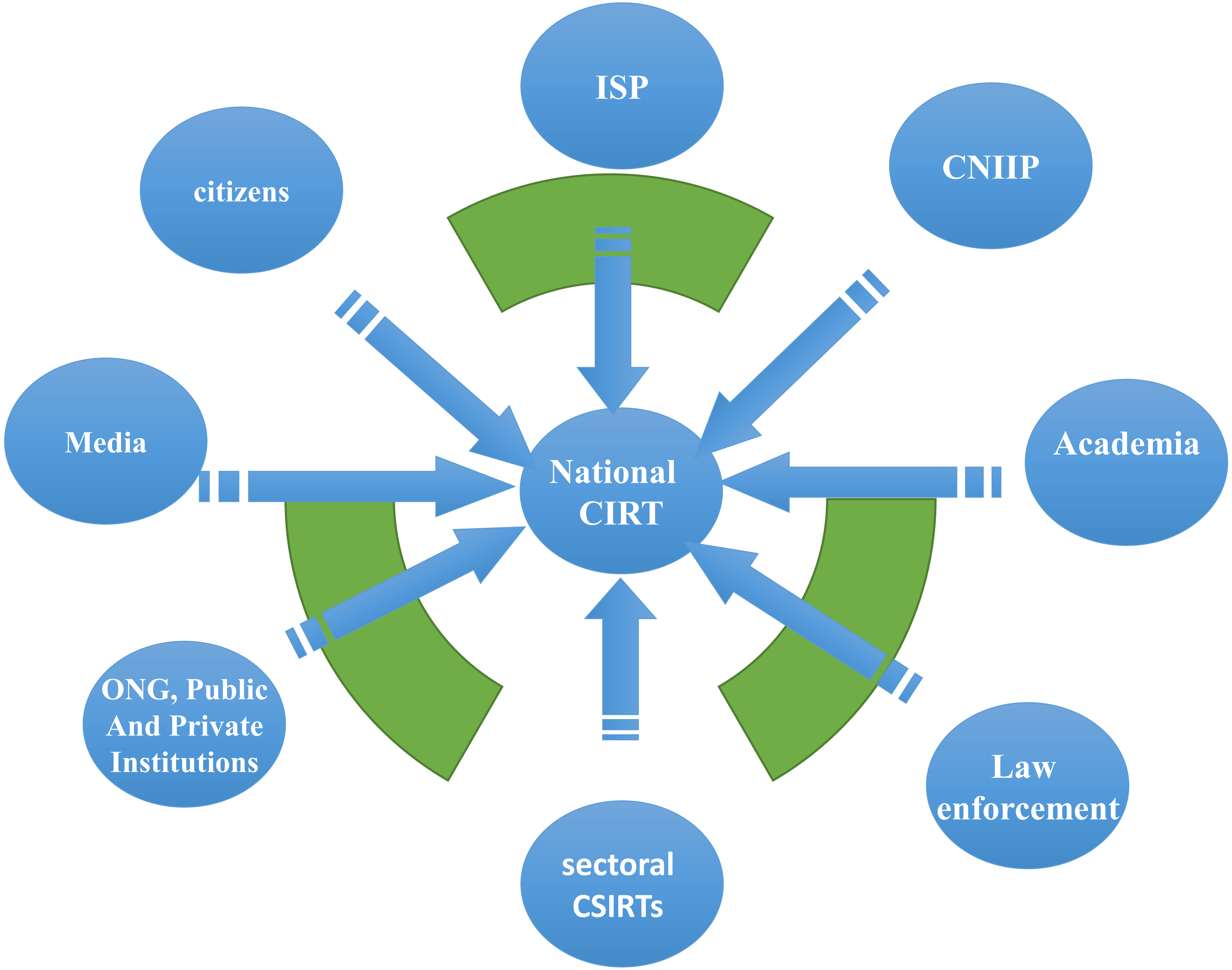
International
Telecommunication
Union

Stakeholders Analysis

Introduction
National Stakeholders



CIRT

□

□ A specialized entity for incident and emergency response, ensuring preventive and proactive services.

□ A CIRT is acting at a national level to secure the cyberspace, and assist home users to handle incidents and to protect their assets.

□ A trusted Point of Contact for national and international cyberspace stakeholders

ISP

□

□ Providing all internet related services, including Security. The first Point of Contact for their customer in case of incident.

