Tunisia's experience in building an ISAC

Haythem EL MIR

Technical Manager – NACS

Head of the Incident Response Team – cert-Tcc

CERT-TCC

Computer Emergency Response Team- Tunisian Coordination Center

Agenda

- Introduction
- ISAC objectives and benefits
- Tunisian approach
- SAHER system
  - Intrusion detection
  - Critical system monitoring
  - Web attacks detection
- Conclusion

Introduction

- Security challenges:
  - Technical issues : Lack of tools for the early detection of threats at the level of the hole national cyberspace
  - Information availability
  - Organizational issues :
    - Information sharing
    - Collaboration and awareness
    - Coordination for Response

→ Establishment of an Information Sharing and Analysis Center : “SAHER” (Vigilant)

Major Objectives of the ISAC « SAHER »

Permits the monitoring of the security of the cyberspace, through :

- **Information** collection (Monitoring in real time of the backbone networks for DDoS events, worms, botnets, massive scans, hacking activity, etc).
- **Information** analysis for early identification of potential big and distributed attacks
- **Information** sharing about real and potential threats, vulnerabilities and incidents
- Early warning and **response (Reaction Plan "AMEN")**

Some specificities of the Tunisian approach

- Deployment of customized **Open source** solutions
- **Confidence and trust** of partners & mandatory declaration of incidents : Existence of a law (law N°5-2004) that stipulate the mandatory declaration of incidents and guarantees its confidentiality.
- Free of charge **assistance**
- Integrates all the communities (Gov, Banks, ISPs, Data Centers, …)
- Provides a **national knowledge base** about threats and potential attack sources and also a research and experimentation framework
- Provides a tracking and investigation system

