National Agency for
Computer Security

MINISTRY OF COMMUNICATION
TECHNOLOGIES
TUNISIA

International
Telecommunication
Union

Implementing a National Strategy :

the case of the Tunisian CERT

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

a fast Historical Overview

□ end **1999 :** Launch of a **UNIT (a "Micro-CERT")** , specialized in IT Security

Objective :

- **to raise awareness decision-makers and Technical staff about security issues**.

& ***to creates a first Task-force of Tunisian Experts in IT Security***

*(**+** Monitoring the security of highly critical national applications and infrastructures..)*

□ From **End 2002** (" **certification of the role of IT security as a pillar of the « Information Society** ») **:**

➢ The unit starts the establishment of a **strategy** and of a **National Plan** in IT Security
(**national survey** , for fixing: priorities, volume of actions, needed logistic, supporting tools, .).

□ **January 2003 :**

- **Decision of the Council of Ministers, headed by the President, and dedicated to informatics and IT Security , of :**

□ 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)

✓ **February 2004** : **Promulgation of an "*original*" LAW,** related to ICT **security**
(Law N° 5-2004 ***and its 3 relatives decrees***) :

➢ **Obligation** for national companies (ALL public + "big" and sensitive private ones) to do **Periodic (Now annually) Security audits of their IS.**

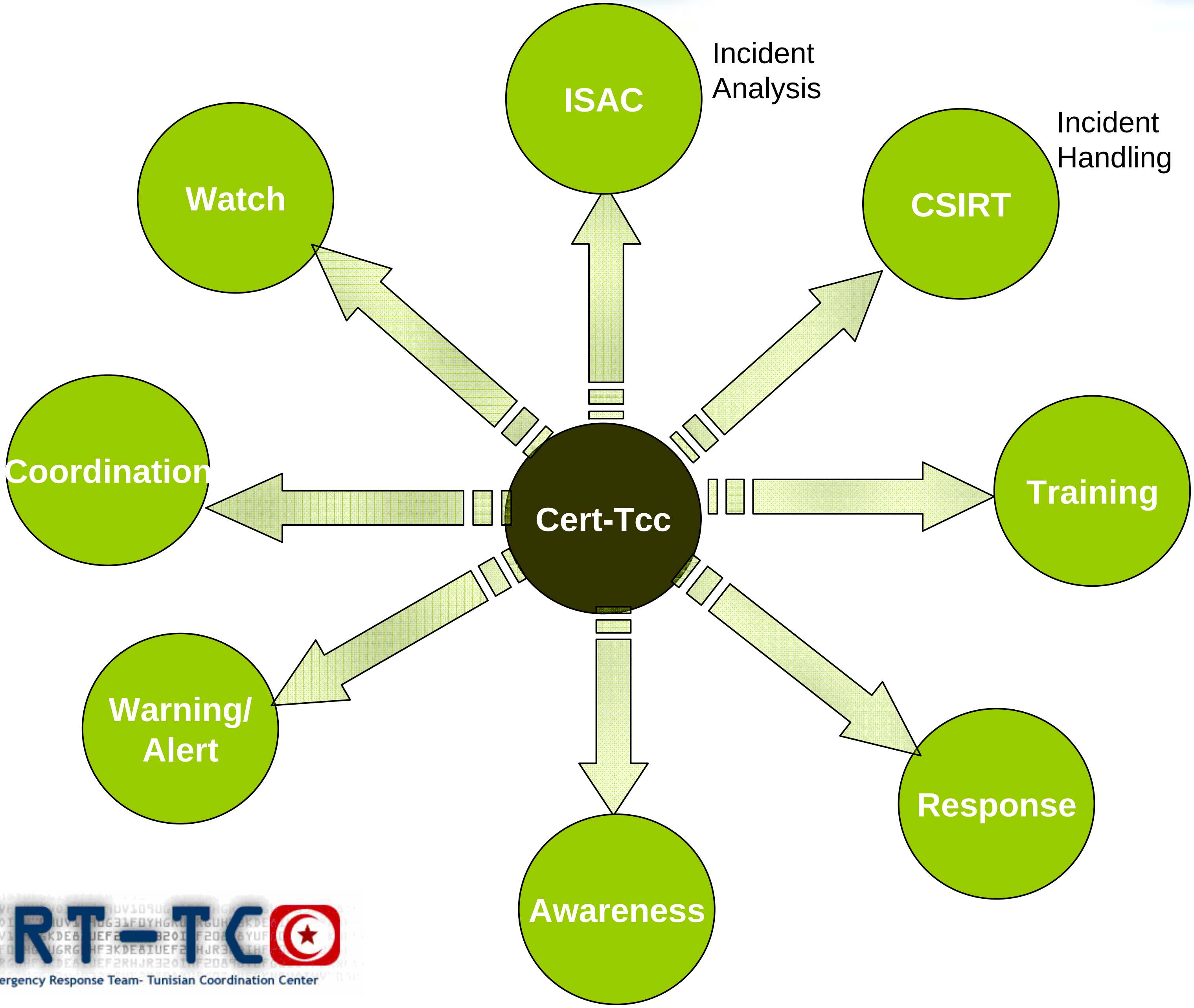
➢ **Organization of the field of Security audits**

