



Who is doing What in Cybersecurity ?

the Tunisian experience

Belhassen ZOUARI,
CEO, National Agency for Computer Security, Head of Cert-Tcc,
E-mail : b.zouari@ansi.tn

3 Pillars of Cybersecurity

The keys to success in a **Cybersecurity** project rely on 3 pillars :

- **Technology**

ICT/Security tools, etc.

- **Methodology**

Policy, procedures, regulation, etc.

- **Social behaviour**

Culture of Cybersecurity





Technology Pillar

Computer & network tools

Antivirus

Firewall

IDS

IPS

Physical security tools

Physical access control

Building Security

Actors : Security professionals (Private sector)

Users, (Private/Public companies, individuals)

Data tools

Storage Media

Cryptography

Availability & applications

Redundant Server

PKI

e-services



Methodology Pillar

Managerial level

Security Policy
Management procedures
Capacity building
Auditing

Legislation level

Laws & regulation texts
Law enforcement

Actors : Government
Security professionals (Private sector)
Users, (Private/Public companies, individuals)

Operational

Access Control rules
Implementation plans
Monitoring, Watching &
Incident handling

Continuity of services

Business Continuity Plan
Crisis Management
Drill Exercises



Social behaviour Pillar

Cultivating the *Culture* of Cybersecurity

- Continuous action
- Diversifying media/channel materials

Raising Awareness

Target public :

- Managers / Decision makers
- Security Responsibles/Managers
- Children
- Parent
- Teachers
- Simple ICT users
- Communities (NGOs)



Legislative Framework

January 2003 :

- ❑ The creation of a **National Agency, specialized in IT Security**
(The Tool for the execution of the national strategy and plan)
- ❑ The Introduction of **Mandatory and Periodic Security audits**
(Pillar of our strategy)
- ❑ The creation of a “body of certified Auditors” in IT Security
+ some accompanying measures (launch of masters in IT security, ...)

In addition to previous Laws :

- Law on Electronic Signature and e-commerce (Law N° 2000-83)
- Law Against Cyber-Crimes (Law N° 1999-89, Art 199)
- Law on consumer protection and respect of Intellectual property (Law N°1994-36)
- Law on protection of Privacy and Personal data (Law n° 2004-63)

