

A hand is holding a white envelope with the word "OSSIM" printed in bold blue letters. The background is a beach with turquoise water and a blue sky with light clouds.

**OSSIM**

**Toni Pérez Sánchez**  
**toni.perez@uib.es**



**Universitat de les  
Illes Balears**

Centre de Tecnologies  
de la Informació



*Ossim en la UIB*

# Índice

- 1. La herramienta
  - Puntos Fuertes
  - Puntos Débiles
- 2. Actual Implantación
- 3. Posibles Mejoras o necesidades
- 4. Grado de satisfacción

# La herramienta





*Ossim*

# La herramienta





*Ossim*

# Tools integrados

## ➤ Pasivos

- Snort
- Ntop y NFSen/Nfdump
- Kismet
- P0f y Pads
- Arpwatch
- Tcptrack
- Nepenthes Honeypot

## ➤ Activos

- OCS inventory
- Nagios
- OpenVas
- OSSEC HIDS
- Nmap
- Otros:
- OSVDB

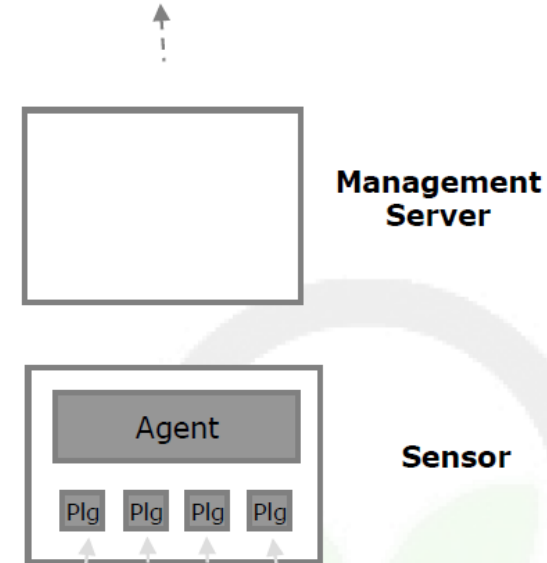


Ossim

# Plugins

```
[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

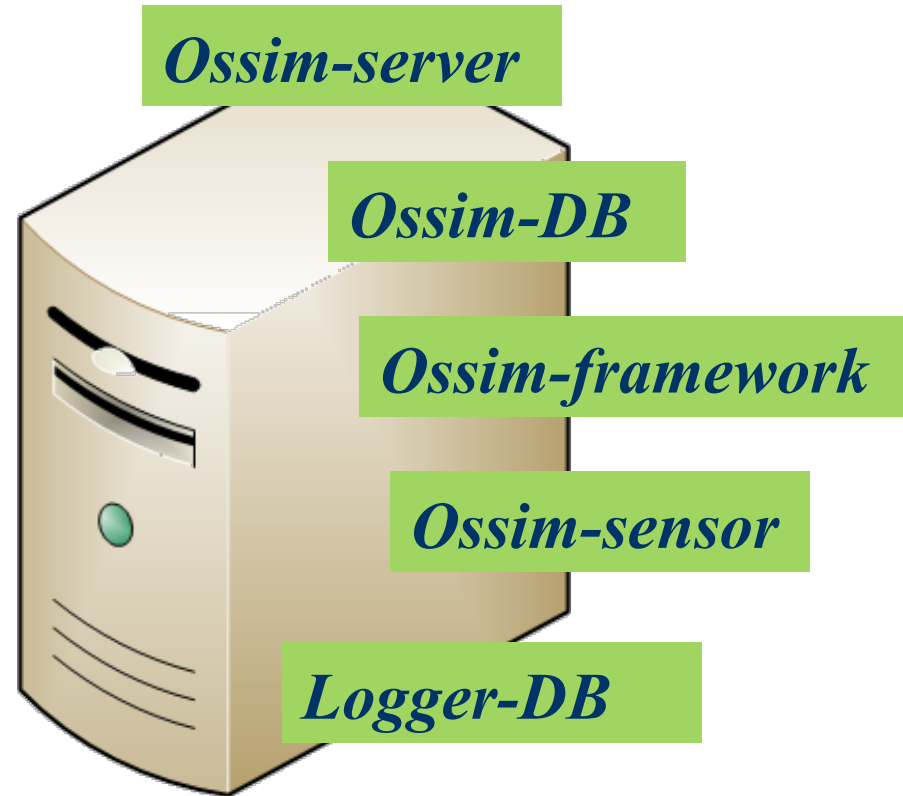
[pads-service]
event_type=host-service-event
regexp="^(\IPV4), ([^,]*) , ([^,]*) , ([^,]*) , ([^,]*) , (\d+)$"
host=${$1}
port=${$2}
protocol=${$3}
service=${$4}
application=${$5}
plugin_sid=1
```





*Ossim*

# Arquitectura All-In-One





*Ossim*

# Instalador



**alienvault**  
creators of ossim

## Debian installer main menu

Select the profile you want to install, you can install them separately or combine them, based on the capacity of your hardware.

