Tunis, Tunisia
04-05 June 2009

REGIONAL CYBERSECURITY FORUM 2009

International Telecommunication Union

Developing national CSIRT capabilities
"Tunisia's case"

Haythem EL MIR

Introduction

CERT-TCC is a CSIRT with national responsibility acting to provide incident management services for:

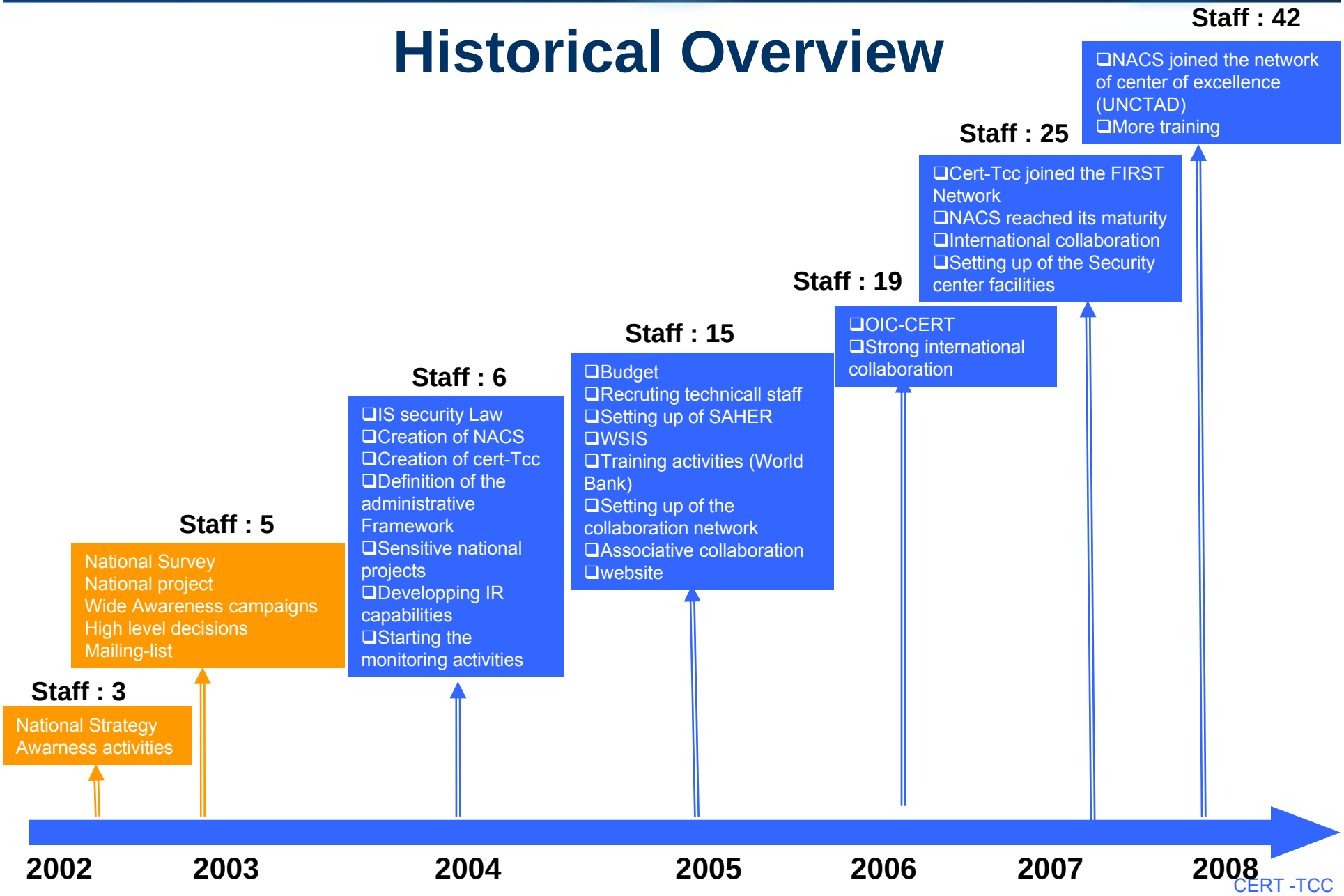
-Government
-Public and Private Sector
-Home users
-Professional
-Banks
-…

➔ Free charge services

The CERT-TCC tries to ensure:

- A centralized **coordination** for IT security issues (Trusted Point of Contact).
- Centralized and specialized unit for **incident response**.
- Technology and security **watch**
- Cyberspace **monitoring**
- The expertise to support and assist to quickly **recover** from security incidents.
- Awareness of all categories of users

Historical Overview



What do we need to set up a CSIRT?

1. Constitency : Define a clear relation
2. Define the mission statement
3. Financial model: Funding and revenue
4. Define list of services to run (Starting, intermidiate and maturity)
5. Poeple: mainly technical staff
6. Training: technical issues and others
7. Procedures: technical and organizational
8. Tools and equipements (Monitoring, IR, …)
9. Identify potential Parteners
10. Identify Source of information

We need also:

11. People motivation and dedicated to the project
12. Demonstrated a ROSI fo decision makers to take part of the project

Tunisian CERT presentation

Constituency	National CSIRT
Mission statementg	Defined by law : protection the Tunisian cyberspace
Offred Services	To be detailed
Funding	Gouvernement
Revenue	Free charge services
Number and quality of staff to be employed	50 for NACS 20 for cert-Tcc
Authority	Partial authority (Law N°5/2004)
Service hours	24/7

tunCERT Tunisian Computer Emergency ResponseTeam

Services

Mandatory service ➔ Incident handling

Core services ➔ Alerts and Warnings
Incident Handling
Incident analysis
Incident response support
Incident response coordination
Announcements

Service to provide ➔ According to the mission statement

Choose the right services : a decision based on the quality of services and feed-backs

1. **Starting phase : core services**
2. **Extension : additional phase**
3. **Maturity : extra services**

Services (According to the CERT/CC model)

Main services

Incident analysis	Incident response on site	Incident response support
Incident response coordination	Publish advisories or alerts	Vulnerability and Virus handling
Provide and answer a hotline	Monitor IDS	Training or security awareness
Technology watch or monitoring service	Track and trace intruders	Penetration testing

Secondary services

Security policy development	Produce technical documents	Vulnerability assessments
Artifact analysis	Forensics evidence collection	Pursue legal investigations
Vulnerability scanning	Security product development	Monitoring network and system logs

Staffing: Skills

Personal skills	Technical skills
Written communication	Security principals (CIA)
Oral communication	Security threats and vulnerabilities
Presentation skills	Internet technologies
Diplomacy	Risk assessement
Ability to follow policies and procedures	Network protocols
Team skills	Network application and services
Integrity	Network security issues
Knowing one's limits	System security issues
Coping with stress	Malicious code
Problem solving	Programming
Time management	Incident handling
	Local team policies and procedures
	Intrusion techniques
	Incident analysis

