Vers un écosystème numérique de confiance

retour d'expérience- cas de la Tunisie

Prof. Belhassen ZOUARI,
Cybersécurité, Gouvernance TIC
SupCom, Univ. de Carthage, Tunisie
DG de l'ANSI- tunCERT (2007-2011)

FFGI
Ouagadougou, août 2019

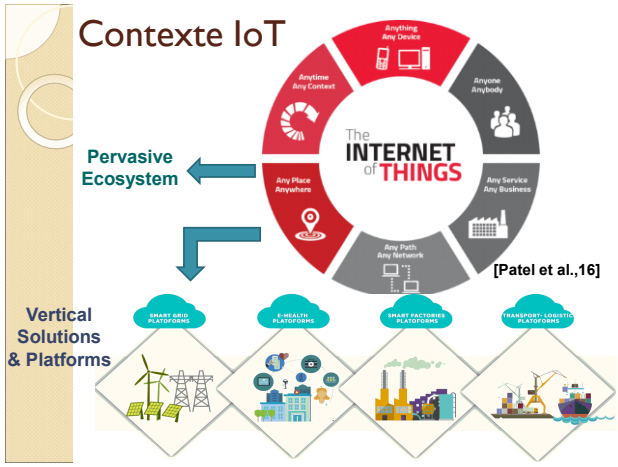
Constat & tendances

Un monde de plus en plus connecté

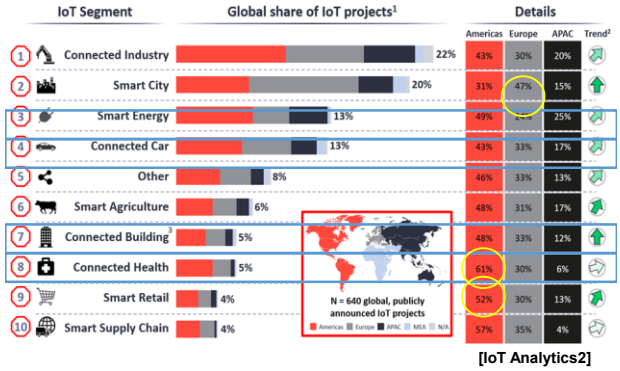
- e-gov, e-commerce, domotique, IoT, …
- Activités sociales & culturelles en ligne
- Tous les secteurs économiques concernés
  (industrie, distribution, agriculture, …)
- Convergence vers TCP/IP
  Internet of Things (IoT)

vers un écosystème IoT interopérable et sécurisé

Contexte IoT



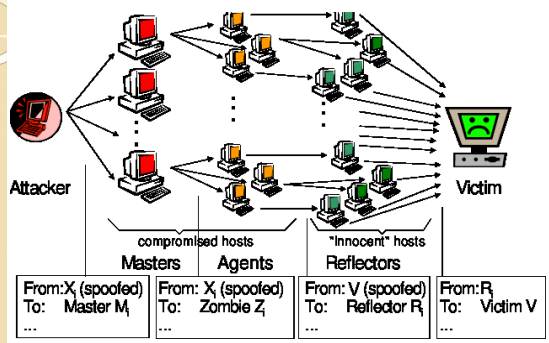
Domaines d'application IoT



Menaces émergentes

- DDoS, Stuxnet : Cyberguerre
- MIRAI : les IoT s'y mêlent !
- WanaCry / WanaCrypt (Ransomware): Cybercrime, Darkweb

DDoS attack- principe



DDoS attack- Historique

Historique:

1ere grande attaque DDoS février 2000, (Mafiaboy) le 7 février :

- Yahoo! et inaccessible pendant 3 h,
- Amazon.com, Buy.com, CNN et eBay ont été touchés par des attaques DDoS, E-Trade et ZDNet (le 8 février 2000)

Pertes:

Yahoo : environ 500 000 dollars.
Amazon : environ 600 000 dollars. en 10 h

- Michael Calce (Mafiaboy,15 ans) condamné à 8 mois dans un centre de détention pour jeune,

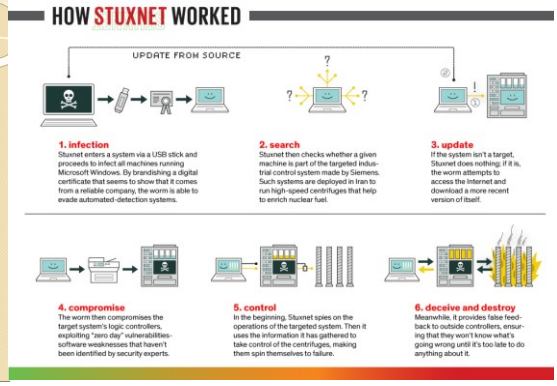
Stuxnet

découvert en 2010,

Virus, 1er de sa génération

- conçu par la NSA en collaboration avec l'unité israélienne 8200
- Objectif : attaquer les centrifugeuses iraniennes d'enrichissement d'Uranium
- cible les systèmes SCADA utilisés pour le contrôle commande de procédés industriels. Stuxnet a la capacité de reprogrammer des automates programmables industriels (API) produits par Siemens

Stuxnet : comment ça fonctionne



MIRAI ?

