AQUARAH

Modern Vulnerability Management

IN PARTNERSHIP WITH

HCLSoftware

3Cs AQUARAH

Modern Vulnerability Management

About Us

3Cs Aquarah Limited is at the forefront of cybersecurity and cloud services innovation, dedicated to providing comprehensive cloud services & solutions while safeguarding your digital world.

Highly motivated experts, consultants and project team with diverse industry expertise & experience and solid track record of quality delivery.

Birth

Founded in 2002

Sectors

Financial Services, Manufacturing, Telcos and Public Enterprises

Focus

Technology company focused on Cloud Infrastructure and Cybersecurity Solutions & Services

Presence

Local in over 10 countries

IN PARTNERSHIP WITH

HCLSoftware

AQUARAH

Vision and Mission

Our Vision

To become Africa's foremost customer-centric technology company, leading the industry through excellence in customer service, innovation, and strategic solutions.

Our Mission

To redefine service delivery by placing our stakeholders at the heart of everything we do. We strive to empower businesses with innovative, robust, and adaptable security & cloud solutions, ensuring their digital journey is both successful and safe.

IN PARTNERSHIP WITH

HCLSoftware

3Cs AQUARAH

Presentation 1

The State of Vulnerability Management in Africa

Presented by Gideon

IN PARTNERSHIP WITH

HCLSoftware

3Cs AQUARAH

State of Vulnerability in Africa

Cybersecurity Threat Intelligence & Strategic Analysis

59	6	2.54B
CVEs Patched Feb 2026	Zero-Days Exploited	Threats Kenya Q1

Executive Summary

The Trillion-Dollar Security Gap

$1T+
Economic Risk

Unprecedented Volatility

Q1 2026 has inaugurated a period of unprecedented volatility in the African cybersecurity landscape. The collision of rapid digital acceleration and systemic infrastructure fragility has created a "Security Gap" that now represents a **trillion-dollar challenge** for African economies, threatening to undermine the digital trust bedrock of the continent's modernization.

Perimeter Collapse

The network perimeter has effectively collapsed under critical failures in Microsoft Windows, Cisco Unified Communications, and Fortinet identity management. The sheer volume of zero-day exploits signals a strategic shift where threat actors commoditize "skeleton key" exploits.

Geopolitical Dimension

The expansion of Sharp Dragon APT (China) into African government networks marks a pivotal evolution in cyber-espionage. Simultaneously, ransomware campaigns target South African logistics/healthcare while banking trojans besiege Nigeria's financial sector.

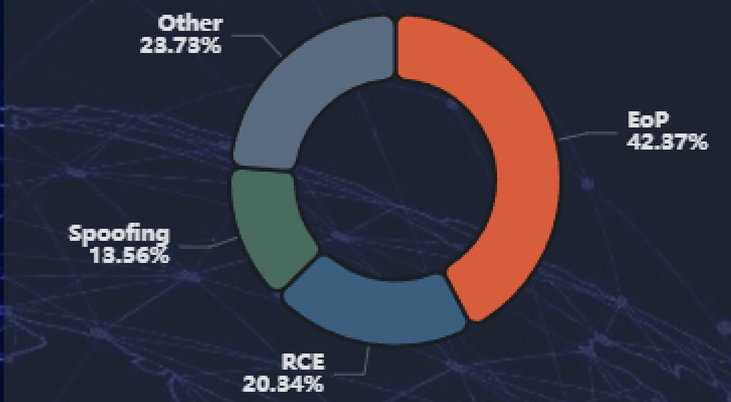
Strategic Shift in Attacker Methodology

Analysis of the 59 vulnerabilities patched in February 2026 reveals attackers now **assume initial access is inevitable**. The operational bottleneck has shifted from network penetration to privilege escalation, with 42% of patches addressing Elevation of Privilege vulnerabilities.

February 2026 Patch Tuesday

Total Vulnerabilities	59
Actively Exploited	6

Vulnerability Distribution



Key Insight: Elevation of Privilege vulnerabilities (42%) now dominate, indicating attackers focus on escalating privileges after initial compromise rather than perimeter breach.

3CS AQUARAH

Network Perimeter Collapse

Critical Infrastructure Under Siege

CVSS 9.8
Max Severity

MICROSOFT

CVE-2026-21533

7.8 CVSS

RDP Elevation of Privilege — Exploit binary modifies RDS service configuration keys in Windows Registry, granting NT AUTHORITY\SYSTEM privileges.

ACTIVE Since Dec 24, 2025

CISCO

CVE-2026-20045

9.8 CVSS

Unified CM Root Access — Code injection vulnerability allows unauthenticated remote attackers to achieve root privileges on voice infrastructure.

