Cyber Incident Management in Low-Income Countries

PART 2: A GUIDELINE FOR DEVELOPMENT

By Hountomey, J., Bahsi, H., Tatar, U., Hashem, S., Dubois, E.

A Report Created for the Global Forum on Cyber Expertise (GFCE)

GFCE
Global Forum on Cyber Expertise

Global Affairs Canada
Affaires mondiales Canada

AfricaCERT
United Teams promoting Cybersecurity in Africa

Disclaimer

The report is an output of a research project that the Global Forum on Cyber Expertise (GFCE) commissioned as part of its Global Cyber Capacity Building Research Agenda 2021. Global Affairs Canada funded the project. AfricaCERT assembled a team of Researchers: Jean-Robert Hountomey (AfricaCERT), Hayretdin Bahsi (Tallinn University of Technology), Unal Tatar (the State University of New York at Albany), Sherif Hashem (George Mason University), Elisabeth Dubois (the State University of New York at Albany).

The information, interpretation and examples set out in this research do not constitute official or informal opinions or positions of the GFCE, its Secretariat, its members and partners, or any government. Neither the GFCE nor its members may be held responsible for the use which may be made of the information contained therein.

Through the Global Cyber Capacity Building Research Agenda mechanism, the GFCE aims to identify and address knowledge gaps relevant to ongoing GFCE work and members' capacity-building activities. For this research project, the topic was identified in 2020 by the Cyber Incident Management Task Force members under the Working Group on Cyber Incident Management and Critical Infrastructure Protection. More information about the Working Group is on the GFCE website.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGEMENTS

We would like to thank the Global Forum on Cyber Expertise for supporting the research resulted in this report. We would also like to thank:

- The National Computer Security Incident Response Teams for their invaluable inputs in the preparation of this report:
  - 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

- The subject matter experts for providing insights from an outsider perspective about challenges and best practices of N-CSIRT capacity development in low-income countries:
  - 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

- The members of the project oversight group for their feedback to improve this report:
  - Klée Aiken, Principal Pacific Partnership Advisor at CERT NZ and GFCE Research Committee Member
  - Abdul-Hakeem Ajijola, Chair of GFCE Working Group B (Cyber Incident Management and Critical Infrastructure Protection)
  - Richard Harris, Principal Cybersecurity Policy Engineer at MITRE Corporation and GFCE Research Committee Member
  - Maarten van Horenbeeck, GFCE WG B Taskforce on Cyber Incident Management Lead

ABBREVIATIONS

AFRINIC	African Network Information Centre
APCERT	Asia Pacific CERT
APNIC	Asia Pacific Network Information Centre
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ENISA	European Network and Information Security Agency
FIRST	Forum of Incident Response and Security Teams
GFCE	Global Forum on Cyber Expertise
IoC	Indicators of Compromise
ISEM	Information Security Event Management
ISIM	Information Security Incident Management
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KT	Knowledge Transfer
MISP	Malware Information Sharing Platform
N-CSIRT	National CSIRT or CSIRT with national responsibilities
OECD	Organisation for Economic Co-operation and Development
OAS	Organization of American States
OIC-CERT	The Organisation of the Islamic Cooperation Computer Emergency Response Team
PSIRT	Product Security Incident Response Team
SIM3	Security Incident Management Maturity Model
SOC	Security Operations Center
SA	Situational Awareness
SCADA	Supervisory Control and Data Acquisition
TLP	Traffic Light Protocol
VM	Vulnerability Management

EXECUTIVE SUMMARY

Cyber-attacks know no borders. In the digitally connected world, no region or country is secure against cyber-attacks. Preventive or reactive countermeasures require collaboration, coordination, and engagement of various organizations, government bodies, the private sector, academia, and citizens of different countries.

National Computer Security Incident Response Teams (N-CSIRTs) play a pivotal role in national-level cybersecurity governance systems of countries as the main coordinator of cybersecurity incidents and a contact point for national and international bodies. They can assume various other roles such as promoting and supporting cybersecurity awareness and training, resolving incidents, taking part in cyber crisis planning and coordination activities, or providing security announcements. They can act as a medium where national-level discussion about cybersecurity matters occurs [1]. In most countries, they initiate or promote the development of national-level policies and strategies; thus, their roles mostly exceed essential incident coordination and awareness activities. Many countries have established their N-CSIRTs since 1988, when the first Computer Emergency Response Team (CERT), namely CERT Coordination Center or CERT-CC, was established in response to the large-scale outage caused by the Morris worm. Nevertheless, in low-income countries, the effectiveness of such teams requires an implementation framework that addresses unique development needs with lessons learned from existing standards.

This report presents Part 2 of a two-stage project.

Part 1 of the report comprises a thorough desk review of academic and grey literature (e.g., reports of security vendors, independent organizations, government entities, N- CSIRTs). It lists the N-CSIRT services and identifies organizational models, applied incident handling processes, workflows, required human skill sets, maturity assessment methods, and best practices in capacity development. Part 1 identified areas of coverage and gaps in research and practice providing significant insight into the survey development highlighted in this report.

Part 2 discusses the findings and recommendations of the 'Cyber Incident Management in Low-Income Countries' project, funded by the Global Forum on Cyber Expertise (GFCE). The project aims to create a tailorable guide for low-income countries to develop or improve their CSIRT capabilities in an affordable way to respond to the evolving cyber threat environment effectively.

The research team conducted surveys with 16 N-CSIRTs in low-income or developing countries to better understand the technical and organizational aspects of N-CSIRT services and sufficiently grasp the needs of the corresponding countries. In these surveys and follow-up semi-structured interviews with three of these N-CSIRTs, we explored which services those CSIRTs deliver, what type of technical and organizational capabilities they have, their medium and long-term goals, and their best practices in capacity building. The findings of the survey analysis are presented in Section 1 of this report.

Based on the desk research and survey findings, the research team created a service roadmap in Section 2 that informs each service area N-CSIRTs offer. The roadmap includes the knowledge/skills/competencies, policies, guidelines, frameworks, tools, and trainings. The final part of this report, Section 3, discusses the innovative approaches of N-CSIRTs in capacity building and includes the recommendations based on the data collected in the interviews.

SECTION 1: STATE OF N-CSIRTs IN LOW-INCOME AND DEVELOPING COUNTRIES: SURVEY RESULTS

1. INTRODUCTION

This section explores the current situation of the N-CSIRTs of the low-income countries through the knowledge obtained from surveys. The exploration starts with the analysis of their current services and future expansion plans. The issues evolving around the human capital development constitute the focal point of the analysis.

Twenty-eight respondents representing N-CSIRTs in low-income countries participated in the survey. However, only fully completed surveys were included in the analysis for this evaluation, resulting in 18 responses. Given the interest in evaluating various N-CSIRT capabilities and differences, the research team merged 3 of the remaining responses from the Trinidad and Tobago CSIRT, resulting in 16 final answers.

2. PARTICIPANT PROFILES

To begin the analysis, Table 1 summarizes the participant countries and their general profile regarding to various development indices, Among the 16 countries represented, ten (10) are in the African region, three (3) are in the Asia Pacific region, and the remaining three (3) are part of Latin America and the Caribbean. All the participating countries qualify as developing and low-income; five (5) countries meet the requirements for the least developed country, and three (3) meet the criteria for small island developing countries. The Global Cybersecurity Index and National Cybersecurity Index of the countries in the project range from 17-125 and 49-109, respectively. Many of the surveyed CSIRTs started their activities around 2012, with a handful launched over the past few years. All but one of the survey respondents stated that their nation has a national cybersecurity strategy, with only a few stating that their strategy mentions an N-CSIRT.

Table 1. Profile of Respondents

Country	Region	Country Status	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	Small Island Developing State	$ 22,989	0.804	17	60.83	2008	Yes
Egypt	Africa	Developing Country	$ 11,763	0.707	23	49.58	2009	Yes
Indonesia	Asia Pacific	Developing Country	$ 11,812	0.718	24	50.22	2013	Yes
Tunisia	Africa	Developing Country	$ 10,756	0.740	45	51.96	2004	Yes
Nigeria	Africa	Developing Country	$ 5,136	0.539	47	35.86	2015	Yes
Bangladesh	Asia Pacific	Least Developed Country	$ 4,754	0.632	53	36.22	2015	Yes
Benin	Africa	Least Developed Country	$ 3,287	0.545	56	30.41	2017	Yes
Uruguay	Latin America/ Caribbean	Developing Country	$ 21,561	0.817	64	67.94	2017	Yes
Dominican Republic	Latin America/ Caribbean	Small Island Developing State	$ 18,419	0.756	66	48.26	2018	Yes
Zambia	Africa	Least Developed Country	$ 3,479	0.584	73	35.56	2012	Yes
Cote d'Ivoire	Africa	Developing Country	$ 1,616	0.538	75	39.99	2009	Yes
Sri Lanka	Asia Pacific	Developing Country	$ 13,078	0.782	83	49.55	2006	Yes
Botswana	Africa	Developing Country	$ 17,766	0.735	88	47.95	2020	Yes
Malawi	Africa	Least Developed Country	$ 1,060	0.483	97	27.99	2018	Yes
Togo	Africa	Least Developed Country	$ 1,596	0.515	105	N//A	2021	No
Trinidad and Tobago	Latin America/ Caribbean	Small Island Developing State	$ 26,176	0.796	125	59.49	2012	Yes

[1] The country status is based on the DAC List of ODA Recipients, an OECD publication, which shows all countries and territories eligible to receive official development assistance (ODA).

[2] Global Cybersecurity Index 2020, published by ITU, ranks 181 countries and is available at https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

3. MAIN FINDINGS

The survey's main findings are summarized below. Survey respondents stated that they offer all of the N-CSIRT services at varying maturity levels. Only a few mentioned they do not provide some of the services within the categories, such as, information security event management, information security incident management and vulnerability management (Table 2). The distribution of the service offerings is consistent between basic, intermediate, and advanced levels. Many of the services provided in the information security event management are intermediate to nonexistent, while a greater emphasis is placed on situational analysis and knowledge transfer. The respondents plan to expand their scope and/or capacity over the next five years in all the service areas, with some signifying that they plan to offer new services (Table 3). It is important to note that information security event management and situational awareness categories draw an important interest among the new services, indicating that N-CSIRTs have big interests in collecting and managing security-related data.

Table 2. Current CSIRT Service Offerings[3]

#	Question	None		Basic		Intermediate		Advanced		Total
1	Information Security Event Management - Monitoring and Detection	8%	1	31%	4	38%	5	23%	3	13
2	Information Security Event Management - Event Analysis	8%	1	23%	3	46%	6	23%	3	13
3	Information Security Incident Management - Information Security Report Acceptance	0%	0	31%	5	38%	6	31%	5	16
4	Information Security Incident Management - Information Security Incident Analysis	6%	1	19%	3	44%	7	31%	5	16
5	Information Security Incident Management - Artifact and Forensic Evidence Analysis	19%	3	19%	3	50%	8	13%	2	16
6	Information Security Incident Management - Mitigation and Recovery	6%	1	19%	3	56%	9	19%	3	16
7	Information Security Incident Management - Information Security Incident Coordination	0%	0	13%	2	63%	10	25%	4	16
8	Information Security Incident Management - Crisis Management Support	0%	0	44%	7	50%	8	6%	1	16
9	Vulnerability Management - Vulnerability Discovery/ Research	0%	0	33%	5	60%	9	7%	1	15
10	Vulnerability Management - Vulnerability Report Intake	0%	0	47%	7	40%	6	13%	2	15
11	Vulnerability Management - Vulnerability Analysis	7%	1	40%	6	33%	5	20%	3	15
12	Vulnerability Management - Vulnerability Coordination	13%	2	53%	8	7%	1	27%	4	15
13	Vulnerability Management - Vulnerability Disclosure	0%	0	44%	7	44%	7	13%	2	16
14	Vulnerability Management - Vulnerability Response	7%	1	33%	5	47%	7	13%	2	15
15	Situational Awareness - Data Acquisition	0%	0	50%	8	44%	7	6%	1	16
16	Situational Awareness - Analysis and Synthesis	0%	0	38%	6	44%	7	19%	3	16
17	Situational Awareness - Communication	0%	0	44%	7	38%	6	19%	3	16
18	Knowledge Transfer - Awareness Building	0%	0	50%	8	25%	4	25%	4	16
19	Knowledge Transfer - Training and Education	0%	0	38%	6	31%	5	31%	5	16
20	Knowledge Transfer - Exercises	0%	0	56%	9	25%	4	19%	3	16
21	Knowledge Transfer - Technical and Policy Advisory	0%	0	50%	8	31%	5	19%	3	16

[3] Columns next to the Percent of Service Ranking are the number of survey respondents that selected that ranking.

Table 3. Services to Expand or Offer in Next 5 Years

#	Question	New Service		Expand Scope/ Capacity		Total
1	Information Security Event Management - Monitoring and Detection	38%	6	63%	10	16
2	Information Security Event Management - Event Analysis	31%	5	69%	11	16
3	Information Security Incident Management - Information Security Incident Report Acceptance	0%	0	100%	16	16
4	Information Security Incident Management - Information Security Incident Analysis	6%	1	94%	15	16
5	Information Security Incident Management - Artifact and Forensic Evidence Analysis	19%	3	81%	13	16
6	Information Security Incident Management - Mitigation and Recovery	13%	2	88%	14	16
7	Information Security Incident Management - Information Security Incident Coordination	13%	2	88%	14	16
8	Information Security Incident Management - Crisis Management Support	6%	1	94%	15	16
9	Vulnerability Management - Vulnerability Discovery/Research	13%	2	88%	14	16
10	Vulnerability Management - Vulnerability Report Intake	13%	2	88%	14	16
11	Vulnerability Management - Vulnerability Analysis	13%	2	88%	14	16
12	Vulnerability Management - Vulnerability Coordination	6%	1	94%	15	16
13	Vulnerability Management - Vulnerability Disclosure	6%	1	94%	15	16
14	Vulnerability Management - Vulnerability Response	6%	1	94%	15	16
15	Situational Awareness - Data Acquisition	44%	7	56%	9	16
16	Situational Awareness - Analysis and Synthesis	31%	5	69%	11	16
17	Situational Awareness - Communication	19%	3	81%	13	16
18	Knowledge Transfer - Awareness Building	13%	2	88%	14	16
19	Knowledge Transfer - Training and Education	0%	0	100%	16	16
20	Knowledge Transfer - Exercises	19%	3	81%	13	16
21	Knowledge Transfer - Technical and Policy Advisory	19%	3	81%	13	16

According to Figure 1, only one CSIRT indicated that they have sufficient resources to fulfill their responsibilities, with 11 stating that their resource problems affect the quality of service and 4 stating that they have major resource problems that limit their ability to provide services.

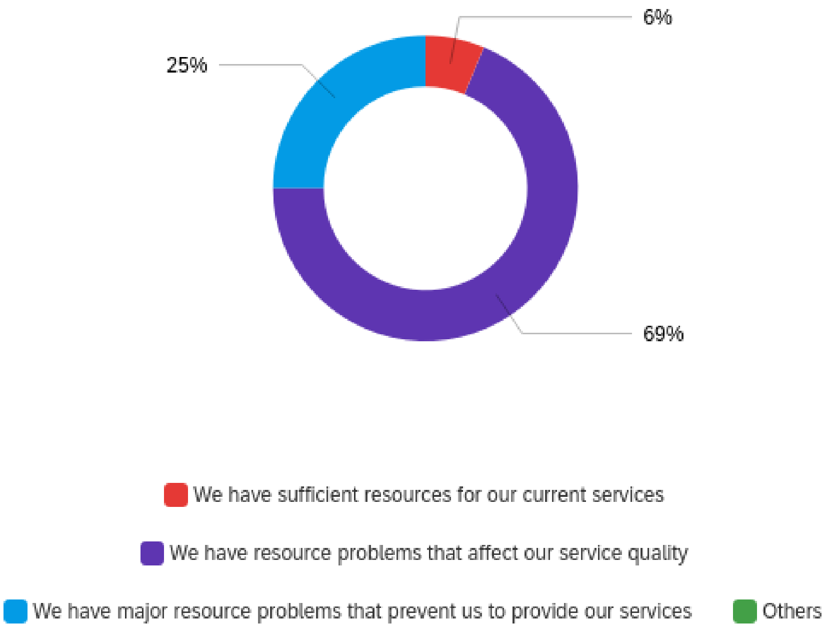

Figure 1. N-CSIRT Resources

Out of the resource allocation problems identified, the report finds that staffing shortages or insufficiently trained staff are among most of the N-CSIRT challenges (Figure 2). A few respondents also indicate that insufficient office space or physical environment is a problem. Along those lines, all but one CSIRT attributes their human resource challenges to poor staff qualification or a staff shortage (Figure 3). The survey also noticed that CSIRTs have difficulty hiring qualified experts because they either do not have sufficient funding or have a limited talent pool due to a shortage of experts in the national job market.

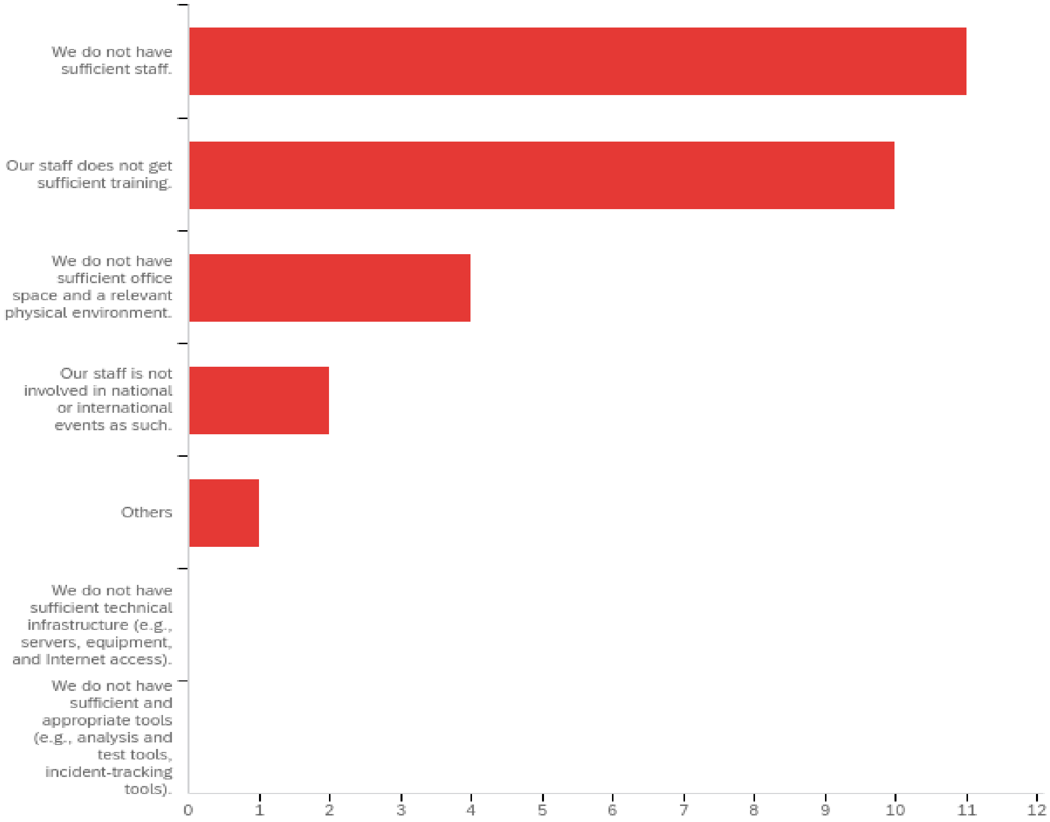

Figure 2. Resource Problems

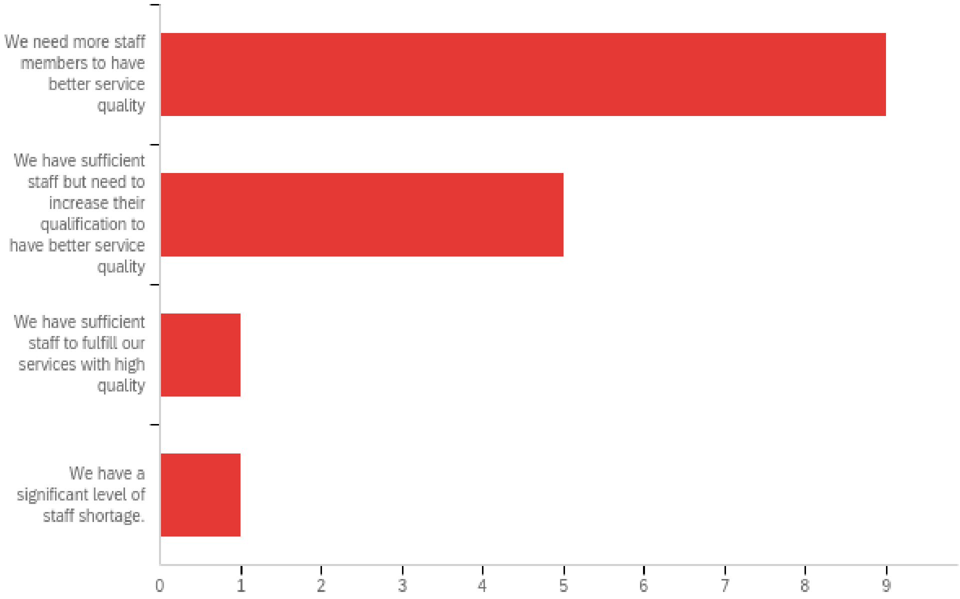

Figure 3. N-CSIRT HR Situation

Concerning skill-building and training, the respondents identified the technical skills needed to improve the functionality of the CSIRT, with malware analysis, industrial control systems/ SCADA, and cyber threat monitoring and analysis leading the pact (Figure 4). The survey results suggested several soft skills to improve CSIRT functionality, including increased staff communication, relationship management at in-house and external levels, ability to cope with stress, and problem-solving (Figure 5).

