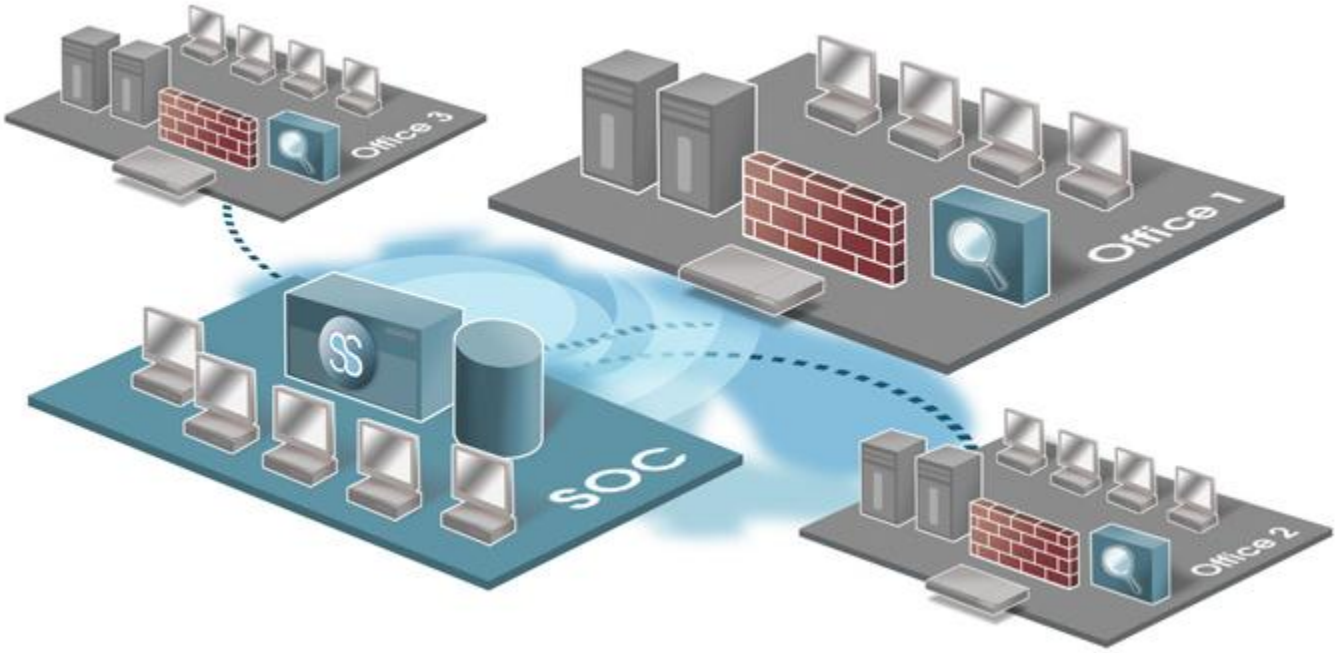
OSSIM

Presentación General



OSSIM en la red

OSSIM es una herramienta de monitorización de seguridad para administradores de sistema. Agrupa 22 programas libres, como cortafuegos, detectores de intrusos o antivirus, algunos tan conocidos como Nessus, Nmap o Snort, todos en un mismo paquete, que puede bajarse gratuitamente de Internet. Pero la función de OSSIM no es sólo poner a trabajar juntos estos programas: recoge y ordena la información que generan y la cruza, para hacer valoraciones sobre el estado de la red o buscar patrones que sirvan para detectar si está siendo atacada….

… La gracia de OSSIM es que, al integrar programas libres, no tiene que encargarse del desarrollo de éstos, que ya tienen su propia comunidad que los perfecciona. Así, todos los esfuerzos van a mejorar el motor que los pone a trabajar juntos. "Es el "efecto red" en su estado más puro: todo se reutiliza y no se hacen las cosas veinte veces. En nuestro caso, heredamos el esfuerzo de 22 productos y simplemente los ponemos a hablar entre ellos", explica Julio Casal, director del Área de Seguridad de IT Deusto y uno de los protagonistas de este éxito.

… La utilizan empresas desde Sudáfrica a Singapur, incluidas corporaciones y bancos españoles. La aventura de estos hackers, cuya empresa compraba IT Deusto a principios de 2004, es un buen ejemplo de cómo hacer negocio con un producto que se regala.

Downloads

SourceForge
+
Imagen
+
CVS

70.000 año

Seguridad Open Source

100%

Seguridad

Open Source

100% Auditable

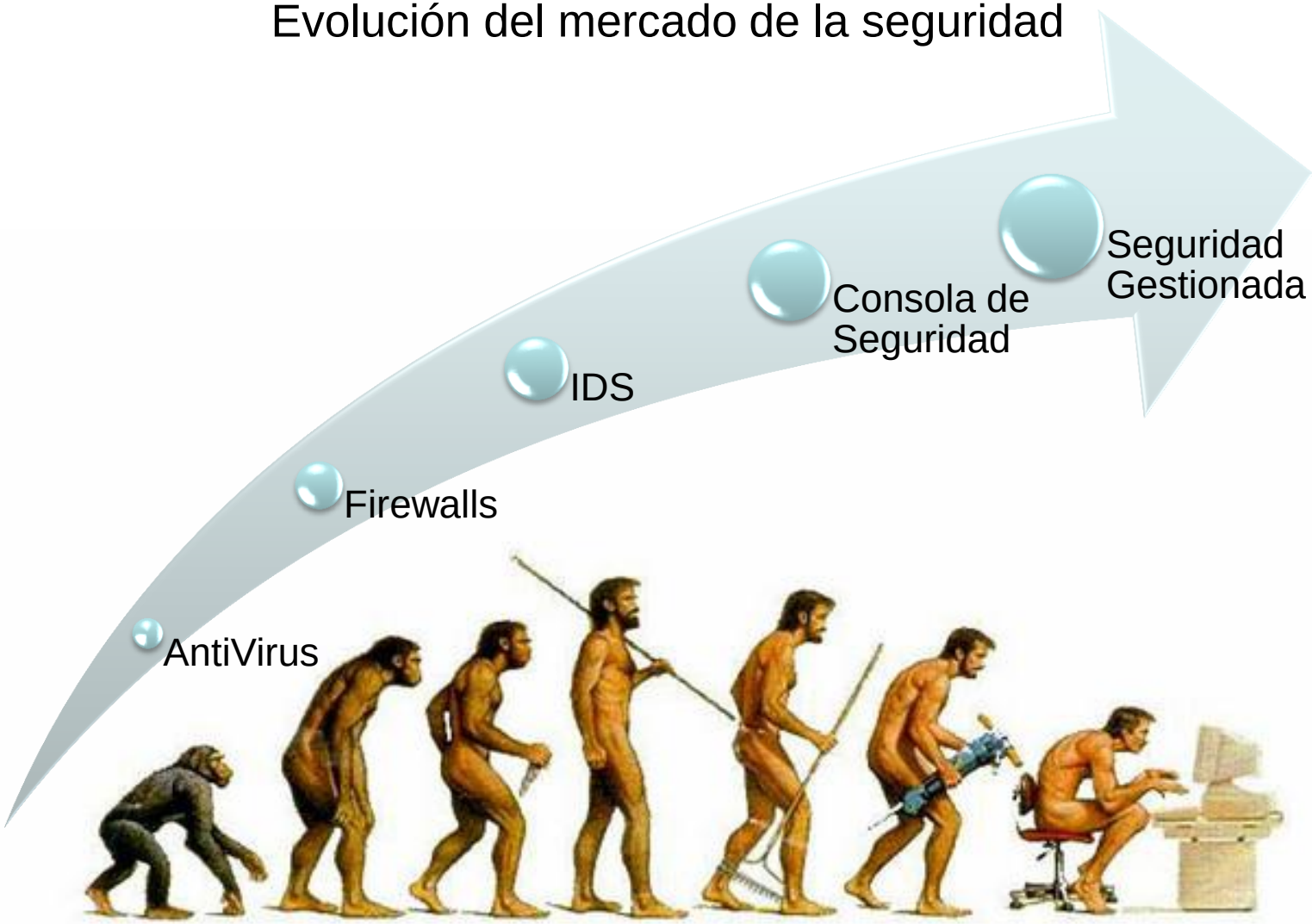
Cualquiera puede auditar el código fuente OSSIM en cualquier momento.