Attaque DDoS & IoT

MIRAI Botnet : octobre 2016

- Botnet de "devices" IP (caméras, imprimantes, modems, …) lançant un DDoS sur le serveur DNS du FSI Dyn,
- flux de 1 To/s entrainant la chute du serveur DNS et provoquant l'indisponibilité des services clients Twitter, the Guardian, Netflix, Reddit, CNN, …
- malware MIRAI sur ordinateurs infectés cherche des devices vulnérables (utilisant login/pwd par défaut) et génère un flood DNS sur Dyn

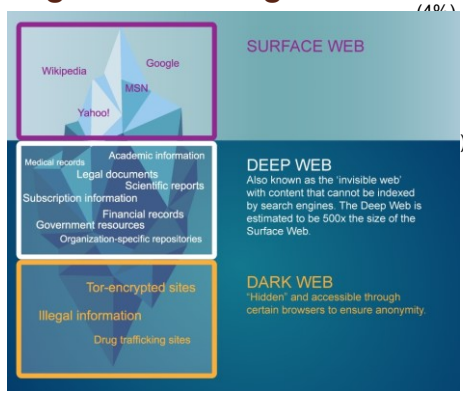
WanaCry / WanaCrypt

Ransomware : mai 2017

- a touché +300 000 ordinateurs, dans +150 pays,
- considérée comme le plus grand piratage à rançon de l'histoire d'Internet, …
- Chiffrement ; clé contre rançon

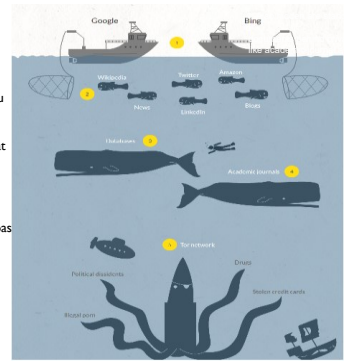
Dark Nets Web Deep Surface

Les étages de l'Iceberg



L'Octopus

1. Les résultats de recherche des moteurs classiques, scrutent les liens et les pages web indexées
2. Ils ne récoltent que 1% du contenu du Web
3. Les SGBD ne livrent que le résultat d'une requête. Le reste de la BD n'est pas indexé forcément
4. Les pages des réseaux privés, les documents académiques ne sont pas forcément indexés
5. La partie la plus cachée est Tor
6. On y accède avec des logiciels assurant l'Anonymat



Source: CNNMoney, accessed 10/05/17

Darknets & DarkWeb

Anonymisation : par exple TOR

Qu'offre t-il:

- Marchandises illicites (drogues, armes, …)
- Places de marchés parallèles
- Forums
- Services illicites

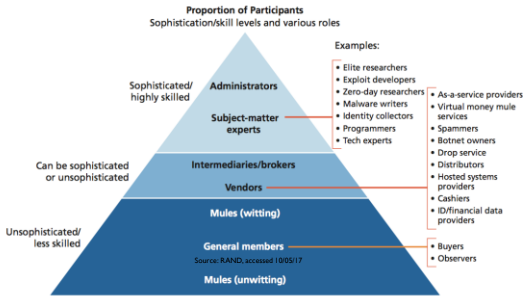
Le Business Model du Cybercrime

- L'économie souterraine « Underground » est organisée et structurée pour favoriser le crime
- **Crime-as-a-Service** (CaaS)

E.g. Ransomware-as-a-Service (RaaS)

Image Source: http://about-threats.trendmicro.com/us/infographic/images/Cybercriminal%20Underground-

Différents niveaux des acteurs du marché Underground



A quoi sert la Cybersécurité ?

doit répondre à un besoin et apporter

- de l'efficacité : Rapidité, Performance
- de la fiabilité : Qualité, Sécurité
- du gain : Coût, Délai

Prérequis pour créer la confiance dans l'usage des e-services

→ Climat de confiance

→ Adhésion de l'usager

Freins, difficultés

Problèmes de Gouvernance :

- décideurs / politiques non sensibilisés
- Absence de vision stratégique
- Savoir-faire non maîtrisé

Cybersécurité : comment réussir ?

