Toni Pérez Sánchez
toni.perez@uib.es

Universitat de les Illes Balears
Centre de Tecnologies de la Informació

Índice

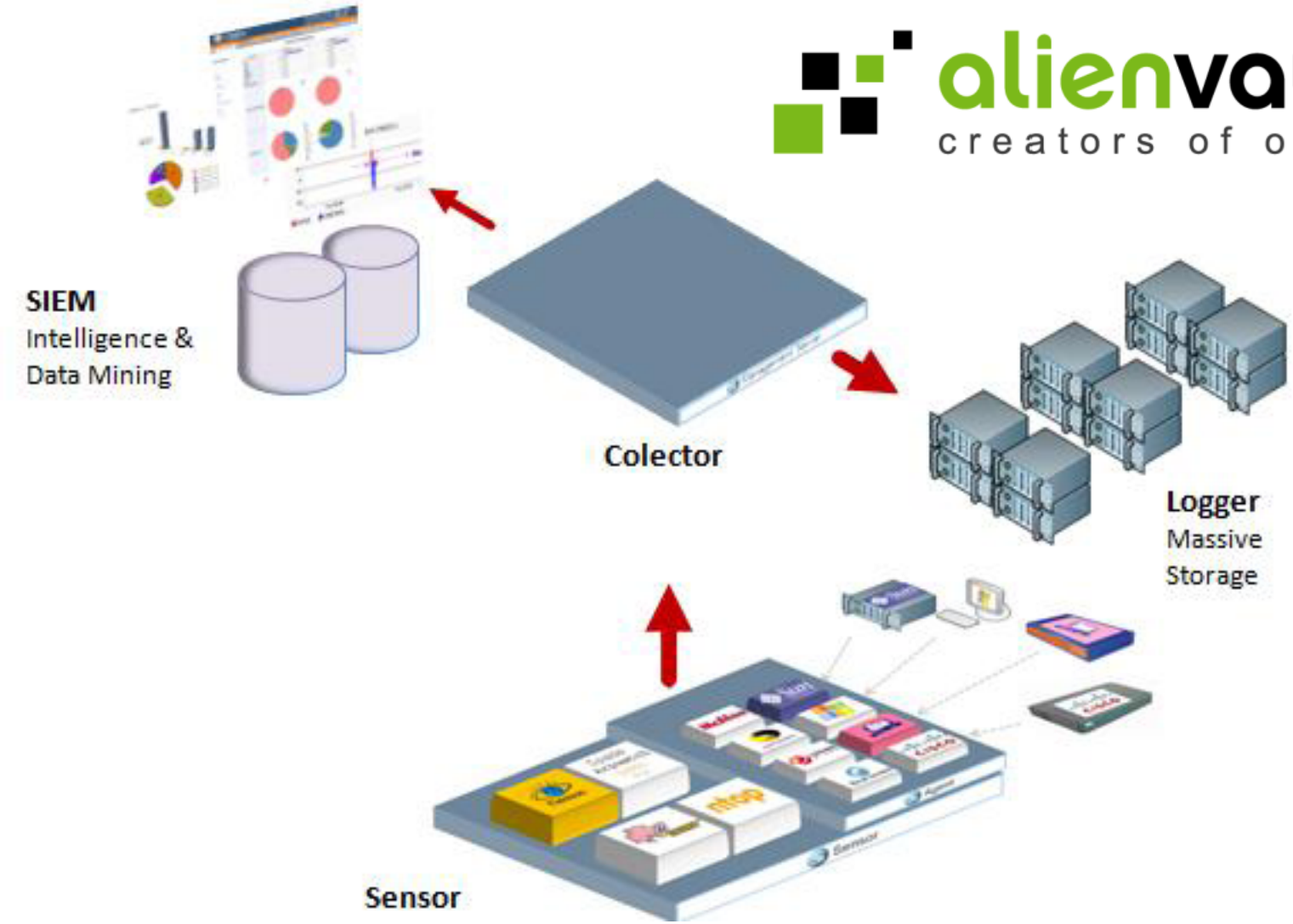
- 1. La herramienta
  - Puntos Fuertes
  - Puntos Débiles
- 2. Actual Implantación
- 3. Posibles Mejoras o necesidades
- 4. Grado de satisfacción

La herramienta

La herramienta

Ossim

alienvault
creators of ossim



Ossim

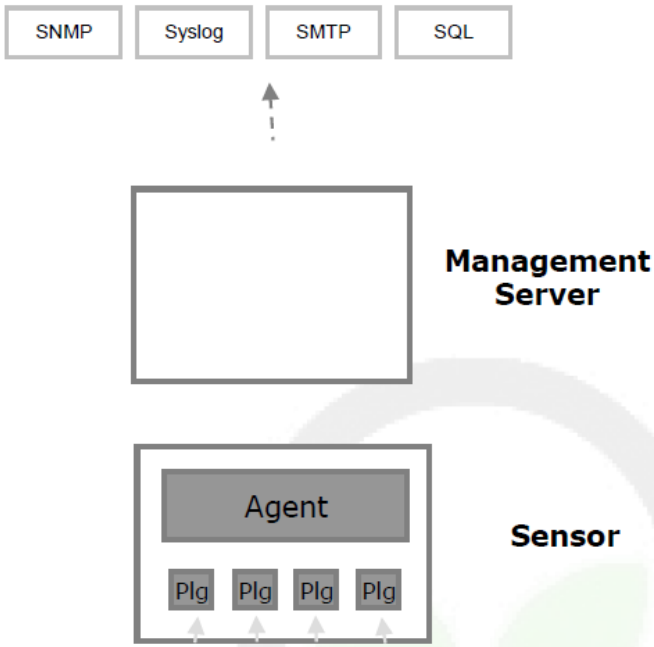
Tools integrados

- Pasivos
  - Snort
  - Ntop y NFSen/Nfdump
  - Kismet
  - P0f y Pads
  - Arpwatch
  - Tcptrack
  - Nepenthes Honeypot
- Activos
  - OCS inventory
  - Nagios
  - OpenVas
  - OSSEC HIDS
  - Nmap
- Otros:
  - OSVDB

Plugins

Ossim

