BRIAC X

CLASSIFICATION
TLP:CLEAR — Public release

REFERENCE
BX-TB-2026-001

ISSUED
April 2026

THREAT BRIEF 2026 · AFRICAN FINANCIAL SECTOR

The continent is online. The *defenders* are not caught up yet.

An assessment of the cyber threat landscape facing African banks, mobile money operators, fintechs, and the public-sector institutions that depend on them — and what changes in 2026.

BRIAC X — Bureau de Recherches en Intelligence Artificielle & Cybersécurité
Douala · Abidjan · Lagos
research@briacx.com

Vol. 01 / 2026
First edition

FOREWORD / 00

A note from the desk of the CEO.

This brief exists because nobody else was going to write it for us.

For the last decade, the cyber threat landscape facing African institutions has been reported on by foreign vendors, foreign think tanks, and foreign press — using foreign frameworks, foreign vocabulary, and a foreign sense of what matters. The intelligence is often correct. It is rarely useful. A Lagos-based bank does not need a 200-page report on Russian state actors targeting Eastern European energy grids. It needs to know what is currently being thrown at *its* mobile banking stack, by whom, with what tools, and what to do about it before Friday.

BRIAC X publishes this brief because we are in the rooms where these incidents are handled. Our engineers have responded to credential-stuffing campaigns against pan-African fintechs, hardened mobile money APIs that were exposing PII through misconfigured object storage, audited SWIFT corridors at second-tier banks, and built fraud-detection models on top of transaction data that no foreign vendor will ever see. This document is what we know, written for the people who need to act on it.

We have one bias, and we will state it on the first page rather than hide it: **we believe that African institutions cannot defend themselves indefinitely with infrastructure they do not control, models they did not train, and audits performed by people who fly in for two weeks a year.** Sovereignty is not a slogan. It is an operational requirement. Every page that follows is written through that lens.

This is the first edition. It will be wrong about some things. We will publish corrections in the open. The next edition lands in October 2026.

Read it. Argue with it. Send it to your board.

— THE BRIAC X RESEARCH DESK

CONTENTS

SECTION 01

Executive summary.

Africa's financial sector is now a primary target rather than a secondary one — and its defenders are operating at a generation's disadvantage in tooling, talent, and intelligence.

Five years ago, an assessment of the African cyber threat landscape would have opened with the observation that the continent was largely a victim of opportunistic, untargeted commodity malware spilling over from campaigns aimed at Europe and the Gulf. That description is no longer accurate. In 2026, African banks, mobile money operators, fintech challengers, and the public-sector entities they connect to are targeted deliberately, by actors who have studied their specific weaknesses and built tooling for them.

Three structural shifts explain why. First, mobile money has crossed the threshold of being a national-scale payment rail in more than fifteen African countries, which means a single API surface now sits between criminal actors and the disposable income of hundreds of millions of people. Second, the rapid digitization of public services — tax filing, civil registry, customs, social transfers — has created a class of state-operated platforms that were built fast, by mixed teams, with security as an afterthought. Third, the talent gap on the defender side has widened rather than narrowed, because the same engineers who could harden these systems are being recruited out of the continent at salaries no local CISO can match.

The threat actors exploiting this gap are no longer a homogeneous group. We track activity from at least four distinct categories: financially-motivated organized crime running industrialized fraud operations against mobile money flows; access brokers selling persistent footholds inside African banks to ransomware affiliates operating out of Eastern Europe and South-East Asia; state-aligned espionage actors targeting public-sector communications and the supply chains that serve them; and a growing population of technically capable insiders monetizing their access through closed Telegram and WhatsApp markets.

The defenders, meanwhile, are over-dependent on three categories of tooling that were not designed for the African operational reality: enterprise security suites priced for European procurement budgets and licensed in ways that make local talent dependent on foreign engineers to operate them; cloud security services hosted in regions outside the continent, creating both latency and jurisdictional exposure; and threat intelligence feeds whose coverage of African threat activity is, in our direct experience, poor to non-existent.