KEV CISA Catalog

FORTINET

CVE-2026-24858

9.4 CVSS

FortiCloud SSO Bypass — "Skeleton key" flaw allows any valid FortiCloud account to bypass authentication on target devices. Service suspended globally Jan 26 .

MSSP RISK Supply Chain

IVANTI

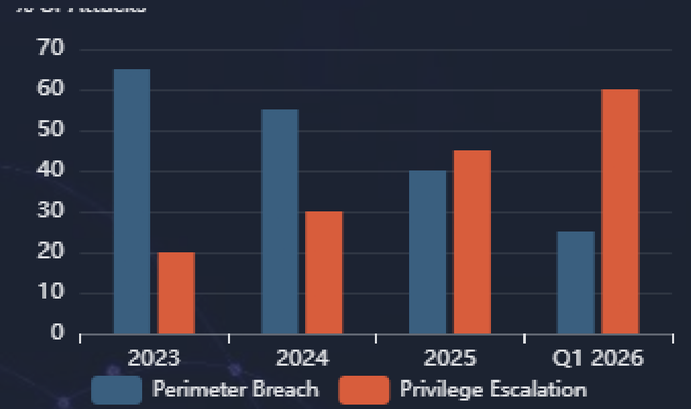
CVE-2026-1603

8.6 CVSS

EPM Auth Bypass — AuthHelper class exposes weak authentication path enabling credential harvesting. Domain Admin equivalence via service accounts.

LATERAL Movement

Attack Vector Shift



Vulnerability Severity Matrix

Critical	85%
High	65%
Medium	40%

42% EoP

20% RCE

Regional Impact: African Telecommunications at Risk

Cisco Unified CM is the **de facto standard** for corporate telephony across Africa. Root access enables real-time voice stream tapping, OTP interception bypassing 2FA, and lateral movement through Voice VLANs. Fortinet's ubiquity in SME/retail sectors creates massive supply-chain risk — a single compromised MSSP account could pivot into hundreds of client networks.

Insight: Attackers now treat initial access as solved; the battleground has shifted to privilege escalation and lateral movement.

AQUARAH

The Mobile Money Battleground

$500B+
Annual Transaction Volume

The "Big 4" Mobile Money Ecosystem

Africa's fintech landscape is dominated by **M-Pesa, MTN MoMo, Airtel Money, and Orange Money**, collectively processing nearly half a trillion dollars annually. As platforms transition from closed USSD systems to open API ecosystems, the risk has shifted from telco core to Third-Party Integrators .

M-Pesa	MTN MoMo	Airtel	Orange
East Africa	West Africa	Pan-Africa	Francophone

Mobile Money Transaction Flow

Mobile OS Vulnerabilities

SAMSUNG KNOX BYPASS
37 vulnerabilities patched Feb 2026. Biometric bypass allows thieves to drain accounts from stolen phones.

iOS ZERO-DAY
CVE-2026-20700 targets African elites. Commercial spyware (NSO Group) actively exploiting.

API & Logic Flaws

BOLA ATTACKS
Broken Object Level Authorization allows users to manipulate transaction/wallet IDs to access others' data.

OVERLAY ATTACKS
Android malware draws fake windows over legitimate apps to harvest PINs — rising in Kenya/Nigeria.

Threat Surface Expansion

API Endpoints **+340%**

Third-Party Integrators **+180%**

Attack Attempts **+520%**

USSD	Apps
More Secure	Higher Risk

Historical Context: The Pegasus Technologies Breach

The **2020 Uganda hack** of Pegasus Technologies compromised both MTN and Airtel money flows, serving as the watershed moment. As platforms integrate with banks, insurance, and lending apps via APIs (Safaricom's Daraja, MTN's Open API), the "Security Gap" arises — governance and security testing lag behind integration speed.

Critical: While USSD's session-based nature provides inherent security, the smartphone app shift exposes users to overlay attacks and malware.

AQUARAH

State-Sponsored Threats

Geopolitical Cyber Warfare

2.54B
Kenya Incidents

Sharp Dragon (China)

APT

The **most significant intelligence development** of Q1 2026. Formerly focused on Southeast Asia, this APT group has realigned to target African Ministries of Foreign Affairs and economic development agencies critical to Belt and Road Initiative.

