Approaches and Practices for Increasing Maturity and Capabilities for CSIRTs in Emerging Economies

Jean-Robert Hountomey, Unal Tatar, Sherif Hashem, Kaleem Ahmed Usmani, Hayretdin Bahsi

March 2, 2022

Project Goal

This project aims to create a tailorable guide for emerging economies to develop or improve their CSIRT capabilities in an affordable way to respond to the evolving cyber threat environment effectively.

Methodology

- Desk review
- Data collection and analysis
  - Surveys
  - Interviews
- Validation

Project Reports

Part 1: Literature review

Literature Review

- Maturity models
- N-CSIRT guidelines and best practices
- Tools
- Trainings
- Legal frameworks
- Specific national practices

Part 2:
Current state and future projection of N-CSIRTs in emerging economies

Results of Survey & Interviews

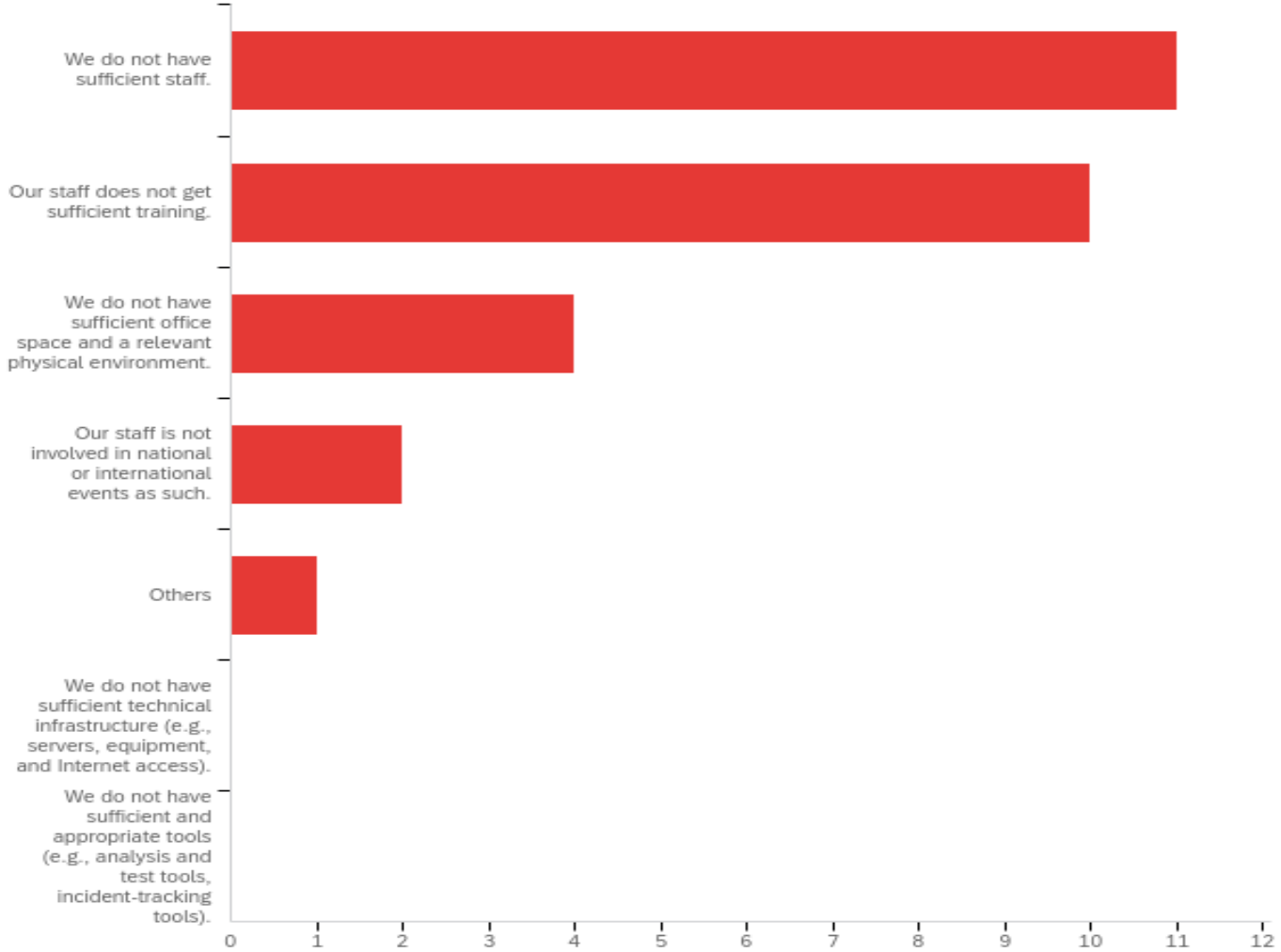
Survey

- Conducted a survey to understand which services those CSIRTs deliver, what type of technical and organizational capabilities they have, what their medium- and long-term goals, and their best practices in capacity building.
- The findings of the desk review were utilized for identifying the objectives and questions of the survey of low-income N-CSIRTs.
- 28 respondents representing N-CSIRTs participated in the survey, but incomplete or repetitive submission were excluded, resulting in 16 final responses.

