



Supporting Partner



Beyond Firewalls

Strategic Cyber Defence for a Digital Age

East Africa's premier cybersecurity summit bringing together C-level executives, technology leaders, and policymakers.

08 July 2026 | Nairobi, Kenya

An Initiative By



Community Partner



Government Endorsement



Keynote Speaker

**Col Dr James
Kimuyu**

Director

National Computer & Cybercrimes
Coordination Committee (NC4)



“

Safeguarding national cyberspace is not only a security imperative but a cornerstone for sustainable economic growth and digital resilience.

Cyberspace is now a central theatre of operations powering economies, governance and national security. As Kenya accelerates its digital transformation, the same ICT dependencies that enable innovation also introduce systemic vulnerabilities.

In response, the Government of Kenya has undertaken critical policy, legal, regulatory and institutional steps including the [Computer Misuse and Cybercrimes Act 2018](#) and the [National Cybersecurity Strategy 2022-27](#)

These interventions ensure protection and resilience of Critical Information Infrastructure, incident response, public safety, harmonized handling and prosecution of cybercrime and national security. Additionally, Kenya's aspiration to accede to the Budapest Convention on Cybercrime underscores its commitment to international cooperation and alignment with global best practices.

The Government continues to build capabilities for cyber threat monitoring, sector-specific training, incident response coordination and enhanced international partnerships.

Kenya welcomes global stakeholders to participate in [Cyber First East Africa 2026 on 08 July in Nairobi](#) a premier platform for cybersecurity dialogue, innovation and collaboration. NC4 affirms its mandate to ensure a secure cyberspace for Kenya and Its People..

Event Overview

Kenya has solidified its position as a digital powerhouse in Africa, with rapid innovations driving unprecedented economic inclusion.

Organizations are currently grappling with a severe **96% talent shortage**, with only 1,700 certified experts available to meet a national requirement of over 40,000. The rise of Agentic AI and Deepfakes has introduced a new era of 'Algorithmic Warfare' that legacy systems are ill-equipped to handle.

Over 4.5 billion cyber threats have been detected between October – December 2025. That is a 441% jump. 21.8 million security advisories sent out by KE-CIRT/CC for the need to patch systems, multifactor authentication, configure firewalls.

Cyber First East Africa 2026 serves as the definitive national nexus for C-level executives, technology leaders, and policymakers to synchronize efforts against a backdrop of escalating digital warfare. Scheduled for **08 July 2026, in Nairobi**, this summit is acting as a launchpad for forward-thinking strategies and tangible resilience in the Silicon Savannah. 2026 is the pivotal year where cybersecurity transitions from a side project to core infrastructure for Africa's digital economy.

Be a part of the Cyber First Movement and lead the charge toward a strategic, resilient and innovative economy!

Facts & Figures

247%

Cybersecurity incidents saw a 247% annual increase in 2025

46,786

In early 2025, Kenya recorded over 46,786 (1116%) DDoS incidents, the highest in East Africa and third highest on the continent.

19.95 million

Over 19.95 million advisories were issued in Q3 2025, a 15.53% rise, emphasizing proactive defenses.

95%

The healthcare sector experienced a 95% escalation in ransomware attacks, while manufacturing accounts for 26% of all ransomware incidents.

70.9 million

System misconfigurations remain a critical vulnerability, contributing to 70.9 million malware attacks.

KES 29.9 billion

Losses from cybercrime reached an estimated KES 29.9 billion in 2025.



Speakers



(Col) Dr James J. Kimuyu

Director

Kenyan National Computer and Cybercrimes
Coordination Committee (NC4)