- Server
- Sensor
- Framework
- Database

New Installer  
GUI Installer

Screenshot

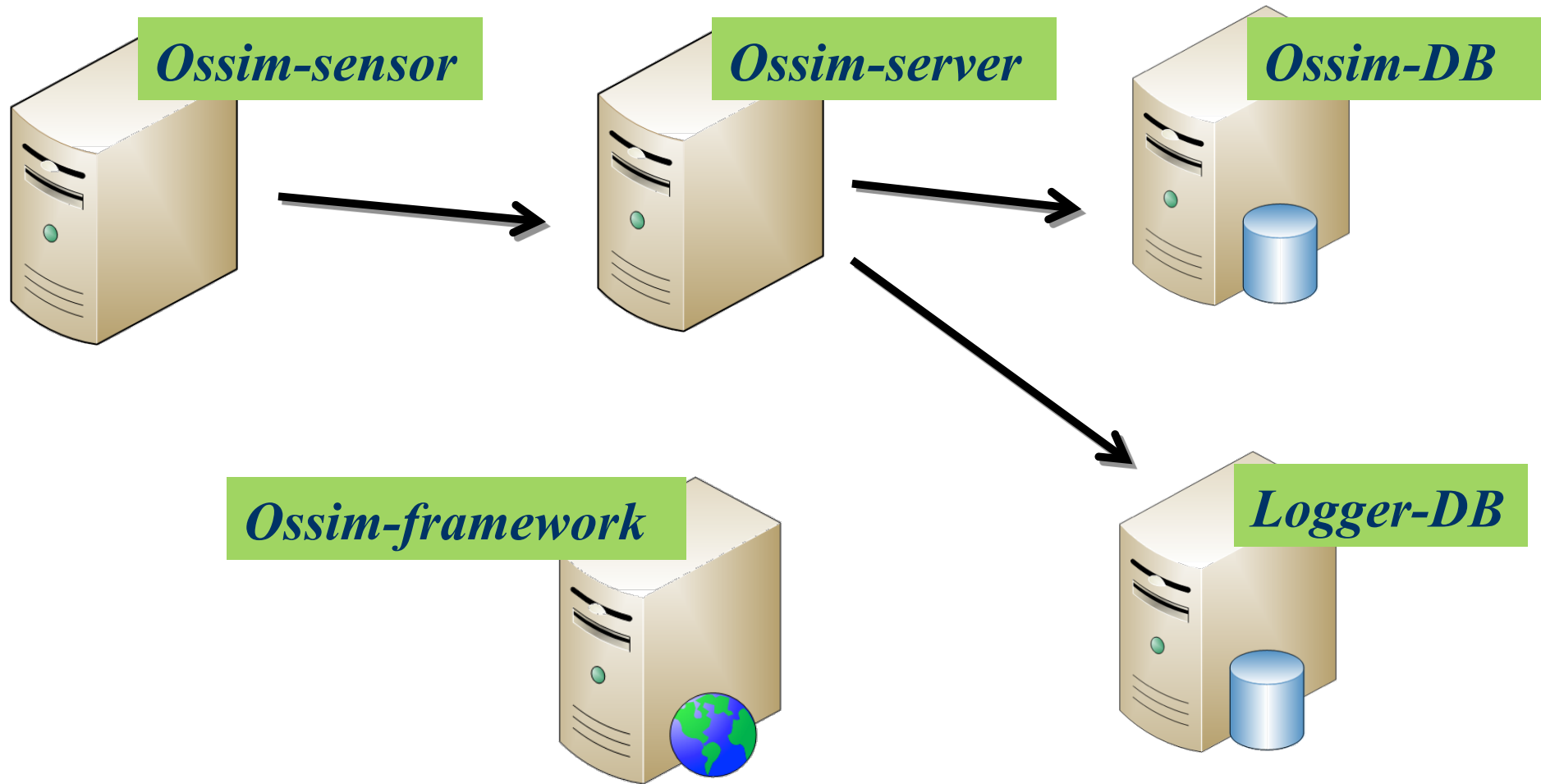
Continue





# Arquitectura distribuida

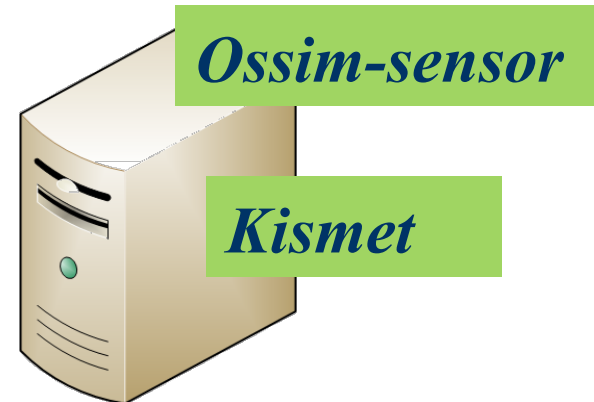
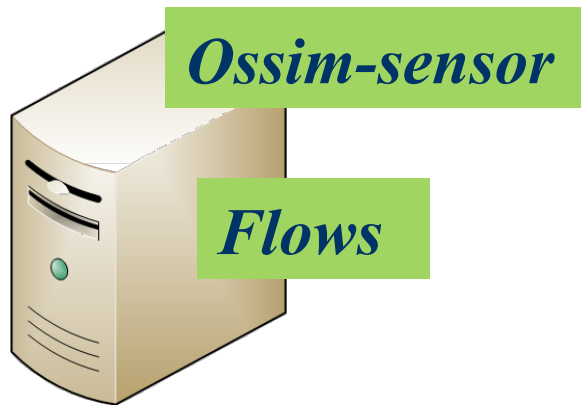
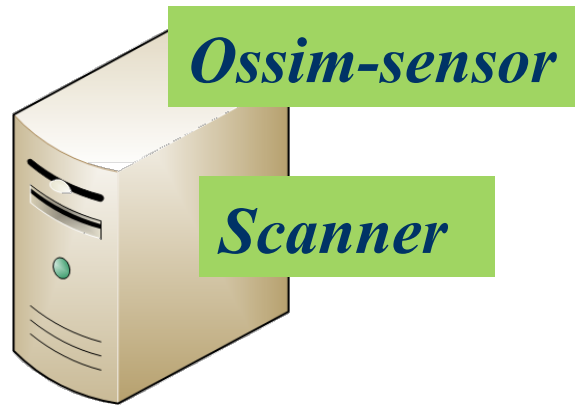
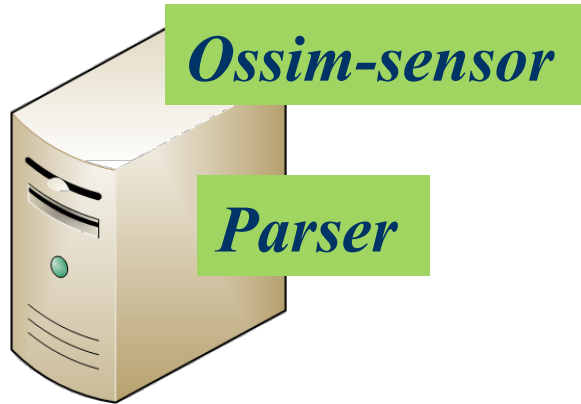
*Ossim*





