IT Deusto

Mayo del 2006
www.itdeusto.com

Gestión de la Seguridad con OSSIM

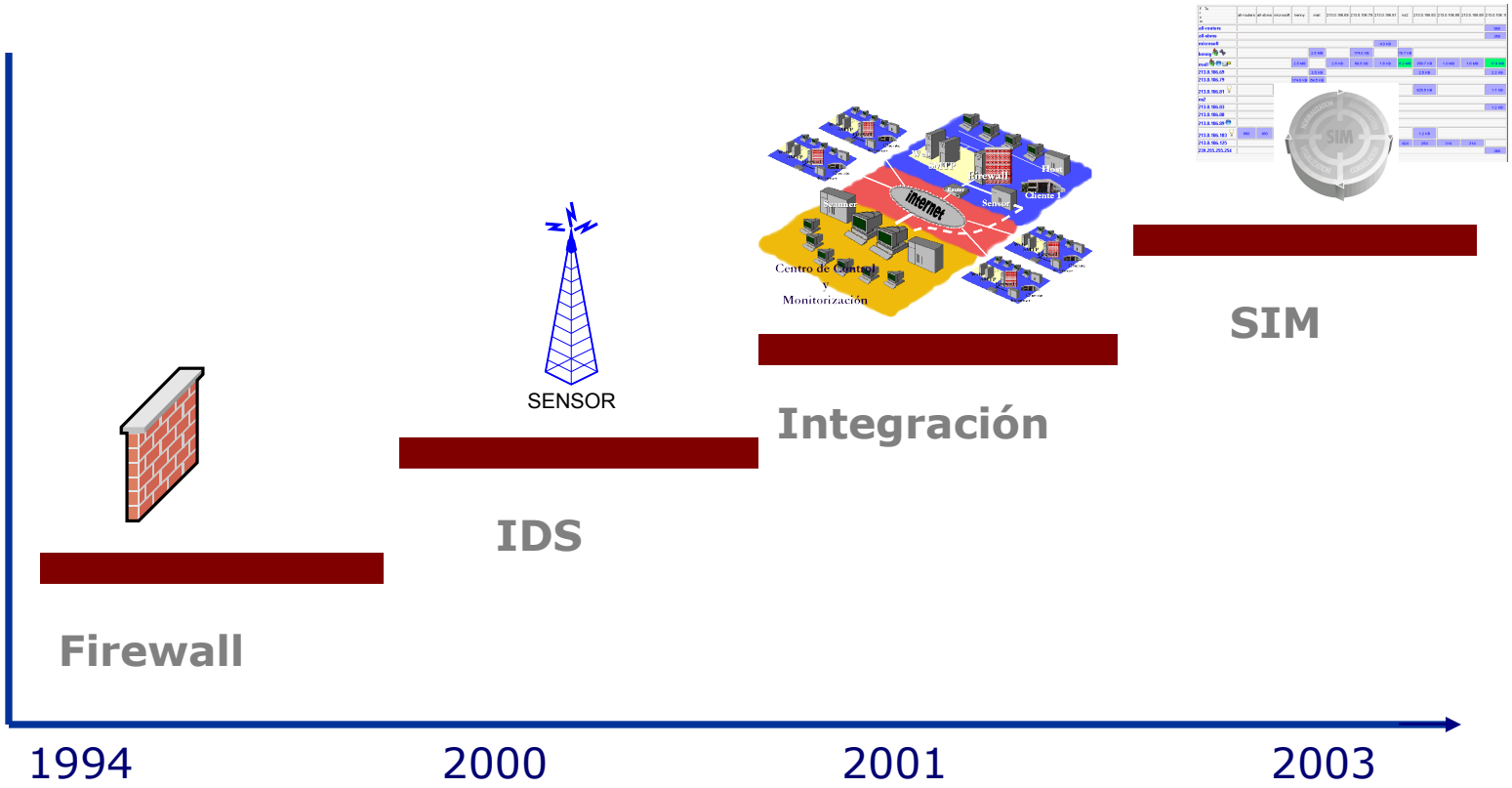
Gonzalo Asensio Asensio
Jefe de Proyecto Seguridad Informática
gasensio@itdeusto.com

La Seguridad en IT-Deusto

Área de Seguridad IT Deusto

- **IT-Deusto posee una larga experiencia y especialización.**
  - Responsables de Seguridad de Primeros ISP
  - Creación de IP6 Seguridad (1997) e IP Soluciones (2000)
  - Integración de IP Soluciones en IT- Deusto (2003)
- **Equipos de expertos: más de 40 personas dedicadas exclusivamente a la seguridad informática**
- **Soluciones de Seguridad propias Open Source (OSSIM)**

Evolución Tecnológica



El Problema

1. ¿Por donde empiezo?
1. ¿Cuales son las alertas de verdad?
1. ¿En que situación estoy?

La solución para Gestionar la Seguridad: OSSIM

Open **S**ource **S**ecurity **I**nformation **M**anagement

Consola de Gestión de Seguridad

(código abierto)

http://www.ossim.net/

SOURCEFORGE ENTERPRISE EDITION
Optimizing Distributed Development

http://sourceforge.net/projects/os-sim/

Se trata de un Producto líder, probado por más de 22.000 usuarios a nivel mundial.

¿Qué es OSSIM?

- **Plataforma de Seguridad Open Source** compuesta por más de 22 Herramientas lideres en el campo de la Seguridad Informática:

- Composición Básica de **OSSIM**;

5. **Servidor OSSIM (Consola de Gestión)**
6. **Framework (Interacción entre Módulos)**
7. **Base de datos de OSSIM (Eventos)**
8. **Agentes (Sondas Colectoras)**

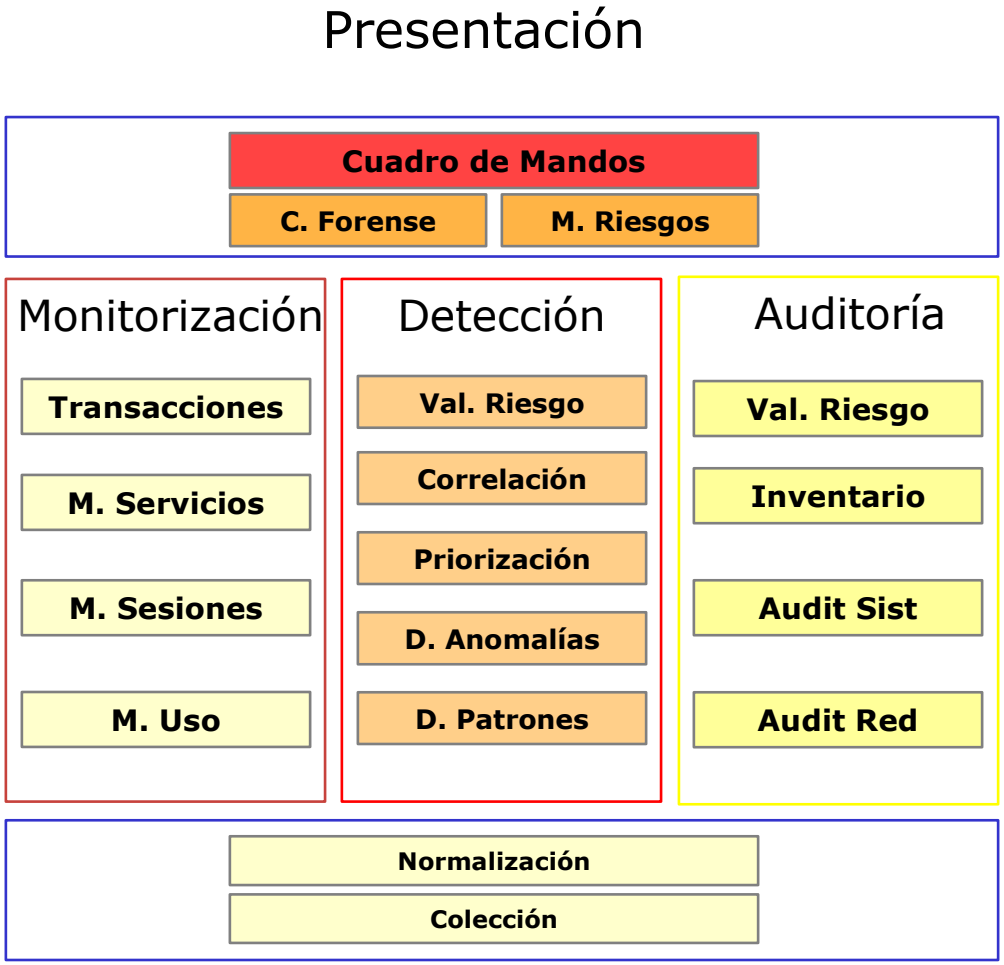
- **Todo montado sobre Sistemas Linux**

OSSIM. Herramientas Pioneras.

- Herramientas más Destacadas de OSSIM

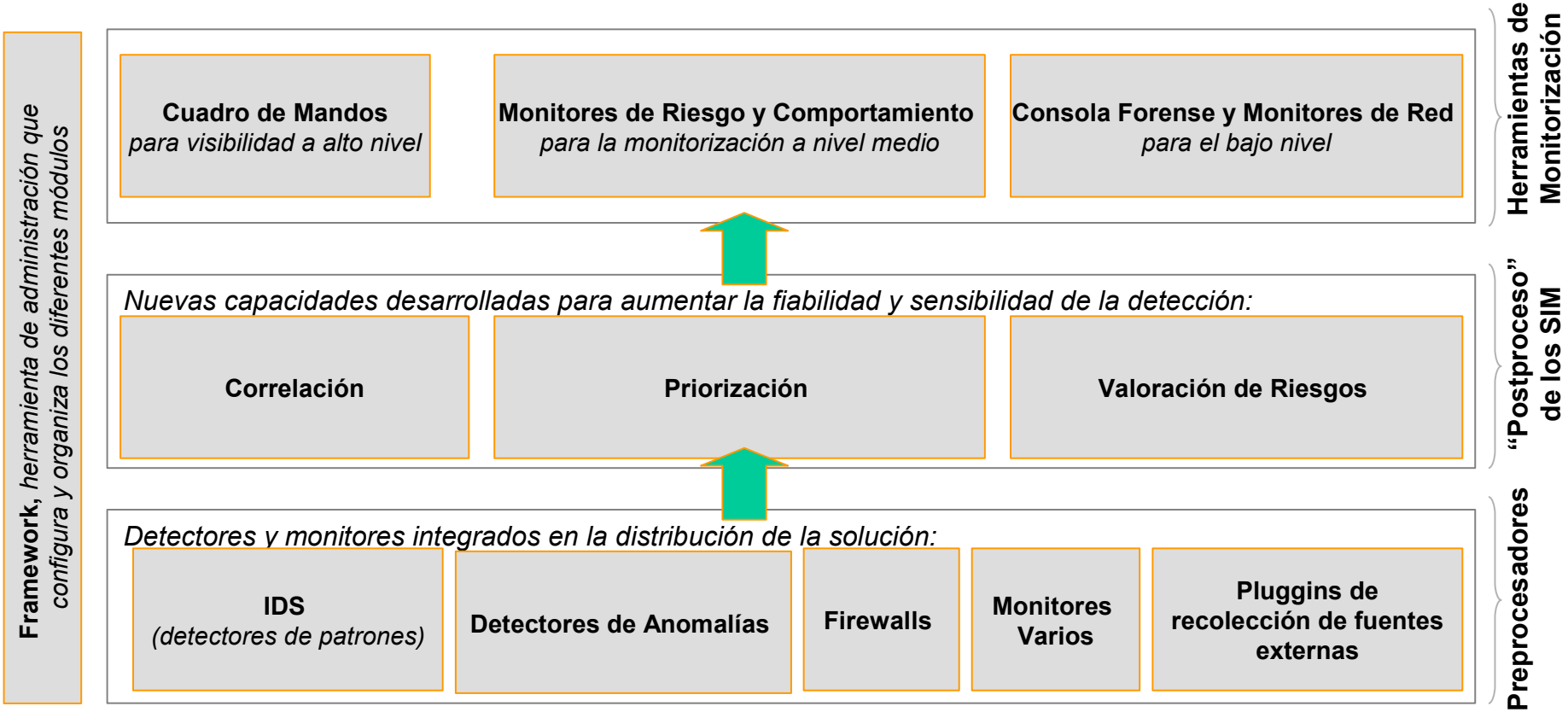
▪ IDS (Snort)
▪ Monitorización de tráfico de Red (Ntop)
▪ Anomalías y detección de nuevos Servicios (Pads)
▪ Anomalías de Red por comportamiento (Spade)
▪ Detección de Cambios de Mac (Arpwatch)
▪ Detección de Cambios de Sistema Operativo (P0f)
▪ Monitor de persistencia (rrd, Spade)
▪ Analizadores de protocolos (Ntop)
▪ Inventariado servicios activo (Nmap)
▪ Scanner de Vulnerabilidades (Nessus)
▪ IDS de HOST (Osiris)
▪ Recolección de Multiples Dispositivos (Plugins)