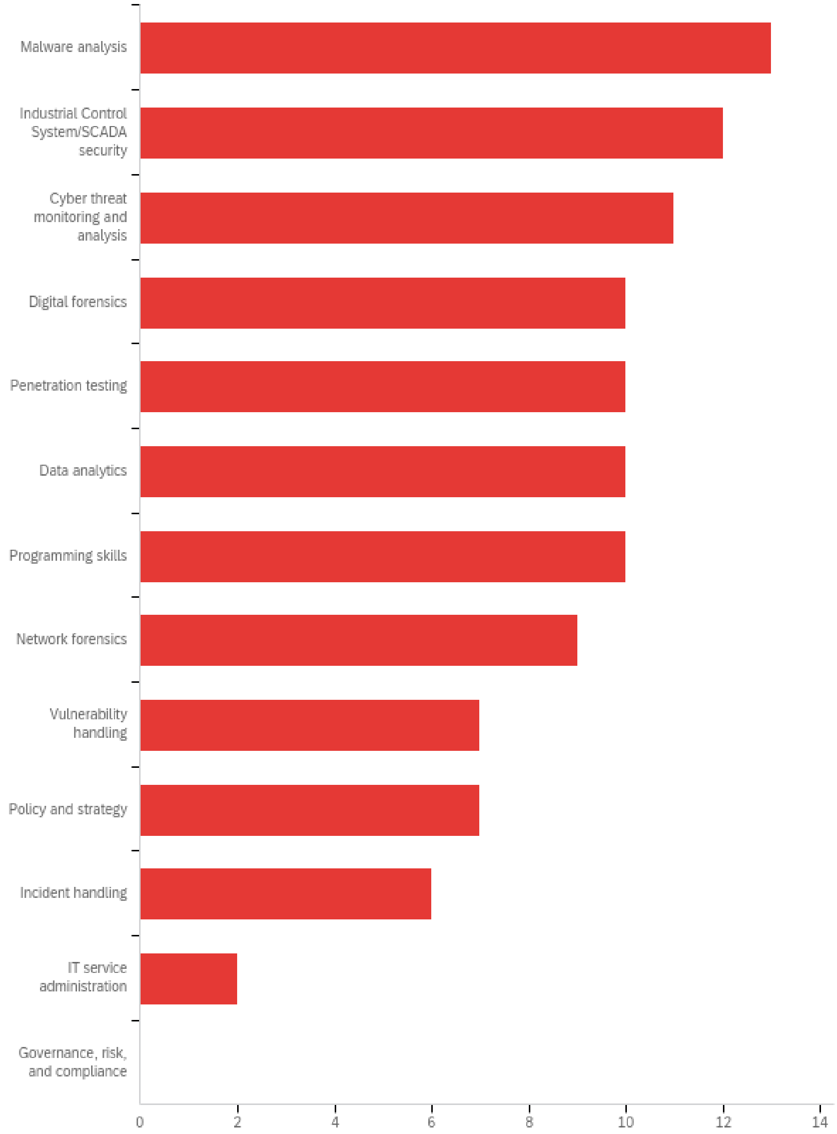

Figure 4. Hard/ Technical Skills Needed

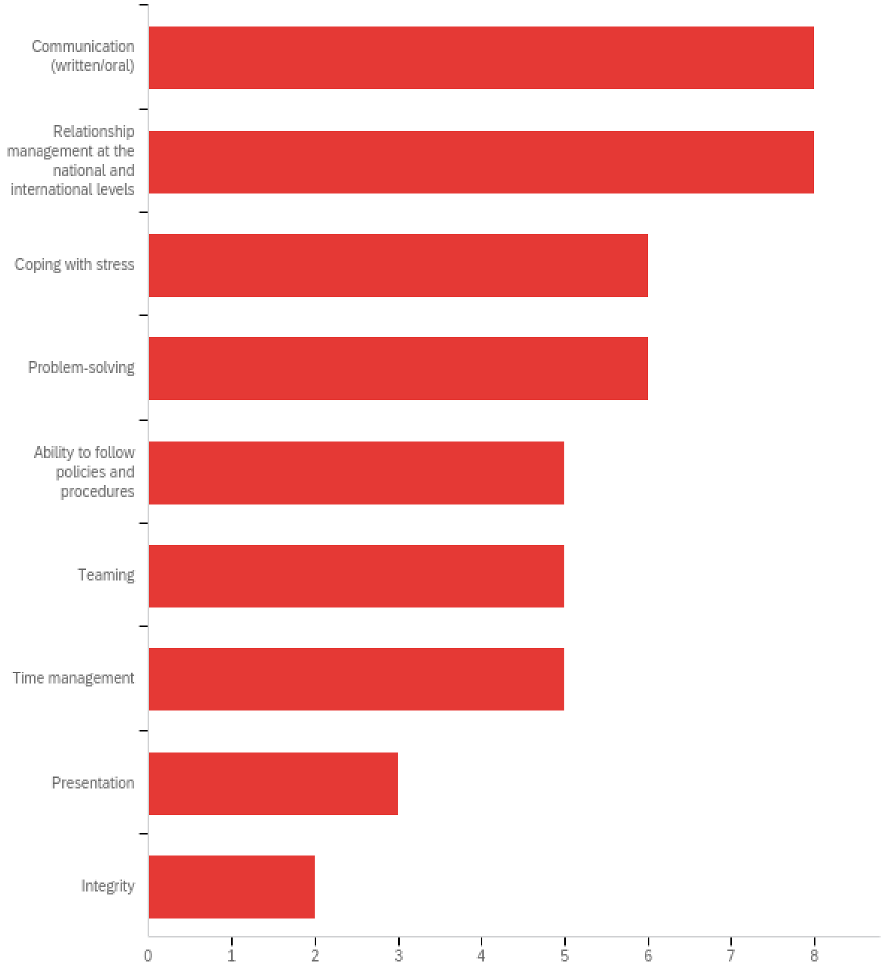

Figure 5. Soft Skills Needed

Although all CSIRTs have an internal training program, eight CSIRTs do not have written external training program guidance. Many of the respondents indicated that their staff needs medium to high levels of technical training. Additional challenges include finding external training alternatives due to limited budgets, lack of competent trainers, and heavy workloads that limit their ability to improve their staff's qualifications (Figure 6).

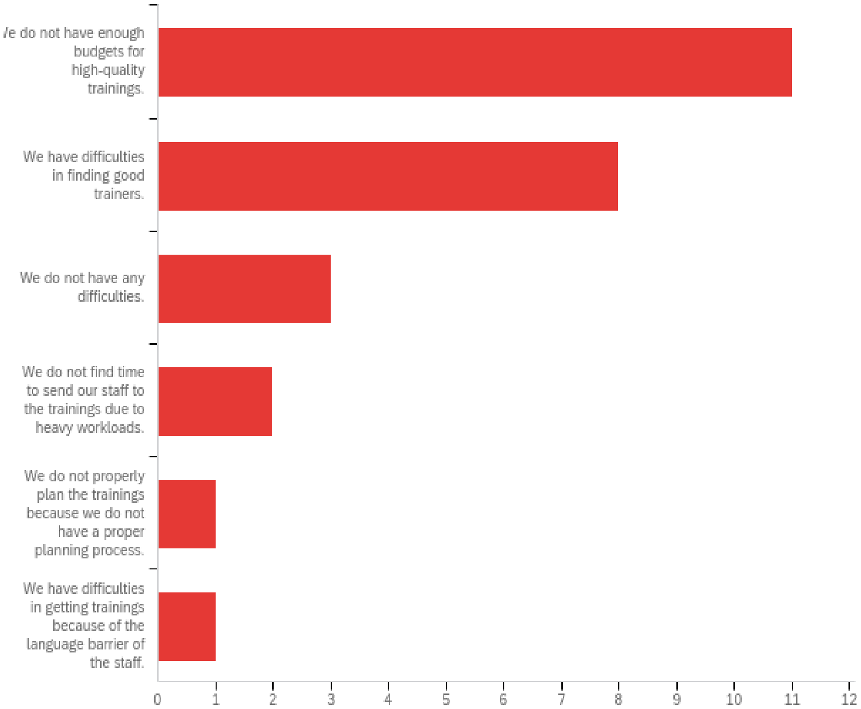

Figure 6. Difficulties in Finding External Training Alternatives

The respondents have never heard of nor used many of the free or affordable training platforms like EDX, Coursera, and Udacity (Table 4).

Table 4. N-CSIRT Experience with Free/ Affordable Training Platforms

Question	Never Heard Of		Heard Of But Not Used		Used At Least Once		Frequently Used		Total
Udemy	13%	2	19%	3	50%	8	19%	3	16
Others	46%	6	23%	3	15%	2	15%	2	13
EDX	31%	5	44%	7	13%	2	13%	2	16
Coursera	13%	2	44%	7	31%	5	13%	2	16
Udacity	38%	6	44%	7	13%	2	6%	1	16
Lynda	44%	7	31%	5	25%	4	0%	0	16

FIRST, APCERT, AfricaCERT, CERT/CC, ENISA, SANS, OIC-CERT, and ITU are the most commonly used training providers. Meanwhile, training providers like OAS and CREST were never heard of or used (Table 5).

Table 5. Experience with Training Providers

Training Provider	Never Heard of		Heard of But Not Used		Used Several Times		Frequently Used		Total
FIRST	0%	0	6%	1	44%	7	50%	8	16
ITU	0%	0	19%	3	31%	5	50%	8	16
AfricaCERT	13%	2	31%	5	19%	3	38%	6	16
Cyber4Dev	19%	3	31%	5	19%	3	31%	5	16
ENISA	0%	0	40%	6	33%	5	27%	4	15
OIC-CERT	7%	1	47%	7	20%	3	27%	4	15
AfriNIC	13%	2	44%	7	19%	3	25%	4	16
SANS	0%	0	27%	4	53%	8	20%	3	15
APCERT	7%	1	47%	7	33%	5	13%	2	15
OAS	40%	6	40%	6	7%	1	13%	2	15
CERT/CC	13%	2	33%	5	40%	6	13%	2	15
APNIC	20%	3	60%	9	7%	1	13%	2	15
RIPE NCC	20%	3	67%	10	0%	0	13%	2	15
Others	67%	8	17%	2	8%	1	8%	1	12
CREST	40%	6	40%	6	13%	2	7%	1	15
TF-CSIRT	20%	3	53%	8	20%	3	7%	1	15
TRANSITS	33%	5	47%	7	13%	2	7%	1	15
LACCSIRT	47%	7	40%	6	13%	2	0%	0	15

The budget for annual skill development varies from less than $5,000 to more than $20,000; 10 CSIRTs have less than a $10,000 budget (Figure 7).

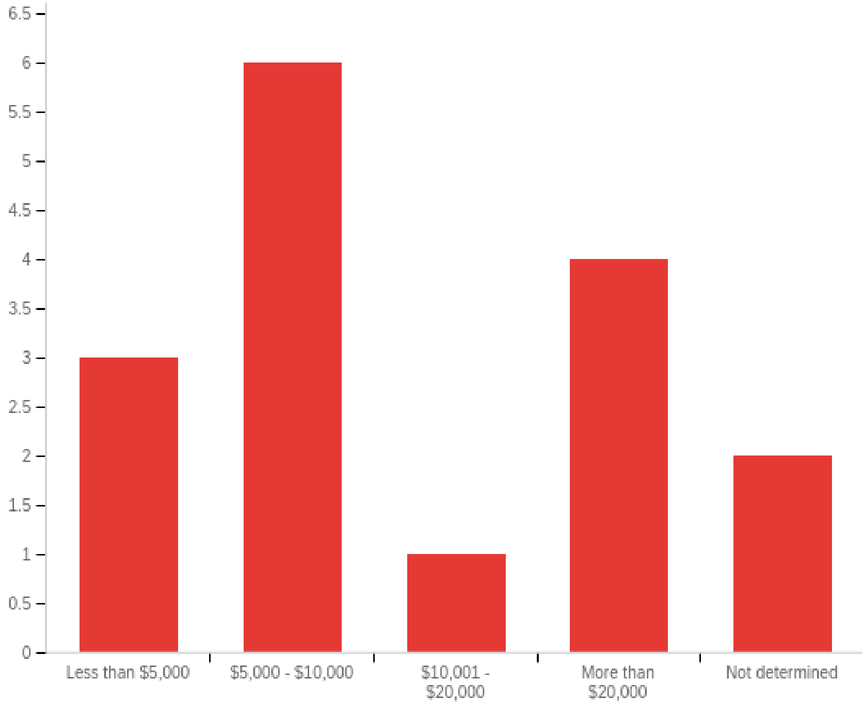

Figure 7. Annual Skill Development Budget

For incident reporting and contact, 4 respondents do not have reliable phone and email, with 2 of the respondents not having reliable Internet.

Figure 8 highlights the areas the respondents suggest enhanced tools are needed. The biggest challenge for tool acquisition is the lack of budget for high-quality tools. The respondent CSIRTs rely on open-source tools. Most of the CSIRTs in this project indicated that their annual budget for purchasing equipment and tools is less than $50,000, with 4 of those CSIRTs having budgets below $10,000.

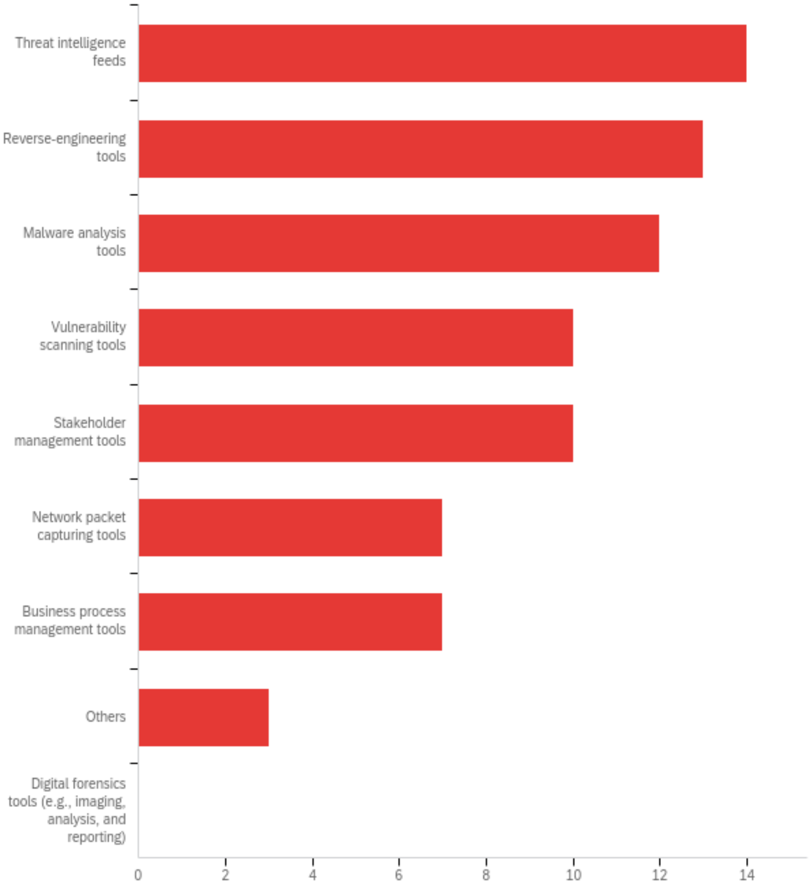

Figure 8. Need for Enhanced Tools and Sources

Table 6 highlights CSIRT's engagement levels with other national entities. Many of the respondents identified that their CSIRT tends to engage more frequently with cyber-crime units, security experts, critical infrastructure owners, operators, and regulators, with room to improve engagement among the judiciary, national crisis management, academic institutions, and the intelligence community.

Table 6. N-CSIRT Engagement Levels with Nationals Entities

National Entity	**None**		**Low**		**Medium**		**High**		**Total**
Cyber-crime units	0%	0	13%	2	44%	7	44%	7	16
Critical infrastructure owners, operators, regulators	0%	0	13%	2	50%	8	38%	6	16
Intelligence community	6%	1	31%	5	38%	6	25%	4	16
Vendors of information technologies and services	13%	2	44%	7	19%	3	25%	4	16
National Crisis Management	13%	2	38%	6	25%	4	25%	4	16
Leading security experts in the country	0%	0	27%	4	53%	8	20%	3	15
Academic institutions	6%	1	38%	6	38%	6	19%	3	16
Judiciary	13%	2	50%	8	19%	3	19%	3	16

4. CONCLUSION

The results of the survey outline the most pressing challenge of most (if not all) CSIRT teams that participated in the survey as a talent management problem affecting their ability to deliver consistent service quality and scale and grow. Needs cover resource allocation, including budget, infrastructure, and talents to support organizational objectives. The ability to identify these talents and nurture them, find, hire, and retain qualified employees, and identify tools and training to grow employees to optimal capacities, keep them, and support their career transitions remain a challenge. The survey highlighted that most of the responding CSIRTs have limited budget allocations for talent management and struggle to find qualified candidates.

The research team selected some N-CSIRT teams and experts to interview for a gap analysis and review of existing good practices. The research team conducted ten in-depth interviews. The team drew from the findings a clearer picture of how low-income countries can best address their challenges, maintain and build their N-CSIRT, protect their respective countries and support their allies.

The interviews revealed that it is vital for CSIRTs to stay focused and avoid turf fights. Some CSIRT started as sectoral CSIRTs then based on successful service delivery to various constituents, those CSIRTs became N-CSIRTs. It is important, especially for an N-CSIRT, to stay focused on its mission, and on enhancing its services and empowering its staff. N-CISRTs must avoid distractions, especially internal and external organizational politics, conflicts, and turf fights. N-CSIRTs should be viewed as "***professional cyber peacekeepers and guardians of safety and security in cyberspace for all.***"

SECTION 2: N-CSIRT SERVICE ROADMAP

1. INTRODUCTION

FIRST CSIRT Services Framework [2] classifies CSIRT services into five areas, Information Security Event Management (ISEM), Information Security Incident Management (ISIM), Vulnerability Management (VM), Situational Awareness (SA), and Knowledge Transfer (KT). Each service area includes several services. The service roadmap presented below outlines each service area that N-CSIRTs can offer. The roadmap suggests resources requirements for each service. It covers knowledge, skills, competencies, policies, guidelines, frameworks, tools, and trainings necessary to manage each service. Although this section does not provide an exhaustive list for each analyzed item, the findings would help N-CSIRTs enhance their services.

The research team looked at the CSIRT services offered by the low-income or developing country N-CSIRTS (see Table-7) and their plans to provide or expand the capacity in the next five years (see Table-8). Information in these tables supports the recommendations in five service areas.

Table 7. Current CSIRT Service Offerings[4]

#	Question	None		Basic		Intermediate		Advanced		Total
1	Information Security Event Management - Monitoring and Detection	8%	1	31%	4	38%	5	23%	3	13
2	Information Security Event Management - Event Analysis	8%	1	23%	3	46%	6	23%	3	13
3	Information Security Incident Management - Information Security	0%	0	31%	5	38%	6	31%	5	16
4	Information Security Incident Management - Information Security Incident Analysis	6%	1	19%	3	44%	7	31%	5	16
5	Information Security Incident Management - Artifact and Forensic Evidence Analysis	19%	3	19%	3	50%	8	13%	2	16
6	Information Security Incident Management - Mitigation and Recovery	6%	1	19%	3	56%	9	19%	3	16
7	Information Security Incident Management - Information Security Incident Coordination	0%	0	13%	2	63%	10	25%	4	16
8	Information Security Incident Management - Crisis Management Support	0%	0	44%	7	50%	8	6%	1	16
9	Vulnerability Management - Vulnerability Discovery/ Research	0%	0	33%	5	60%	9	7%	1	15
10	Vulnerability Management - Vulnerability Report Intake	0%	0	47%	7	40%	6	13%	2	15
11	Vulnerability Management - Vulnerability Analysis	7%	1	40%	6	33%	5	20%	3	15
12	Vulnerability Management - Vulnerability Coordination	13%	2	53%	8	7%	1	27%	4	15
13	Vulnerability Management - Vulnerability Disclosure	0%	0	44%	7	44%	7	13%	2	16
14	Vulnerability Management - Vulnerability Response	7%	1	33%	5	47%	7	13%	2	15
15	Situational Awareness - Data Acquisition	0%	0	50%	8	44%	7	6%	1	16
16	Situational Awareness - Analysis and Synthesis	0%	0	38%	6	44%	7	19%	3	16
17	Situational Awareness - Communication	0%	0	44%	7	38%	6	19%	3	16
18	Knowledge Transfer - Awareness Building	0%	0	50%	8	25%	4	25%	4	16
19	Knowledge Transfer - Training and Education	0%	0	38%	6	31%	5	31%	5	16
20	Knowledge Transfer - Exercises	0%	0	56%	9	25%	4	19%	3	16
21	Knowledge Transfer - Technical and Policy Advisory	0%	0	50%	8	31%	5	19%	3	16

[4] Columns next to the Percent of Service Ranking are the number of survey respondents that selected that ranking.

Table 8. Services to Expand or Offer in Next 5 Years

#	Question	New Service		Expand Scope/ Capacity		Total
1	Information Security Event Management - Monitoring and detection	38%	6	63%	10	16
2	Information Security Event Management - Event Analysis	31%	5	69%	11	16
3	Information Security Incident Management - Information Security Incident Report Acceptance	0%	0	100%	16	16
4	Information Security Incident Management - Information Security Incident Analysis	6%	1	94%	15	16
5	Information Security Incident Management - Artifact and Forensic Evidence Analysis	19%	3	81%	13	16
6	Information Security Incident Management - Mitigation and Recovery	13%	2	88%	14	16
7	Information Security Incident Management - Information Security Incident Coordination	13%	2	88%	14	16
8	Information Security Incident Management - Crisis Management Support	6%	1	94%	15	16
9	Vulnerability Management - Vulnerability Discovery/Research	13%	2	88%	14	16
10	Vulnerability Management - Vulnerability Report Intake	13%	2	88%	14	16
11	Vulnerability Management - Vulnerability Analysis	13%	2	88%	14	16
12	Vulnerability Management - Vulnerability Coordination	6%	1	94%	15	16
13	Vulnerability Management - Vulnerability Disclosure	6%	1	94%	15	16
14	Vulnerability Management - Vulnerability Response	6%	1	94%	15	16
15	Situational Awareness - Data Acquisition	44%	7	56%	9	16
16	Situational Awareness - Analysis and Synthesis	31%	5	69%	11	16
17	Situational Awareness - Communication	19%	3	81%	13	16
18	Knowledge Transfer - Awareness Building	13%	2	88%	14	16
19	Knowledge Transfer - Training and Education	0%	0	100%	16	16
20	Knowledge Transfer - Exercises	19%	3	81%	13	16
21	Knowledge Transfer - Technical and Policy Advisory	19%	3	81%	13	16

2. SERVICE AREA #1 – INFORMATION SECURITY EVENT MANAGEMENT (ISEM)

The service area identifies “information security incidents based on the correlation and analysis of security events from by a wide variety of event and contextual data sources” [2]. The purpose is to identify the relevant sources, establish event flows, analyze the collected event data and forward the resulting output to incident management systems. Such results are helpful to other areas such as situational awareness and knowledge transfer.

ISEM is composed of two services: Monitoring and Detection and Event Analysis. The former aims to establish an event collection framework that extracts data from various system sources such as host-based or network-based intrusion detection sensors, application/OS log agents, network devices and converts them to security events through rules, signatures, statistical techniques, or machine learning models. The later service focuses on grouping and correlating the events, triaging them to eliminate false positives, and relaying the results to the incident management services.

The survey suggests that 13 CSIRT members from low-income countries have varying maturity levels. One of the respondents states that they do not orchestrate any service within the ISEM area. As presented in Table 7, 3 N-CSIRTs declared that their respective services are advanced, whereas the remaining stated they had basic or intermediate maturity. The comparison to other service areas suggests services from ISEM area are usually intermediate to nonexistent. ISIM and KT are more popular.

Nevertheless, plans tell a considerable interest in developing capabilities in this area. Table 8 highlights the services N-CSIRTs plan to expand on or offer in the next five years, emphasizing not only expanding the scope or capacity of this service area but also creating a new service. ISEM and situational awareness categories have the most significant percentage of respondents planning to offer a new service. 6 N-CSIRTs plan to provide Monitoring and Detection, and 5 plan to develop Event Analysis capabilities in the next five years. While a majority, 10 N-CSIRTs for Monitoring and Detection and 11 for Event Analysis planning to expand their current service area offerings and scope.

2.1. Knowledge/ Skills/ Abilities/ Competencies

According to the results obtained from the survey, the primary technical skills that N-CSIRTs aim to improve are in the subject areas of malware analysis, digital forensics, and cyber threat monitoring and analysis (i.e., majority of the respondents listed these skills). Additionally, ten respondents out of 16 identified data analytics. These results, in general, correlate with their expansion plans since monitoring and detection and event analysis require those skills.

Based on the NICE framework, the research team identified the competencies required for ISEM as written in Table 9. Column one of the table highlights the general purpose of the corresponding competency; the second, third, and fourth columns present the competency id, the name of the competency, and its description, respectively.

N-CSIRTs should have the competencies “C013 - Data management”, “C026 - Infrastructure Design,” “C033-Network Management,” and “C034 – Operating Systems” to create and sustain monitor and detection services. The first one has a more general-purpose competence as processing and storage of event data can be achieved by effective data management practices. The remaining competencies are required to identify the suitable host- and network-based sensor locations and properly install monitoring and data collection agents.

Event analysis service mainly relies on “C055 - Threat Analysis” as this competency enables the N-CSIRTs to have the core technical knowledge about the threat actors and their attack techniques which are vital for analyzing collected event data. “C012 – Data Analysis” provides the necessary knowledge and skill to collect, correlate, synthesize and analyze the event data. Although “C021 - Incident Management” should be a core competency in the ISIM service area, ISEM necessitates this competency to some extent for checking the collected event data for false positives and prioritizing the data before forwarding the output to incident management systems. In some cases, a more in-depth analysis of the event data would be necessary (e.g., analysis of volatile memory); thus, “C-05 Computer Forensics” would be included in the competency list.

