Proof of Concept: Implementing your CSIRT security architecture and Toolboxes, “free of charge” and with ROI

Prof Nabil SAHLI
AfricaCERT

FIRST Regional Symposium for Arab and African Regions
Sharm El Sheikh (EGY) 02 – 03 November 2016

PLAN

I- About Open-Source and CSIRT implementation

CSIRT Infrastructure

II- Security Architecture

II- Cyber-space Monitoring and Honeynet systems

CSIRT Activities

IV- CSIRT Process Management systems

V- Incident Handling tools

I-
About Open-Source and CSIRT implementation

Cost of Implementation of a CSIRT **Infrastructure**

- Equipments (Powerful PCs+ Little Servers)
- Software tools :

  - **License fees**

  + Recurent **heavy annual Maintenance fees**

How to decrease this big « cost center »
+ **avoid delays (+…) in CSIRT implementation, (escape from « our » painful and long procedures)**

Proof of Concept

Be able to **Invest More** in Capacity building & the funding of CSIRT activities

CSIRT's Software Needs

Need for a Very Good CSIRT Security Architecture

➔ **Cardinal and qualitative Completness of deployed Solutions**

Need for Tools implementing the CSIRT process

Need for various and multi-platform investigation and forensics tools

Bigs Budgets (Expensive licenses, Recurent cost of maintenance fees,..)

SOLUTION =Use of OPEN-SOURCE tools

~ 0 Licences

Open-Source

"Beautiful world"

- Free Licences
- Sources Codes available

+ Respect of standards
+ GUIs and Good Community assistance
+ Perinity proofed (better than some commercial solutions)

+ NOW: more and more «Contractual Assistance »& Training sessions offered (OpenCore)

Free access to Source codes

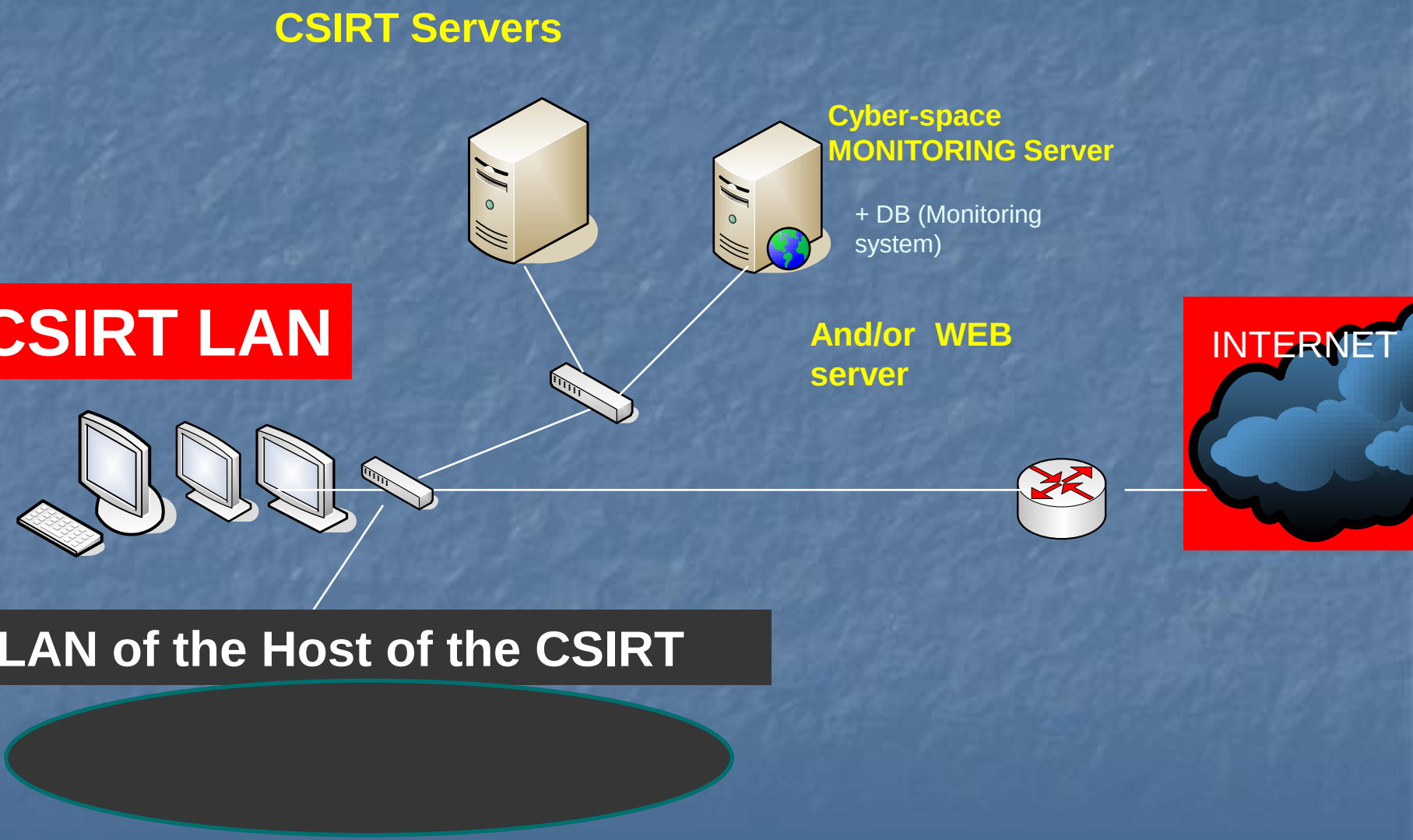
- Tools Can be Customized/Extended

An enabler for **R&D activities launch**

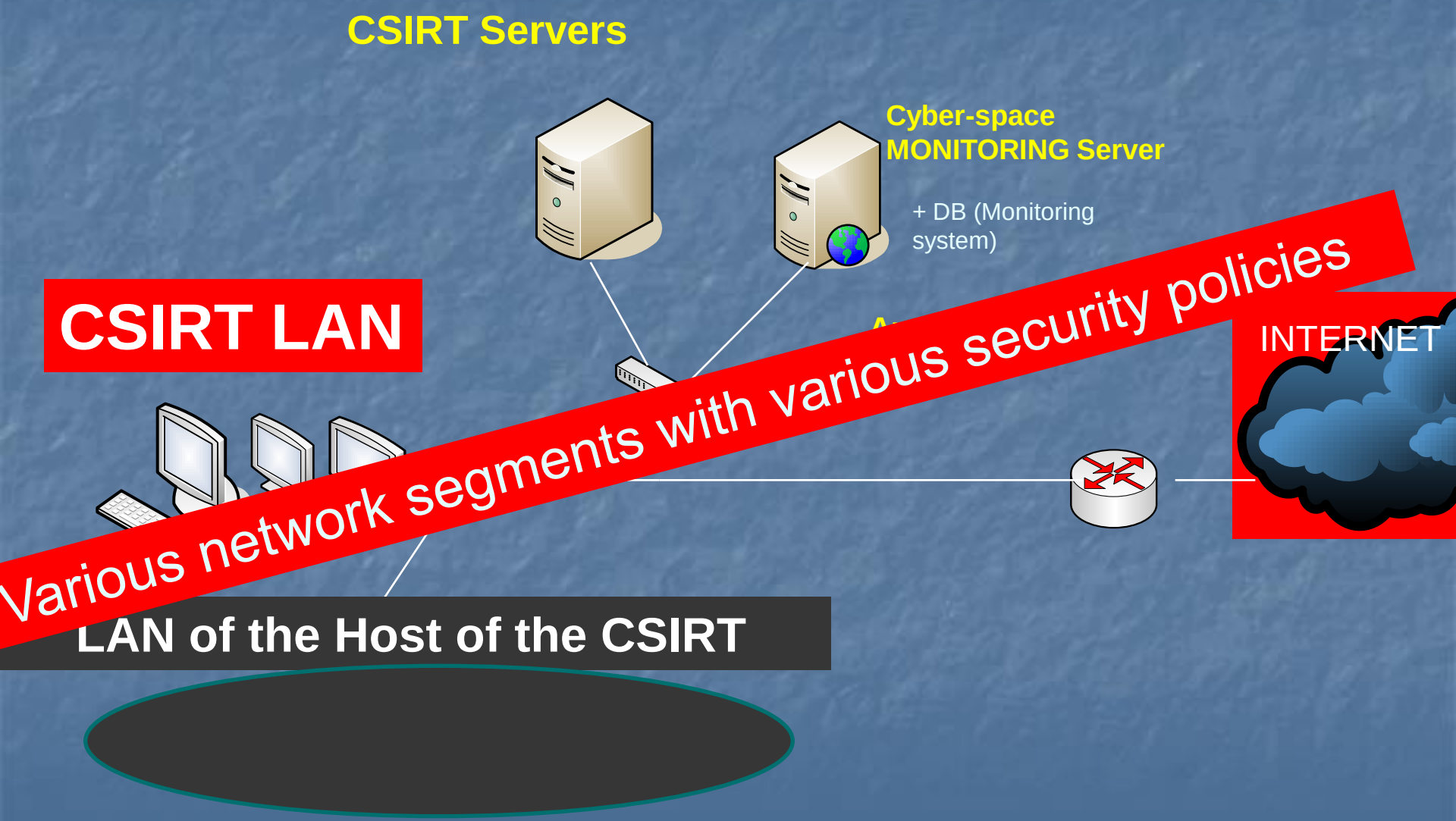
(= One potential ROI)