Security Information Management (SIM)



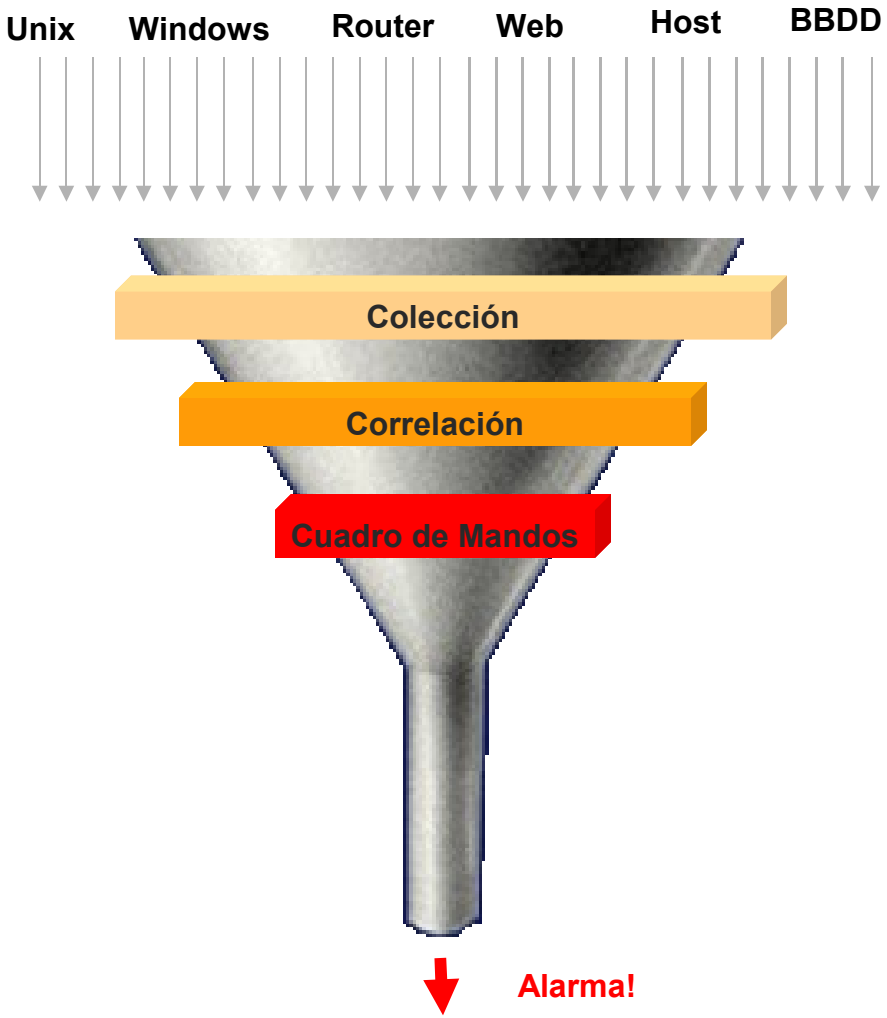
Funcionalidades de OSSIM

¿Cuáles son las principales funcionalidades?

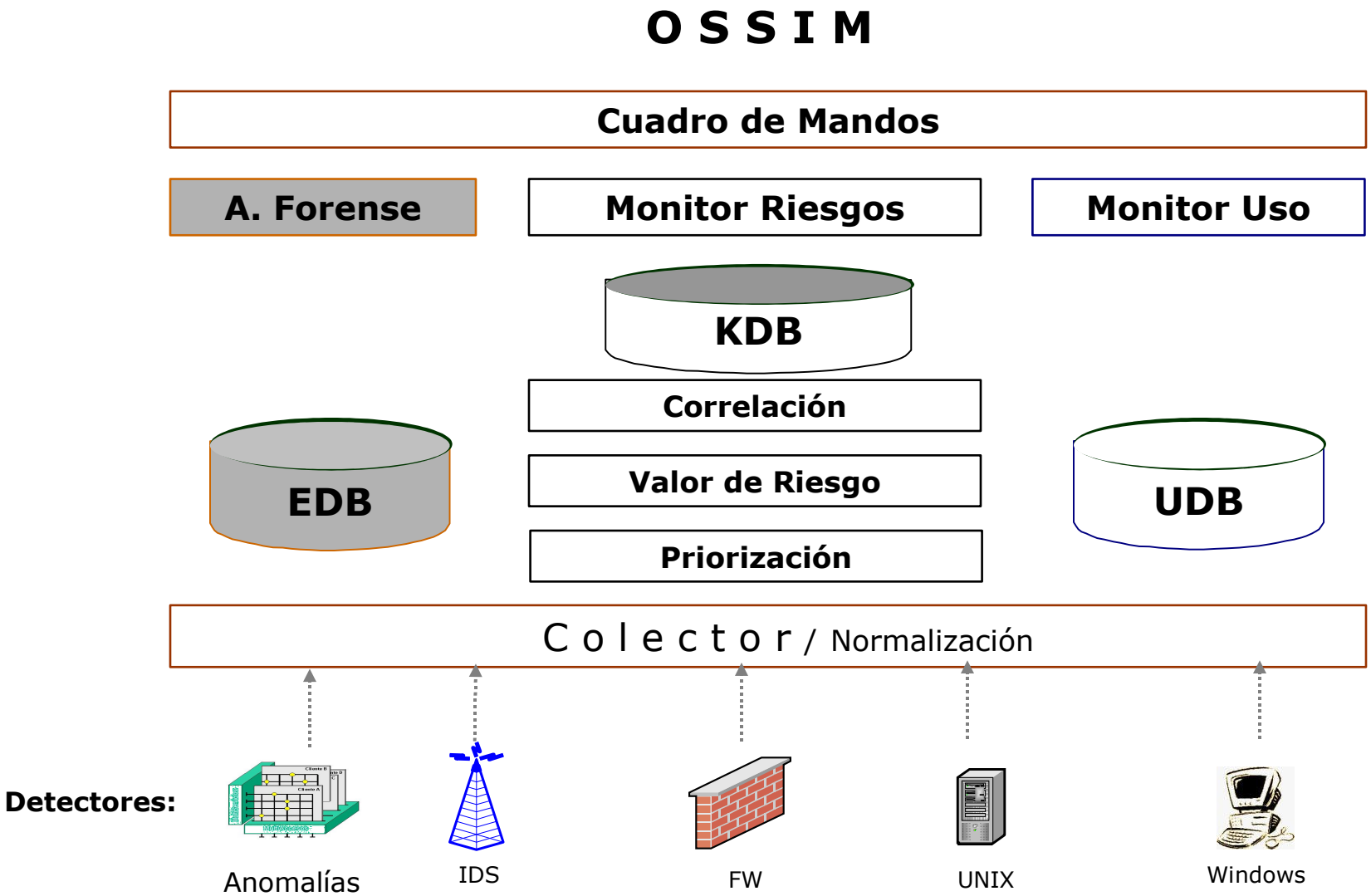


OSSIM complementa muchos otros productos de mercado que no disponen de todas sus funcionalidades

Efecto embudo

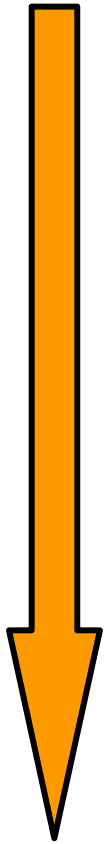


Arquitectura



De los Eventos a la Gestión de la Seguridad

1.- Colección
2.- Anomalías
3.- Priorización
4.- Valor del Riesgo
5.- Correlación
6.- Consola Forense
7.- Cuadro de Mandos



