Building a cyber security resource center in low capacity environments

Pascal Steichen, SECURITYMADEIN.LU
Jean-Louis Perrier, Suricate Solutions

November 20th, 2019
About us

A consortium of >200 high-level cybersecurity experts from Europe and Africa

SECURITYMADEIN.LU: cybersecurity agency of the Luxembourg Ministry of the Economy
  • Mission: improve and enable cybersecurity of the Luxembourg ecosystem and fostering innovation
  • R&D in tools and methodologies (e.g. ROOM#42, the 1st cyber attack simulator made in Luxembourg; MISP, the reference Threat Sharing Platform; MONARC, a pragmatic risk management method and platform)
  • Part of the international CERT community (e.g. FIRST); Involved in international Awareness Raising (e.g. INHOPE); Member of the national Cybersecurity Board Crisis Management at national level

SnT: Interdisciplinary Centre for Security, Reliability and Trust from UNIversity of Luxembourg, 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, delivers all cyber security services required to Identify, Protect, Detect, Respond and Recover.
  - Recognized experts on incident response & a strong track record for FSP
  - Leading cybersecurity company in Luxembourg with >130 experts
Objectives

Improve the resilience of financial inclusion institutions and protect their customers against cyber attacks, to

(1) foster financial inclusion
(2) secure the development of Digital Financial Services
(3) allow building interoperable payment systems

A model for Sub-Saharan Africa
General directions

Inspired by
- CGAP’s cybersecurity diagnosis and strategy
- Sectoral experience (worldwide) in Financial Services and Telecom
- Momentum and lessons learned from Suricate Solutions’ “Regional Cybersecurity Operation Centre” in Senegal

Continental and regional strategy, with proximity teams
- Sub Saharan Africa and Financial Inclusion in 1st phase, other sectors/regions possible once established
- Proximity for appropriate and continuous institutions support and capacity building

Sustainable business model and lasting capacity building
- Fast & cost effective setup: rely on/reuse existing structures, ecosystems, know-how, experience, open source software
- PPP: Setup and investments have to be subsidized, operation costs should gradually be supported by users
- Scalability: Prototype then roll out in SSA, coordination between entities to avoid duplicates
- Efficiency: lessons learned taken from proven international best practices & organisations
- Fostering innovation & local development

Inclusivity
- Services available to all size of FSP & Fintech at reasonable costs, all partners welcome
- Contribute to close the gender gap
Two great sectoral inspiration sources
Lessons learned from FS-ISAC and GSMA Fraud and Security Forum

Efficient and long-standing initiatives build on the strength of the private sector
To information sharing trust communities are key
  • Closed or open meetings depending on members’ decision and information sensitivity
  • Closed to exchange most sensitive data with trusted peers
  • Opened to third parties if relevant/needed to share best practices
  • Not a substitute to the legal or regulatory processes
Central banks, policy-makers, supervisors have a specific status to ensure FSPs are sharing in trust.
Regular physical meetings and workgroups are necessary to build trust and share high-level analysis.
Services that do not include sensitive data, e.g. capacity building, training, threats observatory, advisory, may be delivered to all stakeholders.

Limitations
  • Most active presence from major players (large FSP, international MNO networks), limited African presence
  • More oriented towards prevention than incident response
  • No automated threat intelligence tools
Organizational concept based on 3 levels

- **Strategic:** Cybersecurity Resource Centre
  - [independent/international organisation]
  - global coordination and partnerships
  - funding (grants from donors, yearly membership depending on size of FSP)
  - strategic advisory for policy makers
  - capacity building, crisis simulation, awareness raising
  - R&D: threat/malware, methods and PoC tools
  - Coordination CSIRT, mainly in charge of Threat Intelligence Management (e.g. via MISP)

- **Tactical:** (Sub-)regional CSIRTs (focus on Incident Response and support services)
  - [private organisation]
  - Covering 3 areas (to start with): West and Central Africa (French-speaking), West Africa (English-speaking), East Africa (English-speaking)
  - Provide Level 3 support for a cluster of SOC (detection, analysis, forensic, remediation, recovery, crisis management)
  - Advisory services (Security Strategies, Policies, Maturity assessment, Risk Management…)
  - Training, Pentesting, Application security…