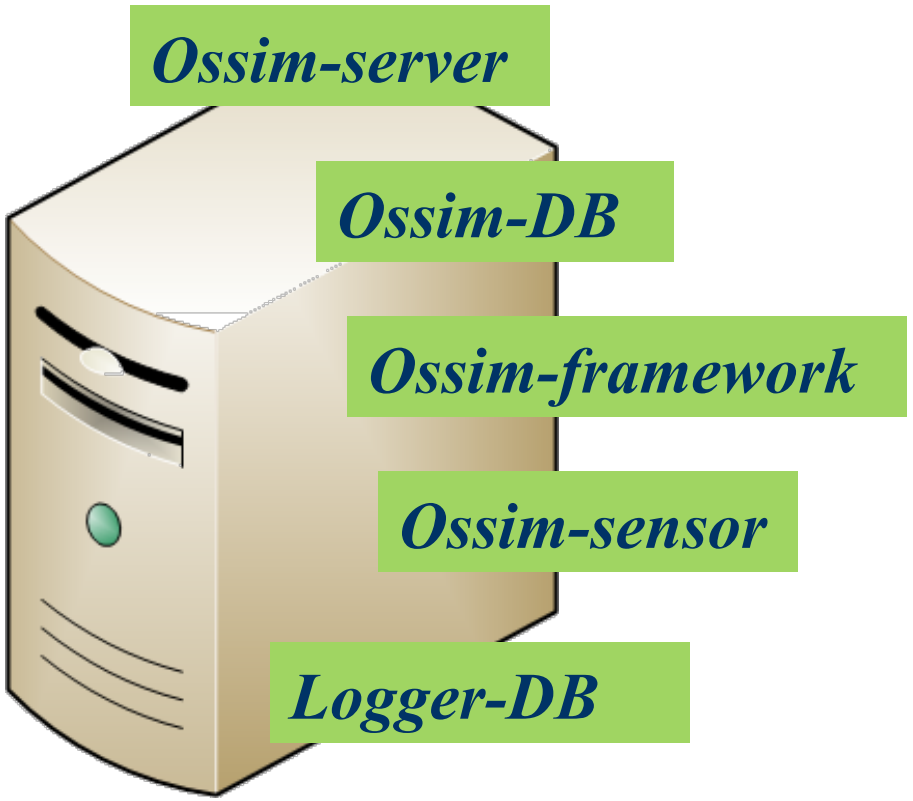
```
[DEFAULT]
plugin_id=1516
[config]
type=detector
enable=yes
source=log
location=/var/log/ossim/pads.csv
# create log file if it does not exists,
# otherwise stop processing this plugin
create_file=true
process=pads
start=yes   ; launch plugin process when agent starts
stop=no     ; shutdown plugin 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 McAfee Real Secure FORTINET NETSCREEN CISCO Sun microsystems

Arquitectura All-In-One

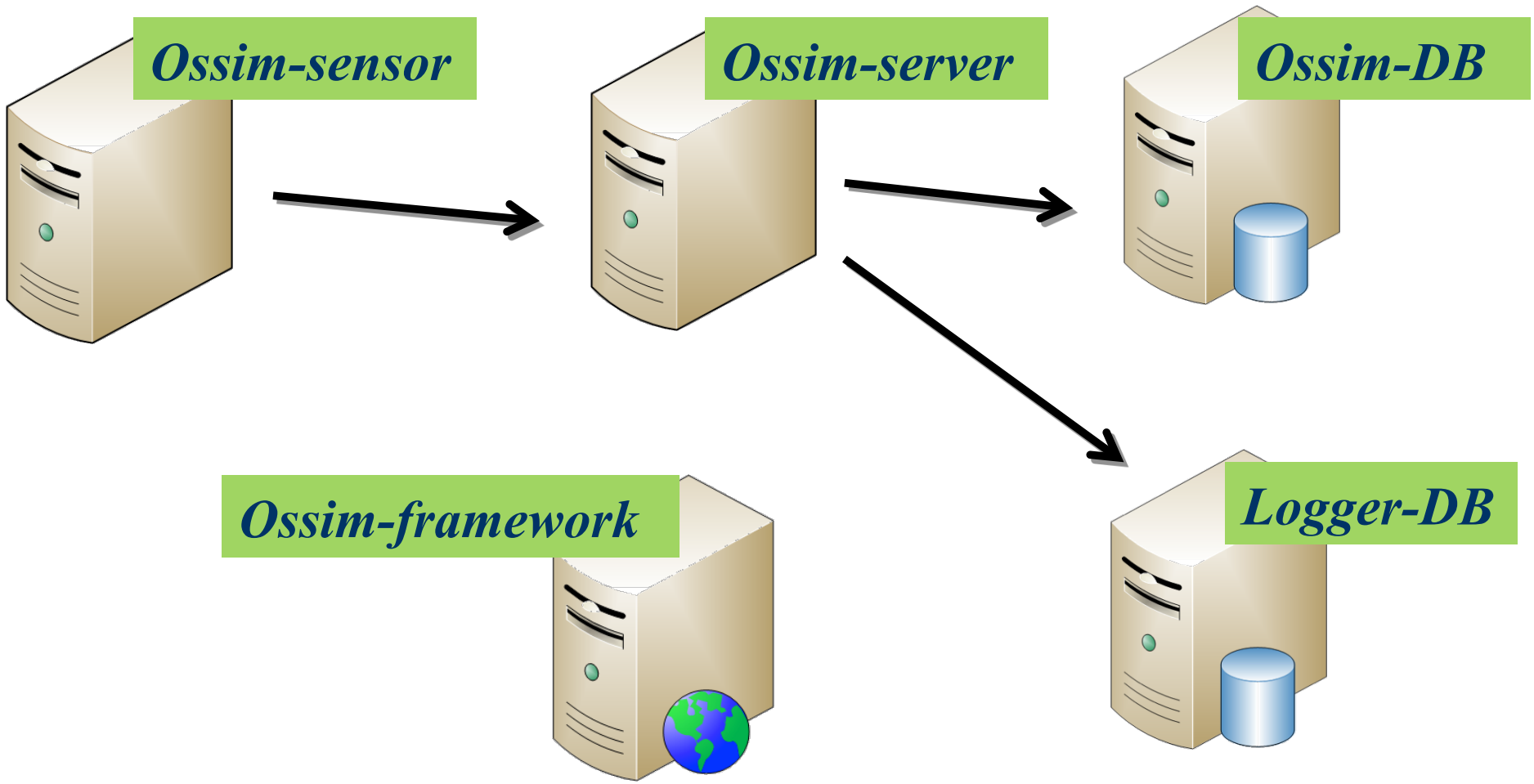


Instalador

Ossim

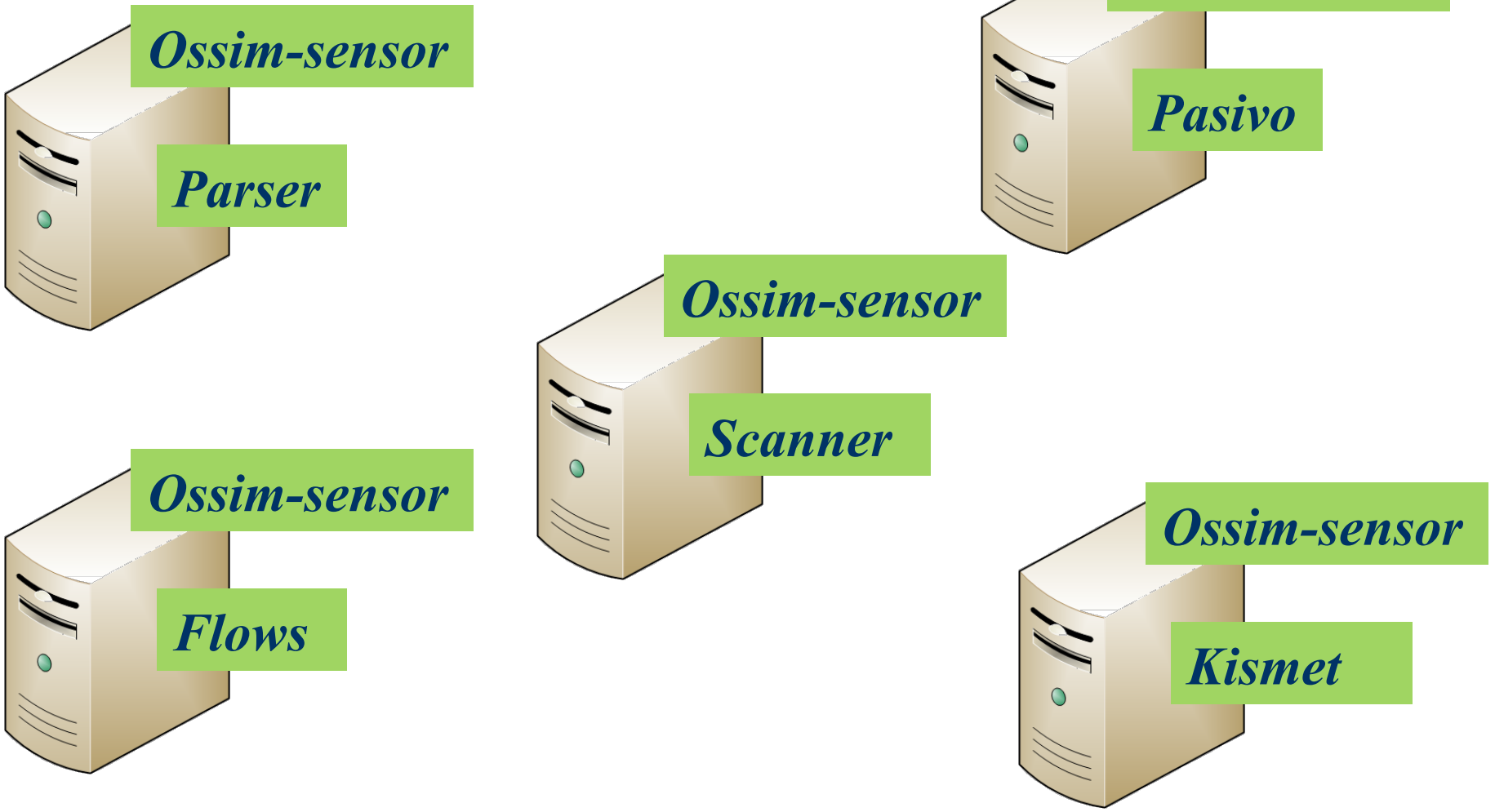
Arquitectura distribuida

Ossim



Arquitectura distribuida

Ossim



Appliance or not!