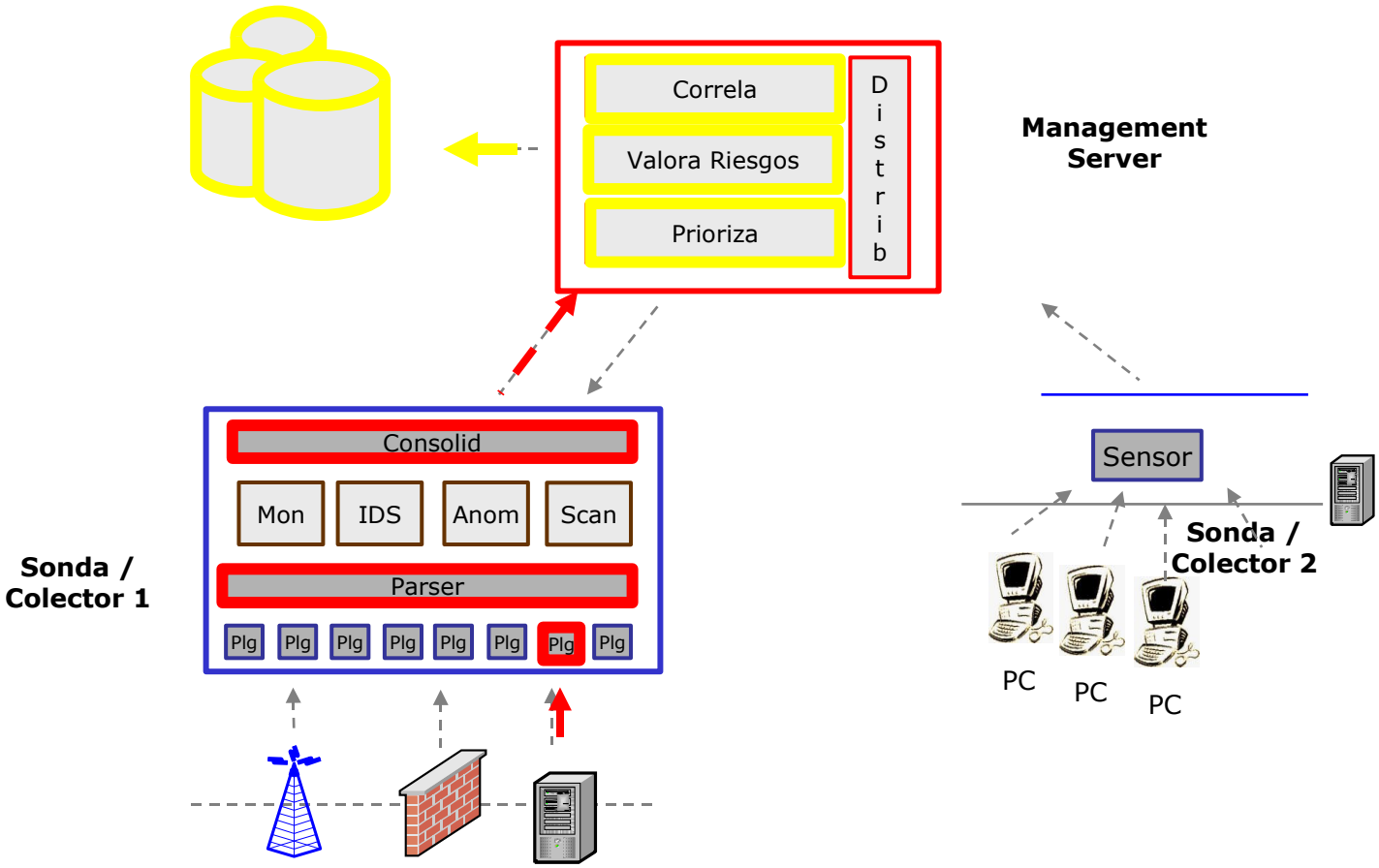
Millones de Eventos

Cientos de Eventos

Decenas de Alarmas

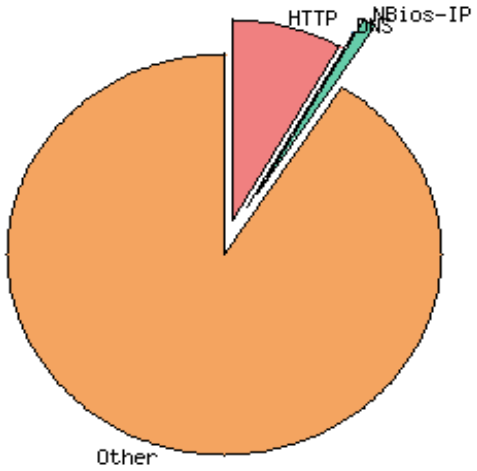
Gestión de la Seguridad

1.- Colección: Topología



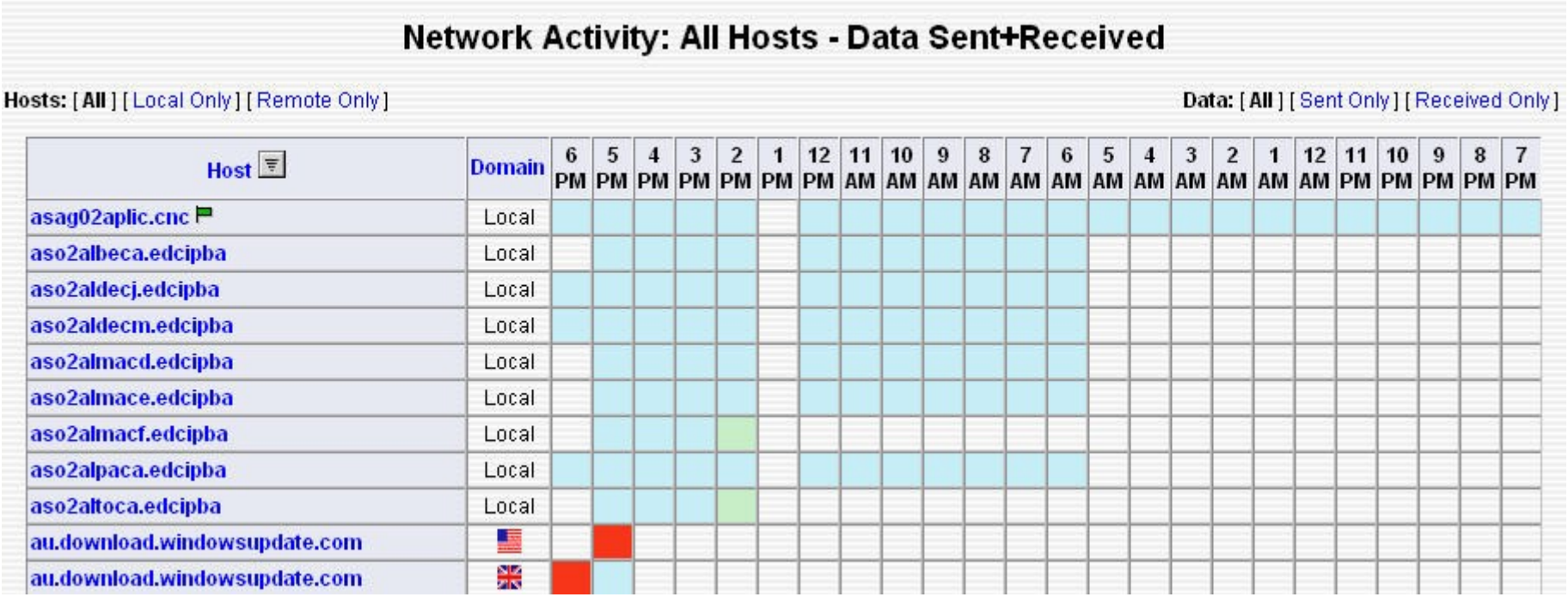
2.1.- Anomalías

- Monitorización del Uso (Estadístico)
- Monitorización de Sesiones (En Tiempo Real)
- Creación de Perfiles por Patrones.
- Anomalías de Red.



2.2.- Anomalías

- Monitorización del Uso (Estadístico)



Network Activity: All Hosts - Data Sent+Received

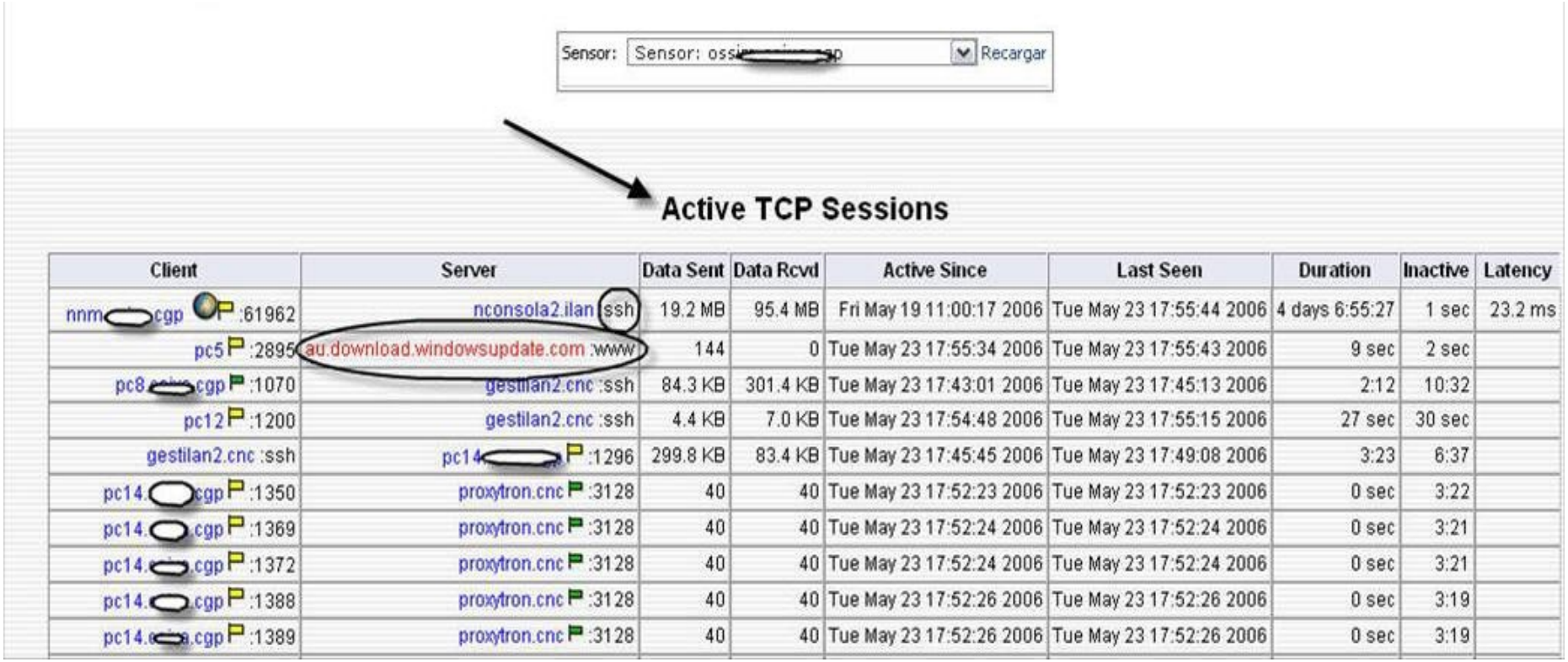
Hosts: [**All**] [Local Only] [Remote Only]

Data: [**All**] [Sent Only] [Received Only]

Host	Domain	6 PM	5 PM	4 PM	3 PM	2 PM	1 PM	12 PM	11 AM	10 AM	9 AM	8 AM	7 AM	6 AM	5 AM	4 AM	3 AM	2 AM	1 AM	12 AM	11 PM	10 PM	9 PM	8 PM	7 PM
asag02aplic.cnc	Local																								
aso2albeca.edcipba	Local																								
aso2aldecj.edcipba	Local																								
aso2aldecm.edcipba	Local																								
aso2almacd.edcipba	Local																								
aso2almace.edcipba	Local																								
aso2almacf.edcipba	Local																								
aso2alpaca.edcipba	Local																								
aso2altoca.edcipba	Local																								
au.download.windowsupdate.com																									
au.download.windowsupdate.com																									

2.3.- Anomalías

- Monitorización de Sesiones (En Tiempo Real)



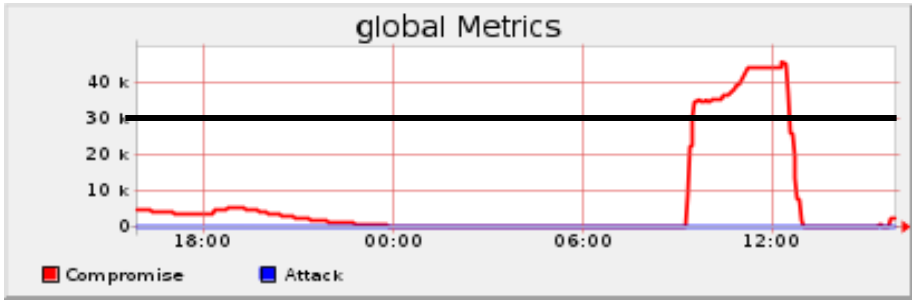
Client	Server	Data Sent	Data Rcvd	Active Since	Last Seen	Duration	Inactive	Latency
nnm cgp :61962	nconsola2.ilan :ssh	19.2 MB	95.4 MB	Fri May 19 11:00:17 2006	Tue May 23 17:55:44 2006	4 days 6:55:27	1 sec	23.2 ms
pc5 :2895	au.download.windowsupdate.com :www	144	0	Tue May 23 17:55:34 2006	Tue May 23 17:55:43 2006	9 sec	2 sec	
pc8 cgp :1070	gestilan2.cnc :ssh	84.3 KB	301.4 KB	Tue May 23 17:43:01 2006	Tue May 23 17:45:13 2006	2:12	10:32	
pc12 :1200	gestilan2.cnc :ssh	4.4 KB	7.0 KB	Tue May 23 17:54:48 2006	Tue May 23 17:55:15 2006	27 sec	30 sec	
gestilan2.cnc :ssh	pc14 :1296	299.8 KB	83.4 KB	Tue May 23 17:45:45 2006	Tue May 23 17:49:08 2006	3:23	6:37	
pc14 cgp :1350	proxytron.cnc :3128	40	40	Tue May 23 17:52:23 2006	Tue May 23 17:52:23 2006	0 sec	3:22	
pc14 cgp :1369	proxytron.cnc :3128	40	40	Tue May 23 17:52:24 2006	Tue May 23 17:52:24 2006	0 sec	3:21	
pc14 cgp :1372	proxytron.cnc :3128	40	40	Tue May 23 17:52:24 2006	Tue May 23 17:52:24 2006	0 sec	3:21	
pc14 cgp :1388	proxytron.cnc :3128	40	40	Tue May 23 17:52:26 2006	Tue May 23 17:52:26 2006	0 sec	3:19	
pc14 cgp :1389	proxytron.cnc :3128	40	40	Tue May 23 17:52:26 2006	Tue May 23 17:52:26 2006	0 sec	3:19	

2.4.- Anomalías

- Creación de Perfiles por Patrones.

- Servicios, Duración, Horario, Tamaño, Contenido, etc.

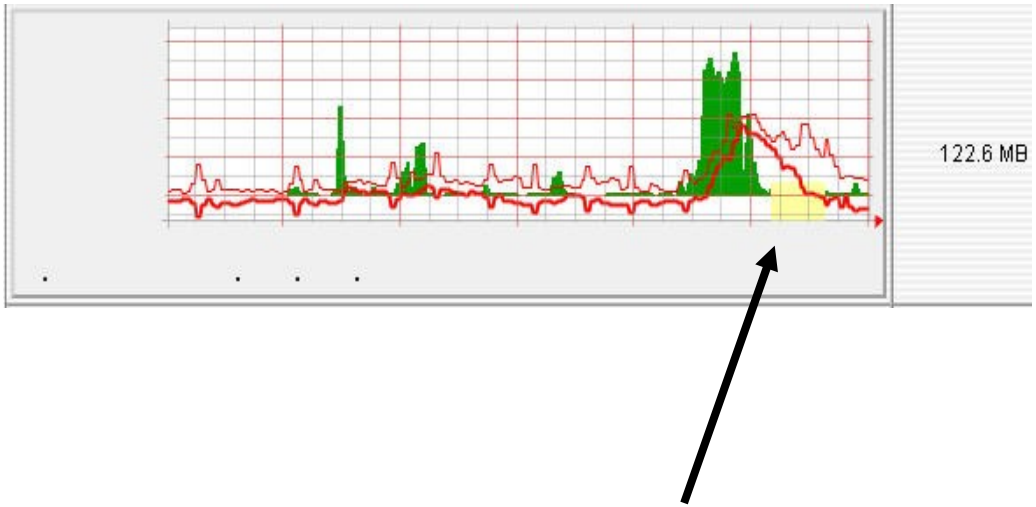
Umbrales máximos permitidos



2.5.- Anomalías

- Anomalías de Red.

