Improve cyber resilience of Financial Inclusion in Africa

- What Matters, what solutions –

4th University of Luxembourg Inclusive and Sustainable Finance Research Conference, Nov 14th 2019

Suricate Solutions
Security & Payments

Jean-Louis PERRIER jlperrier@suricatesolutions.com +352 691 613 163

SETTING THE SCENE
– Real life cases -

West Africa recent attacks

show the cyber security situation is getting more critical

- **April 2018 : 5PM : Private Cloud of a group of MFI** : Intrusion in system administration after downloading malicious content on social networks, undetected by Antivirus. Malware started **crypto currency mining in China,** detected after a few minutes by Suricate security supervision before spreading
- **December 24th, 2019: 6PM** : Intrusion in the Core Banking System (CBS) of one of the **largest MFI in WAMU**. Phishing to the CIO email granted systems access with privileged accounts! Fraudulent transactions immediately started, stopped after detection by Suricate
- **March 2019 : Intrusion in the CBS of Banque de Dakar (Sénégal). Losses # € 0.8M.** Accounts opened fraudulently with real IDs, fraudulent large money transfers through an intrusion undetected for several weeks, and withdrawals. 6 people arrested, head of international criminal organization and hackers still running.
- **March 2019 : Major oil company in WAMU.** Large Scale RansomWare attack (servers encrypted until a ransom in Bitcoin is paid)
- **April 2019 : Large Scale RansomWare attack for one of the largest utilities in Senegal.** 80 % of servers infected, including backup system, **IT and operations halted for 8 days** (email, invoicing, customer service, field operation). Recovery through the assistance of our Cyber Security Incident Response Team.
- **May 2019 : Intrusion in the CBS of Sonibank CBS (Niger). Losses # € 0.5M.**

West Africa MFI incident deep dive

reveals cyber security awareness way below minimum standards

- **Tier II MFI, SME oriented, >20 years experience with good track record, no refinancing problem (yet)**
- **Losses > 60 k€ in 2 months with fraudulent money transfers entered remotely on cashier's workstations**
  - **Losses exceed fees** earned in a couple of years and **yearly net result**
  - Money Transfer stopped in emergency **= loss of fees**
  - All providers : Wari, MoneyGram, Western Union, RIA
  - Transfers destination : Ivory Coast, Morocco, Guinea
- **Emergency audit & forensic investigations : critical, but typical, situation**

Outgoing data transfers towards **Ivory Coast** and **Yemen,** management and employees **not aware** of information security risks , technical **team not trained** on security, poor token management (bank and MFI), **unsecure passwords**, inadequate allocation of **privileged accounts,** few computers protected with antivirus, and with **obsolete signatures database, devices not updated** (servers, PC, Firewall, ...), **firewall wrongly configured,** inadequate **network architecture, inappropriate Internal controls**, **no operational security supervision,** no cyber security **Insurance,** no Fraud clause in **DFS contracts,** ...

- **Basic Remote Access Trojan "NanoCore" undetected for 2 months, until the money transfer partner invoice**

STATUS ON CYBER THREATS

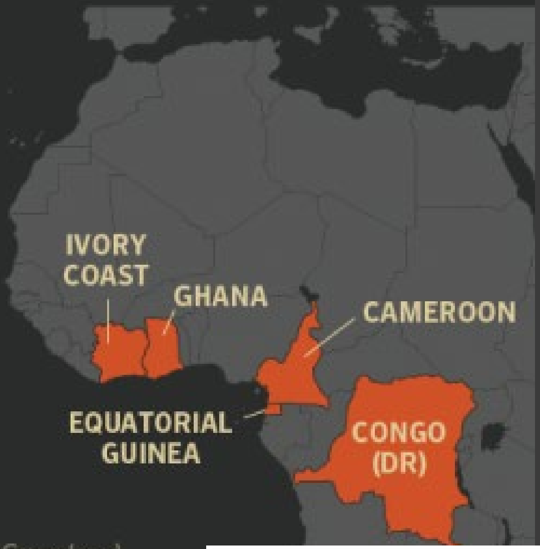
West Africa

Financial Institutions Hit by Wave of Attacks

Attackers using commodity malware and living off the land tools against financial targets

Malware used

- NanoCore *(Trojan.Nancrat)*
- Cobalt Strike *(Trojan.Agentemis)*
- Mimikatz *(Hacktool.Mimikatz)*
- Imminent Monitor RAT *(Infostealer.Hawket)*
- Remote Manipulator System RAT *(Backdoor.Gussdoor)*