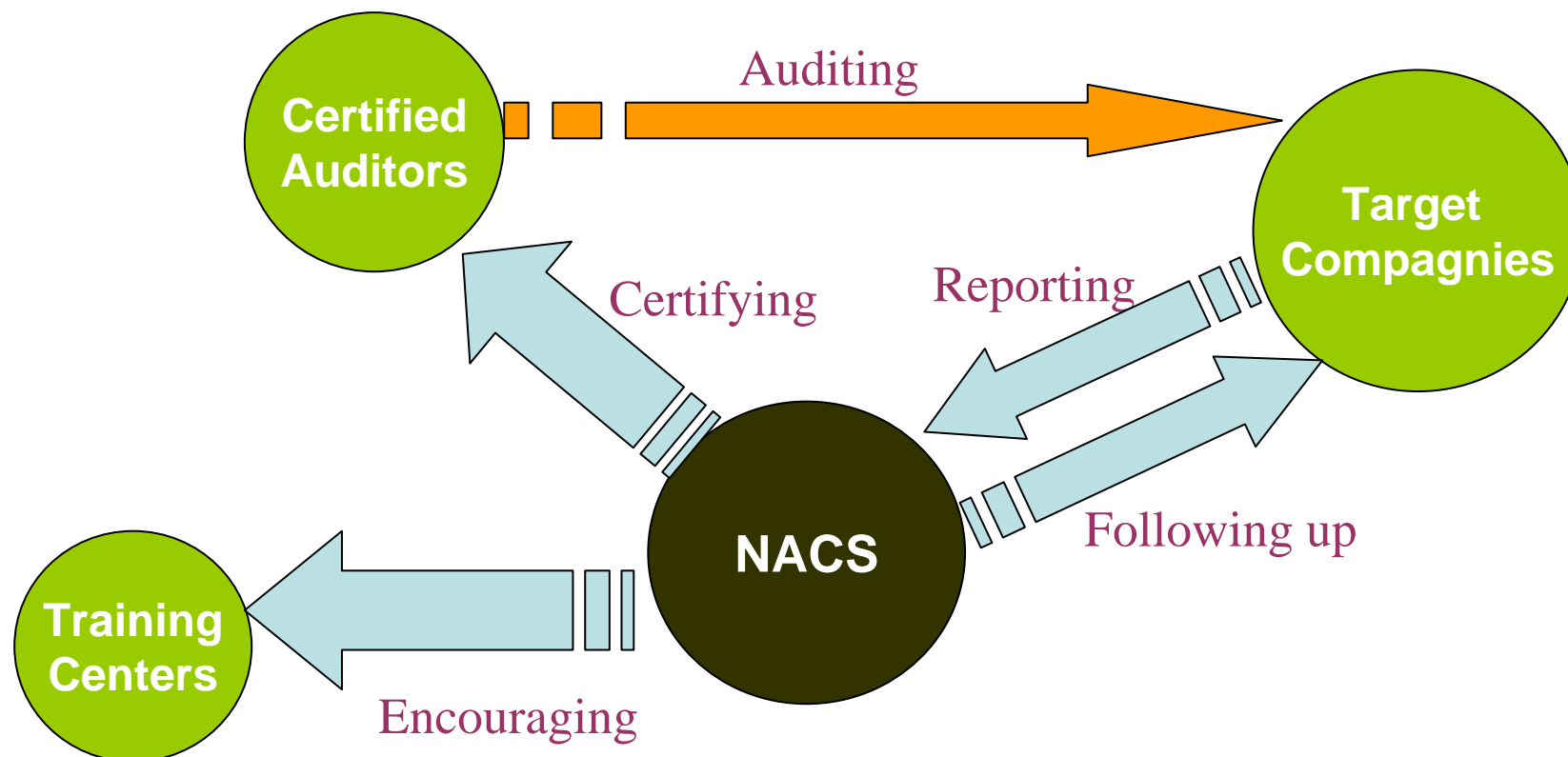
✓ **September 2005** : launch of Cert-Tcc
(Computer Emergency Response Team / Tunisian Coordination Center)

✓ May 2007: Full Member of FIRST (Forum of Incident Response Teams)