The opportunity in 2026 is this: the institutions that recognize this gap and invest in sovereign defensive capability — meaning local talent, local tooling, locally-trained models, and intelligence written for their specific reality — will pull decisively ahead of peers that continue to import their security posture wholesale. The institutions that do not will discover, in the worst possible way, that nobody is coming to save them.

> BOTTOM LINE
>
> The African financial sector is being targeted with a sophistication that its defensive posture was not designed to absorb. The next 18 months will separate the institutions that adapt from the ones that become

case studies.

SECTION 02

Methodology and scope.

This brief is an open-source assessment, not a confidential incident dossier. It is grounded in publicly-available reporting and cross-checked against BRIAC X's own field observations from engagements conducted across West, Central, and East Africa.

Sources

This assessment synthesizes four categories of input. First, public reporting from international bodies including Interpol's African Cyberthreat Assessment series, the African Union's Malabo Convention secretariat, ENISA, and the threat intelligence publications of major vendors where their data covered African geographies. Second, the public disclosures, regulatory filings, and press communications of African financial institutions and regulators including BCEAO, BEAC, the Central Bank of Nigeria, the Central Bank of Kenya, and the South African Reserve Bank. Third, monitoring of the open and semi-open criminal ecosystem, including underground forums, Telegram channels, and marketplaces where access to African institutional targets is bought, sold, or advertised. Fourth, the anonymized, aggregated observations of BRIAC X's own engagements with clients in financial services, telecommunications, and the public sector, contributed only where doing so does not compromise client confidentiality and only in non-attributable form.

What this brief is not

This is not a tactical incident report. We do not name specific compromised institutions, we do not attribute incidents to specific named threat actors where attribution is not publicly established, and we do not publish indicators of compromise that could be operationalized by an adversary against a third party. Defenders who require tactical intelligence at that level should engage us directly through a research subscription or an active engagement.

Scope

Geographically, this edition focuses on the financial ecosystems of fifteen African countries where BRIAC X has either current operational presence, prior engagement experience, or sustained intelligence visibility: Cameroon, Côte d'Ivoire, Senegal, Nigeria, Ghana, Togo, Benin, Burkina Faso, Mali, Gabon, Republic of Congo, Democratic Republic of Congo, Kenya, Rwanda, and South Africa. We make no claim of representativeness for other geographies. Sectorally, we cover commercial banking, mobile money operators, fintech and neo-banks, payment service providers, microfinance institutions, and the public-sector entities that interconnect with them — tax authorities, customs, civil registry, and social transfer programs.

Confidence levels

Where this brief makes a forward-looking judgment, we use a three-level confidence scale. **High confidence** indicates an assessment we are willing to bet operational decisions on. **Moderate**

confidence indicates an assessment supported by multiple independent indicators but with material uncertainty. **Low confidence** indicates a hypothesis we consider plausible and worth tracking but for which the evidence is partial. Readers should treat these labels as load-bearing.

Honesty clause

Where we do not know something, we say so. Where we have changed our assessment between drafts, we say so in the corrections appendix of subsequent editions. Where a finding could be misread to favor BRIAC X commercially, we have asked an external reviewer outside the firm to challenge it before publication. The list of reviewers will be published in the second edition once they have agreed to be named.

SECTION 03

The 2026 landscape, in nine numbers.

A snapshot of the operating environment, drawn from public reporting and BRIAC X field observations. Each number is a starting point for a longer conversation, not a conclusion.