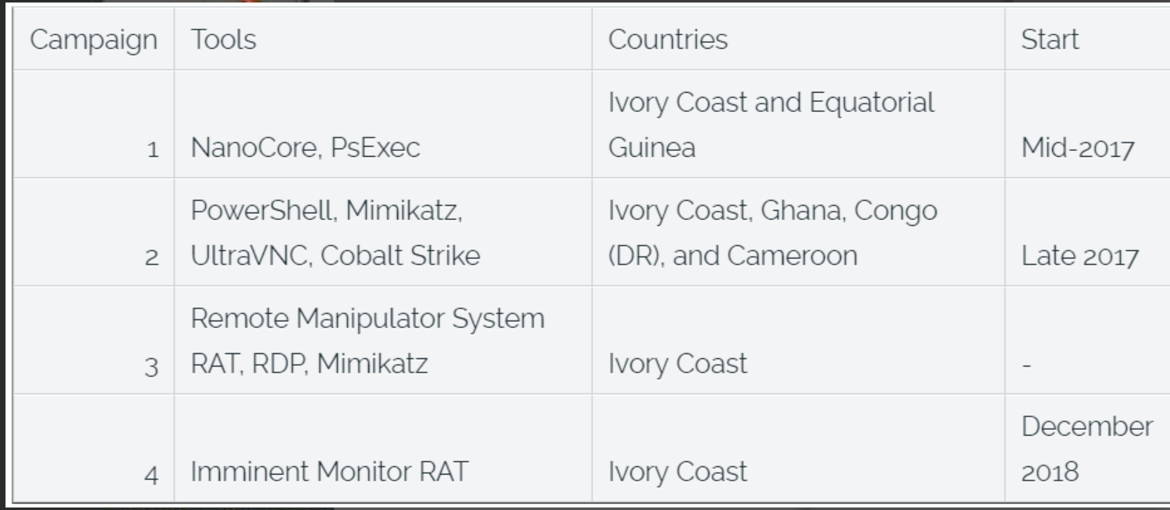


Living off the land tools used

- PowerShell
- PsExec
- RDP
- UltraVNC

Symantec.

- 1st Symantec review of large scale attack in West Africa
- 5 countries affected
- Same basic tools & techniques
- 1 or several groups ?
- 4 campaigns in 18 months
- +2 similar attacks we spotted in Benin and Senegal



Campaign	Tools	Countries	Start
1	NanoCore, PsExec	Ivory Coast and Equatorial Guinea	Mid-2017
2	PowerShell, Mimikatz, UltraVNC, Cobalt Strike	Ivory Coast, Ghana, Congo (DR), and Cameroon	Late 2017
3	Remote Manipulator System RAT, RDP, Mimikatz	Ivory Coast	-
4	Imminent Monitor RAT	Ivory Coast	December 2018

Source https://www.symantec.com/blogs/threat-intelligence/african-financial-attacks