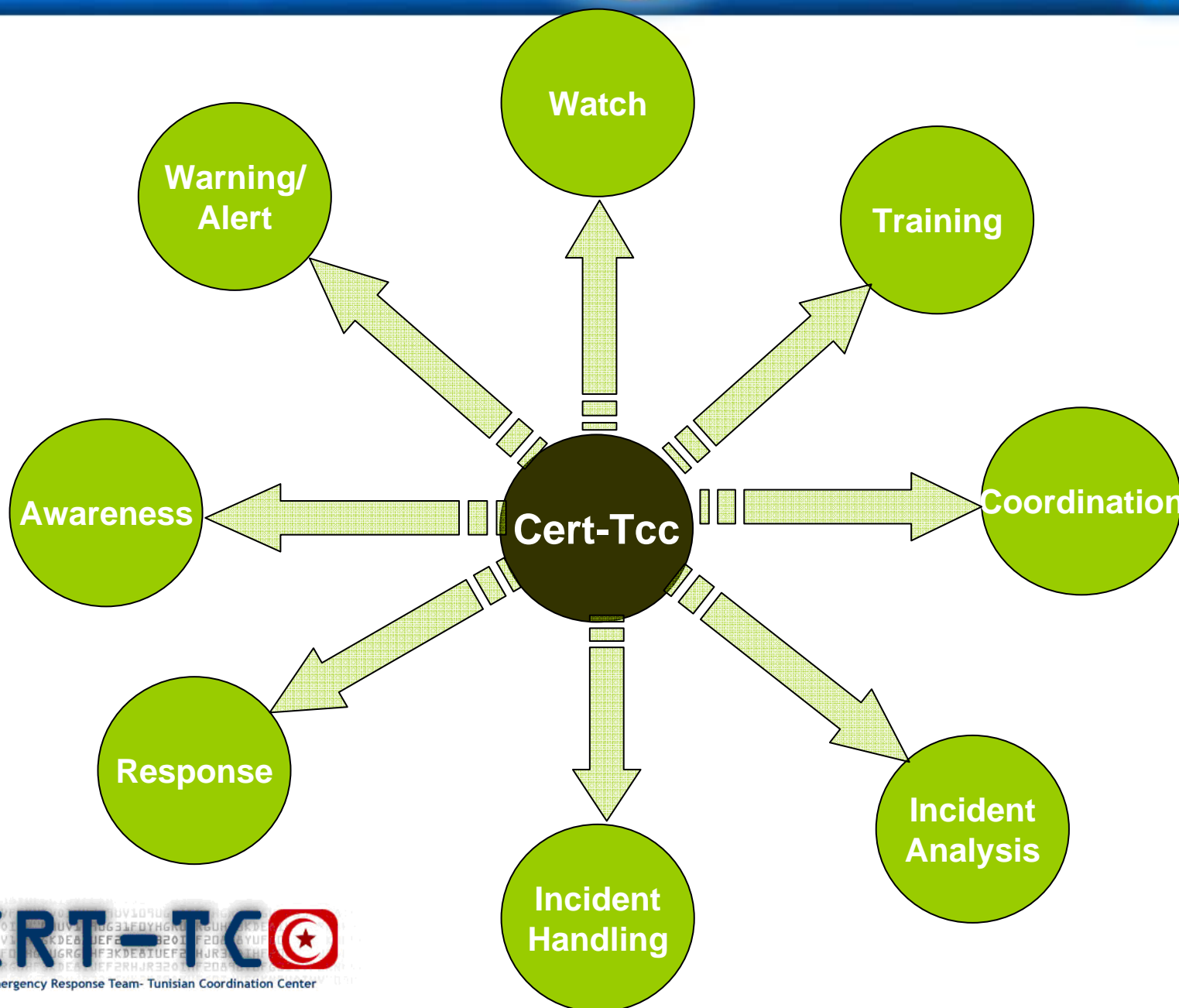
How are organized the Tunisian structures