Gobierno y organizaciones estratégicas no deberían confiar en software ajeno.

100% Adaptable

Tener acceso al código fuente nos ofrece adaptabilidad del sistema.

Evolución del mercado de la seguridad

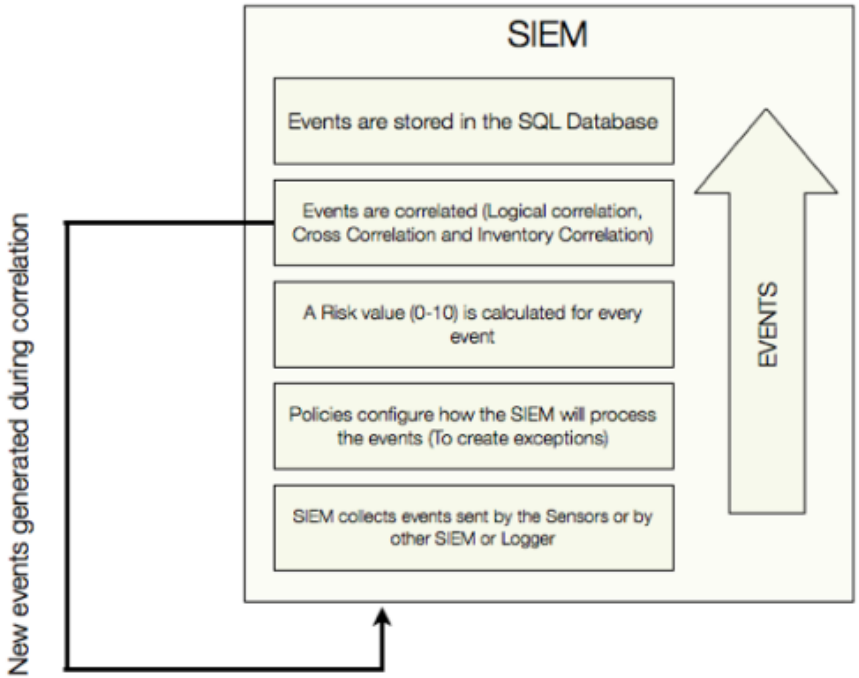


Quién Revisa los Logs

OSSIM Areas


Detection
Audit
Monitoring
Collect
Correlate
Analyze
Respond
EXECUTE
WAY
OSSIM

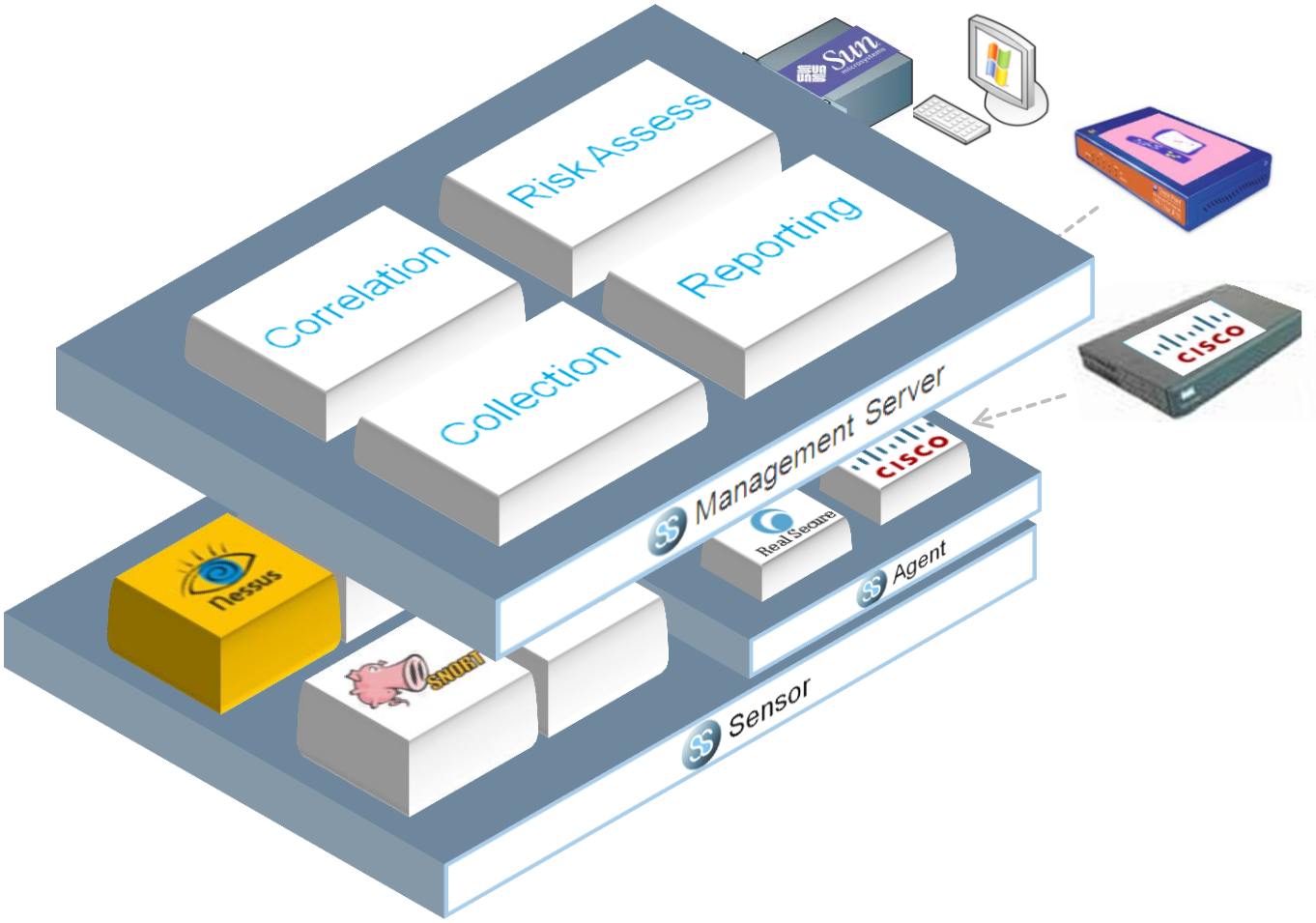
El flujo de un evento de seguridad a través de las componentes de OSSIM puede dar una idea suficientemente clara del proceso de correlación y normalización que es llevado a cabo.