*Ossim*

# Arquitectura distribuida





*Ossim*

# Appliance or not!

*SIEM: 5.000 eps*  
*Logger: 15.000 eps*  
*Sensor: 10Gbps*

*“Tuned operating system and kernel.”*

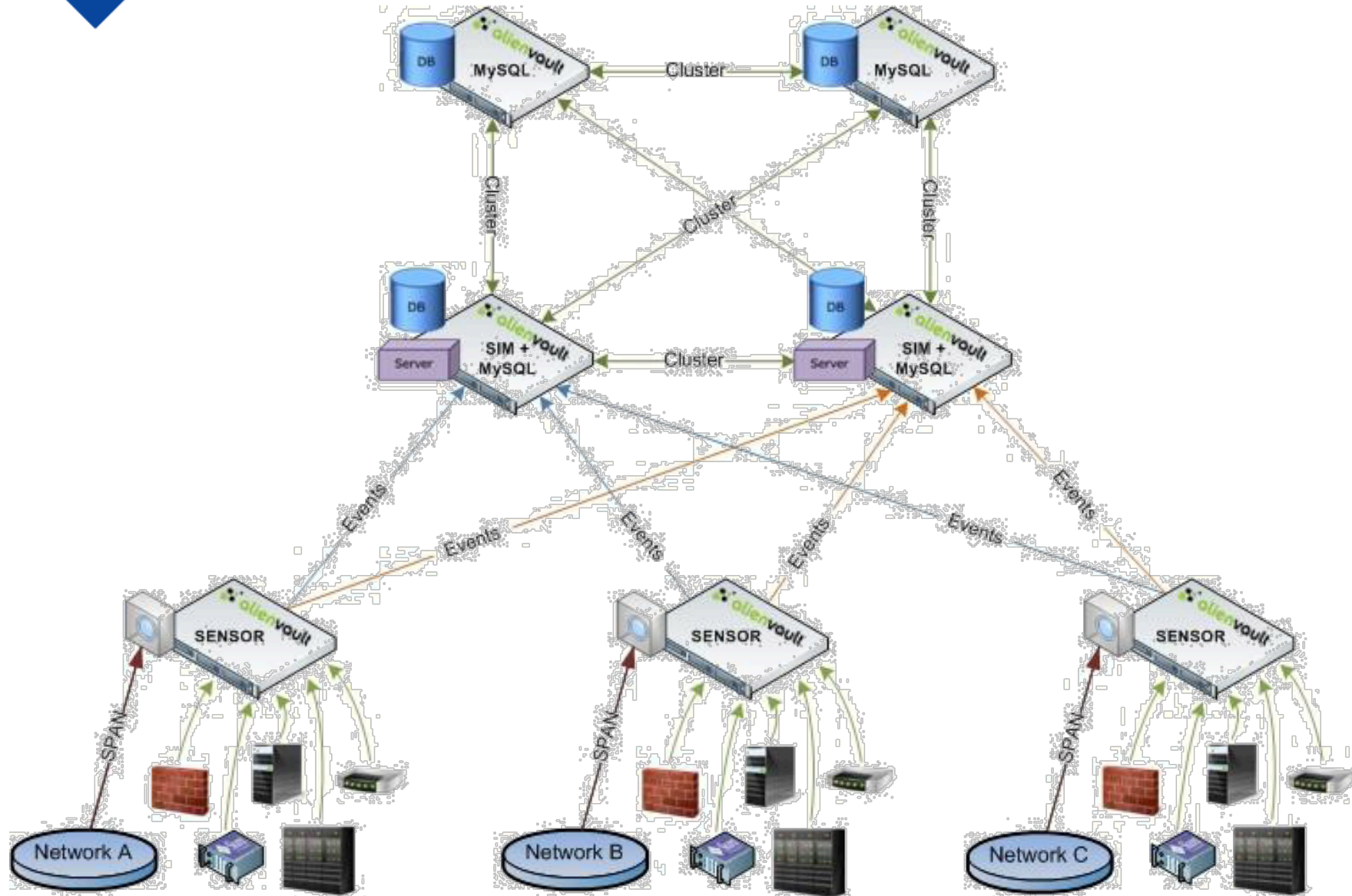
*“Network optimization for high load network capture.”*





# Arquitectura distribuida

*Ossim*





Ossim

# Alarmas

**alienvault** Professional SIEM

Tickets **Opened** 361 | Last updated: 2010-02-05 13:37:25  
 Unresolved **Alarms** 1.158 | Last updated: 2010-02-07 00:08:11