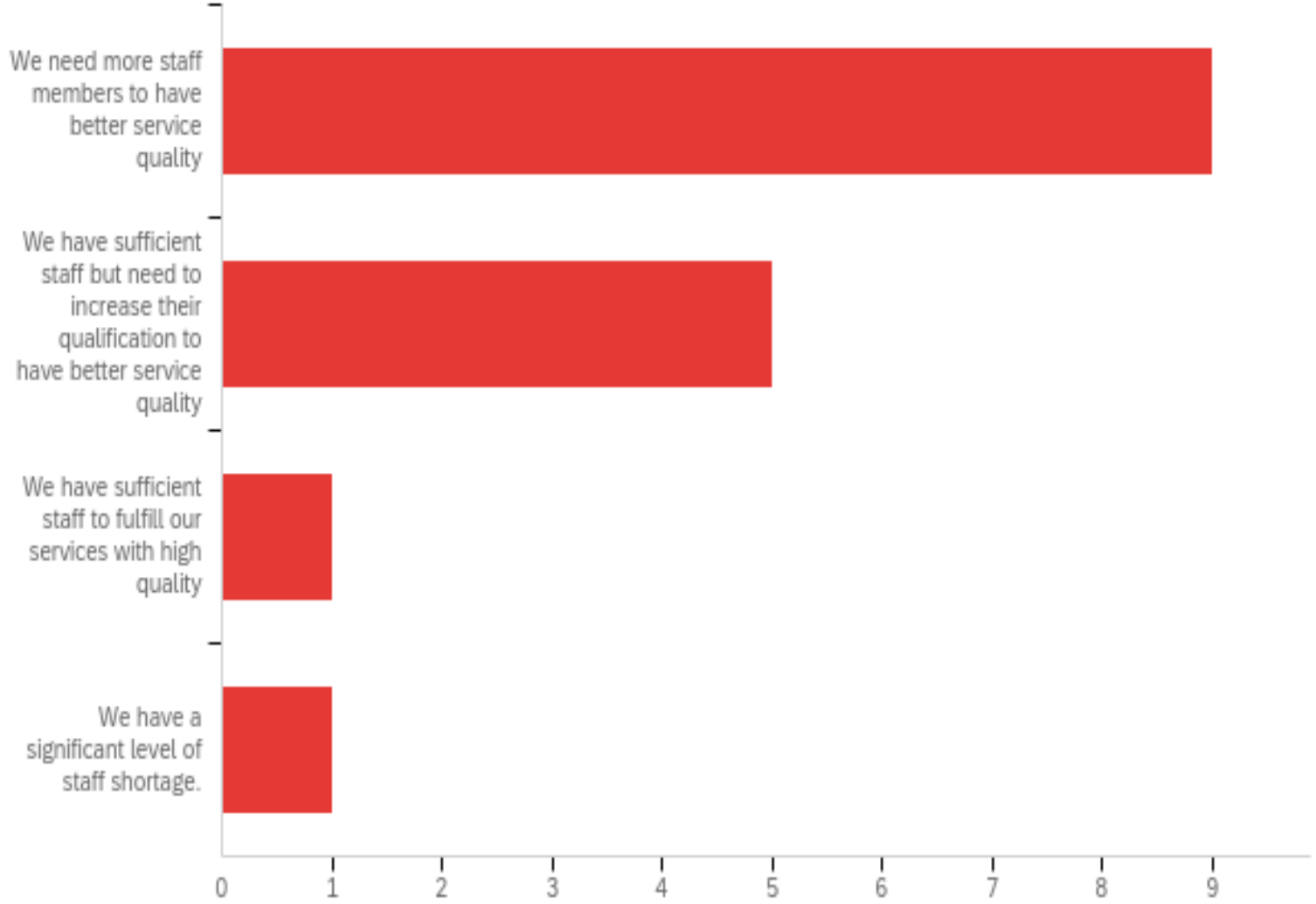
Profile of the Survey Respondents

Country	Region	GDP Per Capita	Human Development Index Ranking	Global Cyber security Index Ranking	Digital Development Level	Which year was your N-CSIRT launched?	Does your nation have a national cyber security strategy?
Mauritius	Africa	$ 22,989	0.804	17	60.83	2008	Yes
Egypt	Africa	$ 11,763	0.707	23	49.58	2009	Yes
Indonesia	Asia Pacific	$ 11,812	0.718	24	50.22	2013	Yes
Tunisia	Africa	$ 10,756	0.740	45	51.96	2004	Yes
Nigeria	Africa	$ 5,136	0.539	47	35.86	2015	Yes
Bangladesh	Asia Pacific	$ 4,754	0.632	53	36.22	2015	Yes
Benin	Africa	$ 3,287	0.545	56	30.41	2017	Yes
Uruguay	Latin America/ Caribbean	$ 21,561	0.817	64	67.94	2017	Yes
Dominican Republic	Latin America/ Caribbean	$ 18,419	0.756	66	48.26	2018	Yes
Zambia	Africa	$ 3,479	0.584	73	35.56	2012	Yes
Cote d'Ivoire	Africa	$ 1,616	0.538	75	39.99	2009	Yes
Sri Lanka	Asia Pacific	$ 13,078	0.782	83	49.55	2006	Yes
Botswana	Africa	$ 17,766	0.735	88	47.95	2020	Yes
Malawi	Africa	$ 1,060	0.483	97	27.99	2018	Yes
Togo	Africa	$ 1,596	0.515	105	N//A	2021	No
Trinidad and Tobago	Latin America/ Caribbean	$ 26,176	0.796	125	59.49	2012	Yes

