmap is not fixed; it's iterative. We run quarterly product reviews, integrate client feedback, and benchmark against global threat intelligence to anticipate emerging attack vectors.

In the financial sector where trust is

everything, our goal is not just to react to fraud but to **predict, prevent, and adapt.** That's how Fraudspect and ReconX help businesses stay one step ahead in safeguarding both transactions and customer trust

Q7: You're a part of the AI for Developing Countries Forum. From your experience, what is the most significant challenge for developing nations in harnessing the power of AI and digital technology securely, and what is a key strategy for overcoming?

The most significant challenge for developing nations in harnessing AI and digital technology securely is the gap between rapid adoption and the supporting infrastructure both in terms of cybersecurity maturity and regulatory readiness. Many organizations embrace AI and digital platforms quickly, but without robust data protection, governance, and security frameworks, they risk exposing sensitive information and undermining trust.

A key strategy to overcome this is building trust by design: embedding security, ethics, and compliance into digital solutions from the start, rather than as an afterthought. At Platview Technologies, we have seen that pairing AI innovation with strong fraud detection, data protection, and regulatory alignment allows businesses to scale confidently while protecting consumers. Ultimately, the opportunity for developing nations is immense, but to unlock it, security and trust must grow at the same pace as innovation.

Fraudspect & ReconX

Q8: The cybersecurity sector faces a global talent shortage. What is your perspective on bridging the skills gap, and what advice would you give to young professionals looking to start a career in this field?

The cybersecurity talent shortage is one of the industry's most pressing challenges, and it's even more pronounced in developing regions. Bridging the gap requires a dual approach: investing in capacity building through training, mentorship, and local talent development, while also leveraging automation and AI to reduce reliance on manual processes for routine security tasks.
For young professionals, my advice is simple:
focus on continuous learning and curiosity. Cybersecurity evolves daily, so certifications and technical skills matter, but so does the ability to think critically, adapt, and solve problems. Start with the basics - networking, cloud, identity management, and build depth in areas you are passionate about, whether that's threat intelligence, fraud prevention, risk management or AI-driven security. At Platview Technologies, we run an agile internship program which has an embedded continuous learning and democratized innovation for all participants, this way, we have been able to continuously contribute our quota to bridging the global skill gap. Most importantly, see cybersecurity not just as a job, but as a mission. You are not just defending systems, you are helping build trust in the digital economy."

Q9: You've spoken about the importance of collaboration between the public and private sectors. Can you give an example of a successful collaboration model you believe could be replicated to enhance national cybersecurity?

Collaboration between the public and private sectors is critical because cyber threats do not respect boundaries. One successful model I often point to is the creation of joint threat intelligence sharing platforms, where governments, banks, telcos, and cybersecurity providers exchange real-time data on emerging threats. For instance, financial sector CERTs (Computer Emergency Response Teams) in some markets have proven highly effective at preventing cross-institutional fraud by enabling rapid detection and coordinated response.
A model like this could be replicated nationally bringing regulators, law enforcement, and private innovators together around a shared cyber defense ecosystem. The public sector ensures governance and alignment with national priorities, while the private sector contributes agility, technology, and innovation.
At Platview Technologies, we advocate for this approach because no single entity can secure the digital economy alone, **resilience comes from collaboration, not isolation."**

> ▶ By implementing our real-time monitoring and adaptive digital risk protection, we were able to reduce losses by over 90% within the first six months, while also cutting manual review times significantly.

One success story that stands out is our deployment of a combination of Cyber Threat Intelligence and Incident Response service for a leading financial institution that was struggling with high levels of transaction fraud, brand abuse, and reputational risk. They had invested in multiple tools, but because the systems were not optimized and had a slim human capacity bandwidth, fraudsters were slipping through the cracks and continuously took advantage of unsuspecting customers.

By implementing our real-time monitoring and adaptive digital risk protection, we were able to reduce losses by over 90% within the first six months, while also cutting manual review times significantly. Beyond the numbers, what mattered most was the renewed confidence their customers expressed in digital banking, which directly boosted adoption rates.
For us at Platview Technologies, that is the ultimate measure of success, not just stopping attacks, but enabling our clients to

Gurucul Unveils the Industry's First AI-SOC Analyst: A Game Changer for the SOC

Gurucul
AI/ML Powered Security Analytics & Incident Response
Gurucul Unveils the Industry's
First AI-SOC Analyst:
A Game Changer for the SOC

Gurucul has shattered expectations by introducing the first AI-native analyst fully embedded within a SOC platform, ushering in the era of the AI-SOC Analyst. Instead of being a trendy add-on, this innovation marks a practical leap in security operations: automating triage, escalating threats, and accelerating response — all without replacing human expertise.

CTO Nilesh Dherange said: "We've developed LLM-enhanced workflows built specifically for the SOC, enabling automated alert triage at scale and giving analysts the speed and efficiency to stay ahead of modern threats."

Automating Alert Triage with Precision
The Gurucul AI-SOC Analyst **automates 100% of alert triage.** It extracts key artifacts, classifies alerts, applies risk scoring, and initiates escalation or remediation — slashing mean time to resolution (MTTR) by **83%**. What would take hours now happens in seconds.

Emulating a Seasoned Analyst with Context
Far from being just another automated tool, the AI-SOC Analyst behaves like an experienced human counterpart. It investigates every alert, gathers relevant context, and elevates only what truly demands human attention offering **evidence-based recommendations** that empower fast, informed decisions.

Powered by the Sme AI Copilot
At its side, the Sme AI copilot enhances investigations with generative AI. It transforms complex logs into plain English, summarizes intelligence reports, suggests further queries, and recommends next steps making analysts' lives smarter and more efficient.

Real Impact for SOC Teams

Here's what Gurucul's AI-SOC Analyst delivers:

24/7 monitoring with no fatigue—no interruptions for weekends, holidays, or burnout.
Reduced noise, laser-sharp focus—it filters out false positives and elevates high-fidelity threats.
Human augmentation, not replacement—it removes bias, accelerates workflows, and lets human analysts zero in on strategic tasks.
Cost-effective scaling—capable of automatically triaging thousands of alerts simultaneously, without needing extra headcount.

Trust Meets Explainability
Trust is built in: the AI-SOC Analyst's decisions are transparent and explainable, giving analysts confidence in the insights and giving teams a loop for feedback and continuous learning.

Why This Matters Now
As CEO Saryu Nayyar emphasizes: "With alert fatigue, analyst burnout, and growing threat complexity, SOCs need relief. This innovation shifts mundane tasks to AI, freeing humans for high-value work."

Gurucul's AI-SOC Analyst isn't just another tool — it's what the modern SOC needs: **always-on, intelligent, trusted automation** that amplifies human capability.

Obadare Peter

Nigeria's First Professor of Practice in Cybersecurity

Obadare Peter Adewale on Championing Cybersecurity and Digital Trust in Africa

First Certified Chief Artificial
Intelligence Officer (CAIO) in Nigeria

INTERVIEW

For over a decade, serving as Technical Partner to the Central Bank of Nigeria's Nigeria Electronic Fraud Forum (NeFF) has been both an honor and a profound responsibility

As the Founder of Digital Encode and a multi-award-winning expert, Professor Obadare Peter Adewale stands as a leading force in shaping a secure digital landscape for Africa. With over two decades of experience and a staggering portfolio of more than 60 international professional certifications, he has earned a reputation as arguably the continent's most "credentialed" digital trust leader.