I- Building your CSIRT Security Architecture, with Open-Source tools

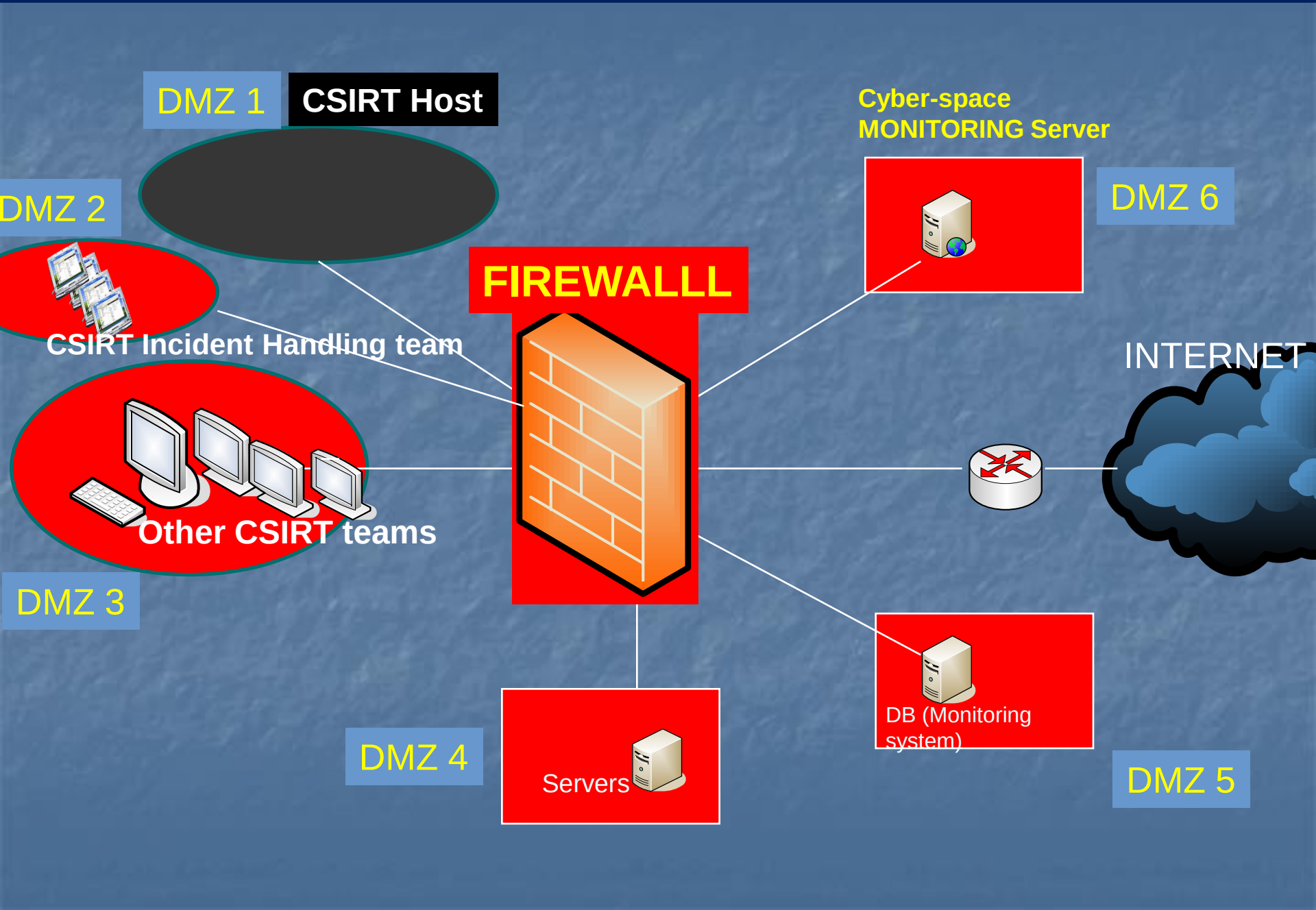
Network Architecture



-I-
Protection of the External Perimeter


CSIRT Servers
Cyber-space
MONITORING Server
+ DB (Monitoring system)
CSIRT LAN
INTERNET
Various network segments with various security policies
LAN of the Host of the CSIRT

Segmentation in DMZs, via FIREWALLs



Example of Open-source Firewall: Pfsense

Stateful Firewall with very rich Filtering capabilities

- **Various options of filtering** on a per-rule basis (Limitation of simultaneous connections, filtering by Operating System initiating the connection, Transparent layer 2 firewalling, …)
- Numerous features allowing **granular control of the state table**

- **High Availability** (CARP, pfsync) and Multi-WAN functionality, with failover +/- load balancing
- web interface for the configuration of all included components + **Graphical Reporting and Real Time Monitoring** (RRD and SVG graphs).
- PPPoE Server and Dynamic DNS
- **VPN** (IPsec, OpenVPN, and PPTP) and **Captive Portal** (RADIUS)-
- Server Load Balancing/ NAT, DHCP Server and Relay functionality

NG Firewall Free

→ works as a **basic UTM (Unified Threat Management) system**, for medium size networks

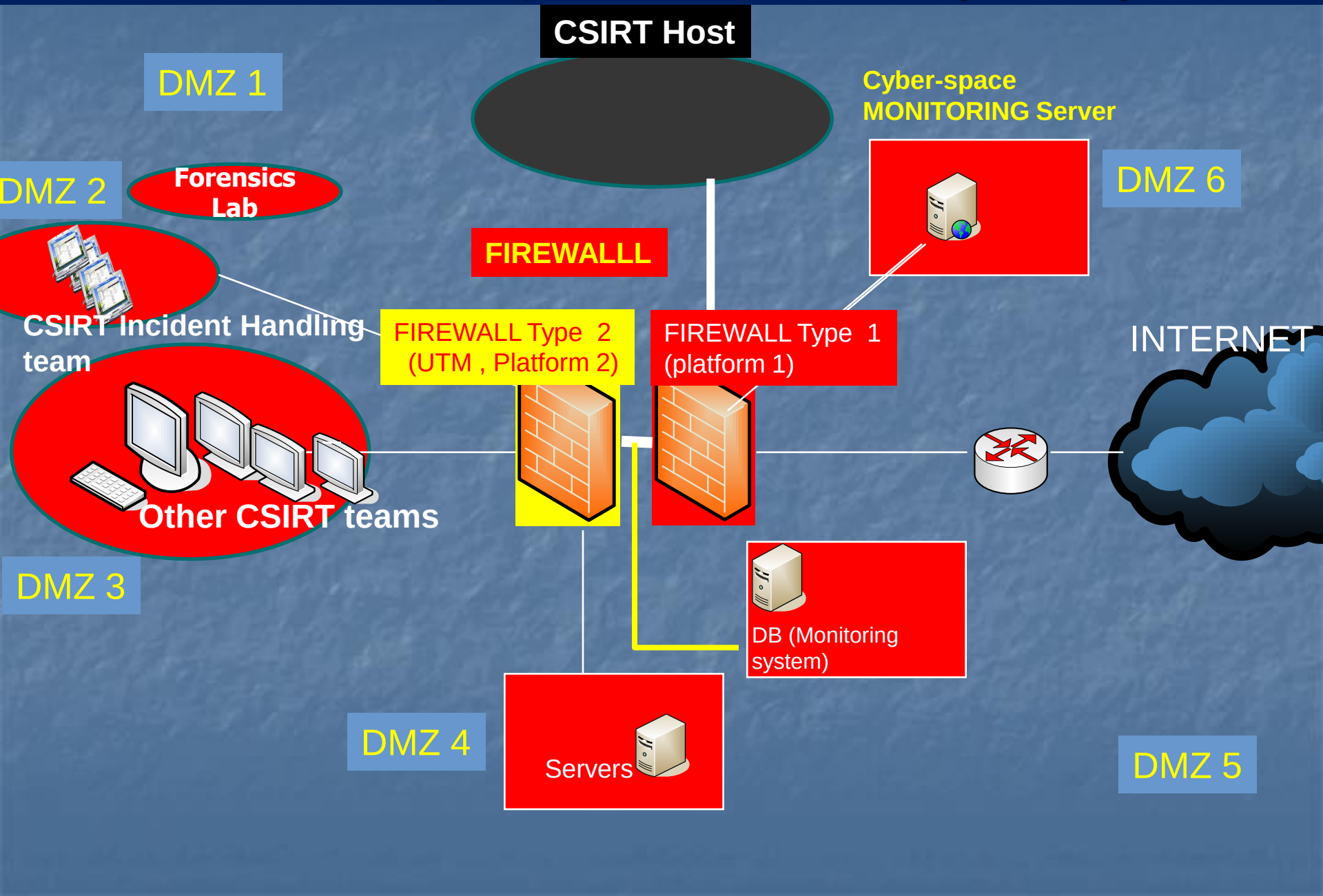
includes a rich collection of free applications:

Firewall

+

- **IPS**
- **Application Control**
- **Virus Blocker**
- **Web Filter**
- **Spam , Phishing and Ad Blocker**
- **OpenVPN**
- **Captive Portal**

→ High Secure Architectures: Serial Firewalls (since Firewalls are based on, also, vulnerable software and platforms)



The OFFER of Open-Source Firewalls is Rich

Zorp GPL : **Next generation firewall** with deep protocol analysis: Network traffic analysis in 7 protocols/Encrypted SSL/TLS channel control/Content filtering (virus scanners, spam filters and URL checkers , ..) with optional modification (proxying)
http://www.balabit.com/network-security/zorp-gpl

ConfigServer Security Firewall, supports almost all Virtualization environments like Virtuozzo, OpenVZ, VMware, XEN, KVM and Virtualbox, http://www.configserver.com/cp

SmoothWall **http://www.smoothwall.org**

Endian Firewall Community, http://www.endian.com/en/community/

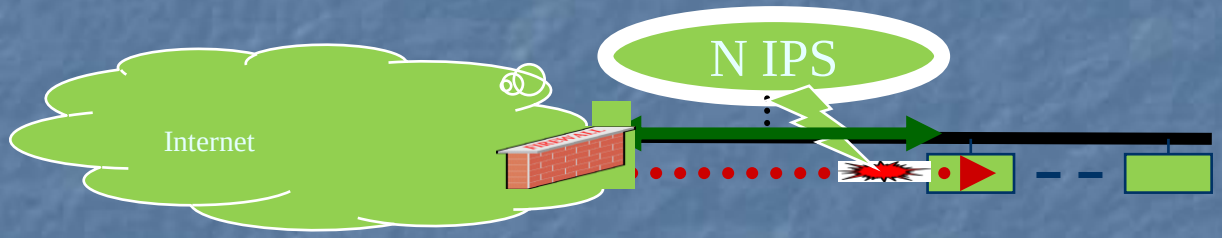
IPCop, http://www.ipcop.org/

ShoreWall (NetFilter), http://shorewall.net/index.html
m0n0Wall, **http://m0n0.ch/wall/**
ISP-FW, **http://isp-fw.sourceforge.net/**
IPFire , **http://www.ipfire.org/**