George Kisaka

Vice President

ISACA Kenya Chapter



Michael Etale

Chief Information Security Officer

Absa Bank



Geoffrey O. OCHIENG

Global AI Delegate to Kenya

Global Alliance for AI

Global Ambassador

Global Council for Responsible AI



Hussein Omar Hussein

Director IT and Digital

SBM Bank Kenya



Rosemary Koech-Kimwatu

Head of Data Protection

KCB Bank Group



Frank Muriuki

CISO

Kenya Airport Authority



Peter Muhumuza

CISO

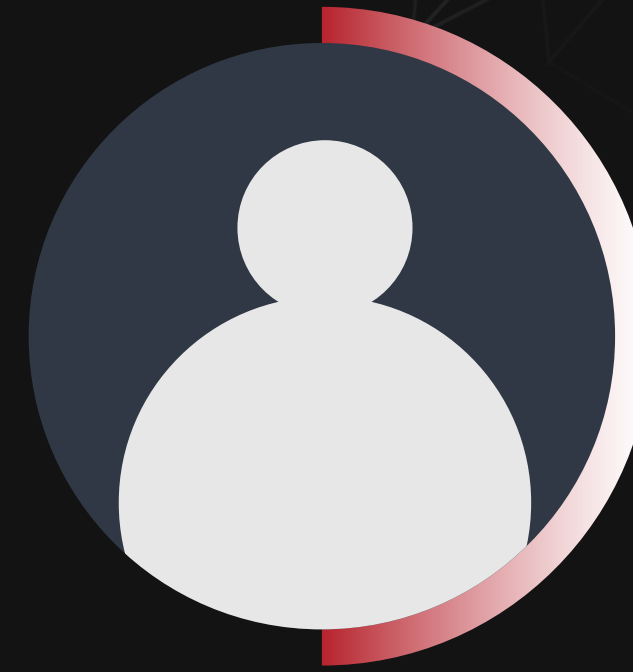
KCB Bank Uganda

Speakers



Steven Mwesige

Ag. Chief Information Security Officer
Pearl Bank Uganda



Dr. Isabelle K

Principal Officer | Frequency Spectrum
Communications Authority Of Kenya (Ca)

Market Drivers

Regulatory Momentum

The operationalization of the Computer Misuse and Cybercrimes (Amendment) Act 2025 has tightened legal definitions and formalized duties for platforms and ISPs. The operationalization of the Cyber Security Operations Centre (CSOC)

Strategic Funding

The launch of the KES 454 million EU-supported Kenya Cyber Resilience Project and World Bank funding for secure networks to enhance governance and incident handling. Catalyzing sector maturity, prominently driven by Microsoft's Advancing Regional Cybersecurity (ARC) Initiative launched to enhance incident response capabilities.

Corporate Investment

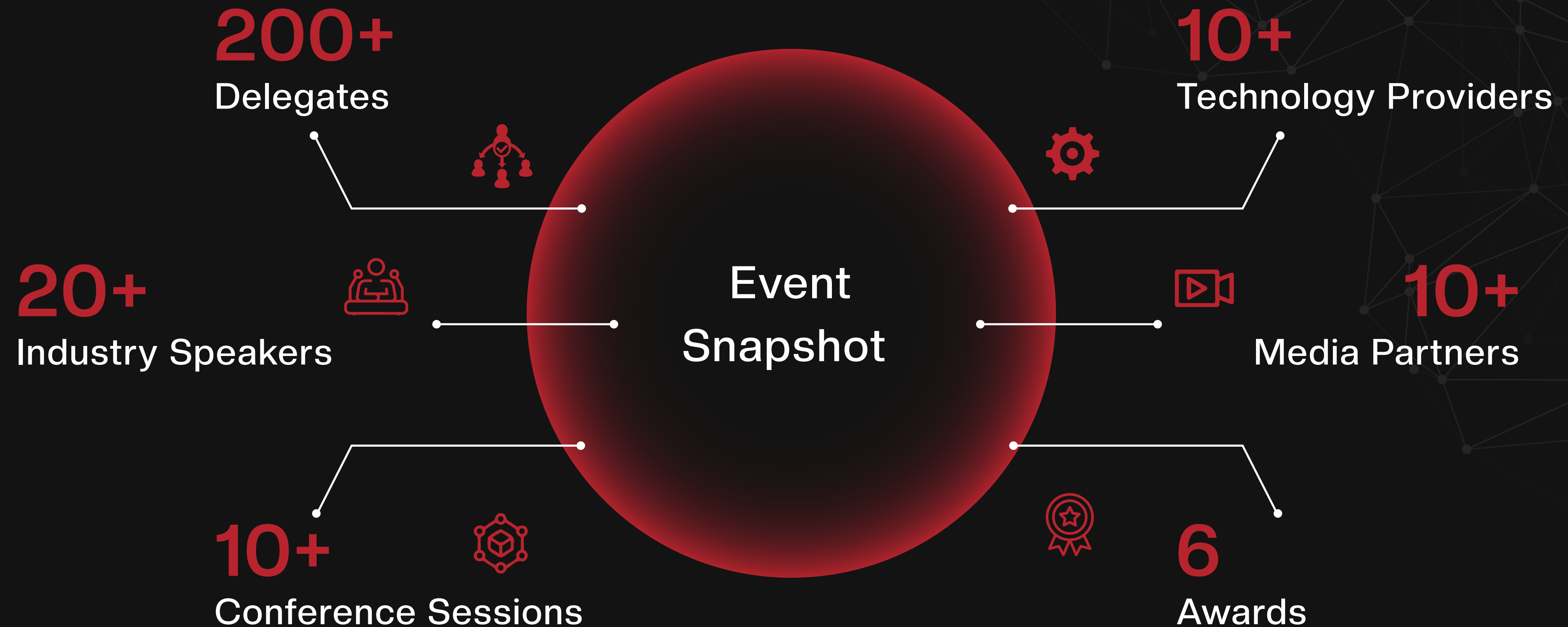
34% of Kenyan organizations plan to increase security budgets through 2026 to combat rising fraud and system disruptions.
Investments in digital infrastructure for secure networks and AI integration.