Driven by a singular vision to make the internet a safer place, he founded Digital Encode to provide cutting-edge IT assurance to businesses across Nigeria and beyond. His pioneering work includes becoming Africa's first EC-Council Licensed Penetration Tester and Nigeria's first Professor of Practice in Cybersecurity. A Fellow of the British Computer Society and a member of the Forbes Technology Council, his influence extends from advising governments on national policy to mentoring the next generation of cybersecurity professionals. His work is guided by the philosophy that technology must serve the purpose of both solving problems and building trust.

Implementing layered, risk-based cybersecurity frameworks across Africa's diverse environments demands a nuanced approach grounded in local realities. My work with standards like ISO 27001, COBIT, PCI DSS, and TOGAF consistently proves that success lies in harmonizing global best practices with regional context.

I treat these frameworks not as rigid checklists but as an adaptive tools for risk-centric integration. This strategy aligns cybersecurity with business objectives, regulatory requirements, and operational maturity. For instance:

For over a decade, serving as Technical Partner to the Central Bank of Nigeria's Nigeria Electronic Fraud Forum (NeFF) has been both an honor and a profound responsibility. In this role, I've focused on developing and implementing evidence-based strategies to strengthen the financial sector's resilience against electronic fraud and cybercrime.

My contributions center on three critical areas:

As a technical thought leader, I've shifted the national conversation from reactive fraud response to proactive cyber risk management. This includes guiding the movement from magnetic stripe card to EMV card and integration of global frameworks—PCI DSS, ISO 27001, and other relevant standards—into policies adopted by banks, fintechs, and regulators.

Africa finds itself at a crucial crossroads—where AI governance, cybersecurity, and digital sovereignty intersect. While this presents immense opportunities, it also demands urgent and strategic action. Many African countries still operate without unified frameworks for responsible AI adoption, leaving gaps that expose us to risks around data protection and algorithmic accountability. My approach as CAIO emphasizes the development of ethical, secure, and locally relevant AI strategies that meet global best practices while addressing our unique regional challenges.

Despite growing cybersecurity awareness, many African organizations still treat testing as a compliance task rather than a risk-focused strategy. Assessments are often superficial, lacking the depth needed to simulate real-world threats. True red teaming—encompassing social engineering, insider threat simulation, and physical breaches—remains rare, and there's a critical disconnect between offensive findings and defensive action. The continent also faces a shortage of advanced offensive security professionals and limited efforts to translate technical risks into business terms.

As a Professor of Practice at Miva Open University, my mission is to deepen town and gown relationship that is bridge the gap between academic theory and the fast-evolving demands of cybersecurity, governance, and digital leadership. Today's complex threat landscape requires more than textbook knowledge—it demands professionals who can think critically, lead with strategy, and adapt swiftly to emerging challenges.

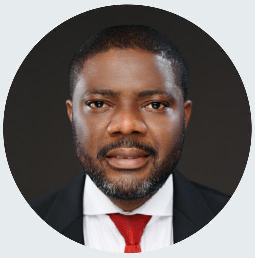
To address this, I have introduced a forward-thinking model that integrates international standards such as the International Organization for Standardization 27001, the National Institute of Standards and Technology Cybersecurity Framework, the Control Objectives for Information and Related Technologies framework, and the Payment Card Industry Data Security Standard.

Serving as Nigeria's first Certified Chief Artificial Intelligence Officer (CAIO) is both a profound honor and a vital responsibility.

As a Professor of Practice at Miva Open University, my mission is to deepen town and gown relationship that is bridge the gap between academic theory and the fast-evolving demands of cybersecurity, governance, and digital leadership. Today's complex threat landscape requires more than textbook knowledge—it demands professionals who can think critically, lead with strategy, and adapt swiftly to emerging challenges.

To address this, I have introduced a forward-thinking model that integrates international standards such as the International Organization for Standardization 27001, the National Institute of Standards and Technology Cybersecurity Framework, the Control Objectives for Information and Related Technologies framework, and the Payment Card Industry Data Security Standard.

Through my work with global technology platforms, I've engaged directly with leaders shaping the future of cybersecurity and artificial intelligence governance. These experiences have



Obadare Peter Adewale is a First Generation and Visionary Global Technopreneur

provided a valuable perspective on how Africa can chart its own course in the digital age.

Globally, there is a shift toward agile, risk-based approaches to cybersecurity—models that emphasize resilience and continuous adaptation over rigid compliance. African governments must tailor such frameworks to local contexts to better manage sector-specific risks. At the same time, responsible governance of artificial intelligence must prioritize ethical design, data protection, data privacy and local innovation. Countries like Rwanda, Kenya, and Nigeria have a key opportunity to lead with policies that uphold digital sovereignty and human rights.

Over the course of my career—advising governments, mentoring professionals, and leading cybersecurity programs across regions—one truth has remained central: cybersecurity is, above all, about people. While frameworks and tools matter, they cannot replace the value of ethical, skilled, and empowered professionals. In building talent, I focus on cultivating purpose, not just career ambition. Cybersecurity should be seen as a mission to achieve digital trust and national stability.

Penetration testing has been central to my career, notably as Africa's first EC-Council Licensed Penetration Tester and a leader in offensive security for nearly two decades.

The legacy I hope to leave in cybersecurity, AI policy, and national digital strategy is to help shape Africa into a digitally sovereign, cyber-resilient, and ethically innovative continent — one that doesn't merely adopt technology but defines its direction, governance, and long-term value.

For me, the true impact lies in building systems that outlive individuals. I am committed to establishing strong institutions, regulatory foundations, and educational structures that consistently produce visionary thinkers, ethical innovators, and trusted digital leaders — well beyond my personal involvement. It's not about creating success stories tied to personalities, but about institutionalizing excellence. In a world increasingly shaped by artificial intelligence, I believe Africa must lead with ethical clarity. Our technologies should reflect our languages, cultures, and rights, not inherit the limitations of models built without us in mind. We must design and govern AI with foresight and cultural relevance, ensuring its application aligns with African values.

Ultimately, I want to be remembered not just as someone who spoke about transformation but as someone who helped entrench it. If Africa rises as a confident, ethical, and sovereign digital power, then I would consider my journey profoundly worthwhile.

Strong collaboration between public institutions and the private sector is essential, particularly in intelligence sharing, critical infrastructure protection, and talent development. Africa must also take its seat at global forums to shape international norms, ensuring the continent becomes a co-creator—not just a consumer—of future digital rules. Ultimately, Africa's digital future depends on leadership, foresight, and the will to act in its own strategic interest.

“

With over 60 global certifications and a track record of shaping national cybersecurity policies, he is redefining how Africa builds resilience, safeguards digital sovereignty, and develops world-class cyber talent.

Identity & Access Management (IAM) at Spire Solutions

Sathyamurthy, Sales Director Identity & Access Management (IAM) at Spire Solutions

From your vantage point as a Sales Director at Spire Solutions, what are the top 3 identity security priorities you're hearing from your clients as they look to future-proof their organizations against emerging threats and evolving regulatory landscapes?