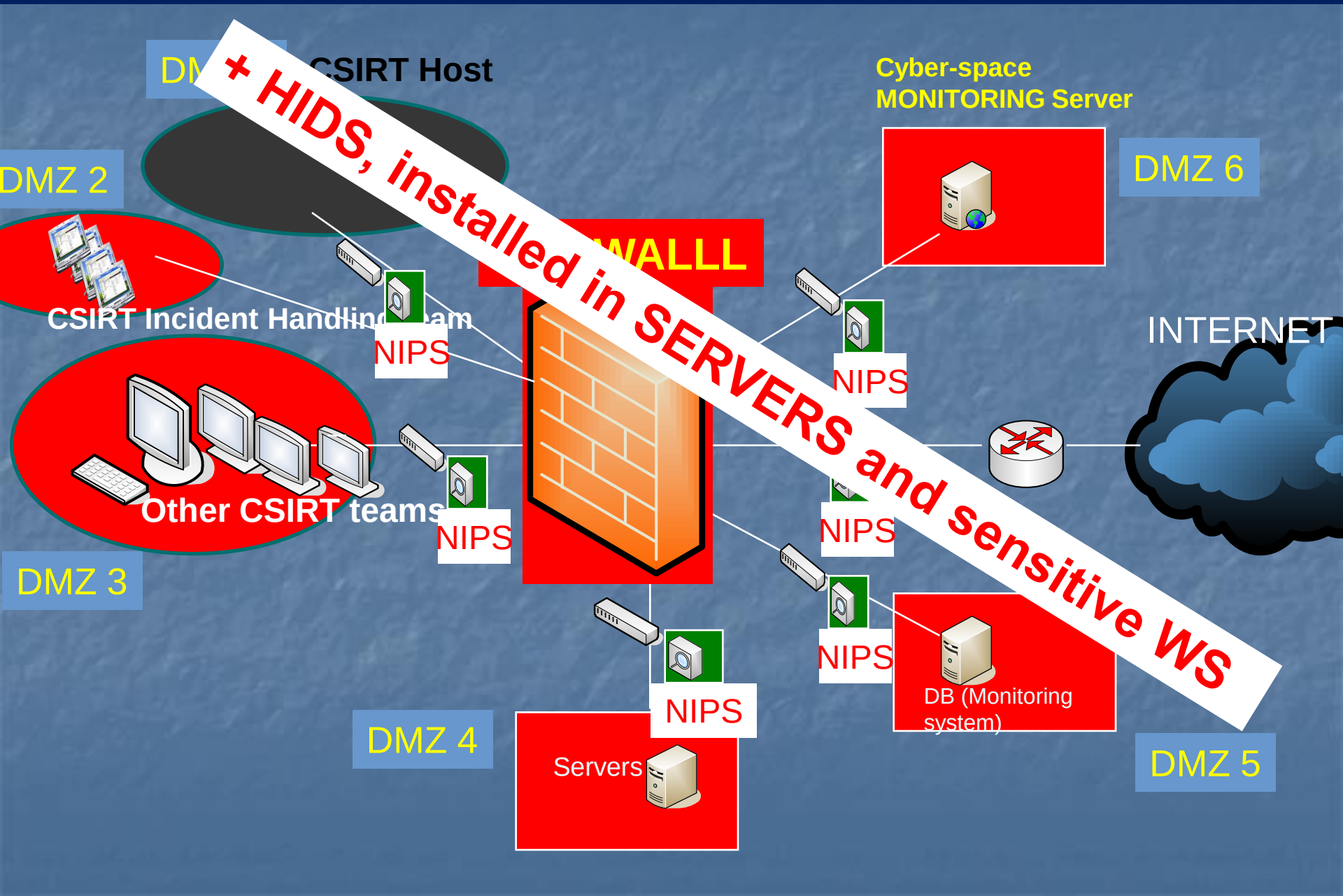
Vyatta, freeware http://community.brocade.com/t5/SDN-NFV/ct-p/SdnNfv

ShellTr: **http://shellter.sourceforge.net/**
FirewallPAPI: **http://sourceforge.net/projects/firewallpapi/**

Intrusion Detection :
Network IPS and Host IDS



Deployment of NIPS/HIDS



Network Intrusion Detectors (NIDS)

Snort

- THE Best NIDS

Pb : You should pay for « fresh » signatures (from 2011)
→399$/year /sensor, for Business usage
(29,99 $/year, for educational/personal purposes)
but
→ **Still Open-source (also after acquisition by Cisco in 2013)**
& Signatures of attacks of **(Month-1 !!) still free**,

More NIPS

Suricata

A **high performance** Network IPS and Network Security Monitoring engine.

Developed by the OISF.

Multi threaded engine that take full advantages of multi-core processors

→Able to achieve 10 gigabit speeds on real life traffic without sacrificing rule set coverage.

Bro

NIPS Based on the behavioural approach (violations of security politicy→
Detection of Zero-Day attacks
Developped by Berkeley
– Very powerful script Langage, for detecting new attack signatures
– Intrusion detection can trigger actions (IPS)
– Compatible with Snort rules (converter snort2bro)
- Learning Mode (false positive)
http://bro-ids.org/

Host Intrusion Detectors (**H**IDS)

OSSEC

Detection of rootkits, Log Analysis , File integrity check and process monitoring

- Available for Linux, MacOS, Solaris, HP-UX, AIX , Vmware ESX, and Windows platforms

- Configurable Alert (via e-mail and handheld devices), and response (HIPS),
- provides a simplified centralized management server to manage policies across multiple operating systems
- **meet compliance requirements, as outlined in PCI DSS 1.2/2.0**

Samhain

Provides file integrity checking and log file monitoring/analysis, as well as rootkit detection, port monitoring, detection of rogue SUID executables, and hidden processes.
+ centralized logging and maintenance.

Administration Tools :
Various Powerful tools for Log processing and Alerting

SIM/SLM/SEM

Prelude OSS Open Source version of Prelude implements a Security event manager (**SEM**)

BASE Provides a web front-end Sec Log Mananger, based on ACID, to query and analyze the alerts coming from a SNORT NIDS system(SIM).

Sagan

Real-time log analysis & **correlation engine**

Supports event-driven script execution**,** GeoIP detection/alerting,

Supports many output formats

→ Maintain compatibility with Snort-oriented rule management software (*oinkmaster …*) and consoles (Snorby, Sguil, BASE, and Prelude).

Swatch : **Alerts** when it matches the configured **log file entries** with your directives (regular expressions)

syslog-ng : allows to flexibly **collect, parse, classify, and correlate logs from various platforms**, store or route them to log analysis tools.

SIEM : **Security Information and Event Management**

OSSIM

A **SIEM**, with event **collection, normalization and correlation**
-> give a view of all the security-related aspects, by combining **Log data + Asset data + Discovery data**
from various information security controls and detection tools

→ **Correlation** to create contexts to the information **not visible from one piece alone.**

OSSIM features a lot of Open-source components:

- Snort, or Suricata. , as NIPS,
- Ossec as HIDS
- Ntop, or Nagios for traffic analysis

And much more :, Tcptrack, Munin, Arpwatch, P0f, PADS, NFSen/NFDump, FProbe, …

+ self developed tools (a generic correlation engine with logical directive support and logs integration with plugins).

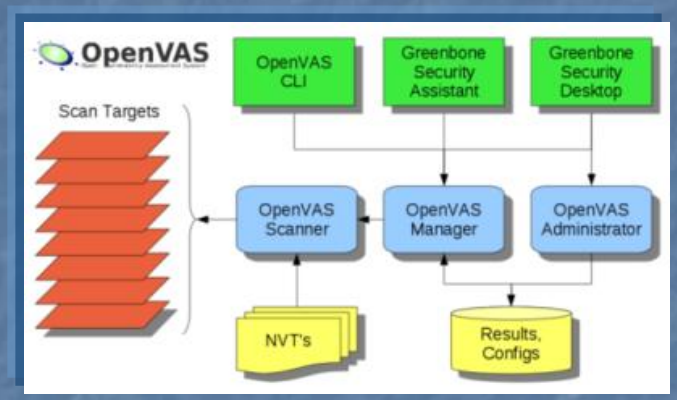
Open-source vulnerability Scanners

Open-source vulnerability Scanners

OpenVAS

- Powerful vulnerability scanning and vulnerability management solution (Fork from NESSUS, which become commercial in 2008).
- Daily update of Network Vulnerability Tests (NVTs),

A service-oriented client-server architecture: 6 modules, which communicate via well established protocols, SSL-secured.



« bad case » : SARA

→ development was ceased after releasing version 7.9.1 in 2009. ..

Open-source Web scanners

NIkTo :

Web server scanner for multiple items, including :

- ➔ over 6700 potentially dangerous files/CGIs
- ➔ checks for outdated versions of over 1250 services
- ➔ checks for Version specific problems on over 270 servers.

skipfish by GOOGLE,

Carry out a recursive crawl of web sites, with dictionary-based probes.

→ Produce a map of the web site, annotated with the output from security checks.

whisker

Webscarab /Websecurify

/Paros

Burp Suite, Netsparker, w3af, Arachni, ….

Kali Linux (previously « BackTrack ») : Linux distribution (Live DVD), regrouping all open-source tools for Vulnerabilty Assesment and PenTesting.

→ allow complex vulnerability assessment scripts :

- INFORMATION GATHERING
- VULNERABILITY ANALYSIS

Pen Testing :

- WIRELESS ATTACKS
- WEB ATTACKS
- EXPLOITATION TOOLS
- STRESS TESTING
- SNIFFING & SPOOFING
- PASSWORD ATTACKS
- MAINTAINING ACCESS
- REVERSE ENGINEERING
- HARDWARE HACKING
- REPORTING TOOLS

+ FORENSICS TOOLS

-3-
User Access Control

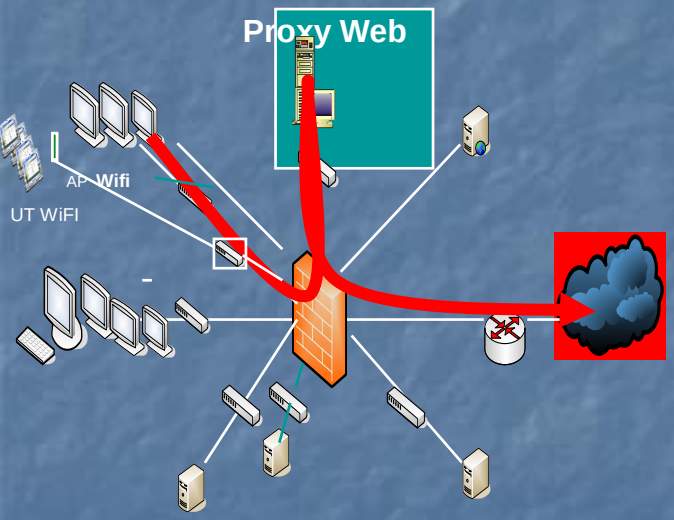
WEB access control

Squid Guard

- ✓ Extension of the « proxy » SQUID

→URL Filtering

- By keyWords **(sex, …), with regular expressions** support
- By Lists :
  - Access allowed to ONLY list of urls (Whitelists)
  - Access prohibited to ONLY list of urls (Blacklist)
- classes of Urls (news, sport, adultes, etc…).
- …



Single Sign On (SSO) solutions

Shibboleth (*Internet2)*
SSO tool.