- doit être adressée globalement
- Les décideurs/politiques doivent
  - définir une stratégie nationale en cybersécurité
  - fournir les ressources nécessaires à son implémentation

Principes à admettre

Approche technologique : insuffisante !

- Principe 1 :

  le Risque Zéro n'existe pas, mais on doit travailler à le minimiser et à limiter l'impact

  → Approche « Management du Risque »

- Principe 2 :

  la sécurité est une chaîne dont la force est celle de son maillon le plus faible

  → **Approche globale** de la sécurité

Les 3 Piliers de la sécurité des SI

la réussite d'un **processus** de **sécurisation** repose sur **3 piliers** :

- Technologie
  outils TIC/Sécurité, etc.
- Méthodologie/Management
  stratégies, procédures, réglementation, etc.
- Comportement social
  Culture de la Cyber sécurité

Le SMSI : une approche globale

Système de **M**anagement de la **S**écurité de l'**I**nformation

Modèle à suivre : Modèle PDCA de l'ISO 27001

Plan : établir les objectifs conformément risques/ exigences (correspondances objectifs / lignes directrices)

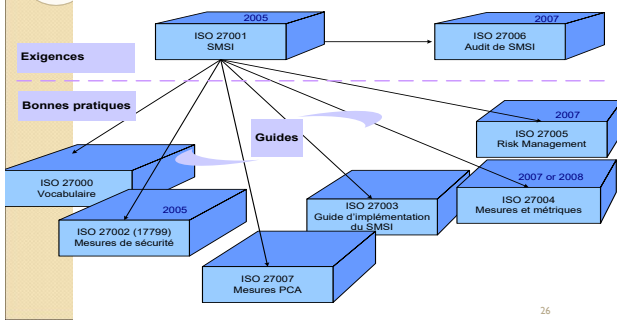
Do : implémenter et opérer les fonctionn procédures

Check : gérer les incidents, les erreurs, au

Act : faire évoluer la politique et les moyer conformément aux besoins

25

La famille des normes ISO 2700x



26

CERT … CSIRT

- CERT/CSIRT : Computer Emergency Response Team (Computer Security Incident Response Team)

- CERTs Gouvernementaux / Agences
  - Technologies de la Communication /Autorité de régulation
  - Intelligence / Défense
  - Police

- CERTs spécialisés
  - Finance / Opérateurs Telecom / Administration / etc.

Eléments d'une stratégie nationale

- Définir un cadre légal pour la cybersécurité
- Protéger le cyber-espace
- Formation
- R & D (maîtrise de la technologie)
- Sensibilisation
- Coopération internationale
- Création de mécanismes d'exécution et d'implémentation (Agences, CERTs, Task force, ...)

Cadre légal pour la cybersécurité

- Besoin d'un cadre légal
- Clarification des "cyber" concepts (crime, preuve, etc.)
- Quelles institutions, quelles Responsabilités ?
- Mesures opérationelles et rôle des CERTs
- Aspects pratiques & Application
- coopération internationale

Outils d'implémentation

- Mise en place de CERT/CSIRT (s)

- Objectifs → Scope & Role ?
  - Gouvernemental
    - (administration, Intelligence / Défense, Police, …)
  - Privé
    - (Finance, télécom, …)

Le rôle d'un CERT

- Fournir une réponse immédiate et efficace à un incident cybernétique
- Préparer les institutions / clients concernés à mieux gérer et traiter les cyber-menances

Missions d'un CERT

- Détection et Réponse aux incidents
- Veille & Alerte
- Gestion des incidents
- Analyse des incidents
- Investigation numérique
- Sensibilisation
- Coopération (nationale & internationale)

Services (According to the CERT/CC model, the US CERT)

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

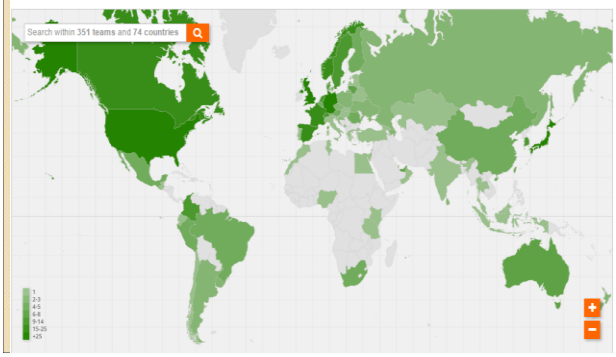
Security policy development	Produce technical documents	Vulnerability assessments
Artifact analysis	Forensics evidence collection	Pursue legal investigations
Vulnerability scanning	Security product development	Monitoring network and system logs

World situation (2010) source www.first.org

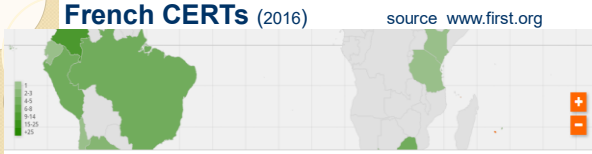
- Need for operational Cybersecurity Centers (CERTs)!