Besides IGA and PAM a still popular asks when it comes to clients Identity Security programs, I am witnessing a great demand on Zero Trust Identity Verification. Especially, with the recent announcement by UAE's Central Bank asking banks to move away from traditional SMS & Email based OTP, to app-based authentication effective July 2025 and before conclusion of March 2026. With client's maturity to move to "never trust, always verify", and layering MFA, continuous risk-based assessment and adaptive access policies at every access request, ensuring that every user, device and session are continuously evaluated against real-time threat signals. I see these to be significant opportunities.

"Using personal data without proper controls can compromise regulations"

Given your leadership experience in identity security and IAM, what's been the most significant lesson you've learned about effectively leading teams and driving innovation particularly across culturally diverse teams in the Middle East?

I am in the region for over three decades, with focus around Identity & Access Management (IAM) past 17 years engaging with clients in various capacity as vendor, SI and VAD, across the Middle East, empathy is just not a soft skill—it is the fundamental of collaboration. Also, the longevity in the region has allowed me to understand the local customs, working style, and communication well. I have built credibility by continuous value creation; made people willing to share ideas and flag risks early. By small gestures, both internal and external clients see a great value collaborating with me. I believe when it comes to innovation it resonates well with the team's values and experiences.

How are you seeing organizations in the Middle East & Africa (MEA) region approach the adoption of zero-trust architectures and what unique challenges and opportunities do they face in implementing these frameworks compared to other regions?

I think with the significant adoption of Zero Trust in the GCC especially organizations the UAE and Saudi Arabia are outpacing. With Government-led digital initiatives and agenda, and rising use of AI-powered deepfakes, ransomware, and state-sponsored attacks in the region has elevated Zero Trust from "nice-to-have" to business imperative. Furthermore, I see other countries in the Middle East are accelerating in line with respective nations digital transformation strategy. Perhaps, countries in Africa, the Zero Trust adoption are subjective but growing rapidly, with cloud migration/cloud adoption is becoming a viable business strategy.

AI is increasingly being used to enhance threat detection in identity systems. How can organizations leverage AI to effectively identifr and respond to sophisticated identity-based attacks, and what are the potential pitfalls to avoid?

In order leverage AI for Identity-based threat detection, organizations can consider AI to move beyond static rules and signatures, unveiling subtle, evolving identity threats in real time. By combining advanced analytics with contextual intelligence, teams can spot anomalies, prioritize risk, and orchestrate automated responses to sophisticated attacks before they escalate. When it comes to potential pitfalls to avoid, be mindful of your AI as it might flag normal user actions as threats (false alarms). The attackers can feed bad data to weaken your detection models. While using personal data without proper controls can compromise regulations. Lastly, one of the most important aspects is cost to build and run AI-based detection requires expert resources, right tools, and ongoing services. Organizations need to partner with the right team.

What role do you believe partnerships and collaborations play in fostering innovation and driving the adoption of advanced identity security solutions in the MEA region, and how is Spire Solutions engaging with technology alliances, Partners and Customers to achieve this?

In the rapidly evolving cybersecurity landscape, partnerships and collaborations serve as the catalyst for both innovation and widespread adoption of advanced identity security solutions in MEA. By leveraging the unique strengths of industry-leading technology partner solutions coupled with Spire Solutions expertise, system integrators, and end-customers, the ecosystem combines to deliver solutions and services that are both cutting-edge and regionally relevant. Through Spire's presence at major regional exhibitions such as GITEX Global, GISEC, LEAP, Blackhat, webinars, workshops, etc., we accelerate customer confidence in adopting and growing their identity security journey. We also play a significant role helping organizations to stay a step ahead in today's dynamic threat landscape.

What is your vision for the future of digital trust in the Middle East & Africa, and what steps can organizations take to build and maintain that trust with their customers, partners and employees?

As MEA accelerate their digital transformation—driven by AI, cloud and related adoption—digital trust will become the cornerstone of economic growth and social inclusion. Organizations will be expected to embed cybersecurity as a strategic asset. A unified regulatory framework across markets will emerge, balancing agility with robust data protection to reduce fragmentation and shore up cross-border collaboration. To build and maintain digital trust, with clients, we need to adopt globally recognized digital trust frameworks (e.g., NIST) to demonstrate rigorous data governance and security practices. With partners, complement compliance protocols across authorities by engaging with regional regulators and industry associations to shape unified standards for data protection and AI ethics. Lastly to workforce, provide an ongoing training programs on cybersecurity hygiene, data-privacy best practices and ethical AI, ensuring everyone understands their role in upholding trust. Furthermore, by investing—cyber resilience, transparent governance, inclusive engagement and human-centric controls—will position organizations in MEA to not only meet rising stakeholder expectations but to turn digital trust into a competitive advantage.

“Innovation resonates well with team's values and experience”

What's your perspective on how African enterprises, especially in fast-growing digital economies can leapfrog in identity security, and what foundational steps should CIOs prioritize?

Enterprises in Africa is fast-growing digital economies are uniquely positioned to leap in identity security. In my opinion, CIOs should prioritize in Identity-first security, adopting passwordless authentication/biometric authentication, integrating AI for threat detection, etc. As both human identities and non-human identities/machine identities are out numbering and exploding in growth, CIOs need to treat identity security as a strategic enabler rather than just a compliance checkbox.

“CIOs should prioritize in identity first security, adopting passwordless authentication/ biometrics authentication, integrating AI for threat detection”

SECLORE™

NITDA's NDPR to Nigeria's NDPA: Persistent Data Security for a Digital Nation

Nigeria is rapidly becoming Africa's digital powerhouse, with banking, telecom, government, and oil & gas driving digital transformation. Yet, with this growth comes escalating cybercrime and regulatory scrutiny. The journey began with the Nigeria Data Protection Regulation (NDPR 2019), issued by NITDA, and has now matured into the Nigeria Data Protection Act (NDPA 2023) under the Nigeria Data Protection Commission (NDPC). Together, these frameworks underscore Nigeria's commitment to global best practices in data governance.

Traditional perimeter-based security stops at the boundary; data, however, doesn't. Organizations need persistent, data-centric protection that stays with information wherever it travels.

The Challenge

Once files and emails leave the enterprise, organizations lose visibility and control. Sensitive data is exposed to insider threats, vendor misuse, and cross-border leakage. In highly regulated sectors like banking and government, this can mean fines, reputational damage, and operational disruption.

Data leakage across partners and third parties.

Limited visibility into how shared data is used.

Seclore's Approach

Seclore enables Nigerian enterprises to align with NITDA's NDPR (2019) principles and NDPA (2023) obligations by embedding security into the data itself.

Persistent protection for files and emails.

Dynamic access control (who, what, when, where).

Real-time tracking and instant revocation.

Industry Impact in Nigeria

- Banking & Financial Services: Meet CBN and NDPA requirements, protect customer data against fraud.
- Government & Public Sector: Secure citizen records, enable controlled inter-agency collaboration.
- Oil & Gas / Manufacturing: Safeguard intellectual property in multi-vendor ecosystems.
- Telecom & Technology: Guarantee customer trust in a high-volume data environment.

Regulatory Evolution (NDPR → NDPA)

- NDPR 2019 (NITDA): Introduced GDPR-like principles of consent, processing, and rights.
- NDPA 2023 (NDPC): Full law with stronger enforcement, penalties, and compliance mandates.
- Seclore bridges both: providing auditability, cross-border controls, and usage governance that map directly to regulatory clauses.