“C14 - Data Privacy and Protection”, “C017 – Encryption,” “C20-Identity Management” and “C024 - Information Systems/Network Security” are required for the application of relevant data privacy procedures, securing the systems that process and store the event data and restoring them when necessary. These competencies should be accompanied by “C030- Legal, Government, and Jurisprudence” for staff to understand applicable privacy and security regulations.

Supporting competencies listed in Table 9 enable the ISEM team to successfully manage the relevant information systems (i.e., sensors, databases, networks, detection, and analysis software) through wellfunctioning system management procedures. The monitoring function always requires a complete understanding of the system assets via “C01- Asset/Inventory Management” (i.e., this competency may also help provide additional contextual data). “C050 – System Testing and Evaluation” is required to evaluate the performance of systems components. The technology utilized in this service area has a rapidly-changing nature, therefore, the competency, “C053 – Technology Awareness,” is essential.

Table 9. Competencies for ISEM Area

Purpose	Competency ID	Competency	Description
Core Competencies for Monitoring and Detection Service	C013	Data Management	This area contains KSAs that relate to the development and execution of data management plans, programs, practices, processes, architectures, and tools that manage, control, protect, deliver, archive, dispose of, and enhance the value of data and information assets.
	C026	Infrastructure Design	This area contains KSAs related to software, hardware, and networks architecture and typology, including LANs, WANs, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate and with associated controlling software.
	C033	Network Management	This area contains KSAs related to the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.
	C034	Operating Systems	This area contains KSAs related to a computer network, desktop, and mainframe operating systems and their applications.
Core Competencies for Event Analysis Service	C021	Incident Management	This area contains KSAs related to tactics, technologies, principles, and processes to analyze, prioritize, and handle incidents.
	C012	Data Analysis	This area contains KSAs that relate to collecting, synthesizing, and/or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence
	C055	Threat Analysis	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.
	C005	Computer Forensics	This area contains KSAs that relate to the tools and techniques used in data recovery and preservation of electronic evidence.
Competencies for Protection of Event Data	C014	Data Privacy and Protection	This area contains KSAs related to the relationship between the collection, storage, and dissemination of data while protecting individuals’ privacy.
	C022	Information Assurance	This area contains KSAs related to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
	C017	Encryption	This area contains KSAs that relate to transforming information to make it unreadable for unauthorized users.
	C020	Identity Management	This area contains KSAs related to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons."
	C024	Information Systems/Network Security	This area contains KSAs related to the methods, tools, and procedures, including the development of information security plans to prevent information systems vulnerabilities and provide or restore the security of information systems and network services.

Purpose	Competency ID	Competency	Description
	C030	Legal, Government, and Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Supporting competencies	C001	Asset / Inventory Management	This area contains KSAs that relate to the process of developing, operating, maintaining, upgrading, and disposing of assets
	C048	System Administration	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.
	C050	Systems Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
	C053	Technology Awareness	This area contains KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results
	C015	Database Administration	This area contains KSAs that relate to managing and maintaining database management systems (DBMS) software
	C035	Operations Support	This area contains KSAs that relate to the policies and procedures to ensure the production or delivery of products and services, including tools and mechanisms for distributing new or enhanced hardware and software.
	C025	Information Technology Assessment	This area contains KSAs related to the principles, methods, and tools (for example, surveys, system performance measures) to assess the effectiveness and practicality of information technology systems.

2.2. Policies, Frameworks, and Guidelines

N-CSIRT staff should incorporate their in-depth knowledge about cyber attacks into the ISEM services. They can benefit from the MITRE ATT&CK framework, which accumulates and classifies the attackers' techniques and tactics [3]. SANS provides a framework that outlines an event management framework in an organizational setting [4]. NIST has published a guideline about log management [5]. CMU SEI's guidance document about the development of sector-based CSIRTs may be helpful for N-CSIRTs to promote establishing services within the ISEM and similar service areas in various sectors [6].

2.3. Tools

Security information and event management (SIEM) systems provide a technical implementation framework in various tools and services to correlate and analyze the events collected from different sources. These systems play an essential role in eliminating false positives. An event originating from one source may not demonstrate enough proof about an incident, abnormal system behavior, or an intrusion. Another source can check the same event. In some cases, the correlation of seemingly innocent events may indicate a malicious act. Varieties of frameworks exist, both open source and commercial, that are currently utilized by various CSIRTs. Splunk is a widely-used event correlation and analysis tool utilized by SOCs and CSIRTs [7]. The open-source SIEM solutions are AlienVault OSSIM [8], Apache Metron [9], Wazuh [10], and Prelude OSS [11]. Similarly, various vendors offer commercial frameworks such as LogRythm [12], ArcSight [13], SolarWinds [14], AT&T Security [15], Exabeam [16], Rapid7 [17], McAfee [18], IBM Qradar [19], SECURONIX [20], RSA [21], FORTINET [22], and FireEye [23].

Network or host-based intrusion detection sensors and log services of applications/OSs generate the events consumed by SIEMs. Zeek [24], Suricata [25], and Snort [26] are prominent open source network-based intrusion detection systems for the generation and analysis of network-based events. WireShark is used for the analysis of the network packets [27]. NfSen is an open-source tool that helps analyze and visualize the network traffic stored in NetFlow formats [28]. OSSEC is an open-source host-based intrusion detection system that can perform process and file-level analysis, file integrity monitoring, and analysis of OS logs [29]. Elastic Stack [30] is a free log monitoring solution with advanced search and visualization capabilities.

Although in-depth malware analysis and digital forensics studies are generally conducted in the ISIM service area, in some cases, ISEM services can also benefit from these efforts to finalize the decision about the collected event data. The research team also included the tools that may facilitate such deeper analysis in this service area.

Automatic malware analysis systems would be considered as another line of event sources. Cuckoo Sandbox [31] is an open-source malware analysis tool that can be included in the toolbox of N-CSIRTs. VirusTotal gives a free service that checks the submitted file or URL with various malware scanners [32]. The Computer Incident Response Center Luxembourg (CIRCL) offers a similar service [33]. Yara is a tool used for the identification and analysis of malware [34]. More hands-on malware investigations can be conducted by the tools delivered in the Linux distribution, REMNux [35]. Autopsy and Sleuth Kit are the widely known open source digital forensic analysis toolkit mostly used for the analysis of disk images [36]. Volatile memory analysis can be conducted by a free tool, Volatility [37].

The additional data sources such as threat intelligence feed, asset inventory information, configuration management content, or identity and access management systems may enrich the collected even data with various contextual aspects [2]. Although all these sources can be somehow utilized, in most cases, N-CSIRTs can easily benefit from threat intelligence feeds obtained from open-source intelligence (OSINT). Team-Cymru [38] and Shadowserver [39] provide free threat intelligence feed and report services to N-CSIRTs. Malware Information Sharing Platform (MISP) [40] could be utilized for exchanging cyber threat intelligence and incorporating them into the event management systems in the form of indicators (IoC) within national and sectoral CSIRT ecosystems. Intel MQ provides a solution for obtaining and processing threat feeds [41]. OpenCTI is another open-source solution that can share and analyze cyber threat intelligence data [42]. The Polish CERT (CERT Polska) has developed a wide-scale data collection and distribution system for security information [43]. There exist various threat intelligence feeds that are free of charge about defaced websites [44], phishing sites [45], and domains hosting malware [46]. Maltego is a tool that collects and provides analysis of cyber threat feeds [47]. Threat Pursuit Virtual Machine [48] enables to do threat hunting.

Various organizations or sources provide valuable data obtained from security scanning of large segments of the Internet. SHODAN [49] is a search engine that identifies specific computers or devices connected to the Internet. Cyber Green [50] presents scanning results of the whole Internet and mostly identifies potential risks that may lead to various denial of service attacks.

Honeypots deployment help understand the attack techniques and tactics and collect threat intelligence about the possible threat actors. N-CSIRTs can use a honeypot for data collection additionally as usual intrusion detection sensors or other log sources. The data collected from honeypots create less privacy and data ownership concerns as they do not host actual services or data. After the compromise of the system, it is easier to re-install the new ones without operational complications in low interaction honeypots; there are research studies that improve the rebuilding of the high interaction ones, though [51].

Several open-source honeypots and related tools exist with Honeynet Project [52]. Dionaea includes various emulators for network services such as HTTP, FTP, SIP [53]. Cowrie provides a honeypot for ssh service[54]. Honeything emulates IoT devices [55], whereas Conpot is a honeypot that helps collect intelligence about the methods and motives of adversaries targeting industrial control systems [56]. Thug emulates client applications to understand client-side attacks [57]. T-pot provides a management platform for different honeypots and intrusion detection systems [58].

The sources providing data from operational systems (e.g., intrusion detection sensors) require control of the protected systems to some degree or highly dynamic information sharing with the system owners. It may not be feasible (even not preferable) for N-CSIRTs due to various reasons such as the large constituency base, legal frameworks regarding system ownership, or creating a single point of failure by collecting highly-critical system information in one center. N-CSIRTs with a solid legal baseline and sufficient technical capability manage data collection from systems running in government networks [59], which could be relatively easy to achieve with the relevant legal framework when compared to the networks of critical infrastructure companies with private ownership. EINSTEIN [60], a wide-scale intrusion detection system deployed and managed by the US Cybersecurity and Infrastructure Security Agency (CISA) to detect cyber attacks targeting US federal agencies, could be considered a significant example.

The interview with the Egyptian National Computer Emergency Response Team reveals that EG-CERT collects endpoint logs from government networks.

A traffic monitoring system, TSUBAME [61], is operated by APCERT in Asia Pacific region. The system detects suspicious scanning activities by using the sensors located in the APCERT members.

The APNIC Community Honeynet Project, established in 2017, has assisted network engineers and network security personnel throughout the Asia Pacific region with setting up individual honeypots in their networks.

Threat intelligence feeds or honeypot logs would always be useful data sources for N-CSIRTs. These sources can act as a reasonable starting point for launching wide-scale ISEM services.

2.4. Trainings

For Incident Security Event Management, various trainings exist that offer applied lessons at medium or advanced levels. The training providers include tailored training by CSIRT Teams, Udemy, SANS, EC Council, ISACA, IBM, ENISA, ISC2, eLearnSecurity, Cyber4Dev, and global CSIRT collaborations. The list of the trainings is in Table 10. SANS, Udemy, EC-Council, and IBM deliver event management and log analysis curriculum. SANS, FIRST, and CIRCL host training about obtaining and analyzing threat intelligence. Information security incident management courses covering the ISEM area use some triage notions of incident management to eliminate event data that do not reflect a real anomaly. ENISA training about security orchestration is noteworthy due to the high need for tool consolidation in this service area.

Table 10. Trainings for ISEM area

Training/Certification Institution	Training/Certification	Training/Certification Content
SANS	GIAC Certified Incident Handler (GCIH) [62]	Information security incident management
SANS	GIAC Certified Detection Analyst (GCDA)	Event monitoring and log analysis
SANS	FOR578: Cyber Threat Intelligence [63]	Threat Intelligence
SANS	SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis [64]	Threat Intelligence
SANS	SEC541: Cloud Security Monitoring and Threat Detection	Event monitoring and log analysis
SANS	SEC503: Intrusion Detection In-Depth [65]	Event monitoring and log analysis
SANS	SEC555: SIEM with Tactical Analytics [66]	Event monitoring and log analysis
Udemy	SIEM Admin - Incident Handling Training - SOC Team [67]	Event monitoring and log analysis
Udemy	Certified Incident Handling Engineer (CIHE) [68]	Information security incident management
EC-Council	Certified SOC Analyst (CSA) [69]	Event monitoring and log analysis
IBM	Certified SOC Analyst - IBM QRadar SIEM V7.3.2 [70]	Event monitoring and log analysis
AfricaCERT	Shadow Server Training	Incident analysis
ENISA	Orchestration of CSIRT Tools [71]	Security Orchestration
FIRST	Threat intel Pipelines [72]	Threat Intelligence
CIRCL	MISP - Open Source Threat Intelligence Platform [73]	Threat Intelligence
CERT-Tools Community	IntelMQ Tutorials [74]	Event monitoring and log analysis
ICANN	Technical Engagement Training Courses [75]	DNS-related event data analysis

CREST [76] provides syllabus and certification exams in addition to certifications such as Practitioner Threat Intelligence Analyst, Registered Threat Intelligence Analyst, Certified Threat Intelligence Manager.

3. SERVICE AREA #2 – INFORMATION SECURITY INCIDENT MANAGEMENT (ISIM)

ISIM seems the common area where each N-CSIRT somehow gives services with varying levels of maturity and capabilities. This area mainly covers the services that collect incident reports and relevant data, analyze them and apply recovery and mitigation actions. Networking and coordination are the essential functions, so the information security incident coordination service is the common one, even usually the first service established by new developing N-CSIRTS, even though this area has various services. In the later steps of a typical evolvement path, N-CSIRTs enrich their incident report acceptance channels and improve their technical capabilities and human resources in-depth incident analysis. The N-CSIRTs with higher maturity may be actively involved in mitigation efforts depending on the incident criticality and resource availability. Crisis management support services are coordinated with national crisis management agencies and other relevant organizations when a crisis arises. This service relies more on well-developed national governance when compared to other services.

The survey results have confirmed the reflection provided above. 14 N-CSIRTs out of 16 stated that they deliver information security incident coordination service at an intermediate or advanced level, and the remaining ones provide basic level service. Incident analysis is not within the service portfolio of only one N-CSIRTs, and the figure for intermediate/advanced level maturity is slightly less than the incident coordination service (i.e., 12 N-CSIRTs). 3 respondents expressed that they do not have the artifact and forensic evidence analysis service, and only 2 of them have the advanced capability to conduct in-depth analysis. Even though all N-CSIRTs somehow offer crisis management support, the figures for maturity levels are relatively worse than the other ones as seven respondents declared a basic level service, whereas only one of them has reached an advanced level. The plans for the next five years indicate that all N-CSIRTs show an ambition to complement or extend their services in this area. The main trend in all services is to advance the maturity from intermediate to advance, but Artifact and Forensic Evidence analysis and crisis management support services require more attention in the upcoming years. While the former could be established by advancing the technical capability via better training, more advanced tools, and technical experts with higher quality, the latter necessitates a better national governance structure in the respective country and more support of public policy, crisis management, and communication experts.

3.1. Knowledge/ Skills/ Abilities/ Competencies

Majority of survey responders answered to the question: “Which hard/ technical skills do you need to improve in your N-CSIRT?” indicating that malware analysis and digital forensics are their priorities. These results are in parallel with the future service plans, especially regarding the artifact and forensic evidence analysis service. Another interesting result is that eight respondents underlined the need for more technical skills in the area of Industrial Control System/SCADA security. With regards to soft-skills, communication (written/oral) and relationship management at the national and international levels have received the highest interest (6 respondents out of 16). These skills could be considered in relation to increasing the maturity level in crisis management support. Considering the maturity gap and such a relatively lower interest level, N-CSIRTs may pay more attention to identify the required soft skills for this service and focus on how to obtain them.

The competencies for the ISIM area according to the NICE framework are outlined in Table 11. “C005 - Computer Forensics”, “C012 - Data Analysis”, “C021 – Incident Management” constitute the main competencies required for main functions in Information Security Incident Report Acceptance and Information Security Incident Analysis services. The experts should also have competencies, “C055 – Threat Analysis” and “C057 – Vulnerabilities Assessments”, to better characterize and comprehend incidents and related impacts. This service area requires the soft skill, “C011 – Critical Thinking”, which is highly demanded by significant tasks such as incident prioritization and root cause analysis.

“C005 - Computer Forensics” could be considered as the core competency for the Artifact and Forensic Evidence Analysis service. The level of this competency should be more advanced when compared to the Information Security Incident Analysis service since, most of the time, this service may be positioned as a higher-triage level. In case of a need for preserving chain-of-custody, competencies, “C008 – Computers and Electronic" and "C030 - Legal, Government, and Jurisprudence" should exist in the corresponding team, the former one provides the baseline knowledge about applying technical countermeasures for protecting the integrity of evidence whereas the later one supplements the required legal and procedural knowledge. "C011 – Critical Thinking" and "C060 – Written Communication" are the necessary soft skills for generating forensically and technically sound reports which could be shared not only within N-CSIRT but constituency, courts, or international ecosystem.

In addition to the competency, "C021 – Incident Management", Information Security Incident Coordination service still needs various competencies related to soft skills as this service relies on the advanced level of communication in many areas such as communication with a diverse set of entities, including the media. In most cases, incident management activities may necessitate the support of "C012 Data Analysis". "C003 Client Relationship Management" and "C029 Knowledge Management" could be considered as a competency that may enhance the communication with the constituency. The incidents involving many entities may induce various conflicts that can be handled by the competency, "C009 Conflict Management".

The corresponding team of N-CSIRT should have well-developed competencies about the administration of varying systems and networks when offering the mitigation and recovery service. The relevant competencies could be identified as "C-024 Information Systems/Network Security", "C033 - Network Management", "C034 Operating Systems", and more general competency, "C047 - System Administration". After the application of mitigation and recovery actions, the experts should be sure that the systems are up and running as expected, requiring the development of the capabilities in the competency area of "C050 - Systems Testing and Evaluation". The evaluation of mitigation options necessitates dealing with various trade-offs affecting many stakeholders; thus, "C009 - conflict management" should be among the competency portfolio of the relevant teams of N-CSIRTs.

The crisis management efforts entail the active participation of various entities/agencies and establishment of effective communication channels, which can be achieved with many soft skills, "C003 - Client Relationship Management", "C009 - Conflict Management", "C060 - Written Communication", "C036 - Oral Communication". Inter-agency cooperation at the national and international level should be supported by the competency, "C030 Legal, Government, and Jurisprudence".

This service area should be supported by incident management and data storage systems. In order to maintain their operations and security, we identified competency categories, "Competencies for Protection of Incident Data and Analysis Results" and "Supporting Competencies," as shown in Table 11.

3.2. Policies, Frameworks, and Guidelines

CSIRT Services Framework [2] released by FIRST provides a comprehensive guideline about all service areas not limited to ISIM. We considered this framework as the main outline of our study. Detailed guidance about the CSIRT services is also given by Carnegie Mellon University Software Engineering Institute (CMU-SEI) [77]. CSIRT policies and services are detailed in RFC-2350 [78]. In the RFC document, Appendix E offers a template frequently utilized by the N-CSIRTs to publish their services on their websites (e.g., CERT-EE [79]). The technological, process, and business aspects of CSIRT establishment have been addressed by ENISA [80]. The ethical responsibilities of CSIRT teams have been outlined by FIRST [81].

Security Incident Management Maturity Model (SIM3) [82] is a widely-used framework for the assessment of CSIRT services, including the N-CSIRT services. Based on SIM3, ENISA published an evaluation methodology that determines three phases, basic, intermediate, and advanced, for the evolvement of CSIRTs [83]. CMU-SEI has released a guideline that proposes indicators for the assessment of incident management activities [84].

Table 11. Competencies for ISIM Area

Purpose	Competency ID	Competency	Description
Core Competencies for Information Security Incident Report Acceptance and Information security incident analysis	C005	Computer Forensics	This area contains KSAs that relate to the tools and techniques used in data recovery and preservation of electronic evidence.
	C011	Critical Thinking	This area contains KSAs that relate to the objective analysis of facts to form a judgment
	C012	Data Analysis	This area contains KSAs that relate to collecting, synthesizing, and/or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence
	C021	Incident Management	This area contains KSAs that relate to the tactics, technologies, principles, and processes to analyze, prioritize, and handle incidents.
	C055	Threat Analysis	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.
	C057	Vulnerabilities Assessment	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.
Core Competencies for Artifact and Forensic Evidence Analysis	C005	Computer Forensics	This area contains KSAs that relate to the tools and techniques used in data recovery and preservation of electronic evidence.
	C008	Computers and Electronics	This area contains KSAs that relate to electronic data management or analysis devices, associated peripherals, accessories
	C011	Critical Thinking	This area contains KSAs that relate to the objective analysis of facts to form a judgment
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.
	C030	Legal, Government, & Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Core Competencies for Information Security Incident Coordination	C021	Incident Management	This area contains KSAs that relate to the tactics, technologies, principles, and processes to analyze, prioritize, and handle incidents.
	C003	Client Relationship Management	This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative).
	C029	Knowledge Management	This area contains KSAs that relate to the value of collected information and the methods of sharing that information throughout an organization.

Purpose	**Competency ID**	**Competency**	**Description**
	C009	Conflict Management	This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming.
	C012	Data Analysis	This area contains KSAs that relate to collecting, synthesizing, and/or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence
Core competencies for Mitigation and Recovery	C009	Conflict Management	This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming.
	C024	Information Systems / Network Security	This area contains KSAs that relate to the methods, tools, and procedures, including the development of information security plans to prevent information systems vulnerabilities and to provide or restore the security of information systems and network services.
	C033	Network Management	This area contains KSAs that relate to the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.
	C034	Operating Systems	This area contains KSAs that relate to a computer network, desktop, and mainframe operating systems and their applications.
	C048	System Administration	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.
	C050	Systems Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
	C011	Critical Thinking	This area contains KSAs that relate to the objective analysis of facts to form a judgment
Core Competencies for Crisis Management Support	C003	Client Relationship Management	This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative).
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
	C029	Knowledge Management	This area contains KSAs that relate to the value of collected information and the methods of sharing that information throughout an organization.

Purpose	Competency ID	Competency	Description
	C009	Conflict Management	This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming.
	C030	Legal, Government, & Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Competencies for Protection of Incident data and analysis results	C014	Data Privacy and Protection	This area contains KSAs that relate to the relationship between the collection, storage, and dissemination of data while simultaneously protecting individuals' privacy.
	C017	Encryption	This area contains KSAs that relate to the process of transforming information to make it unreadable for unauthorized users.
	C022	Information Assurance	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
	C020	Identity Management	This area contains KSAs that relate to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons."
	C024	Information Systems / Network Security	This area contains KSAs that relate to the methods, tools, and procedures, including the development of information security plans to prevent information systems vulnerabilities and to provide or restore the security of information systems and network services.
	C030	Legal, Government, & Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Supporting competencies	C001	Asset / Inventory Management	This area contains KSAs that relate to the process of developing, operating, maintaining, upgrading, and disposing of assets
	C048	System Administration	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.
	C050	Systems Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
	C015	Database Administration	This area contains KSAs that relate to managing and maintaining database management systems (DBMS) software
	C035	Operations Support	This area contains KSAs that relate to the policies and procedures to ensure the production or delivery of products and services, including tools and mechanisms for distributing new or enhanced hardware and software.

Recently, FIRST extended the usual CSIRT services with a new category, Product Security Incident Response Team (PSIRT), and published a service framework document [85]. This category addresses product development companies by framing the security teams that conduct vulnerability management throughout the secure development life cycles. N-CSIRTs use these documents to PSIRTs and related practices in the national framework. N-CSIRT can also initiate efforts for developing sectoral CSIRTS, to foster cybersecurity capabilities using the framework document published by CMU-SEI that outlines how such sectoral capability can be established [6].

ISO has a standard entitled ”ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management” for guiding the establishment and maintenance of incident handling processes in large and medium-sized organizations [86]. Although this standard does not directly correlate with maturity models (e.g., SIM3), it can provide significant guidance to reach higher maturity levels. Another guide about incident handling has been published by NIST [87].

Incident classification taxonomies play an important role in handling and sharing incident information with other entities. Although various CSIRTs may use their taxonomies for internal use and some research studies have proposed taxonomies for specific systems (e.g., smart grids [88]), it is apparent that Europol, ENISA, and TF-CSIRT recommend taxonomies adopted from eCSIRT.net mkVI taxonomy3 [89]–[91]. FIRST has adopted Traffic Light Protocol (TLP) to classify sensitive information exchanged among the security communities [92].