The 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

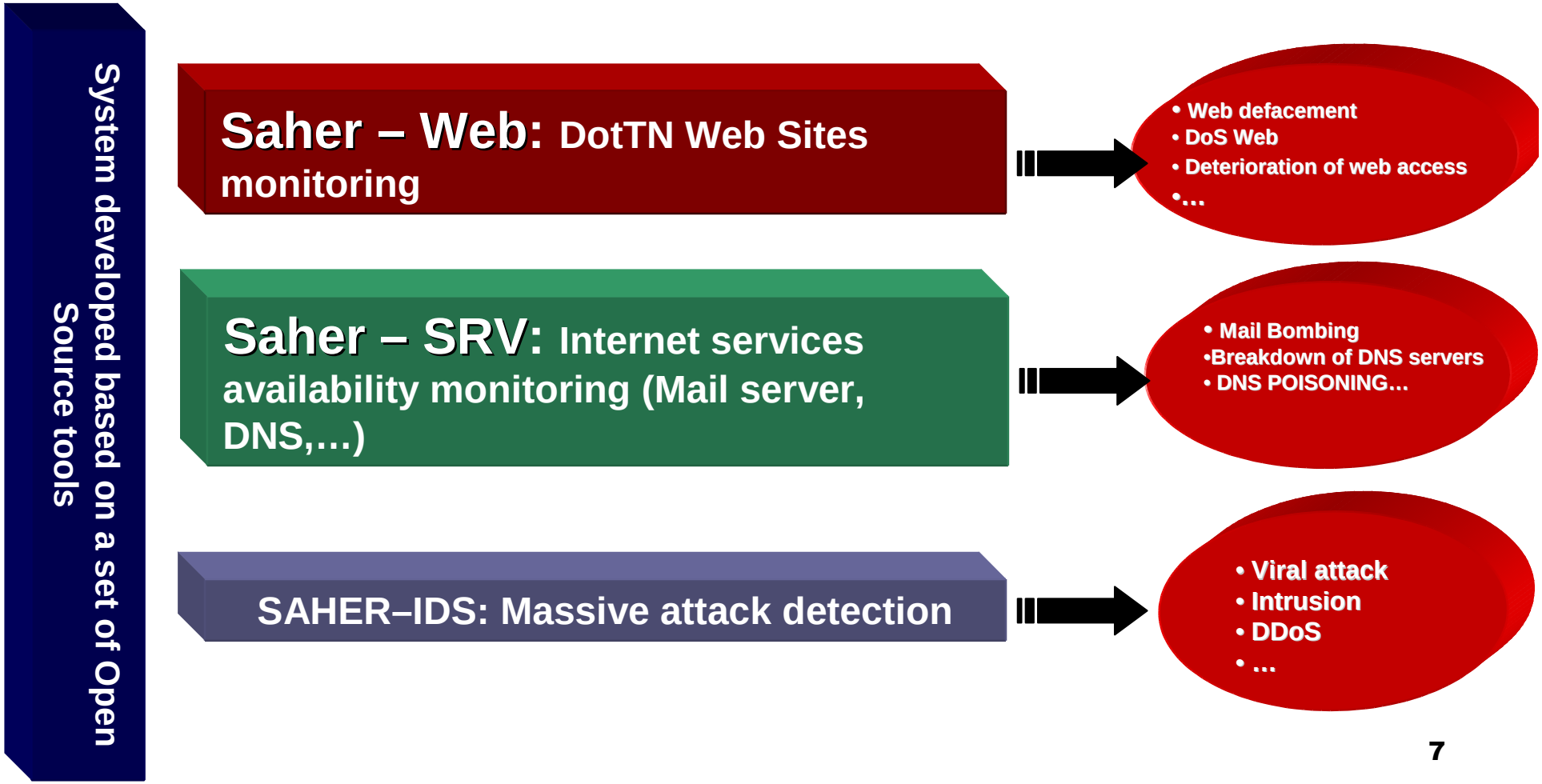
Botnets

Intrusion activities

Web defacement

System breakdown

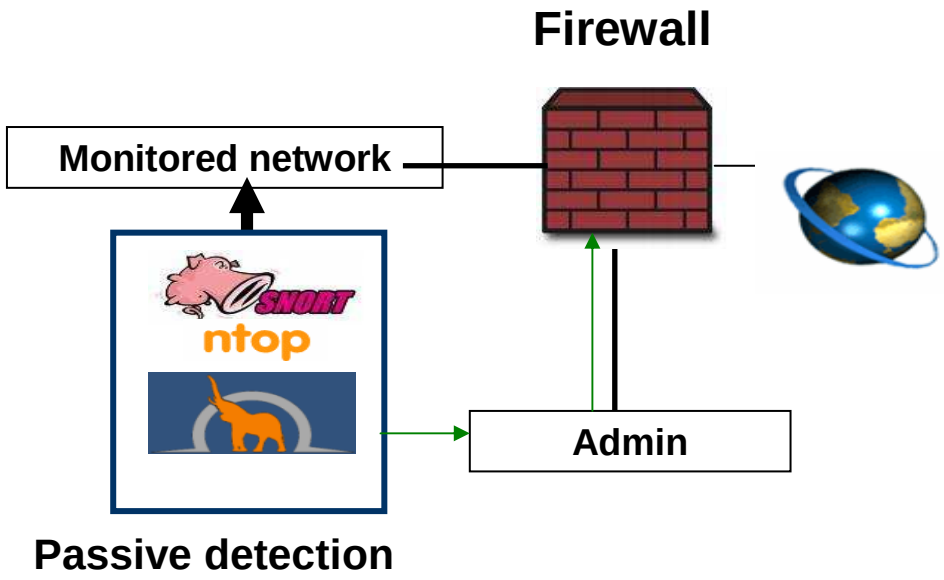
SAHER : The technical platform



SAHER-IDS

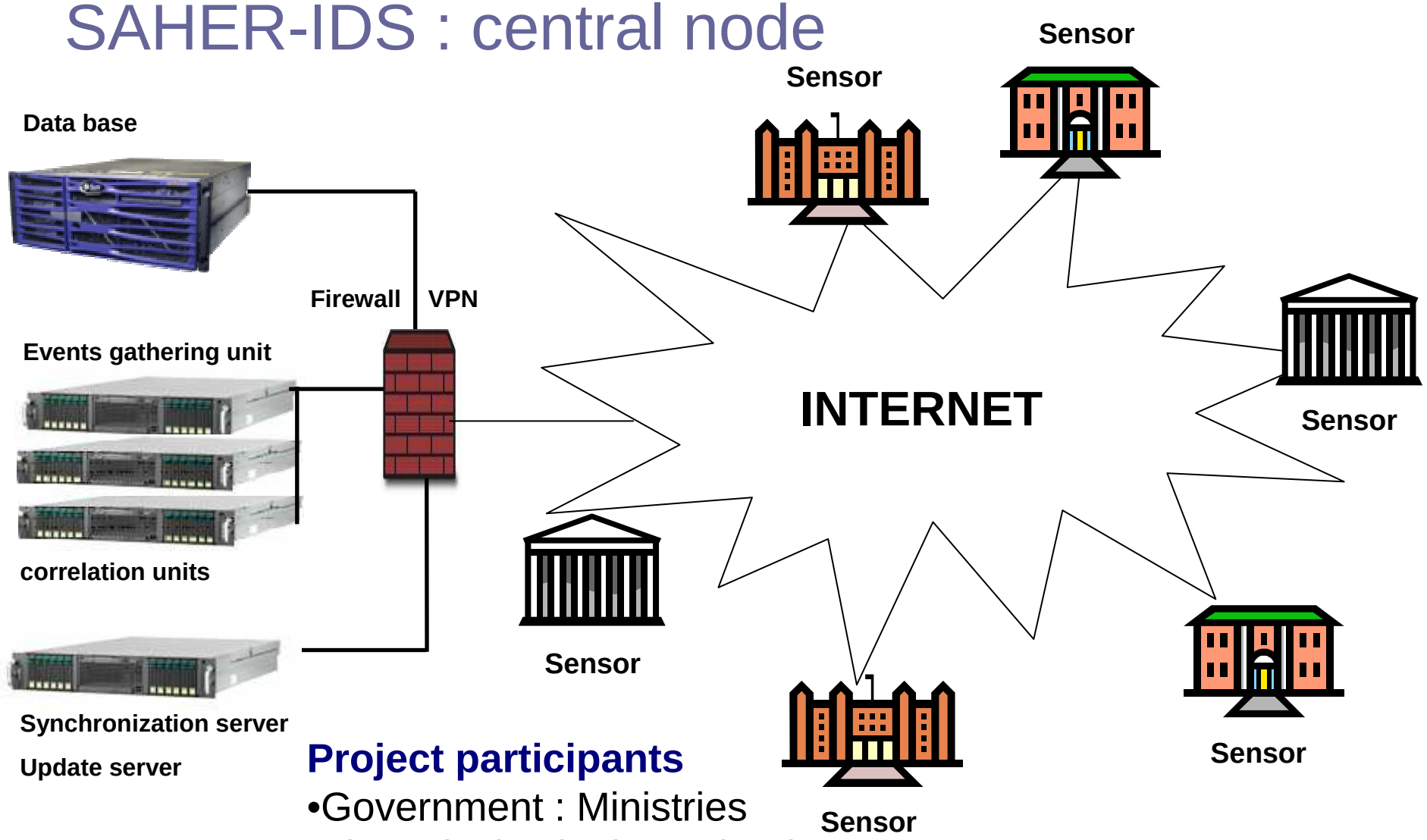
- Main Goals :
  - Set-up a distributed intrusion detection system
  - Detects massive and distributed attacks
  - Detects malware spread
  - Detects known attacks : signature
  - Detects unknown attacks: Anomaly based
- Context:
  - Based on a set of **customized** open source tools
  - Distributed environment with a centralized framework
  - Partnership with private and public enterprises
  - Micro-IDS (partners), Macro-IDS (National level)