That Implements the OASIS SAML Langage, to provide a federated single sign-on and attribute exchange framework.
+ Offers 2 APIs : OpenSAML-C++/Java

CAS (Yale University)

→ Provide **SSO (Single Sign On) protocol** for 3-Tiers applications
→ Offer CAS-clients for various plateforms (Java, .Net, PHP, Apache, ...)

-4-
Antivirus /Anti Spam

Antivirus Proxy

ClamAv

- **One of the Best Anti-virus Engines**
- Anti-virus proxy for mail server

Acquired by CISCO in 2013, but STILL Open-source,

RazorBack

Framework that allow in-line blocking on "store and forward" services, such as email services or web proxies,

→ coordinate the response against Advanced Persistent Threats (APT), by permiting to implement customized enterprise- and threat-specific detection and remediation.

Workstation solutions

Freeware Immunet ,
Based on the Open source ClamAV engine
Includes a Real Time Monitor

→provides cloud-based protection, wit… the P…
need to download any virus signa…
Immunet is up to 35 times li… an… lutions
PB: has to be connecte…

PB : Signatures Less « rich » than those of commercial ones
(task-force Problem)
+ No Central Administartion
+ A lot of free versions for Domestic use

ClamWI…
, open… …AV
Microso… …/2003/Vista.
No real …

CLAMWIN FREE ANTIVIRUS
open source security for your PC

ClamXav … for **Mac OS** , including Real Time monitor → become commer… …June 2015 …

Open-source Anti-Spam Gateways

SpamAssassin

- **Very popular (ISPs …)**
- **Various techniques for Spam detection**
  (exclusion Lists, DNS, fuzzy-checksum-based, filtering Bayesian, programmes externes, blacklists, BD online).

Anti-Spam + Anti-virus Gateway ASSP

- integration of Anti-virus Plug-ins (ClamAV, …)

+ Amavis

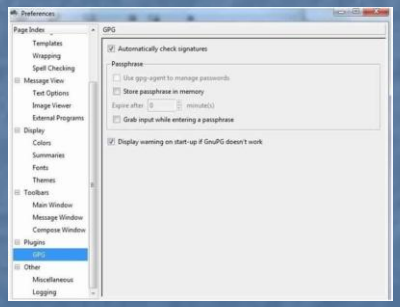
-5-
Tools for encryption of Communications and storage

Encryption/Signature of e-mails

GNU PRIVACY GUARD (GNUPG)

- Gnu Implémentation of the standard OpenPGP (RFC 4880, PGP).
- No algorithms under patent (Supports ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 et TIGER).
- Includes a little PKI manager .

Windows Version of GPG



Disk encryption tools

VeraCRYPT

multi-platform Disk encryption software,

create a virtual encrypted disk within a file or encrypt a partition or the entire storage device with pre-boot authentication

→based on TrueCrypt 7.1a, development has been abruptly ended in 2004

DiskCryptor

offers encryption of any and all disk partitions, including the system partition

. Support for encryption algorithm AES, Twofish, Serpent, including their combinations.

- Transparent encryption of disk partitions.
- Full support for dynamic disks.
- Support for disk devices with large sector size (RAID).

VPN

SSL VPN

OpenVPN

- Offer various cryptographic algorithms (OpenSSL)
- Good Support of bulk connections (big number of simultaneous connections)

•Available for Linux, Windows, OpenBSD, FreeBSD, NetBSD, Mac OS X, et Solaris

IPSec VPN

StrongSwan : Derived from FreeSWAN (2004), implements IPSec For Linux, **Android and Mac OS X**

OpenSwan : Derived from FreeSWAN (2004), implements IPSec For Linux and **Windows**,

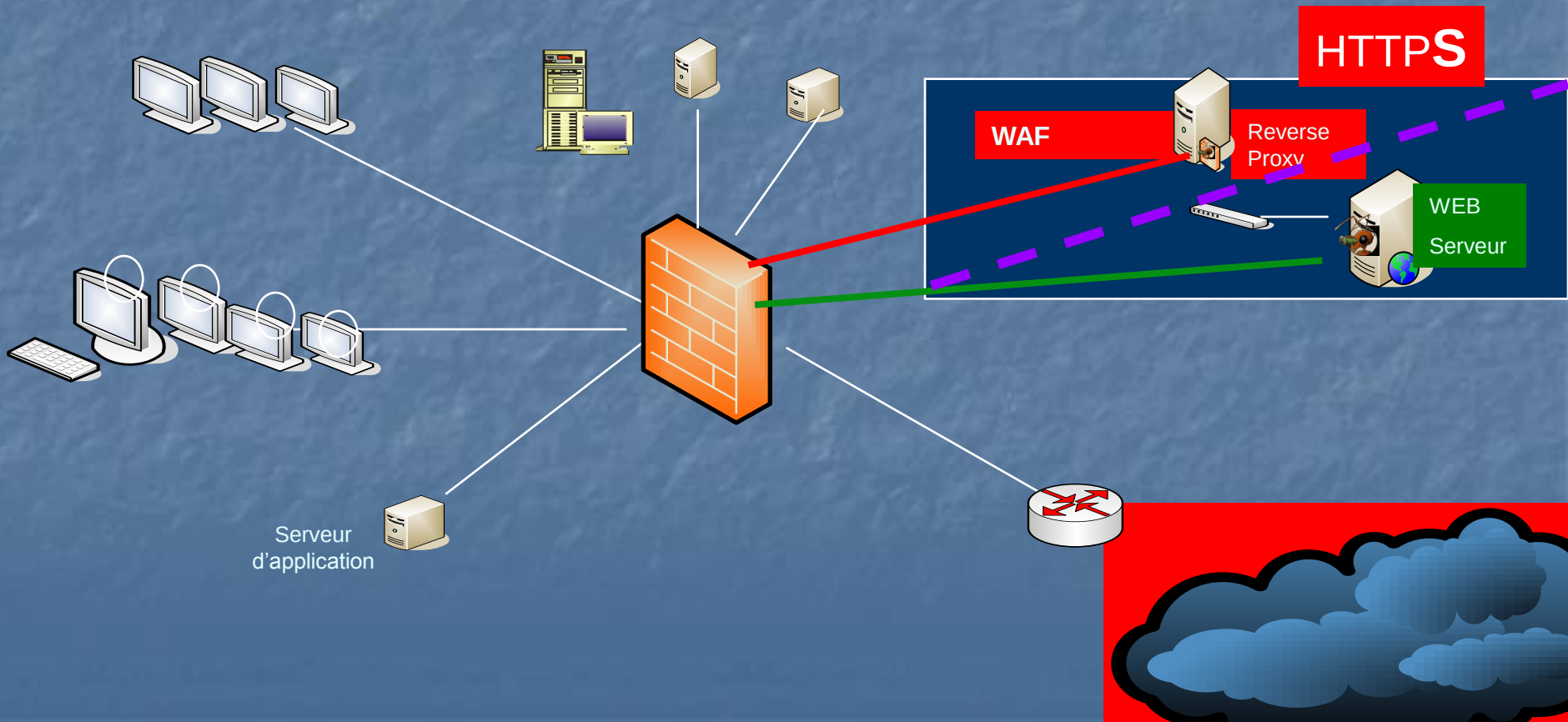
VPN Client : IPsec client for Windows/Linux
→ VPN gateways for ipsec-tools, FreeSWAN, OpenSWAN, StrongSWAN, isakmpd)

SSH

-6-
Protection of the CSIRT public Web server

Protection of the Web Server

→Web Application Firewalls
→ « Reverse proxy »
→ HttpS



Open-source WAF

→ Inspect the HTTP traffic stream, in real-time, with event correlation. and reliable blocking.

ModSecurity

- **Real-time Blacklist Lookups**
- **HTTP Denial of Service Protections**
- **Generic Web Attack Protection**
- **Error Detection and Hiding**

+ WAF-FLE : a OpenSource ModSecurity Console

IronBee - WAF sensor intended for real-time monitoring

Open-source Toolkits, for HTTPS

mod_ssl

HTTPS for Apache servers (based on SSLeay).

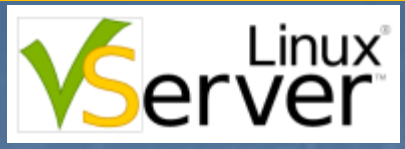
Apache-SSL

An Alternative, based on OpenSSL

Secure and Virtualization Platforms

Open-Source Secure OS

Linux-VServer



- a jail mechanism in that it can be used to securely partition resources on a computer system in such a way that **processes cannot mount a DOS on anything outside their partition.**

Qubes OS

Implements a *"Security by Isolation"* approach :

- **Isolate the various environments**, so that if one of the components get compromised, the malicious software would get access to only the data inside that environment.
- not a multi-user system

SELinux (NSA & RedHat)

provides a mechanism for supporting access control security policies , including DoD's **Mandatory Access Controls (MAC).**

AppArmor

→ includes a **learning mode**

Virtualization platforms

VirtualBox : powerful Type 2 virtualization solution

Runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8), DOS/Windows 3.x, Linux (2.4, 2.6 and 3.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

open-source type-1 hypervisor (run directly on the host's hardware), and permit to run many instances of an operating system or indeed different operating systems in parallel on a single machine (or host).

