kenet
Kenya Education Network

Strengthening Kenya's Cybersecurity Posture

Inclusive Capacity Building Across Five Regions- Funded by ICANN Grant

A presentation by KENET

Opening Remarks

- Welcoming
- Introductions
  - Trainees/Participants
  - KENET Trainers
- House Keeping Matters

House Keeping

- Daily schedule Time – 8am – 4.30pm
- Wi-fi –
  - KENET – kenet@25
  - Eduroam
  - Conclave B – Abai@2021
- Breakout Rooms
  - Track 1 – Conclave D
  - Track 2 - Conclave B
- Workshop Resources

training.kenet.or.ke
training-labs.kenet.or.ke

Why are educational and research institutions in Kenya Key Targets for Cyber Criminals?

	%
A. Government agencies & services	17
B. Information technology	17
C. Research and academia	11
D. Non-governmental organizations	8
E. Critical manufacturing	6
F. Transportation systems	6
G. Consumer retail	6
H. Communications infrastructure	5
I. Financial services	4
J. Healthcare and public health	4

Home > Cybersecurity

Cyber threats in Kenya skyrocket, with 2.5 billion attacks recorded in three months

Kenya recorded over 2.5 billion cyber threats in just three months, with AI-driven attacks and system vulnerabilities pushing the country's digital defences to the brink.

Home / News / IT, Education, Research Most Targeted Sectors By Cybercriminals

IT, Education, Research Most Targeted Sectors By Cybercriminals

System Attacks Dominate, AI Now Weaponized

NATIONAL KE-CIRT/CC

Cyber Threat Landscape Roundup

Total Cyber Threats Detected

2,538,283,798 |  **201.85%**

The National KE-CIRT/CC detected over **2.5 billion** cyber threat events during the three-month period between **January - March 2025**, which represented a **201.85% increase** from the threat events detected in the previous period, October - December 2024. We continued to enhance the dissemination of cyber threat advisories to critical information infrastructure sectors, in response to the cyber threats observed.

Inadequate patching of systems, low user awareness of various threat vectors including phishing and other forms of social engineering attacks, and the increasing use of AI-driven attacks and machine learning technologies are among the reasons for the rise in cyber threats that have been detected.

Slido

Question 1: **"In ONE WORD, describe how you feel about your institution's current cybersecurity posture"**

Question 1: **"In ONE WORD, describe how you feel about your institution's current cybersecurity posture"**

Skilling the Hunters and Hunted

Training Agenda

- About ICANN Grant
- What is the problem?
- What is our solution?
- Project timelines
- Goal of the Training?
- Q&A

About ICANN Grant

- In May 2025, KENET was awarded **$500,000** for Capacity Building Project titled:
  "Strengthening Kenya's Cybersecurity Posture: Inclusive Capacity Building Across Five Regions"
- The capacity building initiative will run for **2 years** from June 2025 to May 2027 targeting about **1,500 ICT staff** of KENET member institutions
- The training will focus on imparting skills on Cybersecurity in the **4 main key areas:**
  - DNS and Email Security
  - IPv6 and IPv6 Security
  - Network Security
  - Identity and Trust Services

The Problem

Increase in Cybersecurity Incidences

- **Increased Incidences** end users experiencing increased phishing and email spamming in Kenya
- **Inadequate Protection of Digital Identities** majority of domains don't have all the required records to help in mitigating against domain spoofing and spamming
- DNS-related attacks increased in year 2023 - 2024

Lack of Adequately-skilled Human Capacity

- Institutions have IT Human Capacity for managing IT Assets
- IT Human capacity most often **not adequately skilled** to mitigate against advance cyber incidences
- IT Human capacity **lacks skills with IPv6 and spoofing-related protection**

Inadequate Budget for Capacity Building

- Institutions **not allocating budgets** for capacity building of IT staff – budgetary constraints
- Institutions in **marginalized areas lack the opportunity to attract highly skilled personnel**
- Most advanced training provided in Nairobi where the **costs of travel and accommodation is high**