SAHER-IDS : Principal



- Detection
  - Intrusion detection (NIDS, Honeypots)
  - Anomaly based sensors
- Monitoring & analysis
  - Event correlation (CALM, Holt-winter, correlation rules, state machine correlation)
  - Risk evaluation
- Forensics
- Management
  - Inventory of protected resources
  - Security policy definition
  - Correlation rules definition

SAHER-IDS : central node



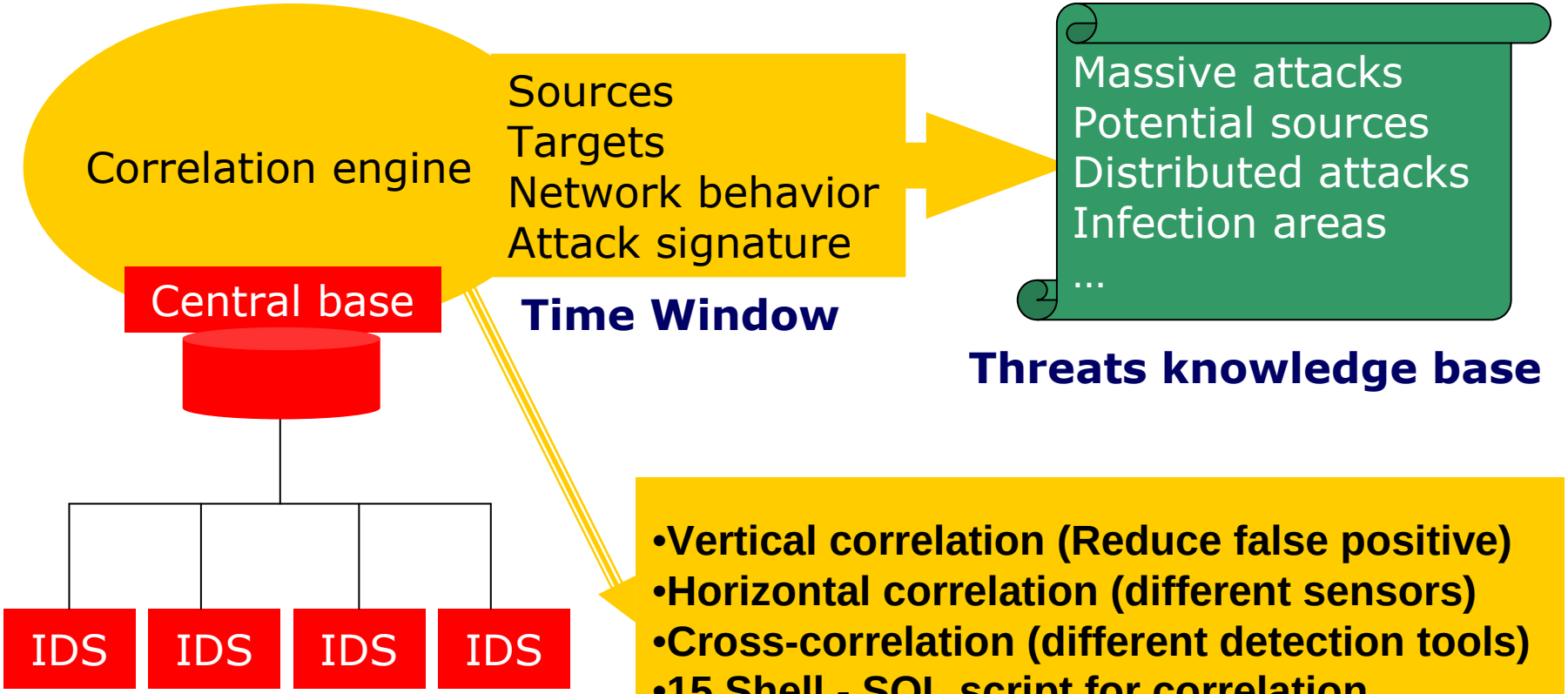
Project participants

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

Gathered information

- Events : information about intrusion (reported by saher agents)
- Security indicators: derived from alerts
  - Attacks (possibility that a machine is being attacked)
  - Compromise (possibility that a machine has been compromised)
- Alarms :
  - Selected events with a high risk surpassing a defined threshold
  - A set of events resulting from the correlation

Correlation



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

SAHER-SRV

- Main Goals :
  - Monitors critical nodes of the cyberspace
  - Detects critical nodes slowdown
- Context:
  - Works in a passive way
  - Monitors ISPs and telecom operator nodes
  - Detects and alerts in real-time

