Establishment of CERTs/CIRTs in the region

Abuja, Nigeria, 27- 29 August 2018
Serge Valery ZONGO
Program officer
ITU regional Office for Africa

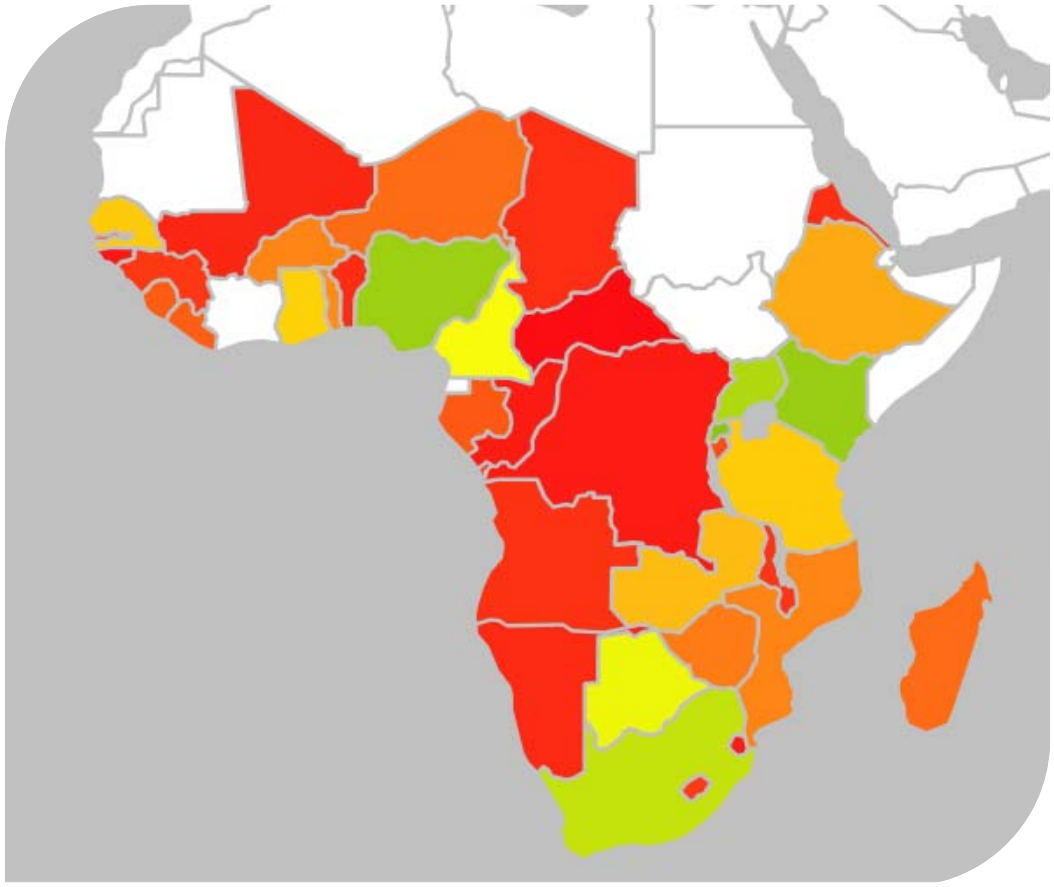
Outline

- Coordinated Response
- Why a CIRT
- ITU CIRT Framework

Coordinated Response

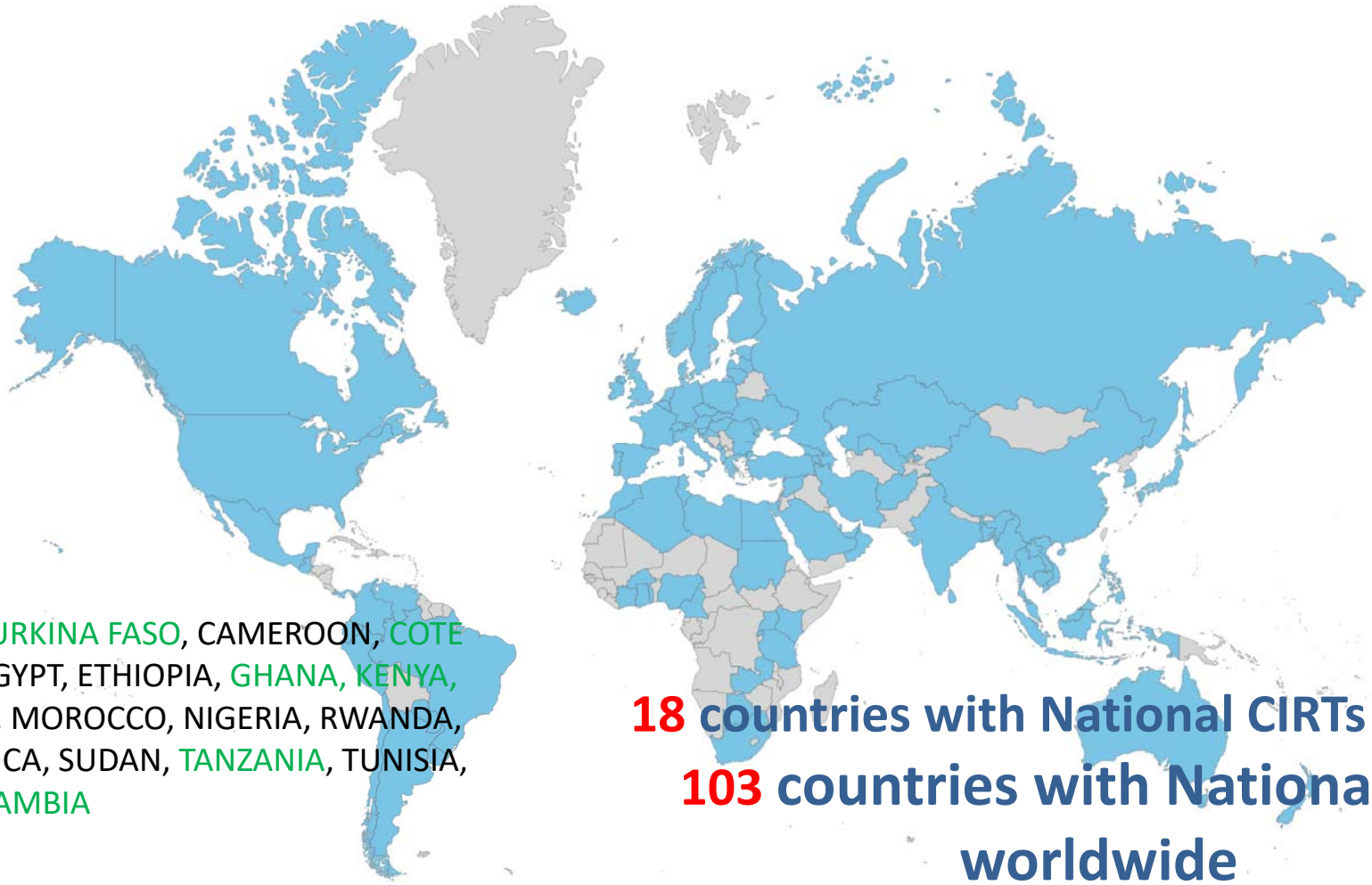
Need for a multi-level response to the cybersecurity challenges

Cybersecurity Heat Map for Africa



Source: GCI ITU

CIRTS in Africa



ALGERIA, BURKINA FASO, CAMEROON, COTE D'IVOIRE, EGYPT, ETHIOPIA, GHANA, KENYA, MAURITIUS, MOROCCO, NIGERIA, RWANDA, SOUTH AFRICA, SUDAN, TANZANIA, TUNISIA, UGANDA, ZAMBIA

18 countries with National CIRTs in Africa

103 countries with National CIRT worldwide

What is a CIRT ?

- CIRT Computer Incident Response Team
- CSIRT Computer Security Incident Response Team
- CERT Computer Emergency Response Team
- CIRC Computer Incident Response Capability
- IRC Incident Response Center or Incident Response Capability
- IRT Incident Response Team
- SERT Security Emergency Response Team
- SIRT Security Incident Response Team

There are different types of CERT/CIRT or response teams
It could be for a government/private/organisation/region
The constituency/mission contributes to the services offered

The Importance of a CSIRT

- It is critical that mechanisms are in place to:
  - Effectively detect & identify the activity
  - Develop mitigation & response strategies
  - Establish trusted communications channels
  - Effect a coordinated response
  - Share data & information about the activity
  - Track & monitor this information to determine trends & long term remediation strategies

