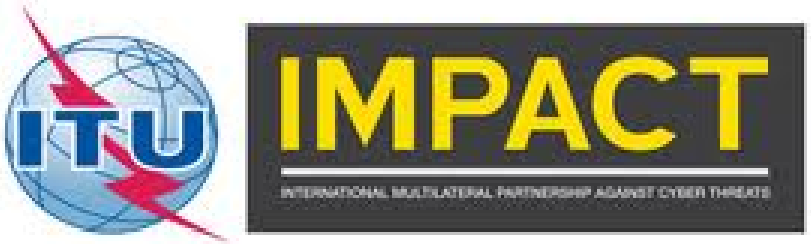
Information Session
ITU-IMPACT

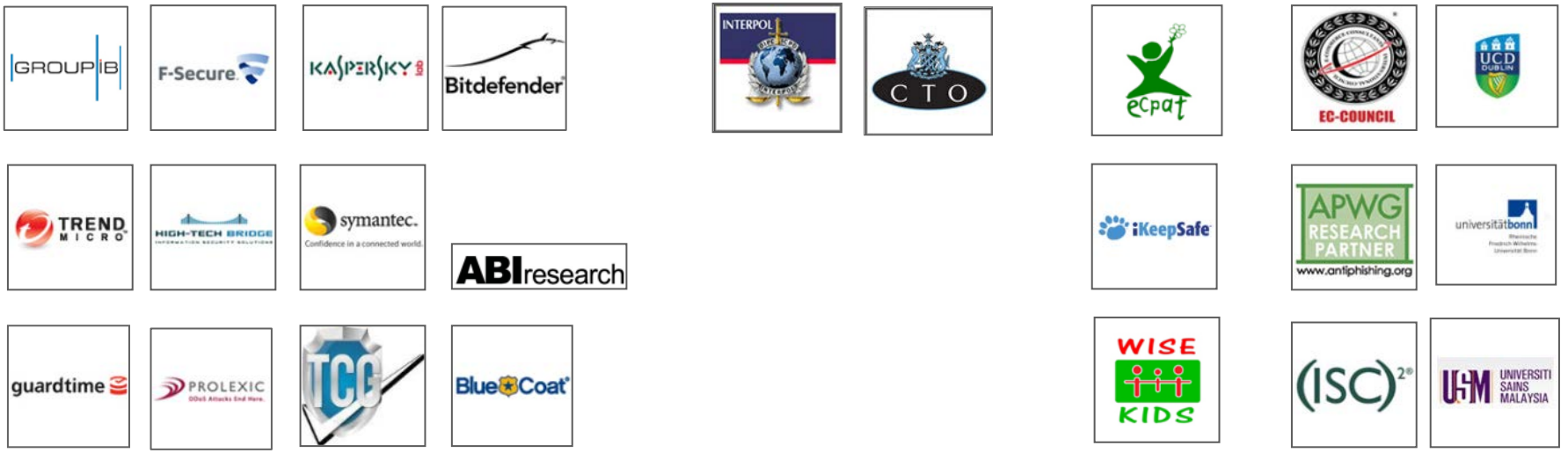
Marco Obiso
Cybersecurity Coordinator

What it is

- A multistakeholder partnership
- Open to all stakeholders – governments, industry, civil society, academia, international and intergovernmental organizations
- Main objective is to share knowledge, build capacity and promote a global culture of cybersecurity