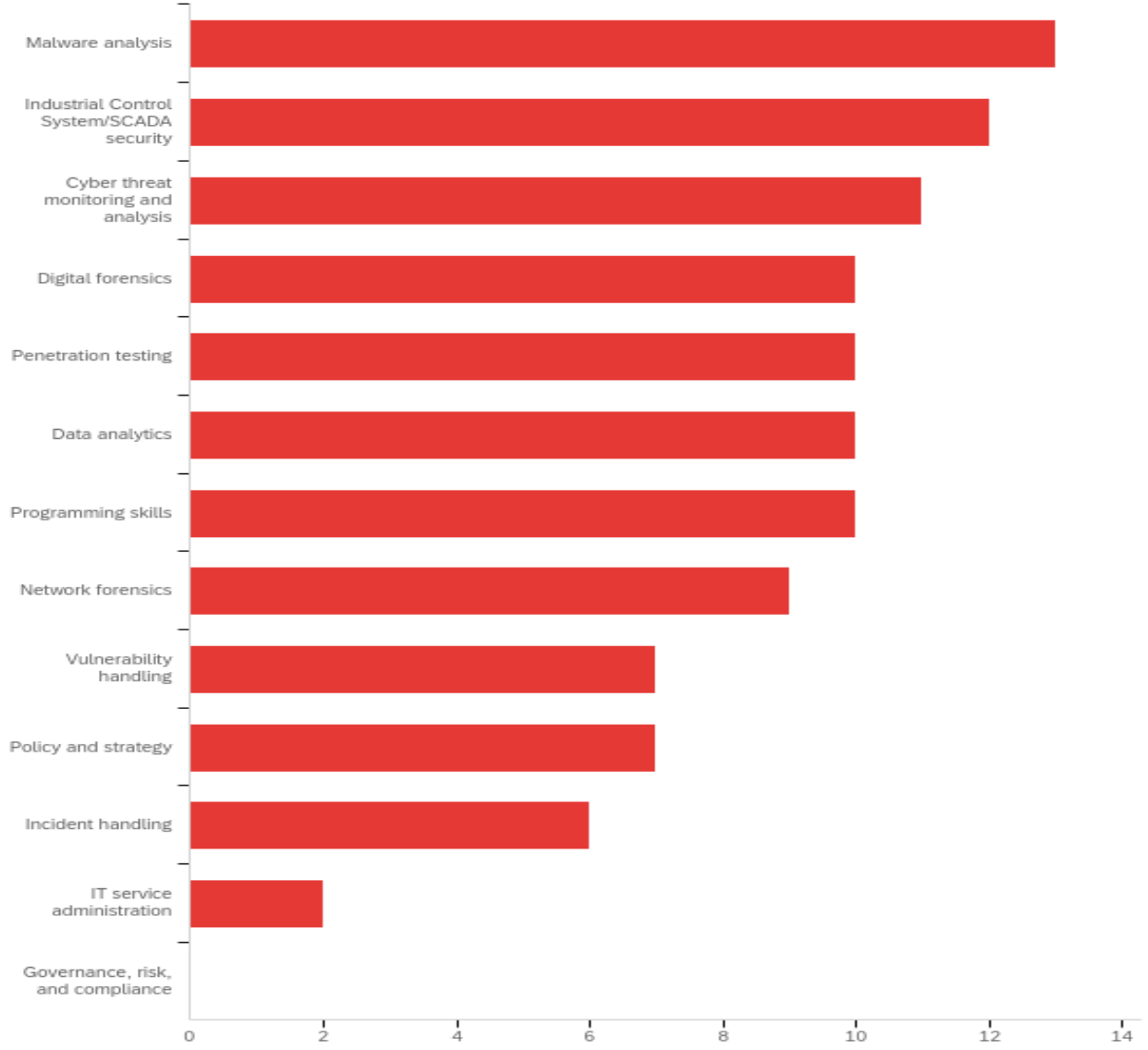
Survey Results: General Challenges for N-CSIRTs