SNORT
Nessus
Nagios
ntop
Acid/Base
SNARE
OSIRIS
Spade
Nmap
Scanmap 3D
osvdb
Arpwatch
pads
P0f
Oinkmaster
OpenVPN
RRD
Aberrant Behaviour
IPTABLES
Flows
OCS
inventory
MySQL
Collection
Correlation
Risk Assess
Reporting
Metrics
> 10 millones lineas código
350.000 lineas código

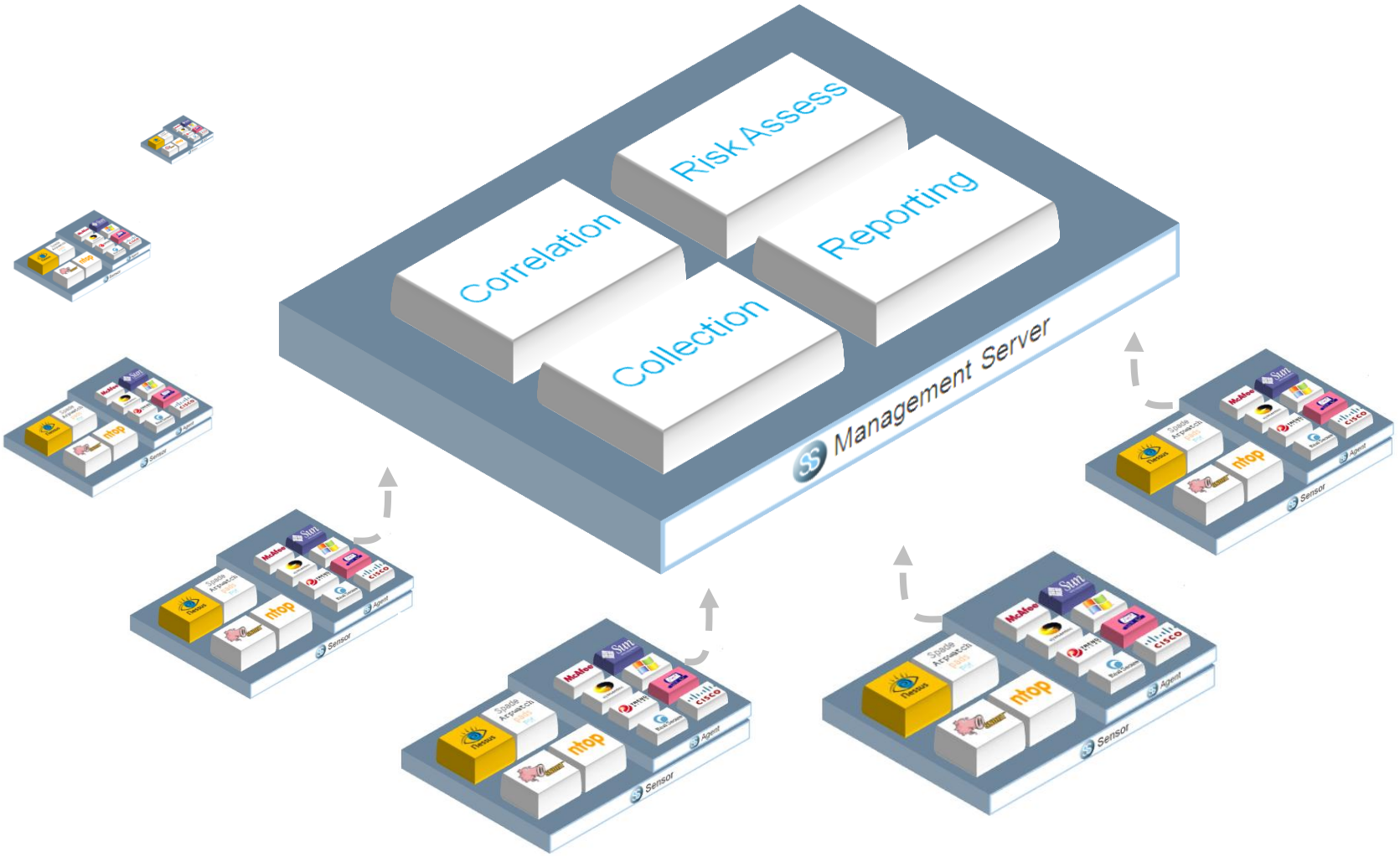
Agregación de logs

Integral Security System



OSSIM

Integral Security System



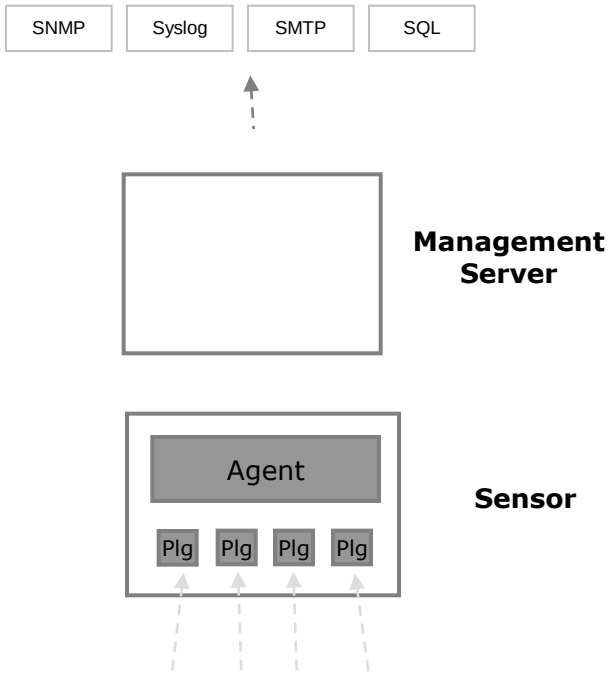
Interoperabilidad

OSSIM puede recoger datos y enviarlos a través de múltiples protocolos..