Ossim

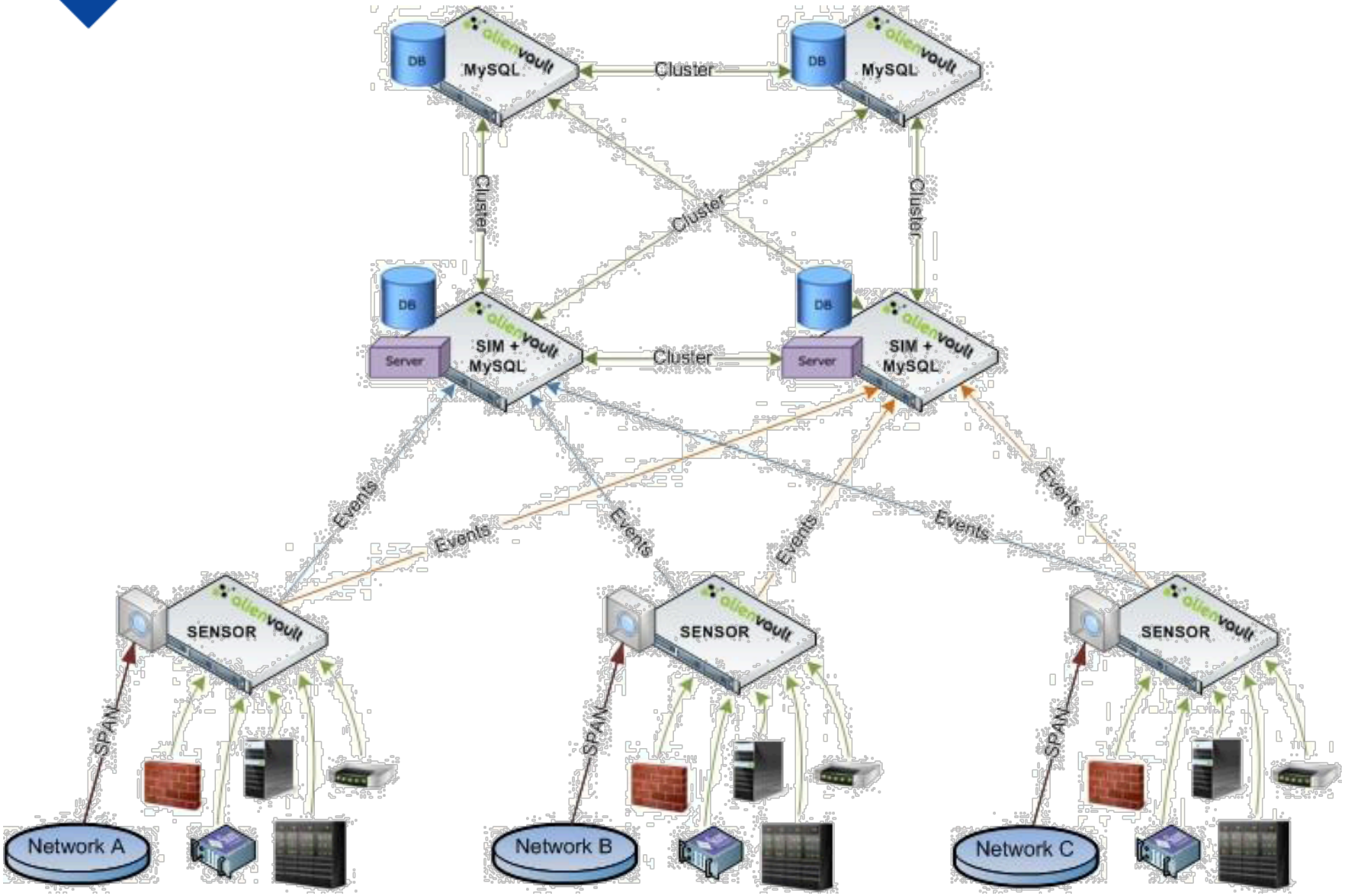
SIEM: ***5.000 eps***
Logger: ***15.000 eps***
Sensor: ***10Gbps***

"Tuned operating system and kernel."

"Network optimization for high load network capture."

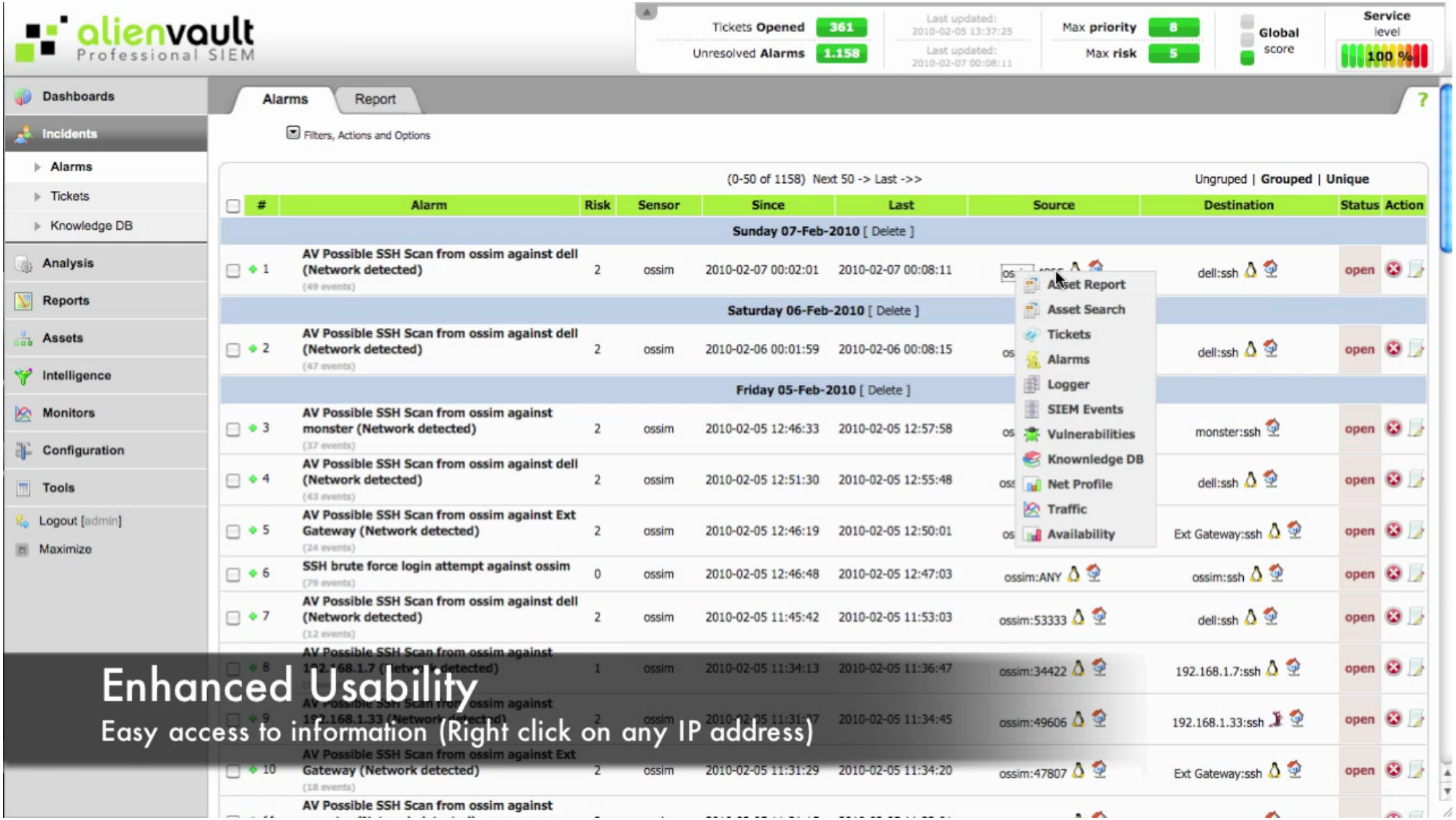
Arquitectura distribuida