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

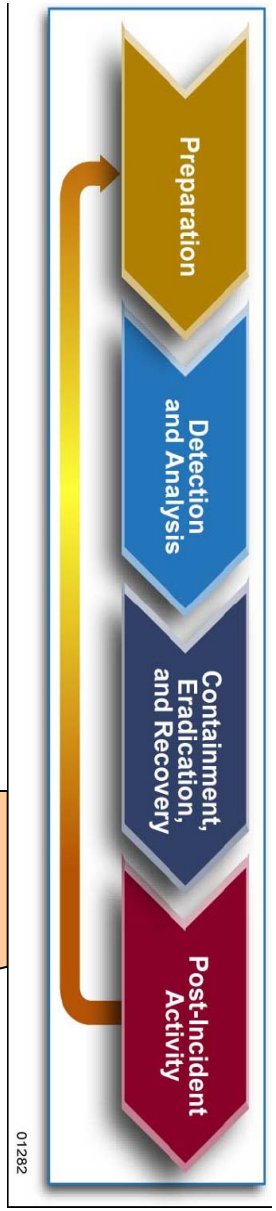
CSIRT

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

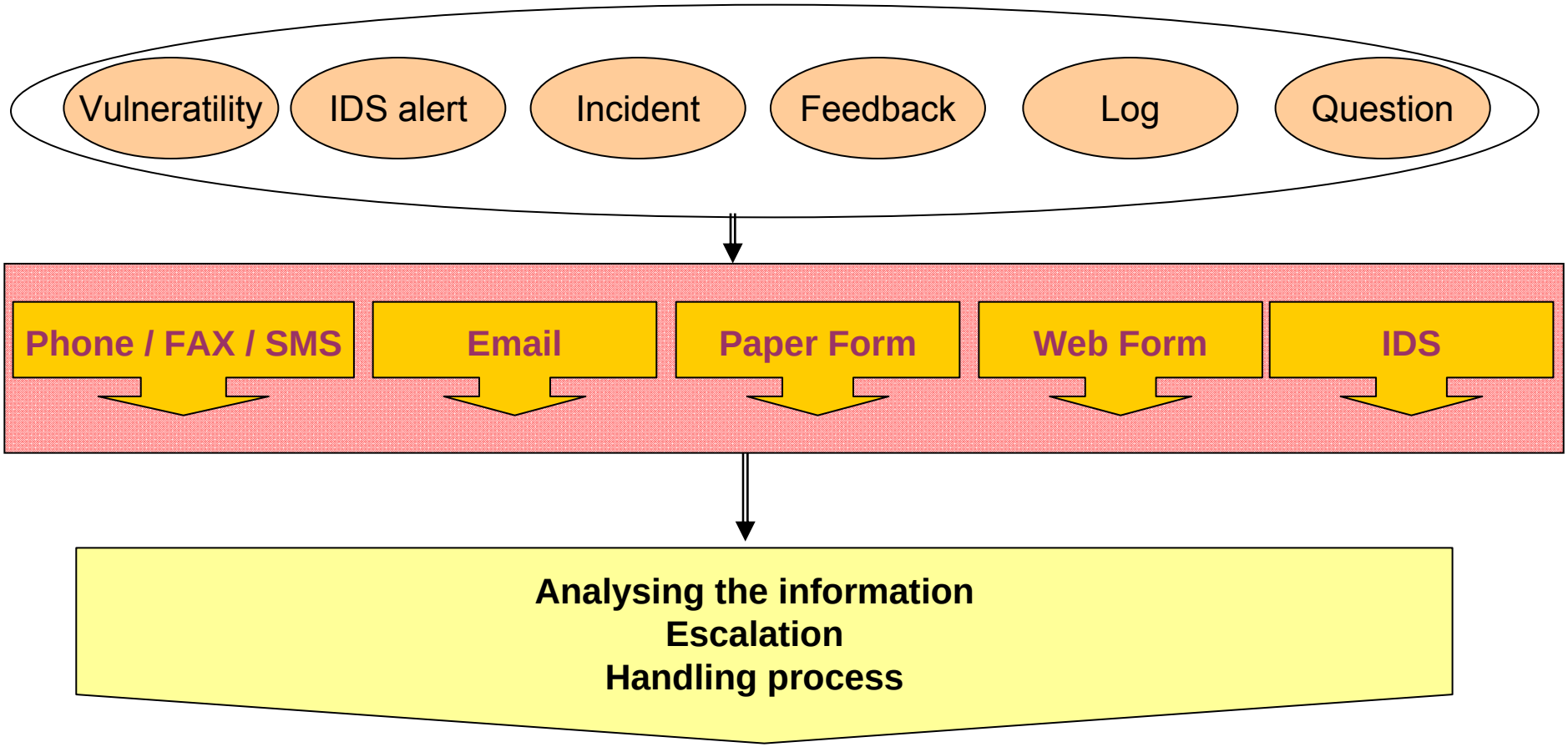
ISAC

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

Incident Analysis and handling



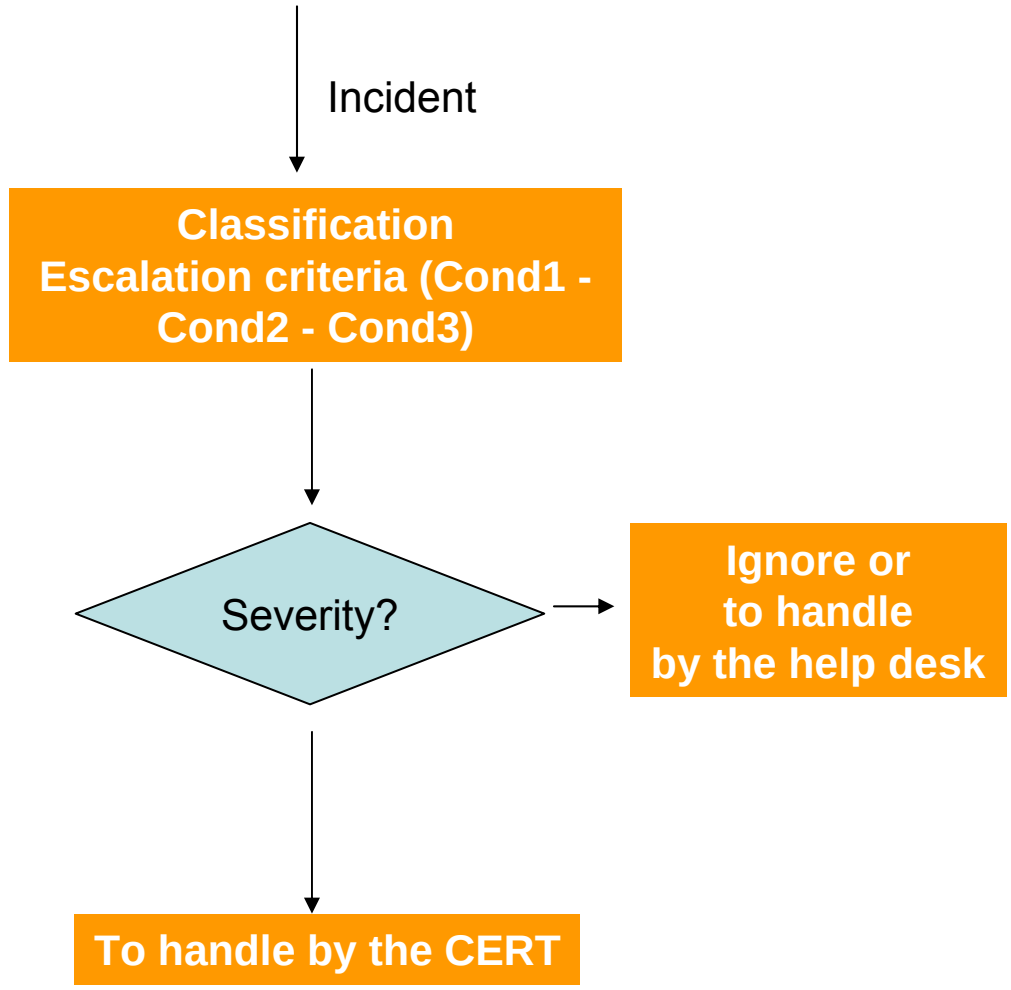
Reporting


Vulneratility
IDS alert
Incident
Feedback
Log
Question
Phone / FAX / SMS
Email
Paper Form
Web Form
IDS
Analysing the information
Escalation
Handling process

Types of Incident

Incident classification

Incident	Severity		
	Cond1	Cond2	Cond3
Spam	S1	S2	S2
Harassment	S2	S3	S3
Pedophilia/Pornography/Violence/..	S4	S4	S4
Malware (Virus, Warm, Trojan, Spyware, Dialer, Keylogger)	S1	S3	S4
Scan	S3	S4	S4
Sniff	S3	S4	S4
Social Engineering	S3	S3	S3
Vulnerability Exploit	S3	S4	S4
Brute Force	S3	S4	S4
Defacement	S2	S4	S5
DoS	S4	S5	S5
DDoS	S5	S5	S5
Sabotage	S3	S4	S4
Copyright	S2	S2	S2
Identity theft	S2	S3	S3
Phishing	S4	S5	S5



Incident handling operational procedures

- Incident reporting