15+

AFRICAN COUNTRIES WHERE MOBILE MONEY IS NOW A SYSTEMICALLY-IMPORTANT PAYMENT RAIL

3×

ESTIMATED GROWTH IN PUBLICLY-DISCLOSED CYBER INCIDENTS AGAINST AFRICAN FINANCIAL INSTITUTIONS, 2022 → 2025

~70%

SHARE OF AFRICAN INTERNET USERS WHO ACCESS FINANCIAL SERVICES EXCLUSIVELY FROM A MOBILE DEVICE

<1%

SHARE OF GLOBAL THREAT-INTELLIGENCE REPORTING THAT MEANINGFULLY COVERS AFRICAN-SPECIFIC ACTOR ACTIVITY

9—18

MONTHS: TYPICAL PROCUREMENT CYCLE FOR A PUBLIC-SECTOR CYBERSECURITY ENGAGEMENT ON THE CONTINENT

2wks

MEDIAN TIME REQUIRED BY AN ORGANIZED FRAUD CREW TO OPERATIONALIZE A LEAKED MOBILE MONEY API KEY

~4×

TYPICAL PREMIUM CHARGED BY FOREIGN INTEGRATORS VERSUS A COMPARABLE LOCAL TEAM FOR EQUIVALENT SCOPE

0

NATIONAL CERTS ON THE CONTINENT THAT BRIAC X CONSIDERS FULLY RESOURCED FOR INCIDENT RESPONSE AT SCALE

1

NUMBER OF STRUCTURAL SHIFTS THAT MATTERS MORE THAN ALL OF THE ABOVE: THE CONSOLIDATION OF AFRICAN PAYMENTS ONTO A SMALL NUMBER OF API SURFACES OPERATED BY ENTITIES WHOSE SECURITY POSTURE NOBODY OUTSIDE THEIR OWN FIRM CAN INDEPENDENTLY VERIFY.

Note on figures. Quantitative values in this section are BRIAC X analytical estimates synthesizing public reporting and field observation. They are deliberately expressed as ranges or rounded approximations to discourage false precision. Readers requiring underlying source decomposition can request it from research@briacx.com.

SECTION 04

Top threat vectors of the year.

Seven categories of activity that BRIAC X assesses as the highest-priority concerns for African financial defenders in 2026, ranked by a combination of frequency, impact, and the gap between the threat and the prevailing defensive response.

TV-01 / 2026

SEVERITY: CRITICAL

Industrialized fraud against mobile money APIs

Targets: MMO platforms, agent networks, PSPs **Actors:** Organized financial crime **Confidence:** High

The single most consequential category of attack on the continent. Organized crews — most operating from within the continent, some from external diaspora hubs — have moved beyond opportunistic SIM swap and social engineering into systematic exploitation of the API layer that sits between mobile money operators, agent applications, and merchant integrations. The pattern we observe in engagements is consistent: an initial foothold via a leaked operator credential or a misconfigured staging environment, followed by quiet enumeration of internal APIs over several weeks, followed by a short, high-velocity cash-out window in which thousands of transactions are pushed through agent floats before detection thresholds trip.

The defensive failure is rarely at the cryptographic layer. It is at the business-logic layer: rate-limiting that doesn't account for legitimate burst traffic, fraud rules written against last year's typology, and detection telemetry that lives in three different systems no human is correlating in real time. Most affected operators discover the loss in reconciliation, hours or days after the window closes.

TV-02 / 2026

SEVERITY: CRITICAL

Initial access brokerage targeting second-tier banks

Targets: Tier-2 commercial banks, microfinance **Actors:** Access brokers + ransomware affiliates **Confidence:** High

The largest African banks have, broadly, invested enough in perimeter defense to make direct intrusion expensive. The economic logic of the criminal ecosystem has therefore shifted one tier down. We observe sustained reconnaissance and access-selling activity targeting second-tier commercial banks and the larger microfinance institutions, where security budgets are an order of magnitude smaller and where the same SWIFT-adjacent and core-banking systems remain accessible. Footholds are typically obtained through phishing of relationship managers, exploitation of unpatched edge devices (VPN concentrators and email gateways are the recurring offenders), and credential reuse from third-party breaches. Once inside, the foothold is groomed for several weeks and then sold — increasingly to ransomware affiliates who have noticed that African mid-tier banks pay quietly to avoid reputational damage and regulatory scrutiny.