Max priority 8 | Max risk 5 | Global score 100% | Service level

Alarms Report

Filters, Actions and Options

(0-50 of 1158) Next 50 -> Last ->> | Ungruped | Grouped | Unique

#	Alarm	Risk	Sensor	Since	Last	Source	Destination	Status	Action
Sunday 07-Feb-2010 [ Delete ]									
1	AV Possible SSH Scan from ossim against dell (Network detected) (49 events)	2	ossim	2010-02-07 00:02:01	2010-02-07 00:08:11	ossim:53333	dell:ssh	open	
Saturday 06-Feb-2010 [ Delete ]									
2	AV Possible SSH Scan from ossim against dell (Network detected) (47 events)	2	ossim	2010-02-06 00:01:59	2010-02-06 00:08:15	ossim:53333	dell:ssh	open	
Friday 05-Feb-2010 [ Delete ]									
3	AV Possible SSH Scan from ossim against monster (Network detected) (37 events)	2	ossim	2010-02-05 12:46:33	2010-02-05 12:57:58	ossim:53333	monster:ssh	open	
4	AV Possible SSH Scan from ossim against dell (Network detected) (43 events)	2	ossim	2010-02-05 12:51:30	2010-02-05 12:55:48	ossim:53333	dell:ssh	open	
5	AV Possible SSH Scan from ossim against Ext Gateway (Network detected) (24 events)	2	ossim	2010-02-05 12:46:19	2010-02-05 12:50:01	ossim:53333	Ext Gateway:ssh	open	
6	SSH brute force login attempt against ossim (79 events)	0	ossim	2010-02-05 12:46:48	2010-02-05 12:47:03	ossim:ANY	ossim:ssh	open	
7	AV Possible SSH Scan from ossim against dell (Network detected) (12 events)	2	ossim	2010-02-05 11:45:42	2010-02-05 11:53:03	ossim:53333	dell:ssh	open	
8	AV Possible SSH Scan from ossim against 192.168.1.7 (Network detected) (12 events)	1	ossim	2010-02-05 11:34:13	2010-02-05 11:36:47	ossim:34422	192.168.1.7:ssh	open	
9	AV Possible SSH Scan from ossim against 192.168.1.33 (Network detected) (12 events)	2	ossim	2010-02-05 11:31:17	2010-02-05 11:34:45	ossim:49606	192.168.1.33:ssh	open	
10	AV Possible SSH Scan from ossim against Ext Gateway (Network detected) (18 events)	2	ossim	2010-02-05 11:31:29	2010-02-05 11:34:20	ossim:47807	Ext Gateway:ssh	open	
	AV Possible SSH Scan from ossim against								

Asset Report  
 Asset Search  
 Tickets  
 Alarms  
 Logger  
 SIEM Events  
 Vulnerabilities  
 Knowledge DB  
 Net Profile  
 Traffic  
 Availability

**Enhanced Usability**  
 Easy access to information (Right click on any IP address)



Ossim

# Report de objeto

**alienvault Professional SIEM**

Open Tickets: 4 | Unresolved Alarms: 171 | Max priority: 6 | Max risk: 4 | Service level: 100% | Global score: [Progress Bar]

### General Data: Server-Win - (192.168.1.222)

#### General Status

Service level: 100% | Global score: [Progress Bar]

Tickets Opened	1	2010-02-01 05:02:35	Max priority: 2
Unresolved Alarms	163	2010-02-06 18:32:46	Highest risk: 4
Vulnerabilities	0		Highest Risk: - (0 events)
SIEM Events	0	-	Highest Risk: - (0 events)
Logger Events	10.067	2010-02-07 11:38:29	Last Week: 25.369 events
Anomalies	0	-	Last Week: 0 events
Availability Events	0	-	Highest Priority: - (0 events)

#### Inventory

Host Info		Host belongs to:	
Name	Server-Win	Net	Pvt_192
Ip	192.168.1.222	Sensor	ossim
OS	Windows	Who is?	
MAC	00:26:08:E1:64:18	Service	Version
		netbios-ssn (139/tcp)	unknown
		Origin	Passive

#### Network Usage

No data Available

---

### SIEM

#### Tickets

Ticket	Title	Priority	Status
ALA06	Possible Virut Infection on Server-Win	2	Open

[More >>](#)

#### Alarms

Alarm	Risk	Source	Destination
AV Mariposa Botnet Activity on Server-Win (3 events)	2	Server-Win	96.31.84.69
AV Mariposa Botnet Activity on Server-Win (3 events)	2	Server-Win	91.207.5.194
AV Mariposa Botnet Activity on Server-Win (5 events)	2	Server-Win	174.139.27.42
AV Mariposa Botnet Activity on Server-Win (3 events)	2	Server-Win	208.53.131.47
AV Mariposa Botnet Activity on Server-Win (3 events)	2	Server-Win	83.149.84.247

[More >>](#)

#### Vulnerabilities

No Vulnerabilities Found for 192.168.1.222

---

## Asset Report

Shows all the information regarding a host or network that can be found in OSSIM

67600 SIEM total events in week range



Ossim

# Vulnerability Scan

## New Vulnerability Management Interface

Easy Scan Objectives Selection



Ossim

# Nessus Plugins

alienvault Professional SIEM

Tickets Opened 361 | Unresolved Alarms 1.159 | Last updated: 2010-02-05 13:37:25 | Max priority 8 | Max risk 5 | Global score | Service level 100%

Vulnerabilities | Reports | Jobs | Threats Database | Profiles | Settings

Search results for this criteria

Keywords: apache | CVE Id: All | Family: All | Risk Factor: All | Start Date: All | End Date: All