→ Audits are Made by **CERTIFIED auditors** (***from the private sector***),
→ *definition of the process of certification of auditors*
→ *definition of the auditing missions and process of follow-up* (**ISO 1 77 99**)

➢ *Creation and definition of the Missions of the* **National Agency for Computer Security**
(created under the **Ministry of Communication Technologies)**

➢ **Obligation to declare** security Incidents (Viral, mass hacking attacks, ..)
that could affect **others** IS, with guarantee of **confidentiality**, by law.

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



Cert-Tcc

ISAC

Incident
Analysis

CSIRT

Incident
Handling

Training

Response

Awareness

Warning/
Alert

Coordination

Watch

Forum of Incident Response and Security Teams

CERT-TCC

Computer Emergency Response Team- Tunisian Coordination Center

Watch

milw0rm

Publication of vulnerabilities, exploits, 0days

MyCERT Malaysian Computer Emergency Response Team

CertIST Industrie Services Tertiaire

FIRST Improving Security Together

Collaboration network

symantec.

PROTECTED BY McAfee SECURITY

KASPERSKY

TREND MICRO

Antivirus suppliers

Microsoft

Collaboration program

Collect information

SANS

SecurityFocus™

Professional community

Secunia Stay Secure

CERT

US-CERT

Watch professionals

Internet Storm Center

zone-h

Trend indicators

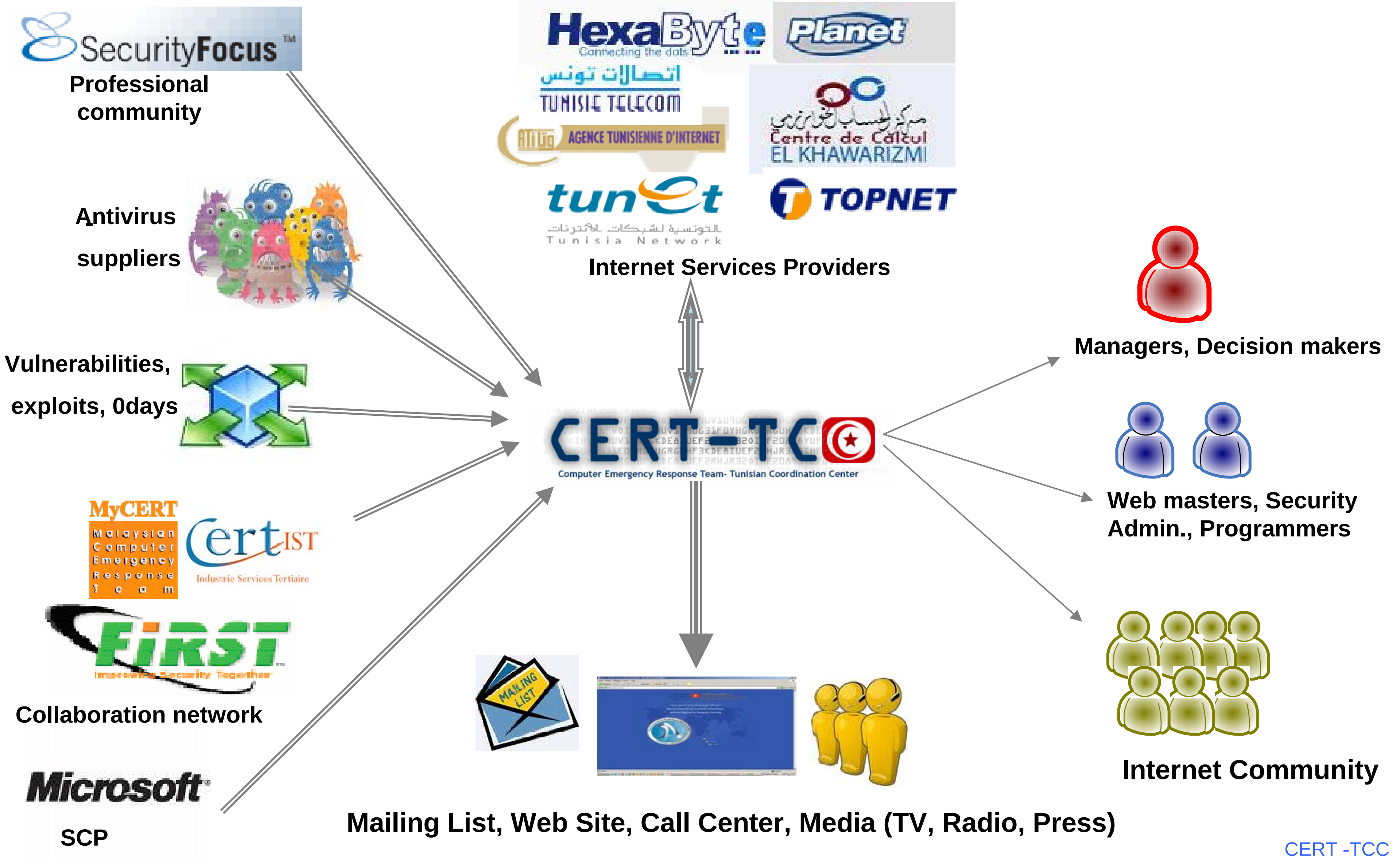
IBM

CISCO

hp invent

Equipments constructors

Warning & Information



Professional community

Antivirus suppliers

Vulnerabilities, exploits, 0days

Collaboration network

SCP

Internet Services Providers

Managers, Decision makers

Web masters, Security Admin., Programmers

Internet Community

Mailing List, Web Site, Call Center, Media (TV, Radio, Press)

SecurityFocus™
HexaByte
Connecting the dots
Planet
اتصالات تونس
TUNISIE TELECOM
ATI
AGENCE TUNISIENNE D'INTERNET
مركز الحساب الخوارزمي
Centre de Calcul EL KHAWARIZMI
tunet
الشبكة التونسية للإنترنات
Tunisia Network
TOPNET
CERT-TCC
Computer Emergency Response Team- Tunisian Coordination Center
MyCERT
Malaysian Computer Emergency Response Team
CertIST
Industrie Services Tertiaire
FIRST
Improving Security Together
Microsoft
MAILING LIST