- Ticket management
- Incident verification
- Incident classification
- Incident referencing
- Incident documentation
- Incident response termination
- Incident triage
- Specific incident response
- Document classification
- Data storage
- Data back-up
- Data destruction
- Documentary management
- Incident follow-up
- Incident report form
- Incident reporting guidelines
- Document templates

⟹

Spam
Harassment
Pedophilia/Pornography/Violence/.
Malware (Virus, Warm, Trojan, Spyware, Dialer, Keylogger)
Scan
Sniff
Social Engineering
Vulnerability Exploit
Brute Force
Defacement
DoS
DDoS
Sabotage
Copyright
Identity theft
Phishing

Tools

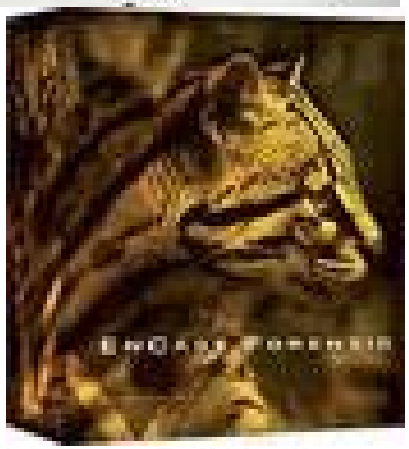
- Dedicated Server and network
- Incident tracking system
- Network analysis software
- Log analysis software
- Forensics tools :CD HELIX ; SYSINTERNELS, …
- Linux Livecd : BACKTRACK, PENTOO
- Data recovery tools
- Security scanner
- Integrity checker (HIDS)
- Vmware
- PGP
- …

•Hard drives, CD & DVD, Duplicators, Write blockers.
•Cables, connectors, etc.