BankingTech

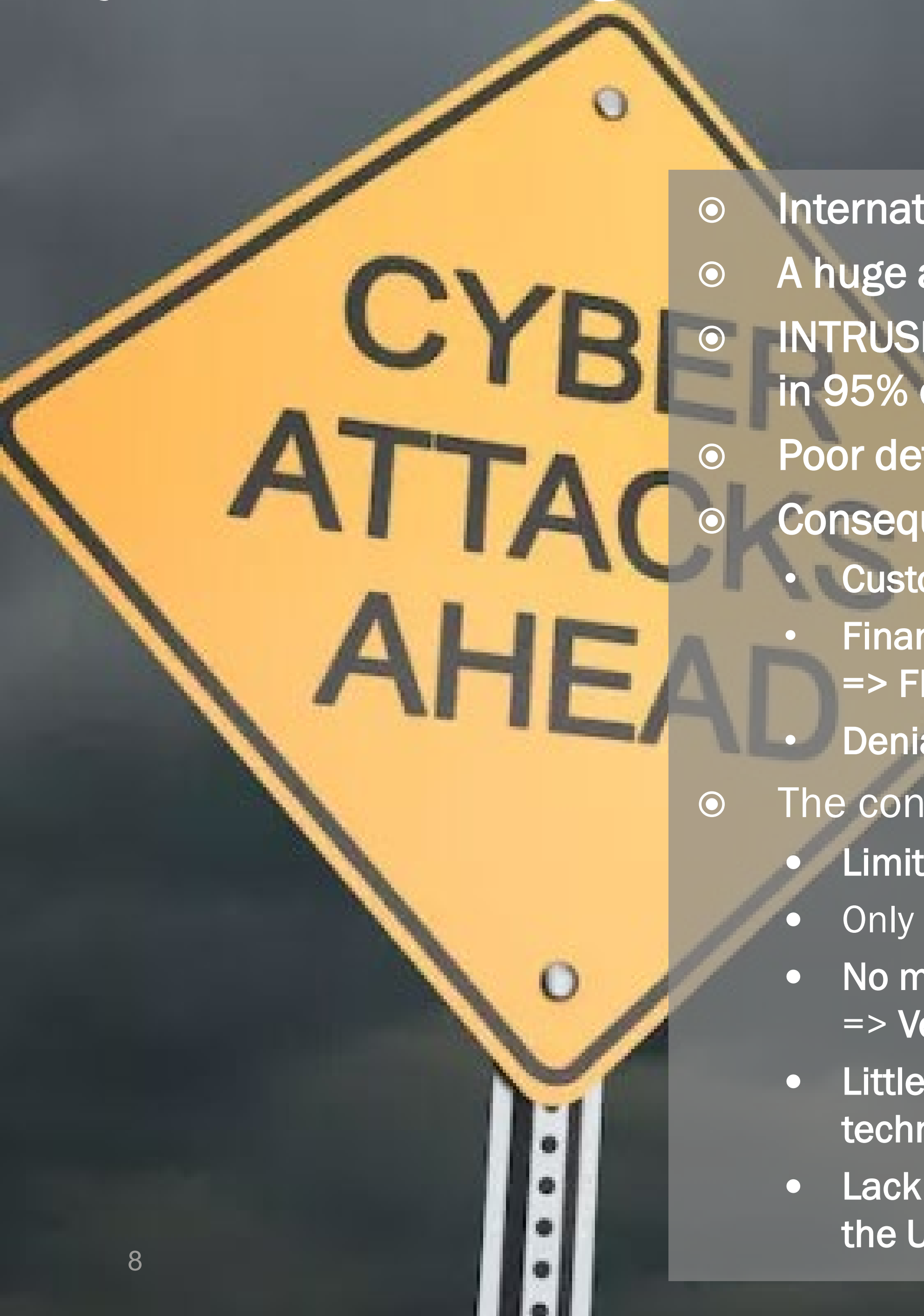
BankingTech

Cyberattack waves wash over West African banks

- **... attacking African banks is a trend** that many industry experts saw coming.
- Over the past two years... **concerted efforts from different hacking crews, some of Russian and some of North Korean** origin, that have focused on banks and financial institutions located in South East Asia, Eastern Europe, and South America.
- **...banks are targeted in these regions because there's a high chance that they have not all invested in their IT infrastructure and cyber-security measures. A poorly designed and unsupervised network** makes attacks easier to carry out and hide for a long time...
- **Lacking from past reports** ...was **Africa**, which surprisingly hasn't been targeted until now,
- **The African financial sector's period of calm appears to be over.**

Source https://www.zdnet.com/article/west-african-banks-hit-by-multiple-hacking-waves-last-year/

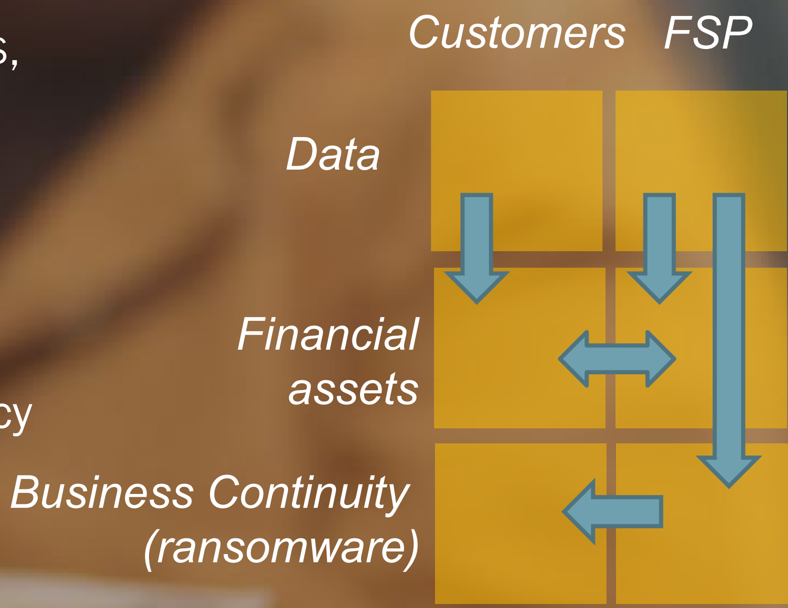
Cyber crime insights



- **International organized criminal networks**
- **A huge and evolving variety of modus operandi**
- **INTRUSIONS DO HAPPEN** : Ethical Hackers get **administration rights in 95% of cases in 8-10 days**
- **Poor detection : you can find only what you know**
- **Consequences worsen AND frequency rises**
  - **Customer data losses** (in a context of stronger regulation)
  - **Financial losses : 80% money related   (93% for FSP**
    => FINANCIAL INSTITUTIONS are **MAJOR TARGETS**
  - **Denial of Service, service outage** (ransomware)
- The continent is not prepared to fight
  - **Limited awareness**
  - Only 15 countries over 54 have a national security centre
  - **No mechanism** to **gather, analyze and report security incidents** in Africa
    => **Very few incidents are publicize**
  - **Little assistance to be expected from Governments and LEA, regulation, technology**
  - **Lack of skills: 10.000 security engineers on the continent, 700.000 in the US (+300.000 open positions)**