Awareness

Oriented campaigns

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

Diversified contents

Prospectus

Posters

Emails

Radio Emission

Cartoon

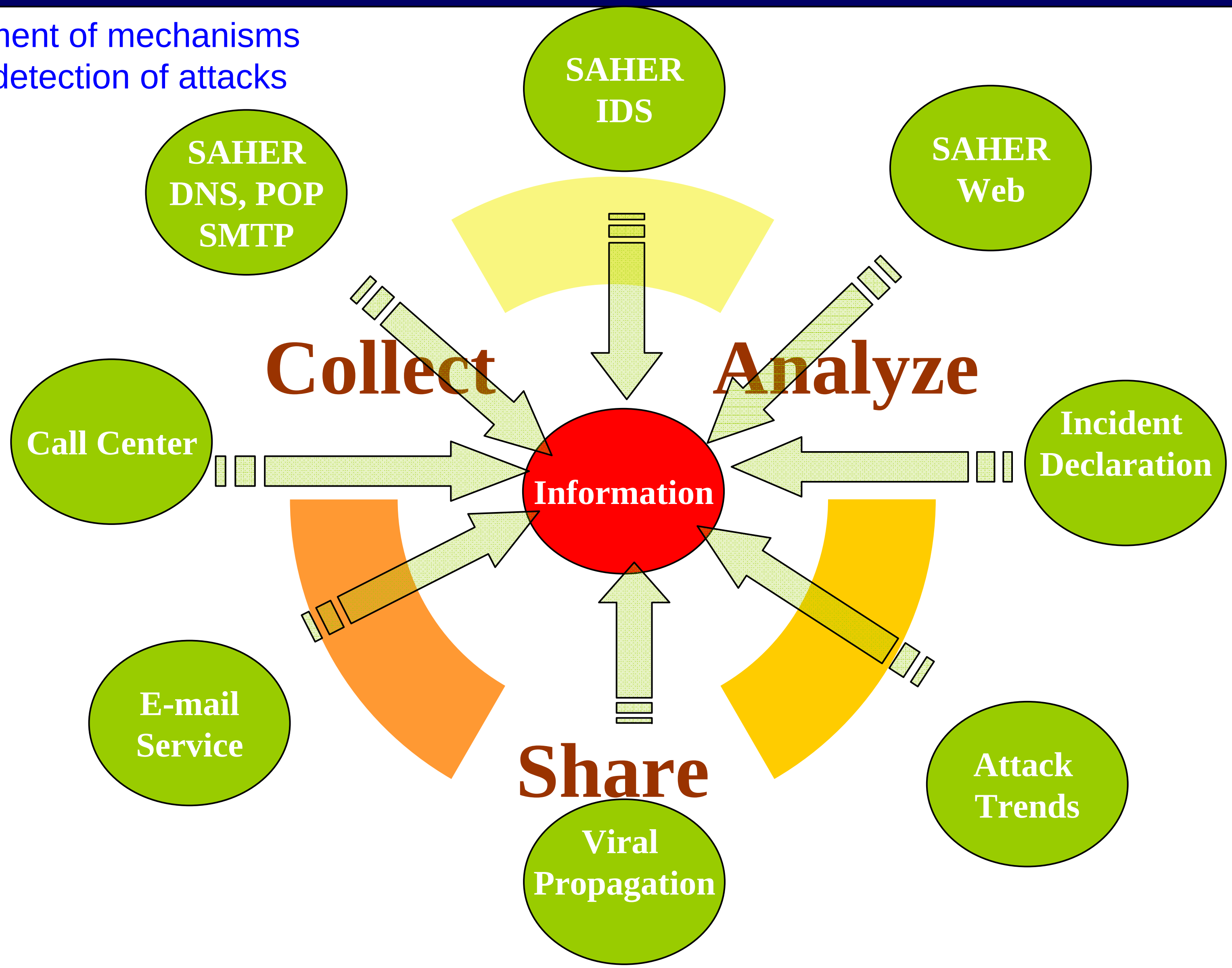
Video Spot

Attack Simulation

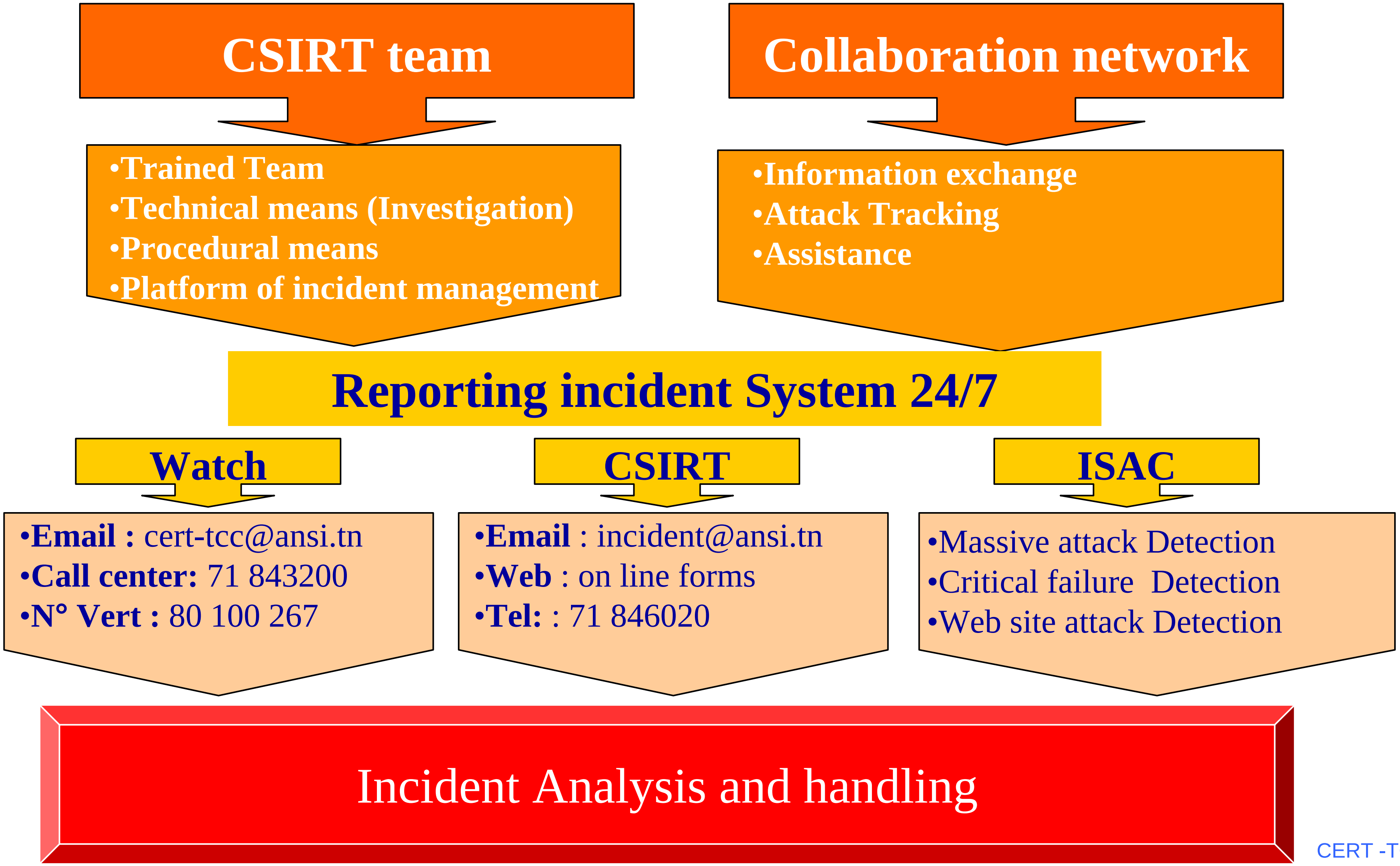
Guide

Information Share, Analysis & Collect (ISAC)

Development of mechanisms for early detection of attacks



Incident Handling (CSIRT)



CSIRT team

- Trained Team
- Technical means (Investigation)
- Procedural means
- Platform of incident management

Collaboration network

- Information exchange
- Attack Tracking
- Assistance

Reporting incident System 24/7

Watch

- **Email :** cert-tcc@ansi.tn
- **Call center:** 71 843200
- **N° Vert :** 80 100 267