National Agency for Computer Security

Ministry of Communication Technologies
Tunisia

Tools



Guidance SOFTWARE

Windows Sysinternals

Incident coordination

CSO / CIO

CEO

Internal business managers

Human Resources Department

Physical Security Department

Audit or Risk Management Department

IT or Telecommunications Department

Legal Department

Public Relations Department

Marketing Department

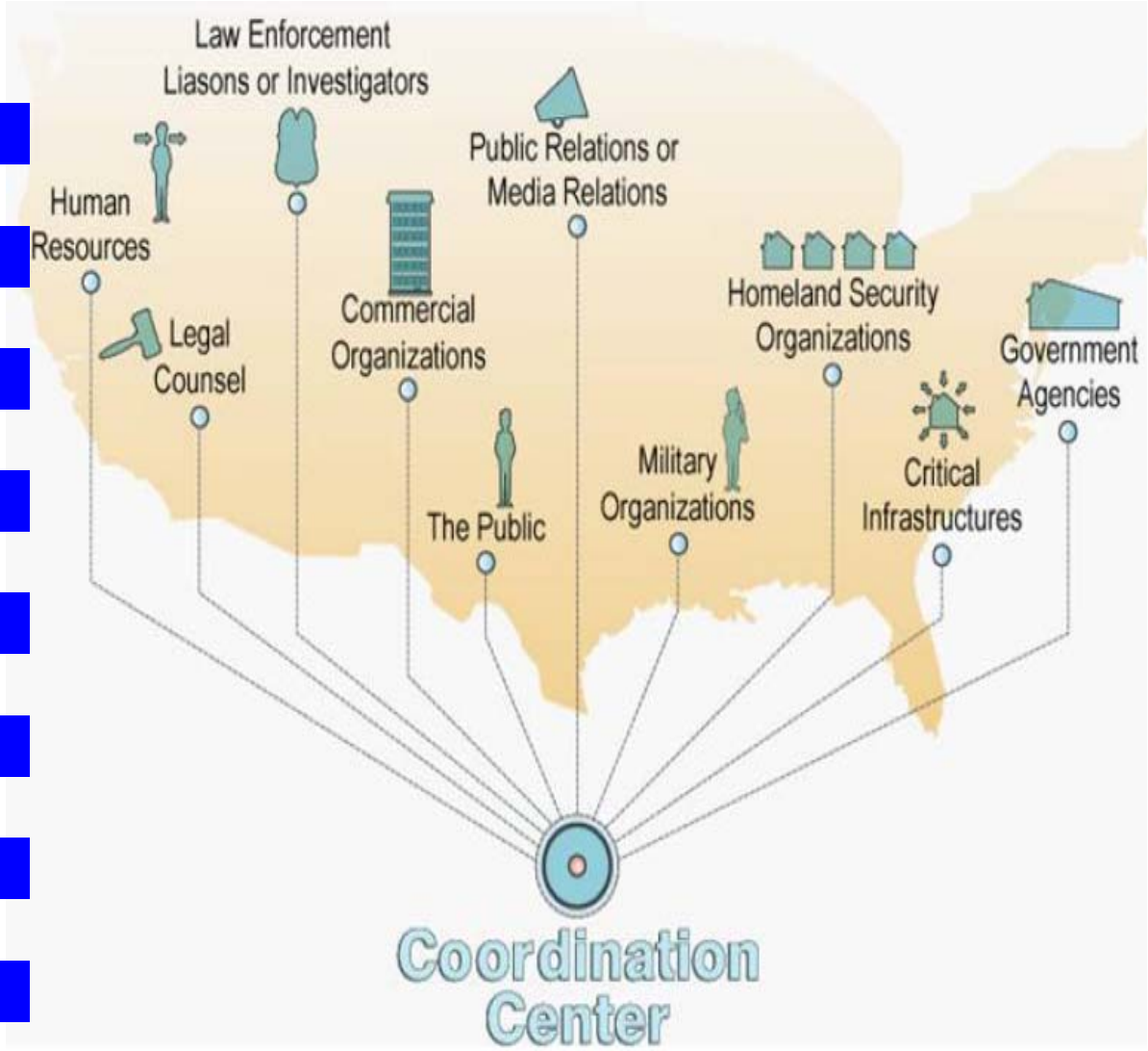
Law Enforcement

Government organization / agencies

Investigators

Other CERTs

Other security experts



Watch

Publication of vulnerabilities, exploits, 0days

Collaboration network

Antivirus suppliers

Collaboration program

Professional community

Collect information

Watch professionals

Trend indicators

Equipments constructors

Alert & warning process

Collect information

Vulnerability, Malware, Attack

Evaluation

- Identificatiuon
- Classification
- Risk assassment
- Impact analysis

Metric

Severity

Distribution

- Public website
- Closed member area on the website
- Mailing lists
- Personalised e-mail
- Phone / Fax
- SMS
- Monthly or annual reports
- Media

Home user
Professional
Customer
CSO
Manager
Webmaster
Programmer
Administrator
etc

Alert & Warning

SecurityFocus
Professional community

Antivirus suppliers

Vulnerabilities, exploits, 0days

MyCERT Malaysian Computer Emergency Response Team
CERTIST Industrie Services Tertiaire
FIRST Improving Security Together

Collaboration network

Microsoft
SCP

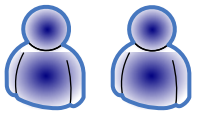
HexaByte Connecting the dots
Planet
اتصالات تونس TUNISIE TELECOM
ATI AGENCE TUNISIENNE D'INTERNET
مركز الحساب الخوارزمي Centre de Calcul EL KHAWARIZMI
tunet الشبكة التونسية للأنترنات Tunisia Network
TOPNET

Internet Services Providers

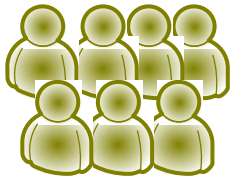
CERT-TCC
Computer Emergency Response Team- Tunisian Coordination Center

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

Managers, Decision makers

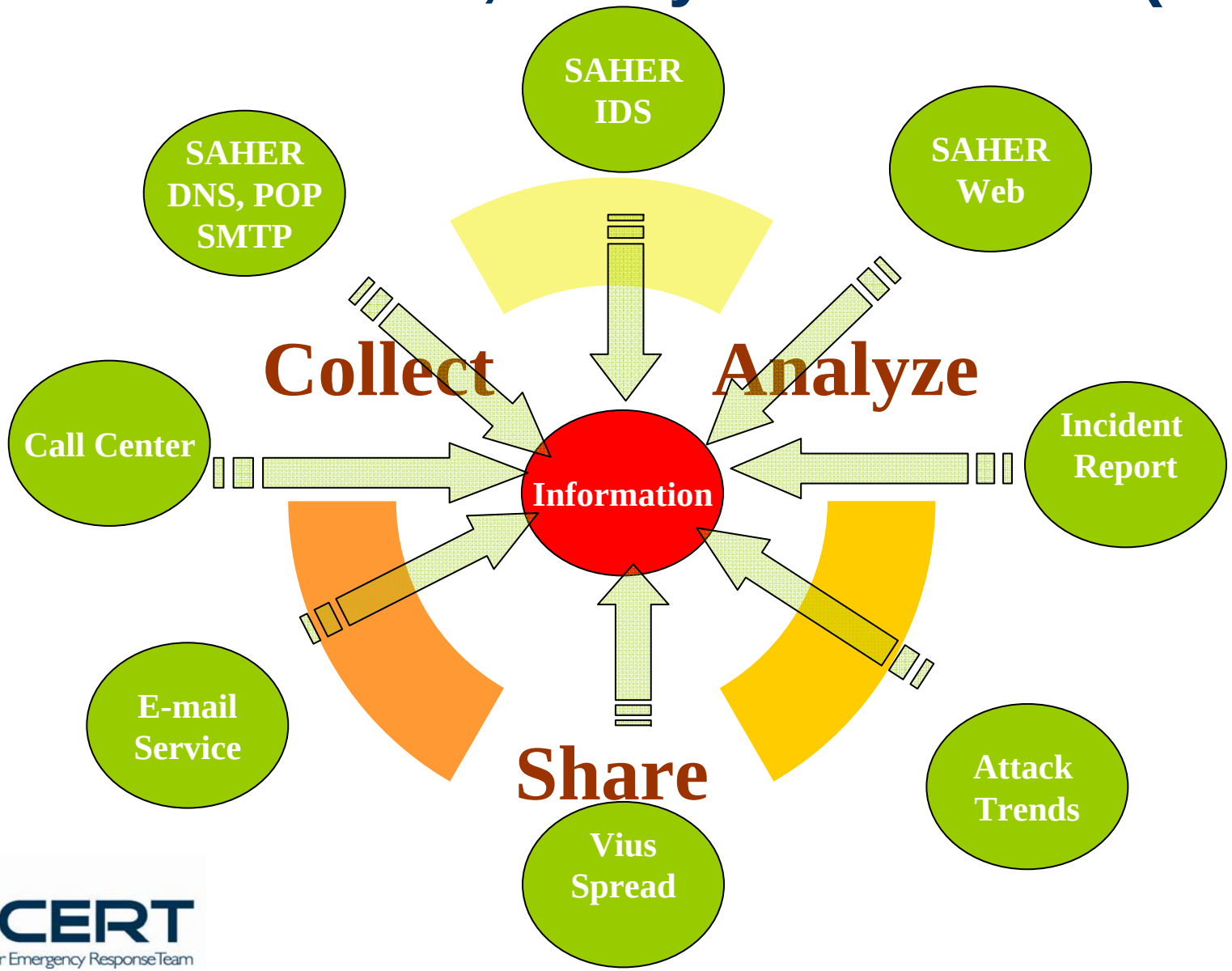


Web masters, Security Admin., Developers



Internet Community

Information Share, Analysis & Collect (ISAC)