TV-03 / 2026

SEVERITY: HIGH

Mobile banking trojans on Android

Targets: Retail banking customers **Actors:** Commodity malware operators **Confidence:** High

The continent's overwhelmingly Android-first mobile market is the natural habitat for banking trojans, and the families targeting African banks have multiplied. The technical innovation in this category is modest — most are forks of long-established overlay-attack frameworks — but the localization is improving fast. We observe campaigns with overlays customized for specific local banks, social-engineering scripts written in regional languages and mixing French and English in ways that match how customers actually communicate, and distribution through cracked APK marketplaces and WhatsApp forwards rather than the Play Store. The defensive response from most banks remains a customer-education campaign and a fraud rule, neither of which scales against a population of millions of low-literacy users.

TV-04 / 2026

SEVERITY: HIGH

Supply-chain compromise via foreign integrators

Targets: Public sector, Tier-1 banks **Actors:** Mixed — opportunistic and state-aligned **Confidence:** Moderate

The most awkward threat in this brief, because the solution to it is structural rather than technical. African Tier-1 institutions and public-sector platforms have, across the last decade, accumulated a sprawling vendor footprint of foreign integrators, software resellers, and managed service providers — most of whom hold privileged remote access into client environments and operate from jurisdictions with limited enforcement reach. We have observed multiple incidents in which the initial intrusion vector was not the bank itself but a regional partner of a global vendor whose credentials were used to pivot into the client environment. Attribution is hard. The defensive lesson is not — privileged third-party access is the single largest underestimated risk in the African Tier-1 environment, and almost no client we have engaged has a credible inventory of who can reach what, from where, with what credentials, under what audit.

TV-05 / 2026

SEVERITY: HIGH

Insider monetization through closed messaging markets

Targets: Banks, MMOs, telcos **Actors:** Technical insiders + recruiters **Confidence:** High

A category that under-features in foreign reporting because it is invisible from outside the continent. We track sustained recruitment activity in closed Telegram and WhatsApp groups offering significant cash sums to technically-positioned employees of African banks, mobile money operators, and telcos in exchange for specific actions: lookups against customer records, SIM swap approvals, KYC overrides, the planting of an agent account, or one-time access to a specific internal tool. The pricing is granular and competitive. The recruiters are patient, and increasingly use the same engineering-recruiter playbook a legitimate firm would — LinkedIn outreach, referral bonuses, multi-step interviews — making it harder for compliance teams to distinguish recruitment from grooming. Insider risk programs at most clients we have audited are still designed around the threat model of a single rogue employee, not a labor market.

TV-06 / 2026

SEVERITY: ELEVATED

LLM-enabled social engineering at scale

Targets: Retail customers, RM teams, treasury **Actors:** All categories **Confidence:** Moderate

The arrival of capable, cheap large-language-model tooling has not produced the new class of attack many predicted. What it has done is collapse the cost of running existing attack patterns at much higher quality and much greater volume. We observe phishing pretexts written in flawless French and English (where the same campaigns last year were detectable on linguistic markers alone), voice-cloning used in authorized-payment fraud against treasury teams at mid-sized corporates, and customer-impersonation chatbots deployed against bank call-center agents to extract account information. The defensive response — training, callback procedures, voice-biometric tooling — exists but has not been deployed at scale in the African context. We assess this as an elevated rather than critical category in 2026, but expect it to shift to critical in the 2027 edition.

TV-07 / 2026

SEVERITY: ELEVATED

Public-sector platform exposure

Targets: Tax, customs, civil registry, social transfer **Actors:** Mixed — espionage and crime **Confidence:** Moderate

Africa's wave of public-sector digitization has produced a generation of state-operated platforms holding citizen-scale datasets — tax records, passport applications, social transfer rolls, customs declarations, electoral rolls — running on infrastructure built quickly, often by mixed teams blending an in-country IT department with one or more foreign software vendors, almost always without an independent security review prior to launch. We have observed several public disclosures and a larger number of non-public incidents in which such platforms were found to be exposing data through trivial misconfigurations: open object storage buckets, predictable resource identifiers, debug endpoints reachable from the public internet. The threat is both criminal (these datasets are a goldmine for identity fraud) and political (the same datasets are of standing interest to foreign intelligence services). The defensive gap is not technical sophistication — the fixes are usually one-week engineering tasks — it is the absence of a procurement model that requires independent audit before launch.