CyberGame for up skilling

Government-backed Cyber Game initiative starting March 2026 to build skills among students and professionals.



East Africa's Top 200+ Security Leaders



The market is projected to expand at a CAGR of 10.54% through 2029, reaching an estimated value of \$92.64 million.

Agenda

08:00 – 9:00

Registration, Networking, and Refreshments

09:05 – 09:10

Welcome Remarks

09:10 – 09:15

National Anthem and Opening Ceremony

09:15 – 09:30

Opening Keynote

The Digital Mandate Roadmap - NC4 and Kenya's Cyber Economy

Col Dr James Kimuyu - Director, National Computer and Cybercrimes Coordination Committee (NC4)

09:30 – 10:00

Leadership Panel

Who Owns the Risk? Boards, Regulators and CISOs under New Expectations

(Governance focused on accountability, reporting, and decision making for cyber risk across sectors, how responsibility is shared, what effective governance looks like in practice)

- Safeguarding national critical infrastructure and policy synchronization
- Regulatory expectations, audit findings, corrective action plans
- Third-party and supply chain risk management

10:00 – 10:15

Fireside Chat

The Sovereign Shield - Harmonizing Critical Infrastructure Defence under the CMCA 2025

(the tactical enforcement of the 2025 Amendment Act, focusing on how government agencies and regulators are transitioning from legislative theory to real-time website deactivation and threat containment)

Agenda

10:15 – 10:30

Technology Presentation

Using Endpoint and Network Telemetry to Spot Business Critical Attacks

(Reserved for Sponsor)

10:30 – 11:15

VIP Exhibition Tour followed by Networking & Refreshments

11:15 – 11:45

Panel Discussion

From Logs to Decisions - Making Threat Intelligence and Analytics Actionable

(how organizations can prioritize a small set of high-value detection and intel use-cases, instead of drowning in data and alerts)

- Identity centric defence for mobile money and digital channels
- Real time fraud and abuse detection across payment rails
- Endpoint and network protection in branch, agency, and shared-device environments
- Prioritizing data sources & automation boundaries

12:00 – 12:15

Technology Presentation

Behavioural Biometrics - The Next Frontier in Anti-Fraud for Digital Lenders

(Reserved for Sponsor)

12:15 – 12:45

Panel Discussion

Keeping the Lights On - Practical Resilience Against DDoS, Ransomware and Network Disruptions

(keeping critical services available under intense pressure and concrete strategies for maintaining availability of critical services under DDoS waves, network issues, and ransomware across sectors)

- Service classification - what must never go down, for how long
- Technology and process for DDoS mitigation on public services
- Ransomware preparation - segmentation, backup strategy, offline copies, recovery drills
- Interplay between physical incidents and cyber resilience

Agenda

12:45 – 13:00

Technology Presentation
Proactive Deception Strategies for Government Portals
(Reserved for Sponsor)

13:00 – 13:30

Networking Break and Refreshments

13:30 – 14:00

Panel Discussion
Identity Under Pressure - Stopping Fraud and Account Takeover in a Mobile First Economy

(how identity abuse drives fraud and disruption across mobile money, digital banking, telco services, and citizen portals)

- Real-time risk scoring for logins and transactions
- Coordinating fraud, cyber, and operations teams
- Securing agents and merchants in mobile money ecosystems
- Protecting privileged admin and operator accounts in telco/gov
- Handling identity in shared-device environments

14:00 – 14:15

Presentation
API Security at Scale - Protecting the Interconnected Ecosystem of the Silicon Savannah
(Reserved Session)