ID	Risk	Defined On	Threat Family & Summary	CVE Id
20874	High	2009-12-15 09:55:05	Gentoo Local Security Checks - Apache: Multiple vulnerabilities	CVE-2005-3352 CVE-2005-3357
14527	High	2009-12-15 09:55:05	Gentoo Local Security Checks - Apache 1.3: Buffer overflow in mod_proxy	CVE-2004-0492
10918	High	2009-12-15 09:55:05	Gain a shell remotely - Checks for version of Apache-SSL	CVE-2002-0082
10938	High		<b>Nessus plugin details</b> ID: 10938 Name: Apache Remote Command Execution via .bat files Family: Web Servers Category: attack Copyright: This script is Copyright (C) 2002 Matt Moore Summary: Tests for presence of Apache Command Execution via .bat vulnerability Description: The Apache 2.0.x Win32 installation is shipped with a default script, /cgi-bin/test-cgi.bat, that allows an attacker to execute commands on the Apache server (although it is reported that any .bat file could open this vulnerability.) An attacker can send a pipe character ' ' with commands appended as parameters, which are then executed by Apache. Solution: This bug is fixed in 1.3.24 and 2.0.34-beta, or remove /cgi-bin/test-cgi.bat Risk factor : High Version: \$Revision: 1.14 \$ CVE IDs: CVE-2002-0061 Bugtraq IDs: 4335	
12239	High		Injection Vulnerability	CVE-2003-0020
14177	High		Vulnerability	CVE-2003-0993
15025	High			CVE-2001-0131 CVE-2002-0839 CVE-2002-0840 CVE-2002-0843 CVE-2002-1233
14443	High		Denial of Service vulnerability	-
17197	High		python	CVE-2005-0088
11438	High		Closure Bugs	CVE-2003-0042
15554	High			CVE-2004-0940
15024	High			CVE-2001-0131 CVE-2002-0839 CVE-2002-0840 CVE-2002-0843 CVE-2002-1233
14508	High			CVE-2003-0993 CVE-2003-0020 CVE-2003-0987 CVE-2004-0174
19682	High		ssl	CVE-2005-2700
11209	High	2009-12-15 09:55:05	Gain a shell remotely - Checks for version of Apache	CVE-2003-0016





Ossim

# Reports ISO-PCI

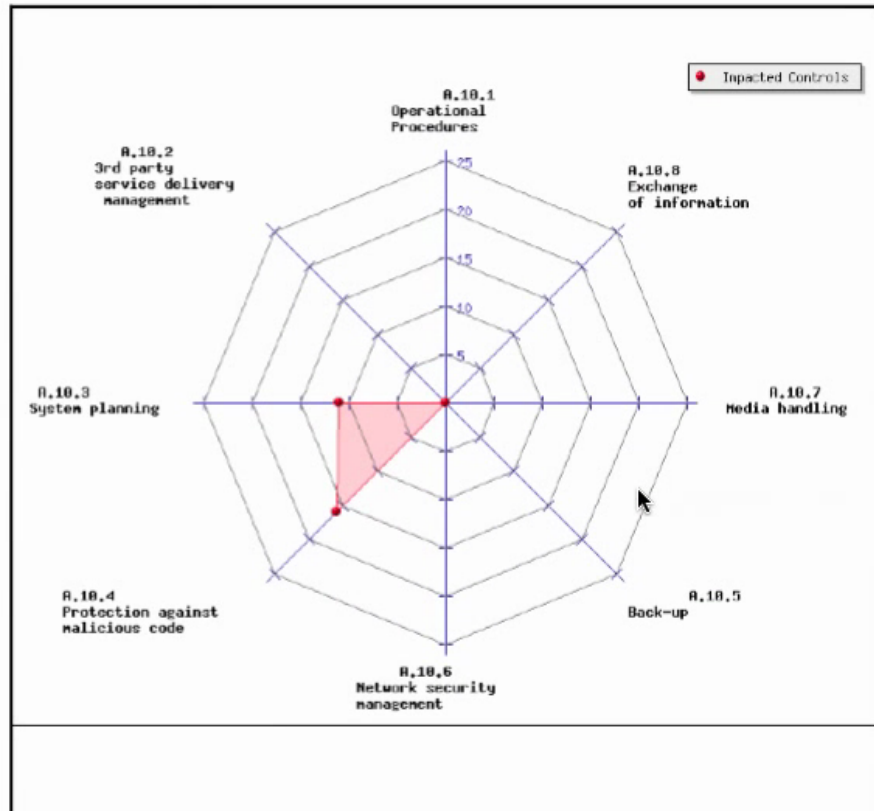
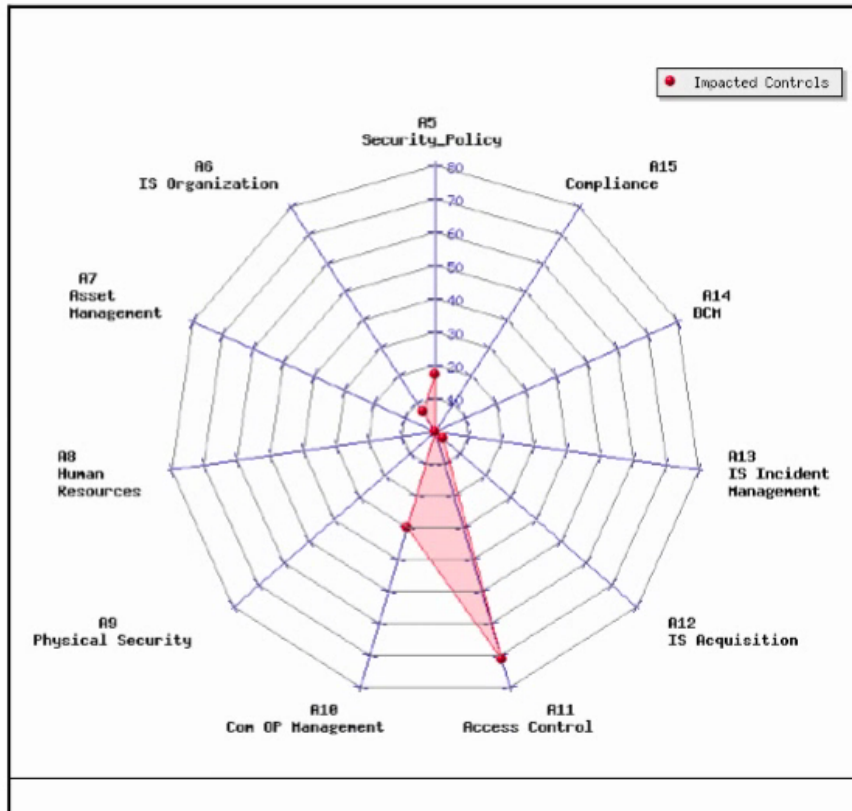
Open Source SIM