Cyber Crime in the financial sector in Africa

- Hackers target **cash**
- **Central banks are hacked**
  - Ecuador 12 M$, Bangladesh 81 M$, Nepal 4.4 M$, Mexico 15 M$, Taiwan 60 M$, Russia 6 M$, India 2 M$
- **Banks are hacked**
  - Russians & Ukrainian hacked 100 financial institutions in 10 european countries, **losses € 1Bn** in 3 yrs
  - Bank of Chile **10 M$ & 9500 PCs and Servers** damaged
- **Bitcoin is hacked** : Coincheck : 500 M$ stolen in crypto-currency
- **Africa is hacked : in 2017 (*)**
  - **$3.5 B annual cost of cybercrime, +20% pa**
  - x2 successful attacks against the financial sector
  - 39 % of losses hitting banks and electronic transactions
- **Financial Inclusion is hacked, not only DFS, and smaller institutions are more at risk**
- **Cyber crime is the # 1 threat to the development of financial inclusion** (**) and potentially a **systemic risks**
- **The under investment in cyber security is massive** : the 4 largest US banks spend #$1.5B a year on cyber security , which is the yearly spending of Africa



Customers *FSP*

Data

Financial assets

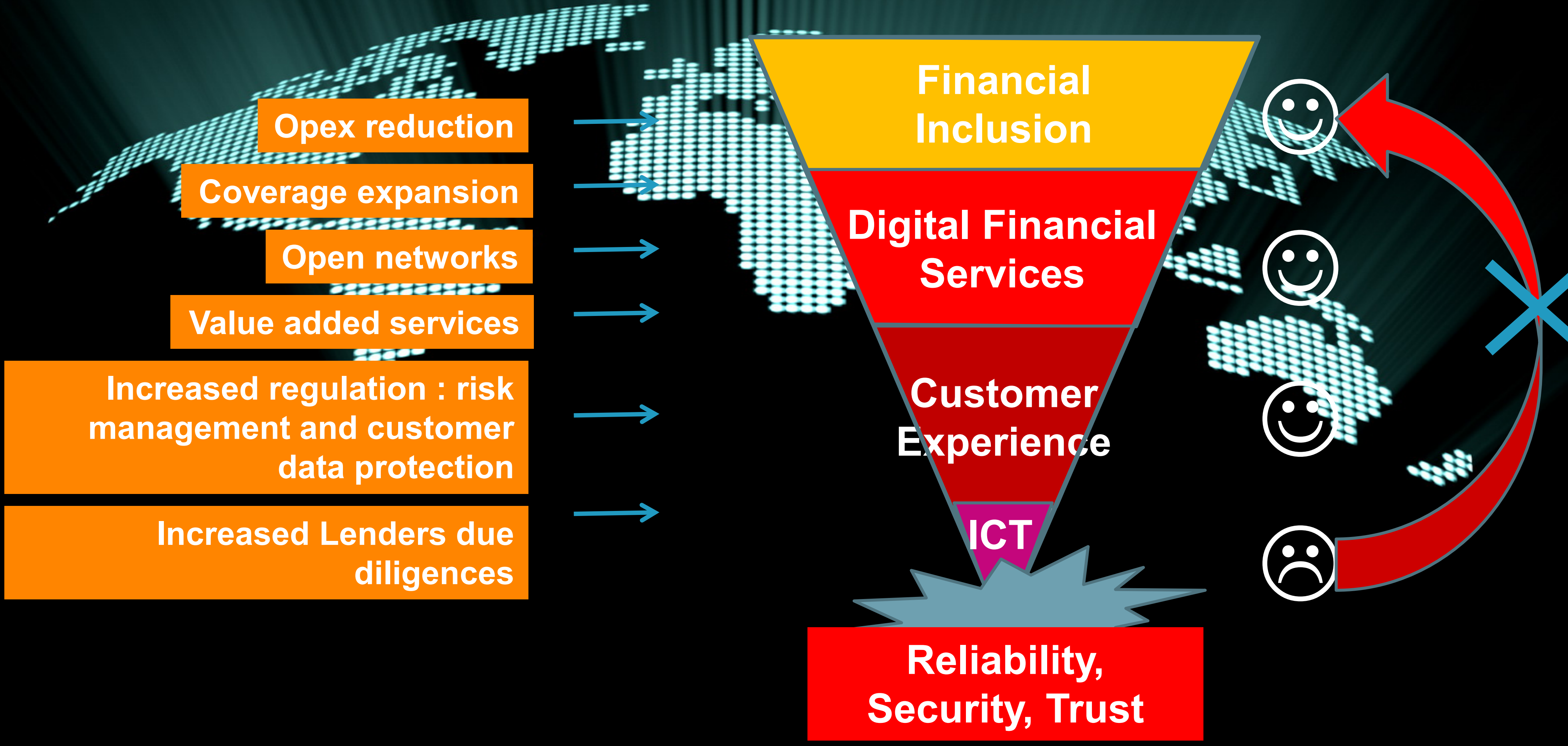
Business Continuity (ransomware)