SECTION 05

Sector deep-dives.

A condensed view of the threat profile, defensive maturity, and 2026 priority for each major sector covered by this brief.

SECTOR	DOMINANT THREAT PROFILE	DEFENSIVE MATURITY	2026 PRIORITY INTERVENTION
Tier-1 commercial banks	Supply-chain compromise via privileged third parties; insider recruitment; targeted ransomware	● Moderate	Third-party access inventory and segmentation; insider risk program redesign around labor-market threat model
Tier-2 banks & microfinance	Initial access brokerage; phishing of relationship managers; unpatched edge infrastructure	● Low to moderate	Edge-device hygiene program; managed detection and response; tabletop exercises against ransomware playbook
Mobile money operators	Industrialized API fraud; agent collusion; reconciliation gaps	● Moderate (uneven)	API surface threat-modeling; real-time fraud detection on the business-logic layer; reconciliation acceleration
Fintech challengers & neo-banks	Credential stuffing; supply-chain compromise via SaaS dependencies; KYC bypass	● Variable	Authentication hardening; SaaS dependency audit; bot detection at the application layer
Telecommunications operators	Insider-enabled SIM swap; signaling fraud; lawful-intercept abuse	● Moderate	SIM swap workflow re-engineering; signaling firewall deployment; access governance for sensitive subsystems
Public sector — financial	Platform exposure; state-aligned espionage interest; politically-motivated disruption	● Low	Mandatory pre-launch security review; sovereign hosting evaluation; CERT capacity-building
Payment service providers	API abuse; merchant-side compromise propagation; card-not-present fraud	● Moderate	Merchant onboarding hardening; behavioral fraud models; PCI-DSS continuous compliance

Reading the maturity column: ● High · ● Moderate · ● Low. Maturity here refers to the gap between the prevailing defensive posture in the sector and what BRIAC X assesses as adequate for the 2026 threat profile — not to the absolute sophistication of any individual institution within the sector, several of which are operating at international standards.

The two sectors that worry us most

If forced to pick the two sectors where the gap between threat and defense is widening fastest in 2026, BRIAC X would name **Tier-2 commercial banks** and **public-sector financial platforms**. The reasoning is structural rather than technical. Tier-2 banks face the same threat model as Tier-1 institutions — they hold the same SWIFT credentials, the same core-banking systems, the same

regulatory exposure — at a fraction of the security budget and without the in-house talent depth to compensate. They are the soft underbelly of the African banking system and the segment most likely to produce a publicly-visible incident in the next 18 months.

Public-sector financial platforms, meanwhile, suffer from a procurement pathology: the security budget is allocated, when it is allocated at all, after the platform has launched, and is sized against the cost of the build rather than against the cost of an incident. The fix is governance, not engineering. Until pre-launch independent security review becomes a hard gate in public procurement, these platforms will continue to ship into production with vulnerabilities that a competent reviewer would have flagged on day one.

SECTION 06

The sovereignty problem.

The hardest problem in African cybersecurity in 2026 is not technical. It is the question of who controls the infrastructure, the tooling, the models, and the people who defend the continent's institutions — and what happens when the answer is "almost nobody on the continent."

Four uncomfortable observations

First, the dominant security tooling deployed in African Tier-1 environments is licensed from a small number of vendors headquartered outside the continent, operated by engineers trained outside the continent, and updated through channels that depend on the continued goodwill of those vendors and their home governments. This is not a hypothetical concern. The history of the last decade includes multiple instances in which technology services to specific countries were curtailed for geopolitical reasons unrelated to the institutions affected. African defenders have built defensive postures whose continuity depends on assumptions about international relations that they themselves cannot influence.

Second, the data on which fraud-detection and risk models are trained increasingly leaves the continent for processing — sometimes contractually, sometimes through SaaS dependencies that nobody in the procurement chain understood would result in transit. Once that data is outside the continent's jurisdictional reach, it is, for practical purposes, no longer under the institution's control. Recovery of that data after a vendor incident, or after a change in vendor terms, is something we have never seen successfully accomplished by an African client.