World situation (2016) source www.first.org

Members around the world



French CERTs (2016) source www.first.org

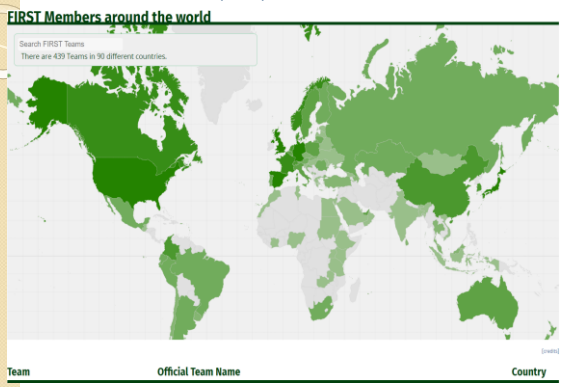


Search results for: France *(10 teams)*

Team name	Official Team name	Country
AlliaCERT	Alliacom Computer Emergency Response Team	
CERT SG	CERT Societe Generale	
CERT-AG	CERT Credit Agricole	
CERT-FR	CERT-FR	
Cert-IST	CERT France Industries, Services & Tertiaire	
CERT-LEXSI	CERT-LEXSI	
CERT-Renater	CERT-Renater	
CSIRT BNP Paribas	Corporate Security Incident Response Team BNP Paribas	
ISIRT	INTERPOL INFORMATION SECURITY INCIDENT RESPONSE	
Orange-CERT-CC	Orange-CERT Coordination Center	

World situation (2018)

source www.first.org



World situation (2019)

source www.first.org

L'expérience tunisienne :

Stratégie en Cyber Security & *tun*CERT

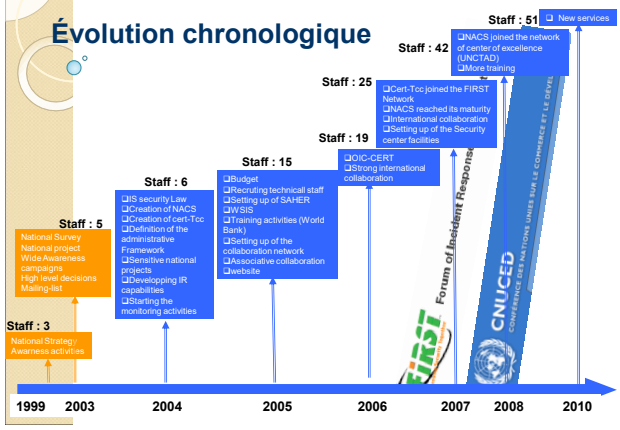
Objectif Général:

élever le niveau de sécurité des SI tunisiens.

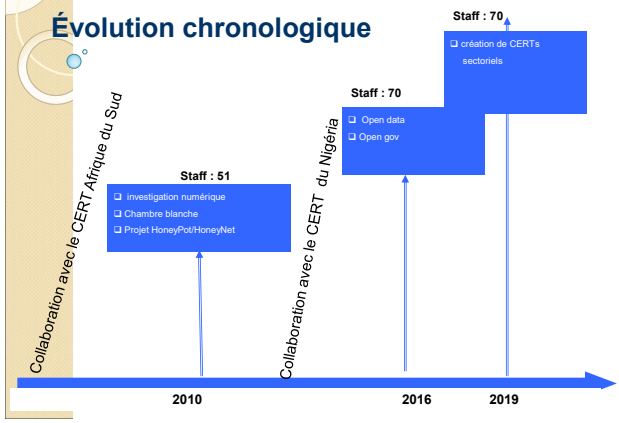
Axes principaux :

- Mise à jour du cadre légal
- Mise en place des outils opérationnels pour évaluer et suivre le processus de sécurisation des SI d'institutions (publics & privés) → obligation d'audit sécurité
- Protection du cyber-espace national (Coordination, Assistance, etc.)
- Développement du "know-how" en IT Security (formation, R&D, capacités open source)
- Sensibilisation