Has a user base in the millions, that include cloud providers such as *Amazon Web Services, Rackspace Hosting, Verizon Cloud* and many others

-9-

And Much more

NAS (Network-Attached Storage) / SAN

FreeNAS

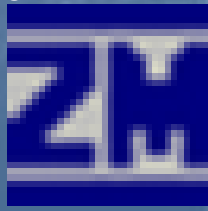
Open source NAS system based on FreeBSD
and the ZFS file system,
with a dedicated management web interface.
- Supports RAID

Openfiler freeware NAS/SAN

Video Control solutions

iSpy : open source

turns a PC into a full security and surveillance system
- Detect and record movement or sound.
- Captured media is compressed to flash video or mp4 and streamed securely over the web and local network.



Freeware ZoneMinder

Provide a complete surveillance solution allowing capture, analysis, recording and monitoring of any CCTV or security cameras attached to a Linux based machine

ROI ?

Able to deliver more CSIRT services :

- **Immediate Assistance** of the constituency in **rapidely deploying Security Architectures**, based on open-source security tools
- Training
- R&D: customisation/combination/ enrichment of open-source tools

Overview about the implementation, with open source solutions, of a

National Cyber Space Monitoring System

Important to Not be BLIND about
what is going on in the National cyber-space

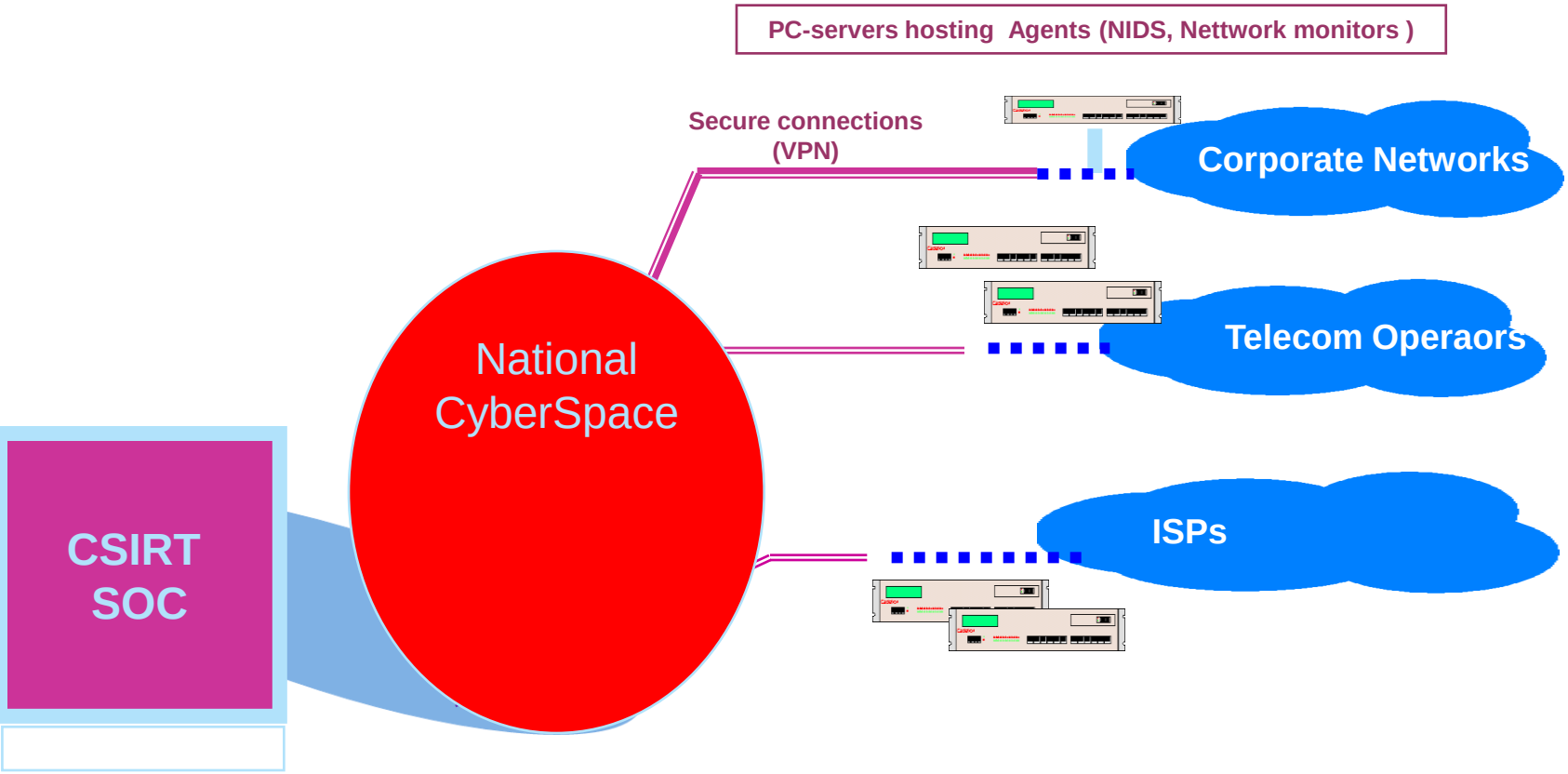
LOGO

-8-
Cyberspace Monitoring Infrastructure

Cyber Space Monitoring System (CSMS)

A **SOC** (based on **open-source solutions**), which permits to monitor the National Cyber-Space security in **Real time**

→For the **early Detection** of **Massive attacks** and minimization of their impact.



Simple
Cyber Space Monitoring System

Security Onion : Linux distro for IDS and NSM for Snort, Suricata, Bro, Sguil(+, Squert, ELSA, Xplico, NetworkMiner,…)
Include an easy-to-use Setup wizard

t / Nmap

Secure connections (VPN)