Conclusion

Nigeria is at an inflection point—digital growth cannot come at the cost of security and compliance. From NITDA's pioneering NDPR to the NDPA today, Seclore empowers organizations to transform compliance into a business advantage. Sensitive data remains protected, auditable, and under control—wherever it travels.

Take the Next Step: Protect your enterprise with Seclore and lead Nigeria's secure digital future.

Visit **www.seclore.com** for more information.

Risk Management

KnowBe4 Africa Human Risk Management Report 2025: Unveiling the Cybersecurity Confidence Gap

Africa Human Risk Management Report 2025

The latest KnowBe4 Africa Human Risk Management Report 2025 exposes a cybersecurity confidence gap that could leave businesses across the continent vulnerable to a new wave of attacks.

The report, which surveyed 124 senior cybersecurity leaders from 30 African countries, found that while a majority of executives believe their staff is cyber-aware, a staggering 90% are not fully confident their employees would report a real phishing attempt or suspicious activity.

One of the most concerning findings is the illusion of effective training. While two-thirds of leaders claim their cybersecurity training is role-specific, the reality for many employees is generic, one-size-fits-all programs. This is particularly prevalent in sectors like manufacturing and healthcare, where 50% and 40% of firms, respectively, admit to having no tailored training at all. You wouldn't train a pilot with the same manual as a flight attendant, yet this is precisely what is happening with cybersecurity.

This training gap is compounded by infrequent testing. While 90% of organizations conduct phishing simulations, a significant 40% only do so twice a year, leaving staff unprepared for the constant evolution of cyber threats. It’s like conducting a fire drill once every six months and expecting people to react perfectly in a real emergency.

The Rise of Shadow AI

- The unprepared revolution of cyber threat
- Infrequent testing training gap in cybersecurity

The report also highlights two emerging threats that are widening the confidence gap: Bring Your Own Device (BYOD) and the unsanctioned use of AI. In North Africa, up to 80% of employees are using personal devices for work, often without adequate security controls

With 46% of organizations still in development with their AI governance policies, employees are left to their own devices, using AI tools that may expose sensitive corporate data. The rise of shadow AI presents a new frontier for data loss and intellectual property theft, making the need for clear governance and training more urgent than ever.

Anna Collard, SVP at KnowBe4 Africa, wisely warns, "Without procedural and cultural follow-through, awareness simply doesn’t translate into readiness." The report is a clarion call to action for African businesses. To bridge this confidence gap, companies must move beyond surface-level awareness and build a true culture of cybersecurity readiness

•**Role-Based Training:** Implementing tailored, relevant training that addresses the specific risks each employee faces.

•**Frequent Simulations:** Conducting monthly phishing tests to keep employees sharp and responsive.

•**Clear Governance:** Establishing and enforcing clear policies for BYOD and AI tool usage.

•**Regional Strategies:** Developing region-specific strategies to address the unique threat landscapes in places like West and Central Africa, which have the highest number of human-related breaches.

In Focus CISO

Certified CISO Philip Aiwekhoe on Shaping the Future of Cybersecurity Strategy in Africa's Financial Sector

CISO AT NPF MICROFINANCE BANK NIGERIA

Philip Aiwekhoe, Chief Information Security Officer (CISO) and Data Protection Officer at NPF Microfinance Bank Plc, is a visionary cybersecurity executive with over 15 years of experience spanning governance, risk, compliance, and digital transformation.

With a dual role as Cybersecurity Consultant to the Police Service Commission, Philip combines deep technical expertise with strategic foresight.

With over two decades of experience traversing senior leadership roles in both financial institutions and regulatory bodies, I've had the exclusive opportunity to understand cybersecurity from multiple vantage points. In financial institutions, the emphasis has often been on innovation, customer trust, and maintaining continuity in a rapidly evolving threat landscape.

Strategic Alignment with Risk Appetite: I've learned that effective cybersecurity must align with an organization's broader risk management strategy and business strategy.

Public-Private Collaboration: Having worked across both sectors, I value the importance of fostering information sharing, joint threat intelligence, and coordinated incident response.

Resilience Beyond Prevention: True cybersecurity resilience isn't just about stopping threats, it's about anticipating, withstanding, and recovering from them

My leadership journey has reinforced that cybersecurity is not just a technical challenge, it's strategic, governance, operational, and cultural priority. Whether advising boards or shaping regulatory policy, I aim to ensure that cyber resilience is treated as a fundamental pillar of long-term institutional sustainability.

Serving as Chief Information Security Officer at NPF Microfinance Bank for nearly five years, I encountered a range of data protection and cyber risk challenges, particularly given the evolving threat landscape and the unique nature of microfinance institutions operating within the Nigerian financial ecosystem.

- **Legacy Infrastructure and Limited Resources:**
- **Data Privacy and Regulatory Compliance:**
- **Insider Threat and User Awareness:**
- **Third-Party Risk Management:**
- **Incident Detection and Response:**

In my advisory role with the Police Service Commission, where I lead efforts to elevate cybersecurity awareness and develop curriculum for government bodies, I've seen firsthand how crucial it is to build a foundational understanding of cybersecurity across all levels of government, from senior leadership to

PROFESSIONAL ROLES

He holds top industry credentials including Certified CISO and Certified Information Security Manager (CISM), and is an active member of professional bodies such as BCS (British Chartered Institute of IT), ISACA, EliteCISO, CyberEdBoard, EC-Council, and Microsoft communities.

Africa's digital payments market by 2030

$1.5 Trillion Dollar

operational teams.

Rather than treating regulatory compliance (like NDPR, GDPR, etc.) a rectly into the Information Security Management System (ISMS). This ensures that compliance isn't separate from security; it enhances it.

As both DPO and CISO, I have been able to streamline governance structures, ensuring policies around data access, encryption, breach notification, and third-party risk management satisfy both legal requirements and technical defenses.

One of the most concerning trends we're observing in Nigeria, particularly within the financial and government sectors, is the convergence of three critical threat vectors: advanced social engineering, supply chain compromise, and ransomware-as-a-service (RaaS).

Social engineering attacks are growing more sophisticated with the advancement of AI. Threat actors are no longer relying solely on phishing emails; they're leveraging voice phishing (vishing), deepfakes, and real-time manipulation tactics, targeting employees at all levels, including privileged users in banks and public service agencies.

Through the Future Cyber Leaders Mentorship Initiative (FCLMI) initiatives we have reached 600 students in two major universities and some of our mentees who are undergraduates are gainfully employed in Charistech Consulting Limited.

Many young talents are highly enthusiastic, which is great. But there's often a misconception that cybersecurity is purely about hacking tools or certifications. What's missing is a strategic, problem-solving mindset, a deep understanding of risk, and the ability to connect cybersecurity to business outcomes.

Implementing ISO 27001 in Nigeria or anywhere in Africa, isn't just about ticking boxes; it's about translating global standards into something that actually works within local constraints."

One major challenge I've seen is that many organizations try to copy-paste the ISO 27001 framework without adapting it to local realities, limited budgets, fragmented infrastructure, leadership buying, or skill gaps. That approach fails.