Ossim



Alarmas

Ossim

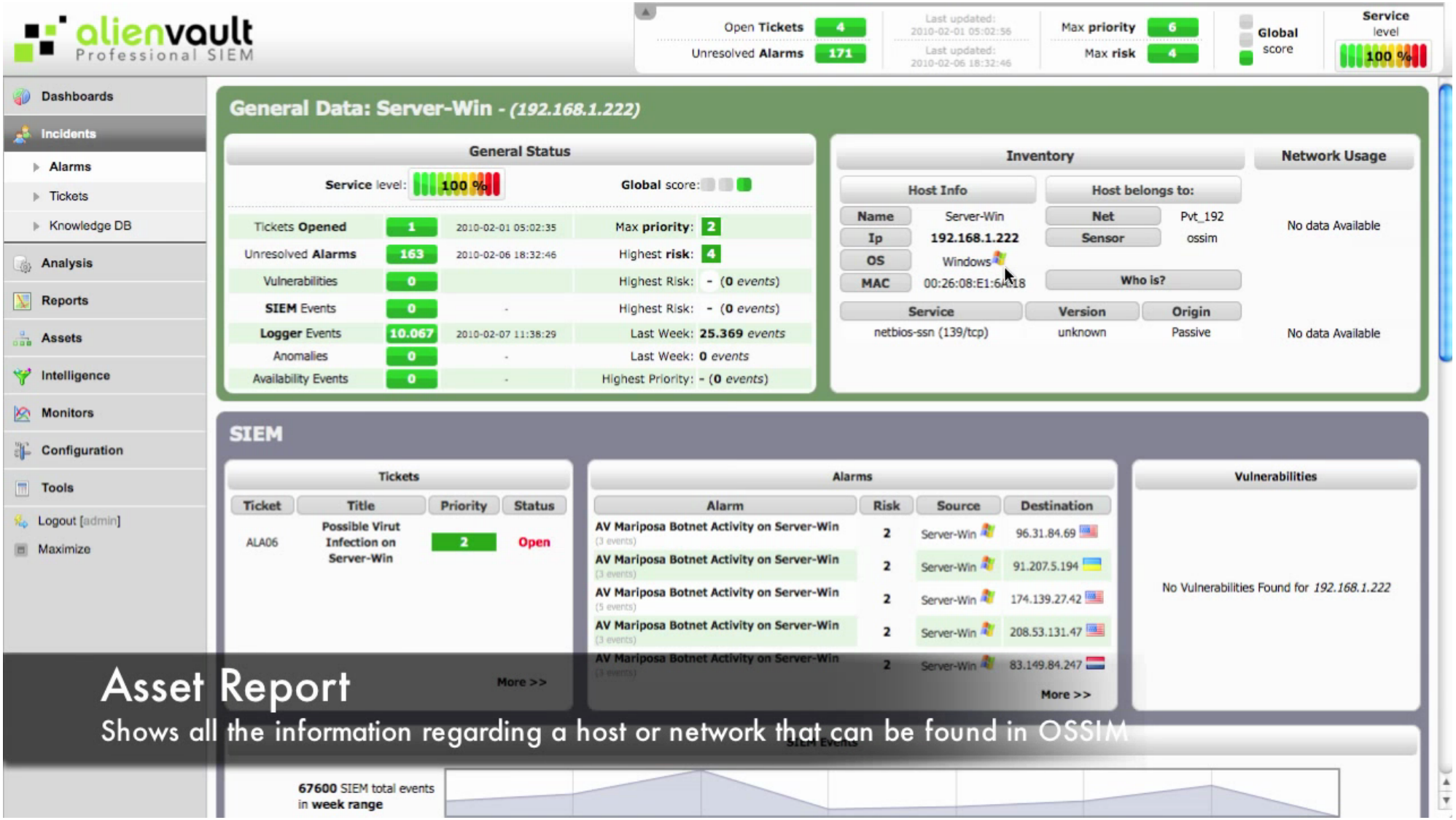


Enhanced Usability

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

Report de objeto

Ossim

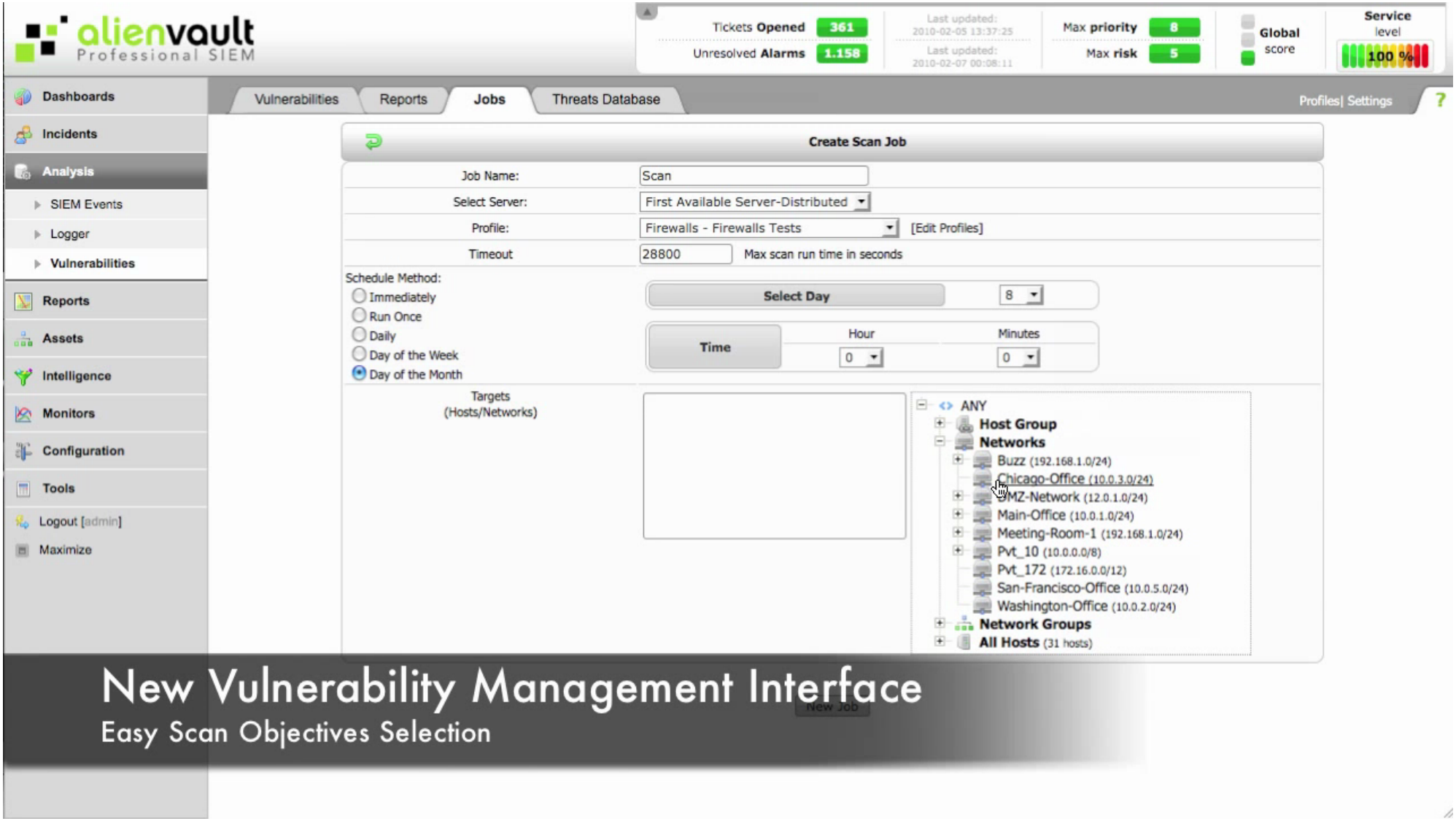


Asset Report

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