How is organized the Security Audit process





Forum of Incident Response and Security Teams





Watch



Publication of vulnerabilities,
exploits, 0days



Collaboration network



Antivirus suppliers



Collaboration
program

Collect
information



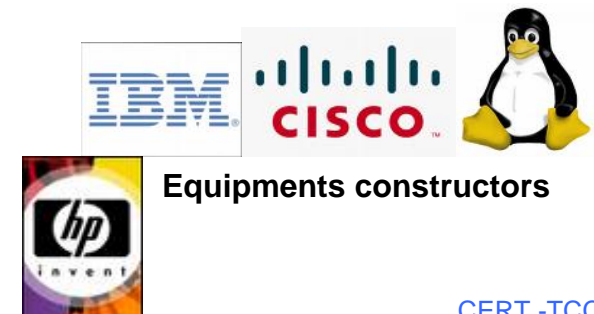
Professional
community



Watch professionals



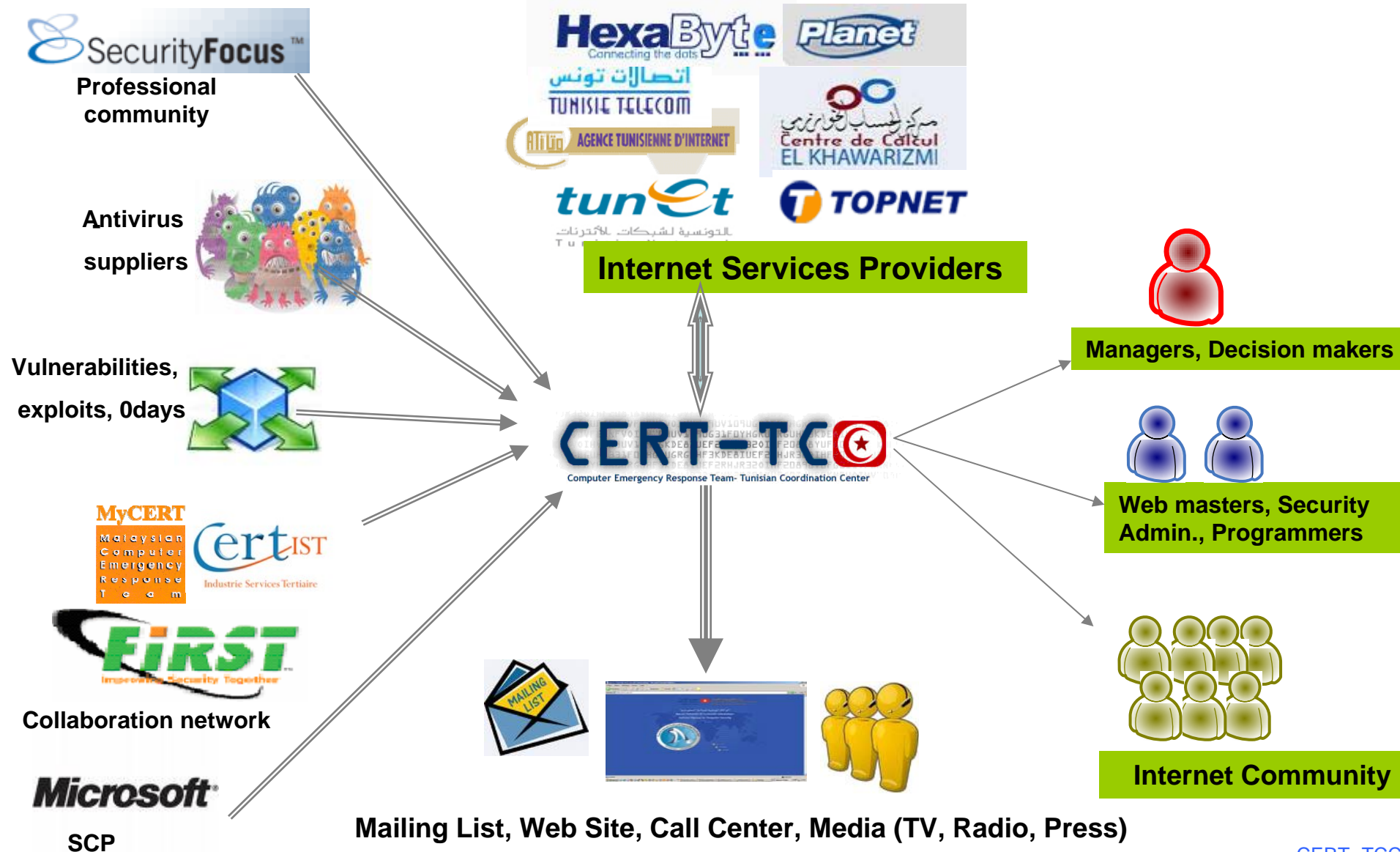
Trend
indicators



Equipments constructors



Information, Warning & Alert

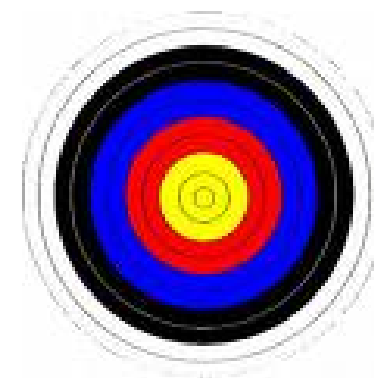




Awareness

Oriented campaigns

- + **Decision makers**
- + **Professionals**
- + **Teachers**
- + **Students**
- + **Users**
- + **Journalists**
- + **Lawyers**