- **Operational:** local/proximity SOCs (focus on detection, analysis and recovery)
  - [private organisation]
  - Detection services with 24x7 security monitoring, vulnerability scanning,
  - Proximity advisory services, armed wing of sub-regional CSIRT (see above) for local interventions and or forensic analysis
  - 1-2 SOCs per CSIRT (can be collocated)
A comprehensive, cost efficient and scalable structure

3 levels: 1 central coordination organization + (sub-)regional Computer Security Incident Response Teams (CSIRT)* + limited number of local/proximity operational teams (SOC)

(*) Project foresees to start with 3 sub-regional CSIRTs, at a later stage more can be implemented
The cybersecurity ecosystem shall include all (volunteer) stakeholders.

Africa CyberSecurity Resource Centre

- Funding
- Coordination & Partnerships
- Communication
- Conferences

FININC-CSIRT Threat Intell Crisis Mgmt

FININC-CSIRT

Sector Policy Makers
(dedicated meetings upon invitation limited membership)

- Policy Makers
- Supervisors

National/International Authorities
(upon invitation)

- Local LEA
- International LEA (Interpol, Europol, FBI...)
- National CSIRT
- National Cybersecurity / Data Protection Agency

Partners
(limited membership)

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

FSPs
(full membership)

- FSP
- SOC

CORE TRUST CIRCLE

Work Groups

Conferences

Communication

Coordination & Partnerships

Funding

On behalf of

CGAP  giz
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Federal Ministry for Economic Cooperation and Development

LUXEMBOURG AID & DEVELOPMENT

EUROPEAN MICROFINANCE WEEK
connecting the inclusive finance world
Project highlights
A breakthrough for Financial Inclusion

❖ North/South public-private partnership: consortium work started in January 2019

❖ Build & mobilise a comprehensive and sustainable cyber security ecosystem in 3 to 5 years

❖ Ability to deliver, fast implementation

❖ A thorough governance

❖ USD 6-10 million budget + service fees from FSP + membership fees → great economies of scale

❖ High Impact for financial inclusion and for the continent

❖ Feedback/contributions welcome
Proposed Governance of Africa-CSRC

**Legal status:** Economic Interest Group (EIG). Flexible status, fits for profit & non-profit organisations, well adapted to projects and NGO.

**Location:** HQ (EIG) hosted in Luxembourg to foster capacity building, rely on longstanding support for Financial Inclusion, and offer a neutral location. Limited HQ resources (program management) progressively transferred to Africa

**Advisory board:** provides strategic direction, contacts, guide quality improvement, assess program effectiveness. 6 to 8 senior experts having quarterly/biannually meetings, chosen amongst
- Representatives of the international CSIRTs and/or Academic cybersecurity community
- Financial Inclusion community (e.g. CGAP, large MFI network, Central Banks)
- International Organisations (e.g. World Bank Group, AFI, GSMA, ITU…)

**Board of Directors:** set out strategic objectives and policies, select, support and review the performance of the executive director, ensure the availability of adequate financial resources, approve and control budgets and salaries, account to the stakeholders for the centre’s performance; Directors shall represent
- Luxembourg Consortium (SECURITYMADEIN.LU, Uni.lu/SnT, Excellium Services, Suricate Solutions)
- Funders, donors, e.g. AfDB
- Partner or hosting country authorities
Timeline of Africa-CSRC setup

**Objective:** Establish coordination centre and 3 sub-regional (West Africa and East Africa) CSIRTs and a few SOCs within the first 3 years, and reach full maturity in the 5th year

**1st year – Initiate:** set up the governance and the central structure, identify countries/regions to establish local entities, hire key managers, start awareness and local prospection, raise interest for the community and identify champions, establish open source model for a comprehensive toolset for CSIRT and SOC activities, reinforce existing SOC in Senegal and extend to other French-speaking countries

**2nd year – Roll-Out:** roll out of 1st CSIRT for French-speaking region, roll out of 2nd CSIRT and SOCs for English-speaking countries (e.g. East Africa)

**3rd year – Replicate and Expand:** roll out of 3rd CSIRT and SOCs for further English-speaking countries (e.g. West Africa); Identify needs for additional SOCs for large countries or group of countries (not budgeted here)