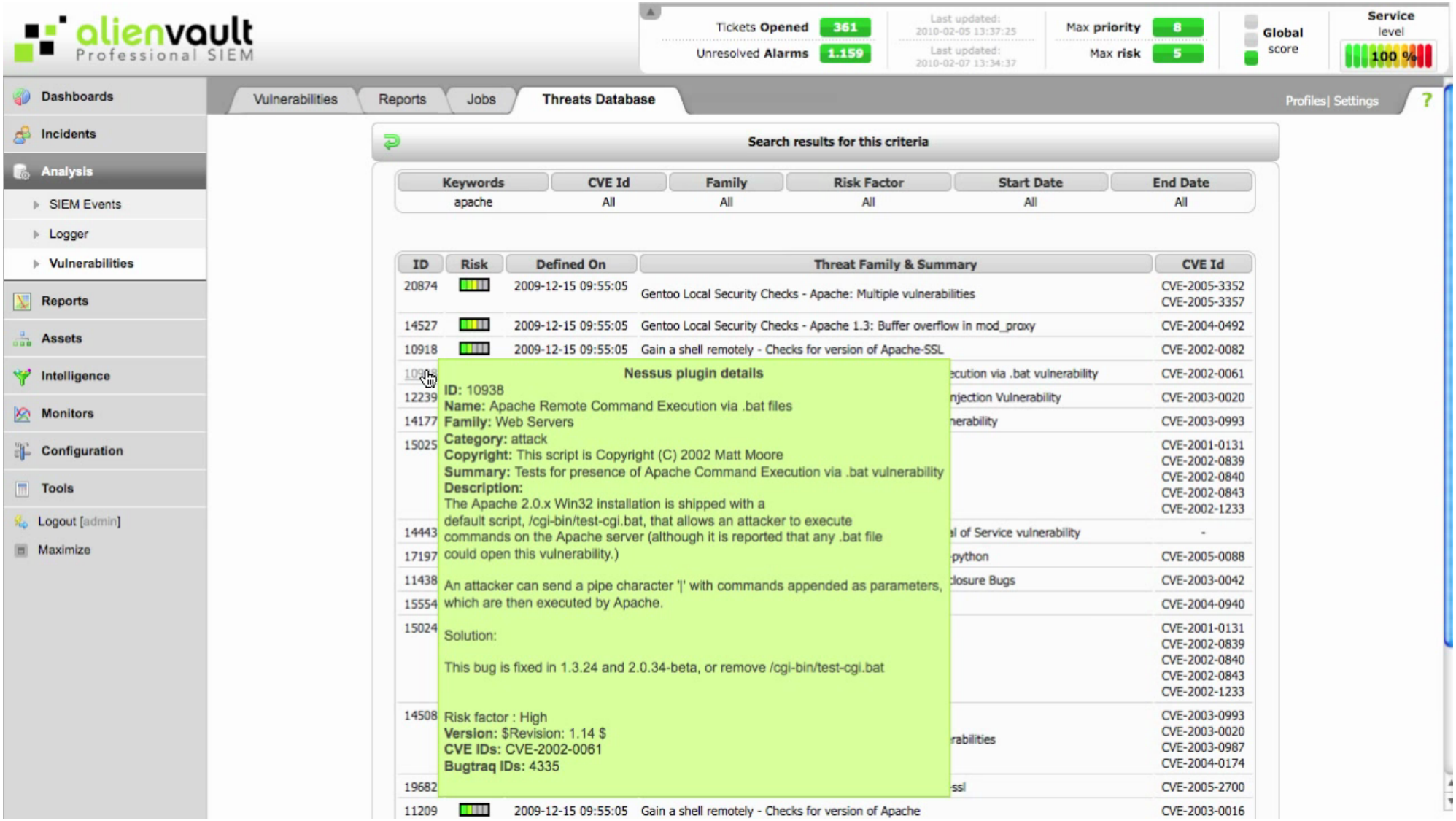
Vulnerability Scan

Ossim



Nessus Plugins

Ossim



Reports ISO-PCI

Ossim

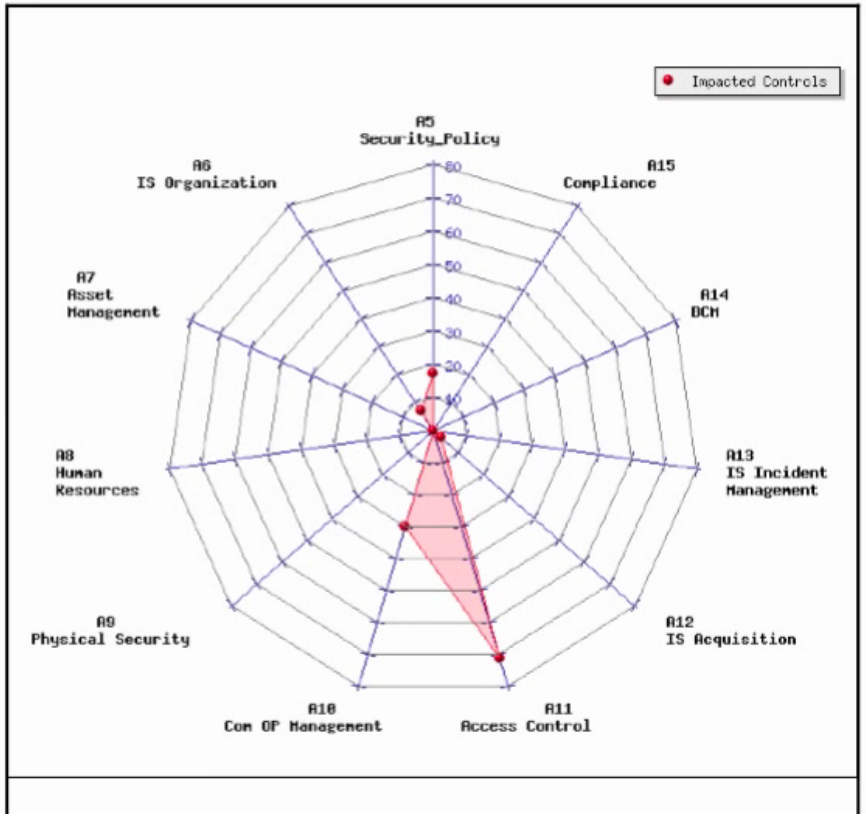
Open Source SIM

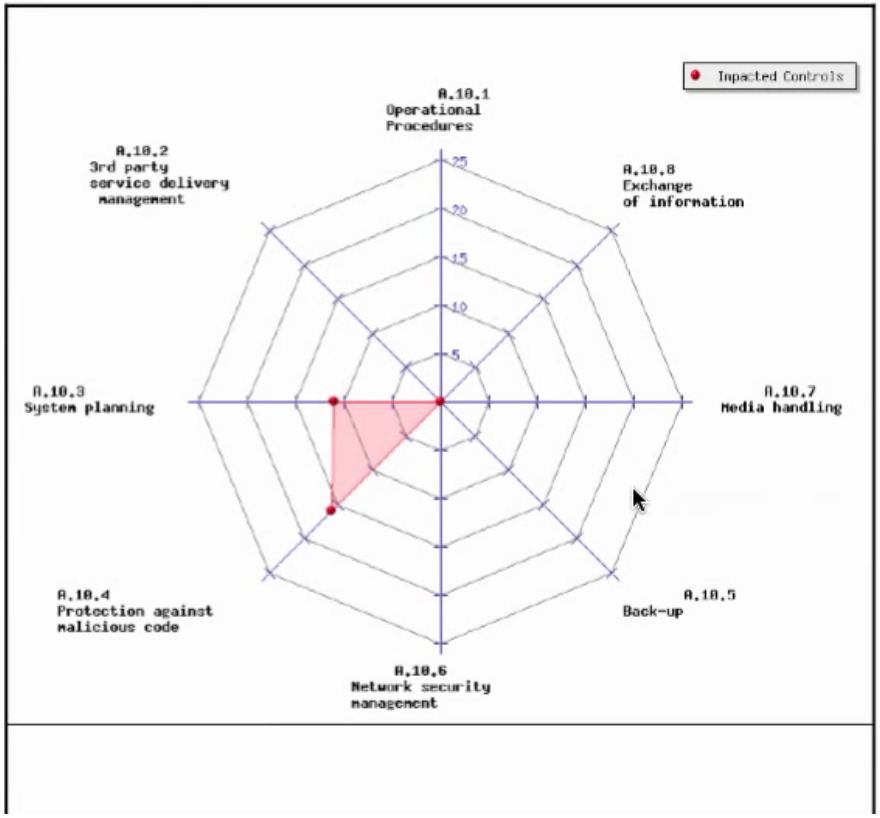
Business & Compliance ISO PCI Report

S@CURITY

ISO27002