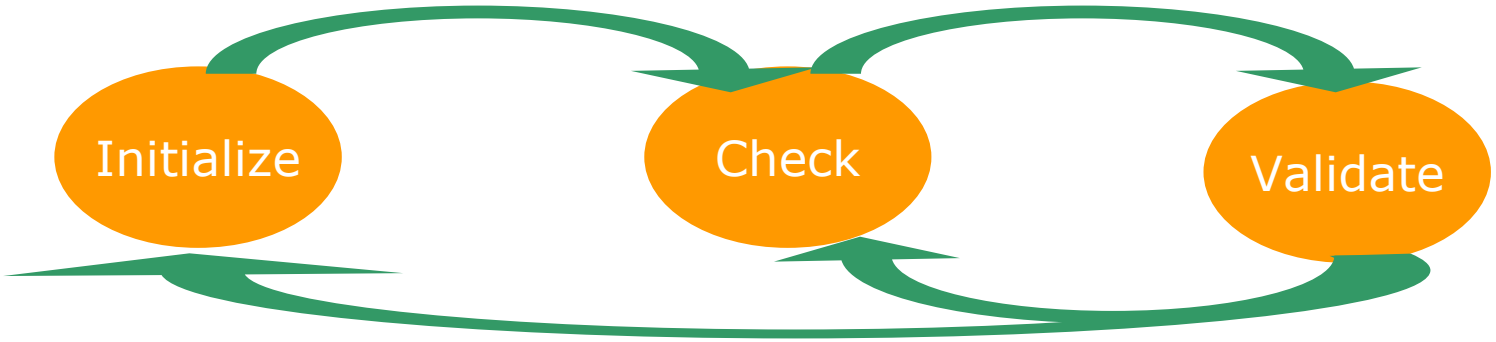
SAHER-SRV : principal

- Checks the availability of critical services
  - Mail : SMTP & POP/IMAP
  - DNS
  - Routers
- Various tests (Checkers)
  - Server Availability
  - Service availability
  - Service integrity
- Correlation
  - Intrusion detection system

SAHER-Web

- Main Goals :
  - Detects web defacement attacks
  - Detects web sites slowdown
  - Clear visibility on the national web space
- Context:
  - Works in a passive way
  - Monitors more than 6 000 web site
  - Reduces/eliminates false positives
  - Detects and alerts in real-time

SAHER-Web : Web defacement analysis component




```
Initialize (Site S)
{
    P = download_page (S)
    I = MD5(P)
}
```

```
Check (fingerprint I, Site S)
{
    P' = download_page (S)
    I' = MD5(P')
    IF I'=I then do_nothing
    Else
        if static_site then generate_Alert(S) // Sound, Visual, e-mail
        else deep_analysis(S_profile, S)
    Validte (S)
}
```

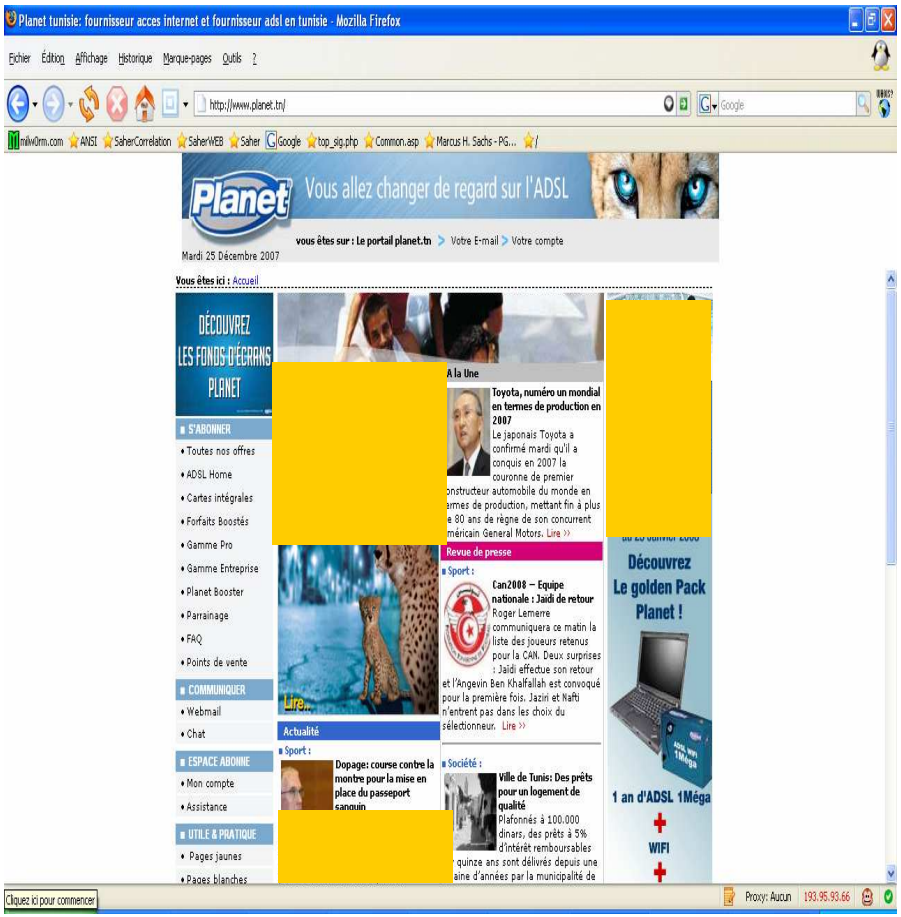
```
Validate (Site S)
{
    IF authorized_modification then
        Initialize (S)
    ELSE
        report_incident(S)
}
```

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

SAHER-Web : List of Tests

Example : Image conversion and analysis



Zone 1 : (a,b,c,d)
Zone 2 : (a',b',c',d')
Zone 3 : (a'',b'',c'',d'')

?