Évolution chronologique



Évolution chronologique

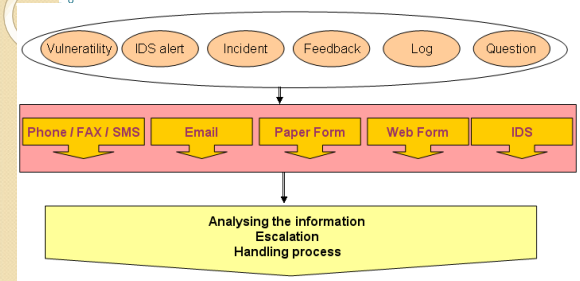


Caractéristiques

Constituency	National CSIRT
Mission statement	Defined by law : protection of the Tunisian cyberspace
Offered Services	To be detailed
Funding	Government
Revenue	Free charge services
Number & quality of employed staff	50 for NACS 20 for tunCERT
Authority	Partial authority (Law n° 5/2004)
Service hours	24/7

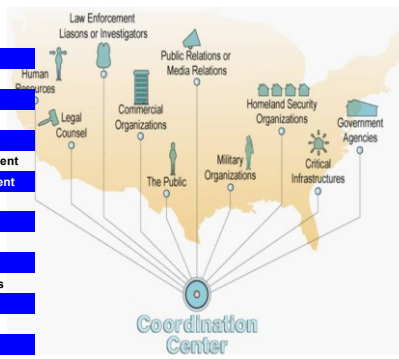
Gestion d'incidents (Incident Handling)

Reporting

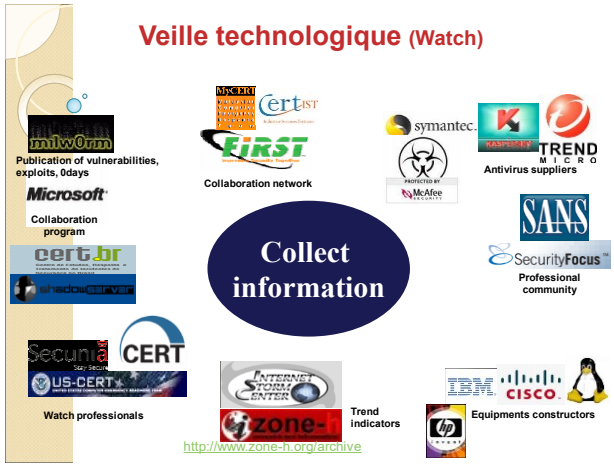


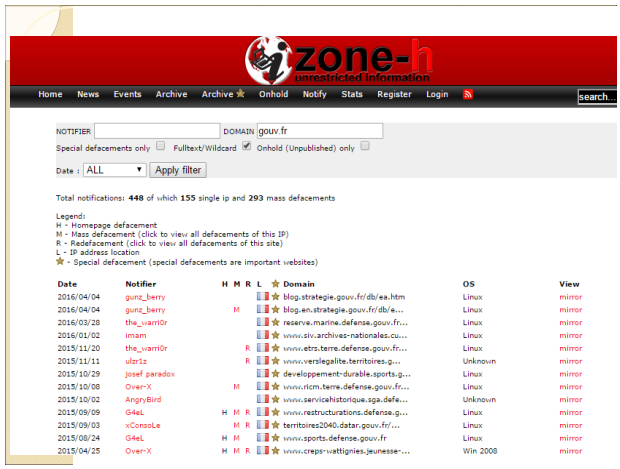
Incident coordination

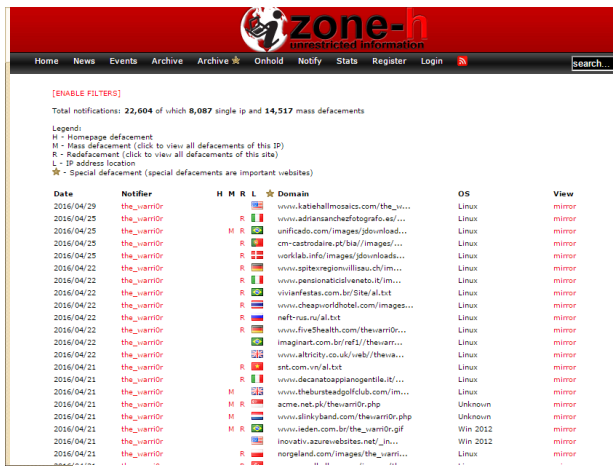
- CSO / CIO
- CEO
- Internal business managers
- Human Resources Department
- Physical Security Department
- Audit or Risk Management Department
- IT or Telecommunications Department
- Legal Department
- Public Relations Department
- Marketing Department
- Law Enforcement
- Government organization / agencies
- Investigators
- Other CERTs
- Other security experts