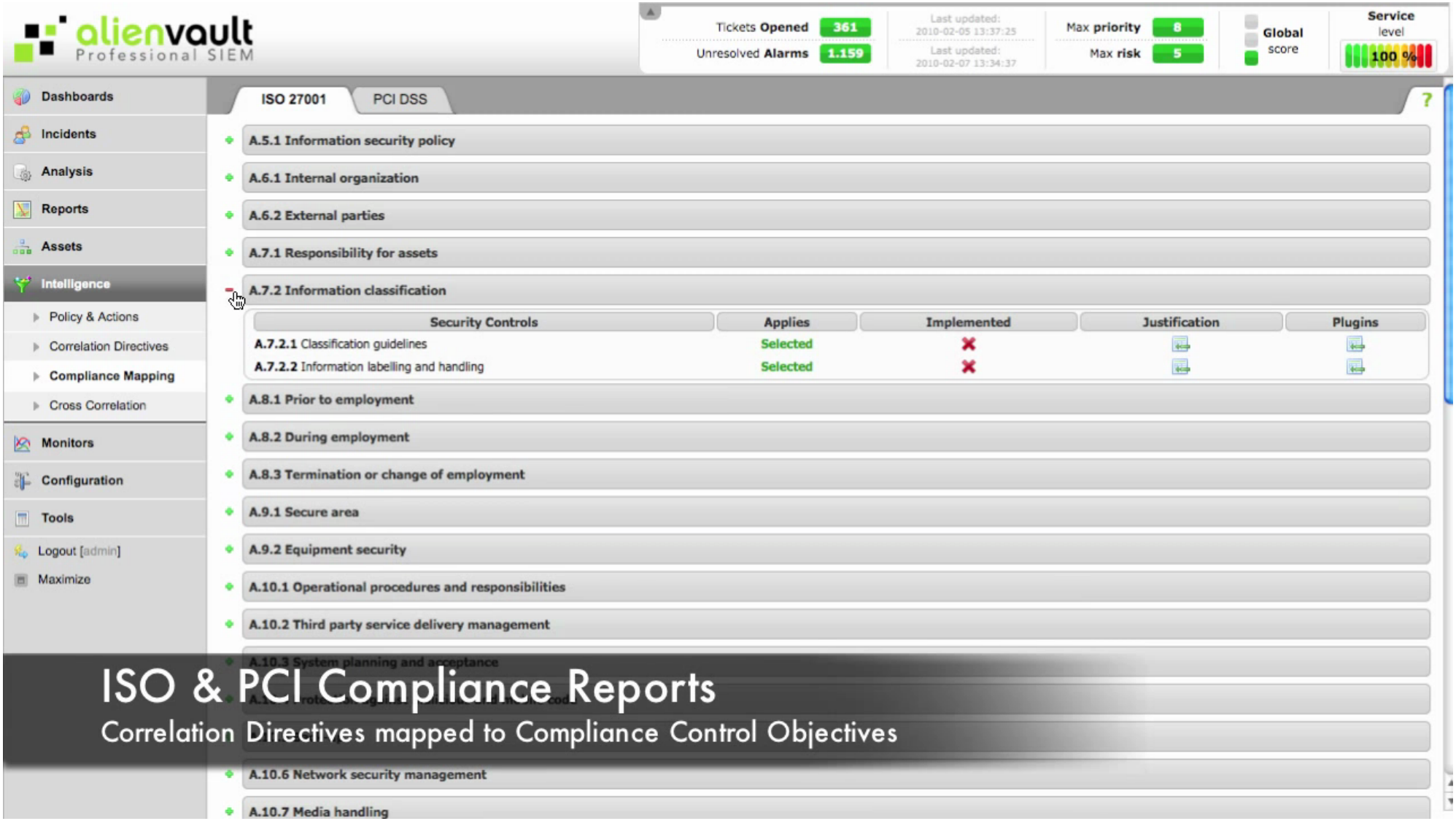
Potential impacts - risks





Reports

Ossim

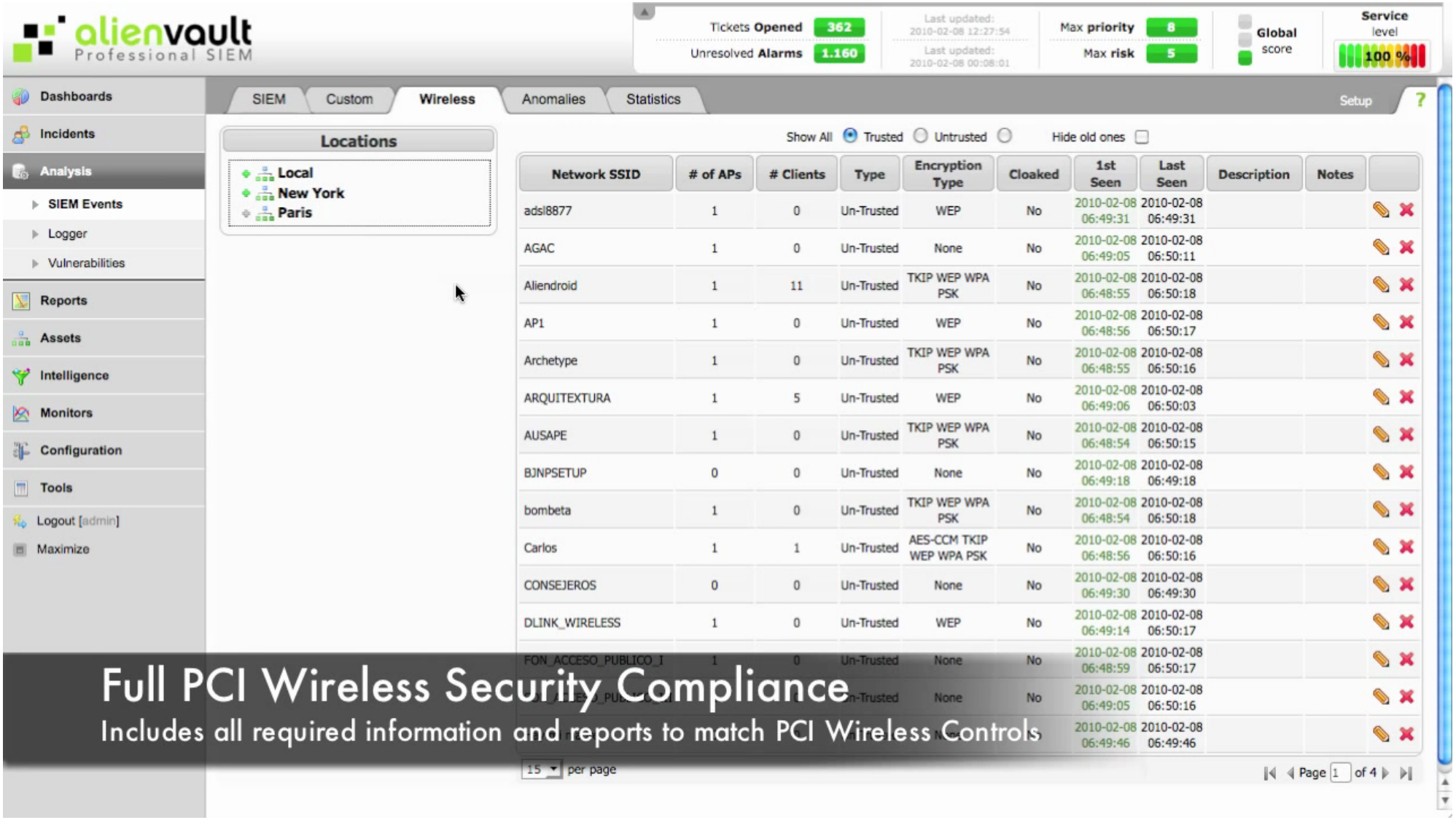


ISO & PCI Compliance Reports

Correlation Directives mapped to Compliance Control Objectives

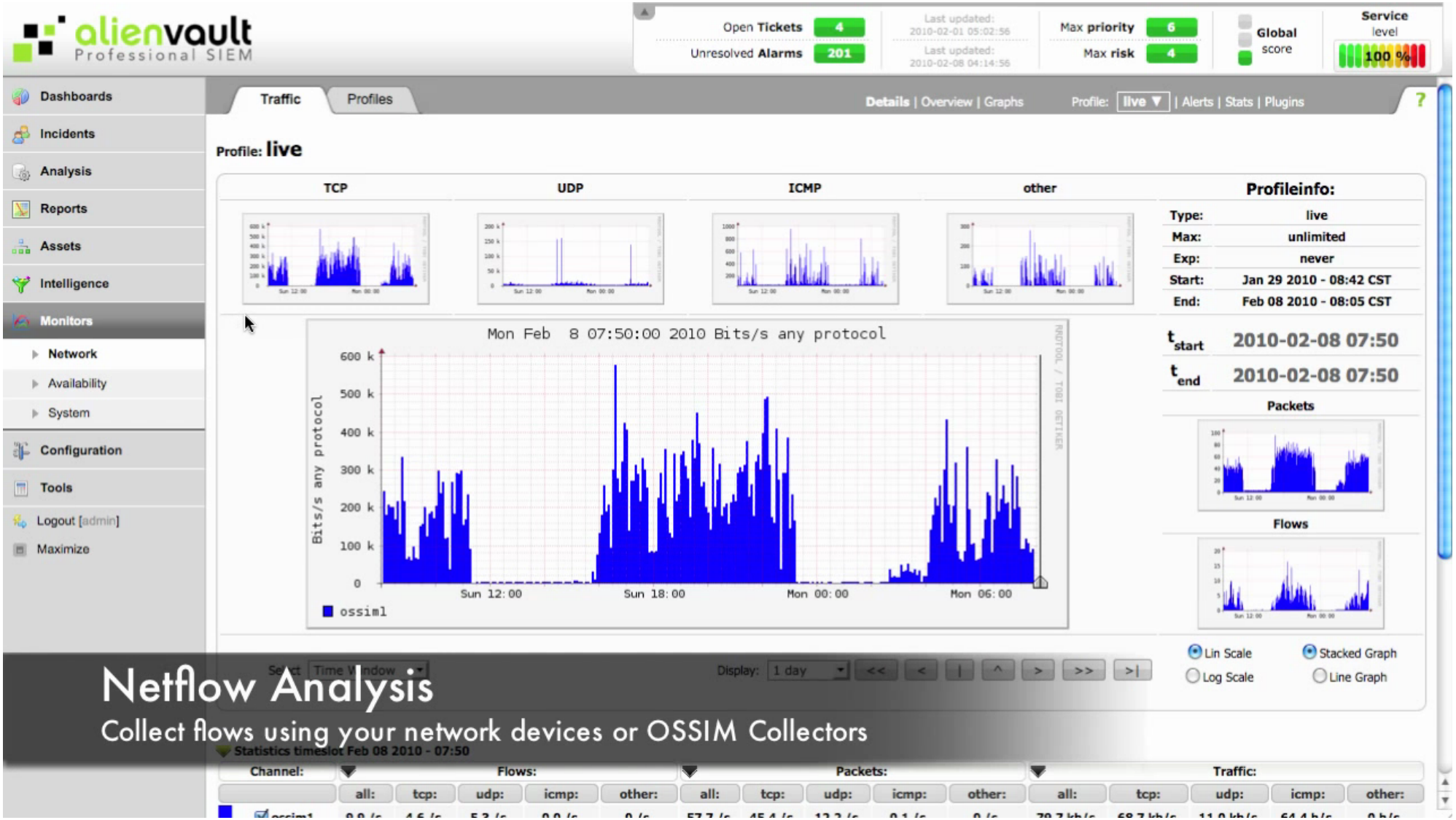
Integración Kismet