Predicción por el Algoritmo **Holt Winters**; Predicción futura, a través de tendencias; **Diarias, Semanales, Anuales**



Tráfico anormal

3.- Priorización

- Inventario de Activos
- Valoración Topológica de Amenaza

Políticas

ID	Origen	Destino	Puertos	Firmas	Sensores	Límite de tiempo	Prioridad	Descripción	
1	terminales	servidores 192.168.1.1	23 (tcp) 25 (tcp) 80 (tcp)	web	sensor1 sensor2	15	3	Descripción de la política 1	Modificar Eliminar
2	192.168.1.1 terminales	terminales	25 (tcp) 110 (udp) 5269 (udp)	web		20	2	Descripción de la política 2	Modificar Eliminar
3	192.168.1.1	terminales servidores	25 (tcp) 25 (udp)	web		10	5	Descripción de la política 3	Modificar Eliminar
4	192.168.1.1	terminales	25 (tcp) 25 (udp) 80 (tcp)	web		30	4	Descripción de la política 4	Modificar Eliminar

Crear nueva política

4.- Valor del Riesgo

- Riesgo Intrínsico e Instantáneo

1.- Valor del Activo

2.- Amenaza del Evento

ACTIVOS

AMENAZA

IMPACTOS

FIABILIDAD

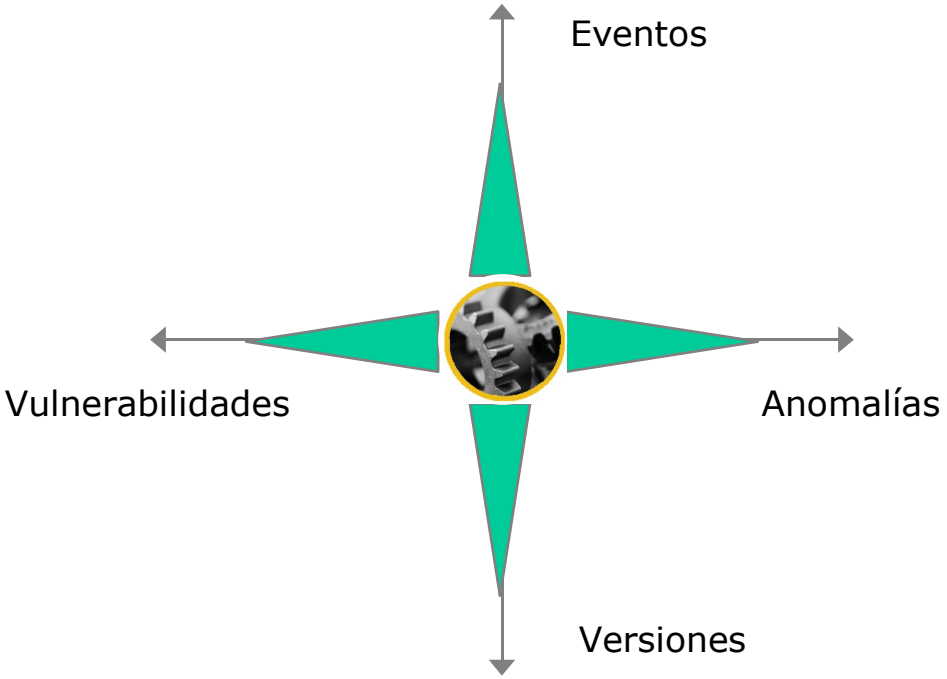
RIESGO

3.- Probabilidad

Riesgo Real de Amenaza

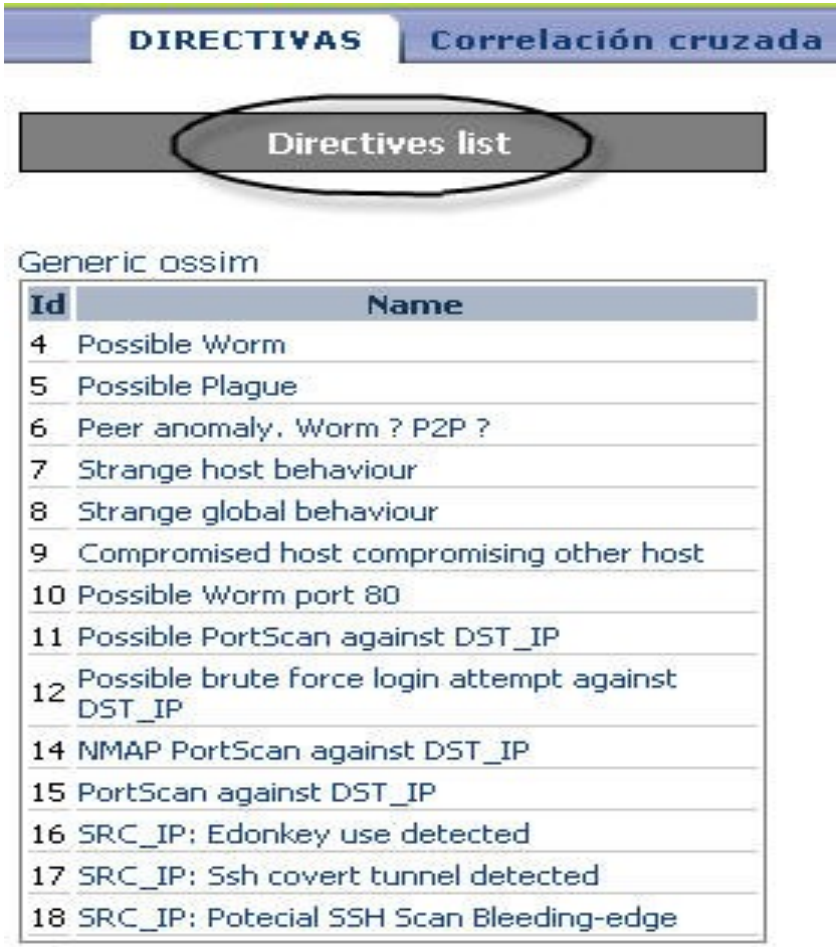
5.- Motor de Correlación. (Valor añadido de OSSIM)

- **Basado en el uso de Directivas lógicas** que ayudan a determinar el riesgo de un Ataque en la Red.
- **Estimación del riesgo** de un ataque, calculado **en función** de:
  - **ASSET** = Activo
  - **PRIORITY** = Valor de la amenaza
  - **RELIABILITY** = Fiabilidad



5.1.- Motor de Correlación. (Directivas)

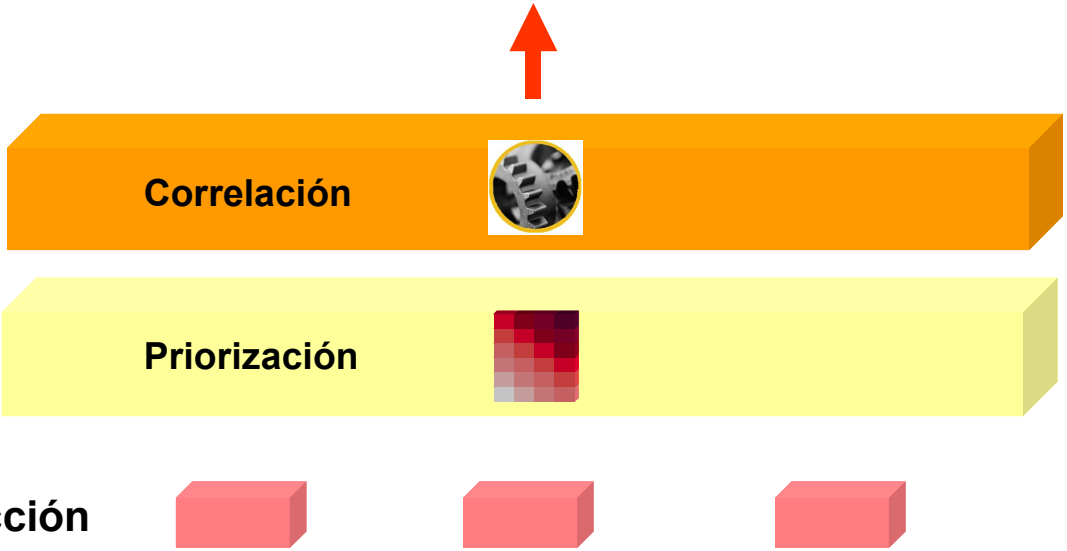
- **Basado en el uso de Directivas lógicas** que ayudan a determinar el riesgo de un Ataque en la Red.

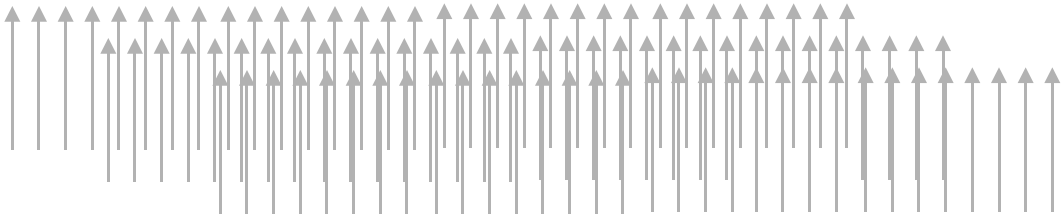


Id	Name
4	Possible Worm
5	Possible Plague
6	Peer anomaly. Worm ? P2P ?
7	Strange host behaviour
8	Strange global behaviour
9	Compromised host compromising other host
10	Possible Worm port 80
11	Possible PortScan against DST_IP
12	Possible brute force login attempt against DST_IP
14	NMAP PortScan against DST_IP
15	PortScan against DST_IP
16	SRC_IP: Edonkey use detected
17	SRC_IP: Ssh covert tunnel detected
18	SRC_IP: Potecial SSH Scan Bleeding-edge