Firstly, we start with contextual risk assessment not theoretical. I help organizations define their risk appetite in terms they understand: "What can we afford to lose? What would shut us down?" That makes the controls real, not abstract. Secondly, I emphasize scalable implementation. You don't need an enterprise-grade SIEM on Day

My advice to executives is modest and clear: if you're still treating cybersecurity as an IT problem, you're already behind and your business is at risk.

A single breach can shut down operations, erode customer confidence, attract legal penalties, and destroy shareholder value all in one blow.

I often tell boards and CEOs: cyber risk is a business risk and managing it should sit squarely at the executive table, not in a back-office IT department.

The same way you monitor financial exposure, you must monitor cyber exposure including your people, your vendors, your data assets, and your crisis readiness.

Cybersecurity needs to be built into your strategy, not layered on top of it. That means:

15 years of experience

- Governance, Risk, Compliance, and Digital transformation.

IN FOCUS CCISO

Olayinka Wilson-Kofi: Championing Cybersecurity, Governance, and Inclusion Across Africa and the Middle East

CCISO-Certified and Leading Across MEA

Information Security and Privacy Specialist at Ericsson

With over 16 years of experience in cybersecurity, governance, privacy, and technology leadership, Olayinka Naa Dzama has become a powerful voice in shaping secure digital ecosystems across Africa and the Middle East.

As a CCISO-certified Information Security Specialist, she leads cybersecurity governance, privacy, and risk efforts across 35+ countries in the Middle East and Africa. Her additional role as President of WiCyS West Africa reinforces her mission to build capacity, promote diversity, and drive impactful change in the region's digital future.

My journey into cybersecurity started with a strong foundation in IT and a passion for teaching, which I pursued on the side to share knowledge and empower others. As I gained more experience, I became increasingly drawn to the critical role of governance, risk management, IT audit and data protection.

Today, I serve as an Information Security Specialist at Ericsson, where I support security governance, privacy, and risk mitigation efforts across Middle East and Africa.

In addition to my corporate role, I lead as the President of Women in Cybersecurity (WiCyS) West Africa, where I advocate for diversity, capacity building, and awareness in the digital space.

Certification

- CCISO, CRISC,ITIL
- ISO/IEC 27001 LI/LA,ISO 27032

What drew me to governance, privacy, and risk in cybersecurity was the influence of my mentor, C.K. Bruce, who helped me see the bigger picture beyond just technical controls. I became passionate about how policies, compliance, and ethical data handling shape trust in digital systems. Over the past 16+ years, my perspective has evolved from seeing GRC as a support function to recognizing it as a critical business enabler.

In my current role at Ericsson, one of the biggest challenges is navigating varying regulatory landscapes across multiple countries in Africa and the Middle East. Each region has its own privacy laws, cybersecurity mandates, and data localization requirements with some well-established, others still evolving. Ensuring compliance while maintaining operational consistency is a constant balancing act.

In my current role at Ericsson, one of the biggest challenges is navigating varying regulatory landscapes across multiple countries in Africa and the Middle East. Each region has its own privacy laws, cybersecurity mandates, and data localization requirements with some well-established, others still evolving. Ensuring compliance while maintaining operational consistency is a constant balancing act.

Her mantra: "When women are empowered, entire communities are strengthened."

In multinational settings, I approach Privacy and Risk Assessments by aligning with global standards like ISO 27001 and GDPR, while adapting to local regulation and laws. I take a risk-based, context-aware approach, engaging with local teams to ensure compliance is both practical and effective.

16+ years

In IT, Cybersecurity, Privacy and Risk Management

The goal is to integrate privacy and security early, manage risks proactively, and maintain agility as laws and threats evolve.

ISO 27001 has had the most significant impact on how I work and lead. Its structured approach to establishing, implementing, and maintaining an Information Security Management System (ISMS) has shaped how I view security as a continuous, organization-wide responsibility.

In addition, NIST 800-53 has influenced my understanding of risk-based controls and how to apply them in complex environments, while ISO 27032 has been valuable in addressing cybersecurity in the broader context of digital collaboration and internet threats.

In my contributions to the ISACA and EC-Council communities, I focus on sharing insights around governance, privacy, and risk management.

I'm particularly passionate about trends like Zero Trust architecture, data protection by design, and AI-driven threat detection. I also emphasize the importance of cybersecurity awareness, ethics, and building resilience in low-resource environments.

With my mentees, I stress the value of certifications, continuous learning, and real-world application, encouraging them to see cybersecurity as both a technical and strategic career path.

Bridging the gap between policy and real-world execution starts with simplifying complex frameworks into actionable steps that stakeholders at all levels can understand and apply.

I prioritize capacity building, cross-sector collaboration, and clear communication to ensure that policies don't just stay on paper but are embedded into daily operations. Whether working with national agencies or mentoring individuals, my goal is to make cybersecurity both practical and sustainable.

To see more women rise into strategic cybersecurity roles across Africa, we need a deliberate ecosystem of support, starting with early exposure, mentorship, and sponsorship. It's not just about training women in technical skills but also equipping them to lead, influence policy, and sit at decision-making tables.

We must also address structural barriers by promoting inclusive hiring, flexible work environments, and visible role models who show what's possible. I strongly believe in creating safe spaces for women to grow, fail, and rise again because when women are empowered, entire communities are strengthened.

I'm most excited about Africa's growing digital transformation and the opportunity to build cybersecurity into the foundation, not as an afterthought. As governments, startups, and industries embrace tech, there's a critical moment to shape a security-first mindset across the continent.

I hope to continue playing a role in strengthening governance, building local capacity, and mentoring the next generation of cybersecurity leaders especially women.

> “With my mentees, I stress the value of certifications, continuous learning, and real-world application, encouraging them to see cybersecurity as both a technical and strategic career path.

The AI Gap in Cybersecurity Leadership: A Silent Risk

Albert Laweh Tetteh | CISO at GCB Bank Ghana

Cybersecurity Leadership

In a world where threats are smarter, defenses must be smarter and that begins with cybersecurity leaders who understand, leverage, and innovate with AI

As cyber threats continue to evolve in both complexity and scale, malicious actors are increasingly leveraging artificial intelligence to automate phishing campaigns, evade traditional security defenses, and exploit vulnerabilities with unprecedented speed. In response, cybersecurity professionals must integrate AI into their defense strategies to effectively counter these advanced threats. AI empowers defenders with predictive analytics, real-time threat detection, and automated incident response capabilities that are now essential in modern cybersecurity operations. Reflecting this growing reliance, the global AI in cybersecurity market valued at $15.7 billion in 2021 is projected to reach $133.8 billion by 2030, expanding at a compound annual growth rate of 23.6%, as reported by Allied Market Research.

The Convergence of Cybersecurity and AI

Artificial intelligence (AI) is increasingly vital in cyber defense due to its ability to process vast amounts of data, detect anomalies, and respond to threats in real time. According to IBM Security AI reduces the average time to detect a cyberattack by up to 96%. Traditional cybersecurity tools often rely on predefined rules and signatures, which can be ineffective against novel or evolving attacks. AI, particularly machine learning and behavioral analytics, enables systems to identify suspicious patterns, predict potential breaches, and automate responses before damage occurs. According to Trend Micro, Incident response platforms using AI handle up to 200% more cases than manual systems. This proactive approach is essential in defending against sophisticated threats like AI-generated phishing, ransomware, and insider attacks, making AI a powerful ally in modern cybersecurity strategies.