3.3. Tools

N-CSIRTs require management tools to store and track the incidents. Request Tracker for Incident Response (RTIR) is one of the tools that can be utilized for this purpose [93]. The Hive [94] and Cortex [95] are open source incident response platforms in which many CSIRT analysts can collaborate and share information. This service area can also benefit from the general-purpose ticketing systems [96].

OASIS published STIX and TAXII, which are widely-used standard formats for sharing cyber threat intelligence [97]. OASIS has recently published a standard format for creating and sharing the cybersecurity playbooks which can be utilized in various incident handling operations with appropriate tools [98]. ENISA and other European CSIRTS have developed the tool, IntelMQ, which enables the collection of threat intelligence feeds and incorporate them into incident handling processes [41]. Malware Information Sharing Platform (MISP) [40] could be used for exchanging operational cyber threat intelligence in the form of indicators of compromise (IoC) within national and sectoral CSIRT ecosystems.

Team Cymru shares cyber threat intelligence with national and regional CSIRTs after signing a memorandum of understanding within the CSIRT Assistance Program [38]. Another threat intelligence company, Shadowserver, delivers free daily remediation reports to the N-CSIRTs [39].

Autopsy and The Sleuth Kit are the widely known open source digital forensic analysis toolkit mostly used for the analysis of disk images [36]. Volatile memory analysis can be conducted by a free tool, Volatility [37]. WireShark is used for the analysis of the network packets [27]. Nfsen is an open-source tool that helps analyze and visualize the network traffic stored in NetFlow formats [28].

Automated analysis of malware can be performed by Cuckoo Sandbox [31]. REMnux consists of analysis tools that can be used for conducting malware investigations [35]. VirusTotal gives a free service that checks the submitted file or URL with various malware scanners [32]. IDA is a widely known binary code analysis tool that is used for reverse-engineering tasks (i.e., a free version is available) [99]. Security orchestration can be done with open-source tools such as Kubernetes [100] and Helm [101].

3.4. Trainings

The research team summarized certifications and training for the ISIM area from their findings in Table 12. As this service area covers many major subject fields such as incident handling, digital forensics, and malware analysis, it has not been possible to create an exhaustive list for each field. Although we included some training for each subject, the list for certifications is limited to only incident handling subjects. We added the certification, "Certified Information Security Manager," which is a more general-purpose one suitable for managerial security positions, contemplating that N-CSIRT team managers would benefit from that certification. It is important to note that N-CSIRT staff can find various certifications about digital forensics and malware analysis subjects in the cybersecurity ecosystem. They could also add more detailed training to their portfolio, especially about different digital forensics topics such as mobile devices, courses addressing specific OSs (e.g., windows forensics), cloud forensics, network forensics, or reverse engineering. In the list given in Table 12, we also included a course, LEG523: Law of Data Security and Investigations from SANS, which covers the legal and regulatory aspects. This could be considered as a reminder that N-CSIRTs may also need such skills as some incidents may turn into legal cases that require high cooperation with law enforcement agencies. On the other side, the laws and regulations have variations in each country, meaning that teams may also need training more customized to local requirements.

We identified that SANS, CMU-SEI, EC-COUNCIL, and Mile2 provide certifications in the field of information security incident management. These institutions offer training that may be taken individually or as a stepping stone towards a certification. CMU-SEI also offers dedicated training addressing much more process and organizational aspects for CSIRT team managers. We identified some incident handling online courses from Udemy; such courses could be found in similar online course platforms, though. We included the various technical training of SANS regarding incident handling and response, threat intelligence, and malware analysis. Although the cost of SANS training may not be easily affordable for some of the N-CSIRTs, nevertheless, the content of the courses addresses the need in the respective technical field.

Table 12. Trainings for ISIM area

Type	Institution	Title	Training/Certification Content	Level
Certifications	SANS	GIAC Certified Incident Handler (GCIH) [62]	Information security incident management	Intermediate/ Advanced
	CMU - SEI	CERT Incident Response Process Professional Certificate [102]	Information security incident management	Intermediate/ Advanced
	Infosec	Certified Computer Security Incident Handler (CSIH) [103]	Information security incident management	Intermediate
	Udemy – Mile2	Certified Incident Handling Engineer (CIHE) [68]	Information security incident management	Intermediate/ Advanced
	EC-COUNCIL	Certified Incident Handler [104]	Information security incident management	Intermediate/ Advanced
	ISACA	Certified Information Security Manager (CISM)	Management of CSIRT teams	Intermediate/ Advanced

Type	Institution	Title	Training/Certification Content	Level
Trainings	Udemy	SIEM Admin - Incident Handling Training - SOC Team [67]	Event monitoring and log analysis	Basic/ Intermediate
	Udemy	Cybersecurity Incident Handling and Response [105]	Information security incident management	Basic/ Intermediate
	CMU - SEI	Foundations of Incident Management [106]	Information security incident management	Basic
	CMU - SEI	Advanced Topics in Incident Handling [107]	Information security incident management	Intermediate/ Advanced
	CMU - SEI	Creating a Computer Security Incident Response Team [108]	Management of CSIRT teams	Basic
	CMU - SEI	Managing Computer Security Incident Response Teams [109]	Management of CSIRT teams	Intermediate/ Advanced
	SANS	FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics [110]	Information security incident management, threat intelligence analysis, and digital forensics	Advanced
	SANS	FOR578: Cyber Threat Intelligence [63]	Threat intelligence analysis	Intermediate/ Advanced
	SANS	LEG523: Law of Data Security and Investigations [111]	Law and Regulatory Aspects	Basic/ Intermediate
	SANS	FOR610A: Introduction to Malware Analysis: Hands-on and Technical [112]	Malware Analysis	Basic
	SANS	FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques [113]	Malware Analysis	Intermediate/ Advanced
	FIRST	Incident Response for Policymakers [114]	Management of CSIRT teams	Basic/ Intermediate

4. SERVICE AREA #3 – VULNERABILITY MANAGEMENT (VM)

The vulnerability management service area consists of services that establish a continuous process to identify, analyze, disseminate and remediate the vulnerabilities in the information systems. Although in an organizational context, successful operation in almost all service areas cannot be achieved without a significant level of coordination and technical capability, this service area necessitates more interaction between the CSIRT and system operation teams. The vulnerability remediation actions should be coordinated as unsuccessful actions may cause longer service unavailability. On the other side, due to the wider constituency base, N-CSIRTs usually focus on coordination efforts among various entities, affected parties, vendors, security researchers, etc.; more advanced N-CSIRTs may take active roles in a detailed analysis of vulnerabilities or even identify new ones though. Actual vulnerability remediation actions are generally left to the system owners, but N-CSIRTs can provide detailed technical guidance.

Following the public sources for the newly discovered vulnerabilities and informing the constituency about these vulnerabilities would be a starting point for the N-CSIRTs having less maturity and limited resources. N-CSIRTs can extend their communication channels for accepting vulnerability claims or reports. It is important to explore which operating systems, applications, or devices are widely used among the constituency as this information helps prioritize the dissemination actions. The development of communication with vulnerability researchers in the global and local cybersecurity communities would be essential. More advanced N-CSIRTs form a technical team that can deeply analyze the reported vulnerabilities. If the findings obtained in ISIM and ISEM service areas indicate a vulnerability, this team should take responsibility to conduct further analysis. Based on the available resources, N-CSIRTs may also actively contribute to vulnerability research. A noteworthy finding from our interviews in this respect is that EG-CERT conducts a source code review of critical e-governance systems to identify the potential vulnerabilities.

All the VM services except vulnerability coordination have been declared as intermediate or advanced in our survey. The maturity is low in vulnerability coordination as five respondents have the service at the intermediate/advanced levels. When compared to ISIM and ISEM areas, the maturity level of VM is similar to ISEM and relatively lower than ISIM. The services related to VM and ISEM areas require more advanced technical capabilities, which may explain the reason for this gap. All N-CSIRTs stated that they aim to create new VM services or enhance existing ones.

4.1. Knowledge/ Skills/ Abilities/ Competencies

Seven of the N-CSIRTs indicated vulnerability handling, and ten of them stated “penetration testing” in response to the question, “Which hard/ technical skills do you need to improve in your N-CSIRT?” in our questionnaire (out of 16 respondents). After completing the survey, we realized that we had not included more vulnerability-oriented skills in the list, such as vulnerability analysis or exploitation. The item, penetration testing, would demonstrate the interest of N-CSIRTs in identifying the vulnerabilities (i.e., vulnerability detection is a part of vulnerability response service), but, still, there is a considerable distinction between the skills for penetration testing and vulnerability analysis/exploitation, which could have been reflected better in our questionnaire.

The services, vulnerability discovery/research, vulnerability report intake, and vulnerability analysis necessitate baseline technical capabilities such as “C006 – Computer Languages” and “C034 – Operating Systems” to comprehend the details of relevant exploitation facts and codes. The analysis of vulnerabilities related to web applications and other related technology is based on acquiring the competency, “C058 Web Technology”. “C057 – Vulnerabilities Assessment” can be considered as the core competency for the application of methods and tools for the identification and analysis of vulnerabilities. “C055 Threat Analysis” should also be included in this service area as the prioritization of the vulnerabilities could be achieved by a well-developed threat understanding. The competency, “C046 – Software Testing and Evaluation”, would be so useful, especially at the stage of confirming and prioritizing the vulnerability findings. The soft skill, “C011 – Critical Thinking,” is highly necessary for achieving technically sound results.

The services, “Vulnerability Coordination” and “Vulnerability Disclosure,” mostly rely on soft skills such as “C003 - Client Relationship Management” and “C009 - Conflict Management” due to the need for establishing an effective communication medium between different entities having varying roles. The information exchanged in this service area is mostly in written format; thus, “C060 - Written Communication” is an essential competency that should be perfectly synthesized with technical abilities. “C036 – Oral communication” can always facilitate the discussions.

The disclosure and dissemination of vulnerabilities may induce various legal issues, necessitating the competency, “C030 Legal, Government, and Jurisprudence.” “C029 Knowledge Management” facilitates establishing better information sharing channels.

Vulnerability response service can be successfully offered with advanced level knowledge and skills in networks, OSs, security controls as the proposed countermeasures to the vulnerabilities should not disturb the operations of information systems. The identification of the best mitigation option among the alternatives would be achieved by solving the conflicts that may arise among the involved entities. Therefore, we included various competencies which are listed within the group named “Core competencies for Vulnerability Response” in Table 13.

N-CSIRTs require to have information systems to store, process, and transmit highly sensitive vulnerability-related information in this service area; thus, the maintenance of the systems should be done perfectly, and their security should be guaranteed. Therefore, similar to ISIM and ISEM areas, this service area should be supported by competency categories, “Competencies for Protection of Incident Data and Analysis Results” and “Supporting Competencies,” as shown in Table 13.

Table 13. Competencies for VM Area

Purpose	Competency ID	Competency	Description
Core Competencies for Vulnerability Discovery / Research, Vulnerability Report Intake, and Vulnerability Analysis	C057	Vulnerabilities Assessment	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.
	C055	Threat Analysis	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.
	C006	Computer Languages	This area contains KSAs that relate to computer languages and their applications to enable a system to perform specific functions.
	C034	Operating Systems	This area contains KSAs that relate to a computer network, desktop, and mainframe operating systems and their applications.
	C058	Web Technology	This area contains KSAs that relate to the principles and methods of web technologies, tools, and delivery systems, including web security, privacy policy practices, and user interface issues as they apply to development.
	C046	Software Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering software test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
	C011	Critical Thinking	This area contains KSAs that relate to the objective analysis of facts to form a judgment

Purpose	Competency ID	Competency	Description
Core Competencies for Vulnerability Coordination and Vulnerability Disclosure	C009	Conflict Management	This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming.
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
	C003	Client Relationship Management	This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative).
	C029	Knowledge Management	This area contains KSAs that relate to the value of collected information and the methods of sharing that information throughout an organization.
	C030	Legal, Government, and Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Core competencies for Vulnerability Response	C009	Conflict Management	This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming.
	C024	Information Systems/Network Security	This area contains KSAs that relate to the methods, tools, and procedures, including the development of information security plans to prevent information systems vulnerabilities and to provide or restore the security of information systems and network services.
	C033	Network Management	This area contains KSAs that relate to the operation, management, and maintenance of network and telecommunication systems and linked systems and peripherals.
	C034	Operating Systems	This area contains KSAs that relate to a computer network, desktop, and mainframe operating systems and their applications.
	C048	System Administration	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.
	C050	Systems Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
	C011	Critical Thinking	This area contains KSAs that relate to the objective analysis of facts to form a judgment

Purpose	Competency ID	Competency	Description
Competencies for Protection of Incident data and analysis results	C014	Data Privacy and Protection	This area contains KSAs that relate to the relationship between the collection, storage, and dissemination of data while simultaneously protecting individuals' privacy.
	C017	Encryption	This area contains KSAs that relate to the process of transforming information to make it unreadable for unauthorized users.
	C022	Information Assurance	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
	C020	Identity Management	This area contains KSAs that relate to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons."
	C024	Information Systems/Network Security	This area contains KSAs that relate to the methods, tools, and procedures, including the development of information security plans to prevent information systems vulnerabilities and to provide or restore the security of information systems and network services.
	C030	Legal, Government, and Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Supporting competencies	C001	Asset / Inventory Management	This area contains KSAs that relate to the process of developing, operating, maintaining, upgrading, and disposing of assets
	C048	System Administration	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.
	C050	Systems Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
	C015	Database Administration	This area contains KSAs that relate to managing and maintaining database management systems (DBMS) software
	C035	Operations Support	This area contains KSAs that relate to the policies and procedures to ensure the production or delivery of products and services, including tools and mechanisms for distributing new or enhanced hardware and software.
	C053	Technology Awareness	This area contains KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results

4.2. Policies, Frameworks, and Guidelines

ISO released a guideline named "ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure" [115] that focuses on reporting and disclosure of vulnerabilities. Another guideline, "ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes," addresses how to handle the vulnerabilities. FIRST has released a service framework for product incident response teams (PSIRTs) [85] which mainly runs vulnerability management processes in software and hardware products. The Dutch National Cybersecurity Center has offered a detailed policy guideline [116] regarding vulnerability disclosure practices.

CVE is the widely-known database that hosts the largest number of vulnerabilities [117]. A comprehensive list of common hardware and software weaknesses, Common Weakness Enumeration (CWE), is maintained by MITRE [118]. The same source also lists the common 25 software weaknesses in each year [119]. MITRE's other frameworks, CAPEC [120] and ATT&CK [3], shed light on the attack patterns, techniques, and tactics, which would be useful for enriching the vulnerability analysis reports.

N-CSIRTs can benefit from various penetration testing guidelines when they offer similar services for vulnerability identification. PCI Security Standards Council has released a standard and guidelines, which address the security testing of the financial sectors [121]. N-CSIRTs can also use other penetrations testing guidelines, penetration testing execution standards [122]. A technical guide for assisting organizations in planning and conducting security tests is published by NIST [123]. ISECOM has published a security testing guideline, The Open Source Security Testing Methodology Manual (OSSTMM 3) [124]. OWASP, as the leading source for web and mobile security, has released testing guides for web [125] and mobile [126] applications. This organization maintains a list of the common web vulnerabilities [127] and provides a general-purpose vulnerability management guideline [128]. N-CSIRTs can utilize the security guidelines, checklists, audit, and benchmarking tools of the Center for Internet Security [129] while giving vulnerability response services.

4.3. Tools

OpenCVE [130] is a querying and alert generation tool that filters the relevant vulnerabilities obtained from CVE. CIRCL CVE is a similar public search service offered by the Computer Incident Response Center Luxembourg (CIRCL).

The vulnerability scanning tools could be utilized for the identification of the known vulnerabilities. OpenVAS [131], Nessus [132], Qualys [133], and VulnIQ [134] are some samples for network scanning tools. N-CSIRTs can find scanner tools such as Nikto2 [135], Burp Suite [136], Acunetix [137], which are specialized in web applications. InsightVM would be a commercial example of the tools which enable to do vulnerability management in an organizational context.

Kali is widely-known Debian-based Linux distribution that hosts many tools that can be benefited in penetration testing studies [138]. Metasploit is a framework for the utilization of exploits for compromising vulnerabilities [139]. The compromise of web browsers can be realized with BeEf [140]. Static code analyzer, Rips, is a free tool developed for testing PHP codes in white-box tests [141]. ZAP [142] and BurpSuite [136] are used as proxies while conducting web application tests. SQL injection attacks can be checked by using Sqlmap [143]. Web Application Attack and Audit Framework (W3af) is a framework for identifying web application vulnerabilities [144]. MobSF addresses the security testing of mobile applications [145]. Source codes of the applications can be reviewed by utilizing tools such as SonarQube LTS [146].

4.4. Trainings

N-CSIRTs can find many training and certifications regarding penetration testing (i.e., some of them are listed in Table 14) as this area is one of the most popular subject areas in the cybersecurity ecosystem. SANS, CREST, Offensive Security, EC-Council, CompTIA, and MILE2 offer various certifications. SANS has more specific certifications and training for the penetration testing of web apps, mobile devices, cloud services, and IoT devices. Online resources such as Udemy offer various penetration testing courses.

We have identified some training focusing on exploit development. The training, Windows User Mode Exploit Development and Advanced Windows Exploitation offered by Offensive Security and Advanced Exploit Development for Penetration Testers, ARM Exploit Development given by SANS belong to this category. Although the usual penetration testing trainings would be useful, the exploit development trainings best suit the need of vulnerability analysis teams of N-CSIRTs as they provide a more in-depth focus on the vulnerability analysis. It is important to note that almost all of these trainings are at an advanced level, meaning that the relevant N-CSIRT experts should have a strong baseline knowledge about OSs, networks, and programming languages before starting those trainings.

Table 14. Trainings for VM area

Type	Institution	Title	Training/Certification Content	Level
Certifications	Offensive Security	OSCP Certification [147]	Penetration Testing	Intermediate
	CREST	Registered Penetration Tester [148]	Penetration Testing	Intermediate
	CREST	CREST Certified Web Application Tester [149]	Web Application Penetration Testing	Intermediate
	CompTIA	CompTIA PenTest+ [150]	Penetration Testing	Intermediate
	SANS	GIAC Certified Penetration Tester (GPEN) [151]	Penetration Testing	Intermediate/ Advanced
	SANS	GIAC Web Application Penetration Tester (GWAPT) [152]	Web Application Penetration Testing	Intermediate/ Advanced
	SANS	GIAC Enterprise Vulnerability Assessor (GEVA) [153]	Vulnerability Scanning	Intermediate/ Advanced
	SANS	GIAC Mobile Device Security Analysis (GMOB) [154]	Mobile Device Testing	Intermediate/ Advanced
	SANS	GIAC Exploit Researcher and Advanced Penetration Tester [155]	Exploit Development	Advanced
	SANS	GIAC Cloud Penetration Tester [156]	Cloud Application Penetration Testing	Intermediate/ Advanced
	EC-Council	Certified Penetration Testing Professional [157]	Penetration Testing	Intermediate
	EC-Council	Licensed Penetration Tester [158]	Penetration Testing	Advanced
	EC-Council	Certified Ethical Hacker [159]	Penetration Testing	Intermediate
	MILE2	Certified Vulnerability Assessor	Vulnerability Scanning	Intermediate
	MILE2	Certified Professional Ethical Hacker	Penetration Testing	Intermediate
	MILE2	Certified Penetration Testing Engineer	Vulnerability Management	Advanced

Type	Institution	Title	Training/Certification Content	Level
Trainings	Udemy	The Complete Ethical Hacking Course	Penetration Testing	Basic/ Intermediate
	Udemy	Web Hacking: Become a Professional Web Pentester [160]	Web Penetration Testing	Intermediate
	Offensive Security	Penetration Testing with Kali Linux [147]	Penetration Testing	Intermediate
	Offensive Security	Evasion Techniques and Breaching Defenses [161]	Penetration Testing	Advanced
	Offensive Security	Advanced Web Attacks and Exploitation	Web Penetration Testing	Advanced
	Offensive Security	Windows User Mode Exploit Development/Advanced Windows Exploitation	Exploit Development	Advanced
	SANS	Advanced Penetration Testing, Exploit Writing, and Ethical Hacking [162]	Penetration Testing, Exploit Development	Advanced
	SANS	Network Penetration Testing and Ethical Hacking [163]	Penetration Testing	Intermediate
	SANS	Web App Penetration Testing and Ethical Hacking [164]	Web Application Penetration Testing	Intermediate
	SANS	Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques [165]	Web Application Penetration Testing, Exploit Development	Advanced
	SANS	Advanced Exploit Development for Penetration Testers [166]	Exploit Development	Advanced
	SANS	Mobile Device Security and Ethical Hacking [167]	Penetration Testing	Intermediate/ Advanced
	SANS	Cloud Penetration Testing [168]	Penetration Testing	Intermediate/ Advanced
	SANS	IoT Penetration Testing [169]	Penetration Testing	Intermediate/ Advanced
	SANS	ARM Exploit Development [170]	Exploit Development	Advanced

5. SERVICE AREA #4 – SITUATIONAL AWARENESS (SA)

The situational awareness service area is not as straightforward as other service areas in terms of its objectives and relations to each other areas due to not having a common understanding of its definition. However, some concepts can help comprehend SA better. This service area obtains data from other services, for instance, ISIM or ISEM, supports and enriches the data with additional sources in various forms (structured and unstructured), disseminates the analysis outputs to the other service areas, and then constituency. It aims to help the constituency in giving informed decisions about operational, tactical, or strategic level security planning activities. The information gathered in other service areas (e.g., event or incident data) has been contextualized by linking that information with the system assets and business processes or missions to understand the current security posture and predict the future. The service area mainly resorts to methods or tools for data collection, dissemination, and analysis, necessitating an advanced capability in information sharing and data analytics. Although the contextualization may be complicated for N-CSIRTs having a large constituency base that includes various types of organizations and thus varying business processes/missions, still, N-CSIRTs can develop the situational awareness capability. This service area consists of three services, data acquisition, analysis and synthesis, and communication.

Our survey results show that eight respondents have intermediate/advanced levels in data acquisition, ten respondents have intermediate/advanced levels in data analysis and synthesis, and nine respondents have intermediate/advanced levels in communication services. These figures are closer to ISEM and VM areas and relatively less than the ISIM service area. All N-CSIRTS give this service to some extent. The maturity of data acquisition is slightly less than the other services, indicating more room for further development. On the other side, all N-CSIRTs have plans for creating new services or extending the existing ones in this area. It should be noted that data acquisition service receives the greatest attention in plans when compared to services of other areas.

5.1. Knowledge/ Skills/ Abilities/ Competencies

SA area requires a careful harmonization of the threat feeds, incident reports, vulnerability assessment results, asset inventory information, and news of internal/external events. Such operational-level information should be supported by trend analysis of "new technologies, methods or practices" and other organizational-level information such as "acceptable policies, plans, normal operating conditions" [2]. Thus, a diverse set of competencies encompassing technical and non-technical subject areas should be developed within a team or across the whole N-CSIRT organization. Considering the complexity of the service area objective and the requirement of a wider competency set, N-CSIRT may need, at least, support from a horizontal organizational structure and well-developed information flow between different service areas.

"C055 Threat Analysis" and "C057 Vulnerability Assessment" constitute the core competencies of this SA service area, similar to the other areas. The competencies, "C001 – Asset / Inventory Management" and "C037 – Organizational Awareness", enable the SA team to comprehend information and system assets and their relations with organizational missions or business processes. "C018 – Enterprise Architecture" is necessary for better integration of these two competencies. "C019 – External Awareness" and "C053 – Technology Awareness" direct the attention to the outer world by acquiring the capability for following the external economic, political, social, and technology trends at national and international levels. SA can be achieved by creating and maintaining automatic or semi-automatic information flows between different systems (e.g., SIEM, vulnerability management systems, threat intelligent collection tools). Thus, "C049 – Systems Integration" should be included in the competency portfolio.