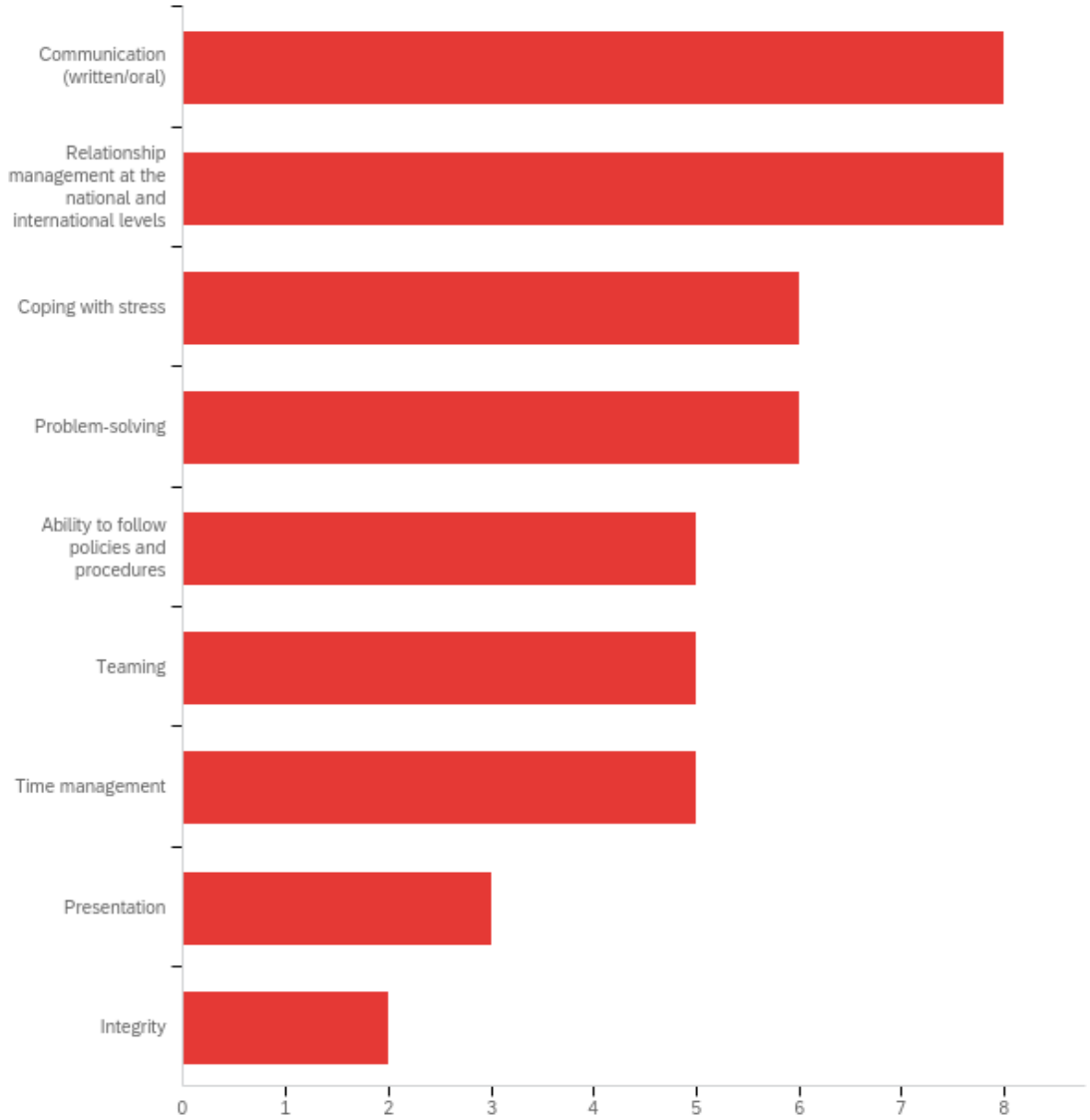
Survey Results: HR Challenges for N-CSIRTs