Ejemplo: Gusano Sasser

Evitamos Falsos Positivos → Alarma única Verdadera

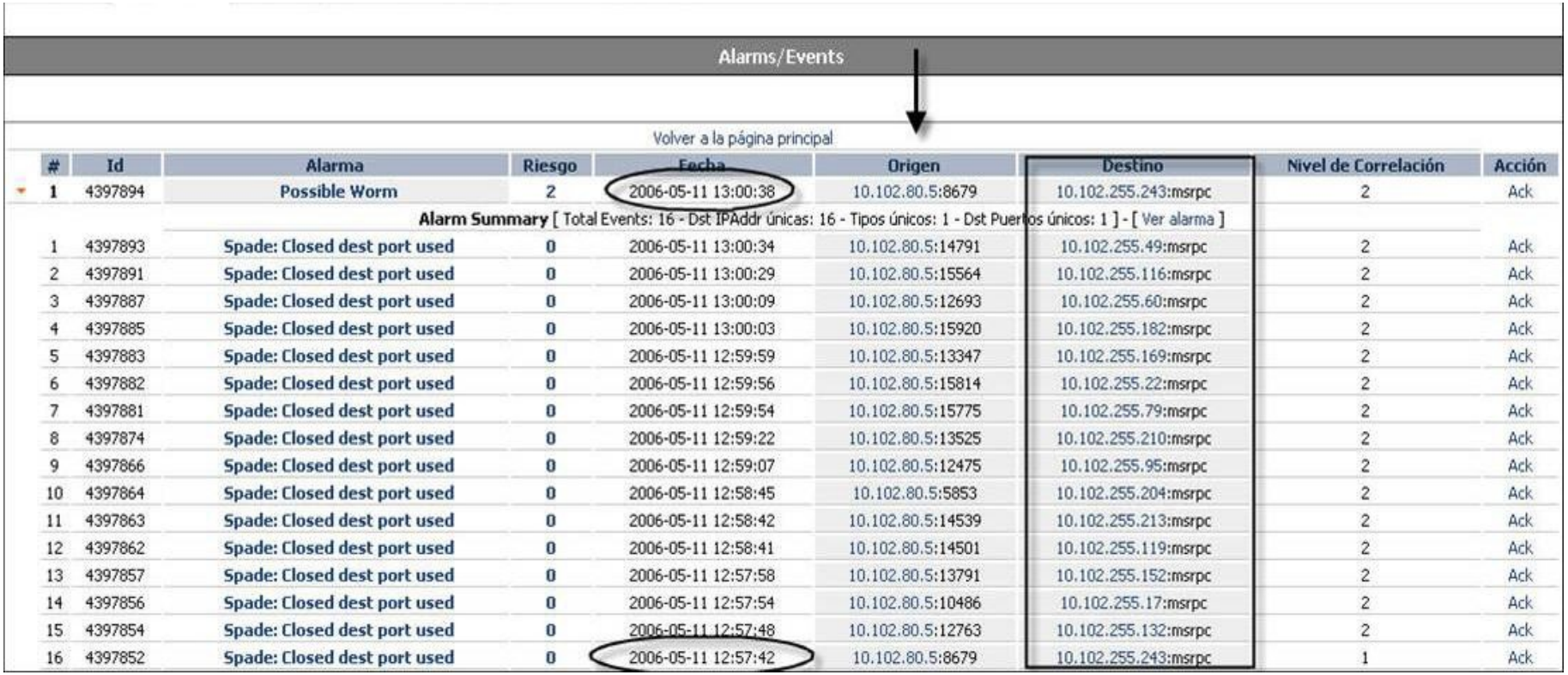




D. Anomalías

5.2.- Motor de Correlación

Ejemplo de Alarma Correlada de un Gusano



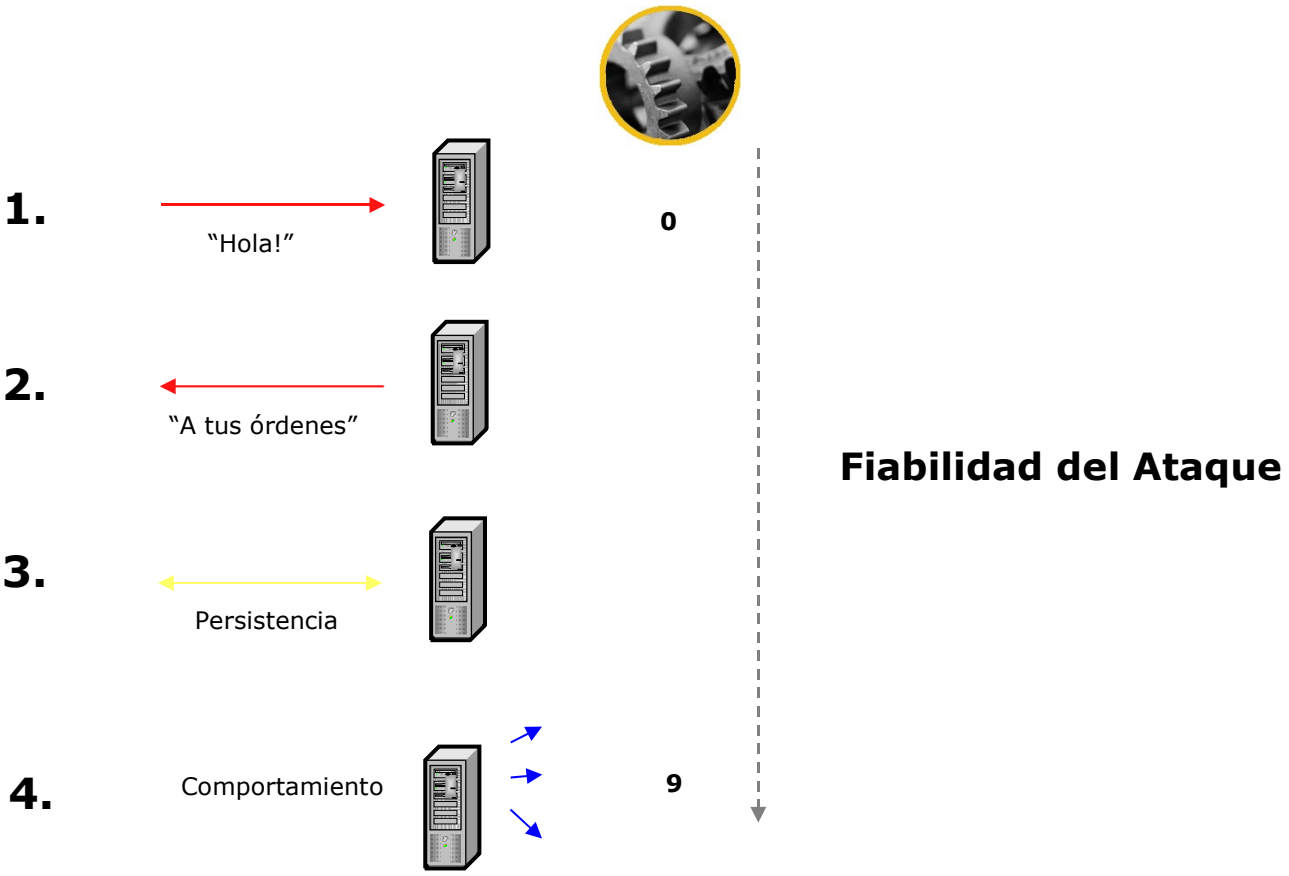
Alarms/Events

Volver a la página principal

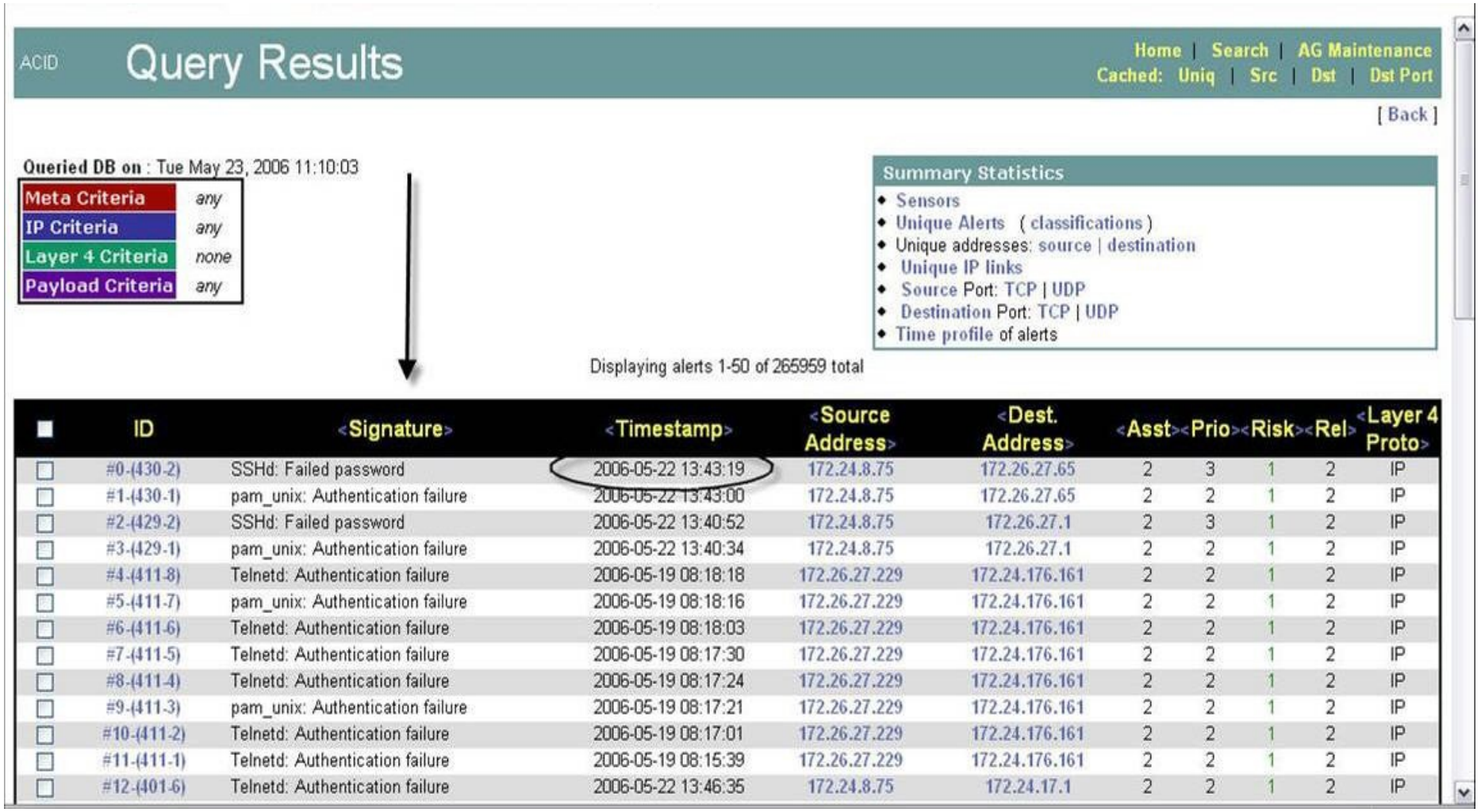
#	Id	Alarma	Riesgo	Fecha	Origen	Destino	Nivel de Correlación	Acción
1	4397894	Possible Worm	2	2006-05-11 13:00:38	10.102.80.5:8679	10.102.255.243:msrpc	2	Ack
		Alarm Summary [Total Events: 16 - Dst IPAddr únicas: 16 - Tipos únicos: 1 - Dst Puertos únicos: 1] - [Ver alarma]						
1	4397893	Spade: Closed dest port used	0	2006-05-11 13:00:34	10.102.80.5:14791	10.102.255.49:msrpc	2	Ack
2	4397891	Spade: Closed dest port used	0	2006-05-11 13:00:29	10.102.80.5:15564	10.102.255.116:msrpc	2	Ack
3	4397887	Spade: Closed dest port used	0	2006-05-11 13:00:09	10.102.80.5:12693	10.102.255.60:msrpc	2	Ack
4	4397885	Spade: Closed dest port used	0	2006-05-11 13:00:03	10.102.80.5:15920	10.102.255.182:msrpc	2	Ack
5	4397883	Spade: Closed dest port used	0	2006-05-11 12:59:59	10.102.80.5:13347	10.102.255.169:msrpc	2	Ack
6	4397882	Spade: Closed dest port used	0	2006-05-11 12:59:56	10.102.80.5:15814	10.102.255.22:msrpc	2	Ack
7	4397881	Spade: Closed dest port used	0	2006-05-11 12:59:54	10.102.80.5:15775	10.102.255.79:msrpc	2	Ack
8	4397874	Spade: Closed dest port used	0	2006-05-11 12:59:22	10.102.80.5:13525	10.102.255.210:msrpc	2	Ack
9	4397866	Spade: Closed dest port used	0	2006-05-11 12:59:07	10.102.80.5:12475	10.102.255.95:msrpc	2	Ack
10	4397864	Spade: Closed dest port used	0	2006-05-11 12:58:45	10.102.80.5:5853	10.102.255.204:msrpc	2	Ack
11	4397863	Spade: Closed dest port used	0	2006-05-11 12:58:42	10.102.80.5:14539	10.102.255.213:msrpc	2	Ack
12	4397862	Spade: Closed dest port used	0	2006-05-11 12:58:41	10.102.80.5:14501	10.102.255.119:msrpc	2	Ack
13	4397857	Spade: Closed dest port used	0	2006-05-11 12:57:58	10.102.80.5:13791	10.102.255.152:msrpc	2	Ack
14	4397856	Spade: Closed dest port used	0	2006-05-11 12:57:54	10.102.80.5:10486	10.102.255.17:msrpc	2	Ack
15	4397854	Spade: Closed dest port used	0	2006-05-11 12:57:48	10.102.80.5:12763	10.102.255.132:msrpc	2	Ack
16	4397852	Spade: Closed dest port used	0	2006-05-11 12:57:42	10.102.80.5:8679	10.102.255.243:msrpc	1	Ack

5.3.- Motor de Correlación

Ej. Intrusión:



6. Consola Forense



ACID **Query Results**

Home | Search | AG Maintenance
Cached: Uniq | Src | Dst | Dst Port

[Back]

Queried DB on : Tue May 23, 2006 11:10:03

Meta Criteria	any
IP Criteria	any
Layer 4 Criteria	none
Payload Criteria	any

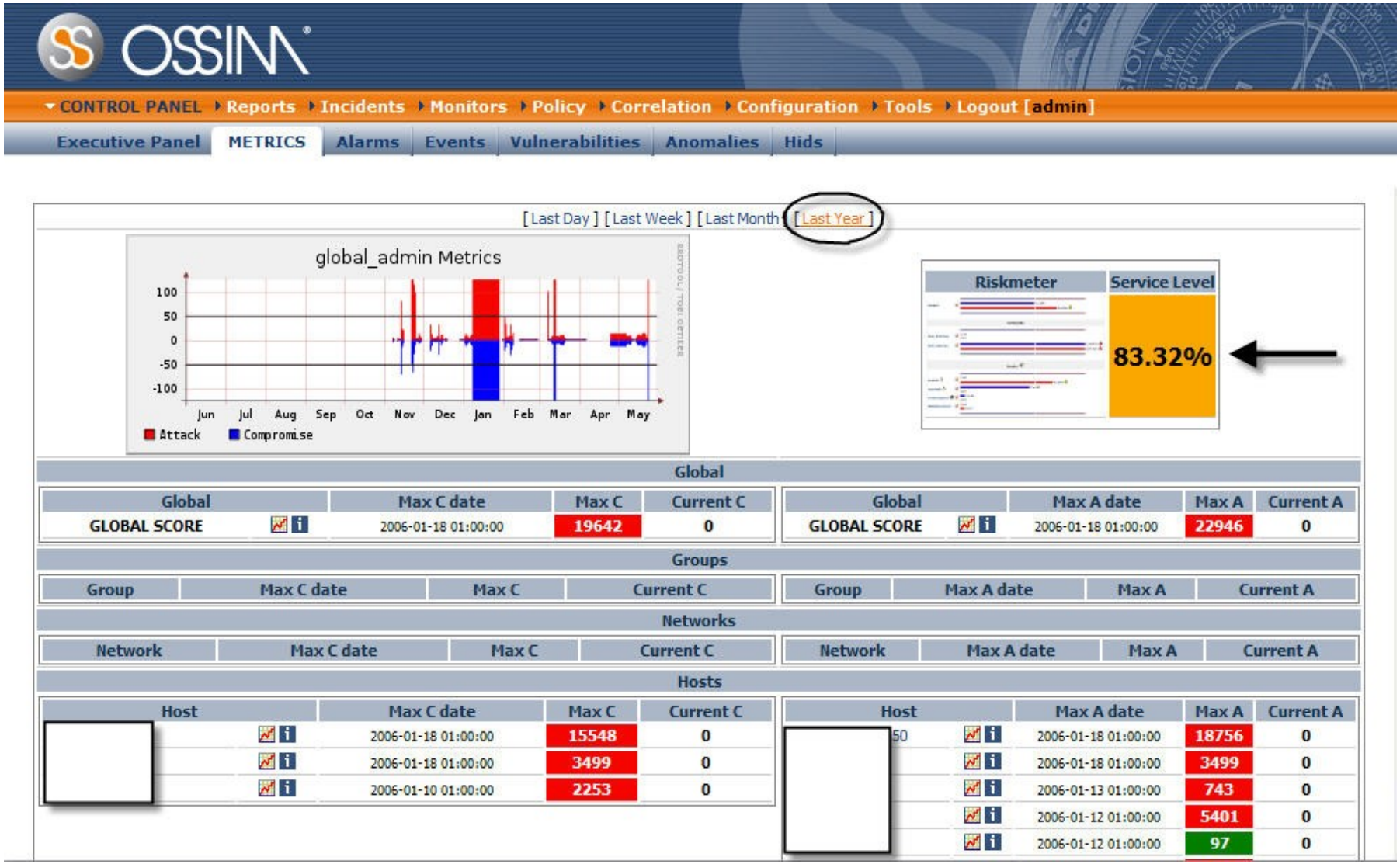
Summary Statistics

- Sensors
- Unique Alerts (classifications)
- Unique addresses: source | destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-50 of 265959 total