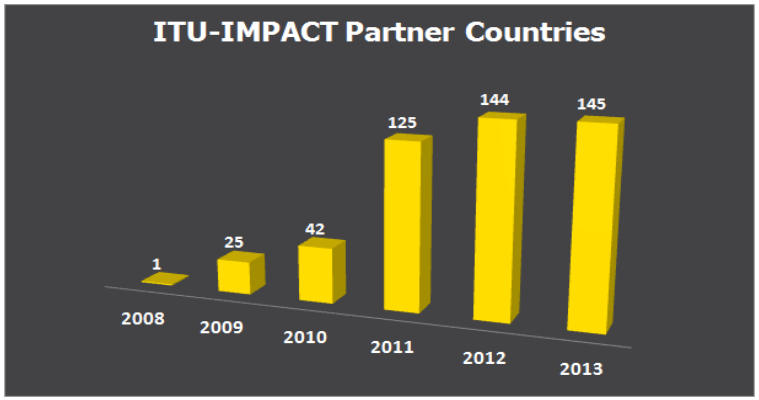
ITU-IMPACT's Global Partnership

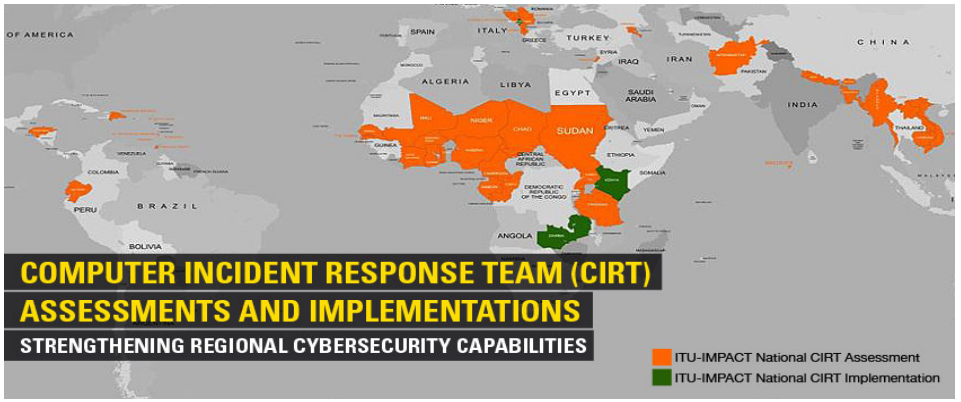


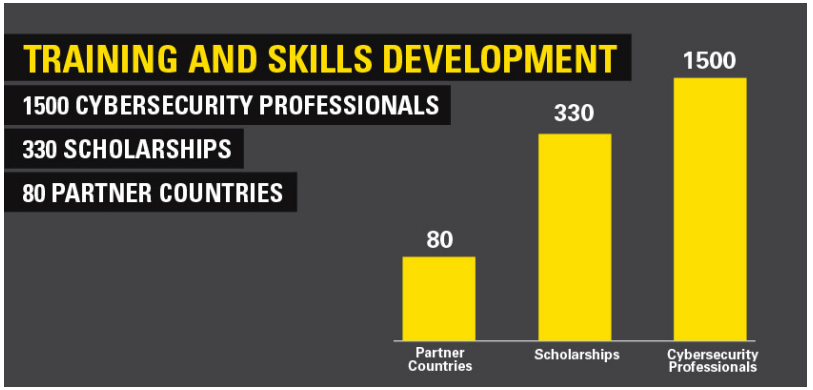
- 18 Partners from Industry – More than 20 partners from academia, research and civil society
- Partners in 5 continents, including countries such US, Russian Federation, Switzerland, Germany, Canada, Japan, Finland, UK, South Africa, Nigeria, Oman, Thailand

145 ITU Member States joined IMPACT

ITU-IMPACT overall status







- National CIRT assessment & implementation conducted for over 40 countries
- Cyber drill conducted for CIRT/CERTs in 18 countries over 3 regions
- Trained over 1500 cybersecurity professionals and practitioners over 80 countries
- Deployed over 300 scholarships to over 40 countries

N-CIRT Readiness Assessment

Readiness assessment on the establishment of national incident response centres N-CIRT, in line with WTSA 12 Res 58 and WTDC 10 res 69 (conducted for over 40 countries)

- The main objective is to study and evaluate the country National CIRT's structure and capability to ensure that ICT security incidents, intrusion attempts, and emergencies are appropriately managed by the countries to levels consistent with industry standards and good business practices
- ITU-IMPACT reports on key issues and analysis, recommending a phased implementation plan for National CIRT.