Ossim



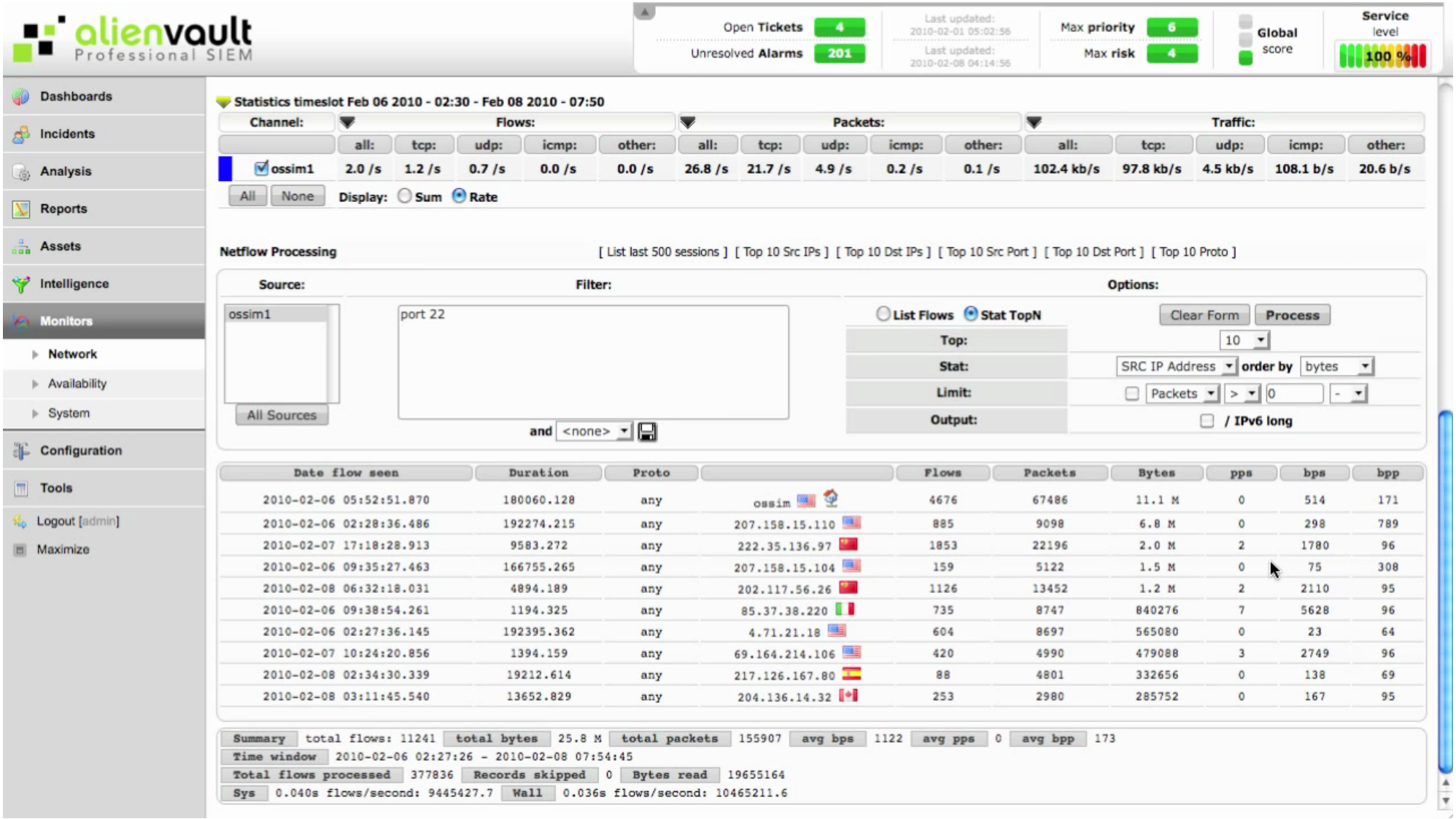
Análisis de Flows

Ossim



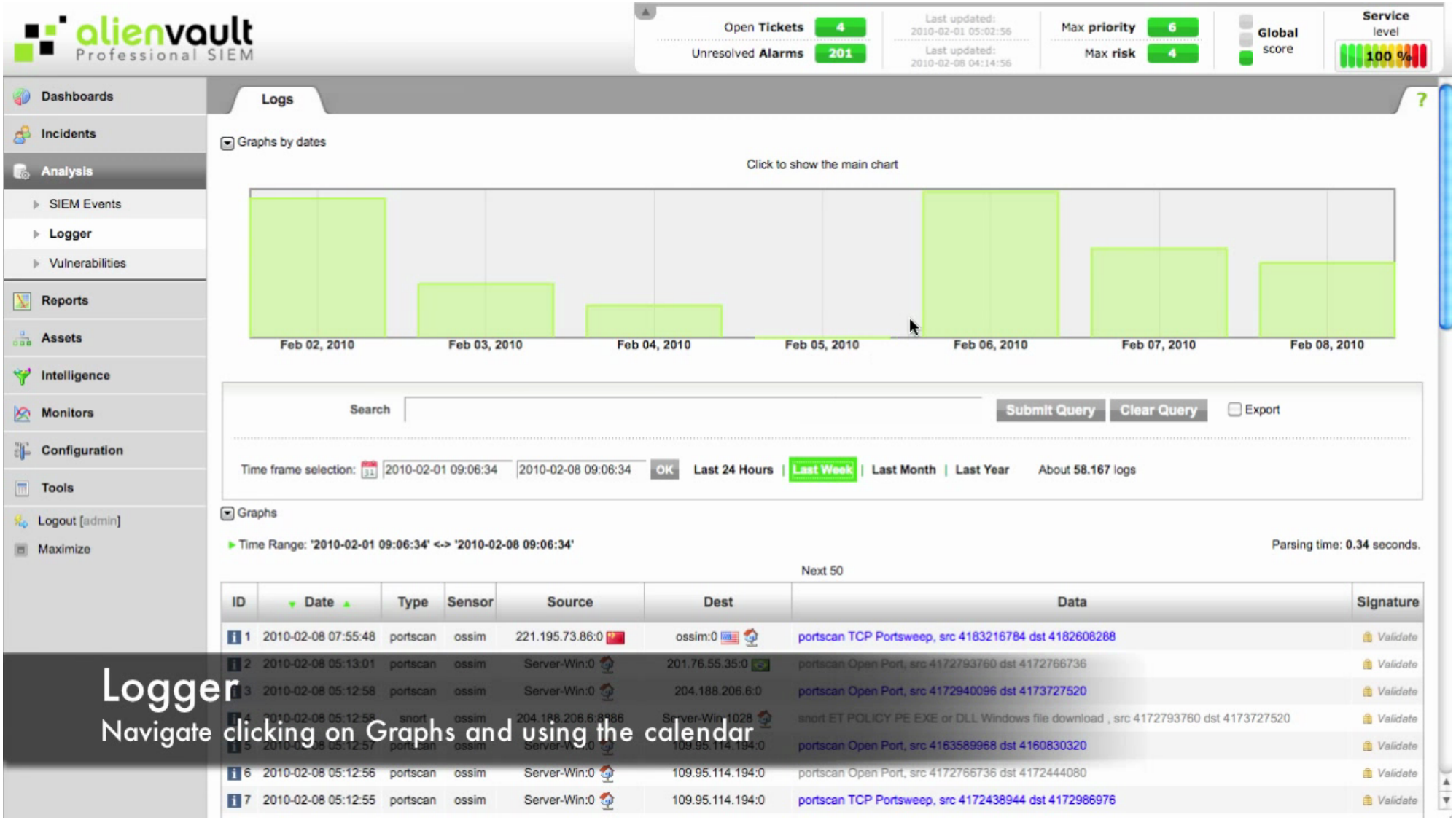
Detalle de Flows

Ossim



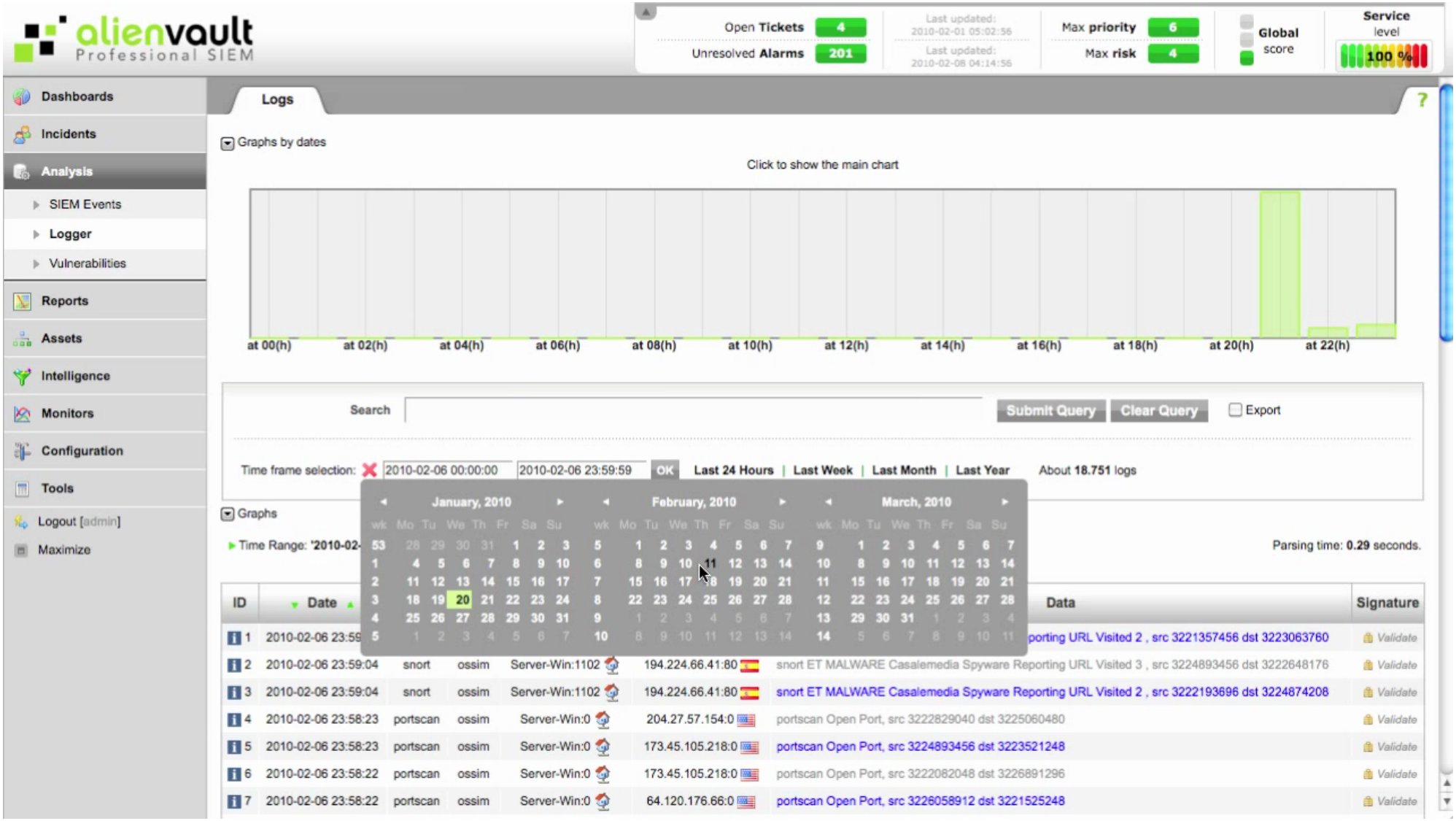
Logger

Ossim



Búsqueda en Logger

Ossim



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 Professional
- 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

Grado de satisfacción

Ossim

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

Toni Pérez Sánchez
toni.perez@uib.es

Universitat de les Illes Balears
Centre de Tecnologies de la Informació