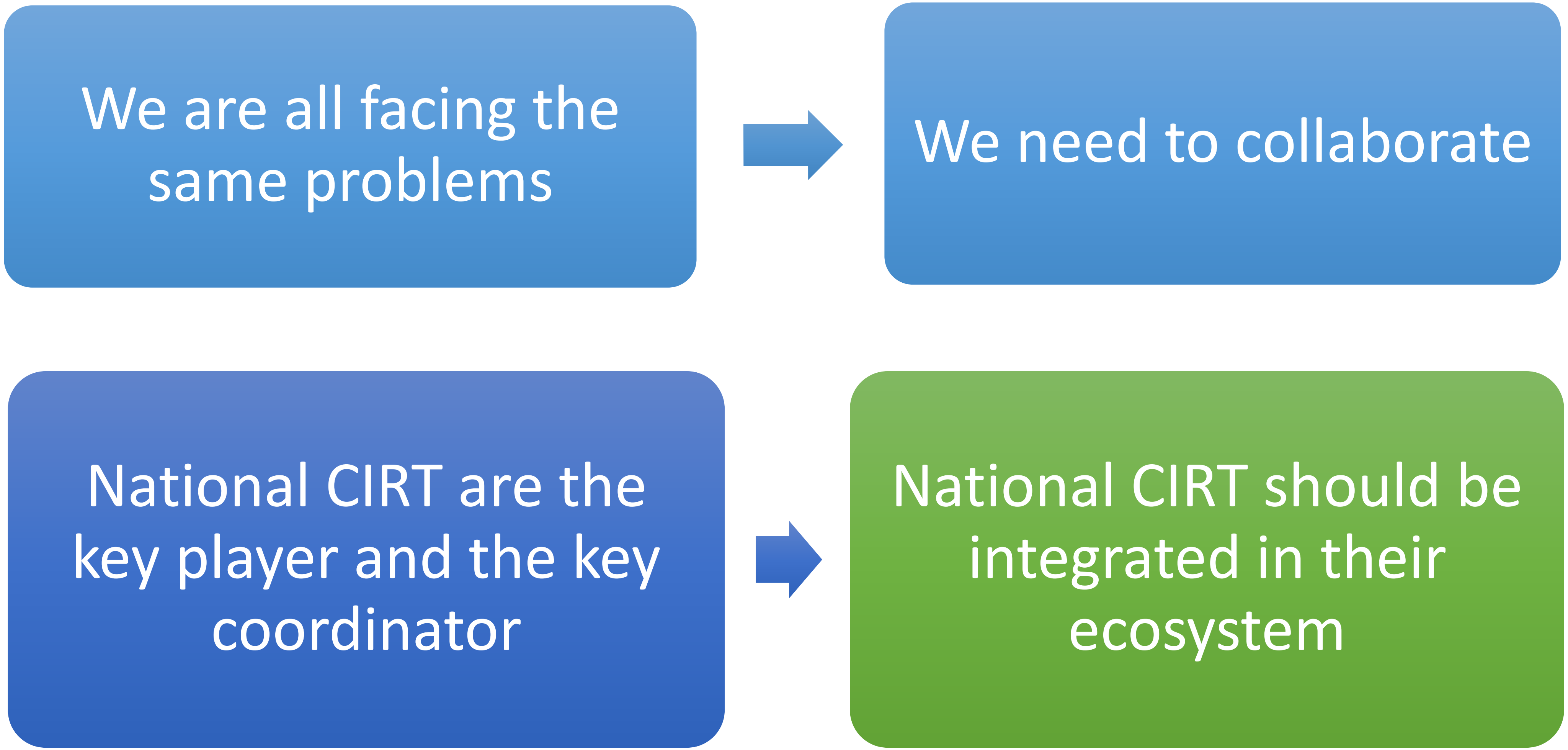
□ Well-positioned to contribute improve cybersecurity

□ A trusted Point of Contact for their customers

Incident response coordination

- Web defacement
- DDoS
- Massive malware infection
- Phishing
- Massive vulnerability exploitation
- Data leakage
- Spamming
- Massive Identity theft
- Massive scan