•N-CIRT assessment already done in
  - Africa
  - Arab
  - Asia Pacific
  - CIS
  - Caribbean
  - 42 countries covered

•Some 10 countries foreseen in 2013
  - Europe
  - South America

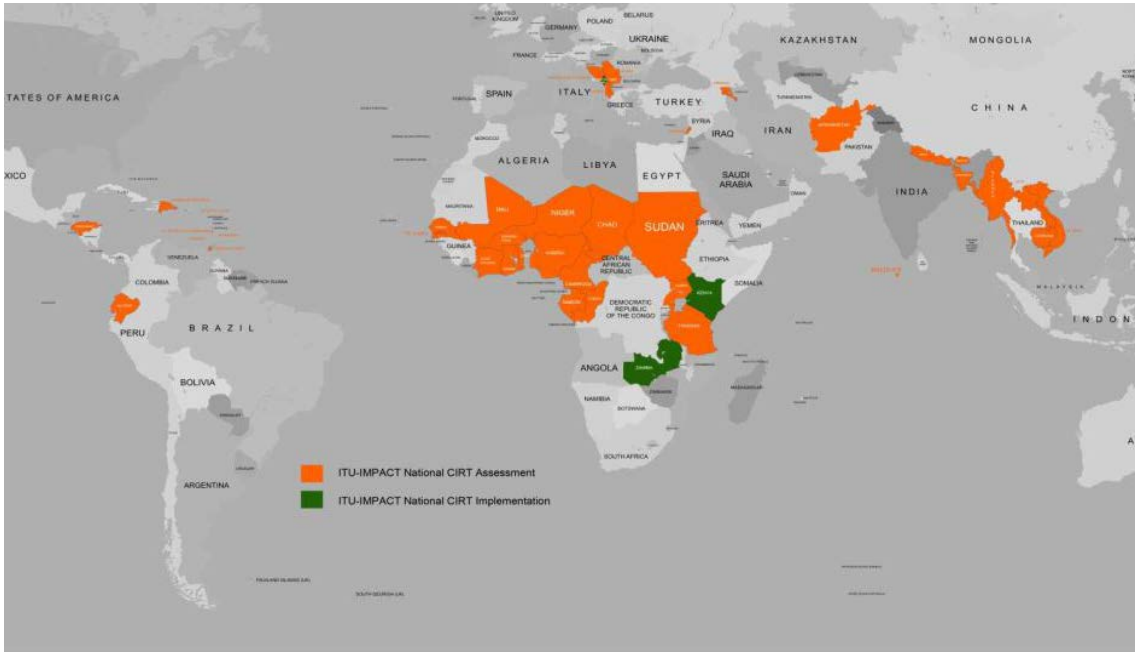
N-CIRT Deployment

National Computer Incident Response Team

- To assist countries to setup National CIRTs to proactively manage ICT incidents and responding to cyber threats
- As of 2013, ITU-IMPACT has implemented 5 national CIRTs
  - Montenegro
  - Zambia
  - Kenya
  - Burkina Faso
  - Uganda

Planned Implementations for 2013 - 2014

- Tanzania
- Ivory Coast
- Burundi
- Barbados
- Monaco
- Trinidad and Tobago
- Jamaica
- Macedonia
- Bhutan



Training & Skills Development

a) Trained more than 900 cybersecurity professionals and practitioners

b) Deployed over 300 scholarships to 46 partner countries globally to create more cybersecurity professionals