A través de un agente genérico es inmediato crear un plugin nuevo. Ejemplo de plugin de pads:

```
[DEFAULT]
plugin_id=1516
[config]
type=detector
enable=yes
source=log
location=/var/log/ossim/pads.csv
# create log file if it does not exists,
# otherwise stop processing this plugin
create_file=true
process=pads
start=yes   ; launch plugin process when agent starts
stop=no     ; shutdown plugin process when agent stops
startup=%(process)s -D -w %(location)s
shutdown=killall %(process)s

[pads-service]
event_type=host-service-event
regexp="^(\IPV4),([^,]*),([^,]*),([^,]*),([^,]*),(\d+)$"
host={$1}
port={$2}
protocol={$3}
service={$4}
application={$5}
plugin_sid=1
```

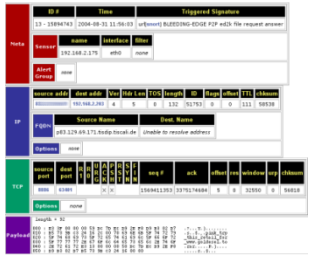


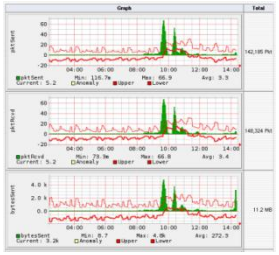
Syslog Syslog SNMP SNMP SNMP SNMP + SQL Syslog Syslog OPSEC Syslog Syslog SNARE

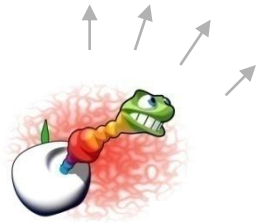
GFi APACHE HTTP SERVER symantec TREND MICRO Proveedor Oficial de Cursos al Canal McAfee Real Secure FORTINET REAL TIME NETWORK PROTECTION NETSCREEN CISCO Sun microsystems