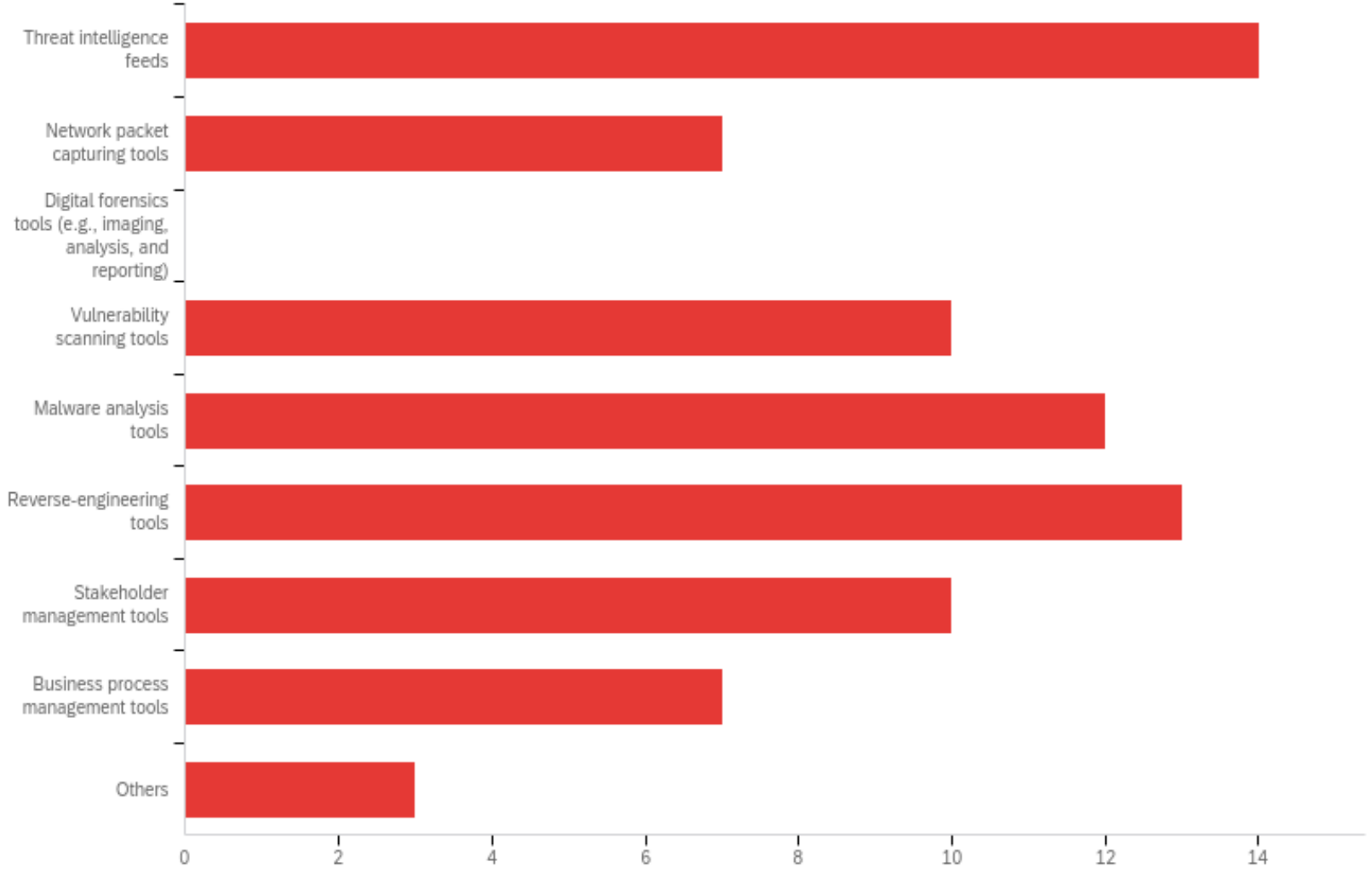
Survey Results: Technical Skills Needed



Survey Results: Soft Skills Needed



Survey Results: Tools Needed



Survey Results: Tool Challenges

Among the 16 N-CSIRTs:

- 13 do not have enough budget to buy high-quality tools.
- 12 use open-source tools in production environments,
  - 4 either prefer not to use or use open-source tools for testing purpose, and
  - 5 prefer open-source rather than commercial tools.

Survey Results: Trainings

- Majority do not utilize platforms like EDX, Coursera, Udemy, Udacity, Lynda, and others.
- A host of training providers exist but for the 16 N-CSIRTs:
  - FIRST, AfricaCERT, and ITU are used several times or frequently
  - Providers like OAS, CREST, LACCIRT are known by or used by a few.
  - There are existing arrangements with organizations like SANS, ISC2, COMPTIA for National level capacity building initiatives.