Benefits

- Serve as a trusted point of contact
- Focused response effort
- Develop capabilities to support incident reporting
  - Standardised process
- Conduct incident, vulnerability & artefact analysis
- Participate in cyber watch functions
- Help organisations to develop their own incident management capabilities
  - Make security best practices & guidance available
- Provide awareness, education & trainings

The role of a CIRT

- Cybercrime is a global problem, so it goes without saying that it needs a global response.
- Need to build up national cyber defense
  - CERTs, CSIRTs, national security agencies, etc.
  - Improve incident response capability – how fast can we respond to attack
- CSIRT can provide a single point of contact for dealing with cyber security incidents

CSIRT Functions

- Provides a single point of contact for reporting security incidents
- Assists the organisational constituency and general computing community in preventing and handling computer security incidents
- Shares information and lessons learned with other response team
- Collaborate with law enforcement agencies and local authority bodies

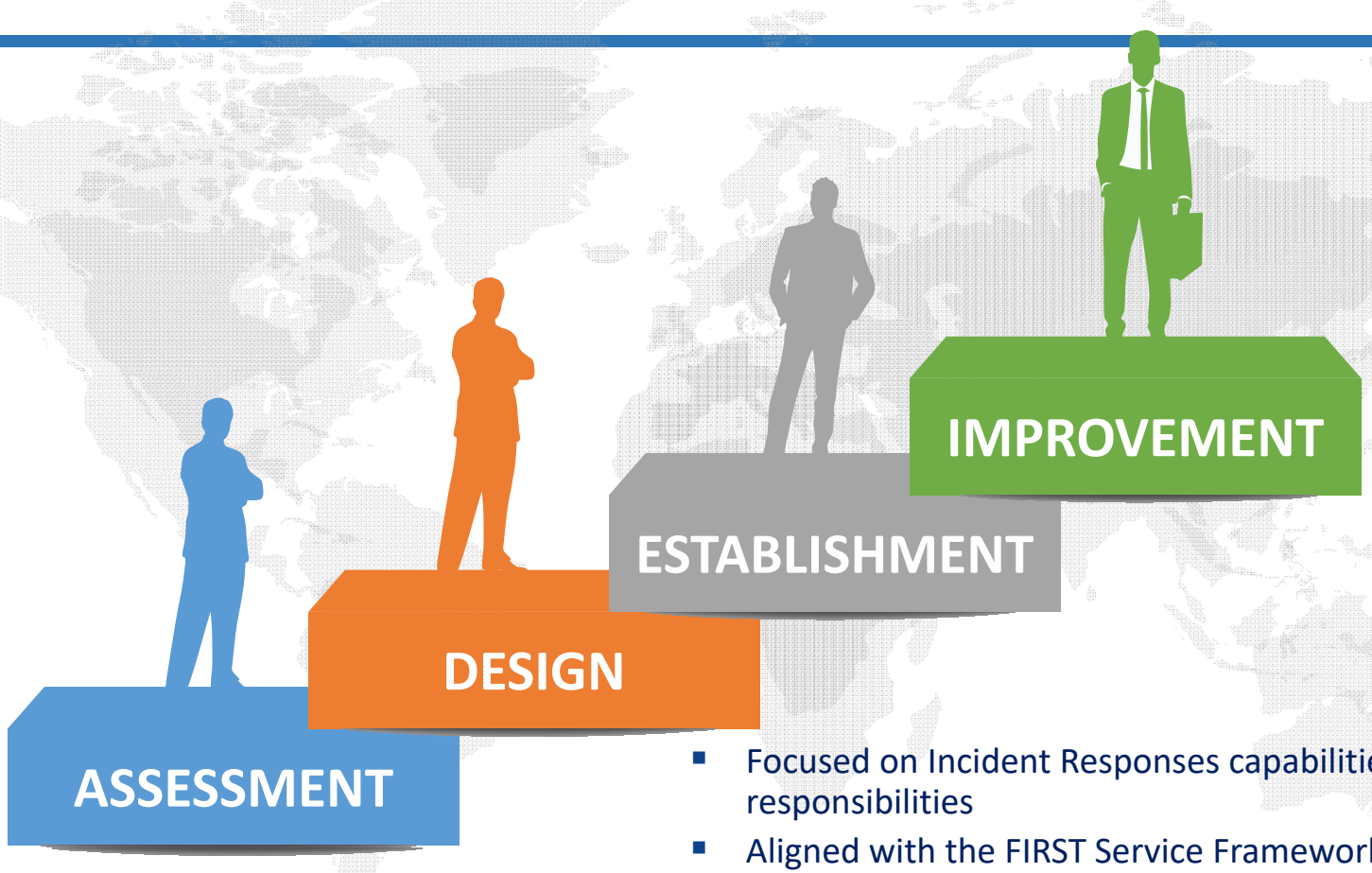
Type of CSIRT

- **Academic Sector** - to academic and educational institutions
- **Commercial** - provides CIRT services commercially to their constituents
- **CIP/CIIP Sector** - covers all critical IT sectors in the country
- **Governmental Sector** - provides services to government agencies
- **Internal** - provides services to its hosting organisation only
- **Military Sector** - provides services to military organisations
- **National** - considered as security point of contact for a country

Type Of Incident Response Team

- National Incident Response Team