ID	<Signature>	<Timestamp>	<Source Address>	<Dest. Address>	<Asst>	<Prio>	<Risk>	<Rel>	<Layer 4 Proto>
#0-(430-2)	SSHd: Failed password	2006-05-22 13:43:19	172.24.8.75	172.26.27.65	2	3	1	2	IP
#1-(430-1)	pam_unix: Authentication failure	2006-05-22 13:43:00	172.24.8.75	172.26.27.65	2	2	1	2	IP
#2-(429-2)	SSHd: Failed password	2006-05-22 13:40:52	172.24.8.75	172.26.27.1	2	3	1	2	IP
#3-(429-1)	pam_unix: Authentication failure	2006-05-22 13:40:34	172.24.8.75	172.26.27.1	2	2	1	2	IP
#4-(411-8)	Telnetd: Authentication failure	2006-05-19 08:18:18	172.26.27.229	172.24.176.161	2	2	1	2	IP
#5-(411-7)	pam_unix: Authentication failure	2006-05-19 08:18:16	172.26.27.229	172.24.176.161	2	2	1	2	IP
#6-(411-6)	Telnetd: Authentication failure	2006-05-19 08:18:03	172.26.27.229	172.24.176.161	2	2	1	2	IP
#7-(411-5)	Telnetd: Authentication failure	2006-05-19 08:17:30	172.26.27.229	172.24.176.161	2	2	1	2	IP
#8-(411-4)	Telnetd: Authentication failure	2006-05-19 08:17:24	172.26.27.229	172.24.176.161	2	2	1	2	IP
#9-(411-3)	pam_unix: Authentication failure	2006-05-19 08:17:21	172.26.27.229	172.24.176.161	2	2	1	2	IP
#10-(411-2)	Telnetd: Authentication failure	2006-05-19 08:17:01	172.26.27.229	172.24.176.161	2	2	1	2	IP
#11-(411-1)	Telnetd: Authentication failure	2006-05-19 08:15:39	172.26.27.229	172.24.176.161	2	2	1	2	IP
#12-(401-6)	Telnetd: Authentication failure	2006-05-22 13:46:35	172.24.8.75	172.24.17.1	2	2	1	2	IP

7. Cuadro de Mandos. Métricas de Seguridad.



OSSIM Gestión de la Seguridad a todos los Niveles

Todo en una Caja Negra

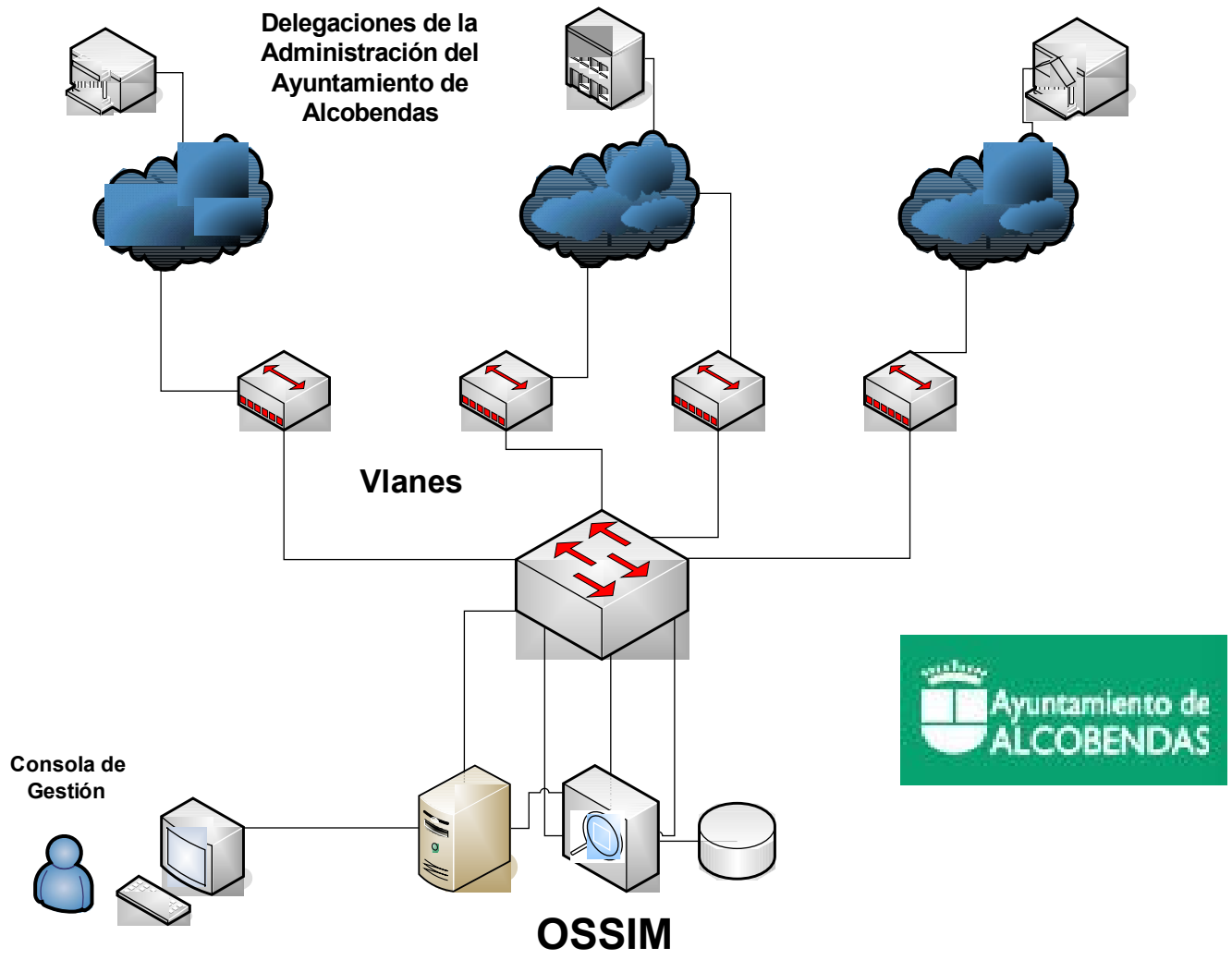
Caso de éxito en la Administración pública

- Cliente: **Ayuntamiento de Alcobendas**

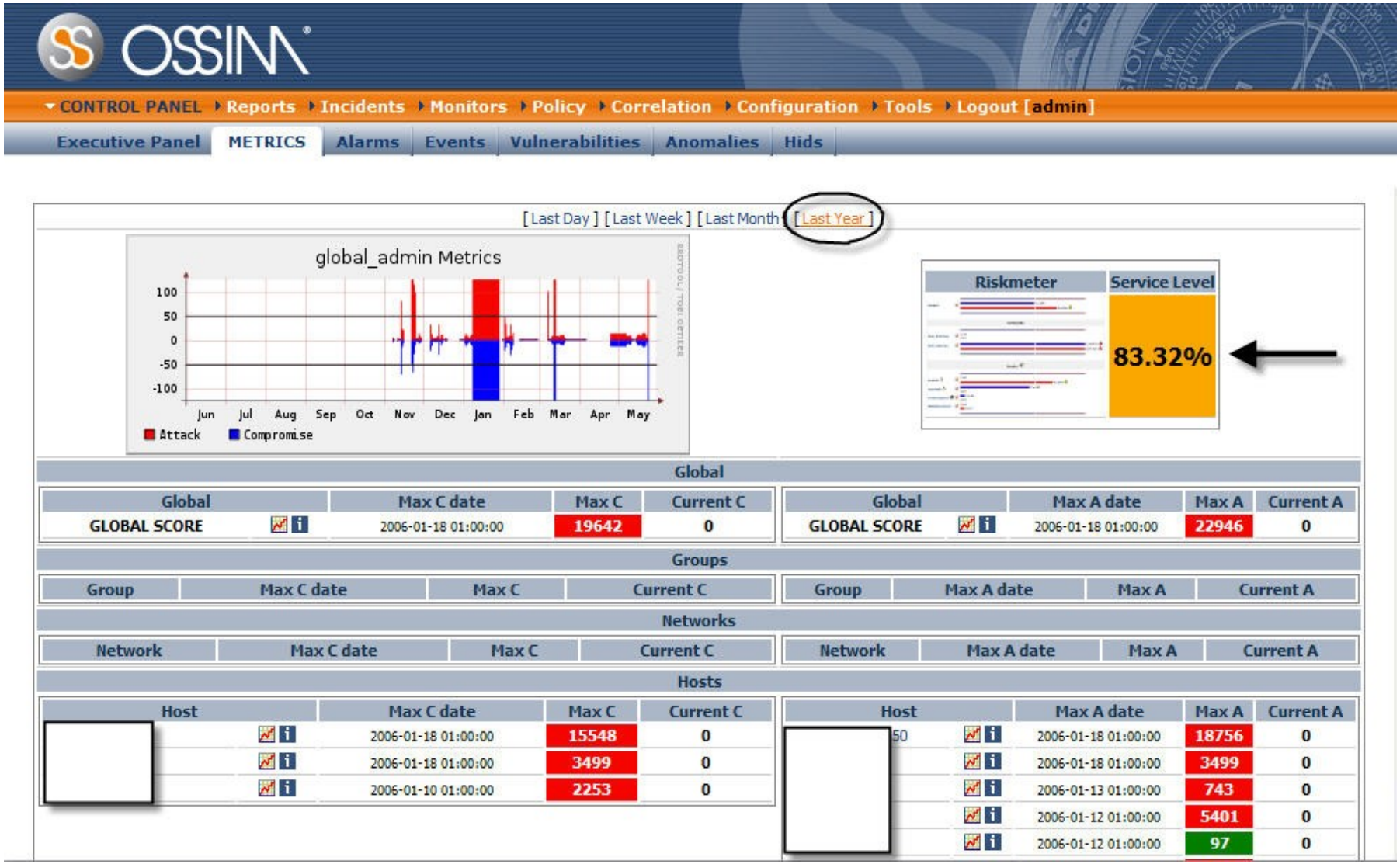
- **Necesidades:**

6. **Monitorización del Tráfico de Red.**
7. **Errores en Aplicaciones de la Administración.**
8. **Gestión de la Seguridad de sus dispositivos.**
9. **Estado Real de la Seguridad en su Red.**

Caso de éxito en la Administración pública: Esquema de red



Gestión de la Seguridad Centralizada.