Business & Compliance ISO PCI Report



## ISO27002

### Potential impacts - risks





Ossim

# Reports

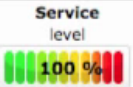


Tickets Opened **361**  
Unresolved Alarms **1.159**

Last updated: 2010-02-05 13:37:25  
Last updated: 2010-02-07 13:34:37

Max priority **8**  
Max risk **5**

Global score



- Dashboards
- Incidents
- Analysis
- Reports
- Assets
- Intelligence
  - Policy & Actions
  - Correlation Directives
  - Compliance Mapping
  - Cross Correlation
- Monitors
- Configuration
- Tools
- Logout [admin]
- Maximize

ISO 27001 PCI DSS

<ul style="list-style-type: none"> <li>◆ A.5.1 Information security policy</li> <li>◆ A.6.1 Internal organization</li> <li>◆ A.6.2 External parties</li> <li>◆ A.7.1 Responsibility for assets</li> <li>◆ A.7.2 Information classification</li> <li>◆ A.8.1 Prior to employment</li> <li>◆ A.8.2 During employment</li> <li>◆ A.8.3 Termination or change of employment</li> <li>◆ A.9.1 Secure area</li> <li>◆ A.9.2 Equipment security</li> <li>◆ A.10.1 Operational procedures and responsibilities</li> <li>◆ A.10.2 Third party service delivery management</li> <li>◆ A.10.3 System planning and acceptance</li> <li>◆ A.10.4 Protection of personally identifiable information</li> <li>◆ A.10.5 Access control</li> <li>◆ A.10.6 Network security management</li> <li>◆ A.10.7 Media handling</li> </ul>	<table border="1"> <thead> <tr> <th>Security Controls</th> <th>Applies</th> <th>Implemented</th> <th>Justification</th> <th>Plugins</th> </tr> </thead> <tbody> <tr> <td>A.7.2.1 Classification guidelines</td> <td>Selected</td> <td>×</td> <td></td> <td></td> </tr> <tr> <td>A.7.2.2 Information labelling and handling</td> <td>Selected</td> <td>×</td> <td></td> <td></td> </tr> </tbody> </table>	Security Controls	Applies	Implemented	Justification	Plugins	A.7.2.1 Classification guidelines	Selected	×			A.7.2.2 Information labelling and handling	Selected	×		
Security Controls	Applies	Implemented	Justification	Plugins												
A.7.2.1 Classification guidelines	Selected	×														
A.7.2.2 Information labelling and handling	Selected	×														

## ISO & PCI Compliance Reports

Correlation Directives mapped to Compliance Control Objectives



Ossim

# Integración Kismet

**alienvault Professional SIEM**

Tickets Opened **362**    Last updated: 2010-02-08 12:27:54  
 Unresolved Alarms **1.160**    Last updated: 2010-02-08 00:08:01

Max priority **8**    Max risk **5**

Global score **100%**    Service level

SIEM   Custom   **Wireless**   Anomalies   Statistics   Setup ?

Locations: Local, New York, Paris

Show All  Trusted  Untrusted  Hide old ones

Network SSID	# of APs	# Clients	Type	Encryption Type	Cloaked	1st Seen	Last Seen	Description	Notes
adsl8877	1	0	Un-Trusted	WEP	No	2010-02-08 06:49:31	2010-02-08 06:49:31		
AGAC	1	0	Un-Trusted	None	No	2010-02-08 06:49:05	2010-02-08 06:50:11		
Aliendroid	1	11	Un-Trusted	TKIP WEP WPA PSK	No	2010-02-08 06:48:55	2010-02-08 06:50:18		
AP1	1	0	Un-Trusted	WEP	No	2010-02-08 06:48:56	2010-02-08 06:50:17		
Archetype	1	0	Un-Trusted	TKIP WEP WPA PSK	No	2010-02-08 06:48:55	2010-02-08 06:50:16		
ARQUITEXTURA	1	5	Un-Trusted	WEP	No	2010-02-08 06:49:06	2010-02-08 06:50:03		
AUSAPE	1	0	Un-Trusted	TKIP WEP WPA PSK	No	2010-02-08 06:48:54	2010-02-08 06:50:15		
BJNPSETUP	0	0	Un-Trusted	None	No	2010-02-08 06:49:18	2010-02-08 06:49:18		
bombeta	1	0	Un-Trusted	TKIP WEP WPA PSK	No	2010-02-08 06:48:54	2010-02-08 06:50:18		
Carlos	1	1	Un-Trusted	AES-CCM TKIP WEP WPA PSK	No	2010-02-08 06:48:56	2010-02-08 06:50:16		
CONSEJEROS	0	0	Un-Trusted	None	No	2010-02-08 06:49:30	2010-02-08 06:49:30		
DLINK_WIRELESS	1	0	Un-Trusted	WEP	No	2010-02-08 06:49:14	2010-02-08 06:50:17		
FON ACCESO PUBLICO I	1	0	Un-Trusted	None	No	2010-02-08 06:48:59	2010-02-08 06:50:17		
FON ACCESO PUBLICO II	1	0	Un-Trusted	None	No	2010-02-08 06:49:05	2010-02-08 06:50:16		
FON ACCESO PUBLICO III	1	0	Un-Trusted	None	No	2010-02-08 06:49:46	2010-02-08 06:49:46		

15 per page    Page 1 of 4

**Full PCI Wireless Security Compliance**  
 Includes all required information and reports to match PCI Wireless Controls