SAHER-Web : List of Tests

- HTTP protocol response analysis (HEAD)
- Virus detection (iFrame)
- Java Script Injection
- Cross-Correlation
  - vulnerability database
  - Vulnerability scanner
  - Intrusion detection system

Define a test profile for each website

SAHER : Risk evaluation

- Goal : reduce false positive and provide reliable alerts
- Solution :
  - Correlation engine
  - Cross-Correlation methods
  - Risk calculation

SAHER : Risk evaluation

- A risk value is assigned to each supervised web site
- An initial value is given depending on the web site importance:
  - Critical : Risk = 2
  - Medium : Risk = 1
  - Low : Risk = 0
- Default value = 0, Maximum value = 10

SAHER : Risk evaluation

- Cross-correlation with intrusion detection

```
Risk_calculation_web_ids(Site S)
{
IF modification_site(S) THEN
        E[] = security_events_list (IP(S), date(), date() – 30 min)
        IF E[] is not_empty then
                R = Max ( risk(E[i] )
                Risk(S) = Risk(S) + R
        EndIF
EndIF
}
```

SAHER : Risk evaluation

- Cross-correlation with vulnerability scanner
  - Periodic web vulnerability assessment (For critical web sites)
  - Vulnerability classification (Risk)

Risk(S) = Risk(S) + Max (Risk (found_vulnerabilities))

SAHER : Risk evaluation

- Cross-correlation with a vulnerability database (OSVDB)
  - Web server vulnerabilities
  - Web application vulnerabilities
  - CMS vulnerabilities (Joomla, Mambo, xoops, phpBB)
  - …

  Vulnerability ➔ Associated risk value

  Risk(S) = Risk(S) + Max (Risk (known_vulnerabilities))

SAHER : Risk evaluation

- Mutualized hosting correlation
  - Many websites hosted on the same server (IP)
  - If a website is hacked, the other similar websites are under a high risk

For each website hosted on the hacked server

$$\text{Risk}(S_i) = (\text{Risk}(S_i) + 1) \times 2$$

SAHER : CMS issues

- **Content management system**
  - Too websites are using open source CMS (joomla, xoops, phpBB, Invision power, …)
  - CMS are the first target for hackers (script kiddies using google search)
  - CMS exploits are rapidly made public
- **Solution**
  - Dedicated engine to identify used CMS at the national scale
  - Scan website to identify CMS signature
  - Identify vulnerable website

  → database indicating used technologies and eventual vulnerability

SAHER : CMS issues

- Website description (URL, ISP, IP, Owner, Webmaster, Administrator, Developer, OS, Web server, **Technology**)
- For each declared or identified vulnerability:
  - Rvj : is the risk value assigned to the vulnerability

    $Risk\ (S_i) = Risk\ (S_i) + Rvj$

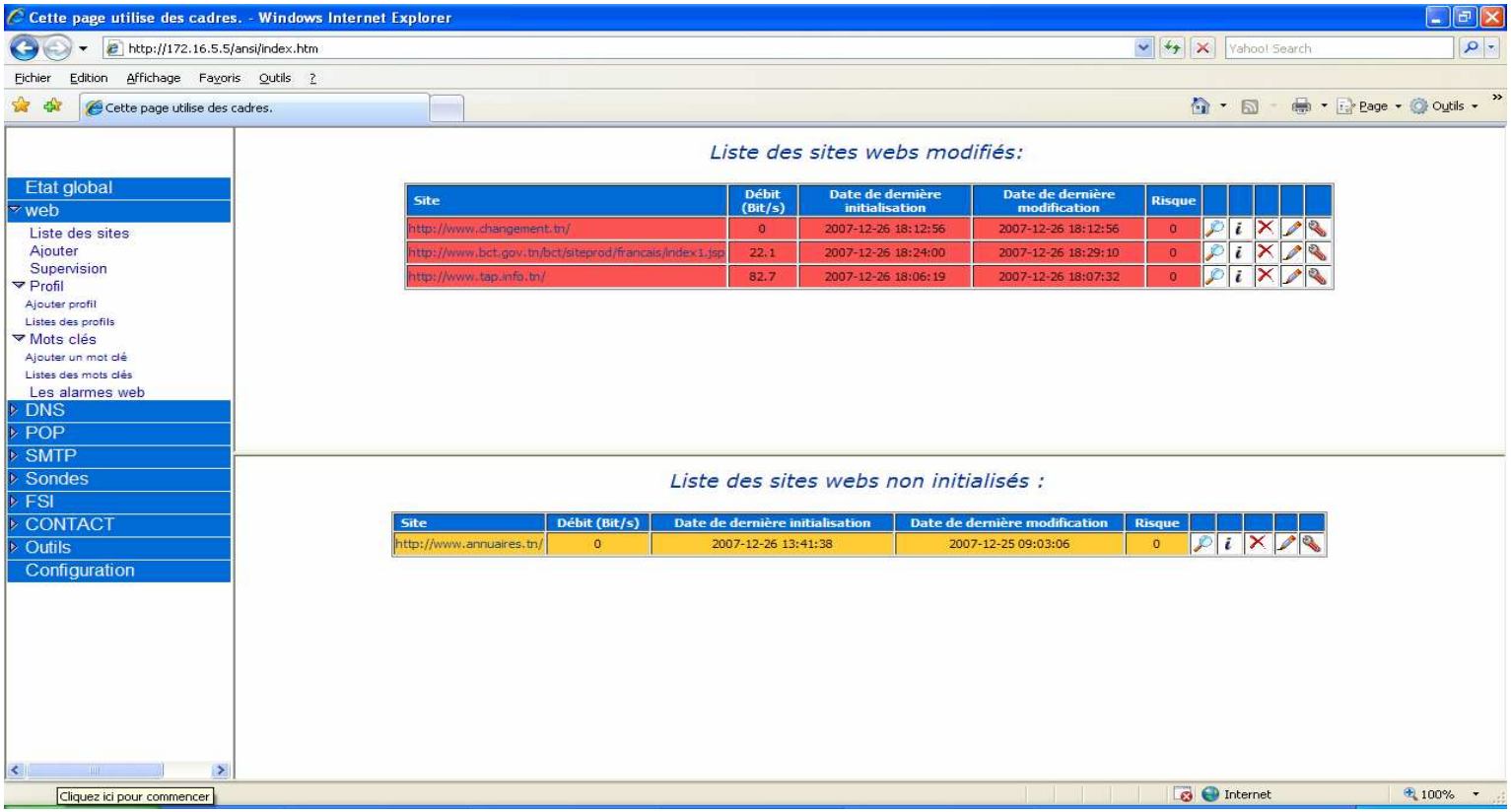
  - A coordination procedure is launched to inform webmaster/Administrator/ISP to patch the website.
  - The risk value is kept until the website is patched (manual process)