Diversified contents

Prospectus

Posters

Emails

Radio Emission

Cartoon

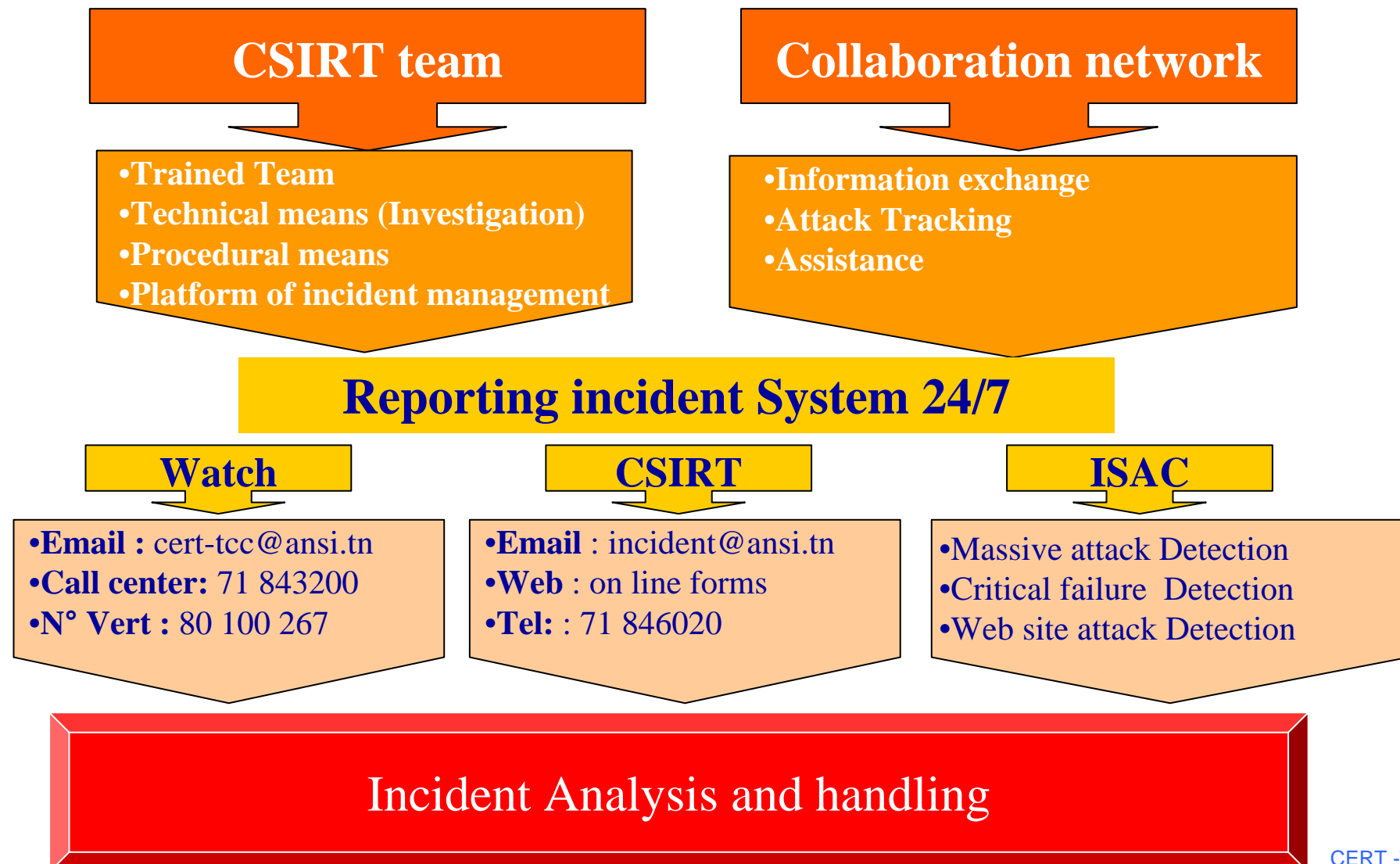
Video Spot

Attack Simulation

Guide

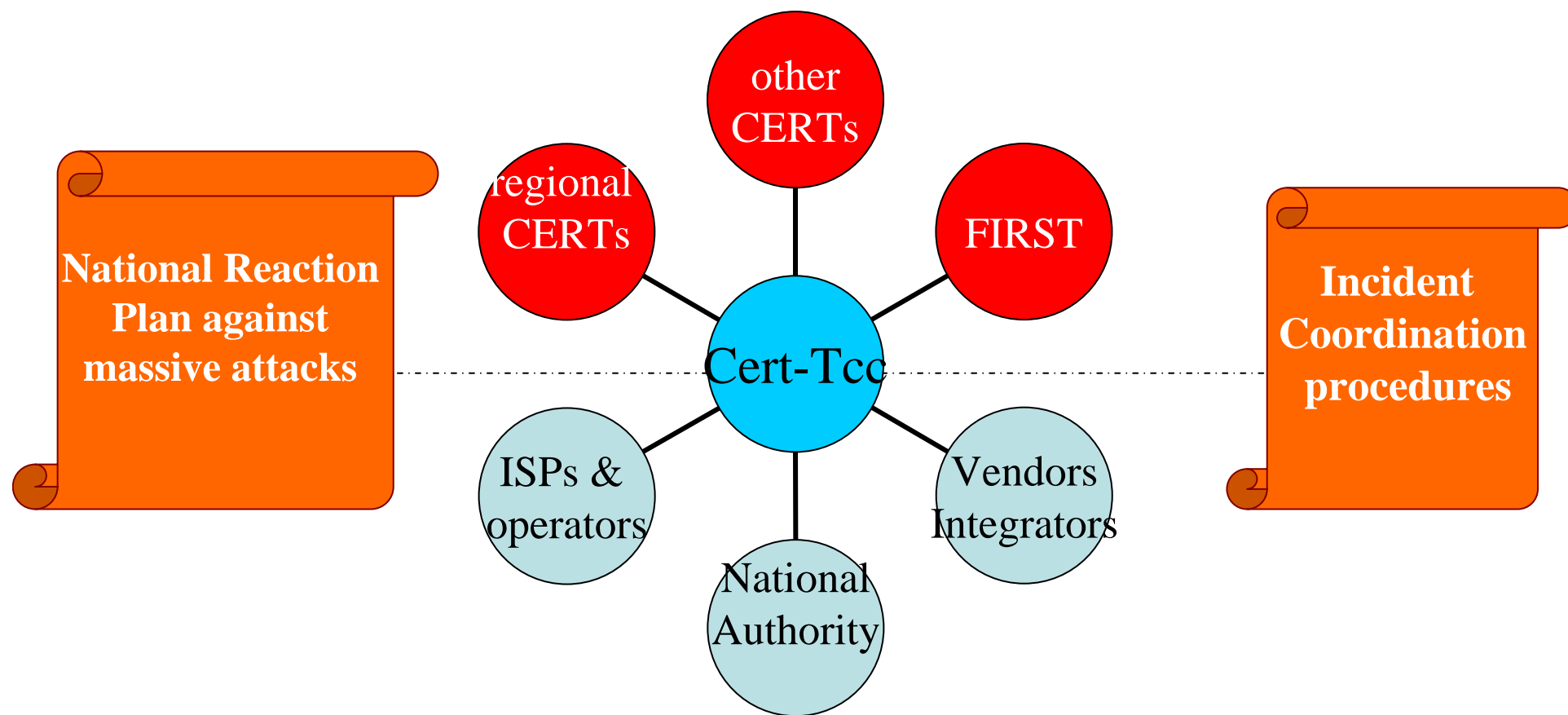


Incident Handling (CSIRT)





Coordination





“Know-How” In IT security

Reaching a relative technological autonomy :

- Supporting Training & Capacity building
- Encouraging the development of national Solutions and Tools, based on **Open-source components**
- Improving R&D capabilities and making it more responsive to urgent needs.
- Encouraging Academic Research in the Important topics of Security (cryptography, methodologies, ...)



Thank you for your attention