Analysis and Synthesis service is based on an advanced level of data analytics capability requiring the competencies, “C012 - Data Analysis” and “C013 – Data Management”. Some N-CSIRTs may resort to the competency, “C032 – Modeling and Simulation”, to support the data analytics tasks. The development of security plans and incorporating the data analytic results into the security decisions can be handled by “C024 - Information Systems/Network Security”.

Communicating the situational awareness results with the constituency can be achieved by establishing proper information sharing processes by acquiring the competency, “C029 – Knowledge Management”. Soft-skill-oriented competencies, “C003 – Client Relationship Management”, “C036 – Oral Communication” and “C060 – Written Communication” facilitate the interaction of the SA team with other teams in N-CSIRT and the constituency. The groups “Competencies for Protection of Incident data and Analysis Results” and “Supporting Competencies” listed in Table 15 provide the baseline capabilities for maintaining and securing the information systems taking part in this service area.

Table 15. Competency Areas for SA

Purpose	Competency ID	Competency	Description
Core Competencies For Data Acquisition	C001	Asset / Inventory Management	This area contains KSAs that relate to the process of developing, operating, maintaining, upgrading, and disposing of assets
	C018	Enterprise Architecture	This area contains KSAs that relate to the principles, concepts, and methods of enterprise architecture to align information technology (IT) strategy, plans, and systems with the mission, goals, structure, and processes of the organization.
	C019	External Awareness	This area contains KSAs that relate to identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization
	C037	Organizational Awareness	This area contains KSAs that relate to understanding an organization’s mission and functions, its social and political structure, and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization.
	C049	Systems Integration	This area contains KSAs that relate to the principles, methods, and procedures for installing, integrating, and optimizing information systems components.
	C053	Technology Awareness	This area contains KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results
	C055	Threat Analysis	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.
	C057	Vulnerabilities Assessment	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.

Purpose	Competency ID	Competency	Description
Core Competencies for Analysis and Synthesis	C012	Data Analysis	This area contains KSAs that relate to collecting, synthesizing, and/or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence
	C013	Data Management	This area contains KSAs that relate to the development and execution of data management plans, programs, practices, processes, architectures, and tools that manage, control, protect, deliver, archive, dispose of, and enhance the value of data and information assets.
	C032	Modeling and Simulation	This area contains KSAs that relate to mathematical modeling and simulation tools and techniques to plan and conduct test and evaluation programs, characterize systems support decisions involving requirements, evaluate design alternatives, or support operational preparation.
	C024	Information Systems/Network Security	This area contains KSAs that relate to the methods, tools, and procedures, including the development of information security plans to prevent information systems vulnerabilities and to provide or restore the security of information systems and network services.
Core competencies for Communication	C003	Client Relationship Management	This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative).
	C029	Knowledge Management	This area contains KSAs that relate to the value of collected information and the methods of sharing that information throughout an organization.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.
	C014	Data Privacy and Protection	This area contains KSAs that relate to the relationship between the collection, storage, and dissemination of data while simultaneously protecting individuals' privacy.
	C017	Encryption	This area contains KSAs that relate to the process of transforming information to make it unreadable for unauthorized users.
	C022	Information Assurance	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
	C020	Identity Management	This area contains KSAs that relate to the security and business discipline that "enables the right individuals to access the right resources at the right times and for the right reasons."

Purpose	Competency ID	Competency	Description
	C024	Information Systems/Network Security	This area contains KSAs that relate to the methods, tools, and procedures, including the development of information security plans to prevent information systems vulnerabilities and to provide or restore the security of information systems and network services.
	C030	Legal, Government, and Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
Supporting competencies	C001	Asset / Inventory Management	This area contains KSAs that relate to the process of developing, operating, maintaining, upgrading, and disposing of assets
	C048	System Administration	This area contains KSAs that relate to the upkeep, configuration, and reliable operation of computer systems.
	C050	Systems Testing and Evaluation	This area contains KSAs that relate to the principles, methods, and tools for analyzing and administering systems test and evaluation procedures, as well as technical characteristics of IT systems, including identifying critical operational issues.
	C015	Database Administration	This area contains KSAs that relate to managing and maintaining database management systems (DBMS) software
	C035	Operations Support	This area contains KSAs that relate to the policies and procedures to ensure the production or delivery of products and services, including tools and mechanisms for distributing new or enhanced hardware and software.
	C053	Technology Awareness	This area contains KSAs that relate to keeping up-to-date on technological developments and making effective use of technology to achieve results

5.2. Tools

It is not easy to discriminate the tools that could be used in the SA service area and other areas as the term “situational awareness” is usually used as a buzzword by the tool vendors for some advanced capabilities of existing technologies (e.g., SIEM, log management, cyber threat intelligence). It could be argued that a specific well-established technology line has not evolved around this term, thanks to the lack of common understanding of the term. Situational awareness requires high interaction and continuous loops between tools in other service areas. The tools regarding the threat intelligence analysis, event management, and incident handling listed in the service areas, ISIM, ISEM, and VM, could be considered as parts of SA systems. Nevertheless, in this subsection of the document, we have listed some other tools that can help N-CSIRTs get SA at the national level.

Cyber threat intelligence vendors, Team-Cymru [38] and Shadowserver [39], consolidate their threat intelligence feeds and provide reporting services to N-CSIRTs. Such consolidated reports could be considered as a significant input for grasping national-level situational awareness.

Wide-scale security scanning of a network range belonging to a corresponding country would be a source for SA systems. SHODAN [49], a search engine that allows the identification of specific OS types or devices connected to the Internet, could be queried for a specific network range. Another security scanning study conducted by Cyber Green [50] reveals the risks of networks against some denial of service attacks.

Wide-scale traffic monitoring systems run by regional or N-CSIRTs (e.g., TSUBAME [61], intrusion detection sensors operated by APCERT) can be another source for situational awareness systems. CMU-SEI has developed a set of tools for monitoring flow data belonging to large-scale networks [171].

6. SERVICE AREA # 5 – KNOWLEDGE TRANSFER (KT)

This service area aims to "collect relevant data, perform detailed analysis, and identify threats, trends, and risks, as well as to create best current operational practices to help organizations to detect, prevent, and respond to security incidents" [2]. Transferring knowledge as part of this service is key to improving a CSIRTs security.

This service area is composed of four services, awareness building, training and education, exercises, and technical and policy advisory. The first one aims to improve the security posture of the constituency and aid in the detection, prevention, and recovering from incidents, through preparedness and education through research and information aggregation, report and awareness materials development, information dissemination, and outreach. The purpose of training and education is to train and educate the constituency on cybersecurity, information assurance, and incident management through knowledge gathering, educational development, content delivery, mentoring, and professional development to establish strong relationships and improve overall cybersecurity posture to mitigate or prevent future incidents. The third, exercises, are aimed to evaluate and enhance the efficiency and efficacy of cybersecurity services and functions through requirements analysis, format and environment development, scenario development, exercises execution, and exercise outcome review. The final service focuses on ensuring that the N-CSIRTs policies and procedures include sufficient incident management consideration to better prepare for and defend against threats through risk management support, business continuity and recovery planning, policy support, and technical advice.

According to the survey of the 16 N-CSIRT members from low-income countries there are varying maturity levels with all respondents stating they offer at least basic services in this service area. As in Table 7, 3 to 5 N-CSIRTs declared their respective services were at the advanced level, with the remaining respondents saying their services were at the basic to intermediate level. Compared to the other service areas, knowledge transfer seems to have a greater emphasis to N-CSIRTs in low-income countries. According to Table 8 which discusses N-CSIRTs plan to expand or offer services in the next 5 years, a majority of respondents, 16 in training and education, 14 in awareness building, and 13 in both exercises and technical and policy advisory plan to expand their current offerings in the next 5 years.

6.1. Knowledge/ Skills/ Abilities/ Competencies

For this service area, policy and strategy, communication, and relationship building were the categories declared by a majority of respondents (i.e., 7 for policy and strategy, 8 for communication, and 8 for relationship building) as the main technical and soft skills needed to improve their N-CSIRT. This indicates that it is important to identify the relevant knowledge, skills, and competencies needed in this area.

According to the NICE framework, we identified the competencies given in Table 17 for the KT area. The first column of the table gives the purpose addressed by the corresponding competency, the second, third, and fourth columns present the competency id, the name of the competency, and its description respectively.

N-CSIRTs should have the competencies, "Analyze (AN)," Collect and Operate (CO)," "Investigate (IN)," "Operate and Maintain (OM)," "Oversee and Govern (OV)," "Protect and Defend (PR)," and "Securely Provision (SP)" to aid in awareness building, training and education, exercises, and technical and policy advisory. The first one is analyzing the threat. The second is collect and operate which involved collecting information and operating a plan to investigate the cyber activity. Investigate means to forensically analyze the information at hand. Next, operation and maintain entails managing and administering technical support and management. Oversees and govern involves the development, advisement, and management of IT investments and services. Protect and defend relies on cyber defense and vulnerability assessments. Lastly, securely provision relies on assessing the systems and security in place.

Awareness building typically relies on research and information aggregation, reports and awareness materials development, information dissemination, and outreach. The competencies in this are "C0-19 External Awareness", "C0- 28 Interpersonal Skills", "C036-Oral Communication", "C052-Teaching Others", "C060- Written Communication". In this area, identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization is vital via "C0-19 External Awareness". "C0- 28 Interpersonal Skills" or developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations, and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors is critical throughout each service area offering. Similarly, "C036-Oral Communication "the process of expressing information or ideas by word of mouth helps people interact improving the end result. "C052-Teaching Others" refers to educating others and imparting knowledge of or giving information about a particular subject, which is necessary for knowledge transfer. Like oral communication, "C060- Written Communication" is expressing information but via written word.

Training and education rely on knowledge, skill, and ability requirements gathering, educational and training materials development, content delivery, mentoring, and CSIRT staff professional development. The competencies in this are "C029- Knowledge Management", "C028- Interpersonal Skills", "C036- Oral Communication", "C039 - Presenting Effectively", "C052 - Teaching Others", "C059 - Workforce Management", "C060- Written Communication". Both "C029- Knowledge Management", the value of collected information and the methods of sharing that information throughout an organization and "C059 - Workforce Management" the activities needed to maintain a productive workforce aid in training and educating individuals. "C039 - Presenting Effectively" is the activity in which someone shows, describes, or explains something to an audience.

Exercises entail requirements analysis, format and environment development, scenario development, exercises execution, and exercise outcome review. The competencies in this are "C019- External Awareness", "C028- Interpersonal Skills", "C036- Oral Communication", "C037 – Organizational Awareness", "C044 – Risk Management", "C052 - Teaching Others", "C059 - Workforce Management", "C060- Written Communication". For exercises to successfully be carried out, "C037 – Organizational Awareness" or understanding an organization's mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization is needed. "C044 – Risk Management" are the methods and tools used for risk assessment and mitigation of risk.

Technical and Policy Advisory rely on risk management support, business continuity and disaster recovery planning support, policy support, and technical advice. The competencies in this are "C002 – Business Continuity", "C003 – Client Relationship Management", "C009 – Conflict Management", "C019- External Awareness", "C028- Interpersonal Skills", "C030 – Legal, Government, and Jurisprudence", "C036- Oral Communication", "C037 – Organizational Awareness", "C038 – Policy Management", "C039 – Presenting Effectively", "C044 – Risk Management", "C047 – Strategic Planning", "C056 – Third Party Oversight/ Acquisition Management", "C059 - Workforce Management", "C060- Written Communication". "C002 – Business Continuity" is the planning and preparation of a company to make sure it overcomes serious incidents or disasters and resumes its normal operations within a reasonably short period. Proper management is also necessary for advisory roles, including: "C003 – Client Relationship Management" the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative); "C009 – Conflict Management" managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming; "C038 – Policy Management" the process of creating, communicating, and maintaining policies and procedures within an organization; "C044 – Risk Management" the methods and tools used for risk assessment and mitigation of risk; "C056 – Third Party Oversight/ Acquisition Management" process of analyzing and controlling risks presented to your company, data, operations and finances by parties other than your own company. Awareness of the business and surroundings also aids in advisory where, "C019- External Awareness" identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization and "C037 – Organizational Awareness" understanding an organization's mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization. "C047 – Strategic Planning" relates to formulating effective strategies consistent with the objective, vision, and competitive strategy of the organization and/or business unit. Controlling legal risks "C030 – Legal, Government, and Jurisprudence" including company data, operations and finances by parties other than your own company.

Table 16. Competencies for KT Area

Purpose	Competency ID	Competency	Description
Awareness building	C019	External Awareness	This area contains KSAs that relate to identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization
	C028	Interpersonal Skills	This area contains KSAs that relate to developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations. Considering and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
	C052	Teaching Others	This area contains KSAs that relate to imparting knowledge of or giving information about or instruction in (a subject or skill)
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.
Training and Education	C029	Knowledge Management	This area contains KSAs that relate to the value of collected information and the methods of sharing that information throughout an organization.
	C028	Interpersonal Skills	This area contains KSAs that relate to developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations. Considering and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth

Purpose	Competency ID	Competency	Description
	C039	Presenting Effectively	This area contains KSAs that relate to the activity in which someone shows, describes, or explains something to an audience.
	C052	Teaching Others	This area contains KSAs that relate to imparting knowledge of or giving information about or instruction in (a subject or skill)
	C059	Workforce Management	This area contains KSAs that relate to the activities needed to maintain a productive workforce
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.
Exercises	C019	External Awareness	This area contains KSAs that relate to identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization
	C028	Interpersonal Skills	This area contains KSAs that relate to developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations. Considering and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
	C037	Organizational Awareness	This area contains KSAs that relate to understanding an organization's mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization.
	C044	Risk Management	This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.
	C052	Teaching Others	This area contains KSAs that relate to imparting knowledge of or giving information about or instruction in (a subject or skill)
	C059	Workforce Management	This area contains KSAs that relate to the activities needed to maintain a productive workforce
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.
Technical and policy advisory	C002	Business Continuity	This area contains KSAs that relate to the planning and preparation of a company to make sure it overcomes serious incidents or disasters and resumes its normal operations within a reasonably short period
	C003	Client Relationship Management	This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative).
	C009	Conflict Management	This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to

Purpose	Competency ID	Competency	Description
			minimize negative personal impact; collaborates with others to encourage cooperation and teaming.
	C019	External Awareness	This area contains KSAs that relate to identifying and understanding how internal and external issues (e.g., economic, political, social trends) impact the work of the organization
	C028	Interpersonal Skills	This area contains KSAs that relate to developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations. Considering and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors.
	C030	Legal, Government, & Jurisprudence	This area contains KSAs that relate to laws, regulations, policies, and ethics that can impact organizational activities.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
	C037	Organizational Awareness	This area contains KSAs that relate to understanding an organization’s mission and functions, its social and political structure and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization.
	C038	Policy Management	This area contains KSAs that relate to the process of creating, communicating, and maintaining policies and procedures within an organization
	C039	Presenting Effectively	This area contains KSAs that relate to the activity in which someone shows, describes, or explains something to an audience.
	C044	Risk Management	This area contains KSAs that relate to the methods and tools used for risk assessment and mitigation of risk.
	C047	Strategic Planning	This area contains KSAs that relate to formulating effective strategies consistent with the objective, vision, and competitive strategy of the organization and/or business unit.
	C056	Third Party Oversight	This area contains KSAs that relate to the process of analyzing and controlling risks presented to your company, data, operations and finances by parties other than your own company.
	C059	Workforce Management	This area contains KSAs that relate to the activities needed to maintain a productive workforce
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.

6.2. Policies, Frameworks and Guidelines

N-CSIRT staff should incorporate and share in-depth knowledge on cybersecurity and information assurance in the KT services. In this, the SANS Security Policy [172] templates serve as a repository on security know-how from leaders and subject matter experts around the world. They can benefit from _ framework. NIST also provides a number of frameworks and guidelines including the NIST Special Publication 800-50 - "Building an Information Technology Security Awareness and Training Program" [173] for awareness building, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" [174] for training and education, and the NIST guide to test, training, and exercise program for IT [175], and risk management system for technical policy advisory [176]. For exercises, the MITRE framework [177], NARUC framework [178], CISA exercise playbook [179], and ENISA cyber exercises [180] are used for exploration. Similarly, NICE presents a framework for Cybersecurity workforce.

6.3. Tools

Knowledge transfer services require a host of tools to help position relevant data, perform analysis, identify risks and trends, and communicate with the consistency. These processes play a critical role in delivery of the service area, which can be further advanced using tools. A variety of open-source tools exist that are currently utilized by various CSIRTs, while commercial tools in this area are lacking. The recommend open-source ones are GCA Cybersecurity Toolkit [181], CREST Cyber Threat Intelligence Maturity Assessment Tool [182], OPENCSIRT SIM3 [183, p. 3], MITRE GitHub [184], and SANS Cybersecurity Tools [185]. Along these lines, the Know to Be [186] free security tool is used to aid in raising awareness.

For training and education and exercises, cyber ranges are deemed beneficial. Players like AfricaCERT use Cyber range platforms to train team and support cyber drills, provide content, and support training, amongst other things. Within these cyber ranges there are opportunities for community collaboration where cyber ranges can excel beginners to security professionals. Interviews with teams have revealed that few available training providers offer hands-on and continuous training opportunities based on real case scenarios. Many experts interviewed also believe that existing solutions focus more on course completion and certification than competence acquisition. Yet, organizations are now using cyber range platforms for skills development at the national level and cross-continental exercises. These platforms provide an environment to develop exercises, run challenges and CTFs, and remove the difficulties of deploying several virtual machines. Cyber ranges provide practical training and offer opportunities for community collaboration to develop a variety of exercises. Exercises provide desired skills and competencies with various levels of complexity. Scores serves to reflect participants' current posture vs. the desired posture in their maturity curve. Besides, the scenarios and scores offer the opportunity for teams to retrain, grow and improve.

Utilizing Cyber Drills can increase collaboration and confidence of exercises and incident response of CSIRTs. Such program includes AfricaCERT, APCERT, ITU, OAS, and OICCERT. For example, AfricaCERT organized its first Cyber Drill: "Testing the Waters," in 2021. The Drill aimed to test the response capability of participating teams facing the following scenarios: Phishing, Defacement, REM, Ransomware investigation. These exercises were designed to put participants into live conditions and tested their communication and technical capabilities. 32 Computer Security Incident Response Teams from 24 countries, including APCERT and OICCERT economies teams, participated in the Drill. Similarly, for exercises, there are a variety of options including the CISA tabletop exercises [187].

6.4. Trainings

For knowledge transfer, a variety of trainings exist that offer applied lessons at beginner to advanced levels, with limited trainings offering theoretical lessons. The recommended trainings are offered by a host of providers at various prices, including CREST, MITRE, SANS, ENISA, NIST, ESET, and a variety of commercial awareness trainings. MITRE, NIST, and ENISA training options are free or offer low-cost solutions, while the CREST cost upwards of $250, SANS typically lie between $1,000-$10,000, and the commercial offerings like NINJIO and CybSafe offer a variety of priced services depending on the size of the business or entity inquiring. Although many of these commercial trainings are used by small to large business, some of them are used by government agencies and offices. In this service area the training offerings are practical in nature, with many using real-world scenarios and storytelling, game play experiences (i.e., NINJIO). The list of trainings we identified for this service area are presented in Table 18. The trainings identified cover all the services in knowledge transfer and are applicable for a range of N-CSIRT staff.

Table 17. Trainings for KT area

Institution	Training	Training Content	Level
CREST	CREST Exams [188]	All	Medium/Advanced
MITRE	MITRE Open Security Training [189], [190]	All	Beginner
MITRE	MITRE Cyber Academy [189]	All	Beginner
SANS	SANS Cybersecurity Courses/ Training [191] SANS #SecureTheFamily [192] Managing Human Risk: Mature Security Awareness Programs [193]	Awareness building, technical and policy advisory	Beginner/Advanced
SANS	Security Strategic Planning, Policy, and Leadership [194]	Technical and policy advisory	Beginner/Medium
SANS	Law of Data Security and Investigations [111]	Technical and policy advisory	Beginner/Medium
SANS	A Practical Introduction to Cybersecurity Risk Management [195]	Technical and policy advisory	Beginner
SANS	Leading Cybersecurity Change: Building a Security-Based Culture [196]	Technical and policy advisory	Beginner/Medium
SANS	IT Project Management and Effective Communication [197]	Technical and policy advisory	Beginner/Medium
ENISA	ENISA Cybersecurity Training [198]	Awareness building, training & education	Medium/Advanced
ESET	Online Cybersecurity Awareness Training [199]	Awareness building	Beginner/Advanced
NINJIO	NINJIO Cybersecurity Awareness Training [200]	Awareness building	Beginner
NIST	Career and Professional Development Educator Training and Curriculum Employee Awareness Training K12 Education and Games [201]	Awareness building, training & education, exercises.	Beginner/Advanced
KnowBe4	Security Awareness Training [202]	Awareness building	Beginner/Medium

Institution	Training	Training Content	Level
Cofense	PhishMe [203]	Awareness building	Beginner/Medium
CybSafe	Security Awareness Training [204]	Awareness building	Beginner/Medium
Elevate Security	Security Awareness Training [205]	Awareness building	Beginner/Medium
Mimecast	Security Awareness Training [206]	Awareness building	Beginner/Medium
Proofpoint	Security Awareness Training [207]	Awareness building	Beginner/Medium
Living Security	Security Awareness Training [208]	Awareness building	Beginner/Medium
LUCY	Security Awareness Training [209]	Awareness building	Beginner/Medium

7. COMPETENCIES REQUIRED FOR MANAGEMENT ROLES IN N-CSIRTS

Depending on the size of an N-CSIRT, various managerial positions would be needed in the organizational structure. Such positions may lead operational teams, manage services, run projects or have auditing responsibilities. The services of N-CSIRTs are highly dependent on each other, and a well-established communication with external entities (e.g., constituency, other N-CSIRTs) is necessary. Thus, in addition to the tasks at operational and tactical levels, necessitating various technical and operational competencies, such positions should also assume important communication and management roles. The common competencies we identified for the management roles are given in Table 16.

Although it may not be possible to expect a position to have a deep level of technical expertise in many subjects, still, a baseline knowledge is necessary. “C021 - Incident Management,” “C022 – Information Assurance,” “C055 – Threat Analysis,” “C057 – Vulnerabilities Assessment,” and “C040 – Problem Solving” constitute the core technical competency set. Excellence in oral and written communication is highly expected. “C028 - Interpersonal skills,” “C039 – Presenting Effectively” and “C009 – Conflict Management” are other competencies to have better interaction with the team/project members and other parties. Managerial positions require a thorough understanding of the main missions and functions of N-CSIRT by having “C037-Organizational Awareness.” They should have the capability to manage organizational policies and procedures referring to “C038 – Policy Management.” The competency, “C047 – Strategic Planning,” enables the position to determine short, medium, and long term goals of the corresponding management unit.

The human resource and its development are one of the most significant items in the agenda of N-CSIRT managers due to the rapidly evolving technical nature of the cybersecurity domain. The number of cybersecurity experts is usually scarce and enhancing the capabilities of the existing staff is costly. Thus, finding the right talents, training them, keeping them in the organization, and thus reducing the turnover rates are necessary. Most of the service areas do not only demand technical skills but various soft skills as well. Therefore, “C059 – Workforce Management” should be included in the competency set. Other leadership competencies such as “C042 – Project Management” and “C011 – Critical Thinking” are also highly needed.