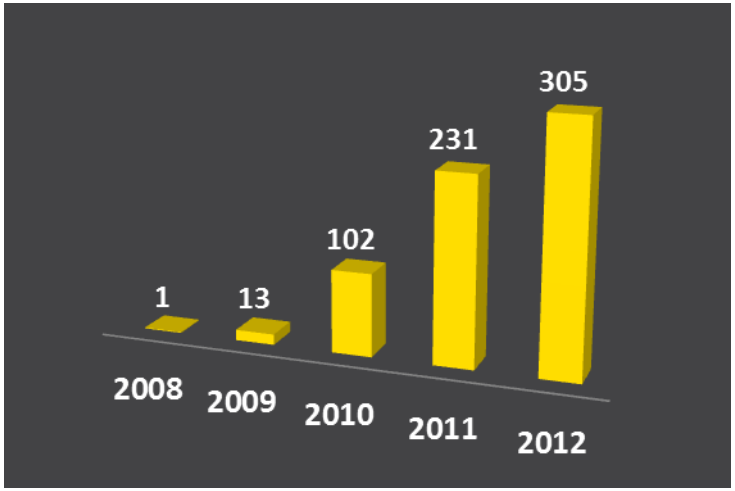
c) Trained 50 law enforcement officers from five countries on Network Investigation to enhance skills and investigation in cybercrime

d) ITU Asia Pacific Centre of Excellence training on Securing Networks (19 countries attended)

a) Planned training for 2012-2013

- Mobile Security – ITU Asia Pacific CoE Training
- ABI Research sponsored training – 2 trainings in 2013
- Regional training:
  - Eastern Europe
  - Asia Pacific
  - Africa
  - South America

b) ITU-IMPACT Security Essentials to be deployed across all 145 partner countries.



ITU Regional Cybersecurity Centres

To further enhance nations' capacity and capability in cybersecurity, the setting up of regional centres will help to provide a more concerted and regional efforts in this endeavour

Oman-ITU-IMPACT Initiative

The 1st regional centre is hosted by Oman for the Arab region covering 22 nations. Oman is represented by the Information Technology Authority (ITA) and Oman CERT (OCERT)

Information Technology Authority
Sultanate of Oman

e.oman

Nigeria-ITU-IMPACT Initiative

NITDA
National Information Technology Development Agency

The 2nd regional centre will be hosted by Nigeria for the African region covering up to 52 countries. Nigeria will be represented by the National Information Technology Development Agency (NITDA)

Other countries have expressed interest to host centers for their respective regions

Cyber Drill

Applied Learning for Emergency Response Team (ALERT)

- Designed to maintain and strengthen international cooperation between partner countries and ensure a continued collective efforts against cyber threats and exercises designed to enhance communication and incident response capabilities.
- The cyber drill simulation runs through a scenario with each participating country divided into two roles, representing a player and an observer
- Cyber drills conducted:
    - Dec 2011 – Cambodia, Lao, Vietnam & Myanmar (4 CERTs)
    - July 2012 – Qatar, Oman, Sudan, Egypt, Tunisia & UAE (5 CERTs)
    - Oct 2012 – Europe & CIS Region (8 CERTs)

Cyber Drills planned for 2013

- South America – 3nd Quarter 2013
- Caribbean – 3rd Quarter 2013
- Arab – 4th Quarter 2013

Collaboration

INTERPOL

- In expanding collaborations, IMPACT have signed MoU with Interpol during the General Assembly in Rome on 6th November, under the framework of ITU-IMPACT
- Memorandum of Understanding (MoU) will see collaboration in the following areas:
  - To promote capacity building in the area of cybersecurity
  - To share and exchange information on digital forensics, malware and information relevant to cybersecurity
  - To assist in cybercrime investigation

Cybercrime Investigation

- ITU-IMPACT initiated malware investigations in 2012 with Kaspersky Labs.
- Kaspersky Labs detected the Flame & Gauss malware. ITU-IMPACT issued the alert to all 145 countries
- ITU-IMPACT immediately made the tool available to all its 145 partner countries globally and this collaboration and effort has helped nations mitigate these attacks that could have potentially cause major disruption any economic losses to these nations

Learn more about ITU-IMPACT

- Regular meetings (once a year) of
  - International Advisory Board (IAB)
  - ITU-IMPACT Partners
- Regular reporting of activities at ITU Council
- Presence at WSIS Forums 2009 until date
- Monthly newsletters distributed to all partners and member countries

CYBERSECURITY (at) ITU.INT