- Organizational Incident Response Team
  - Governmental CIRT
- Multi-Organizational Incident Response Team
  - UN-CSIRT , CERT-EU
- Sectorial Incident Response Team
  - Financial Institution CIRT
- Regional Incident Response Team
  - AfricaCERT, APCERT , OIC-CERT

ITU CIRT Framework



- Focused on Incident Responses capabilities with National responsibilities
- Aligned with the FIRST Service Framework

ITU CIRT Framework Explained

Assessment Service	
Description	Review the current incident response capabilities present at the national level
Activities	▪ Administering CIRT questionnaire ▪ Analyzing response ▪ Performing on-site visit for review and finalization
Key Deliverables	Assessment report
Modality	Off-site and On-site
Finance	Covered by ITU

ASSESSMENT

ITU CIRT Framework Explained

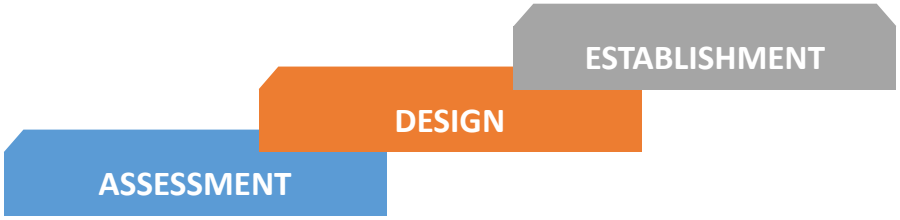
Design Service	
Description	Develop a blueprint of the National CIRT project, with the related implementation processes
Activities	▪ CIRT positioning ▪ Identify CIRT Services ▪ Identify processes and related workflows ▪ Identify policies and procedures ▪ Relationship with constituency and communication strategy ▪ Technology ▪ Premises ▪ HR
Key Deliverables	CIRT design document and implementation plan
Modality	Off-site and On-site
Finance	Covered by the country

ITU CIRT Framework Explained

Establishment Service	
Description	Execute the project as agreed with the Member States and based on the outcomes of the Design Service's deliverables
Activities	▪ Capabilities development ▪ Capabilities deployment and testing ▪ Customization, fine tuning and training ▪ Operations ▪ Handover and closure
Key Deliverables	▪ SOPs ▪ Operating manuals ▪ Training material ▪ Tools
Modality	Off-site and On-site
Finance	Covered by the country