(*) source Africa Cyber Security Report 2017, Serianu

(**) AFI Alliance for Financial Inclusion Global Thought Leadership Conference, Abidjan, 1/3/2019

Digital Financial Services, a key to financial inclusion

… DFS security is a MUST DO & a PREREQUISITE for SUSTAINABILITY and RESPONSIBLE FINANCE



Opex reduction

Coverage expansion

Open networks

Value added services

Increased regulation : risk management and customer data protection

Increased Lenders due diligences

Financial Inclusion

Digital Financial Services

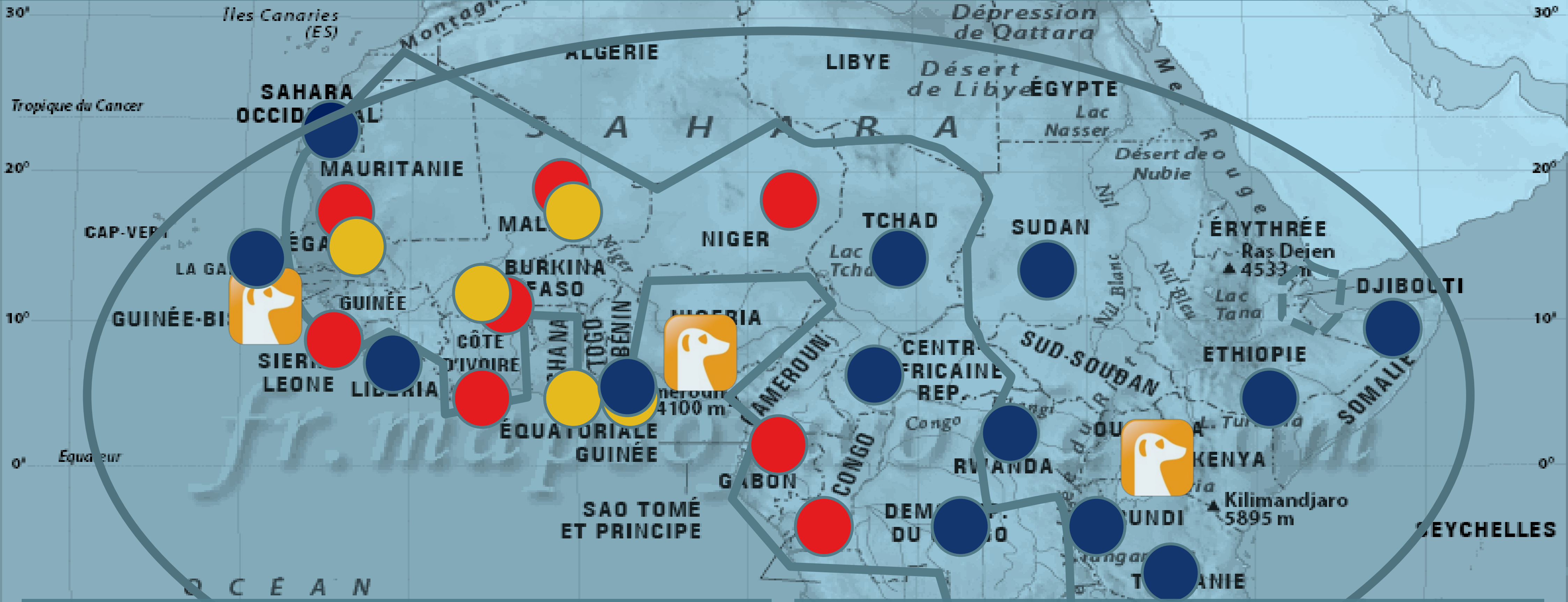
Customer Experience

ICT

Reliability, Security, Trust

Uh guys, can we do anything ?