CSIRT

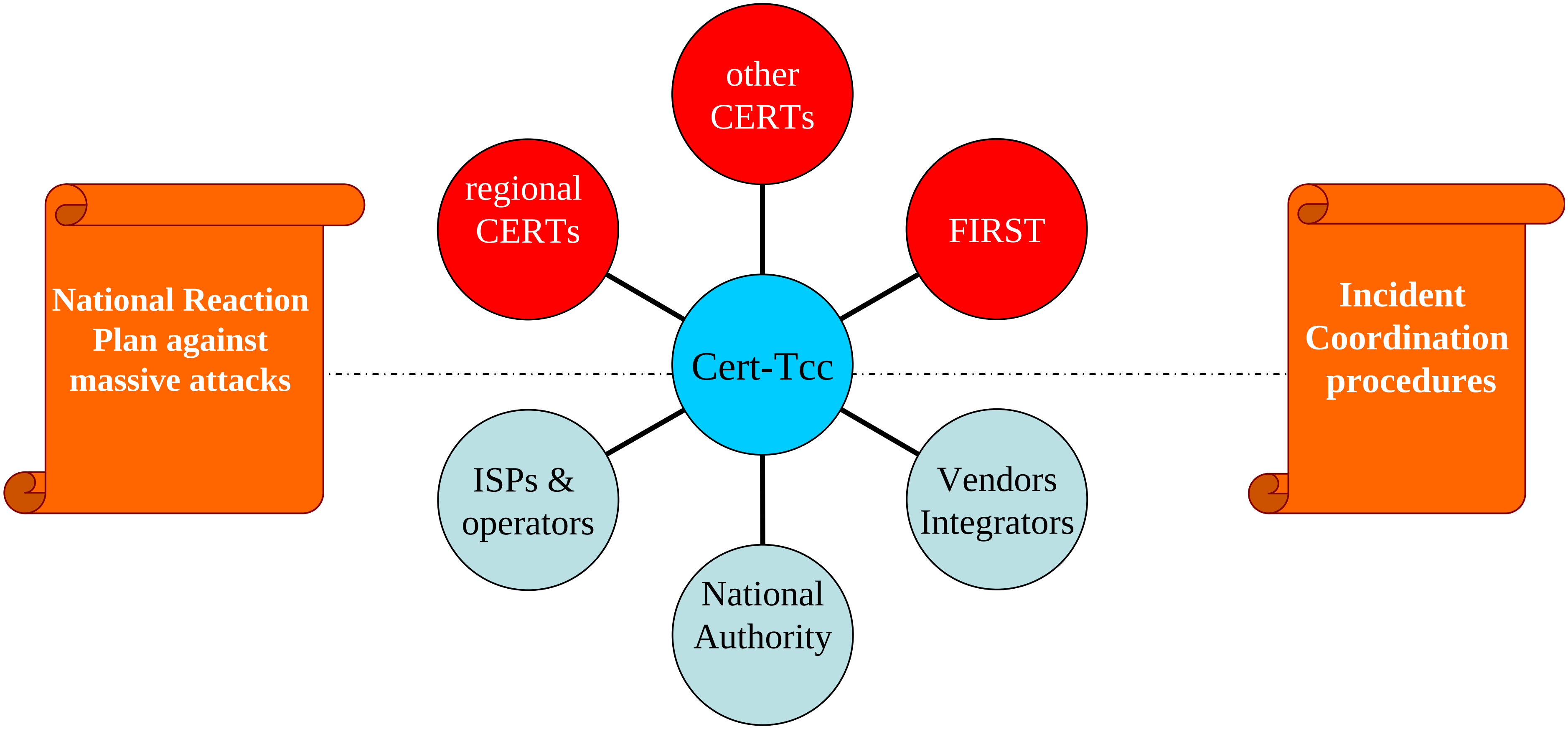
- **Email** : incident@ansi.tn
- **Web** : on line forms
- **Tel:** : 71 846020

ISAC

- Massive attack Detection
- Critical failure Detection
- Web site attack Detection