Table 18. Competencies for Managerial Positions

Purpose	Competency ID	Competency	Description
Technical	C021	Incident Management	This area contains KSAs that relate to the tactics, technologies, principles, and processes to analyze, prioritize, and handle incidents.
	C022	Information Assurance	This area contains KSAs that relate to the methods and procedures that protect information systems and data by ensuring their availability, authentication, confidentiality, and integrity.
	C040	Problem Solving	This area contains KSAs that relate to determining the accuracy and relevance of information and using sound judgment to generate and evaluate alternatives; making well-informed, objective decisions that take into account facts, goals, constraints, and risks while perceiving the impact and implications of decisions.
	C055	Threat Analysis	This area contains KSAs that relate to the process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks.
	C057	Vulnerabilities Assessment	This area contains KSAs that relate to the principles, methods, and tools for assessing vulnerabilities and developing or recommending appropriate mitigation countermeasures.
Operational	C003	Client Relationship Management	This area contains KSAs that relate to the concepts, practices, and techniques used to identify, engage, influence, and monitor relationships with individuals and groups connected to a work effort—including those actively involved, those who exert influence over the process and its results, and those who have a vested interest in the outcome (positive or negative).
	C037	Organizational Awareness	This area contains KSAs that relate to understanding an organization’s mission and functions, its social and political structure, and how programs, policies, procedures, rules, and regulations drive and impact the work and objectives of the organization.
	C038	Policy Management	This area contains KSAs that relate to the process of creating, communicating, and maintaining policies and procedures within an organization
Leadership	C042	Project Management	This area contains KSAs that relate to the principles, methods, or tools for developing, scheduling, coordinating, and managing projects and resources, including monitoring and inspecting costs, work, and contractor performance.
	C047	Strategic Planning	This area contains KSAs that relate to formulating effective strategies consistent with the objective, vision, and competitive strategy of the organization and/or business unit.
	C059	Workforce Management	This area contains KSAs that relate to the activities needed to maintain a productive workforce
	C009	Conflict Management	This area contains KSAs that relate to managing and resolving conflicts, grievances, confrontations, or disagreements in a constructive manner to minimize negative personal impact; collaborates with others to encourage cooperation and teaming.

Purpose	Competency ID	Competency	Description
	C011	Critical Thinking	This area contains KSAs that relate to the objective analysis of facts to form a judgment
Professional	C028	Interpersonal Skills	This area contains KSAs that relate to developing and maintaining effective relationships with others; relating well to people from varied backgrounds and different situations—considering and responding appropriately to the needs, feelings, and capabilities of subordinates, peers, and seniors.
	C036	Oral Communication	This area contains KSAs that relate to the process of expressing information or ideas by word of mouth
	C039	Presenting Effectively	This area contains KSAs that relate to the activity in which someone shows, describes, or explains something to an audience.
	C060	Written Communication	This area contains KSAs that relate to any type of message that makes use of the written word.

SECTION 3: INNOVATIONS IN N-CSIRT CAPACITY BUILDING AND RECOMMENDATIONS

In this section of the report, we share innovative applications of N-CSIRTs in finding funding, effective governance mechanisms, and national cyber workforce development, which we identified in the interviews with N-CSIRT representatives and subject matter experts.

1. TAKE A HOLISTIC APPROACH

Many capacity builders focus on providing technical training to national CSIRTs. Developing the technical skills of a national CSIRT's staff is important, but capacity building can have a more long-term impact if the national CSIRT is assessed more holistically. In other words, other organizational gaps need to be identified and addressed. For example, national CSIRTs need

- designated, long-term funding
- government buy-in and support of its mission
- placement at the appropriate governmental or organizational level that provides it the necessary authority or influence to engage constituents
- a parent organization that serves as a champion for its mission

Addressing technical and organizational gaps through capacity building helps to ensure ongoing development and maturation of a national CSIRT.

2. TAILOR SOLUTIONS

Those responsible for creating a national CSIRT frequently ask what their national CSIRT should look like. However*, there is no single or "right" way to build a national CSIRT*. Every organization/country is different, and there are many variables to consider when determining structure, services, and daily operations. While best practices for creating a CSIRT are important to incorporate into development plans, it is equally important to align the plans with the following:

- parent organization's mission and processes
- national CSIRT's mission, authority, and constituency
- cybersecurity needs and capabilities of the national CSIRT's constituents
- national cybersecurity strategies, policies, and legislation
- available funds

While looking at the structures and processes of other national CSIRTs and seeking the advice of capacity builders is helpful, teams should not be afraid to tailor their efforts – *what works for one may not necessarily work for another.*

3. ESTABLISH A STRONG OPERATIONAL FOUNDATION

What a national CSIRT provides operationally depends on its mission, authority, and constituency. Things to consider when determining and establishing operations include

- Services – Provide services with the most value and impact for constituents and adjust as needed. This may mean starting with a few services and expanding over time. It is much better to provide 2-3 key services and be really good at them than it is to provide many services that you do not have enough staff or expertise to provide or maintain effectively.

- Documentation – Ensure policies and procedures are accurately documented, routinely reviewed, and updated as needed; ensure they are understood and followed by staff. Documented policies and procedures are required for the provision of consistent, accurate, and trustworthy services. While you may choose not to document every process, at minimum you should maintain accurate and documented standard operating procedures (SOPs) for your core incident response procedures.
- Tools – Select tools based on the services you are providing and your budget. Evaluate tool requirements in conjunction with assessing skills needed to hire the right staff. Open source tools may be free, but they can still be costly if they require modifications to meet the team's needs or highly skilled staff to maintain the tools. Commercial off-the-shelf tools may have an expensive initial cost, but they *may* come with support for maintaining, tailoring, and training staff how to use them.

4. CREATING A PIPELINE OF CYBERSECURITY WORKFORCE: COOPERATION WITH UNIVERSITIES AND ACADEMIC INSTITUTIONS

N-CSIRTs can cooperate with the universities in reaching the young talents, motivating them to choose cybersecurity as a career goal, and providing them the initial training. Short-term education programs (e.g., summer training camps) could be a significant starting point for accessing the young talent pool. In these programs, although the attendants would get some knowledge in that short time frame, the main objective would be to create or increase motivation regarding the cybersecurity subjects among the students.

N-CSIRTs can identify the students who have an interest in the subject and even hire them if they have junior-level vacancies. More long-term cooperation with the universities can be established by creating individual courses or long-term programs (e.g., certification, graduate, or undergraduate programs). It is important to note that even though some academicians who are interested in the field would initiate some efforts in their universities, the establishment of long-term programs requires more instructors. On the other side, finding such instructors is always hard for the universities as cybersecurity requires academicians who are equipped with a combination of theoretical and practical knowledge in an area that is relatively new. N-CSIRTs can actively cooperate with the universities, help them design their cybersecurity curriculum, and even provide instructors for some courses. They can reach out to cybersecurity experts from local or global ecosystems and introduce them to the universities. After these proactive efforts of N-CSIRTs about academic program development, universities would have the initial capability to develop further.

Turkish National Computer Emergency Team (TR-CERT) can be considered as an example of such cooperation between N-CSIRT and universities. TR-CERT organized various summer camp programs for university students in cooperation with the private companies and some universities starting from 2011. One noteworthy aspect of these efforts is that some of the summer camps addressed not only the students with a technical background but also students with a social science background. In those programs, two main tracks were established; one of them was for technical subjects (e.g., penetration testing, network forensics, web application security), and the second one addressed strategic topics (e.g., national strategy development, cyber conflicts). TR-CERT has actively contributed to two universities in establishing graduate-level cybersecurity programs in which the experts from TR-CERT acted as instructors of many courses. It is important to note that the amount of active contribution given by TR-CERT has gradually decreased as the universities managed to develop their capabilities in time.

Another innovative approach is from Tunisian National CERT, tunCERT, which conducted a wide-scale project aiming to develop a national framework for assessing the skill needs of the local market. This framework, which is based on a more simplified version of the NICE Cybersecurity Workforce Framework [210], enables the analysis of current training offerings of the universities and private sector, perform a gap analysis between the offerings and the actual need of the market and propose updates on their curriculums.

Since its launch, EG-CERT reached out to a leading IT professional institute, the Information Technology Institute (ITI) [211] that is affiliated with the Egyptian Ministry of Communications and Information Technology, to establish and further develop a special track for cybersecurity. EG-CERT professionals participated in developing curricula, teaching courses and supervising graduation projects at ITI. In addition, there has been on-going collaboration with universities including the 1st ranked Egyptian university, Cairo University, and many others. Such partnerships secured a continuous supply of cyber talents to EG-CERT and to the Egyptian market at large.

5. IMPROVING THE TECHNICAL CAPABILITIES

In our survey, we identified that most of the participating N-CSIRTs deliver services from each service area with varying maturity levels, which indicates that they have passed the initial establishment phase, demonstrated a considerable level of progress, and had ambitious plans for further advancing their service portfolio. Their maturity levels are relatively lower in service areas such as Information Security Event Management, Vulnerability Management, and Situational Awareness. To fulfill their service improvement plans, acquiring more technical capabilities (e.g., malware analysis, threat intelligence management, digital forensics) will play an essential role. Although N-CSIRTs underlined the need for better tools, a considerable part of the respondents referred to their experience with the open-source tools. On the other side, they pointed out that accessing the necessary trainings is still a problem due to limited budgets or difficulties in finding good trainers.

The international and regional organizations and donor countries have established various training programs, mostly addressing the establishment of CSIRT teams and developing national cybersecurity strategies. Considering our survey findings regarding the high-level engagement of respondents with international and regional organizations, the efforts of such organizations would more focus on technical trainings, which can be given with the support of cybersecurity training companies. The training content could include open-source tools while introducing the subjects.

6. LEVERAGING PUBLIC-PRIVATE PARTNERSHIP TO OPERATE

The national Computer Emergency Response Team of Togo, CERT.tg, has a mission to identify, analyze and mitigate cyber threats affecting the Togolese state, citizens, companies, and organizations. It contributes to ensuring the cybersecurity of the Togolese nation. Cyber Defense Africa (CDA) operates CERT.tg as a service delegated by the National Cybersecurity Agency (ANCy).

The funding mechanism is very interesting where CERT.tg generates its own funds and is fully sustainable. CERT.tg provides fee-based value-added services to critical sector operators, through membership dues and fees, and offers value-added training services to its private sector. CERT.tg has achieved financial independence by choosing a public-private partnership (PPP) model to raise funding. These arrangements have positively influenced the trust of National stakeholders and served the need to provide service excellence and maintain operations. The organisational structure of CERT.TG gives them the agility of a private company and enables various talent acquisition and retention strategies.

The PPP model chosen by CERT.TG has also other benefits. It allow to provide incentives to motivate and retain the staff.

7. TRUST BUILDING

CSIRT professionals should be open to sharing knowledge and expertise with their peers. N-CSIRTs often provide seminars, workshops, and training to professionals working in key entities and organizations, nationally, regionally, and internationally. They also may support organizing cyber competitions, such as Capture the Flag (CTFs) and cyber drills. At the operational level, public-private partnerships and empowering the cybersecurity industry are key to the success of CSIRT operation as well as for drafting and implementing cybersecurity strategies at the organizational and the national levels.

In one of our interviews, the expert who led the development of tunCERT has given consultancy to many national and organizational CSIRTs stating that the best way of increasing trust between N-CSIRT and its constituency is adopting a strategy so-called “service strategy.” This means N-CSIRTs should be proactive in reaching the constituency, instead of waiting for them to report incidents, N-CSIRTs should first initiate information sharing by providing them valuable information, for instance, identifying cyber threat intelligence (CTI) related to their networks from open CTI sources and sharing them with the corresponding organization would be a beginning for trust-building. N-CSIRTs can give free trainings or deliver information about security tools.

8. KNOWLEDGE TRANSFER FROM OTHER N-CSIRTS

In some regions, several N-CSIRTs have developed coaching strategies between teams through mutual assistance arrangements, internships, and study tours. An illustration of these arrangements is a more mature team sending trainers to another country for training. The research team has also found a model where a team would send staff as interns to another N-CSIRT to acquire on-the-job knowledge. A good example is between the Egyptian Computer Emergency Readiness Team (EG-CERT) and the Tanzanian Computer Emergency Response Team (TZ-CERT). EG-CERT experts visited TZ-CERT in Dar es Salaam to train their experts. EG-CERT provided similar support to Uganda CERT as well [212], [213].

When the required expertise is unavailable in the region, the international network serves to put in place requests for proposals to invite international experts to deliver train-the-trainers programs. Various arrangements from fee-based to free or sponsored assistance sustains these approaches. For instance, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) supported incident response capacity-building efforts in Africa [214], and CERT/CC transferred internet security knowledge to Cote d'Ivoire (Ivory Coast) computer security incident response (CSIRT) team [215].

During this research project, we realized that a database of lessons learned could benefit N-CSIRTs in low-income regions as they might have a repository of local experience, success stories, and good practices

APNIC Experience

Background:

APNIC (Asia Pacific Network Information Centre) is an open, member-based, not-for-profit organization, whose primary role is to distribute and manage Internet number resources (IP addresses and AS numbers) in the Asia Pacific region's 56 economies. These number resources are the building blocks for the Internet to operate and grow.

APNIC helps build essential technical skills across the region, supports Internet infrastructure development, produces insightful research, and is an active participant in the multi-stakeholder model of Internet cooperation and governance. APNIC performs these activities as part of its commitment to a global, open, stable and secure Internet that serves the entire Asia Pacific region.

Security at APNIC:

APNIC plays an important role in Internet infrastructure security by:

- Sharing global security best practice information with APNIC Members and building regional security capacity through training and technical assistance
- Supporting Members' efforts to maintain network security through resource certification and DNSSEC
- Supporting the creation of CERT/CSIRTs in the Asia Pacific to strengthen the community's ability to mitigate security incidents
- Coordinating with the Asia Pacific security community, including the law enforcement community, to enhance mutual understanding and share views from the numbers community.

APNIC's Experience of CERT/CSIRTs creation and capacity building in Asia Pacific Region

As part of its security initiatives, APNIC is supporting the creation of CSIRTs in the Asia Pacific region. The countries who benefitted from this initiative include Tonga, Samoa, Vanuatu and Papua New Guinea.

Two of the successful examples of Pacific Islands CERTs are Tonga and Vanuatu. The setup of the Kingdom of Tonga CERT was completed in 2016 with an objective to provide a safe and secure digital environment for the country and it citizens. The team aimed at conducting incident handling, performing vulnerability handling, and providing security consultation and advice at Tonga and greater Pacific. The cybersecurity grant, funded by Internet Society, assisted in the setting up of Tonga CERT's capacity and capability to undertake its mandated function. APNIC helped find opportunities for CERT Tonga Staff to partake in capacity building activities and chances to collaborate and form partnerships with relevant organizations.

CERT Tonga is now playing a vital role in the Tonga Police investigation process which has placed the CERT Tonga in a position to be actively planned to grow in all areas to be able to cope with the demand. There is a particular focus on building capacity of the team as it is now essential to the continuous operation of the CERT as well as obtaining a reliable information obtained from a verified source.

CERT Vanuatu (CERT VU) is the central cyber security information and incident response hub for Vanuatu and was setup with the support of APNIC and other stakeholders in June 2018. It serves with primary objectives to respond to malicious incidents penetrating Vanuatu's Internet and IP communications network. CERT VU is working alongside government agencies and other international and national partners to help Vanuatu to be more resilient to cyber-attacks. APNIC facilitated the desktop security exercises and strategic discussions for the CERT setup.

The setup of Pacific Islands CERT/CSIRTs is based on the fact that the government has realized the importance of such national institutions and started with the basic services with the support of APNIC and many other stakeholders. It is seen that these CERTs are expanding their services over time. As part of its operations these CERTs are using a combination of open source and commercial tools for incident handling and forensic investigation.

For capacity building and acquiring knowledge, freely available training platforms such as Udemy, Elastic Search and others are being used. Workshops and Conferences are the other ways for these CERTs to acquire capacity.

One of the interesting aspects of the mentoring support provided by APNIC to these national CERTs is pairing them with the developed CERTs of the region. Another notable point is the central management of gained knowledge by documenting the processes in appropriate forms such as Standard Operating Procedures. It is useful to train newcomers and helps when a key staff leaves the organization.

For upskilling their people, some CERTS in this region such as Samoa's National Computer Emergency Response Team (SAMCERT) which was set up in June 2019 is playing a key role in training their people by tying up with the academic institutions.

9. FUNDING AND SUPPORT THROUGH REGIONAL AND INTERNATIONAL COOPERATION

Although there is a need for innovative and affordable solutions to N-CSIRT capacity challenges, there are mechanisms to provide expensive training at low cost to individuals or groups. An array of international grants and reduced-cost training opportunities exist that developing countries can utilize. These solutions come from collaborations between ISACA, SANS, Cyber4Dev, NATO SPS, and a variety of ISAC's. In this part, we will give information about several of these initiatives and their achievements.

10. USING OPENSOURCE TOOLS.

CSIRTs are often considered cost centers; therefore, it is common that they face operational constraints such as lack of resources, low budgets, and staff shortages. Many teams seize the opportunity offered by open-source and free(ware) tools even if sometimes adjustments are required between funding vs time and skills to deploy the tools.

12. KNOWLEDGE BASE ARTICLE AND DOCUMENTATION.

Institutional memory is critical for CSIRTs especially when senior staff members leave the team. Many teams are avoiding the loss of lessons learned and institutional memory loss by setting up internal wikis and knowledge libraries. These resources empower team members to share knowledge, lessons learned and build a library of information.

13. MENTORING, UPSKILLING AND RESKILLING.

A company-wide mentoring program is an excellent way to bring together senior and junior team members. Mentoring programs bridge the knowledge gap between new team members and counterparts that are more experienced and increase engagement. The demand for continuous development of skilled workers has led some teams to recruit nontraditional cybersecurity engineers and train them with various mentoring programs, exercises and training plans.

14. TRAININGS, EXERCICES, DRILLS.

Teams defend and protect their organisations and countries the best when they are prepared. The 5 P's rule suggests that "proper planning prevents poor performance". Exercises are key to build relationship with stakeholders, confidence and trust, understand real adversary attacks and systems, and learn. Exercises should be regular and involve a range of participants from senior leadership, policy makers, to technical staff. Teams are using innovative ways including leveraging knowledge base of adversary tactics and techniques and frameworks to develop training and exercises.

International Telecommunication Union (ITU) Cyber Capacity Development

The cybersecurity programme offers ITU membership – particularly developing countries – the opportunity and tools to increase cybersecurity capabilities at the national level, in order to enhance security, build confidence and trust in the use of ICTs – making the digital realm more safe and secure for everyone. The ITU assists countries on the following:

Conducting Cyber Drills and Events

ITU assists in improving cybersecurity readiness, protection, and incident response capabilities of countries by conducting cyber drills at regional and national level. The ITU regional cyber drills are designed with a dual purpose: as a platform for cooperation, information sharing, and discussions on current cybersecurity issues, as well as to provide hands-on exercises for national Computer Incident Response Teams (CIRTs) / Computer Security Incident Response Teams (CSIRTs). This capacity development is provided to countries free of charge. ITU conduct different cybersecurity events throughout the year [216].

Development of National Cybersecurity Strategy

At the national level, cybersecurity is a shared responsibility which requires coordinated action for prevention, preparation, response, and incident recovery on the part of government authorities, the private sector and civil society. For this to operate smoothly and to ensure a safe, secure and resilient digital realm a comprehensive framework or strategy is necessary which has to be developed, implemented and executed in a multi-stakeholder approach. This framework is often referred to as National Cybersecurity Strategy (NCS) – and is a critical element for any country's socio-economic security. ITU presents members with a reference guide to help countries create an effective national cybersecurity framework. ITU offers a new free online training: Lifecycle, principles and good practices of national cybersecurity strategy development and implementation.

National CSIRT Establishment

ITU is working with Member States to build capacity at national and regional levels, deploy capabilities, and assist in establishing and enhancing National Computer Incident Response Teams (CIRTs). ITU has established or enhanced CISRTs in 14 countries.

Global Cybersecurity Index: The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue. This index helps countries to assess their cyber capacity.

Legislation

An integral component of any national Cybersecurity strategy is the adoption of appropriate legislation against the misuse of ICTs for criminal purposes – which is harmonized with regional and international policy and practices. To help ensure a safe, secure and equitable internet – and combat cybercrime – ITU is assisting Member States in implementing appropriate cybersecurity legislation and harmonizing the legal and policy framework. Over the years more than 80 countries from all regions of the world have benefited from such support.

Trainings: The Centres of Excellence (CoE) programme was launched by ITU at the turn of the millennium, with the aim to support capacity development in the field of information and communication technologies (ICTs) by offering continuous education to ICT professionals and executives in the public and private spheres through face-to-face, online or blended learning. The list of trainings includes cybersecurity foundations, Lifecycle, principles and good-practices on national cybersecurity strategy development and implementation, and CSIRT/SOC establishment and modernization [217].

Carnegie Mellon University – Software Engineering Institute (SEI) CERT Division

The CERT Division (formerly CERT/CC) of the Software Engineering Institute (SEI) has been significantly involved in the development and maturation of incident response capabilities around the globe. Over the last three decades, the SEI has produced numerous frameworks, courses, and resources for the creation, implementation, and development of computer security incident response teams (CSIRTs).

The CERT Division collaborates with the international incident response community, government stakeholders, private sector, academia, and relevant regional and international organizations to promote and advance the state of cybersecurity cooperation, build cybersecurity capacity, and promulgate security operations and incident response best practices.

The SEI supports the U.S. Vision for Cyberspace and Approach to Cyberspace Policy through the following activities:

- Implementing and improving upon sustainable incident response capabilities with teams around the world
- Enhancing state of the art techniques and practices in the cyber threat information sharing field and applying this knowledge in a regional setting in order to promote trust-based incident response communities
- Developing the global cybersecurity workforce through tailored capacity building.

Global Cybersecurity Capacity Building:

To improve effectiveness and increase capability, it is essential for national CSIRTs to build strong relationships with national CSIRTs in other countries and economies. Since all national CSIRTs operate in a unique space with constrained resources, each one benefits from sharing information, expertise, and capabilities, and from collaborating on tool development. In 2014 the SEI's CERT Division and the U.S. Department of State's Office of the Coordinator for Cyber Issues (S/CCI), in coordination with the Department of Homeland Security's Office of International Affairs, began developing and implementing global cybersecurity capacity building activities that support capability and capacity building for national-level CSIRTs [218].

Case of Côte d’Ivoire National Computer Security Incident Response Team (CI-CERT):

The Cote d'Ivoire (Ivory Coast) Computer Security Incident Response (CI-CERT) team reached out to the SEI through the U.S. Department of State Office of the Coordinator for Cyber Issues (S/CCI) to request a collaborative workshop to help Cote d'Ivoire address the threats of distributed denial-of-service (DDoS) attacks and botnets [215]. Through this engagement, SEI developed a set of training documents and guides that can help other CSIRTs in developing countries. In support of the objectives of CI-CERT and S/CCI, the SEI CERT Division sent a team to Abidjan, Côte d’Ivoire to conduct a five-day advanced incident-handling workshop. The purpose of the workshop was to expose CI-CERT analysts to needed skills in the areas of artifact analysis, log analysis, and vulnerability handling, all of which are needed to address advanced incidents such as distributed denial of service attacks and rootkits. SEI personnel lectured on a variety of incident- handling topics and practical exercises that gave participants an opportunity to practice skills learned in the lectures. In addition to CI-CERT staff, participants included representatives of the Telecommunications and ICT Regulatory Authority of Côte d’Ivoire (ARTCI). Incident handlers from Cote d‘Ivorian telecommunications companies also participated. ARTCI provided translation services for both students and instructors [219].

REN-ISAC and SANS Education Partnership

Summary:

The partnership draws on the mission to ensure that information security practitioners in organizations, including N-CSIRTs, have the skills to protect national security and enhance cybersecurity readiness and response. The program offers security awareness and online technical training to qualifying educational institutions at a significant cost saving.

Partnership:

Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) and SANS Institute

Scope of Training:

Enables all higher education and K-12 organizations in the US and Canada to purchase essential security training at over 50% reduction in cost.

Training Offerings: There are three training options through SANS Online Training, NetWars Continuous, and Security Awareness Training.