Ossim

# Análisis de Flows

**alienvault Professional SIEM**

Open Tickets: 4 | Unresolved Alarms: 201 | Last updated: 2010-02-01 05:02:56 | Max priority: 6 | Max risk: 4 | Global score: 100% | Service level: 100%

Profile: **live** | Details | Overview | Graphs | Profile: live | Alerts | Stats | Plugins

**Profile: live**

TCP | UDP | ICMP | other

**Profileinfo:**  
 Type: live  
 Max: unlimited  
 Exp: never  
 Start: Jan 29 2010 - 08:42 CST  
 End: Feb 08 2010 - 08:05 CST  
 t\_start: 2010-02-08 07:50  
 t\_end: 2010-02-08 07:50

**Mon Feb 8 07:50:00 2010 Bits/s any protocol**

Bits/s any protocol

oossim1

Display: 1 day

Lin Scale | Stacked Graph | Log Scale | Line Graph

**Netflow Analysis**  
 Collect flows using your network devices or OSSIM Collectors

Statistics timeslot Feb 08 2010 - 07:50

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
oossim1	0.0 /s	45.0 /s	53.0 /s	0.0 /s	0.0 /s	573.0 /s	454.0 /s	123.0 /s	0.1 /s	0.0 /s	70.7 kb/s	59.7 kb/s	11.0 kb/s	64.4 kb/s	0.0 /s



Ossim

# Detalle de Flows



Open Tickets **4** | Last updated: 2010-02-01 05:02:56 | Max priority **6** | Global score

Unresolved Alarms **201** | Last updated: 2010-02-08 04:14:56 | Max risk **4** | Service level **100 %**

- Dashboards
- Incidents
- Analysis
- Reports
- Assets
- Intelligence
- Monitors
  - Network
  - Availability
  - System
- Configuration
- Tools
- Logout [admin]
- Maximize

Statistics timeslot Feb 06 2010 - 02:30 - Feb 08 2010 - 07:50

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
ossim1	2.0 /s	1.2 /s	0.7 /s	0.0 /s	0.0 /s	26.8 /s	21.7 /s	4.9 /s	0.2 /s	0.1 /s	102.4 kb/s	97.8 kb/s	4.5 kb/s	108.1 b/s	20.6 b/s

Display:  Sum  Rate

Netflow Processing [ List last 500 sessions ] [ Top 10 Src IPs ] [ Top 10 Dst IPs ] [ Top 10 Src Port ] [ Top 10 Dst Port ] [ Top 10 Proto ]

Source: ossim1 | Filter: port 22 | Options:  List Flows  Stat TopN

Top: 10 | Stat: SRC IP Address | order by: bytes | Limit:  Packets > 0 | Output:  / IPv6 long

Date flow seen	Duration	Proto		Flows	Packets	Bytes	pps	bps	bpp
2010-02-06 05:52:51.870	180060.128	any	ossim	4676	67486	11.1 M	0	514	171
2010-02-06 02:28:36.486	192274.215	any	207.158.15.110	885	9098	6.8 M	0	298	789
2010-02-07 17:18:28.913	9583.272	any	222.35.136.97	1853	22196	2.0 M	2	1780	96
2010-02-06 09:35:27.463	166755.265	any	207.158.15.104	159	5122	1.5 M	0	75	308
2010-02-08 06:32:18.031	4894.189	any	202.117.56.26	1126	13452	1.2 M	2	2110	95
2010-02-06 09:38:54.261	1194.325	any	85.37.38.220	735	8747	840276	7	5628	96
2010-02-06 02:27:36.145	192395.362	any	4.71.21.18	604	8697	565080	0	23	64
2010-02-07 10:24:20.856	1394.159	any	69.164.214.106	420	4990	479088	3	2749	96
2010-02-08 02:34:30.339	19212.614	any	217.126.167.80	88	4801	332656	0	138	69
2010-02-08 03:11:45.540	13652.829	any	204.136.14.32	253	2980	285752	0	167	95

Summary total flows: 11241 | total bytes: 25.8 M | total packets: 155907 | avg bps: 1122 | avg pps: 0 | avg bpp: 173

Time window: 2010-02-06 02:27:26 - 2010-02-08 07:54:45

Total flows processed: 377836 | Records skipped: 0 | Bytes read: 19655164

Sys: 0.040s flows/second: 9445427.7 | Wall: 0.036s flows/second: 10465211.6



Ossim

# Logger



Open Tickets **4**  
Unresolved Alarms **201**

Last updated:  
2010-02-01 05:02:56  
Last updated:  
2010-02-08 04:14:56

Max priority **6**  
Max risk **4**

Global score

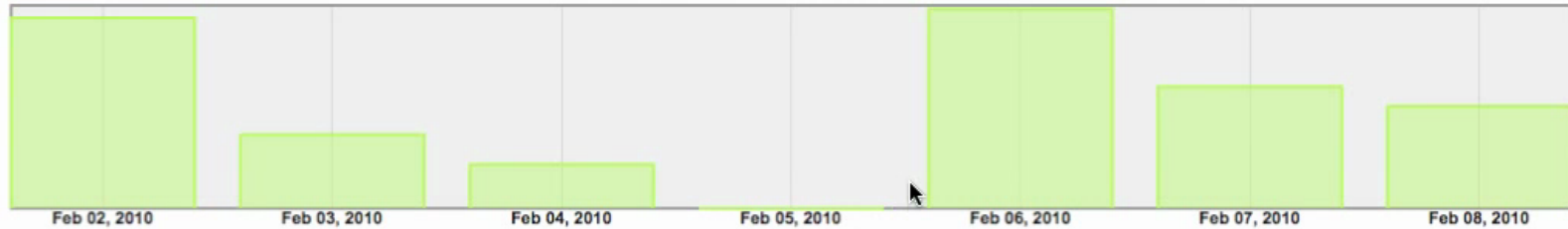
Service level  
100 %

- Dashboards
- Incidents
- Analysis
  - SIEM Events
  - Logger
  - Vulnerabilities
- Reports
- Assets
- Intelligence
- Monitors
- Configuration
- Tools
- Logout [admin]
- Maximize

## Logs

Graphs by dates

Click to show the main chart



Search

Submit Query

Clear Query

Export

Time frame selection: 2010-02-01 09:06:34 2010-02-08 09:06:34 OK Last 24 Hours **Last Week** Last Month Last Year About 58.167 logs

Graphs

Time Range: '2010-02-01 09:06:34' <-> '2010-02-08 09:06:34'

Parsing time: 0.34 seconds.