African Cyber Security Resource Center for financial inclusion in SSA



Suricate, EOY 2019 : 8 countries, 47 MFI, 1.2 M end customers ●

Suricate, EOY 2021 Burkina MFI + CIF Networ ●
10 countries, 67 MFI, Fintech
5.4 M end customers

African Cyber Security Resource Centre ●
Consortium at funding stage : 1 coordination organisation, 3 sub regional centres, 50 countries,
x00 FSP : MFI, Fintech, Micro Insurance, x0 M end customers

Improve cyber resilience of Financial Inclusion in Africa

African Cyber Security Resource Centre Project

Based on work by and with

Jean-Louis Perrier — Suricate Solutions

Pascal Steichen, Bertrand Lathoud, Elena Kaiser — SMILE

Tegawendé Bissyandé — SnT/UNI.LU

Nov. 14th, 2019

About us

A consortium of >200 high level cyber security experts in Europe and Africa

- **SMILE : cyber security centre of the government of Luxembourg.**
  - Mission : to improve cyber security of Luxembourg, including developing the cyber security ecosystem and fostering innovations
  - R&D in tools and methodologies (eg ROOM42, a cyber security crisis management simulation room, MISP : the reference Malware Information Sharing Platform)
  - Threat Intelligence sharing with other CERTs, Awareness Rising, Crisis Management at national level

•**SnT**: **Interdisciplinary Centre for Security, Reliability and Trust from UNIversity of Luxembourg**, with a **strategic research priority in cyber security.**

- Mission: conducts internationally competitive research in ICT creating socio-economic impact.
- Industry Partnerships in Financial Services
- University Partnerships in Africa

- **Excellium Services and Suricate Solutions**, it's affiliate for Sub Saharan Africa, offer **all cyber security services required to Identify, Protect, Detect, Respond and Recover.**

  - Recognized experts on incident response & a strong track record for FSP
  - Leading Cyber security company in Luxembourg with >130 experts

Objectives

Improve the resilience of financial inclusion institutions and protect their customers against cyber attacks in Sub Saharan Africa, to (1) foster financial inclusion, (2) secure the development of Digital Financial Services, and (3) allow building interoperable payment systems

THINK BIG

START SMALL

MOVE FAST

General directions

Continental and regional strategy : Sub Saharan Africa and Financial Inclusion in 1st stages, can later be expanded or replicated in other sectors/regions

Proximity for appropriate and continuous institutions support and capacity building

Fast & cost efficient setup: rely on/reuse existing structures, ecosystems, know how, experiences, open source software for prevention, detection & remediation

Scalability: Prototype then roll out in SSA, coordination between entities to avoid duplicates

Inclusivity :

-Services available to **all size of FSP & Fintech at reasonable costs**

-**All partners associated**, with specific modalities to develop trust circle

Contribute to close the gender GAP

- **Encourage presence of women** in the ICT & cyber security sector (scholarships, internship, startups)
- **Equal opportunity employer,**
- **Incentive program** to facilitate the access to services for **institutions supporting women**

Efficiency : be inspired from proven best practices & organisations, and **innovate**

Project highlights

- Inspired by
  - **CGAP's cyber security diagnosis and strategy**,
  - **sectorial experiences** worldwide (FS ISAC, GSMA Fraud and Security Forum),
  - momentum and lessons learned from **Suricate Solutions' Dakar Regional Cyber Security Operation Centre** in the last 3 years

- Build & mobilize a **comprehensive and sustainable cyber security ecosystem in 3 to 5 years.**

- **USD 6-10 M budget + fees from FSP and membership fees**

- **North/South public private partnership**

- Based on **proven international cyber security best practices for efficiency,** should ensure **lasting capacity building** and a **sustainable business model.**