The 10 major cybersecurity incidents in Kenya from 2023-2025

Major Incidents Covered:

1.July 2023 DDoS Attacks ("Anonymous Sudan") - The big one that shut down M-Pesa, eCitizen, Kenya Power

2.University of Nairobi Data Breach - Student management system compromised

3.Kenya Bureau of Standards Ransomware - Government entity hit

4.Data Protection Compliance Violations - 5 specific cases with fines:

1. Oppo Kenya (KES 5M - maximum fine)
2. Roma School (KES 4.55M - minors involved)
3. Casa Vera Lounge (KES 1.85M)
4. Whitepath/Digital Credit Provider (KES 2.975M)
5. Aga Khan Hospital (enforcement notice)

5.University Network Vulnerabilities - Research findings on persistent attacks

6.November 2025 Website Defacement - Government sites hit

7.M-Pesa Fraud Epidemic - 47.4% fraud rate in 2021

8.Sectoral Impact Analysis - Which sectors are hit hardest

9.Skills Gap Crisis - Only 1,500 graduates vs 45,000 positions

Key Goals of the Project

- **Goal 1:** To strengthen the cybersecurity posture of the academic sector in Kenya by training the IT Staff on software technologies and policies that will improve their ability to protect their institutional IT assets.
- **Goal 2:** To improve the IT Skills of the Personnel using a **"Train the Trainer" (ToT)** model

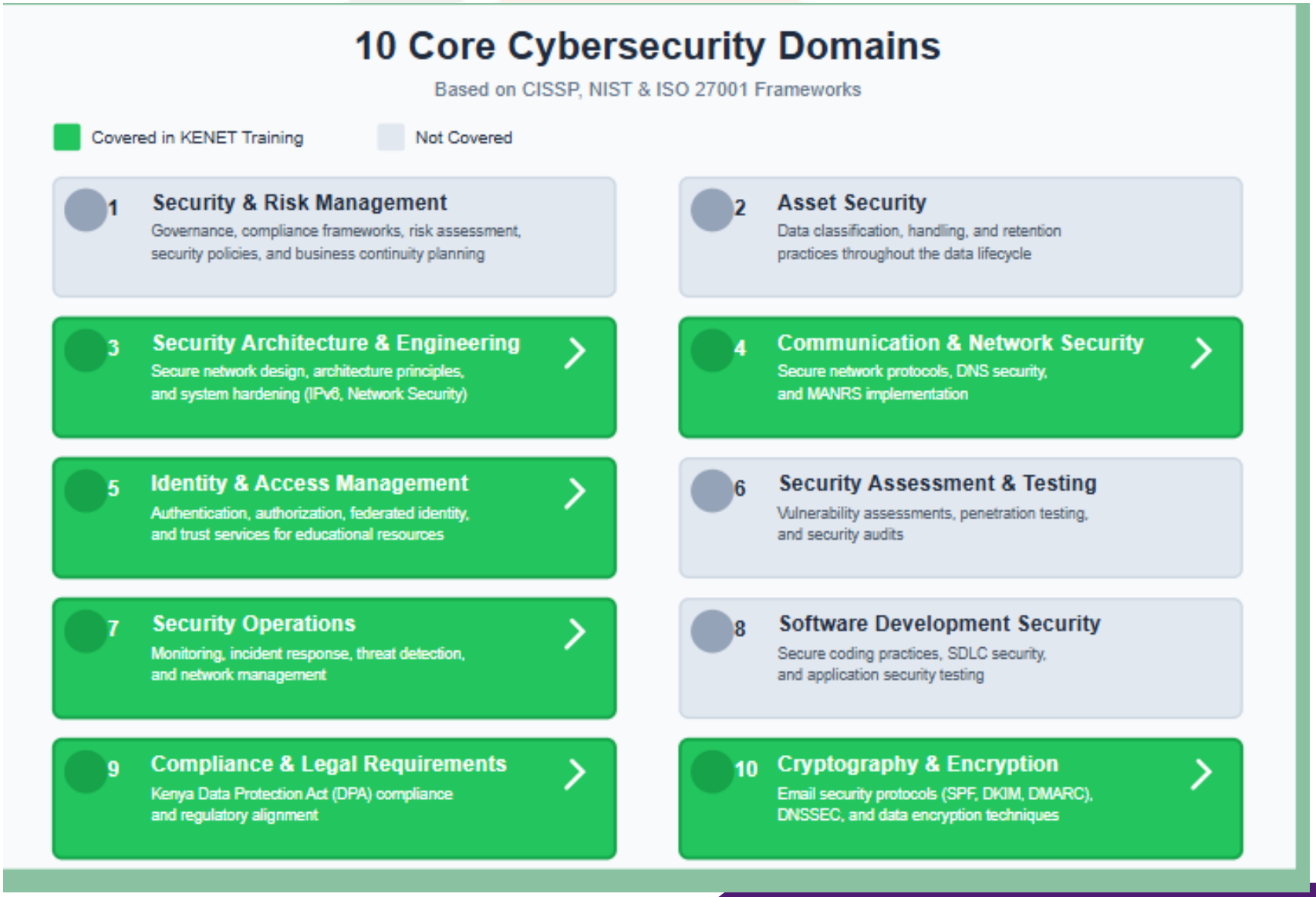
➢ **Target:** Skill about 1,500 IT Personnel to improve their cybersecurity posture and skill level for protection of Critical Digital Assets and Infrastructure