- For each hacked website using a particular CMS, all the similar website using the same CMS will be considered under threat

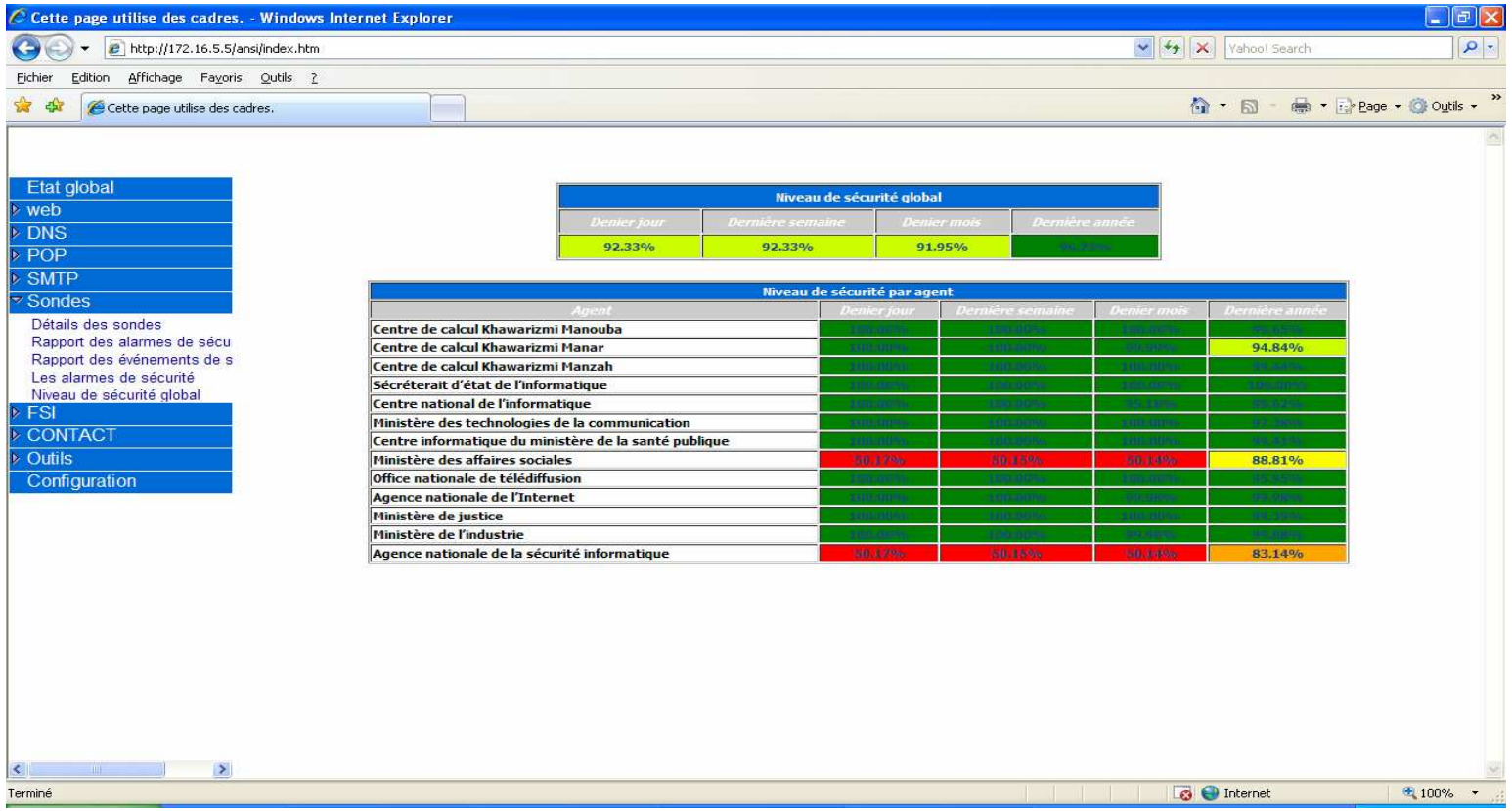
SAHER : Performance monitoring

- A bandwidth measurement is conducted for each site
- Bandwidth = (Data_amount / download_duration)
- A threshold is fixed for each website (200 bit/s by default), under this threshold an alert is generated
- Correlation with the IDS to prevent DoS and DDoS attacks