- SANS Online Training – Offers the same content, instructors, and results as live courses with the flexibility for information security professionals to learn anytime and anywhere. These courses have hands-on labs and access to subject-matter experts to assist in challenging concepts or questions. Some of the course or certification offerings include cyber defense, management, penetration testing, industrial control systems, incident response and threat hunting, and application security.
- NetWars – An online challenge that is a four-month experimental program with real-world scenarios that test hands-on skills in vulnerability assessments, incident response, system hardening, packet analysis, malware analysis, penetration testing, digital forensics, and intrusion detection.
- SANS Security Awareness – A comprehensive technical solution for end-users and individuals at all levels to adopt security awareness training and understanding compliance. Several products in this solution include end user, healthcare, developer, engineer, and phishing.

Timeline: Twice a year (June 1 – July 31 and December 1 – January 31), your organization can purchase SANS training credits that provide access to over 30 online courses.

IT-ISAC and ISACA Strategic Partnership

Summary:

The partnership seeks to provide additional cybersecurity leadership to ISACA members and expand offerings to technology professionals. Through this partnership, IT-ISAC and ISACA will offer members additional discounts, educational offerings, events and create a research and leadership collaboration.

Partnership:

The Information Technology - Information Sharing and Analysis Center (IT-ISAC) and ISACA

Scope of Training:

Additional discounts and educational offerings on all ISACA certification, certificate, and training courses.

Training Offerings: There are multiple training and certification options through ISACA for members, including:

- Certifications – ISACA's certifications include CISA, CRISC, CISM, CGEIT, CSX-P, CDPSE, ITCA, CET.
- Certificates – COBIT, IT Risk Fundamentals, Cloud Auditing Knowledge, CSX Nexus Cybersecurity, Cybersecurity Audit, Computing Fundamentals, Networks and Infrastructure, Cybersecurity, Software Development, Data Science, Cloud, Blockchain, IoT, AI.
- Trainings – A comprehensive list of ISACA trainings exists catered to improving a variety of technical skills like audit and assurance, emerging technology, governance, information security, information technology, privacy, and risk in in-person or online formats.

EU Cyber Resilience for Development (Cyber4Dev) Program

Summary:

The Cyber4D program central purpose is to (1) strengthen cybersecurity policy coordination through the sharing of knowledge and awareness, (2) capacity building of cyber incident response teams, and (3) program management and engagement training.

Partners:

Northern Ireland Co-operation Overseas (NI-CO) in partnership with the Foreign, Commonwealth, and Development Office (FCDO) in the UK, the Estonian Information System Authority (RIA), and the Netherlands Ministry of Foreign Affairs (MFA)

Funding: EU's Instrument to Stability and Peace (IcSP) for €11 million

Scope of Training:

Provides a wide range of technical assistance, capacity building, collaborative and information sharing activities through series of workshops, conferences, working groups, on-the-job training, and mentoring. Free training opportunities include fundamental offerings underpinning the delivery of National Cybersecurity strategies and the development of effective and robust Cybersecurity Incident Response Team (CSIRT) capabilities. The courses include technical content as well as management and policy tools necessary for the effective and efficient management of cybersecurity resources. The partners support the development of increased cyber resilience in partner countries based on sharing knowledge, skills, and learning and policy development.

Training Offerings:

There are several training options, including review, assessment, and analysis; workshops/roundtables/table-top exercises/seminars/conferences; working groups; training courses; on-the-job training including skills transfer and mentoring; and study visits. Some of the available trainings are basic and advanced CSIRT technical training, advanced CSIRT management training, exploit defense, secure logging, ethical hacking, advanced networking, advanced scripting, securing industrial control systems (ICS/SCADA).

Timeline: Start in March 2018 which a 42-month duration

Program Achievements: From 2018- 2021, the program has engaged nine priority countries, 15 associate countries, 327 public institutions, and 229 private sector organizations. Over 5,000 people have been trained by Cyber4Dev experts, 153 training courses delivered, and 250 activities delivered.

NATO Science for Peace and Security Program

Summary:

The program promotes collaborations and conversations between NATO member states and partner countries through research, innovation, and information sharing. The SPS program offers funding, expert advice, and support to aid and improve security offerings and maturity aligned with NATO's strategic objectives, including cyber defense.

Source of Funding: NATO Science for Peace and Security Program (SPS)

Partnerships: NATO Countries and Partners (i.e., Azerbaijan, Armenia, Belarus, Bosnia and Herzegovina, Colombia, Egypt, Georgia, Iraq, Jordan, Kazakhstan, Kyrgyz Republic, Mauritania, Moldova, Mongolia, Morocco, Pakistan, Serbia, Tajikistan, Tunisia, Turkmenistan, Ukraine, Uzbekistan)

Key Priorities: Facilitate mutually beneficial cooperation on issues of common interest, including international efforts to meet emerging security challenges such as cyber defense, which includes critical infrastructure protection, including sharing of best practices, capacity building and policies; support in developing cyber defense capabilities, including new technologies and support to the construction of information technology infrastructure; cyber defense situation awareness.

Grant Options: SPS supports cooperation by providing funding for Multi-Year Projects and Events.

- **Multi-Year Projects** –Research and Development (R&D) projects that enable NATO and its partner nations to collaborate on applied research and capacity building that results in new civil science advancements with practical application in the security and defense fields. The typical duration of such projects usually lasts 24-36 months. The budget is €150,000-350,000 for the duration of the project. Under this category, NATO funded several developing nations' computer emergency response teams and national cyber strategy creation efforts by providing tools and infrastructure.
- **Event | Advanced Research Workshops** – Advanced-level discussions that provide a platform for different countries to share their experiences and knowledge on security-related topics to address current security challenges. The typical duration is 2-5 working days. Budget is around €40,000.
- **Event | Advanced Study Institutes** – High-level tutorial courses about the latest developments in relevant topics for NATO and the SPS Key Priorities to an advanced-level audience. The typical duration is 7-10 working days. Budget is EUR $60,000.
- **Event | Advanced Training Course**s – Tailor-made, flexible, interactive courses to enable specialists in NATO countries to share their security-related expertise in one of the SPS Key Priority areas. The typical duration is 5-7 working days. Budget is EUR $60,000. The courses include cybersecurity awareness, pre-emptive security strategies, digital forensics, and threat identification and response.

Completed Projects: The completed NATO-funded projects include cyber incident response capability establishment in the Republic of Moldova [220], cyber defense trainings for Azerbaijan [221], support for implementing a cybersecurity strategy for Jordan, and enhancing Jordan's established Computer Emergency Response Teams (CERT) [222], and developing a cyber threat forecast using big data for Morocco [223].

REFERENCES

[1] J. Haller, S. A. Merrell, M. J. Butkovic, and B. J. Willke, “Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability,” Carnegie-Mellon University Software Engineering Institute, Pittsburgh, PA, Jun. 2010. Accessed: Sep. 12, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA536721

[2] Forum of Incident Response and Security Teams, Inc., “Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1,” FIRST, Nov. 2019. [Online]. Available: https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf

[3] The MITRE Corporation, “MITRE ATT&CK®.” https://attack.mitre.org/ (accessed Sep. 13, 2021).

[4] N. Pachis, “An approach to the ultimate in-depth security event management framework,” SANS Institute, Jun. 2008. Accessed: Sep. 13, 2021. [Online]. Available: https://www.sans.org/white-papers/32819/

[5] K. Kent and M. P. Souppaya, “Guide to computer security log management,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-92, 2006. doi: 10.6028/NIST.SP.800-92.

[6] J. Novak, B. A. Manley, D. Mcintire, S. Mudd, A. L. Hueca, and T. A. Bills, “The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities,” CMU/SEI-2021-TR-002, Jun. 2021. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_734796.pdf

[7] “Splunk: The Data-to-Everything Platform,” *Splunk*. https://www.splunk.com (accessed Sep. 13, 2021).

[8] “OSSIM: The Open Source SIEM | AlienVault,” *AT&T*. https://cybersecurity.att.com/products/ossim (accessed Sep. 13, 2021).

[9] “Apache Metron Big Data Security.” http://metron.apache.org/ (accessed Sep. 13, 2021).

[10] “The Open Source Security Platform,” *Wazuh*. https://wazuh.com/ (accessed Sep. 13, 2021).

[11] “Security monitoring software | The European SIEM,” *Prelude SIEM*. https://preludesiemdev.wpengine.com/en/ (accessed Sep. 13, 2021).

[12] “Security Information and Event Management (SIEM),” *LogRhythm*. https://logrhythm.com/solutions/security/siem/ (accessed Sep. 13, 2021).

[13] CyberRes, “ArcSight Enterprise Security Manager.” https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm (accessed Sep. 13, 2021).

[14] “SolarWinds Security Event Manager.” https://www.solarwinds.com/security-event-manager (accessed Sep. 13, 2021).

[15] AT&T Cybersecurity, “SIEM Software & Service Solutions.” https://cybersecurity.att.com/solutions/siem-platform-solutions (accessed Sep. 13, 2021).

[16] “Exabeam Fusion - A Modern SIEM Solution,” *Exabeam*. http://https%253A%252F%252Fwww.exabeam.com%252Fproduct%252F (accessed Sep. 13, 2021).

[17] “Rapid7 Cloud SIEM Solution,” *Rapid7*. https://www.rapid7.com/solutions/siem/ (accessed Sep. 13, 2021).

[18] “McAfee Security Information and Event Management (SIEM).” https://www.mcafee.com/enterprise/en-us/products/siem-products.html (accessed Sep. 13, 2021).

[19] “IBM QRadar SIEM,” Jul. 29, 2021. https://www.ibm.com/products/qradar-siem (accessed Sep. 13, 2021).

[20] “Securonix - Next-Gen Security Information and Event Management (SIEM),” *Securonix*. https://www.securonix.com/products/next-generation-siem/ (accessed Sep. 13, 2021).

[21] “RSA NetWitness® Platform Redefines SIEM to Optimize Security Operations,” *RSA.com*. https://www.rsa.com/en-us/company/news/rsa-netwitness-platform-redefines-siem-to-optimize-security (accessed Sep. 13, 2021).

[22] “FortiSIEM Solutions,” *Fortinet*. https://www.fortinet.com/products/siem/fortisiem?utm_source=google&utm_medium=paid-search&utm_campaign=fortisiem&gclid=CjwKCAjw7fuJBhBdEiwA2lLMYbQz5y_fLtSJVGa8u3B9XTRQxHKoU8H7TLDH2Z70qY4bRGbP_cNsdxoCN7AQAvD_BwE (accessed Sep. 13, 2021).

[23] “FireEye SIEM Security Solution,” *FireEye*. https://www.fireeye.com/products/helix/siem.html (accessed Sep. 13, 2021).

[24] “The Zeek Network Security Monitor,” *Zeek*. https://zeek.org/ (accessed Sep. 13, 2021).

[25] “Suricata,” *Suricata*. https://suricata.io/ (accessed Sep. 13, 2021).

[26] “Snort - Network Intrusion Detection & Prevention System.” https://www.snort.org/ (accessed Sep. 13, 2021).

[27] “Wireshark.” https://www.wireshark.org/ (accessed Sep. 13, 2021).

[28] “NfSen- Netflow Sensor.” http://nfsen.sourceforge.net/ (accessed Sep. 13, 2021).

[29] “OSSEC - Server Intrusion Detection for Every Platform,” *OSSEC*. https://www.ossec.net/ (accessed Sep. 13, 2021).

[30] “Elastic - ELK Stack: Elasticsearch, Logstash, Kibana.” https://www.elastic.co/what-is/elk-stack (accessed Sep. 13, 2021).

[31] “Cuckoo Sandbox - Automated Malware Analysis.” https://cuckoosandbox.org/ (accessed Sep. 13, 2021).

[32] “VirusTotal.” https://www.virustotal.com/gui/home/upload (accessed Sep. 13, 2021).

[33] “CIRCL - Dynamic Malware Analysis Platform.” https://www.circl.lu/services/dynamic-malware-analysis/ (accessed Sep. 13, 2021).

[34] “VirusTotal/yara,” Sep. 13, 2021. https://github.com/VirusTotal/yara (accessed Sep. 13, 2021).

[35] “REMnux: A Linux Toolkit for Malware Analysis.” https://remnux.org/ (accessed Sep. 13, 2021).

[36] “The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools.” https://www.sleuthkit.org/index.php (accessed Sep. 13, 2021).

[37] Volatility Foundation, “Volatility,” Sep. 14, 2021. https://github.com/volatilityfoundation/volatility (accessed Sep. 13, 2021).

[38] “CSIRT Assistance Program,” *Team Cymru*, Apr. 07, 2020. https://team-cymru.com/community-services/csirt-ap/ (accessed Sep. 13, 2021).

[39] The Shadowserver Foundation, “Celebrating Milestones (European CERT/CSIRT Report Coverage),” Feb. 23, 2020. https://www.shadowserver.org/news/celebrating-milestones-european-cert-csirt-report-coverage/ (accessed Sep. 13, 2021).

[40] “MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing.” https://www.misp-project.org/ (accessed Sep. 13, 2021).

[41] “IntelMQ,” Sep. 11, 2021. https://github.com/certtools/intelmq (accessed Sep. 13, 2021).

[42] “OpenCTI - Open platform for cyber threat intelligence,” *OpenCTI - Open platform for cyber threat intelligence*. https://www.opencti.io/en/ (accessed Sep. 13, 2021).

[43] “CERT Polska - n6,” Sep. 03, 2021. https://github.com/CERT-Polska/n6 (accessed Sep. 13, 2021).

[44] “Zone-H.org - Unrestricted information.” http://www.zone-h.org/?hz=1 (accessed Sep. 13, 2021).

[45] “PhishTank | Join the fight against phishing.” https://www.phishtank.com/index.php (accessed Sep. 13, 2021).

[46] “Malware Domain List.” https://www.malwaredomainlist.com/mdl.php

[47] “Mine, Merge, Map data with Maltego.” https://www.maltego.com/product-features/ (accessed Sep. 13, 2021).

[48] FireEye, “ThreatPursuit-VM,” Sep. 14, 2021. https://github.com/fireeye/ThreatPursuit-VM (accessed Sep. 13, 2021).

[49] “Shodan - Search Engine for the Internet of Everything,” *Shodan*. https://www.shodan.io (accessed Sep. 13, 2021).

[50] “CyberGreen - Cyber Health Statistics.” https://stats.cybergreen.net/ (accessed Sep. 13, 2021).

[51] M. Dodson, A. R. Beresford, and M. Vingaard, “Using Global Honeypot Networks to Detect Targeted ICS Attacks,” in *2020 12th International Conference on Cyber Conflict (CyCon)*, May 2020, vol. 1300, pp. 275–291. doi: 10.23919/CyCon49761.2020.9131734.

[52] “The Honeynet Project – Honeypot research.” https://www.honeynet.org/ (accessed Sep. 14, 2021).

[53] DinoTools, “Dionaea Honeypot,” Sep. 13, 2021. https://github.com/DinoTools/dionaea (accessed Sep. 14, 2021).

[54] “Cowrie,” Sep. 13, 2021. https://github.com/cowrie/cowrie (accessed Sep. 14, 2021).

[55] Ö. Erdem, “HoneyThing,” Sep. 01, 2021. https://github.com/omererdem/honeything (accessed Sep. 14, 2021).

[56] “Conpot - ICS/SCADA Honeypot.” http://conpot.org/ (accessed Sep. 14, 2021).

[57] “Thug,” *Thug*. https://buffer.github.io/thug/ (accessed Sep. 14, 2021).

[58] “Introduction into T-Pot: A Multi-Honeypot Platform,” *Telekom Security*, Mar. 17, 2015. https://github.security.telekom.com/2015/03/honeypot-tpot-concept.html (accessed Sep. 14, 2021).

[59] H. Bahsi, “Analysis of National Cyber Situational Awareness Practices,” in *Strategic Cyber Defense: A Multidisciplinary Perspective*, vol. 48, IOS Press, 2017, pp. 31–41.

[60] “EINSTEIN,” *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/einstein (accessed Sep. 14, 2021).

[61] “TSUBAME Working Group,” *Asia Pacific Computer Emergency Response Team (APCERT)*. http://www.apcert.org/about/structure/tsubame-wg/index.html (accessed Sep. 14, 2021).

[62] “GIAC Incident Handler Certification | Cybersecurity Certification,” *GIAC*. https://www.giac.org/certification/certified-incident-handler-gcih?msc=giac-focus-area (accessed Sep. 14, 2021).

[63] SANS Institute, “Cyber Threat Intelligence Training | SANS FOR578.” https://www.sans.org/cyber-security-courses/cyber-threat-intelligence/ (accessed Sep. 14, 2021).

[64] SANS Institute, “Open-Source Intelligence (OSINT) Gathering Training | SANS SEC487.” https://www.sans.org/cyber-security-courses/open-source-intelligence-gathering/ (accessed Sep. 14, 2021).

[65] SANS Institute, “Network Intrusion Detection | SANS SEC503 | Intrusion Detection Training.” https://www.sans.org/cyber-security-courses/intrusion-detection-in-depth/ (accessed Sep. 14, 2021).

[66] SANS Institute, “SIEM Training | SIEM with Tactical Analysis | SANS SEC555.” https://www.sans.org/cyber-security-courses/siem-with-tactical-analytics/ (accessed Sep. 14, 2021).

[67] Asia Pacific Computer Emergency Response Team, “SIEM Admin - Incident Handing Training - SOC Team,” *Udemy*. https://www.udemy.com/course/siem-administration-training-arcsight-splunk-qradar-nitro-rsa/ (accessed Sep. 14, 2021).

[68] “Certified Incident Handling Engineer (CIHE),” *Udemy*. https://www.udemy.com/course/certified-incident-handling-engineer-cihe/ (accessed Sep. 14, 2021).

[69] “Security Operations Center | Certified SOC Analyst | CSA,” *EC-Council*. https://www.eccouncil.org/programs/certified-soc-analyst-csa/ (accessed Sep. 14, 2021).

[70] “IBM Professional Certification Program - IBM Certified SOC Analyst - IBM QRadar SIEM V7.3.2,” *IBM*. https://www.ibm.com/certify/www.ibm.com/certify/cert (accessed Sep. 14, 2021).

[71] European Union Agency for Network and Information Security, “Orchestration of CSIRT Tools Student Toolset - Analyst Modules,” Dec. 2019. [Online]. Available: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/orchestration-of-csirt-tools-1/orchestration-of-csirt-tools-tools-analyst.pdf

[72] “Trainings,” *FIRST — Forum of Incident Response and Security Teams*. https://www.first.org/education/trainings (accessed Sep. 14, 2021).

[73] “MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing - Training Materials,” *CIRCL*. https://www.circl.lu/services/misp-training-materials/ (accessed Sep. 14, 2021).

[74] CERT-Tools, “IntelMQ Tutorial,” Aug. 18, 2021. https://github.com/certtools/intelmq-tutorial (accessed Sep. 14, 2021).

[75] "Technical Engagement Training Course Catalogue," *ICANN*. https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en#dns-abuse-threats-mitigation (accessed Sep. 14, 2021).

[76] "Assurance in Information Security," *CREST*. https://www.crest-approved.org/ (accessed Sep. 14, 2021).

[77] M. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek, "Handbook for Computer Security Incident Response Teams (CSIRTs)," Carnegie-Mellon University Software Engineering Institute, CMU/SEI-2003-HB-002, Apr. 2003. Accessed: Sep. 12, 2021. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

[78] N. Brownlee and E. Guttman, "Expectations for Computer Security Incident Response." 1998. [Online]. Available: https://www.hjp.at/doc/rfc/rfc2350.html

[79] CERT-EE and Estonian National CERT, "RFC 2350 Description for CERT-EE." Feb. 04, 2020. [Online]. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/rfc_2350_description_for_cert.pdf

[80] H. Bronk, M. Thorbruegge, and M. Hakkaja, "A Step-by-Step Approach on How to set up a CSIRT." ENISA, Dec. 22, 2006. Accessed: Sep. 14, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/csirt-setting-up-guide/view/++widget++form.widgets.fullReport/@@download/CSIRT_setting_up_guide_ENISA.pdf

[81] "EthicsfIRST: Ethics for Incident Response and Security Teams," *FIRST — Forum of Incident Response and Security Teams*. https://www.first.org/global/sigs/ethics/ethics-first (accessed Sep. 12, 2021).

[82] D. Stikvoort, "SIM3 : Security Incident Management Maturity Model." May 01, 2019. Accessed: Sep. 14, 2021. [Online]. Available: http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf

[83] European Union Agency for Network and Information Security, "ENISA Maturity Evaluation Methodology for CSIRTs," ENISA, Apr. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[84] A. Dorofee *et al.*, "Incident Management Capability Assessment," Carnegie-Mellon University Software Engineering Institute, CMU/SEI-2018-TR-007, Dec. 2018. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=538848

[85] Forum of Incident Response and Security Teams, Inc., "Product Security Incident Response Team (PSIRT) Services Framework Version 1.1," FIRST, 2020. [Online]. Available: https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf

[86] International Standards Organization, "ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management," 2016. Accessed: Sep. 13, 2021. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/08/60803.html

[87] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology," National Institute of Standards and Technology, NIST SP 800-61r2, Aug. 2012. doi: 10.6028/NIST.SP.800-61r2.

[88] R. de J. Martins, L. A. D. Knob, E. G. da Silva, J. A. Wickboldt, A. Schaeffer-Filho, and L. Z. Granville, "Specialized CSIRT for Incident Response Management in Smart Grids," *J. Netw. Syst. Manag.*, vol. 27, no. 1, pp. 269–285, Jan. 2019, doi: 10.1007/s10922-018-9458-z.

[89] D. Stikvoort, "Incident Classification/Incident Taxonomy according to eCSIRT.net – adapted." 2015. [Online]. Available: https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

[90] European Union Agency for Network and Information Security, "Reference Incident Classification Taxonomy," ENISA, Report/Study, Jan. 2018. Accessed: Sep. 13, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

[91] Europol, "Common Taxonomy for Law Enforcement and The National Network of CSIRTs Version 1.3," Europol European Cybercrime Center, 2017. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf

[92] Trusted Introducer, "Traffic Light Protocol (TLP) — Version 1.0," FIRST. [Online]. Available: https://www.trusted-introducer.org/ISTLP.pdf

[93] "RT for Incident Response," *Best Practical Solutions*. https://bestpractical.com/rtir (accessed Sep. 14, 2021).

[94] "TheHive Project." https://www.thehive-project.org (accessed Sep. 14, 2021).

[95] "Cortex Docs." TheHive Project, Sep. 09, 2021. Accessed: Sep. 14, 2021. [Online]. Available: https://github.com/TheHive-Project/CortexDocs

[96] "osTicket - Support Ticketing System." https://osticket.com/ (accessed Sep. 14, 2021).

[97] "Cyber Threat Intelligence Technical Committee," *Oasis*. https://oasis-open.github.io/cti-documentation/ (accessed Sep. 14, 2021).

[98] "CACAO Security Playbooks Version 1.0," *Oasis*. https://docs.oasis-open.org/cacao/security-playbooks/v1.0/security-playbooks-v1.0.html (accessed Sep. 14, 2021).

[99] "IDA Freeware," *Hex Rays*. https://hex-rays.com/ida-free/ (accessed Sep. 14, 2021).

[100] "Production-Grade Container Orchestration," *Kubernetes*. https://kubernetes.io/ (accessed Sep. 14, 2021).

[101] "Helm." https://helm.sh/ (accessed Sep. 14, 2021).

[102] "CERT Incident Response Process Professional Certificate." https://www.sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=15102 (accessed Sep. 14, 2021).

[103] "Certified Computer Security Incident Handler (CERT-CSIH)," *Infosec Institute*. https://www.infosecinstitute.com/skills/learning-paths/cert-csih/ (accessed Sep. 14, 2021).

[104] "EC-Council Certified Incident Handler | CERT." https://cert.eccouncil.org/ec-council-certified-incident-handler.html (accessed Sep. 14, 2021).

[105] "Cyber Security Incident Handling and Response," *Udemy*. https://www.udemy.com/course/cyber-security-incident-handling-and-response/ (accessed Sep. 14, 2021).