Third, threat intelligence — the specific knowledge of who is currently targeting whom, with what tools, from where — is overwhelmingly produced and curated outside the continent, and reflects the priorities of the markets that pay for it. The result is that an African CISO subscribing to a Tier-1 commercial threat feed receives detailed reporting on threat actors targeting Western European banks and almost nothing on the actors actively targeting their own institution. We do not say this with any pleasure: the foreign feeds are often technically excellent. They are simply pointed at someone else's problem.

Fourth, and most consequentially, the engineers capable of operating sophisticated security tooling — performing red-team exercises, building detection content, training models, responding to incidents at speed — are scarce on the continent and are being recruited away from it at rates no local employer can match. The institutions that train them rarely retain them. The institutions that hire them rarely train them. The resulting equilibrium is a population of African CISOs running mature programs with rotating teams of mid-level engineers backed by expensive foreign consultants flown in for set-piece exercises.

> THE BRIAC X POSITION
>
> None of these four observations imply that African institutions should refuse to use foreign vendors, foreign tooling, or foreign intelligence. They imply that these inputs should be one component of a defensive posture whose foundations — talent, intelligence, and ideally tooling — sit on the continent and are operated by people who answer to local leadership. This is what we mean by sovereignty. It is a structural goal, not a slogan, and it will take a decade of deliberate investment to achieve.

What sovereign defense looks like in practice

A sovereign defensive posture, in BRIAC X's working definition, has five characteristics. The institution can operate its primary defensive controls without dependency on a single foreign vendor's continued goodwill. The institution has independent telemetry of its own environment, retained on infrastructure within its jurisdictional reach. The institution has at least one in-house team capable of incident response without external escalation for the first 72 hours. The institution has access to threat intelligence that specifically covers the actors targeting its own ecosystem, written by people who understand that ecosystem. And the institution's machine-learning models for fraud, risk, and detection are trained on its own data, by engineers it employs, on infrastructure it controls.

Almost no African institution we have engaged meets all five criteria today. We assess that the institutions that move deliberately toward this profile across 2026–2028 will define the next generation of African digital infrastructure. The institutions that do not will eventually discover, in circumstances they did not choose, what dependency costs.

SECTION 07

What 2026 will demand of defenders.

Five shifts BRIAC X expects to see in capable defensive programs over the next twelve months. Some are already underway. None are optional.

01 **Continuous offensive testing replaces annual penetration tests.** The annual pentest, scheduled, scoped, and reported to the regulator, has become a compliance ritual disconnected from the actual threat tempo. Capable institutions are moving to continuous red-teaming — a small, persistent offensive function that probes the environment week after week, surfaces issues in real time, and is measured on time-to-detection rather than vulnerability count. This is the single most consequential operational shift on this list.

02 **Detection content is written locally, not imported.** Off-the-shelf detection rules from international vendors do not catch the attack patterns we observe in African environments because those patterns were not in the training data. Mature programs in 2026 will employ at least one detection engineer whose full-time job is writing and tuning content against the specific telemetry of their own environment.

03 **Third-party access is treated as the primary attack surface.** Inventory of who can reach what, from where, with what credentials, under what audit — and aggressive reduction of that inventory — becomes a board-level metric, not a quarterly governance task.

04 **Fraud and security functions converge.** The historical separation between the fraud team (sitting under the COO) and the security team (sitting under the CIO or CISO) is incompatible with the threat model. Industrialized fraud is a security incident with a financial settlement attached. The institutions that recognize this and merge the two functions, or at least force them to share telemetry and on-call rotation, will detect incidents that the others will reconcile after the fact.

05 **Sovereign capability is built deliberately, not accidentally.** Talent pipelines, in-house intelligence functions, locally-trained detection models, and the infrastructure to run them: each requires a multi-year investment that does not pay back in a single budget cycle but compounds dramatically over three. The institutions that start in 2026 will be unrecognizable by 2029.

SECTION 08

Recommendations, by buyer profile.

Concrete next steps for the four reader profiles BRIAC X wrote this brief for. None of these recommendations require BRIAC X specifically — they require seriousness.