Conversely, as AI systems become more integrated into critical sectors such as finance, healthcare, and education they themselves become targets for exploitation. Cybersecurity must be embedded into AI projects from the ground up to protect sensitive data, ensure model integrity, and prevent adversarial manipulation. This includes securing training datasets, safeguarding algorithms from reverse engineering, and enforcing privacy and compliance standards. Without robust cybersecurity measures, AI systems can be compromised, leading to biased decisions, data breaches, or operational failures. Therefore, cybersecurity and AI must evolve together, with leaders ensuring that every AI deployment is both innovative and secure.

> **Without robust cybersecurity measures, AI systems can be compromised leading to biased decisions, data breaches, or operational failures.**

Albert Laweh Tetteh | CISO at GCB Bank Ghana

Use Cases and Practical Applications

AI in Fraud Detection and Scam Prevention

Financial institutions are prime targets for cybercrime. AI plays a crucial role in fraud detection and scam prevention by analyzing large volumes of transactional and behavioral data to identify anomalies such as suspicious patterns, location mismatches, or rapid fund transfers. According to McKinsey, AI detects 53% of fraudulent transactions that traditional methods miss. Natural language processing (NLP) helps identify phishing attempts by analyzing the tone, structure, and intent of messages. Additionally, AI systems continuously learn and adapt to new scam tactics, improving their accuracy and reducing false positives over time. According to IBM, AI reduces false declines in transactions by 70%.

AI in Threat Intelligence and Response

Machine learning algorithms can sift through massive volumes of log data to identify patterns that indicate a breach. Tools like Darktrace and CrowdStrike use AI to detect lateral movement, privilege escalation, and other tactics used by advanced persistent threats (APTs). AI enhances malware analysis by rapidly identifying malicious code patterns, behaviors, and signatures across vast datasets, significantly reducing detection time. It also enables dynamic analysis by simulating malware execution in virtual environments, allowing cybersecurity teams to understand its behavior and develop targeted countermeasures. Cybersecurity leaders must understand how these models work, how to interpret their outputs, and how to integrate them into broader security strategies.

AI in Cybersecurity Awareness

Agentic AI systems capable of autonomous decision-making can personalize learning paths, simulate attack scenarios, and provide real-time feedback. This approach not only improves learning outcomes but also prepares students for real-world challenges. A few AI-based Cybersecurity platforms such as Cybrary and Brightside AI use AI to create dynamic training environments. Cybersecurity leaders must be able to evaluate these tools, ensure they align with learning objectives, and adapt them to evolving threats.

AI and Cybersecurity Workforce

The convergence of artificial intelligence (AI) and cybersecurity is reshaping the workforce landscape, creating both opportunities and challenges for professionals in the field. As cyber threats become more sophisticated and data volumes grow exponentially, organizations increasingly rely on AI to automate threat detection, analyze behavioral patterns, and respond to incidents in real time. This shift has led to a rising demand for cybersecurity professionals who possess AI and data science skills, with industry reports indicating a significant skills gap in areas such as machine learning, threat modeling, and AI governance.

Emerging Trends:

Emerging trends in cybersecurity highlight the transformative role of artificial intelligence across key operational areas. AI-augmented Security Operations Centers (SOCs) are streamlining workflows by automating routine tasks such as log analysis and alert triage, enabling analysts to concentrate on strategic threat mitigation and incident response. In access management, AI is enhancing Zero Trust architectures by enforcing dynamic, context-aware controls based on real-time risk assessments. Privacy and data protection are also benefiting from AI tools that detect data leaks, enforce compliance with privacy regulations, and manage user consent more efficiently. According to PWC, 54% of companies use AI to ensure adherence to GDPR and other regulations.The integration of AI into cybersecurity is not optional, it's essential. Leaders therefore must develop multidisciplinary expertise to navigate this new era. In a world where threats are intelligent, defenses must be smarter and that begins with cybersecurity leaders who understand, leverage, and innovate with AI.

SECLORE™

Know, Protect, and Control Your Data Wherever It Goes

Securing Digital Assets Across

Any User

Any Device

Any App

Any Cloud

Third-Party Risk • Insider Threat • IP Protection • App/Cloud Data Security • Data Privacy

Prevent Data Theft & Achieve Compliance

Know
Protect
SECLORE™
Data-Centric Security
Control

Know

Exactly what's shared and where your data is

- Risk insights & trends
- Access patterns & usage analytics
- Location awareness

Protect

Every single asset wherever it goes

- Policy management
- Dynamic watermarking
- Classification labeling
- AES256 bit encryption

Control

Who has access and revoke it at any time

- Granular access control
- Real-time access revocation
- Dynamic policy federation

Risk Insights

Understand the organization's current risk exposure & identify top opportunities to mitigate risk.

Digital Asset Classification

Organize business data by sensitivity to drive appropriate protect and control actions.

Trusted	5+ billion documents and emails protected and 2,000+ global customers.
Multi-sector	Trusted by companies in the financial services, manufacturing, government, and more.
Global	Deployed in 30+ countries with offices in six countries.

Our Customers

AMERICAN EXPRESS
flex
gm FINANCIAL
EA
LARSEN & TOUBRO
ICICI
Ford
CHENIERE
HDFC BANK

www.seclore.com

How AI-ready is Africa

AI INSIGHT & REPORT

South Africa 0.50

•AI adoption: Leading the continent in AI research and infrastructure.

•Key players: South Africa Artificial Intelligence Association, Center for Artificial Intelligence Research.

•Trends: National Artificial Intelligence Plan is one of the first regulatory frameworks. Innovation hubs in Cape Town and Johannesburg foster start-ups.

Nigeria 0.34

•AI adoption: Ranks second after South Africa in terms of the number of AI start-ups in Africa.

•Key players: National Center- for AI and Robotics.

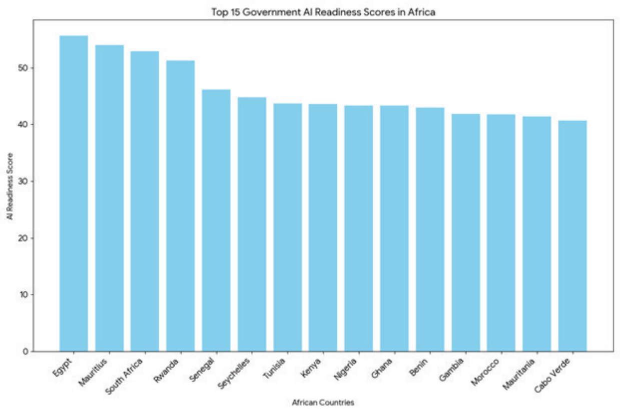
•Trends: Among top 15 countries in AI and crypto in 2024. Host of GITEX 2025, the world's largest technology fair.

Morocco 0,43

•AI adoption: Growing hub for AI solutions in renewable energy, aggrotech, and healthcare.

•Key players: Mohammed VI Polytechnic University, Technopark Casablanca, Deep Echo.

•Trends: Morocco AI Annual Conference. New Development Model will lead to a national strategy.



How AI-ready is Africa

Based on the IMF AI Preparedness Index, which ranks countries with scores ranging from 0.8 and more, 0.6-0.8, 0.4-0.6, and 0.2-0.4. The average score of advanced economies is 0.68 while that of emerging market economies is 0.46 on the index.