- **Note:** This is an advanced hands-on training with practical labs.

Proposed Solution- key focus areas

- **Protection of Campus Networks of Member Institutions** - to reduce number of network devices in campus networks that are hijacked and controlled by cybercriminals through malware, viruses and ransomware
- **Protection of Portals and Digital Services Platforms of Member Institutions** - to reduce the impersonation of institutional domains (e.g. mu.ac.ke) and protect the integrity of the domain for purposes of email use
- **Identity & Trust Services** - to increase secure access to requisite education and research resources and can communicate securely within the networks and systems among KENET member institutions and their partners

Core Cybersecurity Domains



Slido

- **Question 2: "Which of the 6 domains we're covering excites you MOST?"**
  - Communication & Network Security
  - Identity & Access Management
  - Security Architecture
  - Security Operations
  - Compliance & DPA
  - Cryptography & Encryption

- Question 2: "Which of the 6 domains we're covering excites you MOST?“

OR visit slido.com and use the code 2844013

Slido

- **Question 2: Opening Poll before JOINT module session**

"What's your institution's BIGGEST cybersecurity challenge?"

- A) Lack of skilled personnel
- B) Budget constraints
- C) Increasing attack sophistication
- D) Lack of management buy-in
- E) All of the above!

Core Cybersecurity Domains

- According to industry frameworks (CISSP, NIST, ISO 27001), comprehensive cybersecurity requires coverage across 10 critical domains:
- **The 10 Domains:**
- Security & Risk Management
- Asset Security
- **Security Architecture & Engineering ✓**
- **Communication & Network Security ✓**
- **Identity & Access Management ✓**
- Security Assessment & Testing
- **Security Operations ✓**
- Software Development Security
- **Compliance & Legal Requirements ✓**
- **Cryptography & Encryption ✓**

❖ **Reference Note:** Source: ISC² CISSP Common Body of Knowledge; NIST Cybersecurity Framework 2.0

How KENET Training Covers the 6 Critical Domains

- **Domain 1: Communication & Network Security** ✓ *What it speaks to:* Protecting the flow of R&E content across campus networks *How we cover it:* MANRS implementation, IPv6 security, DNS security, and anti-spoofing techniques to ensure secure communication channels for collaborative research and online learning platforms
- **Domain 2: Identity & Access Management** ✓ *What it speaks to:* Ensuring only authorized users access sensitive research data and educational resources *How we cover it:* Federated identity services and authentication systems enabling secure access to global research repositories, digital libraries, and institutional resources
- **Domain 3: Security Architecture & Engineering** ✓ *What it speaks to:* Building secure-by-design campus network infrastructure for research and learning *How we cover it:* Network architecture best practices, secure campus network design, and implementation of 802.1X for controlled access to research and educational networks