If you are a CEO or board member of an African financial institution

Stop treating cyber as an IT line item. Move it to a standing board agenda item, with quarterly briefings, and require your CISO to present in plain language without slides full of acronyms. Demand a third-party access inventory within 90 days; if your CISO cannot produce one, that is the finding. Ask one question that almost no board asks: *"If our primary security vendor became unable or unwilling to support us tomorrow, how long until we are operating blind?"* The answer will surprise you, and the discomfort it produces is the point.

If you are a CISO or head of security

Three priorities for the next 180 days. One: commission an independent red-team exercise scoped against the threat profile in this brief, not against last year's compliance checklist. Two: stand up — even at minimum viable scale — a detection-engineering function staffed by people who write content for your environment specifically. Three: begin the conversation with leadership about sovereign capability, framed as risk reduction, not as nationalism. The vocabulary matters; "operational independence" lands better than "sovereignty" with most boards.

If you are a regulator or central bank

The most valuable thing you can do in 2026 is mandate independent pre-launch security review for any public-sector or systemically-important financial platform. This single requirement, properly enforced, would close more vulnerability than any amount of post-incident enforcement action. Beyond that: invest in CERT capacity, fund threat-intelligence sharing across institutions in your jurisdiction, and create a safe-harbor framework for responsible disclosure that protects researchers acting in good faith. The continent's defensive posture is held back as much by the absence of these structures as by any technical gap.

If you are a founder or operator of an African fintech

You are building on infrastructure that will be targeted. Bake the assumption into your architecture from day one. Specifically: deploy authentication that is resistant to credential stuffing before you need it (not after), instrument your business logic with telemetry rich enough to detect anomalous patterns at the API layer, audit your SaaS dependency tree at least quarterly, and treat your KYC pipeline as a security control rather than a compliance checkbox. The fintechs that reach scale on the continent in the next five years will be the ones that survived the first serious attempt to break them — that attempt is coming, sooner than you expect.

A FINAL NOTE

BRIAC X publishes this brief for free because we believe the conversation it provokes is more valuable than the engagements it might generate. If it helped you, the most useful thing you can do is forward it to one peer who needs to read it. If it provoked you, write to us — corrections and disagreements will be acknowledged in the next edition.

SECTION 09

About BRIAC X.

BRIAC X is a Douala-based technology firm working at the intersection of applied artificial intelligence, software engineering, and offensive cybersecurity. We design, build, and defend the digital infrastructure of African institutions that cannot afford to fail.

Our practice

We work across three integrated disciplines — Defend, Intelligence, and Build — and most of our engagements span at least two of them. The integration is the point: an institution that engages us for a security audit leaves with a roadmap for the AI systems that will replace its highest-risk manual processes; an institution that engages us to build a mobile platform receives a hardened, model-augmented product on day one. We are not a security firm that also does software, or a software firm that also does AI. We are one practice with three disciplines.

Why we publish

This brief, and the other research BRIAC X publishes through its Field Notes program, exists because the African cyber conversation is missing a voice that is rigorous, locally-grounded, and willing to say uncomfortable things in public. We intend to fill that gap. Research is not a marketing function for us; it is an obligation we accept as part of operating on the continent.

How to engage

Institutions interested in working with BRIAC X — whether on a single diagnostic, a multi-month engagement, or a long-term retainer — can reach the firm at **hello@briacx.com**. Researchers, journalists, regulators, and peers wishing to discuss this brief, contribute corrections, or propose collaboration on the next edition can reach the research desk directly at **research@briacx.com**. PGP key and key fingerprint available on request.

Sovereign systems.
Built in Africa.
Engineered to outlast the threat.

THE FIRM PRACTICE CONTACT

BRIAC X — Bureau de Recherches en Intelligence Artificielle & Cybersécurité.
Headquartered in Douala, Cameroon.
Operating across West, Central, and East Africa.

Defend — offensive security & compliance.
Intelligence — applied AI & ML systems.
Build — production software engineering.

hello@briacx.com
research@briacx.com
+237 688 420 310
briacx.com