ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

cooperation germany – ecowas

EUROPEAN UNION

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Global Gateway

SHADOWSERVER

ECOWAS Region:

Cybersecurity Insights and Recommendations

The Challenge:

Cybercrime is rising sharply across Africa.

In Western Africa, cybercrime accounts for more than 30-percent of all reported crime.

ECOWAS Member States recently suffered costly and devastating cyberattacks against electric companies, banks, telecommunications providers, government services websites, manufacturers, and more.

30% OF REPORTED CRIME in Western Africa is cybercrime

Contributing Factors:

- Rapid economic growth and development: attracts financially motivated attackers
- Expanded digital footprint: increases available attack vectors to breach networks
- Cybersecurity deficiencies / "gaps": capabilities failing to keep pace

Primary Cyber Threats:

- Ransomware
- Attacks against critical infrastructure
- Distributed denial of service (DDos) attacks
- Business email compromise (BEC)
- Online fraud scams

The Risks in Failing to Act:

- Jeopardizing continued economic investment, growth, and development
- Eroding public trust
- Impacting critical services that affect citizens' quality of life

Institutional Cybersecurity Gaps and Recommendations:

Effective Institutions

Each ECOWAS Member State needs an operationally effective National CSIRT, access to an ECOWAS ISAC, and Sectoral CSIRTs capable of providing services tailored to the unique needs of each sector.

Access to Free / Affordable Threat Data, Tools and Services

Limited funding and costly threat data, tools, and services means network defenders should take advantage of free and/or affordable options. These include Shadowserver's free network remediation reports and tools like IntelMQ, Elasticsearch, and Kibana needed to effectively use threat data feeds. Affordable commercial options exist, including Arctic Hub, available through Arctic Security's CSIRT Development Program.

Training and Capacity Building

To develop technical skills within a CSIRT or ISAC, Member States should actively seek training and capacity building projects funded by government ministries, private sector companies, and entities such as the World Bank, the United Nations, and the European Union.

In-House Technical Experts

Acquiring and maintaining employees with superior technical skills can be difficult, particularly for government entities unable to compete with private sector salaries. Member States should work with universities and the private sector to develop training and mentorship programs that can act as a pipeline for skilled talent.

Partnership Development

National CSIRTs must not work in isolation. Frameworks should be devised to foster meaningful partnerships with fellow National CSIRTs, Internet service providers, critical infrastructure operators, government entities, businesses, universities, and the like. Doing so will facilitate information sharing, collaboration, and capacity building. Partnership opportunities are available through FIRST.org and through Shadowserver's Alliance Mattermost online community.

Maturity Assessments

To establish a baseline maturity level and track developmental progress, National CSIRTs should undergo the Open CSIRT Foundation's Security Incident Management Maturity Model (SIM3) self-assessment online tool and implement recommendations for improvement.

Early Warning Services

Using Shadowserver's free, daily network remediation reports and other threat data feeds, National CSIRTs should offer free Early Warning Services to all constituents. These services allow subscribing businesses and other constituents to receive automated alert notifications about exposed, vulnerable and compromised devices and services on their networks that need to be timely remediated. Consultation with one of the many National CSIRTs that offer Early Warning Services is recommended, including the UK's National Cyber Security Centre (UK NCSC) and the Dominican Republic's CSIRT-RD.

Operational Cybersecurity Gaps and Recommendations:

Asset Inventories

Network owners are often unaware of the assets that comprise their networks. Policies should be established to mandate periodic asset inventories, particularly in government and critical infrastructure sectors, to facilitate timely remediation as new vulnerabilities emerge.

Exposed Assets

The region contains assets needlessly exposed to the public internet, thereby increasing attack surfaces and providing attackers with greater opportunities to breach networks. Focused initiatives with National CSIRTs, Internet service providers, and other network owners in the region could lead to proactive surge activity to reduce instances of exposed devices and services.