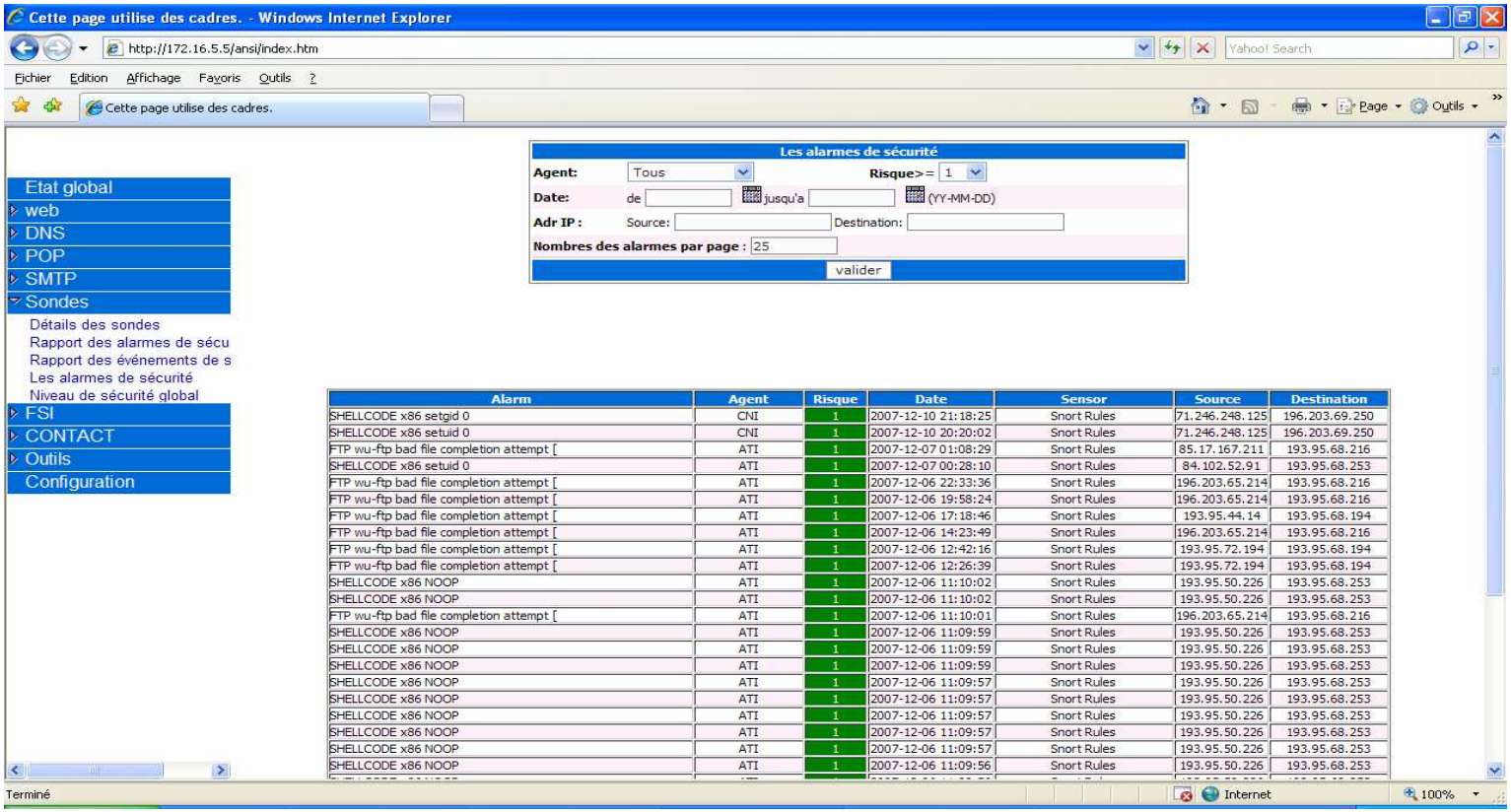
Some Screenshots



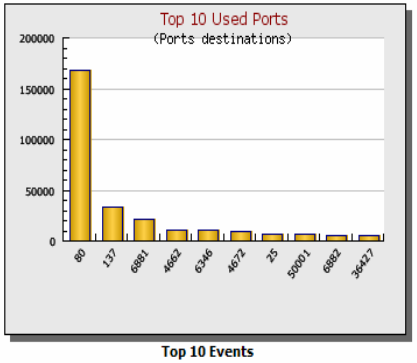
Screenshot


Cette page utilise des cadres. - Windows Internet Explorer
http://172.16.5.5/ansi/index.htm
Fichier Edition Affichage Favoris Outils ?
Cette page utilise des cadres.
Etat global
web
DNS
POP
SMTP
Sondes
Détails des sondes
Rapport des alarmes de sécu
Rapport des événements de s
Les alarmes de sécurité
Niveau de sécurité global
FSI
CONTACT
Outils
Configuration
Niveau de sécurité global
Denier jour
Dernière semaine
Denier mois
Dernière année
92.33%
92.33%
91.95%
Niveau de sécurité par agent
Agent
Denier jour
Dernière semaine
Denier mois
Dernière année
Centre de calcul Khawarizmi Manouba
Centre de calcul Khawarizmi Manar
94.84%
Centre de calcul Khawarizmi Manzah
Sécréterait d'état de l'informatique
Centre national de l'informatique
Ministère des technologies de la communication
Centre informatique du ministère de la santé publique
Ministère des affaires sociales
50.17%
50.15%
50.14%
88.81%
Office nationale de télédiffusion
Agence nationale de l'Internet
Ministère de justice
Ministère de l'industrie
Agence nationale de la sécurité informatique
50.17%
50.15%
50.14%
83.14%
Terminé
Internet
100%

