Generating CTI In New Frontiers: An African Case Study.

Muchilwa Lawrence – I craft solutions.
Cyber Security Operations Center Manager, Threat Intelligence
https://overwatch.or.ke www.testmyids.ke
Generating CTI In New Frontiers: Africa Case Study

We started consuming…now we start cooking and spicing what we consume.

Planning and Direction

- How do you generate relevant CTI in an environment where technical competencies, budget, politics and trust want to slow you down and finish you off?
Let's Go Back.....Where Have We Come From?

- CTI consumption has matured. From getting and processing feeds to a need of generating feeds.
- CTI sharing platforms, frameworks have also matured and improved.
  - BUT ???
- CTI generation is still more focused on honey**...deploy this and get that, and repeat.
  - Do we have Ferraris but lack drivers???
  - Individual honeypot deployment doesn’t scale well on a national level.
    - You can’t deploy and manage all honeypots and sensors
Generating CTI In New Frontiers: Africa Case Study

> How do you generate relevant CTI in an environment where technical competencies, budget, politics and trust want to slow you down and finish you off?
Generating CTI In New Frontiers: Africa Case Study

Planning and Direction
- Know your constituency and what is important, relevant to them.
  - Public Private partnerships
  - Shared Prosperity
  - OT Needs are different to Telco Need.
  - Threat modelling can help with narrowing down what needs to be collected.

Collection
- Use constituencies and deploy relevant sensors.
- Give access to the insights for operational, tactical or strategic use
As a national CERT or similar body.....

- Adopt, refine the multi stakeholder approach as championed by eg ISOC.
  - Go horizontal
    - Public Private partnerships
    - Shared Prosperity
  - Identify your constituency.
    - You cant do this alone, too big a surface
  - Communicate, identify champions.
    - Build trust
  - Foster transparency and gain trust
  - You need to scale efficiently and get visibility.
As a national CERT or similar

- Reduce or eliminate the learning and management overhead.
  - Create simple manuals to setup sensors, do basic troubleshooting.
  - Avoid burdening constituencies with operational responsibilities.
  - Docker compose files can do magic

- Go affordable and open source.
  - Docker based honeypots...maximize each hardware you have
  - ELK
  - MISP

- Integrate Other CTI feeds to reduce noise or further enrich what you have.
  - No need to reinvent the wheel.

- Finally, share with CTI community using existing tools:
  - MISP
Final Product