Interviews

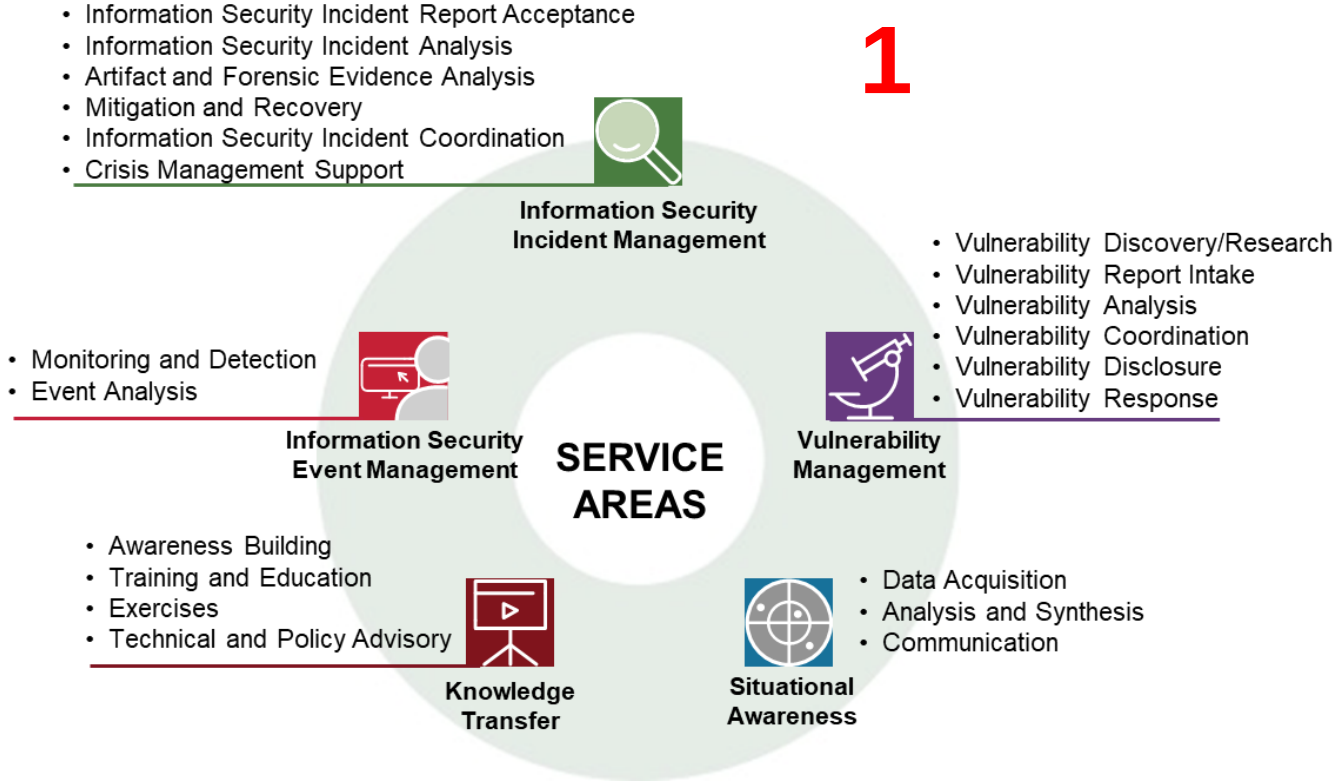
- Interviews with N-CSIRTs
  - To clarify the survey responses and get a deeper view, the following

  N-CSIRTS were interviewed:
    - Ivory Coast CERT
    - TG-CERT
    - EG-CERT
- Interviews with Leading Experts and SMEs
  - To get insights from an external party about challenges and best practices of N-CSIRT capacity development in low-income countries

Affordable tools and trainings for N-CSIRTs

A recommendation per FIRST Services Framework

Mapping Services with Tools & Trainings



1

2

3

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

4

TOOLS + TRAINING

Innovations in N-CSIRT capacity building & Recommendations

Innovations and Recommendations (Selected)

- Creating a pipeline of cybersecurity workforce: cooperation with universities and academic institutions
- Leveraging public-private partnership to operate
- Trust building
- Knowledge transfer from other N-CSIRTs
- Funding and support through regional and international cooperation

Thank you!

Global Affairs Canada
Affaires mondiales Canada

- BGD e-GOV CIRT, Bangladesh
- BJCSIRT, Benin
- BwCIRT, Botswana
- CI-CERT, Cote d'Ivoire
- DR-nCSIRT, Dominican Republic
- EG-CERT, Egypt
- BSSN, Indonesia
- MACRA, Malawi
- CERT-MU, Mauritius
- NITDA-CERRT, Nigeria
- Sri Lanka CERT|CC, Sri Lanka
- CERT.TG, Togo
- TTCSIRT, Trinidad and Tobago
- TunCERT, Tunisia
- CERTuy, Uruguay
- ZMCIRT, Zambia

- Vladmin Aman, CICERT
- Palakiyem Assih, CERT.TG
- Vilius Benetis, NRD Cybersecurity, Lithuania
- Tracy Bills, CERT/CC
- Haythem El Mir, Keystone, Tunisia
- David Hunt, Prelude
- Jacomo Piccolini, Team Cymru
- Mahmoud Raouf, EG-CERT
- Don Stikvoort, Cyber4DEV
- Adli Wahid, APNIC

- Klée Aiken
- Abdul-Hakeem Ajijola
- Richard Harris
- Maarten van Horenbeeck

Questions and Discussion