Detección de Red

Detección de ataques de red a través de patrones y anomalías







pattern

anomalies

Spade

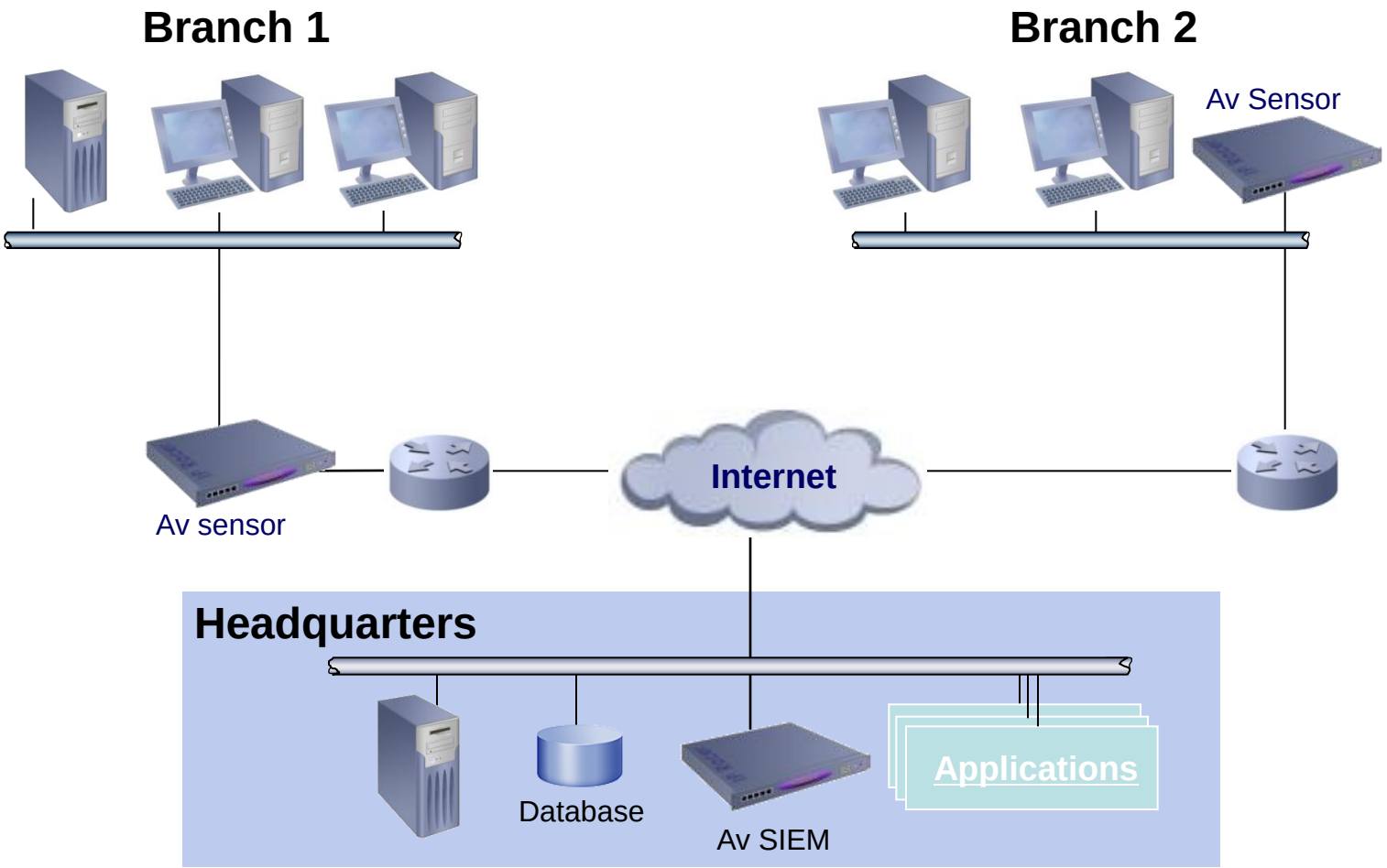
SNORT

RRD Aberrant Behaviour

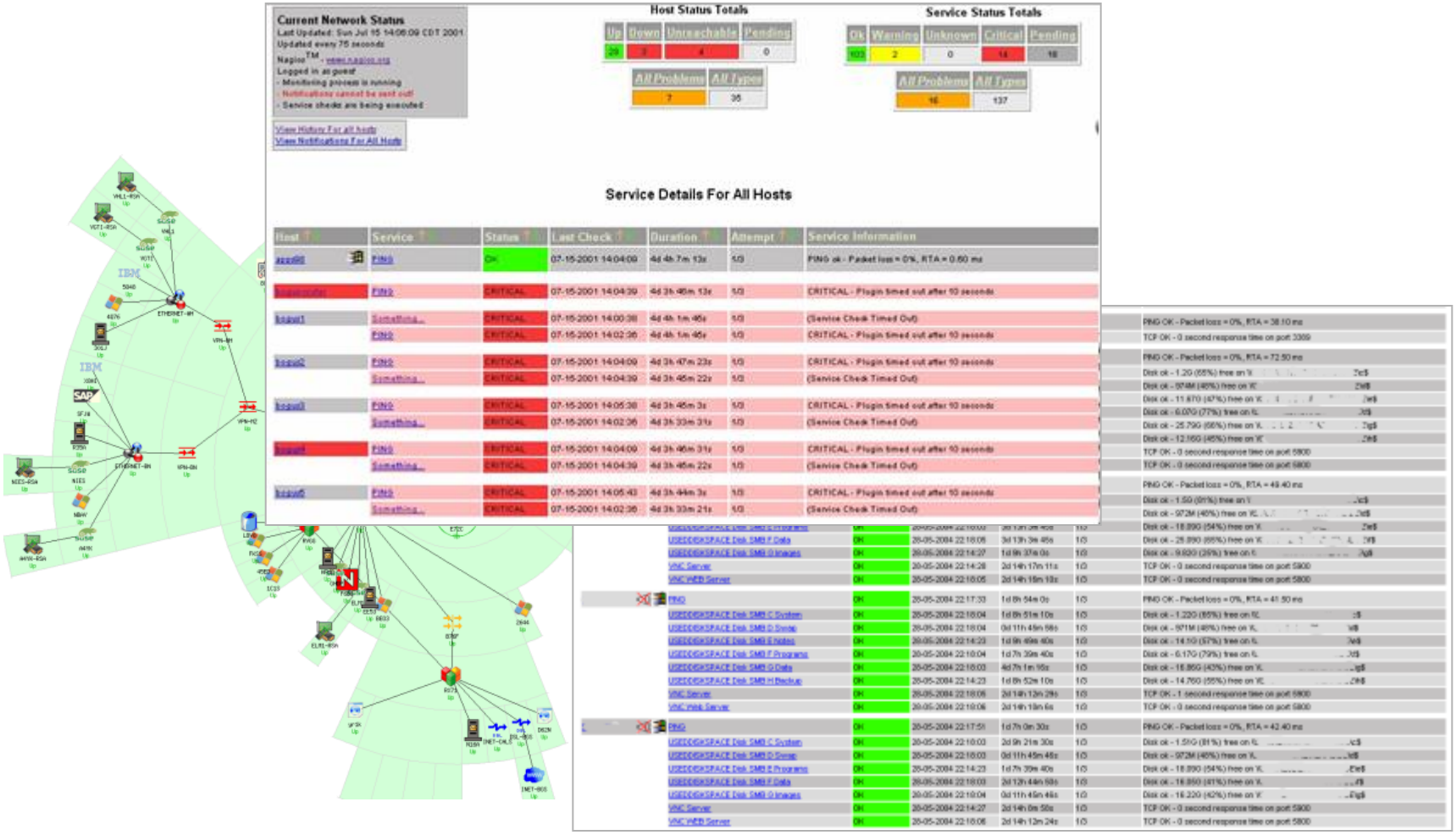
Arpwatch

pads

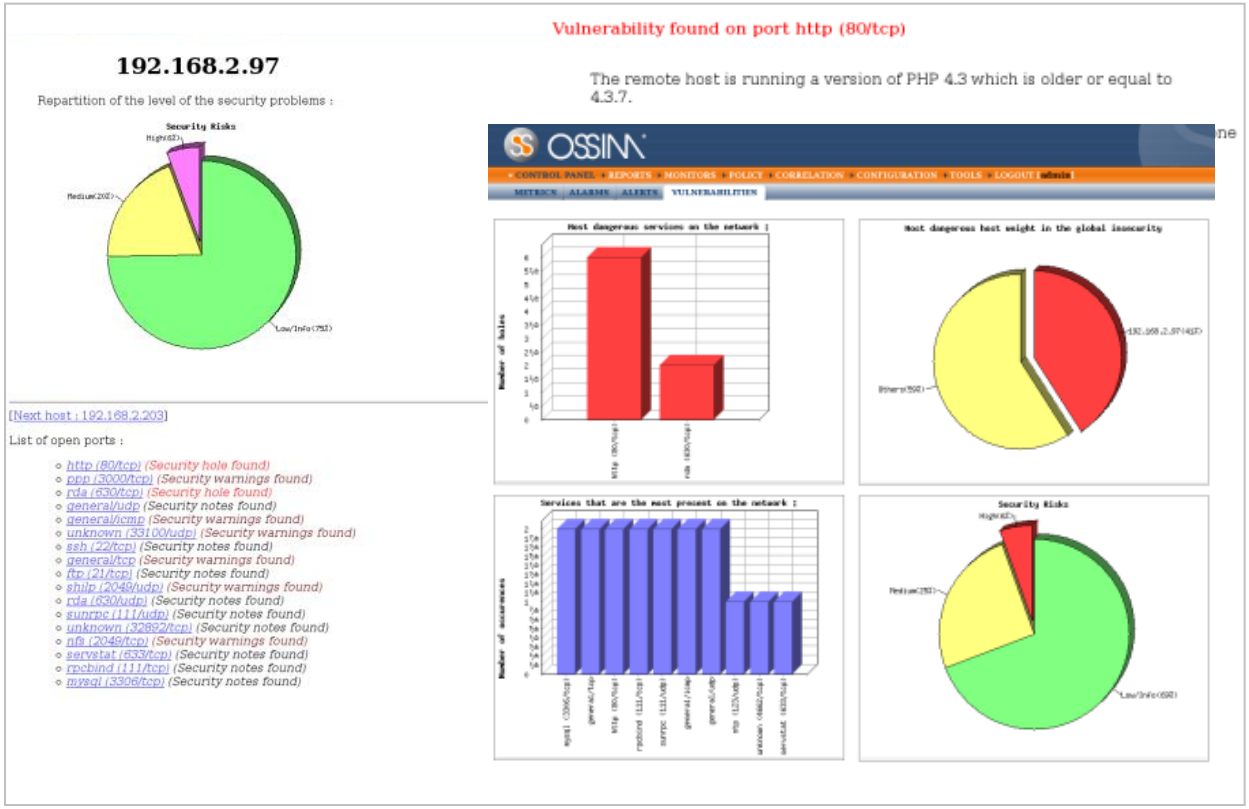
P0f


Branch 1
Branch 2
Av Sensor
Av sensor
Internet
Headquarters
Database
Av SIEM
Applications