TACTIC
Inter-Governmental Trust Phishing using compromised SE Asian gov emails

TOOL
Cobalt Strike Beacons (C2: 103.146.78.152) masquerading as JSON

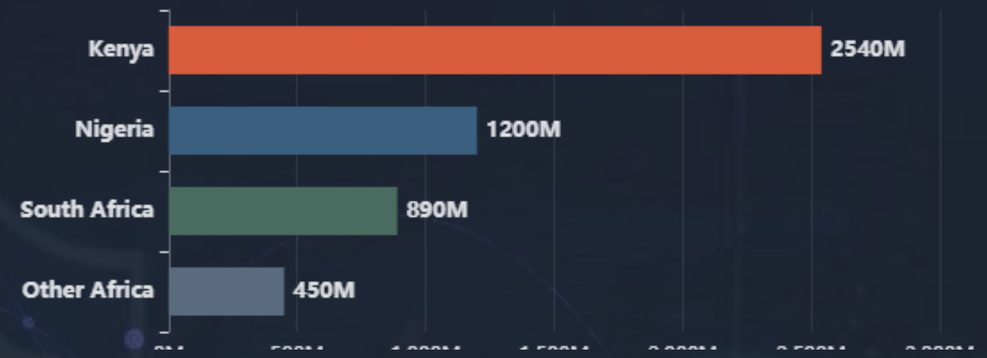
Russia: Africa Corps

WAGNER

In the Sahel and Sudan, Russian influence operations engage in "Total Reality Synthesis" — blending kinetic support with cyber-enabled disinformation. Ukrainian cyber specialists have assisted African nations in exfiltrating data from Russian encryption hardware.

SANDWORM (APT44)
Linked to disruptions in West African maritime logistics and insurance databases — using cyber-sabotage as economic warfare.

Country-Specific Threat Metrics



Regional Threat Breakdown

KE Kenya — CRITICAL

2.54 billion incidents in Q1 2026 (201% increase). PCP@Kenya group defaced ministries. PKI mandate issued for telecom operators.

NG Nigeria — HIGH

Banking trojan siege: Veeam ransomware (CVE-2023-27532), sophisticated vishing campaigns, M0yv malware from Maze creators.

ZA South Africa — ELEVATED

36% ransomware increase YoY. Rogers Capital Credit breach. Deepfake voice cloning targeting voice banking — projected R5B cost in 2026.

Strategic Assessment: Cyber operations in Africa are no longer just about crime — they are an extension of geopolitical statecraft . State-sponsored actors leverage cyber capabilities to secure strategic influence, mineral rights, and economic dominance.

Strategic Recommendations

Strategic Imperatives for Resilience

1 Immediate Technical Priorities

- **Patch the "Big Six" Zero-Days**
  Within 24 hours. If impossible, disable RDP or enforce VPN+MFA.
- **Sanitize Identity Layer**
  Global password reset for admin accounts. Invalidate all active SSO tokens.
- **Web Shell Hunting**
  Active hunt in c:\inetpub\wwwroot for files modified in Q1 2026.

2 Architectural Transformation

- **Adopt Zero Trust Network Access**
  Granular, real-time access decisions based on identity and device health.
- **Sovereign Cloud Strategy**
  Ensure data residency and legal jurisdiction remain within Africa.
- **API Security Governance**
  DAST/SAST testing and runtime protection to detect BOLA attacks.

From "Patch Management" to "Resilience Engineering"

The velocity of threats in Q1 2026 demands a **fundamental shift in defensive strategy**. Traditional patch management is no longer sufficient. Organizations must move toward Resilience Engineering — designing systems that can withstand, adapt to, and rapidly recover from attacks. This requires continuous threat hunting, identity-centric security, and the agility to survive the inevitable breach.

24h
Patch Window

Zero
Trust Model

Sovereign
Cloud First

Critical Vulnerability Matrix

CVE-2026-20045	RCE/Root	Cisco 9.8
CVE-2026-24858	Auth Bypass	Fortinet 9.4
CVE-2026-21510	Shell Bypass	Microsoft 8.8
CVE-2026-1603	Auth Bypass	Ivanti 8.6
CVE-2026-21533	RDP EoP	Microsoft 7.8

> **The "Zero Day" is no longer an anomaly; it is the baseline operating condition of the African digital landscape in 2026.**
>
> The goal is not **invulnerability**, but the agility to survive the inevitable breach.

Critical High Elevated

3Cs AQUARAH

Presentation 2

Managed Services Approach for SMEs

Presented by Emmanuel

IN PARTNERSHIP WITH
HCLSoftware

AQUARAH

Introduction

Small and medium-sized enterprises (SMEs) are not insignificant targets; in fact, 43% of cyberattacks are aimed at them, and cybercriminals often exploit known vulnerabilities through automated scanning.

