

CYBERSECURITY SOLUTIONS

Africa's rapid digital transformation brings tremendous opportunities, yet it increasingly makes countries vulnerable to cyber threats and attacks. Cybersecurity is a necessary foundation for tech-enabled growth and a powerful tool in protecting national infrastructure, safeguarding data, and ensuring trust in digital systems.

Strengthening a nation's cybersecurity capabilities is vital to Africa's sustainable growth and prosperity. With extensive experience deploying comprehensive cybersecurity programs across Africa, Cybastion solutions takes a multifaceted approach to deliver customized and robust protection against evolving digital threats.

Digital sovereignty—where African nations control their own digital infrastructure and data—is critical for long-term stability and growth. African governments partnering with Cybastion can now prepare for, prevent, detect, and respond to potential cyber threats and strengthen their cyber-resilience.



Foundation

To ensure a country's digital environment is fully protected, our comprehensive cybersecurity solutions provide a foundation for African governments to maintain full control over their data security.

Legal and regulatory framework.

Cybastion conducts a thorough review of the country's existing legal framework and regulatory environment governing cybersecurity. After the review, the legal landscape is aligned with contemporary cybersecurity challenges and global best practices.



Preparation

Center of Excellence Cybersecurity Academy.

The academy serves as a hub for training and capacity building, fostering a digitally skilled workforce adept in addressing the evolving challenges of cybersecurity.



Prevention

Public key infrastructure (PKI).

Through the implementation of a Public Key Infrastructure (PKI), African nations will strengthen the security of digital infrastructure and transactions. This cryptographic framework helps to secure sensitive information and ensure the integrity of digital assets.

Homologation Laboratory.

The homologation laboratory evaluates and certifies cybersecurity products, systems, and components to ensure adherence to predefined standards, specifications, and regulatory requirements.



Detection

Security Operations Center (SOC).

The SOC is an advanced cybersecurity solution that enhances organizations resilience against cyber threats. It collects and analyzes data from all connected devices, while monitoring networks, servers, databases, and other applications.



Response

Computer Emergency Response Team (CSIRT).

The CSIRT is responsible for maintaining the confidentiality, integrity, and availability of corporate assets and mitigating cybersecurity incidents affecting IT systems and networks.

Forensics Laboratory.

A state-of-the-art National Forensics Analysis Laboratory investigates and analyzes cyber incidents to enhance a nation's ability to respond effectively to cybersecurity threats.

Cybastion's Cybersecurity Program