**4th and 5th year – Optimise and reach break-even**
Financial inclusion: small market with low resources and low profitability, limited interest from ICT/Security players (looking after more profitable banks and Telco) and traditional investors in ICT (3 or 4 years long ROI)

Long and hazardous process: Recruiting, training and retaining qualified resources, awareness cycle, decision cycle, funding cycle, achieving profitability, quality control

Limited number of local actors/partners, split between IT players delivering some security services, mostly infrastructure, and small security players who cannot deliver SOC/CSIRT services due to the need for specialized expertise and investments

The innovative approach of the consortium

• Focus on developing local champions and capacity and specialised knowledge transfer to Africa relying on Luxembourg’s (and partners’) long-term expertise and experience
• Minimise technical and financial execution risk thanks to the available know-how (200 experts),
• Knowledge of the field, credibility and references acquired in the last 3 years in Senegal

Key lessons learned from previous experience (Suricate SOC in Senegal)

Business Model 1/2
Business Model 2/2

Ensure sustainable operations within 3 to 5 years

- **Donors**
  - 1) Grants, loans

- **Investors**
  - 2) Equity, loans

- **Africa CyberSecurity Resource Centre**
  - 3) Subsidising setup
  - 4) Membership fees
  - 5) Community Membership fees

- **Unit 1 CyberSecurity Response Team**
  - CSIRT
  - SOC
  - Advisory

- **Policy Makers**
  - National CERTs
  - Universities
  - Cyber Security Service Providers

- **FSP**
  - 6) SOC Setup costs
  - 6) Periodic costs
  - 6) Advisory fees

---

1), 2) Initial Financing to set up the structures on the 3 levels and ensure the balance of operations for the launch within 3 years. Loans may be introduced in a 2nd step.

3), 4) CSIRT/SOC structures are subsidised the first years but pay a membership fee for support and coordination.

5) Participants to the CSRC pay a yearly fee depending on their size and category.

6) FSP pay for the service they get from the CSIRT (incident response) and SOC (monitoring) or advisory services (one time or recurring fees). SOC setup may also be subsidised.
Our contribution to Public-Private partnership investment and capacity building for developing countries, especially in ICT/cybersecurity.

- Strengthen the capacity of financial institutions to extend access to banking and financial services.
- Stimulate the growth of micro-enterprises and SMEs and their integration into the formal sector, including through access to financial services.
- Facilitate the establishment of a sustainable and resilient infrastructure by strengthening financial, technological and technical support.
- Increase access to ICT technologies and ensure that all inhabitants have access to the Internet.
- Support national institutions in the fight against (cyber) crime.
- Support women’s access to security engineering, ensure equal opportunities, special support for financial inclusion institutions oriented towards women.

Ensure the access to technical education including at university-level, significantly increase the number of digitally-skilled people (all ages), including technical and vocational skills, relevant for employment and entrepreneurship.
Thank you and welcome in the venture!

pascal.steichen@securitymadein.lu
tegawende.bissyande@uni.lu
jlperrier@suricatesolutions.com
## Work packages and « owners »

<table>
<thead>
<tr>
<th>WP</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central organisation</td>
<td></td>
</tr>
<tr>
<td>Governance &amp; PMO</td>
<td>Consortium</td>
</tr>
<tr>
<td>Strategic Advisory</td>
<td>Consortium</td>
</tr>
<tr>
<td>Capacity Building</td>
<td>SECURITYMADEIN.LU</td>
</tr>
<tr>
<td>Coordination &amp; Partnership</td>
<td>Consortium</td>
</tr>
<tr>
<td>RDI Research, Development, Innovation</td>
<td>SnT</td>
</tr>
<tr>
<td>Information Sharing &amp; Analysis Centre</td>
<td>SECURITYMADEIN.LU</td>
</tr>
<tr>
<td>Regional organisations (x3)</td>
<td></td>
</tr>
<tr>
<td>CyberSecurity Incident Response Team (CSIRT)</td>
<td>Suricate / Excellium</td>
</tr>
<tr>
<td>CyberSecurity Operation Centre (C-SOC)</td>
<td>Suricate / Excellium</td>
</tr>
</tbody>
</table>