Veille technologique (Watch)

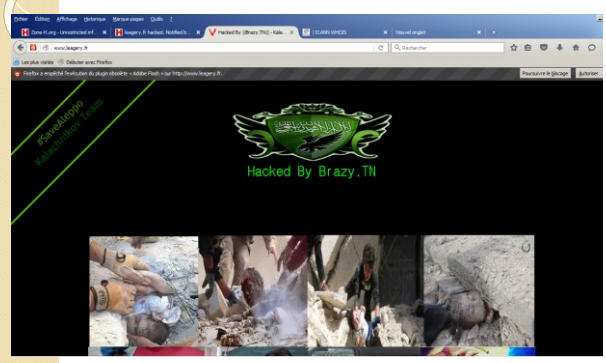




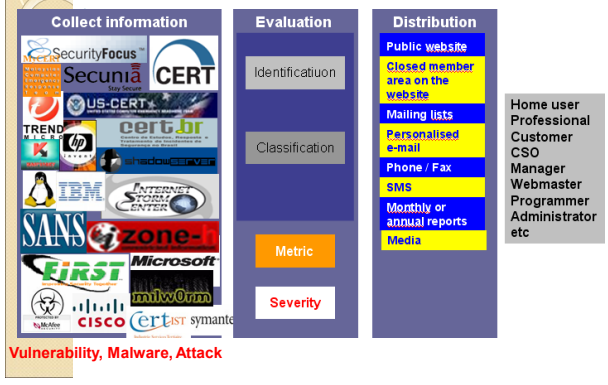


Cas de webdefacements

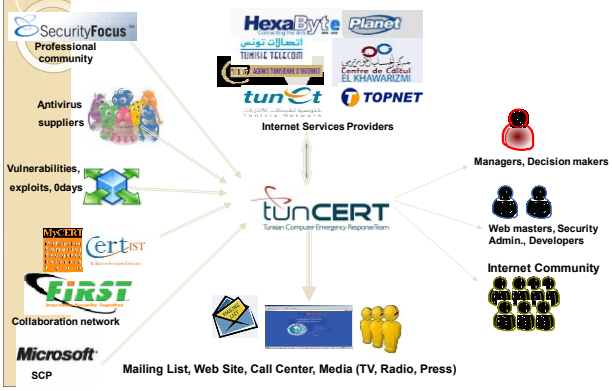
www.leagery.fr



Alert & warning process



Acteurs du processus d'Alerte

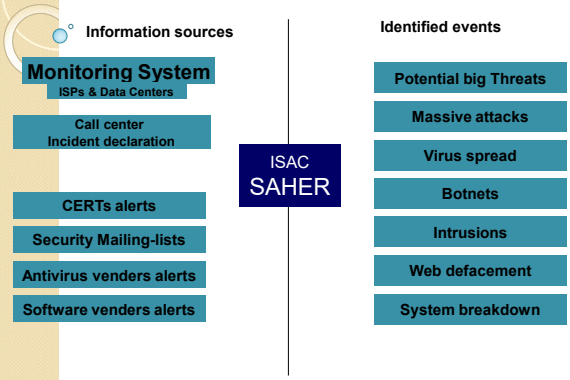


Veille : Plateforme d'outils

« Saher »

Une solution développée par *tun*CERT

Système SAHER : missions



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
- ...

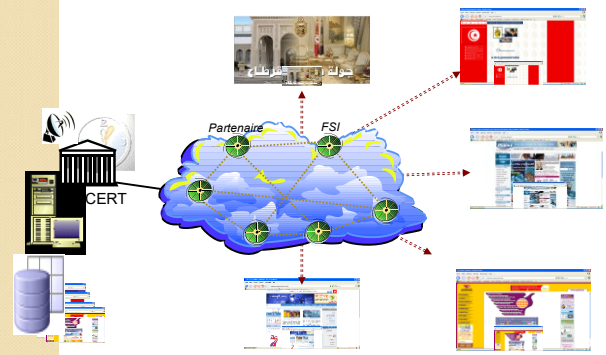
Saher – SRV: Internet services availability monitoring (Mail server, DNS,...)
- Mail Bombing
- Breakdown of DNS servers
- DNS POISONING...

SAHER–IDS: Massive attack detection
- Viral attack
- Intrusion
- DDoS
- ...