[106] "Foundations of Incident Management," *Carnigie Mellon University Software Engineering Institute*. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P139 (accessed Sep. 14, 2021).

[107] "Advanced Topics in Incident Handling," *Carnigie Mellon University Software Engineering Institute*. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P23B (accessed Sep. 14, 2021).

[108] "Creating a Computer Security Incident Response Team," *Carnigie Mellon University Software Engineering Institute*. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P25 (accessed Sep. 14, 2021).

[109] "Managing Computer Security Incident Response Teams," *Carnigie Mellon University Software Engineering Institute*. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P28 (accessed Sep. 14, 2021).

[110] SANS Institute, "Advanced Incident Response Training | Threat Hunting & Digital Forensics Course | SANS FOR508." https://www.sans.org/cyber-security-courses/advanced-incident-response-threat-hunting-training/ (accessed Sep. 14, 2021).

[111] SANS Institute, "Cybersecurity Law Training | Data Security Investigations | LEG523." https://www.sans.org/cyber-security-courses/cybersecurity-law-data-security/ (accessed Sep. 14, 2021).

[112] SANS Institute, "Introduction to Malware Analysis: Hands-on and Technical | SANS FOR601A." https://www.sans.org/cyber-security-courses/introduction-malware-analysis/ (accessed Sep. 14, 2021).

[113] SANS Institute, "Reverse Engineering Malware Training | Malware Tools & Techniques | SANS FOR610." https://www.sans.org/cyber-security-courses/reverse-engineering-malware-malware-analysis-tools-techniques/ (accessed Sep. 14, 2021).

[114] Forum of Incident Response and Security Teams, Inc, "Incident Response for Policymakers," *FIRST*. https://www.first.org/events/training/tallinn2019 (accessed Sep. 14, 2021).

[115] International Standards Organization, "ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure," 2018. Accessed: Sep. 14, 2021. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/23/72311.html

[116] National Cyber Security Centre, "Coordinated Vulnerability Disclosure: the Guideline," Ministry of Justice and Security, publicatie, Oct. 2018. Accessed: Sep. 12, 2021. [Online]. Available: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

[117] The MITRE Corporation, "CVE." https://cve.mitre.org/ (accessed Sep. 14, 2021).

[118] The MITRE Corporation, "CWE - Common Weakness Enumeration." https://cwe.mitre.org/ (accessed Sep. 14, 2021).

[119] The MITRE Corporation, "CWE - 2021 CWE Top 25 Most Dangerous Software Weaknesses." https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html (accessed Sep. 14, 2021).

[120] The MITRE Corporation, "CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC^{TM})." https://capec.mitre.org/ (accessed Sep. 14, 2021).

[121] "Document Library - Verify PCI Compliance, Download Data Security and Credit Card Security Standards," *Official PCI Security Standards Council Site*. https://www.pcisecuritystandards.org/document_library (accessed Sep. 14, 2021).

[122] "The Penetration Testing Execution Standard," *PTES*. http://www.pentest-standard.org/index.php/Main_Page (accessed Sep. 14, 2021).

[123] K. A. Scarfone, M. P. Souppaya, A. Cody, and A. D. Orebaugh, "Technical guide to information security testing and assessment.," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-115, 2008. doi: 10.6028/NIST.SP.800-115.

[124] P. Herzog, "The Open Source Security Testing Methodology Manual (OSSTMM 3)." Institute for Security and Open Methodologies (ISECOM). [Online]. Available: https://www.isecom.org/OSSTMM.3.pdf

[125] Open Web Application Security Project, "OWASP Web Security Testing Guide," *OWASP*. https://owasp.org/www-project-web-security-testing-guide/ (accessed Sep. 14, 2021).

[126] Open Web Application Security Project, "OWASP Mobile Security Testing Guide," *OWASP*. https://owasp.org/www-project-mobile-security-testing-guide/ (accessed Sep. 14, 2021).

[127] Open Web Application Security Project, "OWASP Top Ten Web Application Security Risks," *OWASP*. https://owasp.org/www-project-top-ten/ (accessed Sep. 14, 2021).

[128] Open Web Application Security Project, "OWASP Vulnerability Management Guide (OVMG)." OWASP, Jun. 01, 2020. [Online]. Available: https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jul23-2020.pdf

[129] "Center for Internet Security," *CIS*. https://www.cisecurity.org/ (accessed Sep. 14, 2021).

[130] "OpenCVE." https://www.opencve.io/welcome (accessed Sep. 14, 2021).

[131] "OpenVAS - Open Vulnerability Assessment Scanner." https://www.openvas.org/ (accessed Sep. 14, 2021).

[132] "Nessus Product Family," *Tenable®*, May 14, 2019. https://www.tenable.com/products/nessus (accessed Sep. 14, 2021).

[133] "Information Security and Compliance | Qualys, Inc." https://www.qualys.com/ (accessed Sep. 14, 2021).

[134] "VulnIQ - Vulnerability intelligence and management solution." https://www.vulniq.com/security-scanner (accessed Sep. 14, 2021).

[135] "Nikto2 | CIRT.net." https://cirt.net/Nikto2 (accessed Sep. 14, 2021).

[136] "Burp Suite - Application Security Testing Software." https://portswigger.net/burp (accessed Sep. 14, 2021).

[137] "Acunetix | Web Application Security Scanner." https://www.acunetix.com/ (accessed Sep. 14, 2021).

[138] "Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution," *Kali Linux*. https://www.kali.org/ (accessed Sep. 14, 2021).

[139] "Metasploit | Penetration Testing Software, Pen Testing Security," *Metasploit*. https://www.metasploit.com/ (accessed Sep. 14, 2021).

[140] “BeEF - The Browser Exploitation Framework Project.” https://beefproject.com/ (accessed Sep. 14, 2021).

[141] “RIPS - free PHP security scanner using static code analysis.” http://rips-scanner.sourceforge.net/ (accessed Sep. 14, 2021).

[142] “The ZAP Homepage.” https://www.zaproxy.org/ (accessed Sep. 14, 2021).

[143] “sqlmap: automatic SQL injection and database takeover tool.” https://sqlmap.org/ (accessed Sep. 14, 2021).

[144] “w3af - Open Source Web Application Security Scanner.” http://w3af.org/ (accessed Sep. 14, 2021).

[145] “Mobile Security Framework (MobSF),” Sep. 14, 2021. https://github.com/MobSF/Mobile-Security-Framework-MobSF (accessed Sep. 14, 2021).

[146] “SonarQube 8.9 LTS - Long Term Support | SonarQube.” https://www.sonarqube.org/sonarqube-8-9-lts/ (accessed Sep. 14, 2021).

[147] “Penetration Testing with Kali Linux (PWK) | Offensive Security.” https://www.offensive-security.com/pwk-oscp/ (accessed Sep. 14, 2021).

[148] CREST, “CREST Registered Penetration Tester.” https://www.crest-approved.org/examination/registered-tester/index.html (accessed Sep. 14, 2021).

[149] CREST, “CREST Certified Web Application Tester.” https://www.crest-approved.org/examination/certified-web-application-tester/index.html (accessed Sep. 14, 2021).

[150] “CompTIA PenTest+ Certification | CompTIA IT Certifications,” *Default*. https://www.comptia.org/faq/pentest/what-is-comptia-pentest-certification (accessed Sep. 14, 2021).

[151] “GIAC Penetration Tester Certification | Cybersecurity Certification.” https://www.giac.org/certification/penetration-tester-gpen (accessed Sep. 14, 2021).

[152] “GIAC Web Application Penetration Tester | Cybersecurity Certification.” https://www.giac.org/certification/web-application-penetration-tester-gwapt (accessed Sep. 14, 2021).

[153] “GIAC Enterprise Vulnerability Assessor Certification | Cybersecurity Certification.” https://www.giac.org/certification/enterprise-vulnerability-assessor-geva (accessed Sep. 14, 2021).

[154] “GIAC Mobile Device Security Analyst | Cybersecurity Certification.” https://www.giac.org/certification/mobile-device-security-analyst-gmob (accessed Sep. 14, 2021).

[155] “GIAC Exploit Researcher and Advanced Penetration Tester Certification | Cybersecurity Certification.” https://www.giac.org/certification/exploit-researcher-advanced-penetration-tester-gxpn (accessed Sep. 14, 2021).

[156] “GIAC Cloud Penetration Tester Certification | Cybersecurity Certification.” https://www.giac.org/certification/cloud-penetration-tester-gcpn (accessed Sep. 14, 2021).

[157] “Certified Penetration Testing Professional | CPENT,” *EC-Council*. https://www.eccouncil.org/programs/certified-penetration-testing-professional-cpent/ (accessed Sep. 14, 2021).

[158] "Licensed Penetration Tester (Master) | LPT (Master) | CPENT | EC-Council." https://www.eccouncil.org/programs/licensed-penetration-tester-lpt-master/ (accessed Sep. 14, 2021).

[159] "Certified Ethical Hacker | CEH Certification | CEH v11," *EC-Council*. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (accessed Sep. 14, 2021).

[160] "Web Hacking: Become a Professional Web Pentester," *Udemy*. https://www.udemy.com/course/webhacking/ (accessed Sep. 14, 2021).

[161] "Evasion Techniques and Breaching Defenses (PEN-300) | Offensive Security." https://www.offensive-security.com/pen300-osep/ (accessed Sep. 14, 2021).

[162] SANS Institute, "Advanced Penetration Testing Training | Exploit Writing | SANS SEC660." https://www.sans.org/cyber-security-courses/advanced-penetration-testing-exploits-ethical-hacking/ (accessed Sep. 14, 2021).

[163] SANS Institute, "Network Penetration Testing & Ethical Hacking Course | SEC560." https://www.sans.org/cyber-security-courses/network-penetration-testing-ethical-hacking/ (accessed Sep. 14, 2021).

[164] SANS Institute, "Web Application Penetration Testing Training | SANS SEC542." https://www.sans.org/cyber-security-courses/web-app-penetration-testing-ethical-hacking/ (accessed Sep. 14, 2021).

[165] SANS Institute, "Advanced Web Application Penetration Testing and Exploitation | SANS SEC642." https://www.sans.org/cyber-security-courses/advanced-web-app-penetration-testing-ethical-hacking/ (accessed Sep. 14, 2021).

[166] SANS Institute, "Advanced Exploit Development for Pen Testers | SANS SEC760." https://www.sans.org/cyber-security-courses/advanced-exploit-development-penetration-testers/ (accessed Sep. 14, 2021).

[167] SANS Institute, "Mobile Device Security and Ethical Hacking Training | SANS SEC575." https://www.sans.org/cyber-security-courses/mobile-device-security-ethical-hacking/ (accessed Sep. 14, 2021).

[168] SANS Institute, "Cloud Penetration Testing Course | SANS SEC588." https://www.sans.org/cyber-security-courses/cloud-penetration-testing/ (accessed Sep. 14, 2021).

[169] SANS Institute, "Learn IoT Penetration Testing | SANS SEC556." https://www.sans.org/cyber-security-courses/iot-penetration-testing/ (accessed Sep. 14, 2021).

[170] SANS Institute, "ARM Exploit Development | SANS SEC661." https://www.sans.org/cyber-security-courses/arm-exploit-development/ (accessed Sep. 14, 2021).

[171] "CERT NetSA Security Suite." https://tools.netsa.cert.org/ (accessed Sep. 14, 2021).

[172] SANS Institute, "Information Security Policy Templates." https://www.sans.org/information-security-policy/?msc=main-nav (accessed Sep. 17, 2021).

[173] M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-50, 2003. doi: 10.6028/NIST.SP.800-50.

[174] M. Wilson, D. E. de Zafra, S. I. Pitcher, J. D. Tressler, and J. B. Ippolito, “Information technology security training requirements :: a role- and performance-based model,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-16, 1998. doi: 10.6028/NIST.SP.800-16.

[175] T. Grance, T. Nolan, K. Burke, R. Dudley, G. White, and T. Good, “Guide to test, training, and exercise programs for IT plans and capabilities,” National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-84, 2006. doi: 10.6028/NIST.SP.800-84.

[176] I. T. L. Computer Security Division, “About the RMF - NIST Risk Management Framework,” *CSRC | NIST*, Sep. 15, 2021. https://csrc.nist.gov/projects/risk-management/about-rmf (accessed Sep. 17, 2021).

[177] J. Kick, “Cyber Exercise Playbook,” MITRE Corp, Bedford, MA, Nov. 2014. Accessed: Sep. 13, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA624910

[178] L. P. Costantini and A. Raffety, “Cybersecurity Tabletop Exercise Guide.” National Association of Regulatory Utility Commissioners, Sep. 2020. [Online]. Available: https://pubs.naruc.org/pub/615A021F-155D-0A36-314F-0368978CC504

[179] Cybersecurity and Infrastructure Security Agency, “CISA Tabletop Exercise Package - Exercise Planner Handbook.” [Online]. Available: https://www.cisa.gov/sites/default/files/publications/2%20-%20CTEP%20Exercise%20Planner%20Handbook%20%282020%29%20FINAL_508_1.pdf

[180] European Union Agency for Network and Information Security, “Cyber Exercises,” *ENISA*. https://www.enisa.europa.eu/topics/cyber-exercises (accessed Sep. 17, 2021).

[181] “Use a Tool. Improve Your Cybersecurity.,” *GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk*. https://www.globalcyberalliance.org/use-a-tool/ (accessed Sep. 17, 2021).

[182] CREST, “Cyber Threat Intelligence Maturity Assessment Tools.” https://www.crest-approved.org/2020/01/10/cyber-threat-intelligence-maturity-assessment-tool/index.html (accessed Sep. 17, 2021).

[183] Open CSIRT Foundation, “SIM3 Online Tool.” https://opencsirt.org/csirt-maturity/sim3-online-tool/ (accessed Sep. 17, 2021).

[184] The MITRE Corporation, “MITRE Cybersecurity,” *GitHub*. https://github.com/MITRECND (accessed Sep. 17, 2021).

[185] SANS Institute, “Cyber Security Tools.” https://www.sans.org/tools/ (accessed Sep. 17, 2021).

[186] KnowBe4, “Free IT Security Tools.” https://www.knowbe4.com/free-it-security-tools (accessed Sep. 17, 2021).

[187] Cybersecurity and Infrastructure Security Agency, “CISA Tabletop Exercise Package | CISA.” https://www.cisa.gov/publication/cisa-tabletop-exercise-package (accessed Sep. 17, 2021).

[188] CREST, “CREST Exams.” https://www.crest-approved.org/professional-qualifications/crest-exams/index.html (accessed Sep. 17, 2021).

[189] The MITRE Corporation, “Awareness & Training,” Aug. 15, 2013. https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources/awareness-training (accessed Sep. 17, 2021).

[190] “OpenSecurityTraining2.” https://opensecuritytraining.info/ (accessed Sep. 17, 2021).

[191] SANS Institute, “Cyber Security Courses.” https://www.sans.org/cyber-security-courses/?msc=main-nav (accessed Sep. 17, 2021).

[192] SANS Institute, “Security Awareness Training | SANS Security Awareness.” https://www.sans.org/security-awareness-training/ (accessed Sep. 17, 2021).

[193] SANS Institute, “Managing Human Risk: Mature Security Awareness Programs | SANS MGT433.” https://www.sans.org/cyber-security-courses/managing-human-risk-mature-security-awareness-programs/ (accessed Sep. 17, 2021).

[194] SANS Institute, “Strategic IT Security Planning | IT Security Policy Training Course | SANS MGT514.” https://www.sans.org/cyber-security-courses/security-strategic-planning-policy-leadership/ (accessed Sep. 17, 2021).

[195] SANS Institute, “Cyber Security Risk Assessment Training | Cyber Risk Assessment Course | SANS MGT415.” https://www.sans.org/cyber-security-courses/intro-risk-assessment/ (accessed Sep. 17, 2021).

[196] SANS Institute, “Cybersecurity Management - Leading Change | SANS MGT521.” https://www.sans.org/cyber-security-courses/leading-cybersecurity-change/ (accessed Sep. 17, 2021).

[197] SANS Institute, “IT Project Management & Effective Communication | SANS MGT525.” https://www.sans.org/cyber-security-courses/project-management-effective-communication/ (accessed Sep. 17, 2021).

[198] European Union Agency for Network and Information Security, “Training Courses,” *ENISA*. https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/training-courses (accessed Sep. 17, 2021).

[199] ESET, “Cybersecurity Awareness Training.” https://www.eset.com/us/cybertraining/ (accessed Sep. 17, 2021).

[200] NINJIO, “Engaging & Behavior Changing Cybersecurity Awareness Training.” https://ninjio.com/lp4c-esecurityplanet/ (accessed Sep. 17, 2021).

[201] “Free and Low Cost Online Cybersecurity Learning Content,” *NIST*, Apr. 07, 2020. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content (accessed Sep. 17, 2021).

[202] KnowBe4, “Security Awareness Training.” https://www.knowbe4.com/ (accessed Sep. 17, 2021).

[203] Cofence, “Phishing Awareness Training & Tools | Phishing Simulations.” https://cofense.com/product-services/phishme/ (accessed Sep. 17, 2021).

[204] CybSafe, “CybSafe – Understand people. Prevent security incidents.” https://www.cybsafe.com/ (accessed Sep. 17, 2021).

[205] Elevate Security, “Stop Reacting. Start Preventing.,” *Elevate Security*, Nov. 12, 2020. https://elevatesecurity.com/ (accessed Sep. 17, 2021).

[206] Mimecast, “Security Awareness Training.” https://www.mimecast.com/products/awareness-training/ (accessed Sep. 17, 2021).

[207] Proofpoint, “Cybersecurity Solutions, Services & Training.” https://www.proofpoint.com/us (accessed Sep. 17, 2021).

[208] Living Security, “CyberSecurity Training | Human Risk Management | Security Awareness Training.” https://www.livingsecurity.com (accessed Sep. 17, 2021).

[209] LUCY Security, “Cyber Security Training Solutions.” https://lucysecurity.com/ (accessed Sep. 17, 2021).

[210] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte, “Workforce Framework for Cybersecurity (NICE Framework),” National Institute of Standards and Technology, Nov. 2020. doi: 10.6028/NIST.SP.800-181r1.

[211] Ministry of Communications and Information Technology (Egypt), “Information Technology Institute.” http://www.iti.gov.eg/

[212] S. Hashem, “Establishing a National CERT/CISRT in Egypt,” in *The Proceedings of the 23rd World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2019*, 2019, vol. II, pp. 38–43.

[213] EG-CERT, “EG-CERT’s Experts Train The Tanzanian Emergency Response Teams, Dar es Salaam,” Apr. 2019. https://www.egcert.eg/eg-certs-experts-train-the-tanzanian-emergency-response-teams-dar-es-salaam-april-2019/ (accessed Sep. 15, 2021).

[214] K. Mori, “Supporting CSIRT Activities for Africa (in Tunisia),” *JPCERT/CC Eyes*, Jan. 07, 2019. https://blogs.jpcert.or.jp/en/2019/01/supporting-csirt-activities-for-africa-in-tunisia.html (accessed Sep. 15, 2021).

[215] V. Sarvepalli, “Securely Connecting Africa,” *Carnigie Mellon University Software Engineering Institute*, Mar. 25, 2019. https://insights.sei.cmu.edu/blog/securely-connecting-africa/ (accessed Sep. 15, 2021).

[216] International Telecommunication Union, “Cybersecurity Events,” *ITU*. https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/cybersecurity-events.aspx (accessed Sep. 19, 2021).

[217] ITU Academy, “Full catalogue of courses.” https://academy.itu.int/training-courses/full-catalogue?search_api_fulltext=cybersecurity&field_taxon_registration=All&field_course_fee=All&field_taxon_region=All&field_taxon_type=All&field_taxon_topics=All&field_taxon_languages=All&date_start=&date_end=&items_per_page=10 (accessed Sep. 19, 2021).

[218] A. L. Hueca, “Engaging the CSIRT Community: Cyber Capacity Building on a Global Scale,” *SEI Blog*, Sep. 10, 2018. https://insights.sei.cmu.edu/blog/engaging-the-csirt-community-cyber-capacity-building-on-a-global-scale/ (accessed Oct. 22, 2021).

[219] Carnegie Mellon University Software Engineering Institute, “SEI CERT Division and State Department Team Up on Sub-Saharan Cybersecurity Effort,” Apr. 04, 2017. https://www.sei.cmu.edu/news-events/news/article.cfm?assetId=496117 (accessed Oct. 22, 2021).

[220] “Cyber Incident Response Capability established in the Republic of Moldova with NATO support,” *NATO - News*, Jan. 21, 2021. https://www.nato.int/cps/en/natohq/news_180758.htm (accessed Sep. 15, 2021).

[221] “Azerbaijan - Country Flyer 2021.” NATO, 2021. [Online]. Available: https://www.nato.int/science/country-fliers/Azerbaijan.pdf

[222] “Jordan - Country Flyer 2021.” NATO, 2021. [Online]. Available: https://www.nato.int/science/country-fliers/Jordan.pdf

[223] “Morocco - Country Flyer 2021.” NATO, 2021. [Online]. Available: https://www.nato.int/science/country-fliers/Morocco-ENG.pdf

AUTHORS

Jean-Robert Hountomey is an Internet pioneer in West Africa. He is also a founding member of the Africa Forum of computer security and incident response team (AfricaCERT) and the African Anti Abuse Working Group. He is member of the African Union Cybersecurity Expert Group. He has worked on Internet policy issues, capacity building, information security, product security, secure software development life cycle, and privacy risk management for two decades. He has contributed to many organizations and many publications. Jean-Robert's research focuses on law, technology, and Internet governance issues.

Prof. Hayretdin Bahsi is a research professor at the Centre for Digital Forensics and Cyber Security at Tallinn University of Technology in Estonia. He received his PhD and MSc degrees in Computer Engineering from Sabanci University and Bilkent University respectively. He was involved in many R&D and consultancy projects on cyber security as a researcher, consultant, and program coordinator at the Information Security Research Centre of the Scientific and Technological Research Council of Turkey between 2000 and 2014. He acted as the founding director of the National Cyber Security Research Institute. His research interests include cyber-physical system security and the application of machine learning methods to cyber security problems.

Dr. Unal Tatar is an assistant professor of cybersecurity in the College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University at Albany. Dr. Tatar worked as a principal cybersecurity researcher in government, industry, and academia for over 15 years. He is the former coordinator of the National Computer Emergency Response Team of Turkey. Dr. Tatar's research is funded by the National Science Foundation, National Security Agency, Department of Defense, NATO, and Society of Actuaries. His main topics of interest are cybersecurity risk management, economics of cybersecurity, cyber insurance, privacy, cybersecurity education, supply-chain security, and blockchain. Dr. Tatar holds a BS in Computer Engineering, an MS in Cryptography, and a Ph.D. in Engineering Management and Systems Engineering.

Dr. Sherif Hashem is a Full Professor of Information Sciences and Technology at George Mason University-USA. He is currently a member of the Board of Directors of FIRST (Forum of Incident Response and Security Teams), and a member of the African Union’s Cybersecurity Expert Group (AUCSEG). He is a **Senior IEEE** member and an ISACA Certified Information Security Manager (CISM). Dr. Hashem received a Ph.D. in Industrial Engineering from Purdue University-USA, a M.Sc. in Engineering Mathematics and a B.Sc. in Communication & Electronic Engineering from Cairo University-Egypt. He completed the Senior Executive Program at Harvard Business School-USA. He received several awards and recognition including: the *Global Bangemann Challenge Award* from the *King of Sweden* (Stockholm – 1999).

Ms. Elisabeth Dubois is a Ph.D. Candidate in Information Science with specializations in crisis communication and information assurance. She holds a BS in Digital Forensics and MBA degree from the University at Albany. Elisabeth's research is interdisciplinary focusing on various aspects of crisis and risk management including cybersecurity, decision making, communication, and education. She has been involved in many academic, research, community-based, and professional projects and experiences in related topics.