tunCERT
Tunisian Computer Emergency ResponseTeam

SAHER System : main mission

Information sources

Monitoring System
ISPs & Data Centers

Call center
Incident declaration

CERTs alerts

Security Mailing-lists

Antivirus venders alerts

Software venders alerts

ISAC
SAHER

Identified events

Potential big Threats

Massive attacks

Virus spread

Botnets

Intrusions

Web defacement

System breakdown

tunCERT
Tunisian Computer Emergency ResponseTeam

SAHER : The technical platform

System developed based on a set of Open Source tools

Saher – Web: DotTN Web Sites monitoring

- Web defacement
- DoS Web
- Deterioration of web access
- …

Saher – SRV: Internet services availability monitoring (Mail server, DNS,…)

- Mail Bombing
- Breakdown of DNS servers
- DNS POISONING…

SAHER–IDS: Massive attack detection

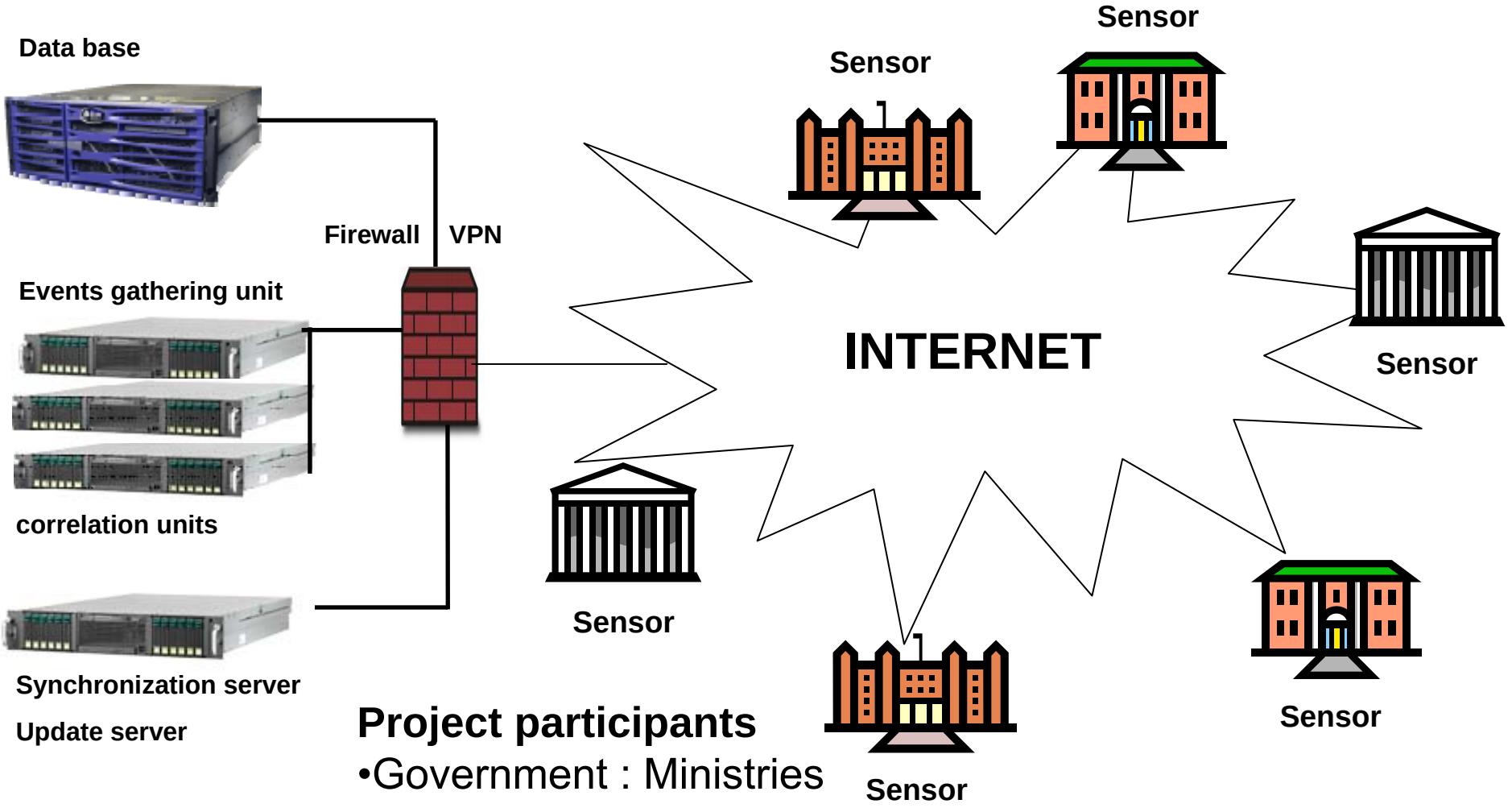
- Viral attack
- Intrusion
- DDoS
- …

SAHER–HONEYNET: Malware gathering

- Viral attack
- Scan
- Possible attacks

tunCERT Tunisian Computer Emergency ResponseTeam

SAHER-IDS : central node

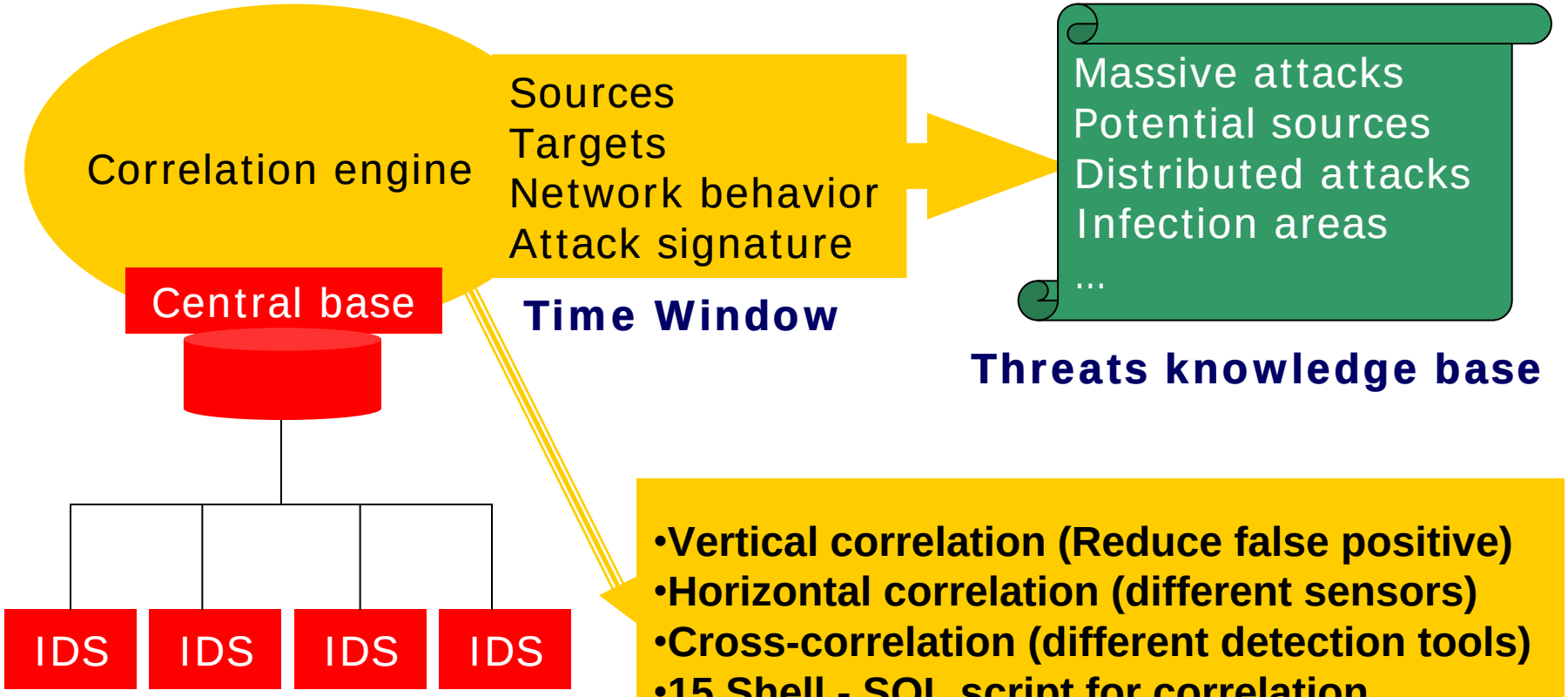


Project participants

- Government : Ministries
- Financial institutions : banks
- Health, Transport, Energy
- ISP : Private and public

tunCERT Tunisian Computer Emergency ResponseTeam

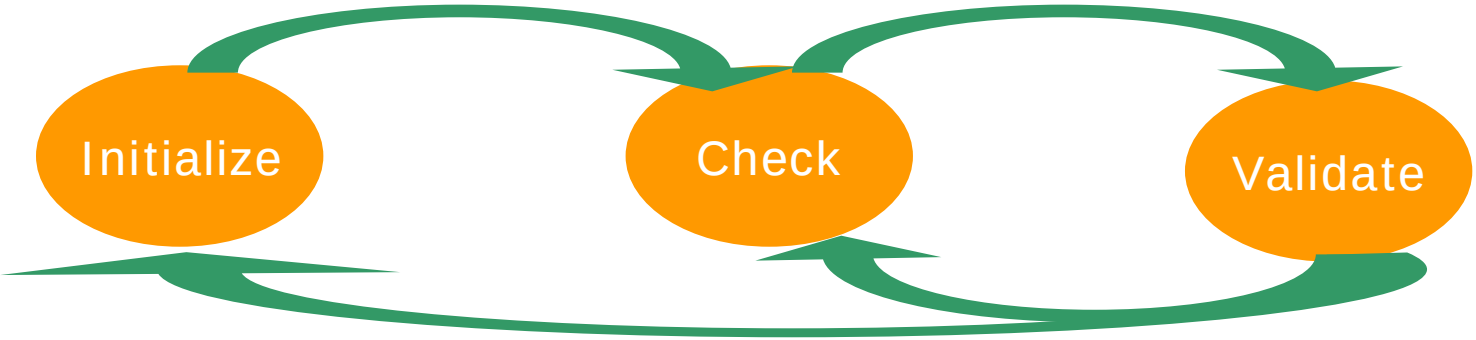
SAHER-IDS : Correlation



- **Vertical correlation (Reduce false positive)**
- **Horizontal correlation (different sensors)**
- **Cross-correlation (different detection tools)**
- **15 Shell - SQL script for correlation**