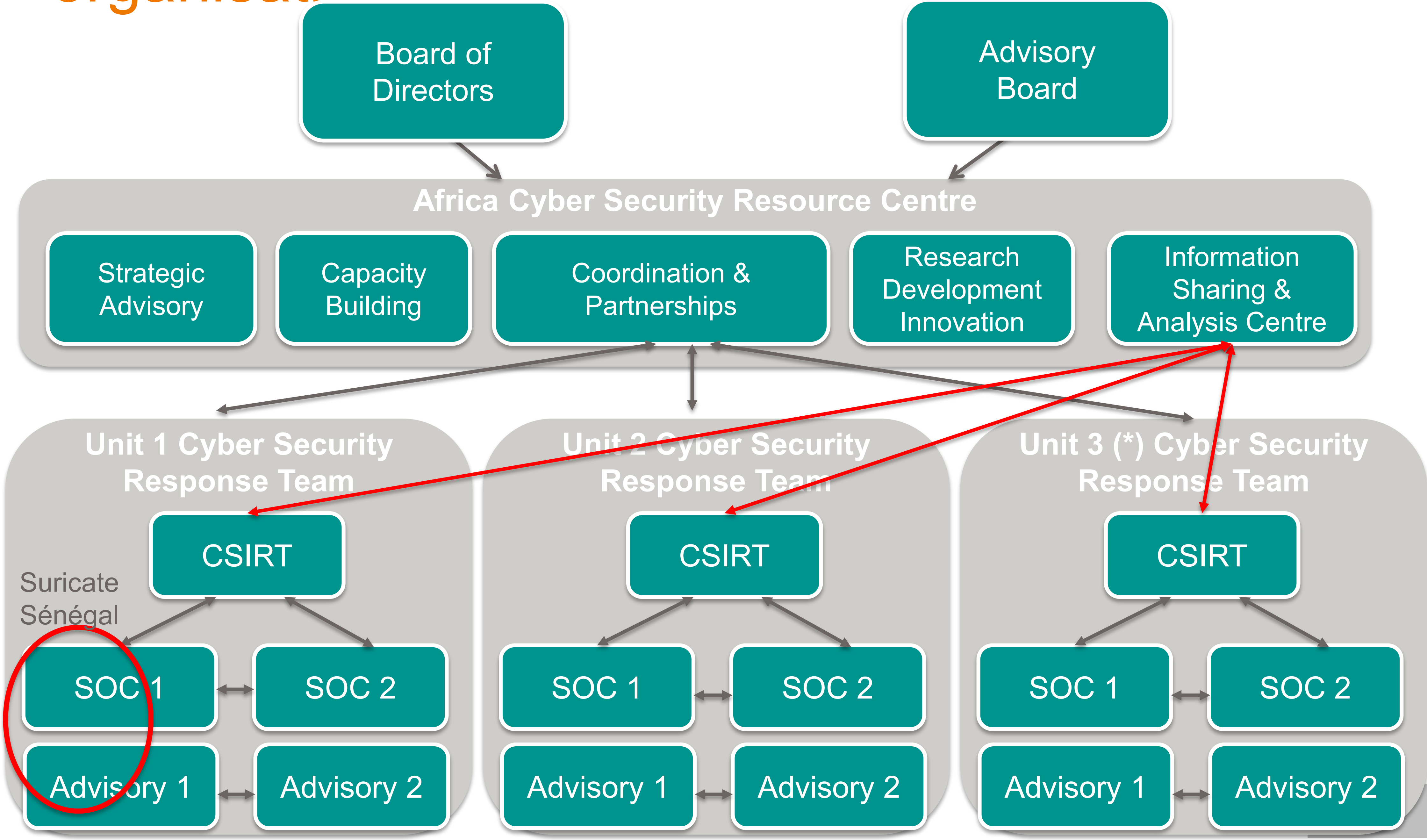
- **3 levels**
  - Coordination : **dedicated organization** (Economic Interest Group in Luxembourg)
  - **3 Computer Security Incident Response Teams** (CSIRT) manage sub regional level (French speaking Africa, East Africa, English speaking West Africa) and support institutions for large scale incidents
  - A **limited number of proximity operational teams (Security Operation Centre SOC)**