14:15 – 14:30

Cyber First Award Ceremony & Raffle Draw

14:30

Networking Lunch and End of Conference

**Kindly note: This is a draft agenda and is subject to minor changes until 4 days prior to the conference*

2026 Strategic Focus Areas

- **Safeguarding National Critical Infrastructure & Neutralizing Advanced Threats**
Formulating resilient defense mechanisms across critical sectors to combat Advanced Persistent Threats (APTs), ransomware proliferation, and high-volume DDoS attacks that exceed 1Tbps.
- **Regulatory Governance, Data Privacy, & Policy Synchronization**
Strategically aligning enterprise architectures with the Computer Misuse and Cybercrimes Act (CMCA) and national directives to ensure robust data privacy and legal compliance within Kenya's rapidly evolving digital economy.
- **Architecting Resilient Cloud Ecosystems & Operationalizing Zero Trust**
Eradicating implicit trust to combat advanced social engineering and insider threats, while securely navigating the migration to hybrid and public cloud environments against credential exploitation.
- **Cultivating the Human Defense Perimeter & Bridging the Talent Deficit**
Accelerating capacity-building models and institutional partnerships to transform the workforce into an active "human firewall," actively addressing the regional cybersecurity skills shortage.
- **Integrating Artificial Intelligence & Next-Generation Threat Intelligence**
Leveraging AI and emerging technologies for automated, proactive threat detection and incident response to outmaneuver algorithmic cyber-attacks.
- **Fostering Strategic Geopolitical Partnerships & Intelligence Synergy**
Driving regional and global collaboration frameworks to democratize actionable cyber intelligence and fortify a collective, cross-border defense posture.



Who Should Attend

Target Job Titles

Chief Information Security Officers (CISOs)
Chief Information Officers (CIOs)
Chief Risk Officers (CROs)
Heads of IT & Network Security
Data Protection Officers (DPOs)
Cybersecurity Engineers & Lead Architects
Governance, Risk, and Compliance (GRC) Directors
Cybersecurity Analysts and Specialists
IT Directors and Senior Managers
Government Officials and Policymakers
Compliance and Risk Professionals
Tech Innovators and Consultants



Who Should Attend

Target Industries

Banking and Financial Services
Government & Public Administration
Telecommunications and ICT
Healthcare & Pharmaceuticals
Energy and Infrastructure
Manufacturing & Supply Chain
E-commerce & Retail

Who Should Sponsor

Targeted Categories

IT Security Vendors
Digital Infrastructure Firms
International Development Agencies
Educational and Training Institutions
Consulting Services Providers
Managed Detection & Response (MDR) and
SOC-as-a-Service Providers
Cloud Security Solutions & Integration Architects
Threat Intelligence & External Attack Surface
Management Firms
Identity & Access Management (IAM) Vendors
Cybersecurity Training, Certification, and
Skilling Organizations

Series Sponsors



2026 Award Categories

Feb 4th, 2026 | Fairwood Hotel, Abu Dhabi

Join us as we celebrate the Cyber First 2026 Awards, honoring those who demonstrate outstanding excellence and innovation in operational practices. We'll shine a spotlight on the visionaries and organizations leading the way in technological advancements.

Cybersecurity Innovation Award - Recognizing groundbreaking solutions in threat detection and defence technologies.

Excellence in Cyber Resilience Award - Honouring organizations that have demonstrated robust recovery and adaptation to cyber incidents.

Emerging Cybersecurity Leader Award - Celebrating young professionals or startups making significant contributions to the field.

Public Sector Cybersecurity Achievement Award - Acknowledging government initiatives that enhance national digital security.

The Master of the Attack Surface (Zero Trust Pioneer) - This awards a C-suite leader or architectural team that has executed the most sophisticated, seamless implementation of Zero Trust Architecture, effectively neutralizing external and internal threats without hindering business operations.

The Sentinel of Critical Infrastructure - This is dedicated to a public sector entity, utility company, or financial institution that has implemented highly creative strategies to safeguard national data and physical infrastructure from disruption.





For Speaking Enquiries

Sanjana Venugopal

+971 50 500 3341

sanjana@eventsfirstgroup.com

For Sponsorship Enquiries

Mohammed Hassan

+971 50 140 1320

hassan@eventsfirstgroup.com

Mohammed Danish

+971 50 500 9655

danish@eventsfirstgroup.com