Typical services that the CIRT will provide to the constituency

- Incident handling
- Incident analysis
- Outreach and communication

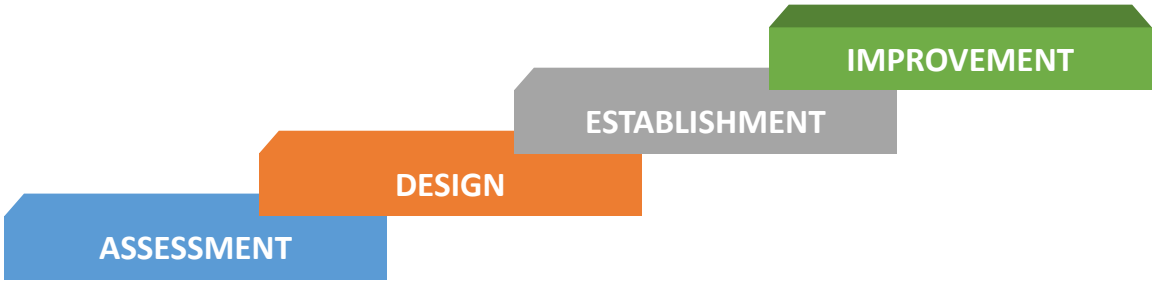


ITU CIRT Framework Explained

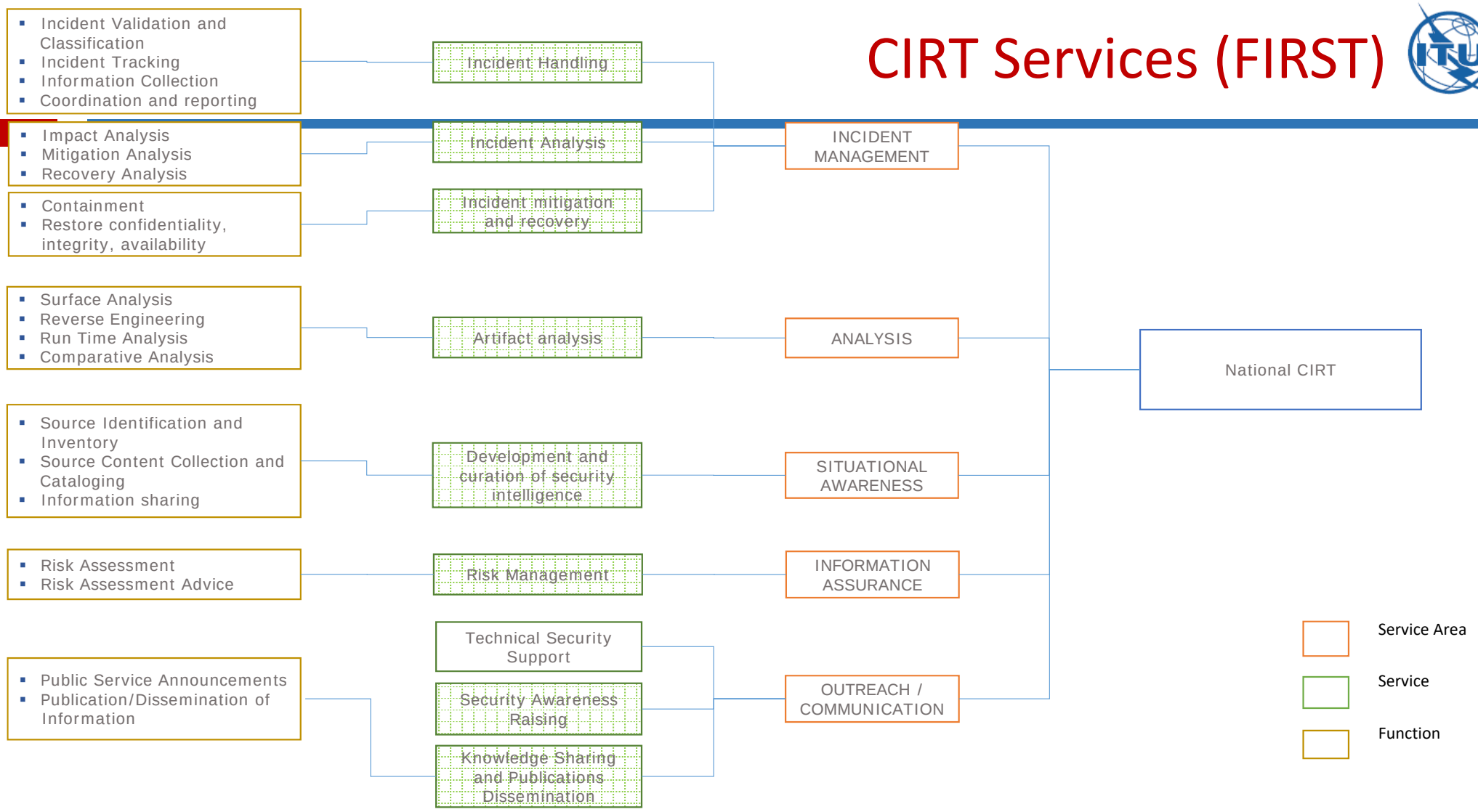
Improvement Service	
Description	Enhance Existing CIRT capabilities and operation
Activities	▪ Environment Analysis ▪ Capabilities deployment and testing ▪ Customization, fine tuning and training ▪ Operations ▪ Handover and closure
Key Deliverables	▪ SOPs ▪ Operating manuals ▪ Training material
Modality	Off-site and On-site
Finance	Covered by the country