Next 50

ID	Date	Type	Sensor	Source	Dest	Data	Signature
1	2010-02-08 07:55:48	portscan	ossim	221.195.73.86:0	ossim:0	portscan TCP PortswEEP, src 4183216784 dst 4182608288	Validate
2	2010-02-08 05:13:01	portscan	ossim	Server-Win:0	201.76.55.35:0	portscan Open Port, src 4172793760 dst 4172766736	Validate
3	2010-02-08 05:12:58	portscan	ossim	Server-Win:0	204.188.206.6:0	portscan Open Port, src 4172940096 dst 4173727520	Validate
4	2010-02-08 05:12:58	snort	ossim	204.188.206.6:8086	Server-Win:0	snort ET POLICY PE EXE or DLL Windows file download , src 4172793760 dst 4173727520	Validate
5	2010-02-08 05:12:57	portscan	ossim	Server-Win:0	109.95.114.194:0	portscan Open Port, src 4163589968 dst 4160830320	Validate
6	2010-02-08 05:12:56	portscan	ossim	Server-Win:0	109.95.114.194:0	portscan Open Port, src 4172766736 dst 4172444080	Validate
7	2010-02-08 05:12:55	portscan	ossim	Server-Win:0	109.95.114.194:0	portscan TCP PortswEEP, src 4172438944 dst 4172986976	Validate

# Logger

Navigate clicking on Graphs and using the calendar



Ossim

# Búsqueda en Logger

**alienvault Professional SIEM**

Open Tickets **4** | Last updated: 2010-02-01 05:02:56 | Max priority **6** | Global score **100 %**  
 Unresolved Alarms **201** | Last updated: 2010-02-08 04:14:56 | Max risk **4** | Service level

**Logs**

Graphs by dates

Click to show the main chart

Search     Export

Time frame selection:  2010-02-06 00:00:00  2010-02-06 23:59:59      About 18.751 logs

Time Range: '2010-02-06 23:59:59'  Graphs

ID	Date	Data	Signature
1	2010-02-06 23:59:59	Reporting URL Visited 2 , src 3221357456 dst 3223063760	Validate
2	2010-02-06 23:59:04	snort ossim Server-Win:1102 194.224.66.41:80 snort ET MALWARE Casalemedia Spyware Reporting URL Visited 3 , src 3224893456 dst 3222648176	Validate
3	2010-02-06 23:59:04	snort ossim Server-Win:1102 194.224.66.41:80 snort ET MALWARE Casalemedia Spyware Reporting URL Visited 2 , src 3222193696 dst 3224874208	Validate
4	2010-02-06 23:58:23	portscan ossim Server-Win:0 204.27.57.154:0 portscan Open Port, src 3222829040 dst 3225060480	Validate
5	2010-02-06 23:58:23	portscan ossim Server-Win:0 173.45.105.218:0 portscan Open Port, src 3224893456 dst 3223521248	Validate
6	2010-02-06 23:58:22	portscan ossim Server-Win:0 173.45.105.218:0 portscan Open Port, src 3222082048 dst 3226891296	Validate
7	2010-02-06 23:58:22	portscan ossim Server-Win:0 64.120.176.66:0 portscan Open Port, src 3226058912 dst 3221525248	Validate

Parsing time: 0.29 seconds.

# Puntos Fuertes







*Ossim*

# Puntos Fuertes

- Utiliza herramientas Open Source conocidas y dispone de versión free (50 eps)
  - Permite colaborar e intercambiar desarrollos propios
- Creación/modificación de plugins
  - Futuros equipos o necesidades personales
- Contacto con el equipo de desarrollo
- Nos dejan jugar...
- Precio... depende...



**Puntos débiles**



*Ossim*

# Puntos débiles

- Nos dejan jugar...
  - ¿Sabemos lo que estamos tocando?
  - Depende de lo jugones que seamos... horas son €!
- Utiliza varias herramientas
  - Algunas muy integradas, otras son incrustaciones
- Definir políticas de storage: BD o Logger
  - Roadmap?

# Actual implantación





*Ossim*

# Actual implantación

- Evaluación Profesional
- Maqueta All-in-One Free
- Maqueta distribuida 5 máquinas Free
  - DB, Framework, Server
  - Sensores: Parser y Capture
- Hemos creado Plugins
  - IPS, Router, Firewall (modificado)

# Posibles Mejoras





*Ossim*

# Posibles Mejoras

- Muchas, pero casi todas en RoadMap
- Mejorar BD inventario
- Taxonomía de SIDs
  - Categorizar los posibles eventos
- Alternativas a MySQL
  - Oracle... en pruebas

# Grado de satisfacción







*Ossim*

# Grado de satisfacción

- Pendientes de inversión
- Mientras... OSSIM Free
- Evaluar nueva versión Professional
- Volver a evaluar DSCC
  - Evaluamos una versión primitiva



**Gracias!!**

**Toni Pérez Sánchez**  
toni.perez@uib.es



**Universitat de les  
Illes Balears**  
Centre de Tecnologies  
de la Informació