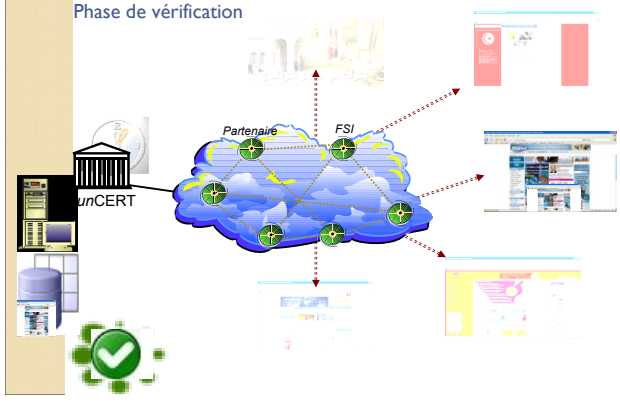
SAHER–HONEYNET: Malware gathering
- Viral attack
- Scan
- Possible attacks

Saher – Web : Supervision des sites Web nationaux

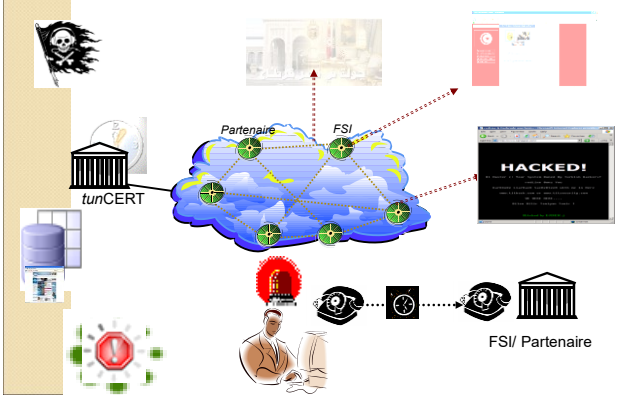
Phase d'enregistrement



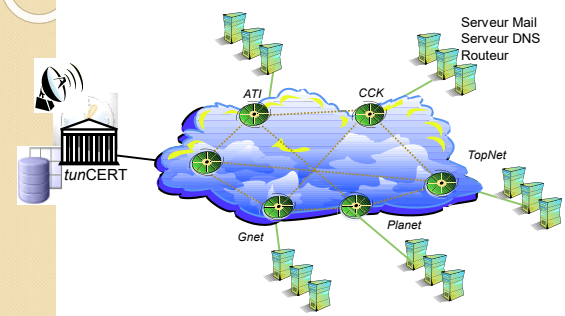
Phase de vérification

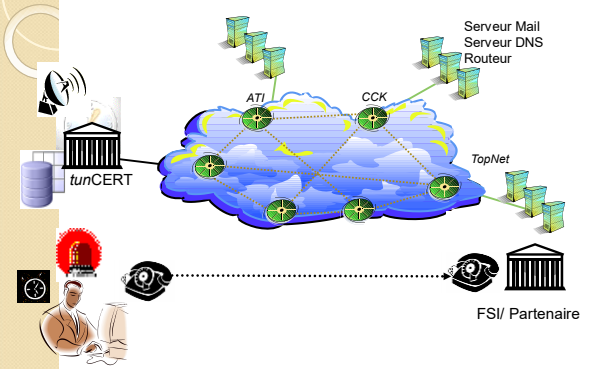


Phase d'Alerte/Réaction

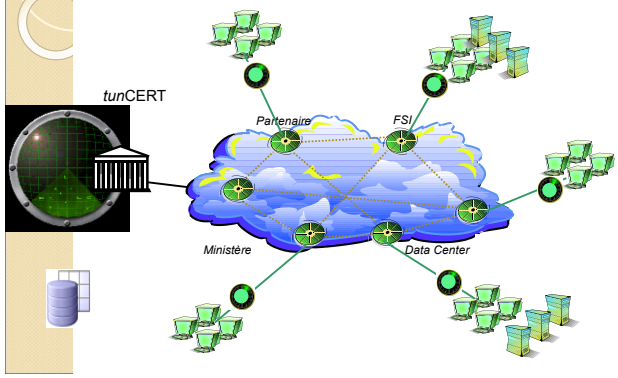


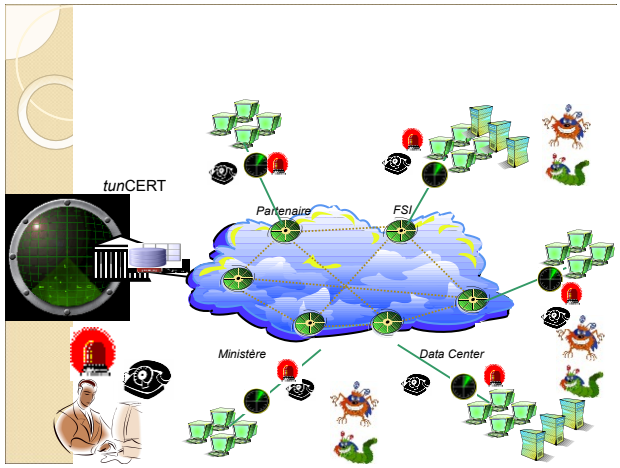
Saher – SRV : Supervision de la disponibilité des services Internet (serveur Mail, DNS, ...)