Corporate Networks

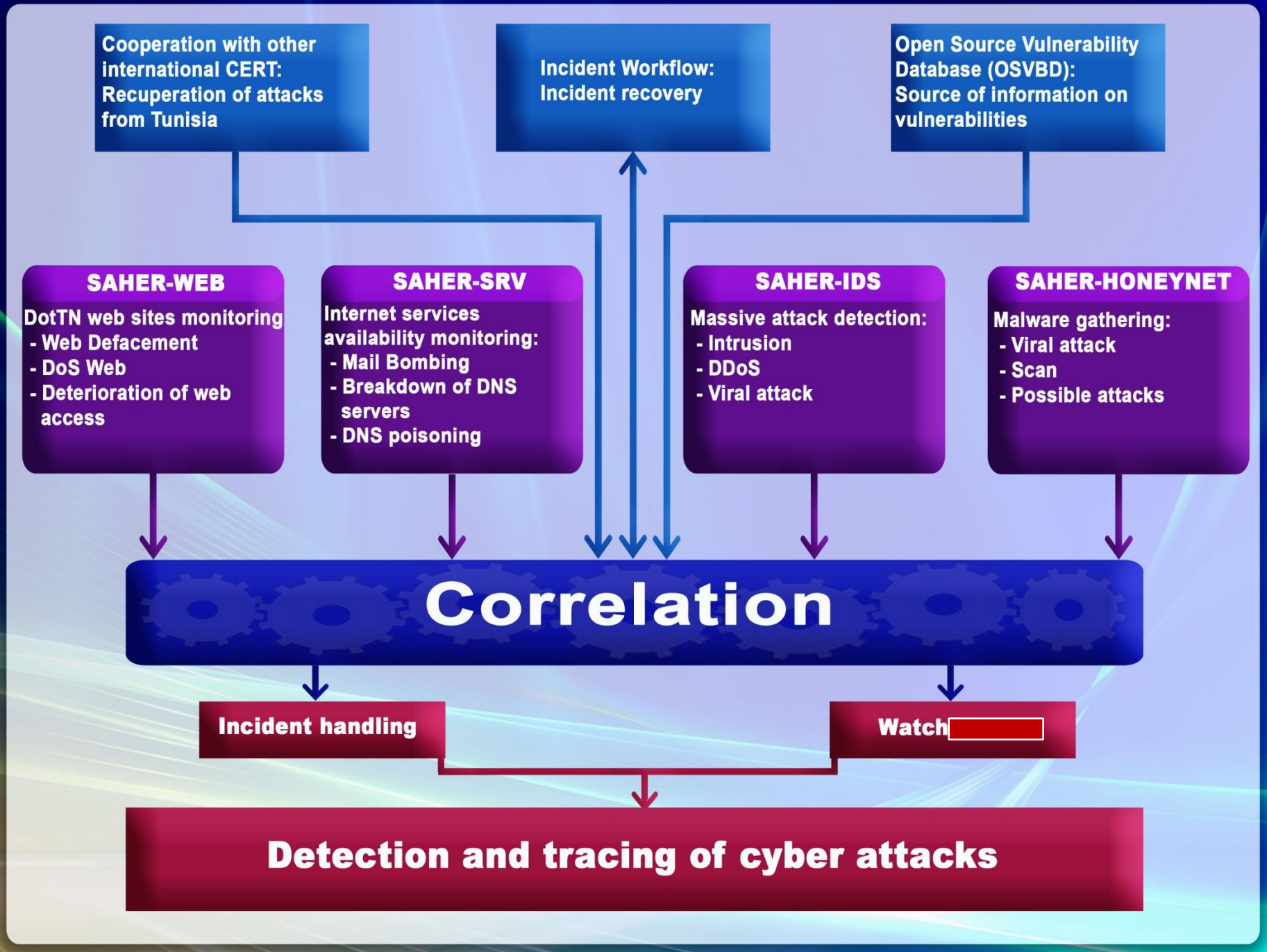
Telecom Operaors

Internet

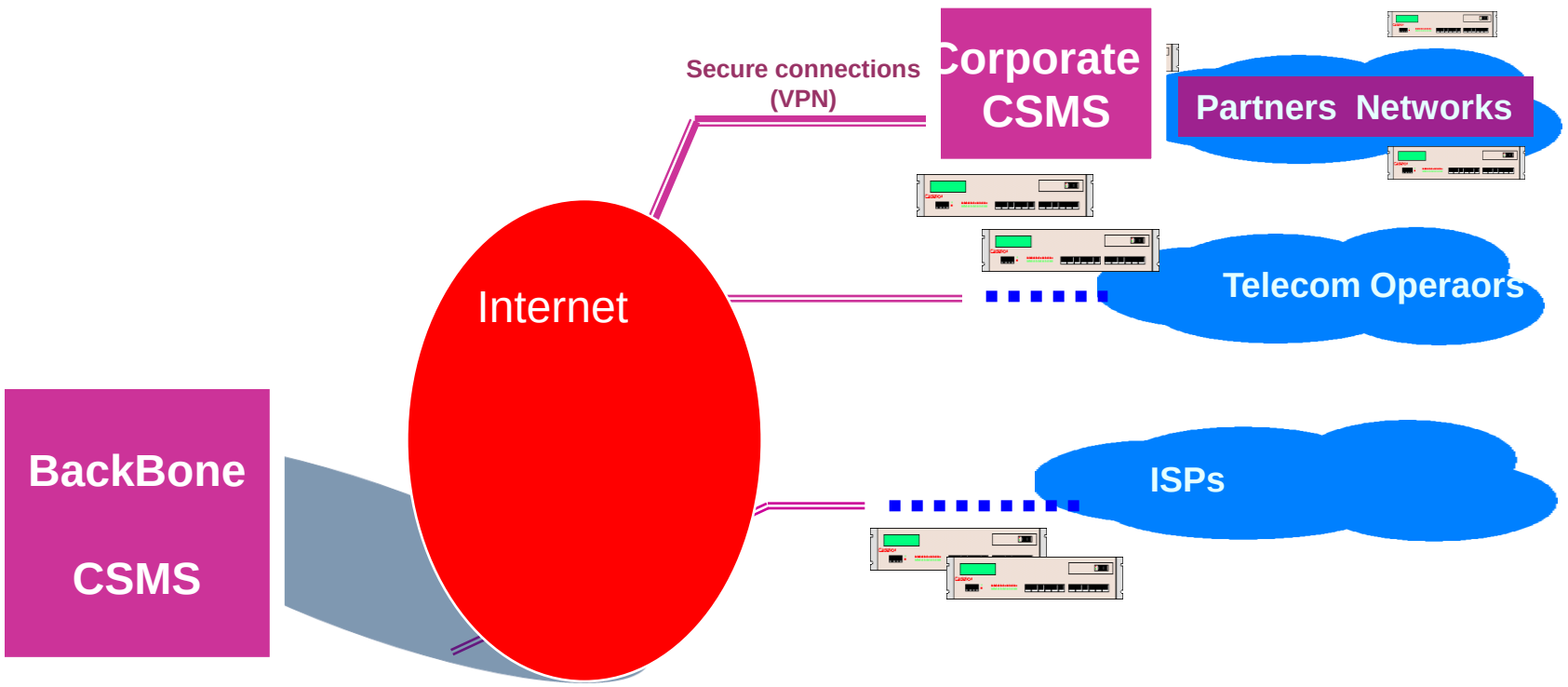
ISPs

Open source tool

Snorby : a ruby on rails web application that interfaces with all popular intrusion detection systems (Snort, Suricata and Sagan)


Cooperation with other international CERT: Recuperation of attacks from Tunisia
Incident Workflow: Incident recovery
Open Source Vulnerability Database (OSVBD): Source of information on vulnerabilities
SAHER-WEB
DotTN web sites monitoring
- Web Defacement
- DoS Web
- Deterioration of web access
SAHER-SRV
Internet services availability monitoring:
- Mail Bombing
- Breakdown of DNS servers
- DNS poisoning
SAHER-IDS
Massive attack detection:
- Intrusion
- DDoS
- Viral attack
SAHER-HONEYNET
Malware gathering:
- Viral attack
- Scan
- Possible attacks
Correlation
Incident handling
Watch
Detection and tracing of cyber attacks

Distributed
Cyber Space Monitoring System (CSMS)



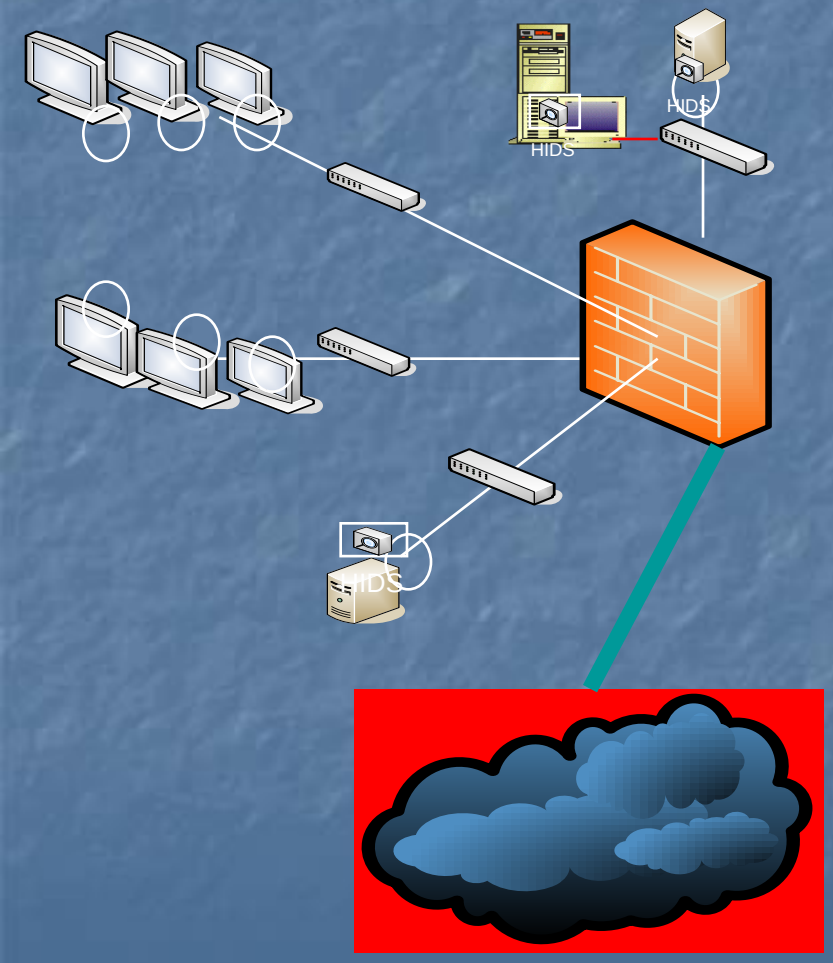
HoneyNet Infrastructure, For Artifact (malware) capture and identification (origin IP, ..)

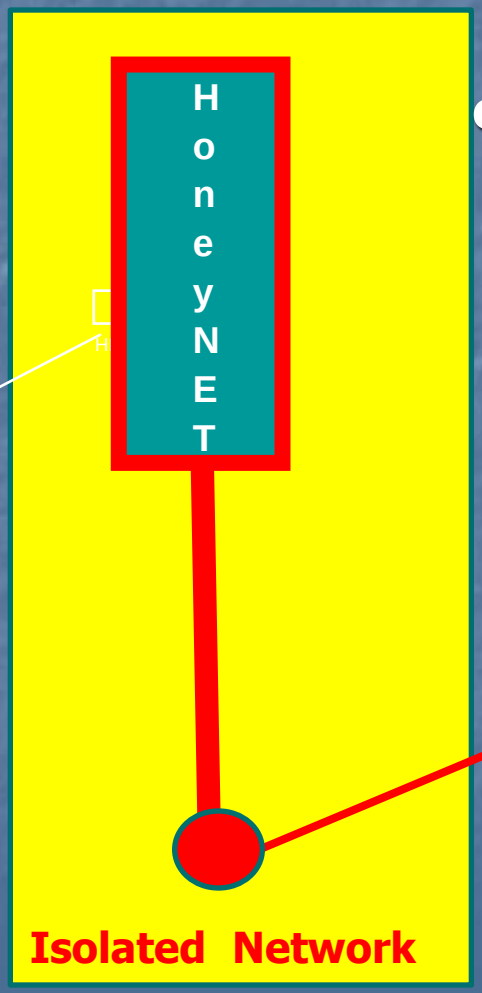
+ Permits also to let your constituency (mainly ISP) beleive in your supervision of the security of the cyber-space (bots, worm propagation, ..)

« Honey-Nets »

« Attract » and « jail »