How KENET Training Covers the 6 Critical Domains

- **Domain 4: Security Operations** ✓ *What it speaks to:* Continuous monitoring and protection of research infrastructure and student data *How we cover it:* Network monitoring and management techniques, proactive threat detection for protecting ongoing research projects and safeguarding student information systems
- **Domain 5: Compliance & Legal Requirements** ✓ *What it speaks to:* Meeting regulatory obligations for handling student and research data *How we cover it:* Kenya Data Protection Act (DPA) compliance training, ensuring institutional alignment with legal requirements for processing personal data in educational settings
- **Domain 6: Cryptography & Encryption** ✓ *What it speaks to:* Protecting confidential research findings and institutional communications *How we cover it:* Email security protocols (SPF, DKIM, DMARC), DNSSEC implementation, and encryption techniques to secure sensitive research data in transit and protect institutional email and network integrity

Key Training Track Areas

Pre-Training Course

- Refresher on Linux Fundamentals
- Refresher on Networking fundamentals
- All participants

Track 1

- DNS & Email Security
- Identity &Trust Services
- System Admins/Engineers/Webmasters

Track 2

- IPv4&IPv6 Addressing
- Network Security
- Network Engineers/Network Admins

Capacity Building Track Areas

DNS and Email Security	Identity and Trust Services	IPv6 and IPv6 Security	Network Security
• Training to secure email communications and DNS queries • Training in DNSSEC, DMARC, DKIM, BIMI and SPF	• Training on implementing authenticated services for all IT Assets (network access, services access, etc) • Training on visibility of the IT Infrastructure and knowing who accessed which asset(s)	• Training on IPv6 and publishing services on IPv6 • Implementing IPv6 for key services in Duatl-stack of IPv6-only services deployments (HTTP/HTTPS, email, DNS, etc	• Training on Implementing MANRS (Mutually Agreed Norms for Routing & Security) • Training on securing campus networks to avoid IP Spoofing, DHCP spoofing, etc