Typical services that the CIRT will provide to the constituency

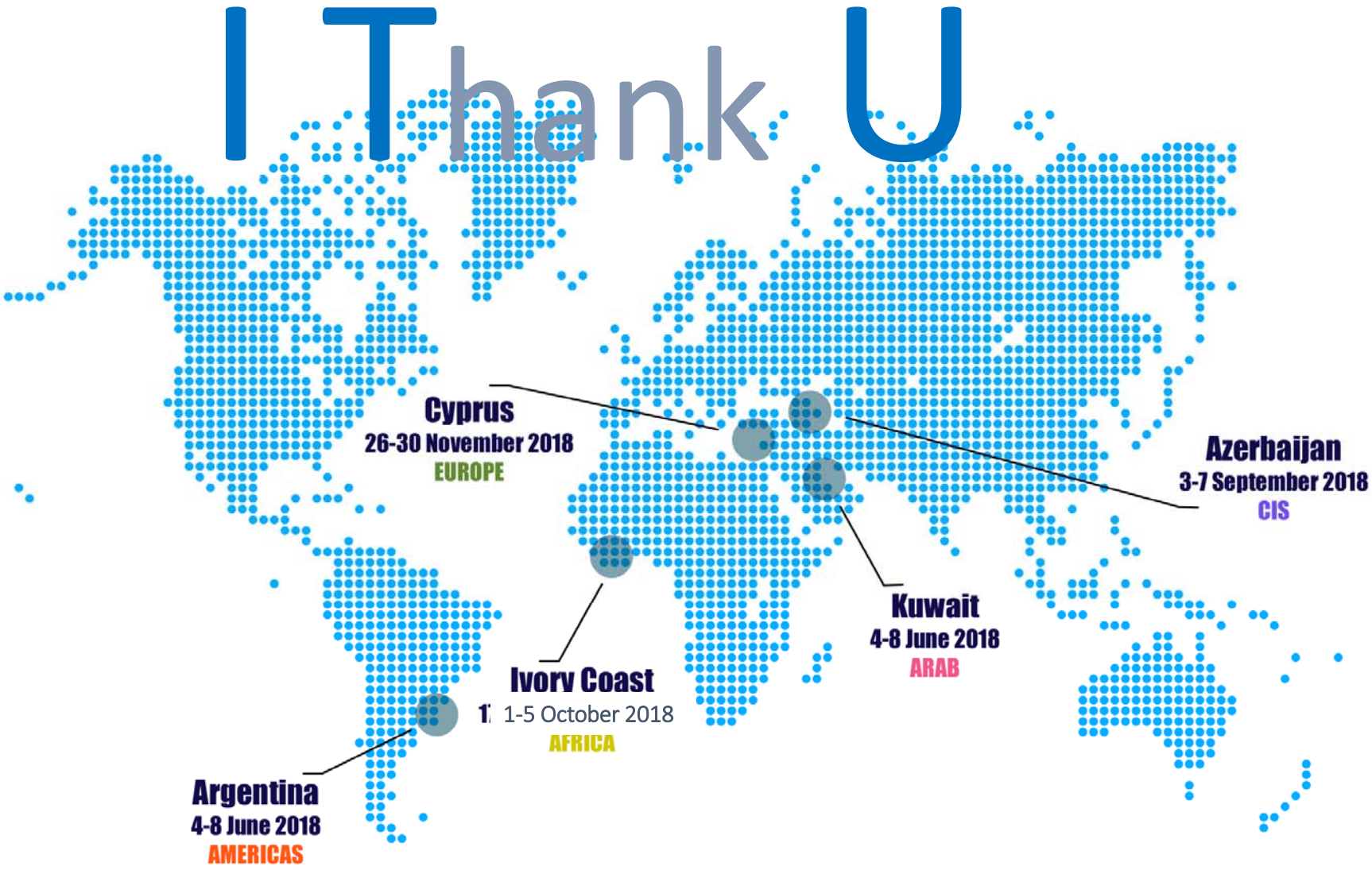
- Analysis (Artifact, media)
- Situational Awareness (Sensor operation, fusion and correlation)



CIRT Services (FIRST)



I Thank U


Cyprus
26-30 November 2018
EUROPE
Azerbaijan
3-7 September 2018
CIS
Kuwait
4-8 June 2018
ARAB
Ivory Coast
1-5 October 2018
AFRICA
Argentina
4-8 June 2018
AMERICAS