Introduction



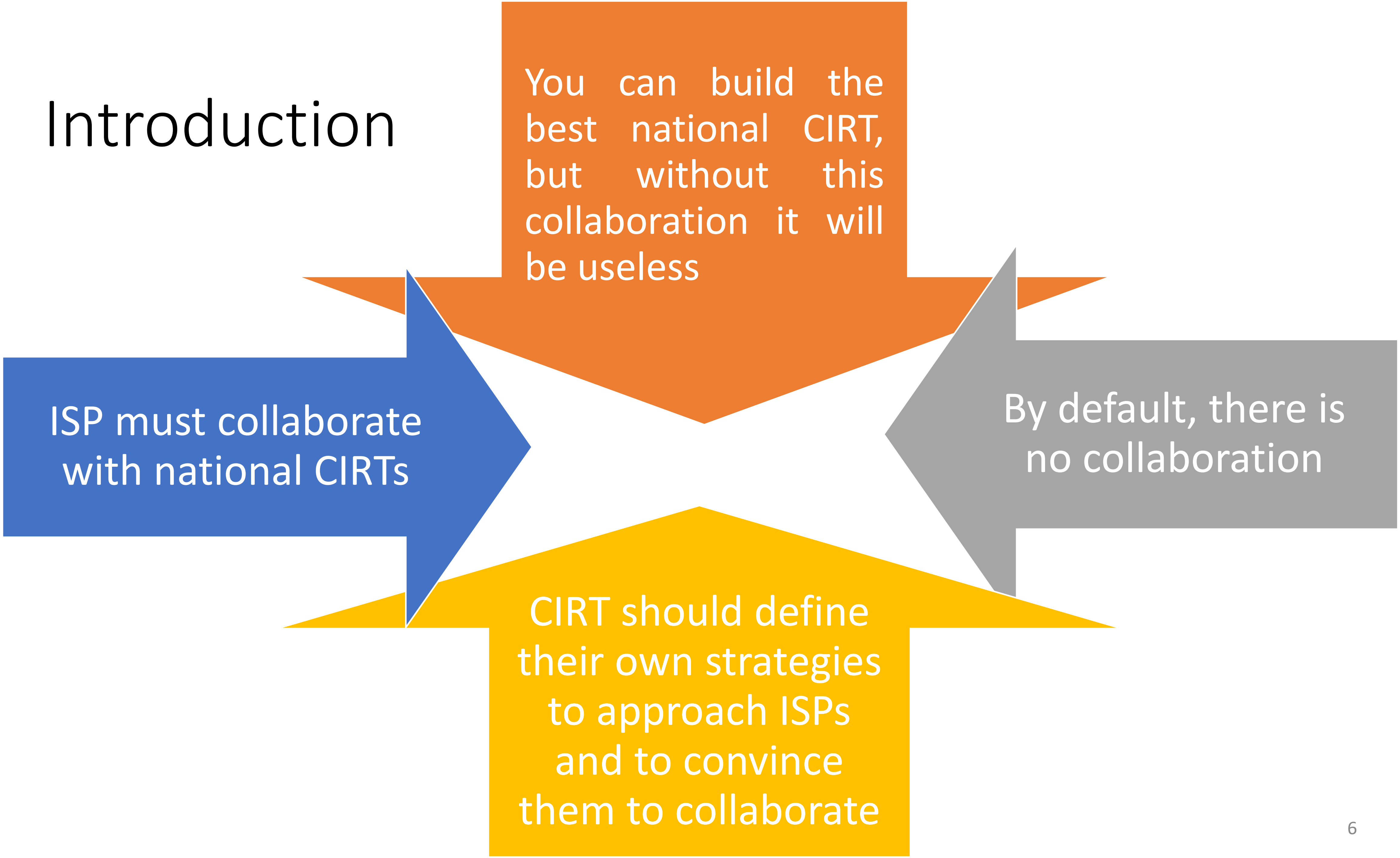
We are all facing the same problems

We need to collaborate

National CIRT are the key player and the key coordinator

National CIRT should be integrated in their ecosystem

Introduction



You can build the best national CIRT, but without this collaboration it will be useless

ISP must collaborate with national CIRTs

By default, there is no collaboration

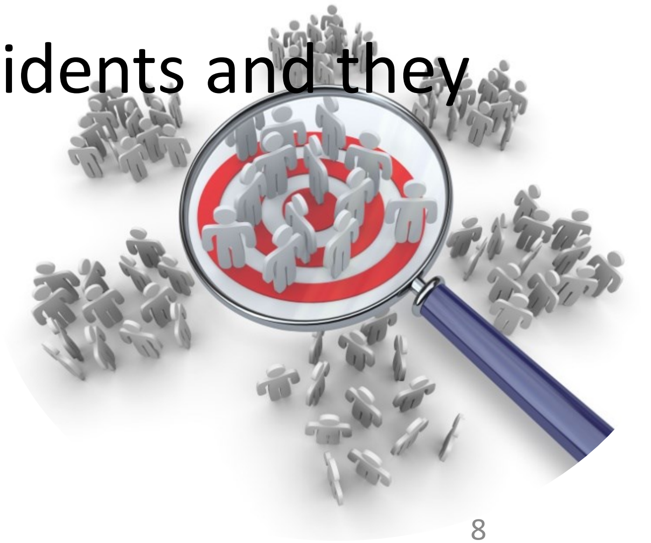
CIRT should define their own strategies to approach ISPs and to convince them to collaborate

How to get ISPs involved?
What CIRTs need to do?

1

Select carefully your target

- Identify the key stakeholders and focus all your efforts on them (the biggest, the most critical, the most targeted, the easiest, etc.)
- Others will follow,
- There will be some good and positive partners and there will be others considering themselves as better than you,
- For those who will resist, just wait for some critical incidents and they will come.