SMEs often lack

- **Dedicated security teams**
- **Formal Patching Processes**
- **Continuous Monitoring**

AQUARAH

Vulnerability Management is NOT just Patching

AQUARAH

How SMEs Typically Handle Vulnerability

- Over-Reliance on Antivirus
- Reactive Patching
- No Asset Inventory
- One-time Scanning
- No Risk-based Prioritization

AQUARAH

Our Managed Vulnerability Management Value

01

DISCOVERY

Continuous discovery across infrastructure, endpoints, applications, and cloud

02

INSIGHT

Threat-informed prioritization enriched by operational security insights

03

COMPLIANCE

Remediation guidance, executive dashboards, and compliance alignment (NIST, ISO 27001)

04

CONTINUITY

Flexible co-managed model extending internal IT and security teams

3Cs AQUARAH

Thank you

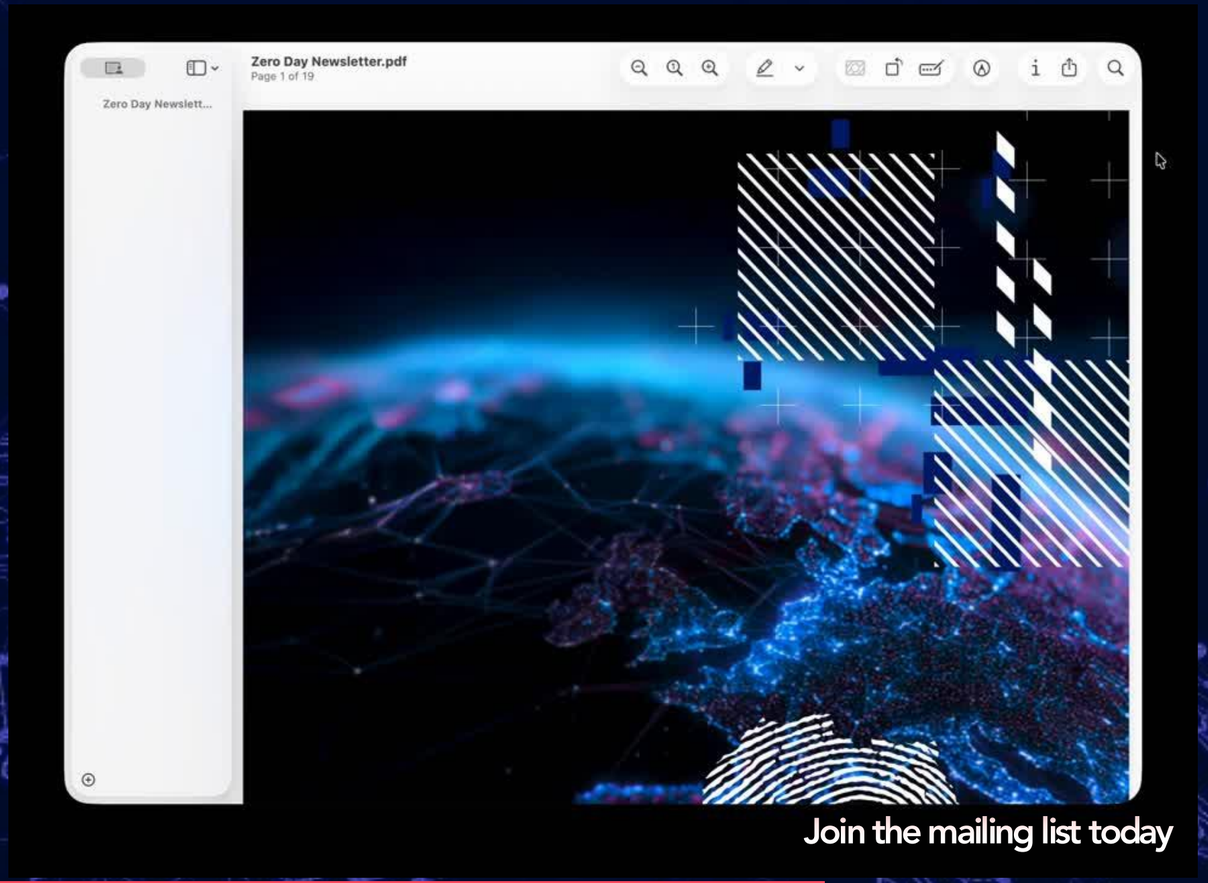
3Cs AQUARAH

Introducing

ZERO DAY AFRICA

Zero Day Africa is a digital cybersecurity report launched by 3Cs Aquarah, aimed at addressing the critical shortage of accessible, accurate, and contextually relevant information on cybersecurity incidents across the African continent

The report seeks to bridge this information gap by systematically documenting, explaining, and contextualizing cybersecurity events tailored to Africa's unique threat landscape and experiences, fostering greater adoption, resilience, and informed decision-making in the field.



Join the mailing list today

AQUARAH

Follow our platforms @3csaquarah

AQUARAH

Thank you