Disponibilidad

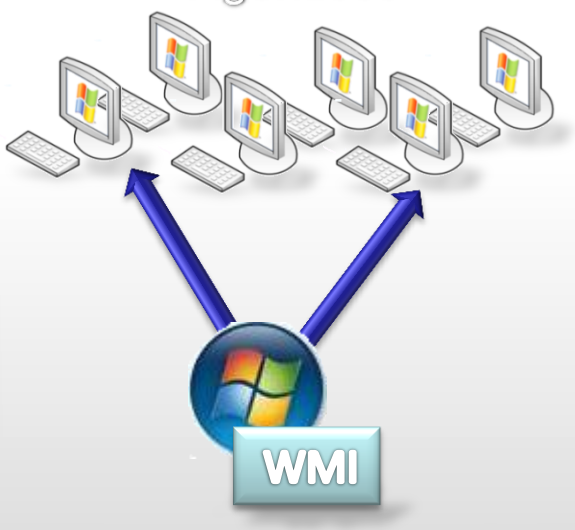


Vulnerabilidades



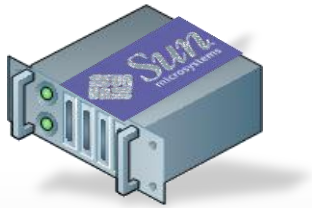
OSSIM

Agentless



- Remote Log Collection
- Real time correlation
- Response Execution

Agent



Server

Desktop

OSIRIS
- Integrity control

SNARE
- Host IDS

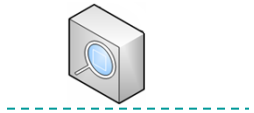
OSSEC
- Host IDS

OCS inventory
- Inventory

Inventario

Pasivo – Sin Agente

Arpwatch
pads
p0f



Activo – Sin Agente

Nmap

Agente

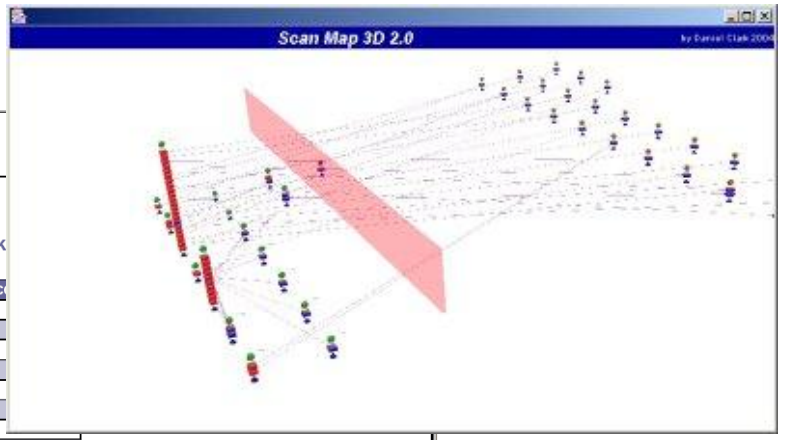
OCS inventory

Number	Software name
726	OCS Inventory Agent 4.0.3.2
723	Trend Micro OfficeScan Client
722	Microsoft Windows XP Professional
688	Crystal Report Viewer
673	SoundMAX
541	WinZip
531	Microsoft Office Professional Edition 2003
465	Broadcom Gigabit Integrated Controller
446	Intel(R) Graphics Media Accelerator Driver
424	Dell ResourceCD
409	Revisión de Windows XP - KB873339

Editor	Nombre
N/A	Diablo II
Microsoft Corporation	Microsoft Office Enterprise 2007
Kaspersky Lab	Kaspersky Internet Security 6.0
Microsoft Corporation	Hotfix for Windows Media Format SDK (KB900399)
Microsoft Corporation	Hotfix for Windows Media Format SDK (KB902344)
Microsoft Corporation	Hotfix for Windows Media Player 10 (KB907658)
Microsoft Corporation	Actualización de seguridad para el Reproductor de Windows Media (KB911564)
Microsoft Corporation	Actualización de seguridad para el Reproductor de Windows Media 10 (KB911565)
Microsoft Corporation	Actualización de seguridad para Windows XP (KB913433)
Microsoft Corporation	Actualización de seguridad para Windows XP (KB916281)
Microsoft Corp	
N/A	
N/A	
N/A	
N/A	
N/A	
Microsoft Corp	

Nombre:	DESKTOP		
Dominio:	INICIOMS	**Nombre del SO:**	Microsoft Windows XP Professional
Userdomain:	DESKTOP	**Versión del SO:**	5.1.2600
Último inventario:	04/04/2007 16:34:12	**Service pack:**	Service Pack 2
Dirección IP:	172.31.0.2	**Comentarios:**	Windows uE
Nombre usuario:	Administrador	**Usuario Windows:**	WinuE
Memoria:	512	**Número licencia Windows:**	55274-640-4350801-23820
Memoria virtual:	1250	**Clave Windows:**	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M
Nombre de red 1:	172.31.0.0	**Agente:**	OCS-NG_windows_client_v4032
Nombre de red 2:	0.0.0.0		

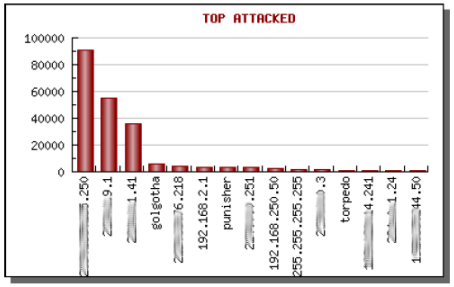
Reportes



OSSIM Security Report

Top 15 Attacked Hosts

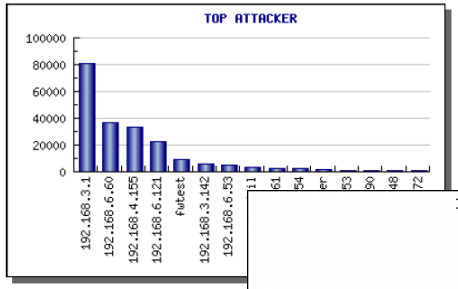
Host	Occurrences
2[redacted]255.250	90529
2[redacted]9.1	54888
2[redacted]1.41	36248
golgotha	6001
2[redacted]76.218	4057
192.168.2.1	3744
punisher	3224
2[redacted]0.251	3221
192.168.250.50	2592
255.255.255.255	1887
2[redacted]0.3	1284
torpedo	963
1[redacted]4.241	923
2[redacted]1.24	678
1[redacted]44.50	444