Consola Forense: Ejemplos Reales

- P2P e-Donkey Detectado

ID	<Signature>	<Timestamp>	<Source Address>	<Dest. Address>	<Asst>	<Prio>	<Risk>	<Rel>	<Layer 4 Proto>
#0-(131-442564)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-17 06:27:18	172.24.8.100:1062	194.30.160.81:4665	2	1	0	1	UDP
#1-(131-448152)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-19 06:07:18	172.24.8.100:1062	66.172.60.133:4665	2	1	0	1	UDP
#2-(131-451282)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-20 02:17:18	172.24.8.100:1034	83.149.72.127:4665	2	1	0	1	UDP
#3-(131-451732)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-20 08:52:18	172.24.8.100:1034	213.251.161.69:4665	2	1	0	1	UDP
#4-(131-453702)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-21 11:07:18	172.24.8.100:1034	209.204.61.10:4665	2	1	0	1	UDP
#5-(131-455571)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-22 10:32:18	172.24.8.100:1034	209.204.61.44:4665	2	1	0	1	UDP
#6-(131-456309)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-22 12:42:18	172.24.8.100:1034	216.28.31.240:4665	2	1	0	1	UDP
#7-(131-458531)	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request	2006-05-23 07:07:18	172.24.8.100:1034	83.149.98.3:4665	2	1	0	1	UDP

Meta

ID #	Time	Triggered Signature
131 - 442564	2006-05-17 06:27:18	url[snort] BLEEDING-EDGE P2P eDonkey Server Status Request

Sensor	name	interface	filter
	172.24.0.36	any	src host not 172.24.0.36 and src host not 172.24.0.24

Alert Group	
	none

IP

source addr	dest addr	Ver	Hdr Len	TOS	length	ID	flags	offset	TTL	chksum
[redacted]	[redacted]	4	5	0	34	62834	0	0	128	11884

FQDN	Source Name	Dest. Name
	v[redacted]c	81-1[redacted].nl

Options	
	none

UDP

source port	dest port	length
1062	4665	14

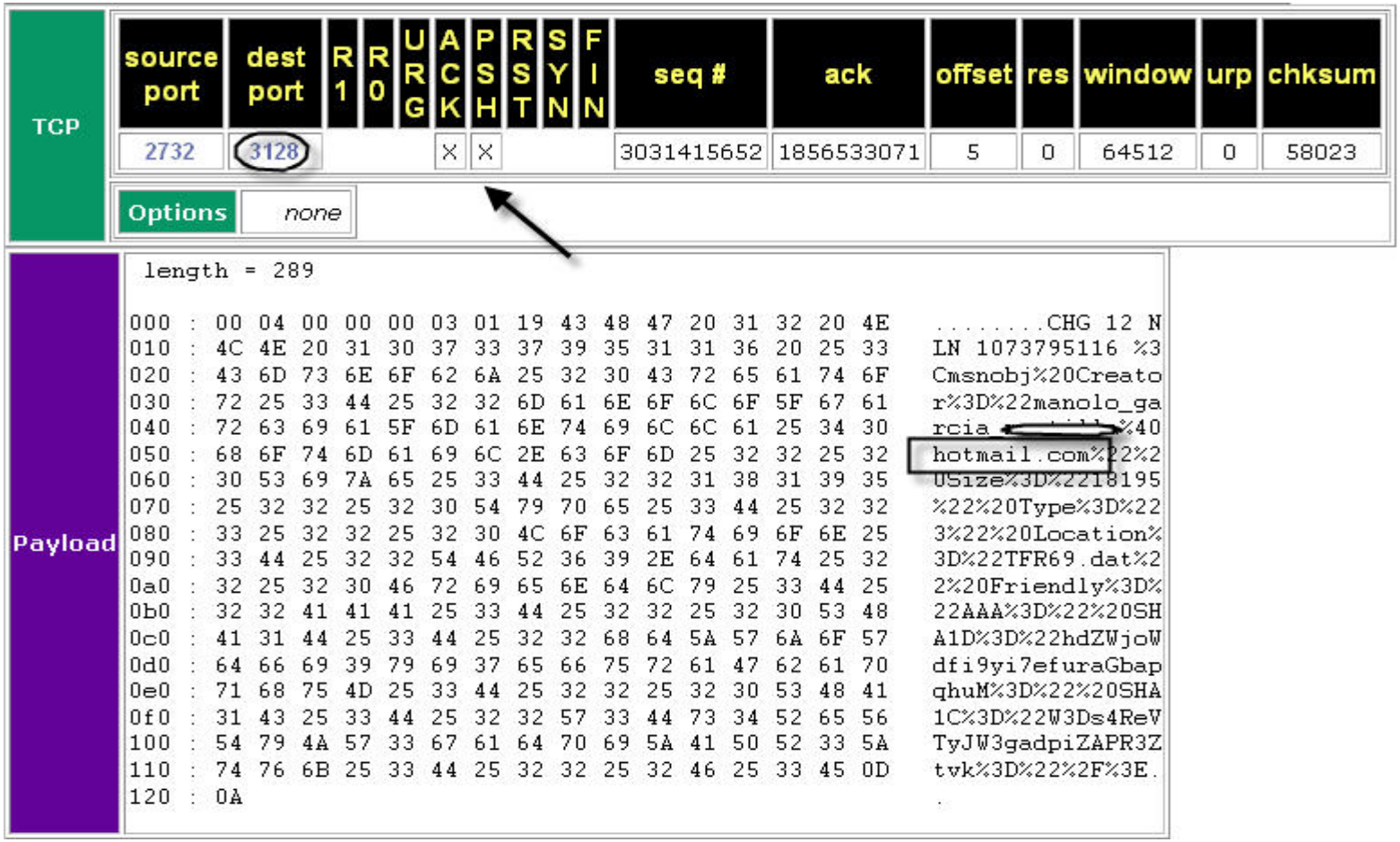
Payload

```
length = 6

000 : E3 96 77 F9 AA 55                                          ..w..U
```

Consola Forense: Ejemplos Reales

- **Detectada Actividad MNS (Messenger) Tunelizado por Tramas HTTP a través del Proxy.**



TCP

source port	dest port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	seq #	ack	offset	res	window	urp	chksum
2732	3128				X	X				3031415652	1856533071	5	0	64512	0	58023

Options: none

Payload

```
length = 289

000 : 00 04 00 00 00 03 01 19 43 48 47 20 31 32 20 4E   ........CHG 12 N
010 : 4C 4E 20 31 30 37 33 37 39 35 31 31 36 20 25 33   LN 1073795116 %3
020 : 43 6D 73 6E 6F 62 6A 25 32 30 43 72 65 61 74 6F   Cmsnobj%20Creato
030 : 72 25 33 44 25 32 32 6D 61 6E 6F 6C 6F 5F 67 61   r%3D%22manolo_ga
040 : 72 63 69 61 5F 6D 61 6E 74 69 6C 6C 61 25 34 30   rcia_[illegible]%40
050 : 68 6F 74 6D 61 69 6C 2E 63 6F 6D 25 32 32 25 32   hotmail.com%22%2
060 : 30 53 69 7A 65 25 33 44 25 32 32 31 38 31 39 35   0Size%3D%2218195
070 : 25 32 32 25 32 30 54 79 70 65 25 33 44 25 32 32   %22%20Type%3D%22
080 : 33 25 32 32 25 32 30 4C 6F 63 61 74 69 6F 6E 25   3%22%20Location%
090 : 33 44 25 32 32 54 46 52 36 39 2E 64 61 74 25 32   3D%22TFR69.dat%2
0a0 : 32 25 32 30 46 72 69 65 6E 64 6C 79 25 33 44 25   2%20Friendly%3D%
0b0 : 32 32 41 41 41 25 33 44 25 32 32 25 32 30 53 48   22AAA%3D%22%20SH
0c0 : 41 31 44 25 33 44 25 32 32 68 64 5A 57 6A 6F 57   A1D%3D%22hdZWjoW
0d0 : 64 66 69 39 79 69 37 65 66 75 72 61 47 62 61 70   dfi9yi7efuraGbap
0e0 : 71 68 75 4D 25 33 44 25 32 32 25 32 30 53 48 41   qhuM%3D%22%20SHA
0f0 : 31 43 25 33 44 25 32 32 57 33 44 73 34 52 65 56   1C%3D%22W3Ds4ReV
100 : 54 79 4A 57 33 67 61 64 70 69 5A 41 50 52 33 5A   TyJW3gadpiZAPR3Z
110 : 74 76 6B 25 33 44 25 32 32 25 32 46 25 33 45 0D   tvk%3D%22%2F%3E.
120 : 0A                                                .
```

Eventos de Seguridad: Ejemplos Reales

- Detectado Cambio de Mac:

Cambios de Mac [Get anom list] [Get full list]

Máquina	Sensor	Mac	Mac anterior	Cuándo	Aceptar	Ignorar
172.24.96.175	172.24.96.161	0:a0:26:2c:65:f6	0:0:e2:5b:b4:a6	2006-05-12 10:06:33	☐	☐
172.24.96.175	172.24.96.161	0:a0:26:2c:65:f6	0:a0:26:2c:65:f6	2006-05-12 10:06:33	☐	☐
172.24.96.175	172.24.96.161	0:a0:26:2c:65:f6	0:a0:26:2c:65:ee	2006-05-12 10:06:33	☐	☐
172.24.96.175	172.24.96.161	0:a0:26:2c:65:ee	0:a0:26:2c:65:72	2006-05-12 09:43:57	☐	☐

- Detectado Cambio de Sistema Operativo:

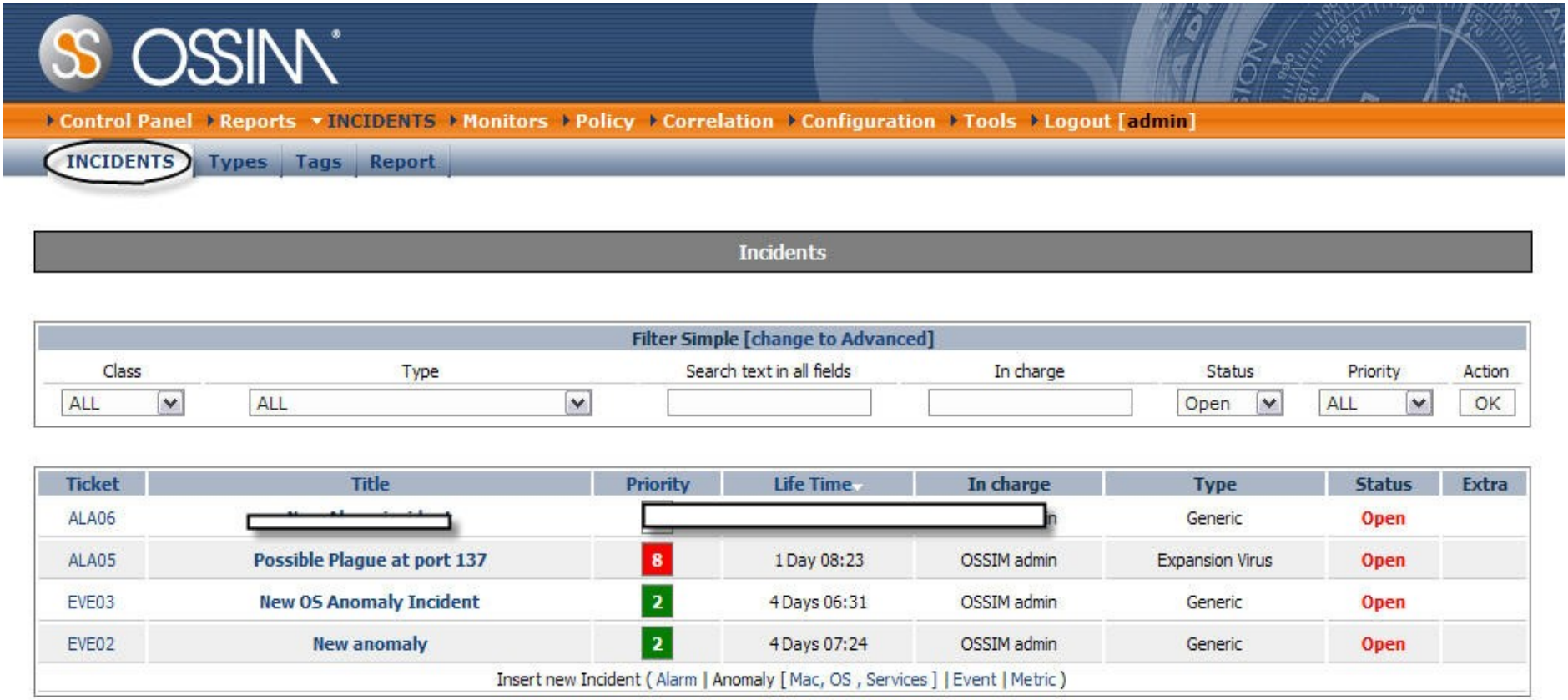
172.24.8.78	172.24.0.36[any]	Linux 2.5	2006-05-19 13:37:18	Windows XP SP1, 2000 SP3	2006-03-10 13:11:32	2 Months, 9 Days 23:25:46	☐	☐