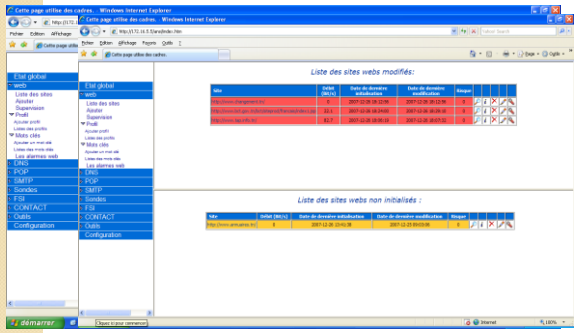


Saher – IDS : Détection des attaques massives

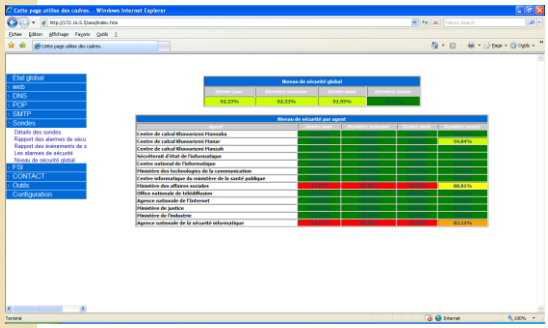




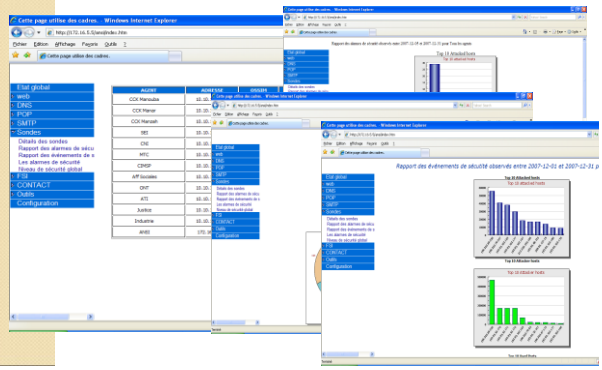
Saher – Web : Supervision des sites Web nationaux



Saher – SRV : Supervision de la disponibilité des services Internet (serveur Mail, DNS, …)



Saher – IDS : Détection des attaques massives



Projets Nationaux

NACS acts as a Security Expert for the government.
It is involved in the main national IT projects.

✓E-Government
- Madania (civil information system)
- INSAF (carrier management system for public employees)
- ADEB (public budget management system)
- National Backup Center
- Social management systems

✓E- (Justice, health, handicap, …)
✓LA POSTE (e-dinar)
✓EDUNET (education systems)
✓University systems :
-Orientation
-Inscription
-Student portal

Formation & Assistance

Formation

- Awareness Training
  - ✓Children and parents
  - ✓Home users
- Professional Training

  Security management, Security audit : Standards and methods, Risk assessment, Network security : risk and solutions, Open source for security, Web security, cryptography, Business continuity & disaster recovery, Incident handling & computer forensics, Vulnerability assessment and Pentesting, …

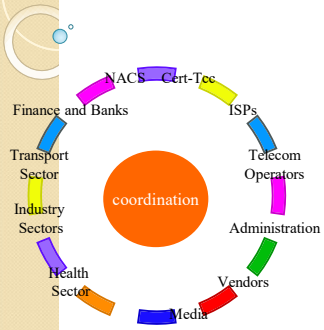
Assistance

Security policies, Security Audit Guides, Terms of reference models for security solution, Best practices (IIS, Apache, CISCO, …)

Vulnerability assessment methodology, Penetration test methodology

Open source security tools guides

Plan de Réaction National



- "Formal" **Global** Reaction Plan.
- Establishment of **Coordinating Crisis Cells** (ISPs, IDCs, Acess Providers).

With *tun*CERT 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 Meeting
2006 : Hand Ball World Cup
2009: Conficker

Sensibilisation (Awareness)

Awareness material

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

Flyers | Posters | Emails

Radio Emission | Cartoon | Video Spot

Attack Simulation | Guide

Conclusion

- 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
- Providing free technical support (Incident management capabilities)

merci de votre attention