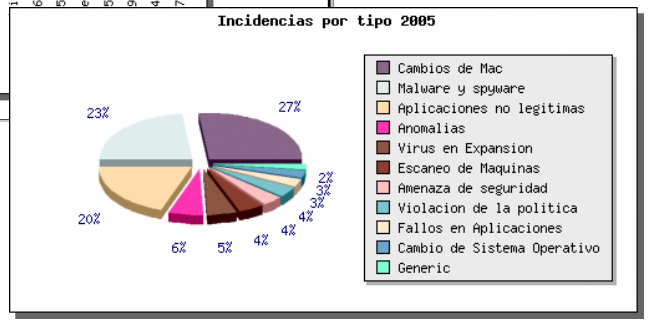
26-Apr-2005 Page 1/2

Top 15 Attack

Host	Occ
192.168.3.1	
192.168.6.60	
192.168.4.155	
192.168.6.121	
fwtest	
192.168.3.142	
192.168.6.53	
dgil	2964
192.168.6.61	2730
192.168.6.254	2613
punisher	2052
192.168.4.153	1108
192.168.6.190	843
192.168.4.148	753
192.168.5.72	703

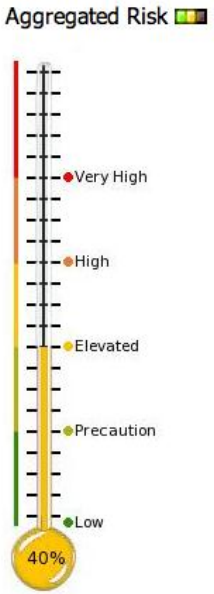


26-Apr-2005



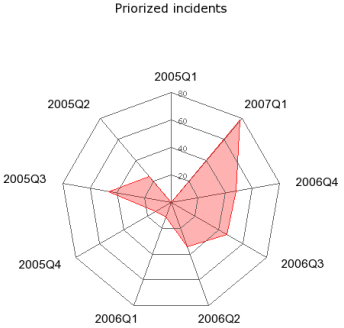
OSSIM posee una gran capacidad para generar objetos gráficos y métricas ordenados en Cuadros de Mando. Estos Cuadros de Mando pueden son modificados y customizados por el cliente a sus necesidades.

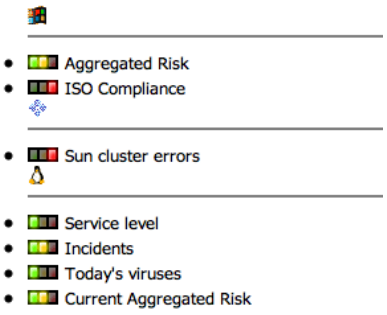
Reportes a Medida

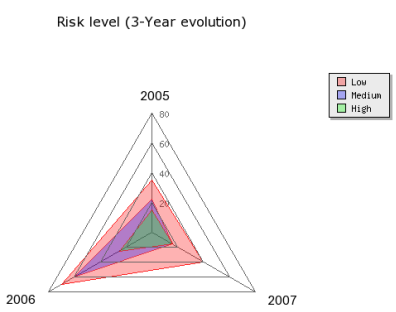


Virus count

e.jonson@acme.corp k.gates@acme.corp k.hamilton@acme
l.crhistensen@acme.corp
l.semsteen@acme.corp m.martin@acme.corp
m.tosi@acme.corp o.samuelson@acme.corp
p.smith@acme.corp p.soherti@acme.cc
q.peratti@acme.corp sservices@acme.corp
w.zafir@acme.corp







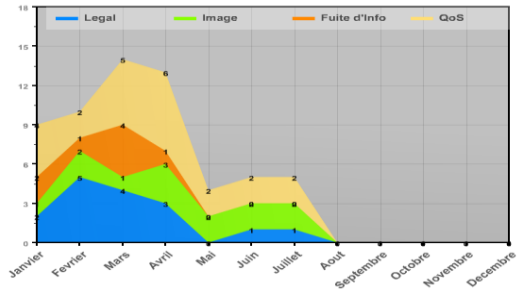
Security news feed [help]

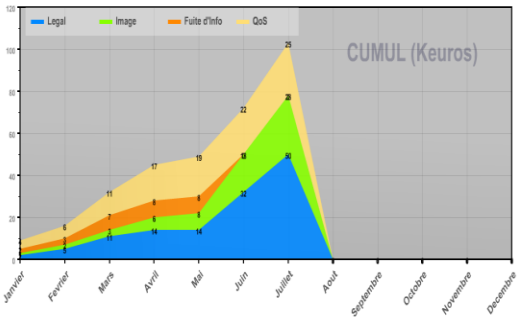
- [4/5] Mozilla Firefox Multiple Vulnerabilities Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to conduct spoofing attacks, bypass certain...
- [3/5] Mozilla Thunderbird Memory Corruption Vulnerability A vulnerability has been reported in Mozilla Thunderbird, which can potentially be exploited by malicious people to compromise a user's system.
- [4/5] Mozilla SeaMonkey Multiple Vulnerabilities Some vulnerabilities have been reported in Mozilla SeaMonkey, which can be exploited by malicious people to conduct spoofing attacks, bypass certa...
- [3/5] Bochs NE2000 RX Frame Overflow and Disk Controller Denial of Service Tavis Ormandy has reported some vulnerabilities in Bochs, which can be exploited by malicious people to cause a DoS (Denial of Service) or comprom...
- [2/5] Sun Solaris update for Adobe Flash Player Sun has issued an update for Sun Solaris. This fixes a vulnerability, which can be exploited by malicious people to bypass certain security restri...
- [3/5] Ubuntu update for freetype Ubuntu has issued an update for freetype. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service...
- [4/5] Gentoo update for mplayer Gentoo has issued an update for mplayer. This fixes some vulnerabilities, which potentially can be exploited by malicious people to compromise a u...
- [3/5] Gentoo update for freetype Gentoo has issued an update for freetype. This fixes a vulnerability, which can be exploited by malicious people to cause a DoS (Denial of Service...
- [4/5] Zenturi ProgramChecker ActiveX Components ActiveX Control "DownloadFile()" Insecure Method shinnai has discovered a vulnerability in Zenturi ProgramChecker, which can be exploited by malicious people to overwrite arbitrary files or compr...
- [4/5] Apple QuickTime Java Extension Two Vulnerabilities Two vulnerabilities have been reported in Apple QuickTime, which can be exploited by malicious people to gain knowledge of potentially sensitive i...