Incident Analysis and handling

Coordination



“Know-How” In IT security

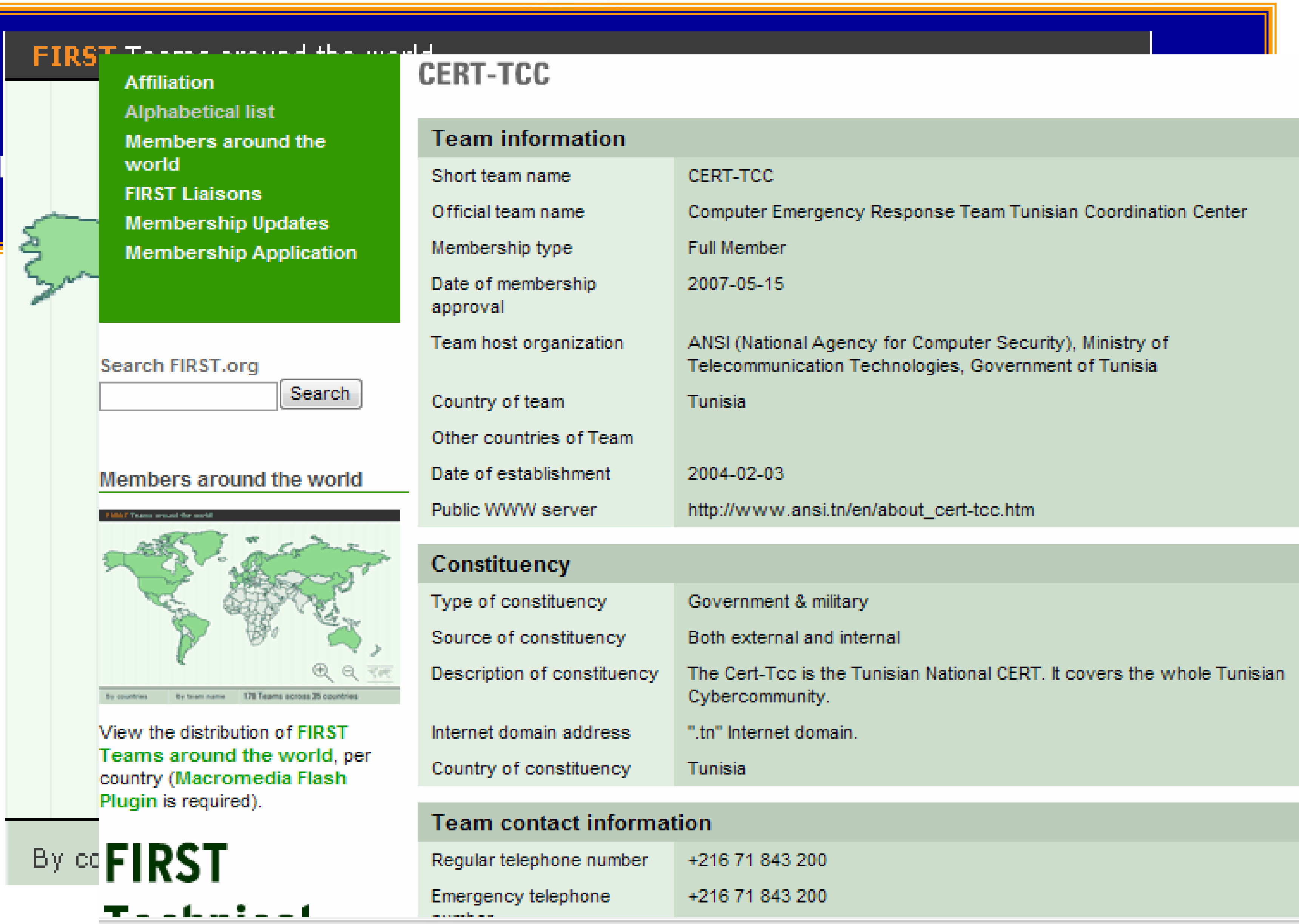
Reaching a relative technological autonomy :

- 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, …)

(Co



FIRST Teams around the world

- Affiliation
- Alphabetical list
- Members around the world
- FIRST Liaisons
- Membership Updates
- Membership Application

Search FIRST.org

Search

Members around the world

View the distribution of FIRST Teams around the world, per country (Macromedia Flash Plugin is required).

By co

FIRST Technical

CERT-TCC

Team information

Short team name	CERT-TCC
Official team name	Computer Emergency Response Team Tunisian Coordination Center
Membership type	Full Member
Date of membership approval	2007-05-15
Team host organization	ANSI (National Agency for Computer Security), Ministry of Telecommunication Technologies, Government of Tunisia
Country of team	Tunisia
Other countries of Team	
Date of establishment	2004-02-03
Public WWW server	http://www.ansi.tn/en/about_cert-tcc.htm

Constituency

Type of constituency	Government & military
Source of constituency	Both external and internal
Description of constituency	The Cert-Tcc is the Tunisian National CERT. It covers the whole Tunisian Cybercommunity.
Internet domain address	".tn" Internet domain.
Country of constituency	Tunisia

Team contact information

Regular telephone number	+216 71 843 200
Emergency telephone number	+216 71 843 200

Thank you for your attention