Remediating Critical / High Severity Vulnerabilities

The region's networks contain unpatched vulnerabilities that can be exploited by threat actors seeking to breach those networks and cause harm through ransomware and other forms of attack. Regulations should be implemented to require government agencies and critical infrastructure operators to remediate vulnerabilities designated as "critical risk" within 15 calendar days, and those designated as "high risk" within 30 calendar days of detection. "Known Exploited Vulnerabilities (KEV)" identified as actively exploited in the wild should receive priority attention and be remediated within 14 calendar days.

Remediating Compromised and Malware-Infected Devices

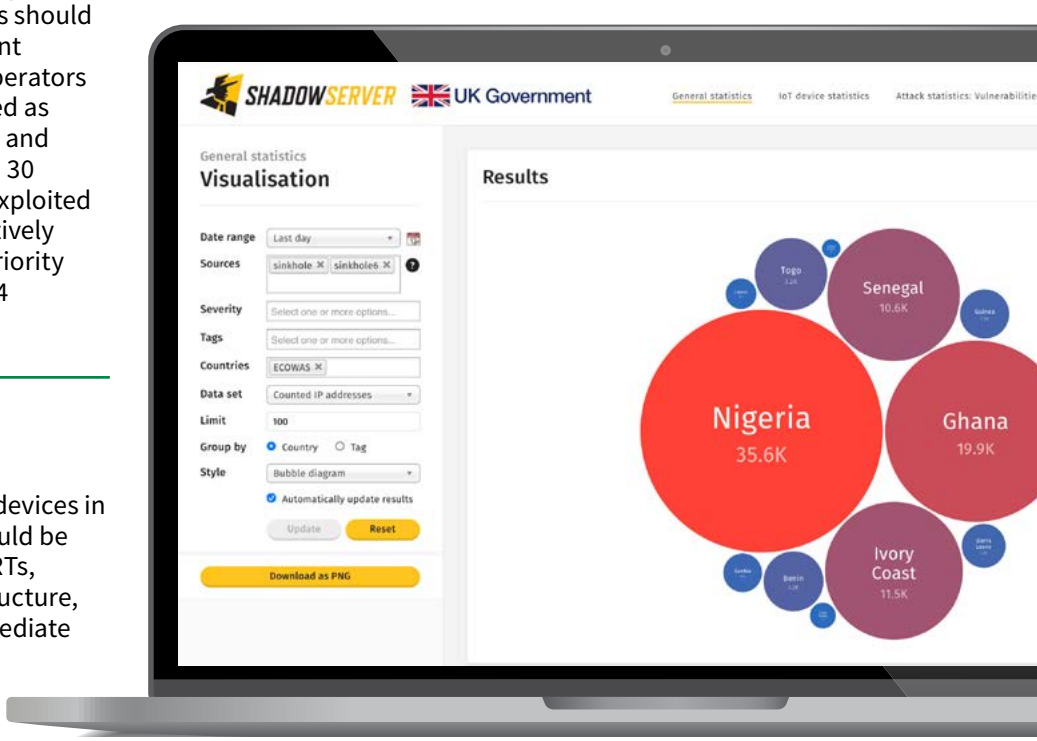
The region's networks also contain compromised and malware-infected devices in need of remediation. Regulations should be implemented to require National CSIRTs, government agencies, critical infrastructure, and other key network owners to remediate identified compromised and malware-infected devices within a specified time period, including those identified in Shadowserver's free, daily network remediation reports available to all National CSIRTs and subscribing network owners across all sectors.

Threat Mitigation / Eradication Campaigns

Devise and implement nationwide threat mitigation and eradication campaigns against critical vulnerabilities and compromised devices on networks throughout the region. One recent example is the nationwide campaign led by the Australian Signals Directorate (ASD) to eradicate implants in certain compromised devices throughout Australia.

Shadowserver's Public Dashboard

Use Shadowserver's Dashboard as a tool to inform key stakeholders (e.g., policymakers, government officials, network defenders, etc.) about the latest cyber threats affecting the region.



ECOWAS region country grouping on Shadowserver's public Dashboard