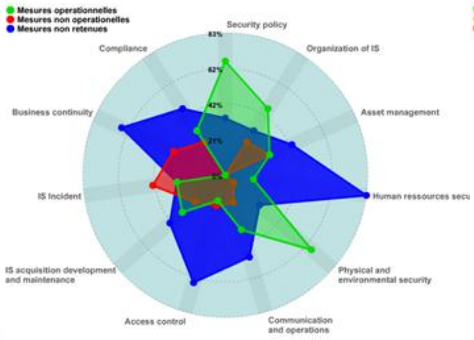
Compliance Framework

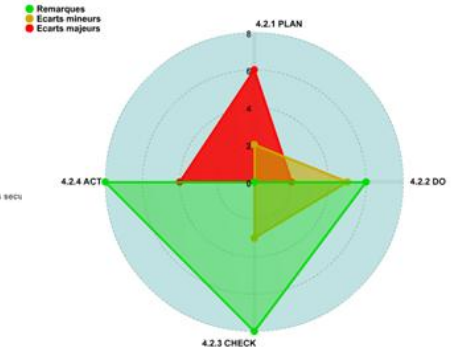
OSSIM Compliance Framework Solution, permite a las organizaciones medir sus niveles de seguridad de acuerdo a regulaciones como:

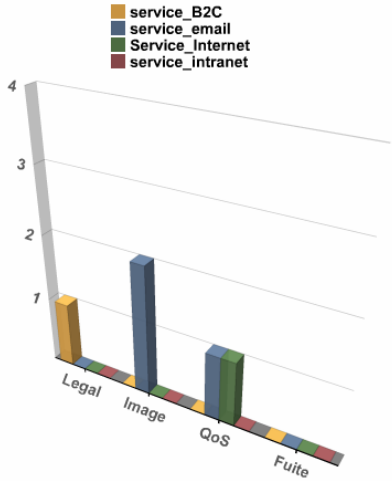
- ISO27001
- SOX
- PCI
- HIIPA

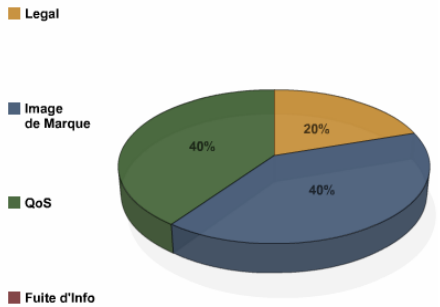




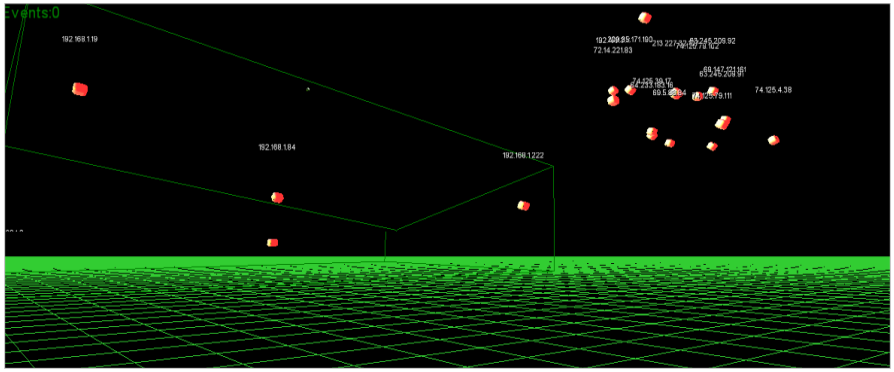




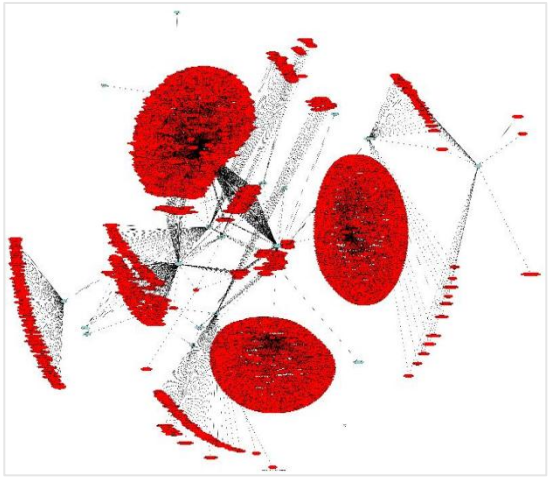




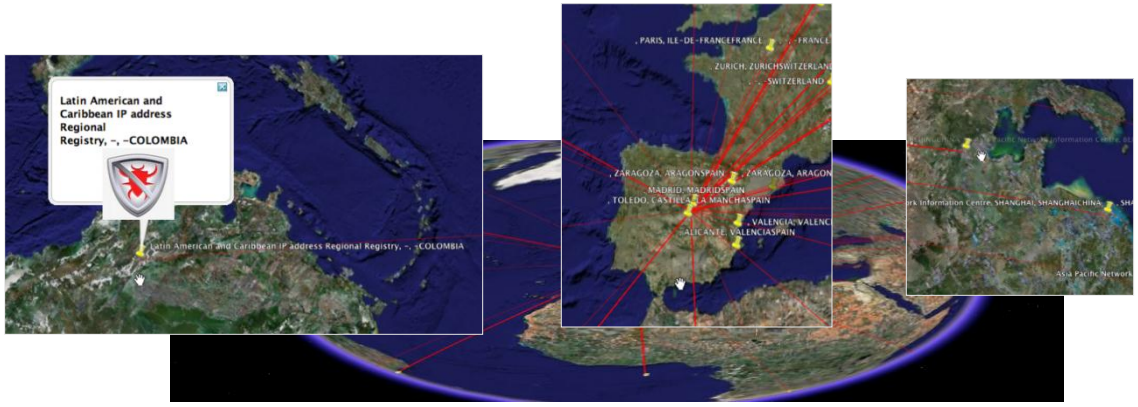
- Diferentes herramientas de visulización:



3D Visualization



World Botnet map 12/8/200



AV CERT Tools

DUDAS Y PREGUNTAS

GRACIAS!!