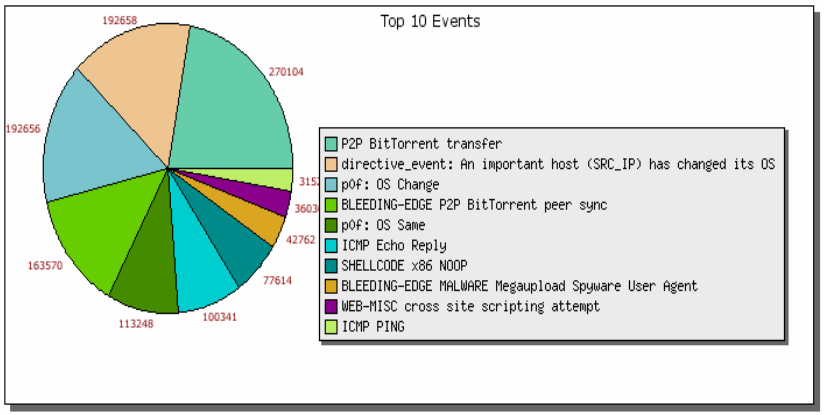
Screenshot


Cette page utilise des cadres. - Windows Internet Explorer
http://172.16.5.5/ansi/index.htm
Fichier Edition Affichage Favoris Outils ?
Cette page utilise des cadres.
Page Outils
Etat global
web
DNS
POP
SMTP
Sondes
Détails des sondes
Rapport des alarmes de sécu
Rapport des événements de s
Les alarmes de sécurité
Niveau de sécurité global
FSI
CONTACT
Outils
Configuration
Les alarmes de sécurité
Agent: Tous
Risque>= 1
Date: de jusqu'a (YY-MM-DD)
Adr IP : Source: Destination:
Nombres des alarmes par page : 25
valider
Alarm | Agent | Risque | Date | Sensor | Source | Destination
SHELLCODE x86 setgid 0 | CNI | 1 | 2007-12-10 21:18:25 | Snort Rules | 71.246.248.125 | 196.203.69.250
SHELLCODE x86 setuid 0 | CNI | 1 | 2007-12-10 20:20:02 | Snort Rules | 71.246.248.125 | 196.203.69.250
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-07 01:08:29 | Snort Rules | 85.17.167.211 | 193.95.68.216
SHELLCODE x86 setuid 0 | ATI | 1 | 2007-12-07 00:28:10 | Snort Rules | 84.102.52.91 | 193.95.68.253
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-06 22:33:36 | Snort Rules | 196.203.65.214 | 193.95.68.216
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-06 19:58:24 | Snort Rules | 196.203.65.214 | 193.95.68.216
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-06 17:18:46 | Snort Rules | 193.95.44.14 | 193.95.68.194
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-06 14:23:49 | Snort Rules | 196.203.65.214 | 193.95.68.216
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-06 12:42:16 | Snort Rules | 193.95.72.194 | 193.95.68.194
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-06 12:26:39 | Snort Rules | 193.95.72.194 | 193.95.68.194
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:10:02 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:10:02 | Snort Rules | 193.95.50.226 | 193.95.68.253
FTP wu-ftp bad file completion attempt [| ATI | 1 | 2007-12-06 11:10:01 | Snort Rules | 196.203.65.214 | 193.95.68.216
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:59 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:59 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:59 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:57 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:57 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:57 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:57 | Snort Rules | 193.95.50.226 | 193.95.68.253
SHELLCODE x86 NOOP | ATI | 1 | 2007-12-06 11:09:56 | Snort Rules | 193.95.50.226 | 193.95.68.253
Terminé
Internet
100%

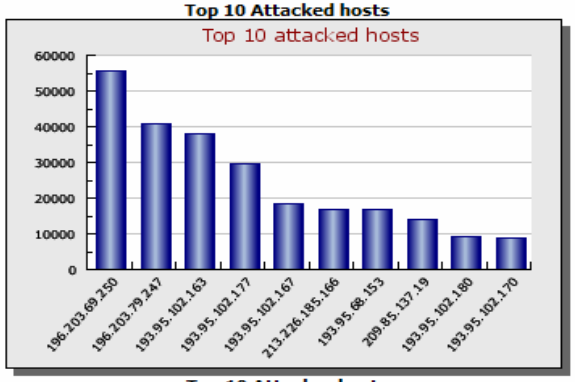
Screenshot



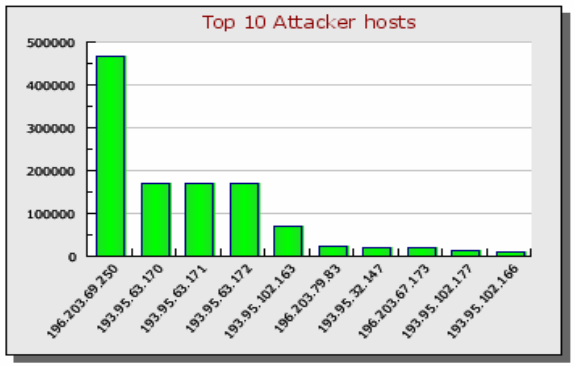
Top 10 Events



Top 10 Attacked hosts



Top 10 Attacker hosts



Future work

- Deployment of other types of sensors and distribution of the centralized framework to optimize servers load
- Integrates an incident handling workflow with partners to improve coordination and response
- Set up a distributed and reactive Honey-Net network to abuse some hacking activities
- Integrates a “hacker profiling” module through the profiling of each hacker and try to anticipate about the possible actions and relative alerts
- Develops an online “malicious IP” information sharing within the collaboration network and enrich the structured knowledge base, by including information from various sources (Audit report, Pentest report, incident report, events, etc.)

Conclusion

- The ISAC is a set of :
  - Tools : Saher
  - Procedures : Reaction plan, incident handling procedures
  - Watch team : operating 24/7
  - Incident response Team
  - Communication channels : email, phone, web, press,…
- The ISAC approach is a challenge
- The use open source tools still a good challenge

haythem.elmir@ansi.tn
www.ansi.tn