2 Show your expertise: you are the expert

- ISPs must consider the CIRT as an expert and focused team ready to help them to respond to their incidents,
- CIRT must spend all their efforts to develop their technical skills and to get ready to any kind of incident while ISP cannot afford this investment,
- ISP will trust this technical expertise and will start to rely on CIRT,
- To show the expertise: workshop, site visit, labs, success stories, procedures, etc.

3 Help ISPs to respond to their incidents

- If needed send them a team on site,
- Offer them a premium 24/7 service,
- Provide a dedicated incident reporting (online ticketing systems, dedicated email, etc.)

4 Help them to detect their incidents

- Run a dedicated monitoring and threat intelligence,
- Alert them in case of attacks: web defacement on their customers websites, infected users, phishing, etc.
- Help them to deploy monitoring systems:
  - IDS,
  - Honeynet,
  - DNS sinkhole,
  - Netflow,

5 Share information

Better to give than ask

Gather information coming from:

- Public sources,
- Other CIRTs,
- Other Honeynet,

- Share information about current threats:
  - vulnerabilities,
  - exploits on the wild,
  - Malware infection,
  - Cyber-threats
  - Detected attacks (Web defacement, Malware infection, Spam, DoS/DDoS, Phishing, etc.)

6 Offer free assistance

- Security assessment after incident closure,
- Assistance to secure and implement recommendations and best practices,
- Help them to deploy security solutions (Firewall, IDS, WAF, VPN, etc.) mainly from open source,
- Help them to develop cybersecurity awareness program for their staff and for their customers.

7 Train and do cyber exercices

- Train them on incident response,
- Train them on coordination procedures,
- Organize periodic cyber exercises/ Cyber drill,
- During incident response ask your team to explain and to do some transfer of competence,
- Share your experience with them.

8 Ensure a continuous communication

- Make sure that you have a good communication with ISPs especially during emergencies,
- Maintain efficient communication channels between teams: email and phone mainly,
- Hold a meeting with top management and periodic ones with technical teams, do technical workshops/forum, etc.

9 Show your engagement to secure their data

- Insist on applying security controls like:
    - Email encryption,
    - Securing your network,
    - Physical security,
    - Data destruction,
    - Etc.
- Make sure they are informed about your security policy and recommend them to adopt similar controls.

10 You are the trusted Point of Contact

- Develop your international collaboration network and inform them that you are the main Point-of-Contact with foreign entities,
- As a trusted PoC you can easily help them to solve their issues: incident, blacklisting, etc.
- Being member of AfricaCIRT, FIRST, OIC-CIRT, etc. can help to achieve it.

What to avoid?

- Don‘t report incident to their top management,
- Don’t ask them to spend q lot of money,
- Don’t be pretentious,
- Don’t tell them you are mandated by law and the should comply,
- Don’t be late in case of emergencies.

Sectoral CSIRTs

CNIIP

Law enforcement

ONG, Public And Private Institutions

citizens

Academia

Media

Build a Trusted and A win-win Relationship

Global Initiatives

Regional Initiatives

enisa
European Network
and Information
Security Agency

APCERT
Asia Pacific Computer Emergency Response Team

OIC-CERT
Computer Emergency Response Team

ORGANIZATION OF AMERICAN STATES

Organization of
American States

AfricaCERT
United in promoting cyber security in Africa

International Telecommunication Union

- The organization of Trainings and Workshops
- Conduction a Regional and National Cyberdrills (16 Cyberdrill)
- Assistance to their member states in the establishment and the improvement of their National CIRT (65 National CIRT Assessment , 14 National CIRT designed and established)
- Development Training Materials , Guidelines and Best Practices
- Development of common standards (X.1500 : cybersecurity information exchange techniques)
- Development of CIRT Tools

Forum for Incident and Security Response Team

- FIRST is a premier organization and recognized global leader in incident response
- Annual FIRST Conference on Computer Security Incident Handling
- The organization of Trainings and Workshops (FIRST Symposia , FIRST Technical Colloquia)
- Development Training Materials , Guidelines and Best Practices
- Development of common standards
- Development of CIRT Tools (CIRT in a BOX).
- Research & development activities

CIRT/CC

- The organization of Trainings and Workshops.
- The Annual Technical Meeting for CSIRTs with National Responsibility
- Development Training Materials , Guidelines and Best Practices
- Research & development activities

TF-CSIRT and TERENA

- Act as accreditation body for the CSIRT
- Development of training materials (TRANSITS I and TRANSITS II)
- Research & development activities (SIM3 : Security Incident Management Maturity Model)

Global Forum for Cyber Expertise

- CSIRT Maturity Initiative
- Help emerging and existing CSIRTS to increase their maturity level
  - ITU
  - Microsoft
  - OAS
  - The Netherland

Organization of
American States

Regional Organizations

- The organization of Trainings and Workshops
- Conduction a Regional Cyber Exercises
- Assistance to their member states in the implementation of a CSIRT
- Development Training Materials , Guidelines and Best Practices