tunCERT Tunisian Computer Emergency ResponseTeam

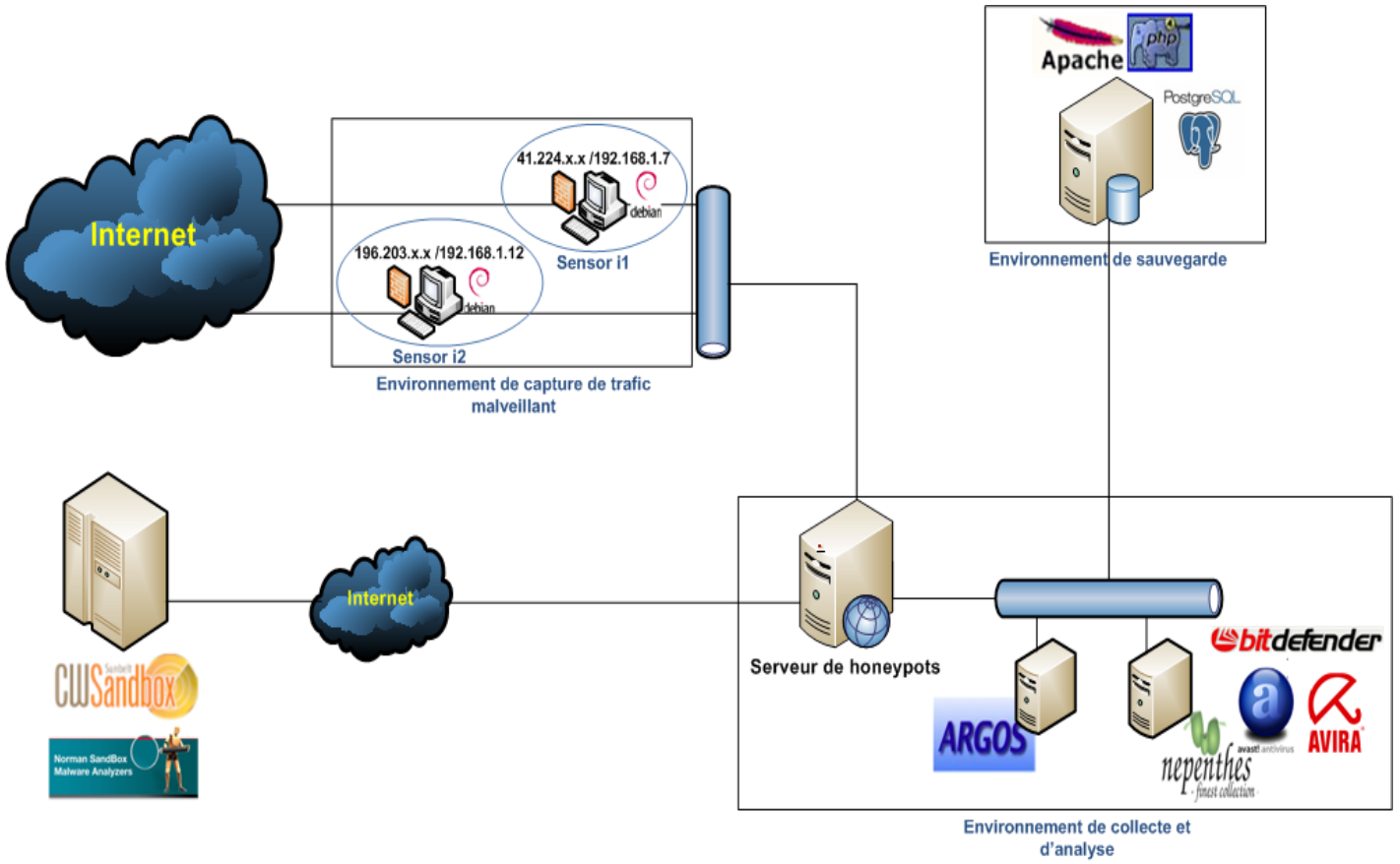
SAHER-Web : List of Tests



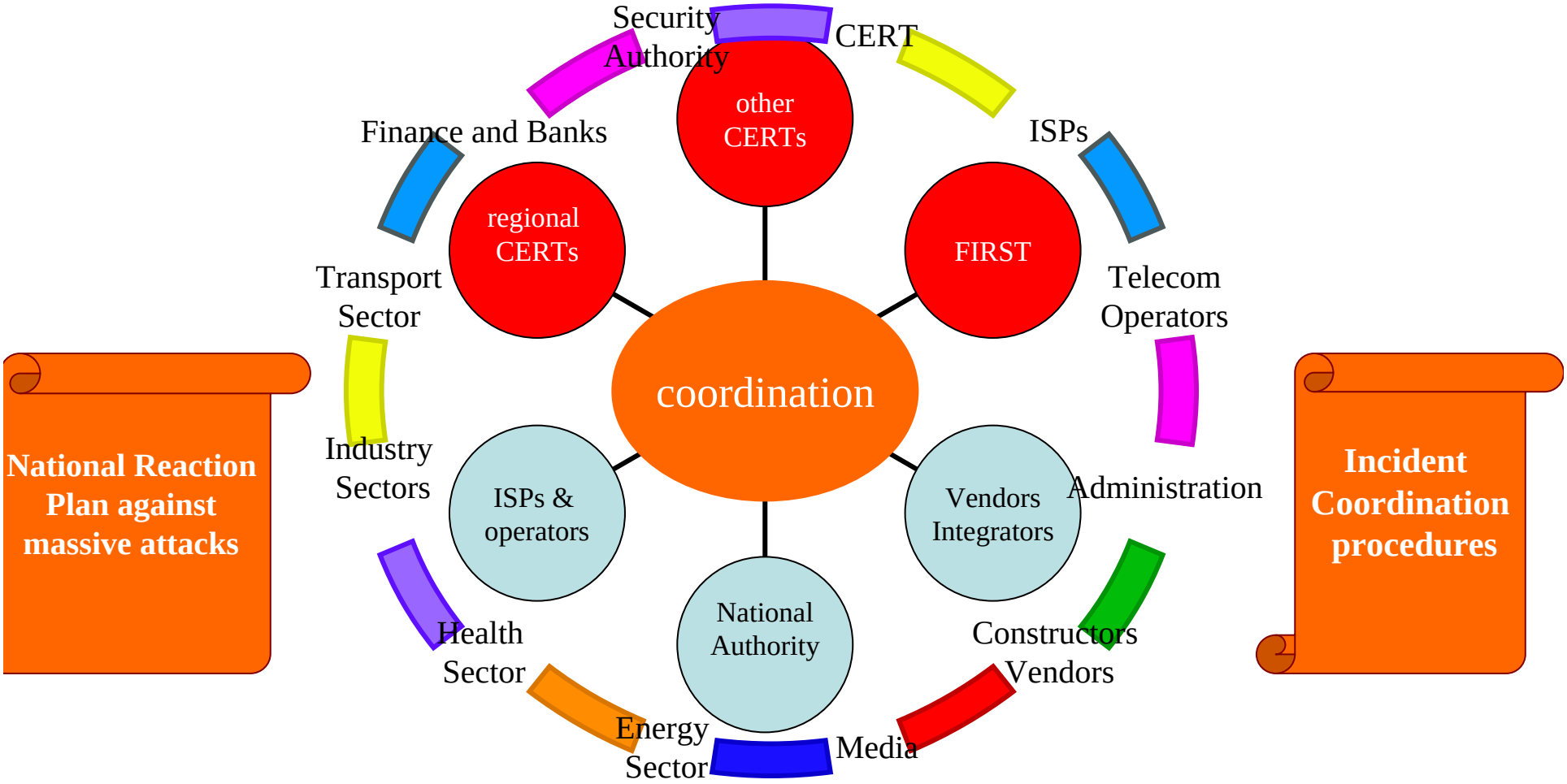
- Comparaison tests
  - Full/ Partial (dynamic sites)
  - Images : Full / Partial
  - Keyword analysis (Hacked, Defaced, Owned, Own3d, ….)
  - HTML code & Components size
- HTML to Image
  - Convert the web page to an image
  - Compares images to a threshold

