ITUEvents

Regional Cybersecurity Summit for Africa

20-23 November 2023
Kampala, Uganda

itu.int/go/_RCSSA

Supported by:

AfricaCERT
United Teams promoting Cybersecurity in Africa

Hosted by:

ucc
UGANDA COMMUNICATIONS COMMISSION

UgCERT
Computer Emergency Response Team

Organized by:

ITU

REGIONAL CYBERSECURITY SUMMIT FOR AFRICA

Security Baselines in the context of Digitization of Government Services

Peter Collins Wasenda

Uganda Revenue Authority

20-23 November 2023
Kampala, Uganda

Environmental Context
The Year 2009 & beyond

Business Technology

i. Centralized database

ii. Endpoints with different windows versions

iii. Servers – Windows 200x & HP-UX

Security Technologies

i. Firewall

ii. Enterprise Antivirus (on some machines)

iii. IDS that no one logged into

Environmental Issues

i. Ever Increasing attack surface (new solutions)

ii. Internal fraud

iii. Business always in a hurry

Team Structure / Culture

i. 2 Staff with no specialized security training

ii. Friction with other Tech Teams

Turning Points
Some Known Breaches

A former staff worked with accomplices to “remotely login” to a system that he developed and altar tax rates to serve his clients – and we lost revenue!

URA website defaced by a discontent external party using a vulnerability in the newly launched mobile application

Lessons Learned
Baselines

Deploy a team

i. Skills

ii. Competence Development

Have a Plan

i. Assessment Reports

ii. Specific Industry adversarial profiles

iii. Management & stakeholder concerns

iv. Identify risk to the organizations mission

v. Adopt a Method of measuring success (KPI, KRI, KCI)

Implement & Monitor the Plan

i. Monitor Performance measures

ii. Adopt Automation

- Open source where feasible
- Standard Operating Procedures / Runbooks

Lessons Learned - Baselines Enforce Uniformity

i. Document Expected Behaviors

ii. Automation should match Documentation

iii. Socialize to build a strong culture

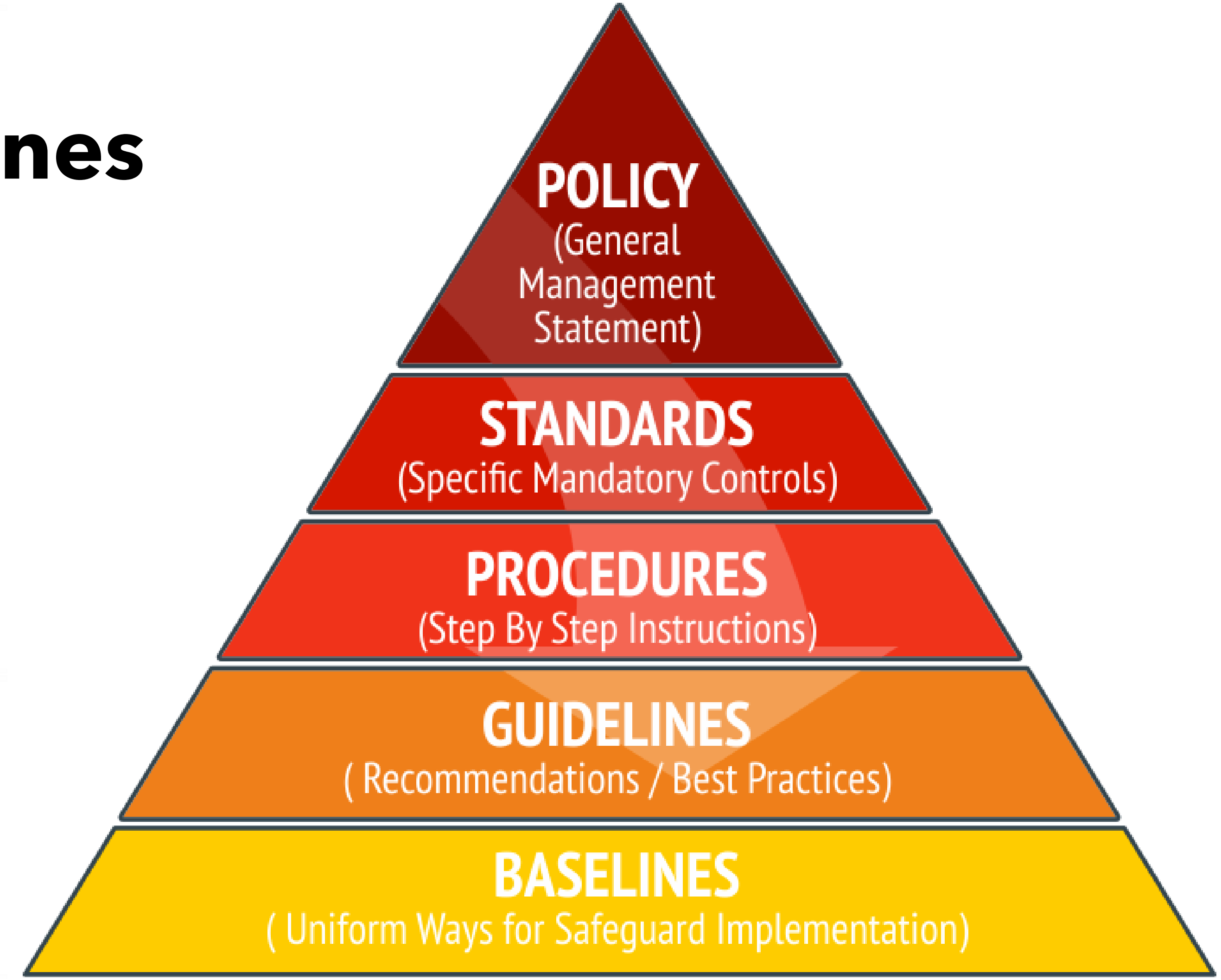
iv. Keep updated asset base, services

v. Leverage Government Published frameworks e.g. NITA(U) NISF

vi. Leverage Industry frameworks (e.g. Collective Control Catalogue/CIS)

vii. Execute Scheduled & ad-hoc VA,PT, Control Reviews

viii.Don’t trust anyone


POLICY
(General Management Statement)
STANDARDS
(Specific Mandatory Controls)
PROCEDURES
(Step By Step Instructions)
GUIDELINES
(Recommendations / Best Practices)
BASELINES
(Uniform Ways for Safeguard Implementation)

Source: https://t.ly/YMekh

Thank you!