Two great inspiration sources

Lessons learned from FS-ISAC and GSMA FASG

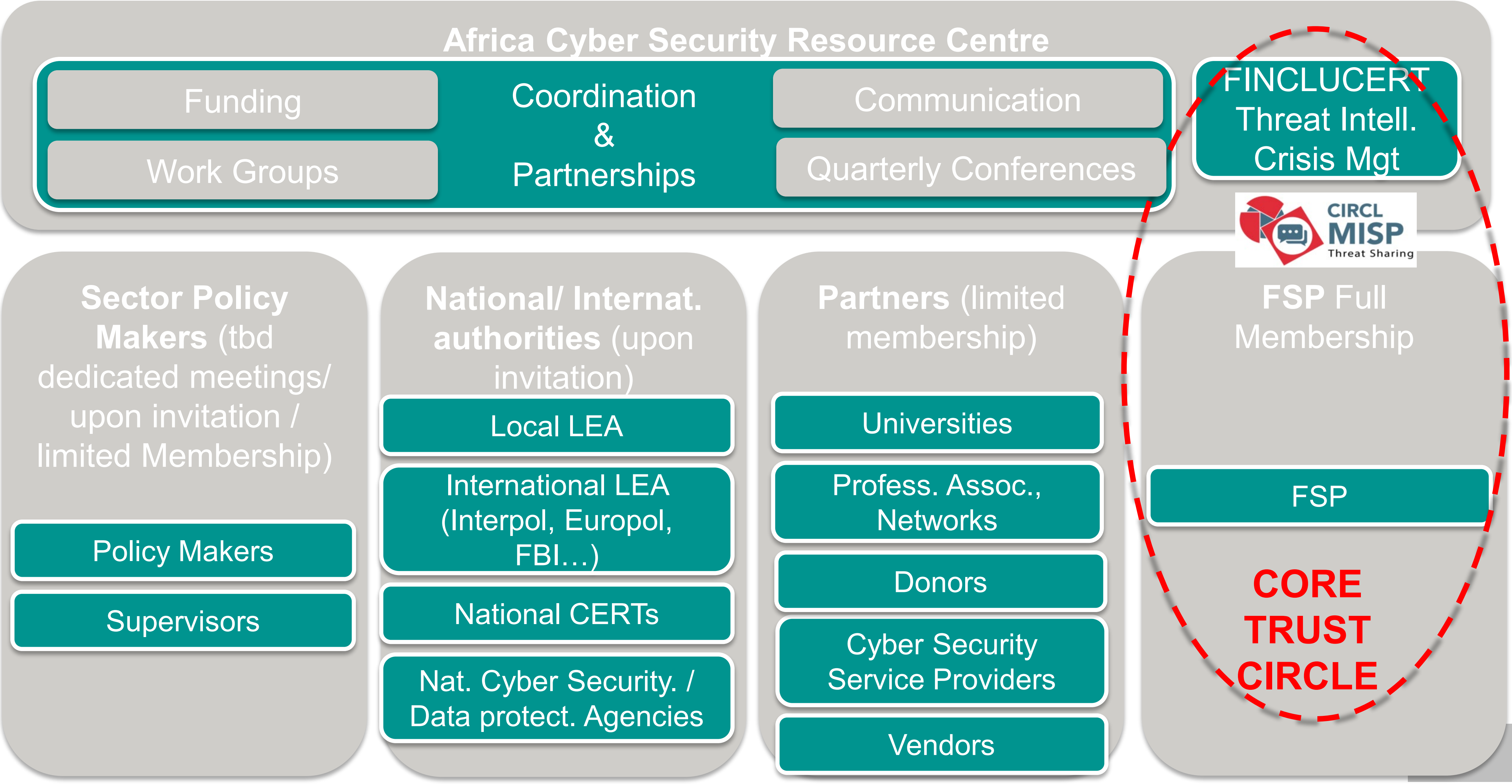
1. **Efficient and longstanding initiatives come from the sector**
2. **A controlled network for information sharing**
   - **Closed network** to exchange most sensitive data with trusted peers with an Opt In policy (what information, with whom).
   - **Opened to third parties** in controlled conditions (vendors and cyber security service providers, local Cyber security or Data privacy agencies, National CERT, local or international Law Enforcement Authorities)
   - **Meeting closed or public** depending on members decision.
   - **Not a substitute to local legal or regulatory processes**.
3. **Central banks, policy makers, supervisors are NOT members,** to ensure FSP are sharing in trust. They may be invited to some events, specific instances may be created or adapted for them, eg AFI (tbd, may evolve in time)
4. **Regular physical meetings** and **WorkGroups** are necessary to build trust and share high level analysis.
5. Services that do not include sensitive data, eg capacity building, training, threats observatory, advisory, may be delivered to all stakeholders
6. **Limitations**
   - **Most active presence from major players** (large FSP, international MNO networks)
   - **Reduced Detection and Incident Response capability**: both are more oriented towards prevention except for some critical situations
   - **No automated threat intelligence tools :** tools like MISP Malware Information Sharing Platform would allow near real time exchange of raw data and Indices of Compromise (IOC)
   - **African FSP or MNO poorly represented** in FS-ISAC and FASG

A comprehensive, cost efficient and scalable organisation


Board of Directors
Advisory Board
Africa Cyber Security Resource Centre
Strategic Advisory
Capacity Building
Coordination & Partnerships
Research Development Innovation
Information Sharing & Analysis Centre
Unit 1 Cyber Security Response Team
Unit 2 Cyber Security Response Team
Unit 3 (*) Cyber Security Response Team
CSIRT
CSIRT
CSIRT
Suricate Sénégal
SOC 1
SOC 2
SOC 1
SOC 2
SOC 1
SOC 2
Advisory 1
Advisory 2
Advisory 1
Advisory 2
Advisory 1
Advisory 2

(*) Number may be increased at a later stage

The cyber security ecosystem will include all (interested) stakeholders.



Africa Cyber Security Resource Centre

Funding

Work Groups

Coordination & Partnerships

Communication

Quarterly Conferences

FINCLUCERT Threat Intell. Crisis Mgt

CIRCL MISP Threat Sharing

Sector Policy Makers (tbd dedicated meetings/ upon invitation / limited Membership)

- Policy Makers
- Supervisors

National/ Internat. authorities (upon invitation)

- Local LEA
- International LEA (Interpol, Europol, FBI…)
- National CERTs
- Nat. Cyber Security. / Data protect. Agencies

Partners (limited membership)

- Universities
- Profess. Assoc., Networks
- Donors
- Cyber Security Service Providers
- Vendors

FSP Full Membership

- FSP

CORE TRUST CIRCLE

Thank you and join the venture !