Based on risk calculation algorithmes

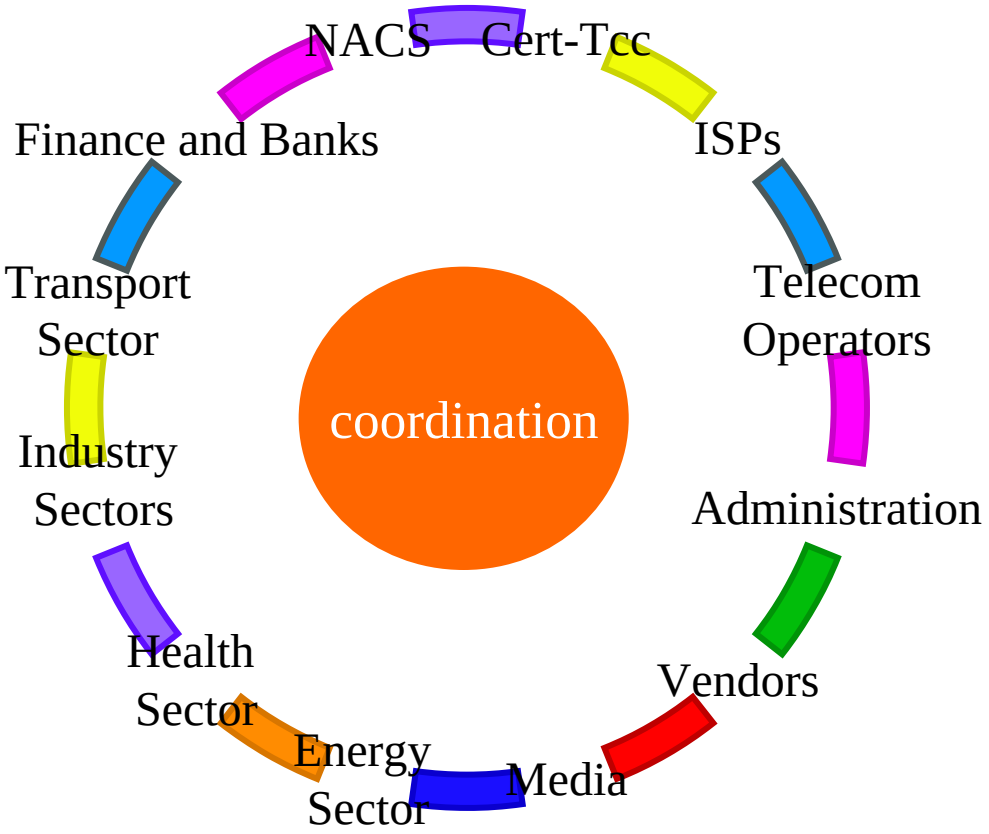
Saher-HoneyNet



National and international collaboration



National Reaction Plan



- "Formal" **Global** Reaction Plan.

- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Acess Providers).

With CERT/TCC acting as a **coordinator** between them

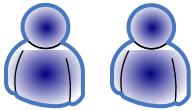
Deployed several times:

2004: African Football Cup
2004: 5+5 summit
2004: Sasser & MyDoom worms
2004: Presidential election
2005: Suspicious hacking activity 2005
2005: WSIS
2005: Arab League
2006 : Hand Ball World Cup
2009: Conficker

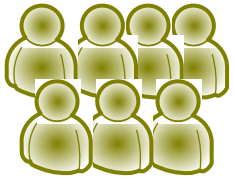
tunCERT Tunisian Computer Emergency ResponseTeam

Awareness

+ **Decision makers**
+ **Professionals**
+ **Teachers**



+ **Students**
+ **Home users**
+ **Journalists**



+ **Lawyers**
+ **Customers**

Awareness material

Flyers | Posters | Emails

Radio Emission | Cartoon | Video Spot

Attack Simulation | Guide

Awareness

Various content

- □ Applying operating patches/updates
- □ Antivirus software and updates
- □ Protecting sensitive personal and proprietary information
- □ Phishing and identity theft
- □ Spywares and Trojans
- □ Software copyright and license compliance
- □ Spam
- □ Business continuity
- □ Physical security
- □ Security policies, standards, procedures, laws and/or regulations

- ➢ **Seminar**
- ➢ **Conference**
- ➢ **Exhibition**
- ➢ **Training**
- ➢ **National event**
- ➢ **Media**
- ➢ **Web**
- ➢ **Mailing-list**

Chocking : Attack simulation

+ **Decision makers**
+ **Professionals**
+ **Teachers**
+ **Students**
+ **Home users**
+ **Journalists**
+ **Lawyers**

Trojans horse attack

Remote intrusion

Vulnerability Exploits

Phishing attacks

XSS

SQL Injection

Password and email Sniff

Password cracking

CMS hacking

Wi-fi hacking

Session hijacking

Web defacement

Awareness

- *Content development*
- *Media information (Radio, TV)*
- *Seminars (Presentations)*

Weekly participation in 8 National Radios

+Saturday night on KNET

4 cdroms

8 booklets

tunCERT
Tunisian Computer Emergency ResponseTeam

National Projects

- ✓AMEN
- ✓CNI
  - -E-Government
  - -Madania, ADEB, INSAF
  - -National Backup-Center
- ✓E- (Justice, health, handicap, ...)
- ✓CNSS, CNRPS, CNAM
- ✓LA POSTE (e-dinar)
- ✓EDUNET
- ✓CCK
  - -Orientation
  - -Inscription
  - -Student portal
- ✓Sector CSIRT (Postal Service: La Poste, Telecom Operator: Tunisie Telecom, Banks: APB)
- ✓Banks projects

Training

- ✓Awareness Training
  - ✓Children and parents
  - ✓Home users
- ✓Professional
  - ✓Hacking techniques
  - ✓Security management
  - ✓Security audit : Standards and methods
  - ✓Risk assessment
  - ✓Network security : risk and solutions
  - ✓Open source solution for network security
  - ✓Linux security
  - ✓Windows security
  - ✓Application security
  - ✓Web application security
  - ✓Access control requirements and techniques
  - ✓Introduction to cryptography
  - ✓Communication encryption
  - ✓Business continuity & disaster recovery
  - ✓Incident handling & computer forensics
  - ✓Vulnerability assessment and Pentesting

Development of policies and guides

- ✓Government security policy
- ✓E-Government security charter
- ✓Security Audit requirement guides
- ✓Commercial security solution specification models
- ✓Best practices (IIS, Apache, CISCO, ...)
- ✓Security audit guidelines
- ✓Vulnerability assessment methodology
- ✓Penetration test methodology
- ✓Open source security tools guides

Key points of the Tunisian experience

- Defined strategy with clear objectives
- Having the power of law and the high level support
- Limited resources (Adopting a low cost approach: open source)
- Making the awareness as one the first priorities
- Improving Training and education
- Relying on local capacities
- Relying on the collaboration with national partners (All sectors) and ensuring PPP
- Providing free technical support (Incident management capabilities)

Experience Sharing

- Experience sharing with others courtiers to set-up security center using the same approach:
  - 2007: Rwanda (Experience Sharing)
  - 2008: Senegal (Training)
  - 2008: Center of Excellence with UNCTAD
  - 2009: South Africa (ECS-CSIRT)
- OIC-CERT
- CERT-AFRICA

Conclusion : problems and challenges

Problems come from:

- Taking on too many services
- Lack of time, staff and funding
- Coordination
- Constituency support
- Incident reporting

Challenges:

- Automatic incident handling process
- Automatic vulnerability handling process
- Deploying efficient sources of information
- Collaborate and share information with others
- Set-up trusted way for data exchange
- Integration between processes

Issues:

- Return on investment
- Certification / Recognition
- Legal issues
- Data sharing
- CERT tools

National Agency for Computer Security

Ministry of Communication Technologies
Tunisia

Thank you

haythem.elmir@ansi.tn