Kenya 0.45

•AI adoption: Driven by mobile money, fintech innovation.

•Key players: M-Pesa, PesaPal, Tala.

•Trends: The 'Silicon Savannah' is a hub for startups. Growth is supported by policies like National AI Strategy 2025–2030.

Egypt 0.39

•AI adoption: Focused on public services, healthcare, agriculture, financial services.

•Key players: Ministry of Communications and Information Technology (MCIT), Applied Innovation Center, Synapse Analytics.

Trends: First Arab and African country to adopt OECD AI Principles. The National AI Strategy 2025–2030 aims to: Raise the ICT sector's contribution GDP to 7.7% by 2030; establish over 250 AI companies; and train 30,000 AI professionals by 2030

Mauritius

•AI adoption: Strong in agriculture, healthcare, and fintech (regtech and digital payments).

•Key players: Mauritius Emerging Technologies Council, ARIE Finance, University of Mauritius, Dayforce.

•Trends: Hosted the inaugural AI Summit in 2024, under UNESCO. Ebene's Cybercity is the primary center for AI and digital innovation, bringing together start-ups and tech firms

Top 15 government AI readiness scores in Africa

According to Government AI Readiness Index 2024 Africa ranking, Oxford Insights

- **Rwanda 71.44**
  The Government pillar assesses vision, governance and ethics, digital capacity, and adaptability.
- **Egypt 42.13**
  The Technology pillar assesses maturity, innovation capacity, and human capital
- **South Africa 65.28**
  The Data & Infrastructure pillar assesses supportive infrastructure, data availability, and data representativeness

What AI Revolution Means for Your Cybersecurity Career

The future belong to those who embrace new skillset that blends technical know-how with strategic thinking and human ingenuity

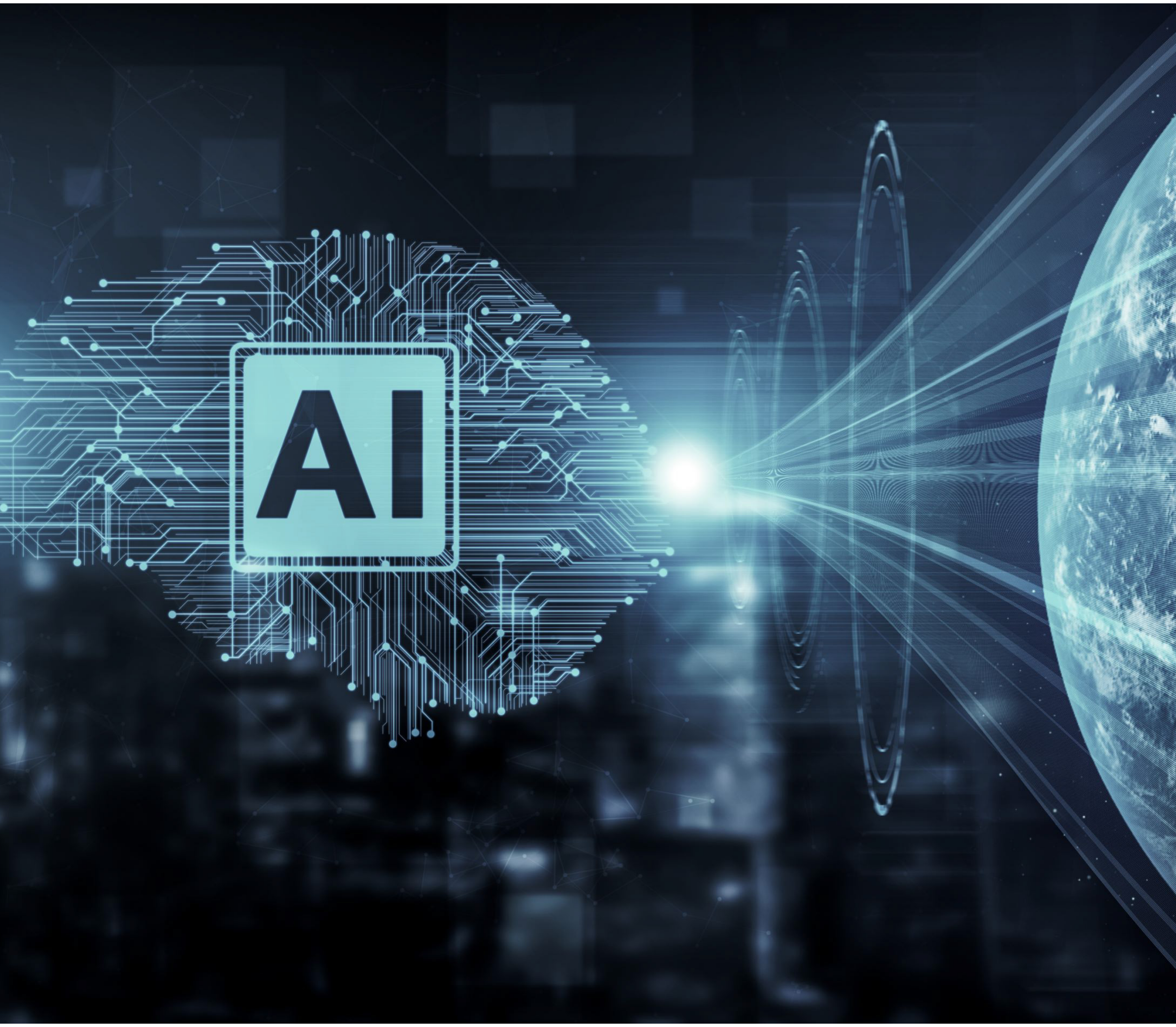
cybersecurity professionals must Master our skills at far beyond firewalls, antivirus, softwares and incident logs

The rise of artificial intelligence has sparked a pivotal debate across every industry, but nowhere is its impact more profound than in cybersecurity. For years, the conversation has centered on whether AI will take jobs. In cybersecurity, the question is not about elimination, but about evolution. AI is creating a new, more strategic, and more demanding role for professionals, making it crucial to re-evaluate what it means to be a guardian of the digital world.

Cybersecurity professionals of today must master a skillset far beyond firewalls, antivirus software, and incident logs. AI is rapidly automating these routine tasks, freeing up human talent to focus on more complex, strategic challenges. This shift requires a new kind of expertise:

•Data Science and Analytics: AI is powered by data. To be effective, security professionals must understand how to interpret AI-generated insights, tune machine learning models to reduce false positives, and use data to predict future threats.
•AI Ethics and Governance: As AI makes critical decisions—like who gets network access or what activity is flagged as suspicious—professionals must ensure these systems are fair, transparent, and compliant with privacy regulations. This requires a strong ethical compass and a deep understanding of evolving governance frameworks.

•Business Acumen: The most valuable cybersecurity professionals will be those who can connect their work directly to business outcomes. They must be able to explain how AI-driven defenses protect revenue, enhance customer trust, and enable secure innovation



The Evolving Roles of the Future

This shift is giving rise to new and specialized roles that were unimaginable just a few years ago. Instead of just security analyst, we now see titles like:

•AI Security Analyst: Professionals who monitor and manage AI-driven security systems, interpreting complex outputs and collaborating with data scientists to improve threat detection algorithms.

•Machine Learning Threat Hunter: These experts use AI models to hunt for advanced threats and hidden vulnerabilities that traditional methods can't find.