Proposed Project Timelines

1. Phase 1: *In-person Trainings* in 5 regions (cohorts) – June 2025 to May 2026 – target 500 ICT staff

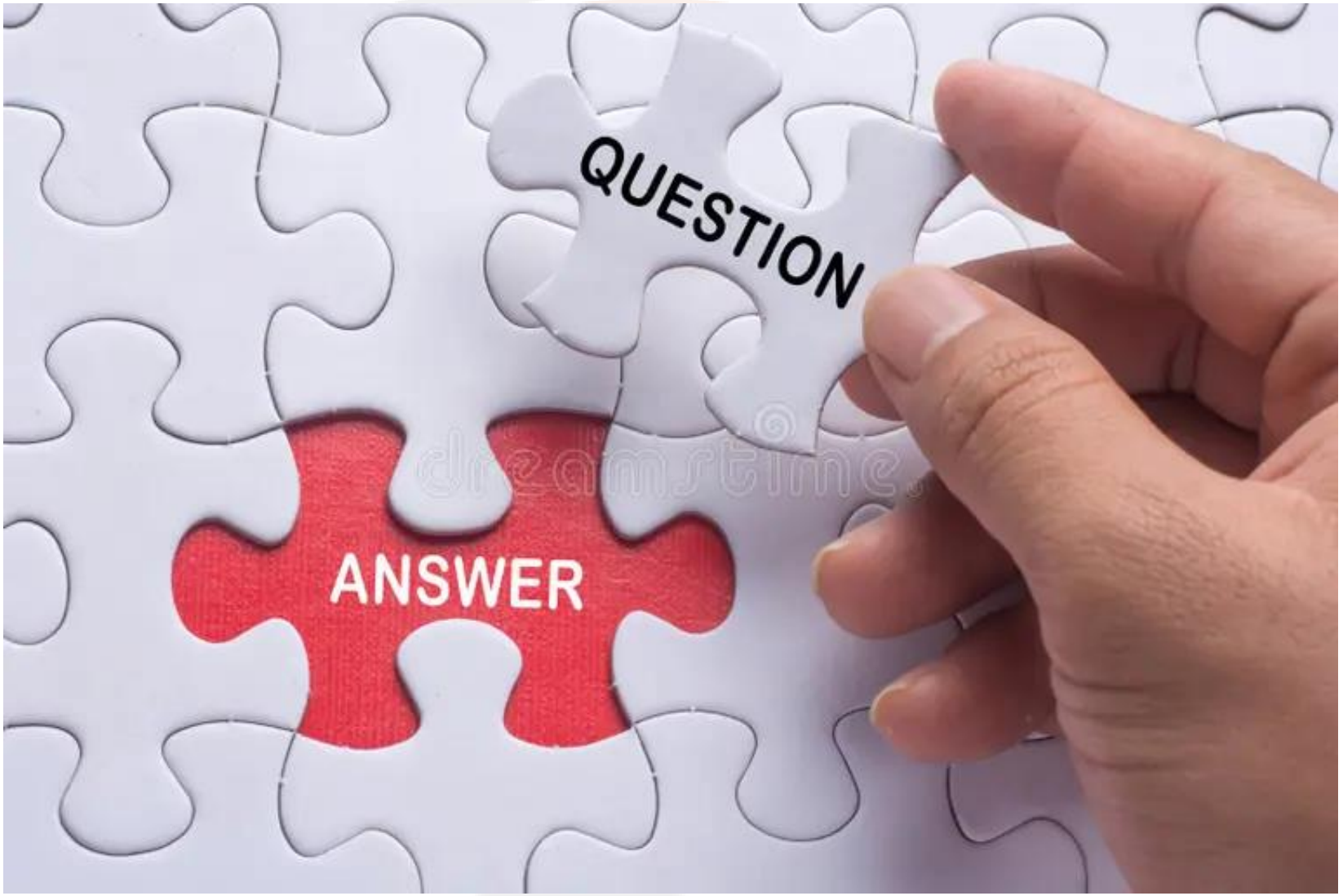
2. Phase 2: *Online Training* – July 2026 – December 2026 targeting 1000 ICT Staff

How Success Looks Like

- **Reach**: Conduct **5 regional training sessions** across all 5 regions in Kenya (Nairobi, Coast, Western, Central and Nyanza).
- **Focus Areas**: Train IT staff in **2 major focus areas**: DNS/Email security and MANRS/Network Security.
- **Capacity Building**: Empower ***2 IT champions per institution*** in the focus areas using the "Train the Trainer" model.
- **Direct Trainees**: Train **500 IT staff** within KENET member institutions.
- **Online Trainees**: Train a further **1000 IT Staff** using the online course material
- **Online Curriculum**: Develop **online interactive curriculum** for the two training focus areas to be availed on KENET LMS.
- **Online Course Impact**: Measure impact through the number of participants certified and time taken to complete the online courses.
- **Expected Security Impact**: At least **80% of 225 institutions** to implement security policies in DNSSEC, DMARC, DKIM, and SPF.

References

- https://ke-cirt.go.ke/wp-content/uploads/2024/04/2023-24-Q3-Cyber-Security-Report.pdf
- https://ke-cirt.go.ke/wp-content/uploads/2025/01/2024-25-Q2-Cyber-Security-Report.pdf
- https://adf-magazine.com/2025/12/cybercrime-outpaces-online-security/
- https://aln.africa/insight/data-protection-commissioner-imposes-fine/


QUESTION
ANSWER

kenet
Kenya Education Network

Transforming education through ICT

Thank You

www.kenet.or.ke
Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500