intrusion toolkits/artifacts



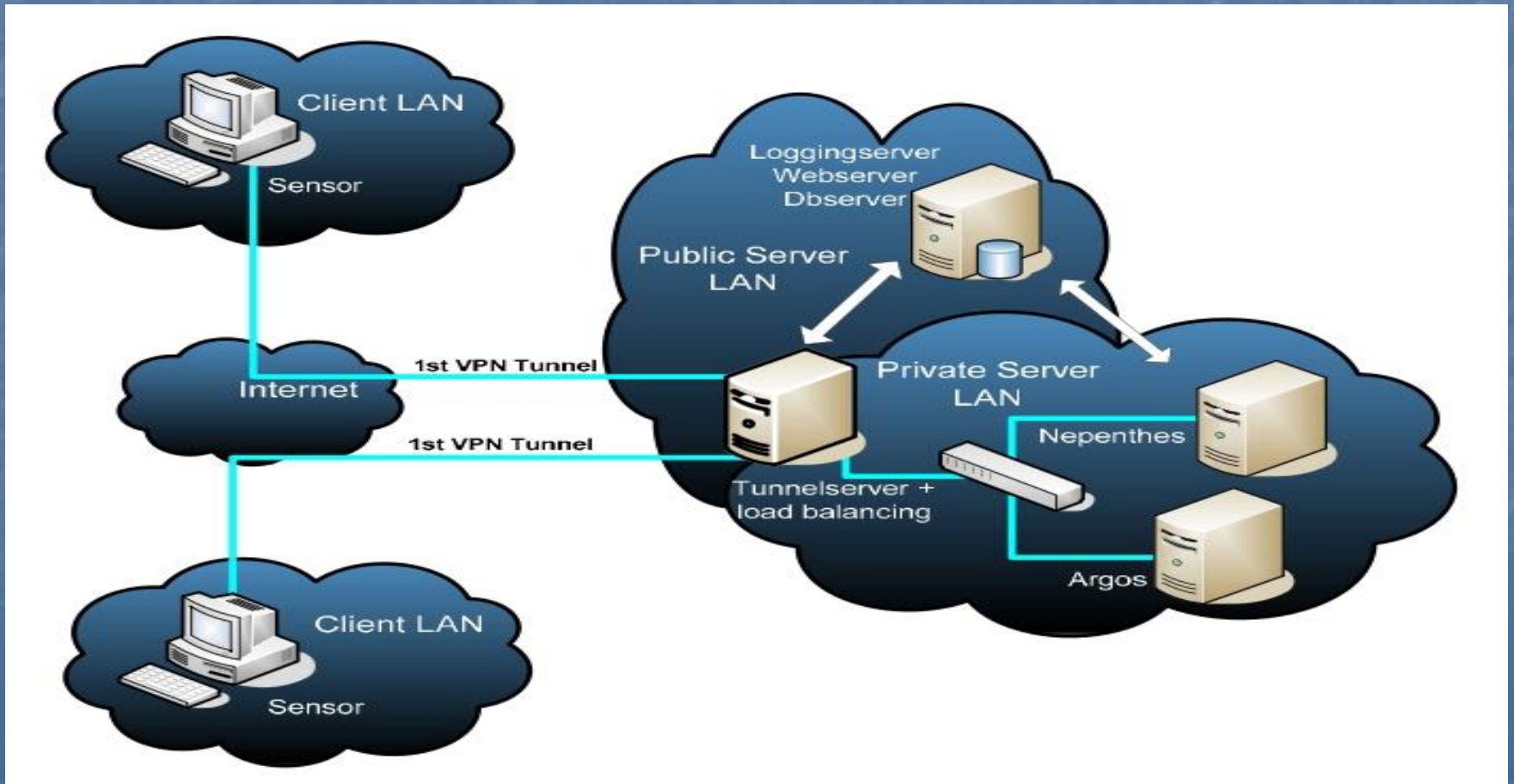


emulate Virtual vulnerable machine/ services(/Networks)

Low Interraction Honeynet System

SURFcert-IDS

Distributed Intrusion Detection System (D-IDS) based on a client-server approach, where the clients (sensors) contain a **honeypot and/or a passive analysis tool like snort.**

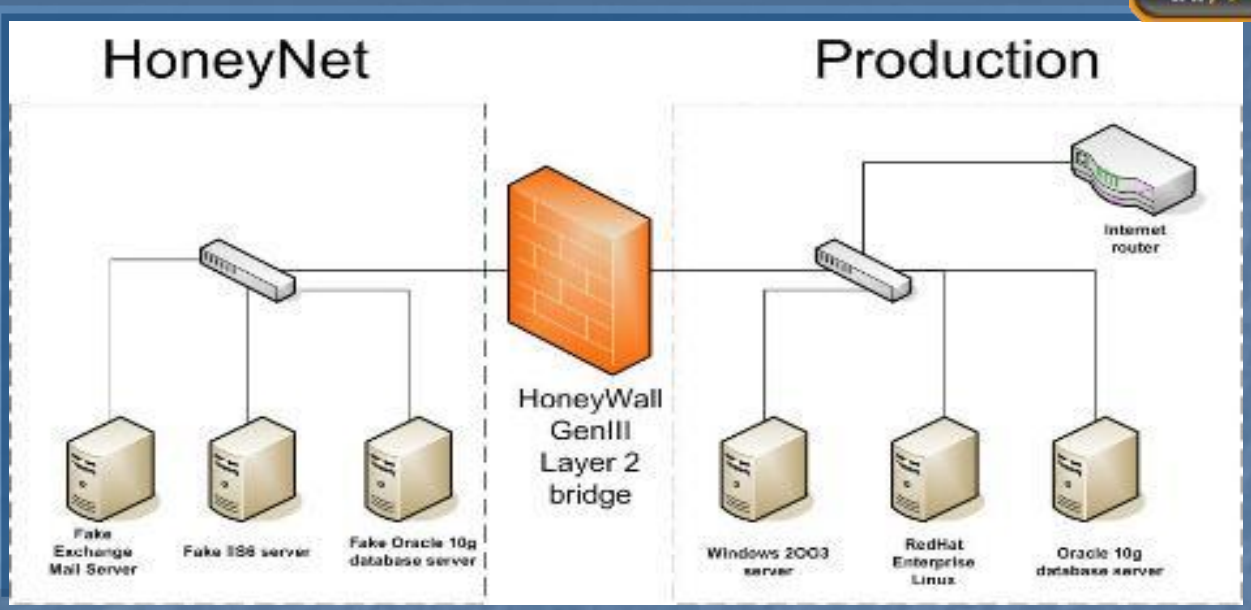


SURFcert-IDS
HoneyPot Tools

SMTP-HP	SMTP-HP	honeypot, which analyze **malicious e-mails** and use these data in SurfNetids system.
Kippo	kippo SSH Honeypot	a medium interaction SSH honeypot designed to **log brute force attacks** and, most importantly, the **entire shell** interaction performed by the attacker.
Dionaea	dionaea	A low interaction Honeypot, which emulates known vulnerabilities and captures worms as they attempt to infect it.
Glastopf	Glastopf	a Honeypot which emulates thousands of vulnerabilities, to gather data from **attacks targeting web applications**.

High Interraction HoneyNet

HoneyWall



HoneyBow

HoneyBow : a high-interaction malware collection toolkit

Honeymole

used for honeypot farms. Permits to deploy multiple sensors that redirect traffic to a centralized collection of honeypots.

Honeyd : a low-interaction honeypot used for capturing attacker activity.

....

Artifact Analysis
« **Laboratory** »

CUKOO : Open source Malware analysis system.

Execute an artifact inside an isolated environment.

Allow to understand how artifact work and what they would do when deployed and understand the context, the motivations and the goals of a breach.
→ respond to it and protect from it in the future

Cuckoo generates :

- Native functions and Windows API calls traces
- Copies of files created and deleted from the filesystem
- Dump of the memory of the selected process
- Full memory dump of the analysis machine
- Screenshots of the desktop during the execution of the malware analysis
- Network dump generated by the machine used for the analysis

REMnux a freeware , which incorporates many tools for analyzing Windows and Linux malware, like examining browser-based threats (obfuscated JavaScript,..)

Zero Wine : a full-featured open-source tool for dynamically analyzing the behavior of Windows malware by running it in a sandbox (WINE emulator).
The output generated by wine are the API calls used by the malware, allowing analysis of malware's behavior

Sandboxie + Buster Sandbox Analyzer : a freeware wrapper around the Sandboxie tool for Windows, which analyze the behaviour of processes and the changes made to system and then evaluate if they are malware suspicious

Malheur a tool for analyzing the volumes of data collected by behavioral sandboxes.

….

Metasploit (community) Framework

Permit to create and test exploits, via a modular approach, allowing the **combination of exploits with payloads**

using the Framework , you are helped in the steps for exploiting a system :

- Permit choosing and configuring an exploit (about 900 different exploits for Windows, Unix/Linux and Mac OS X) and check whether the intended target system is vulnerable to the chosen exploit
- Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server);
- Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;

→ Executing the exploit.

Metasploit runs on Unix (including Linux and Mac OS X) and on Windows

II-Implementing the CSIRT process , with Open-Source tools

Alert and Warning (& announcement) Process

"The" Tool for the Management of the Alert and Warning Process's Workflow

Taranis, developed by GOVCERT.NL. specifically designed to fit the workflow of a CSIRT Watch unit, and used by more than twenty countries.

- **implement a workflow for this process** and permit to assist the team in the **collection, analysis and publishing of security information**:
  - **Collect**: Collect information from different sources. Taranis supports around 900 sources: HTTP sources, IMAP and POP3, based sources
  - **Assess**: Determine the relevance of news-items.
  - **Analyze**: Analyze relevant news-items and determine the appropriate products that are to be created on the subject.
  - **Write**: Write **advisories and alert e-mails** and apply the standard quality assurance cycle.
  - **Publish**: Send out the products to the **relevant target audience**. The publicly available version of Taranis currently only supports e-mails. Other output mechanisms as SMS and CMS (websites) can be integrated.
- Vulnerabilities are directly indicated with **CVE IDs**, and is based on the **CPE** Common Platform Enumeration) list, with mechanisms to keep both lists and the mapping between them up to date.

Tool for the management of the publishing (NEW CSIRTs)

PHPList : an open-source mailing-list management tool.

Provide interesting features, especially for a **new CSIRT** :

- **Open/View Tracking :**Tells you how many users opened your message.
- **Click Tracking : tracks links and URLs. Statistics by message, URL and subscriber**
- define automated actions on receipt of bounce messages according to matches with regular expressions.
- Batch Sending Processing