•Security Automation Engineer: They build and maintain the AI-powered systems that handle everything from alert triage to automated incident response, ensuring that the machines are running smoothly.

Bridging the Talent Gap

Despite the exciting opportunities, a significant talent gap exists. Organizations struggle to find professionals with the right mix of technical and strategic skills. To address this, a two-pronged approach is essential for both individuals and organizations.

For Professionals: The most resilient careers will be those built on a foundation of continuous learning. Individuals should seek out training and certifications in AI, data science, and governance. They must cultivate soft skills like problem-solving, communication, and adaptability, which will become even more valuable in an automated world.

For Organizations: It's no longer enough to simply hire from the outside. Companies must invest in upskilling their existing teams, providing them with the training and mentorship needed to thrive in an AI-driven environment. Fostering a culture of learning and interdisciplinary

Cybersecurity Forum

Nairobi Hosts Landmark Cybersecurity Forum to Boost Digital Resilience

15 Aug 2025 - JW Marriott Nairobi

Identity & Data Governance for Secure Digital Transformation

A high-level cybersecurity forum in Nairobi brought together over 100 industry leaders, signaling a unified and urgent call to strengthen Africa's digital defenses. On August 15, 2025, the JW Marriott Nairobi became a hub for CISOs, CIOs, and data governance leaders from across central banking, fintech, telecommunications, and government agencies, all with a shared mission, to build a more cyber-resilient future for the continent.

The forum's discussions were centered on three pillars of digital trust, identity security, data governance, and overall digital resilience. As the digital economy in Africa expands, these topics have become more critical than ever, with organizations facing increasingly sophisticated threats. The presence of leaders from diverse sectors underscored a key reality. In today's interconnected world, cybersecurity is not a siloed issue but a shared responsibility that requires cross-industry collaboration.

This landmark gathering was made possible through the collaborative efforts of its hosts, Sechpoint Technologies and iSolutions Associates. Their vision for a platform dedicated to high-level dialogue was brought to life with the support of SHAHPER Media, which served as a crucial event partner. The forum's success is a testament to the power of a coordinated effort to address complex challenges.

The event, which was widely praised for its curated and insightful content, provided a forum for leaders to share best practices and forge new partnerships. It highlighted the proactive steps being taken by African organizations to fortify their defenses from within. The success of these gathering serves as a clear indicator of the growing commitment within the continent to secure its digital future and build a foundation of trust for its citizens and businesses.

100+ CISOs, CIOs, compliance heads, data & senior cybersecurity officers

▶ The forum welcomed leaders from central banking commercial banking, insurance, telecommunications, fintech, government agencies, and critical infrastructure

Nigeria Data Protection Act (NDPA)

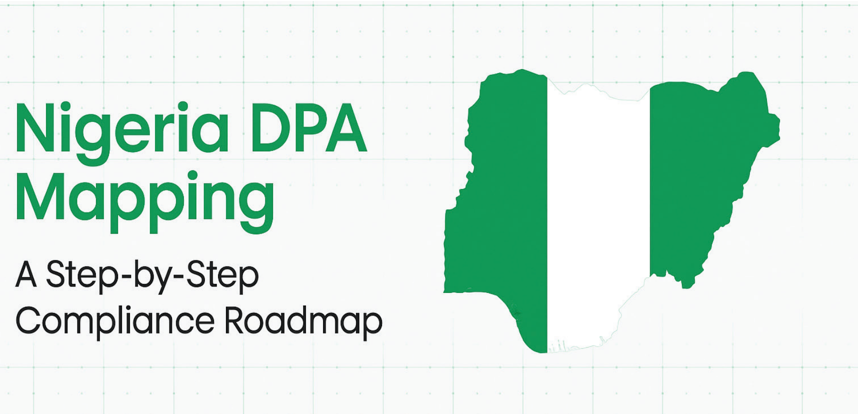
Nigeria's Data Leader Unite for Automation-First NDPA Compliance Webinar Hosted by Platview

Nigeria Data Leaders

Lagos, Nigeria: With the Nigeria Data Protection Act (NDPA) reshaping the country's regulatory landscape, Platview Technologies Ltd organized a strategic webinar on April 9, 2025, to help businesses navigate compliance using cutting-edge automation tools. Titled "Protecting Data, Avoiding Penalties: The Critical Role of Automation in NDPA Compliance," the session was powered by leading data privacy vendor Securiti.ai.

The session opened with a warm welcome address by Olawunmi Hassan-Faduola of Platview Technologies, setting the tone for an engaging and insightful event.

The virtual event brought together data protection officers, CISOs, compliance leaders, and IT professionals from across Nigeria to explore how automation can reduce compliance risks, lower operational burden, and ensure alignment with NDPA mandates.



Tahir Latif, a globally renowned expert in AI Governance and Data Privacy, headlined the session. With deep experience advising governments and global enterprises, he offered practical strategies for integrating ethical AI and privacy-by-design principles into compliance programs.

Tahir Latif

C-SUITE STRATEGIC AI GOVERNANCE & DATA PRIVACY ADVISOR

Prashanth Manchaiah, CISSP, CIPM (IAPP), presented an overview of Securiti.ai's Data Command Center and its role in automating NDPA compliance. He also delivered a live demo, highlighting real-time capabilities in data mapping and privacy operations.

Webinar Highlights Included:

Clear breakdown of NDPA's key requirements and penalties
. Real-world challenges of manual compliance and how automation solves them
. A live showcase of Securiti's AI-powered Data Command Center
. Strategies for managing cross-border data flows, regulatory scrutiny, and digital sovereignty

Attendees also gained insight into Nigeria DPA Mapping, understanding how local organizations must adapt data practices to meet legal obligations.

Why This Matters:

With the NDPA now in effect, Nigerian organizations face rising expectations around data protection. The webinar underscored automation as a key enabler of scalable, proactive, and cost-effective compliance.

Platview's initiative reflects its growing role in empowering Nigerian businesses to stay ahead of evolving regulatory frameworks and digital transformation trends.

SECHPOINT
Be secured

We Don‘t Just Defend We Innovate, Collaborate & Elevate Africa’s Digital Future.

Core-Tech Cyber Technology

IDENTITY & ACCESS MANAGEMENT

- PingIdentity
- ForgeRock
- SailPoint
- Saviynt
- pathlock
- CYBERARK
- Kron

DATA SECURITY

- Fortanix
- KEYFACTOR
- SECLORE
- fileorbis
- securiti
- mage data
- Kron
- OVALEDGE

SECURITY OPERATIONS

- Gurucul
- HORIZON3.ai
- positive technologies
- corelight
- JetPatch
- PENTERA

INFRA & NETWORK SECURITY

- HPE aruba networking
- FORESCOUT
- CERTES
- Array
- SECURE DOMAINS
- THREATLOCKER

CLOUD SEC

- AXONIUS
- AppOmni
- WIZ
- wallarm

CONSULTING & INTERNAL AUDIT

- protiviti

GOVERNANCE RISK & COMPLIANCE

- metricstream

Sechpoint Technologies
Unit 1109, Preatoni Tower, Cluster L, JLT, Dubai - UAE

Sechpoint Technologies Kenya Limited
Unit 402, 4th Floor, Eden Square, Chiromo Road
P.O. Box 856-00606, Nairobi - Kenya

sales@sechoint.com