Sistema Operativo Actual

Sistema Operativo Anterior

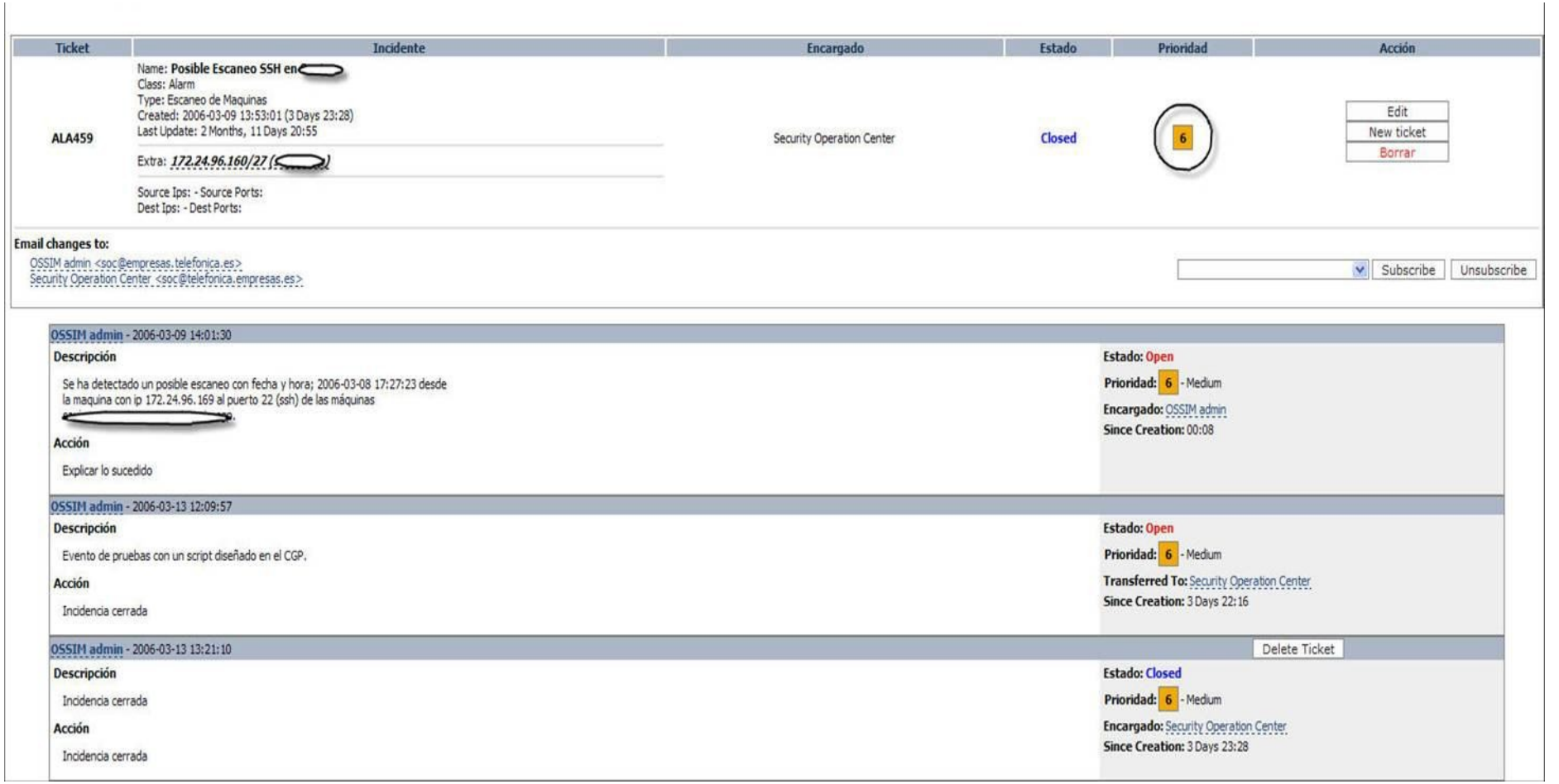
Gestión de la Seguridad: Incidencias

- Gestor de Incidencias:



Gestión de la Seguridad: Incidencias

- Comunicado y Escalado de Incidencias:



Ticket	Incidente	Encargado	Estado	Prioridad	Acción
ALA459	Name: **Posible Escaneo SSH en** [redacted] Class: Alarm Type: Escaneo de Maquinas Created: 2006-03-09 13:53:01 (3 Days 23:28) Last Update: 2 Months, 11 Days 20:55 Extra: *172.24.96.160/27 ([redacted])* Source Ips: - Source Ports: Dest Ips: - Dest Ports:	Security Operation Center	Closed	6	Edit New ticket Borrar

Email changes to:

OSSIM admin <soc@empresas.telefonica.es>
Security Operation Center <soc@telefonica.empresas.es>

Subscribe | Unsubscribe

OSSIM admin - 2006-03-09 14:01:30

Descripción

Se ha detectado un posible escaneo con fecha y hora; 2006-03-08 17:27:23 desde la maquina con ip 172.24.96.169 al puerto 22 (ssh) de las máquinas [redacted].

Acción

Explicar lo sucedido

Estado: Open
Prioridad: 6 - Medium
Encargado: OSSIM admin
Since Creation: 00:08

OSSIM admin - 2006-03-13 12:09:57

Descripción

Evento de pruebas con un script diseñado en el CGP.

Acción

Incidencia cerrada

Estado: Open
Prioridad: 6 - Medium
Transferred To: Security Operation Center
Since Creation: 3 Days 22:16

OSSIM admin - 2006-03-13 13:21:10 — Delete Ticket

Descripción

Incidencia cerrada

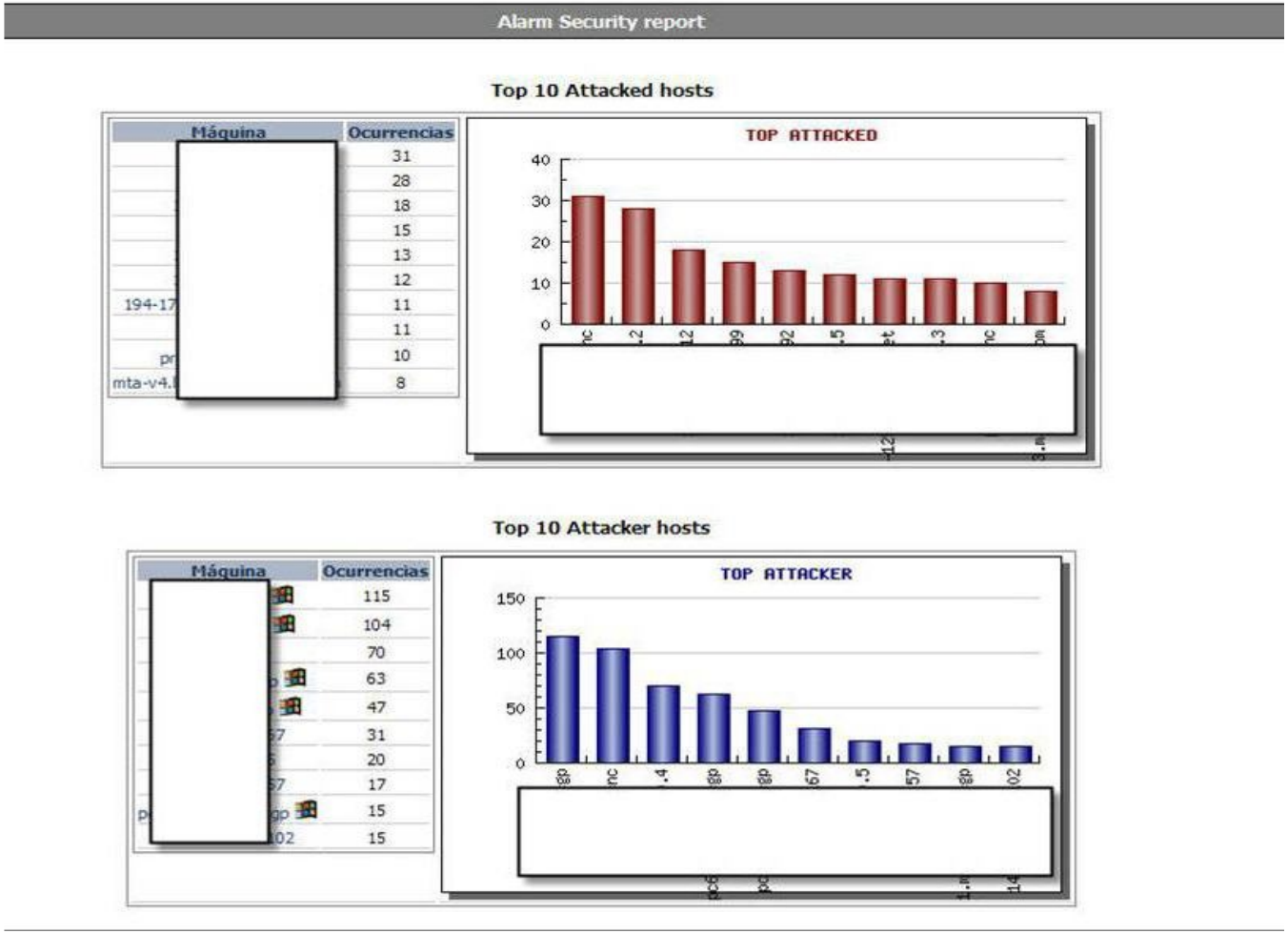
Acción

Incidencia cerrada

Estado: Closed
Prioridad: 6 - Medium
Encargado: Security Operation Center
Since Creation: 3 Days 23:28

Gestión de la Seguridad: Informes de Seguridad

- Ejemplo de Informes propios del sistema;



Caso de éxito en la Administración pública: Beneficios

- **Beneficios con la herramienta OSSIM**:

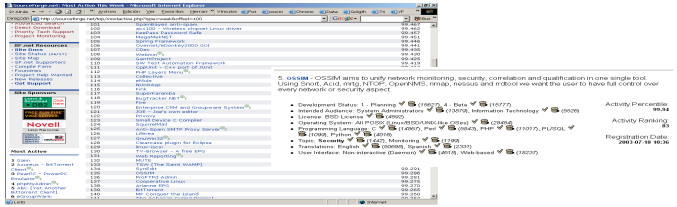
3. **Disponibilidad de Información para la Toma de Decisiones.**
4. **Mejora del Rendimiento de Redes.**
5. **Optimización de la Productividad del equipo técnico del Cliente.**
6. **Incorporación de Nuevos Servicios.**
7. **Aumento de la capacidad de Gestión de la seguridad de la información.**

Referencias OSSIM

Referencias de la plataforma de seguridad OSSIM

¿Por qué OSSIM es Nº 1 como producto?

- **Es la 1º Consola Open Source de Seguridad del Mundo**



- **Esta en el puesto 85 como producto open source** *(sourceforge)*
- **Tuvo alrededor de 30.000 downloads en el año 2005**
- **Es visitada por 15.000 especialistas al mes**


EL PAÍS, JUEVES 3 DE FEBRERO DE 2005

PROGRAMAS

Cuatro 'hackers éticos' españoles triunfan en el mundo con un programa de seguridad

La NASA, organizaciones militares y 22.000 personas han descargado este paquete libre, de aplicaciones para administradores de sistemas ● El Ministerio de Economía francés y Philips participan en su desarrollo

MERCE MOLIST

Eran cuatro amigos españoles que gustaban de llamarse *hackers éticos*. Hace cinco años, decidieron crear una herramienta de seguridad de licencia libre, OSSIM (Open Source Infrastructure for Security Monitoring). Hoy, es la *suite* libre de seguridad más copiada del mundo y la utilizan empresas desde Suráfrica hasta Singapur, incluidas empresas 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.

Más de 22.000 personas han copiado el programa OSSIM de Sourceforge, la principal lista de proyectos de *software* libre del mundo. No es fácil estar en Sourceforge. Y menos ser el programa líder en su categoría de *suites* de seguridad. Pero, OSSIM, un programa creado por cuatro jóvenes españoles veinteañeros, es casi

Los creadores de OSSIM.

LUIS MAGÁN


>accesogroup 04/10/04 CINCO DIAS (SUPLEMENTO ESPECIAL)
MADRID

Cód 2831599

Prensa Otra
Tirada: 50.226 Ejemplares
Difusión: 25.535 Ejemplares
Documento: 1/1
Impresión: Blanco y Negro
Sección:

IT DEUSTO Pionera en software libre

Intrusos con buenas intenciones

MÓNICA GUERRA *Madrid*

Un intruso se acerca a la puerta de su hogar, intenta forzar la cerradura y comprueba si es posible colarse por la ventana. Una vez evaluada la seguridad, en vez de robarle, su perfil psicológico, ya que necesitamos personas de confianza", reflexiona el responsable de IT Deusto. Mirando de reojo el ejemplo estadounidense, donde auditar a través de ataques es una práctica habitual, IP6 Seguridad fue creciendo con el boom de Internet. Con

Referencias

España

- CASA/EADS Espacio
- Telefónica Móviles
- Telefónica Empresas
- Mercados Financieros
- People ETT
- Chronoexpress
- Grupo Bergé
- Ayto Alcobendas

Referencias (no implantados por IT Deusto)

Extranjero

- Navy (EEUU)
- Nasa (EEUU)
- Min. Defensa (Australia)
- Min. Economía (Francia)
- Dep del Gobierno (Mexico)
- Philipps (Holanda)
- BellSouth (EEUU)
- Universidad de Pekin (China)

Área Seguridad IT Deusto

¡ Ruegos y Preguntas !

Gonzalo Asensio Asensio
Jefe de Proyecto Seguridad Informática
gasensio@itdeusto.com
Tlf: 659 43 43 33

GRACIAS POR LA ATENCIÓN