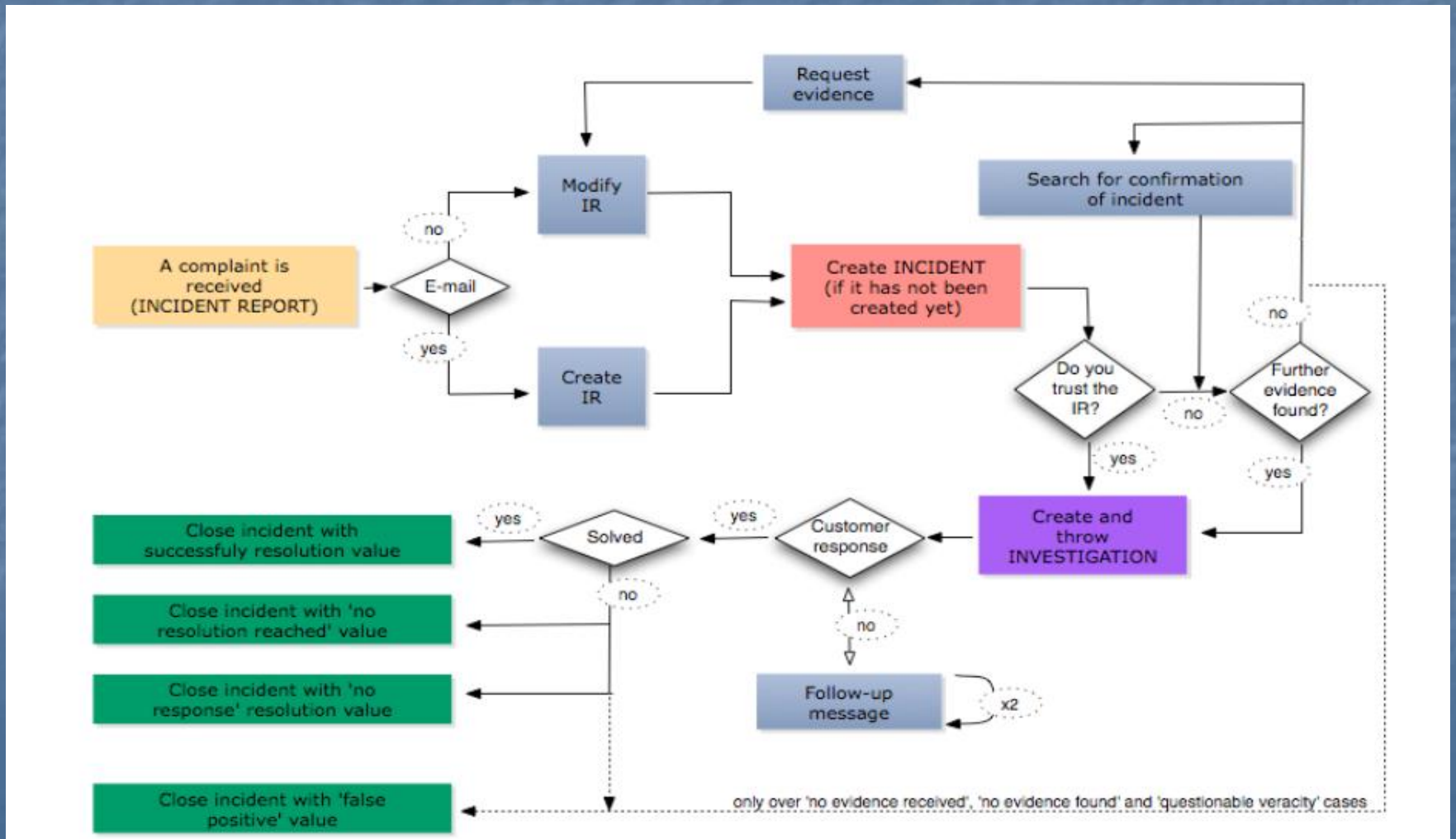
....

Incident Handling Process

RTIR tool *(Request Tracker for Incident Response)*

Incident handling and ticketing open source system, originally developed by JANET CSIRT, And now TF-CSIRT

→ Implement the complete **workflow for Incident Handling** management :



GLPI, Amended version used by TunCERT

originally an Information Resource-Manager (ITIL compliant Service desk)

- offers very rich functionalities for intervention handling and ***Technical knowledge sharing***, along with rich statistics and report generation and ***ease of amendment of its code***

- *GLPI Incident Tracking functionalities*
  - Tracking requests opened **manually** or by **processing of incoming email requests**
  - Tracking of Reports, with priority management, and possible Link between them (**correlated events**)
  - Management of the tracking requests and rules when opening tickets and SLA with **escalation** , customizables
  - Concept of “problems” (**set of related incidents**)
  - Assignment of incident, with display of the interventions assigned to an IH and assignment of time of intervention
  - Handling of requests for validations and **mail tracking of interventions**
  - Management of **planning of intervention** and display of History of done interventions

III- Open-source tools for Managing CSIRTs activities

Examples Of Performant Tools for File&Memory Forensics

Sleuth Kit

A **C library** and collection of **command line** **file forensic tools**.

-Runs on Windows and Unix)

- Supports the NTFS, FAT, ExFAT, UFS 1, UFS 2, EXT2FS, EXT3FS, Ext4, HFS, ISO 9660, and YAFFS2 file systems .
- show files that have been deleted /"hidden" by rootkits
- Analyzes raw , Expert Witness (EnCase) and AFF file system and disk images.

The TSK Framework allows incorporation of file analysis modules written by other developers.

Pb : Command Line =>

Autopsy

→ A **GUI** to the tools in The Sleuth Kit,

→ Provides case management, image integrity, keyword searching, and other automated operations :

- Timeline Analysis - Advanced graphical event viewing interface .
- Hash Filtering - Flag known bad files and ignore known good..

Web Artifacts (extract history, bookmarks, and cookies from Firefox, Chrome, and IE).

Data Carving (Recover deleted files from unallocated space)

Multimedia (eExtract EXIF from pictures and watch videos)

Indicators of Compromise (Scan a computer using STIX).

Volatility : A tool for Memory Forensics

Collection of open source tools, for the extraction of digital artifacts from volatile memory (RAM) **samples**

Supports a variety of sample formats (ie, Crash dump, Hibernation, DD)

Supports analysis for **Linux, Windows, Mac, and Android systems** :

Extract information (processes, threads, sockets, connections, modules) from physical memory samples:

- Running processes
- Open network sockets/network connections
- DLLs loaded /Open files /Open registry handles for each process
- A process' addressable memory
- OS kernel modules
- Mapping physical offsets to virtual addresses (strings to process)/Virtual Address Descriptor information

Open source/Freeware tools for Digital forensic investigation (Live DVD distributions)

DFF (Digital Forensic Framework)

Digital file forensic tool and a development platform for digital forensics and evidence gathering.

- *Windows and Linux OS forensics*
- *P**reserve digital chain of custody**, by including **Software write blocker**, cryptographic hash calculation and Virtual machine disk reconstruction VmWare (VMDK) compatible*
- ***volatile memory forensics** (Processes, local files, binary extraction, network connections).*
- ***Recover hidden and deleted artifacts**(Deleted files / folders, unallocated spaces, carving)*
- *Read standard digital forensics file formats (Raw, Encase EWF, AFF 3 file formats) and offer Quickly triage and search for (meta-)data, with various tools for Windows and Linux OS forensics (Registry, Mailboxes, NTFS, EXTFS 2/3/4, FAT 12/16/32 file systems).*

http://www.digital-forensic.org/

DEFT

A Linux Live CD which bundles some of the most popular open source and freeware) computer forensic tools (**and distributions**) .

Contains **hundreds** of tools for **Mobile Forensics**, Network Forensics, Data Recovery, and Hashing.

DEFT most important package and tool list:

- Full support for Bitlocker encrypted disks
- Sleuthkit , analyze disk images and perform in-depth analysis of file systems
- Mobile Forensics : Full support for Android and iOS logical acquisitions
- File Manager with disk mount's status
- Skype Extractor, utility for reading and extracting information from the Skype Internet telephone software user data files
- open source intelligence tools

http://www.deftlinux.net/download/

SANS Institute's Investigative Forensic Toolkit SIFT

VMware appliance, pre-configured with the necessary tools to perform and conduct an in-depth forensic or incident response investigation.

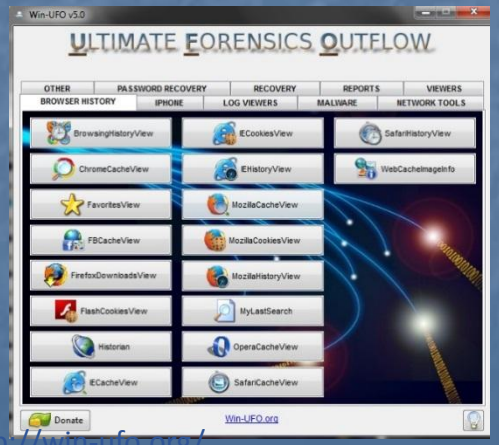
- includes **more than one hundred open-source tools**, including Autopsy, log2timeline for generating a timeline from system logs, Scalpel for data file carving, Rifiuti for examining the recycle bin, and lots more.
- supports analysis of almost all forensics file formats (Expert Witness Format (E01), Advanced Forensic Format (AFF), ..) and RAW (dd) evidence formats.

http://digital-forensics.sans.org/community/downloads

CAINE (Computer Aided INvestigative Environment)

CAINE - an (Italian) Linux Live distribution that contains a wealth of digital forensic tools.
Include a **user-friendly GUI**, semi-automated report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more.
http://www.caine-live.net/

- **Windows version** : Win-Ufo , **http://win-ufo.org/**



http://win-ufo.org/

PlainSight

A versatile computer forensics environment for **inexperienced** forensic practitioners.
→ Open source forensic/security tools, customized and combined with an **intuitive user interface to create an easy to use forensic environment** :

- Examine physical memory dumps
- Discover USB storage information
- Discover recent documents
- Recover/Carve over 15 different file types
- Examine UserAssist information
- Extract LanMan password hashes
- Get hard disk and partition information
- Extract user and group information
- View Internet histories

http://www.plainsight.info/index.html

Open Source Intelligence Platforms

Maltego

Offer **timous mining and gathering of information** as well as the representation of this information in a easy to understand format.

- Helps for the **information gathering phase** of all security related work (discovery of "hidden" information).
- Aids in the thinking process, by **visually demonstrating interconnected links between searched items**.

→ Determine the "**hidden**" relationships and real world links between:

- Target and Groups of people (social networks)
- Companies & Organizations
- Web sites
- Internet infrastructure (Domains,DNS names,Netblocks,IP addresses)
- Phrases
- Affiliations
- Documents and files

→ provides a GUI that makes seeing these relationships instant and accurate
→ Highlight hidden connections.

And much more :

Open Computer Forensics Architecture OCFA (http://ocfa.sourceforge.net/ **)**

…

And also tools for auditing source codes

RATS : tool for scanning C, C++, Perl, PHP, Python and Ruby source code
and flagging common security related programming errors such as buffer overflows and TOCTOU (Time Of Check, Time Of Use) race conditions, …

Sonar : JAVA
Seven analysis axis, with potential bugs detection :

+ Plugins for C, C#, PHP, PL/SQL, also Cobol ...

FindBugs, for Java

Other code source checkers, for C :

C++ lint: http://sourceforge.net/projects/clint/
flawfinder, : http://www.dwheeler.com/flawfinder/
PScan: http://www.striker.ottawa.on.ca/~aland/pscan/
Splint : http://splint.org/
Cqual : http://www.cs.berkeley.edu/~jfoster/cqual/
MOPS : http://www.cs.berkeley.edu/~daw/mops/
BOON http://www.cs.berkeley.edu/~daw/boon/
Blast : http://www-cad.eecs.berkeley.edu/~rupak/blast/
LCLint: http://lclint.cs.virginia.edu/
ITs4: http://www.cigital.com/its4/

Start Small, and increment gradually

Skills FIRST!!!

THANKS FOR YOUR ATTENTION

Prof Nabil SAHLI
E-mail : nabilsahli@gmail.com