Correlación de eventos de seguridad en entornos HPC

HPC Knowlegde 2011 (Barcelona)

Àlex Vaqué

12 - 10 - 2011

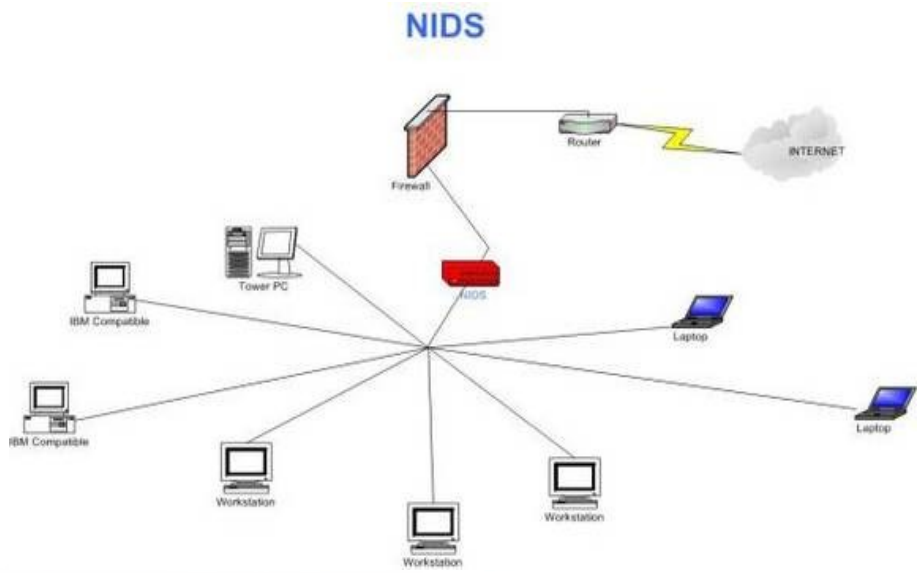
1. Sistemas de detección de intrusos (IDS)
   - NIDS
   - HIDS

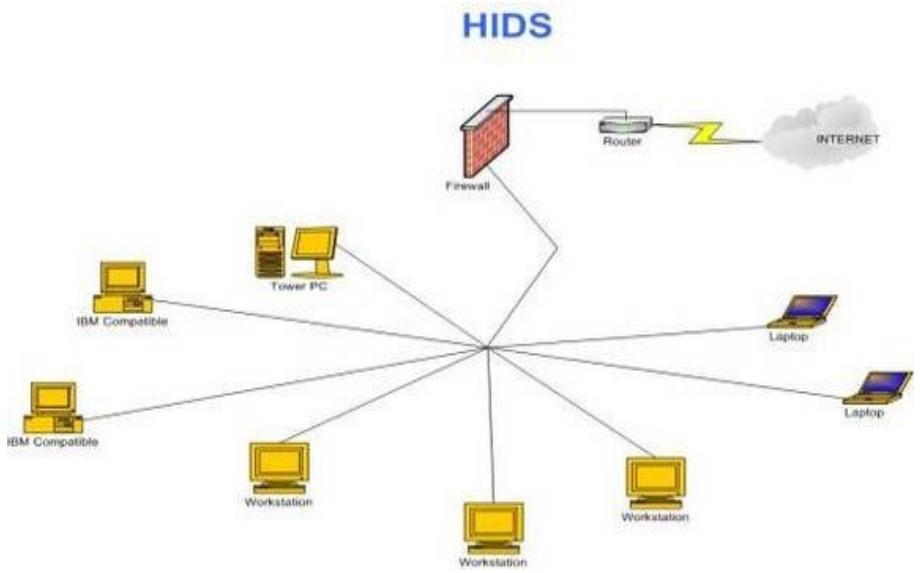
2. Caso de uso mediante OSSEC
   - Introducción
   - Reglas y ejemplos
   - OSSEC WUI

3. Integración con sistemas de inteligencia operacional
   - Splunk
   - OSSEC for Splunk

1. Sistemas de detección de Intrusos (IDS)

- Intrusion detection system (IDS)
- Distinto de un IPS (intrusion prevention system) que es un sistema activo
- Monitoriza información para identificar comportamiento malicioso
  - Detección de anomalias o coincidencia de patrones
- Básicamente automatiza la monitorización del tráfico





Els HIDS como complemento estratégico

- Fácil implementación
- Pocos requerimentos de Hardware y bajos falsos positivos
- Alta visibilidad en protocols encriptados
- Visibilidad de la actividad del sistema (kernel, comportamiento de usuarios, etc.)
- Requieren centralització y agentes en los clientes
- Basados en tractamiento de logs y cambios
- Los cortafuegos son cada vez menos eficaz (puerto 80) y la defensa de las aplicaciones requiere de nuevos enfoques

Soluciones libres HIDS

- Osiris
- Samhain
- **OSSEC**
- Integrity
- AIDE
- Samhain+Osiris

2. Caso de uso mediante OSSEC

- Open source HIDS
- Centrado en el análisis de logs
  - Las aplicaciones generan información relevante que se tendrían que considerar, no?
  - Más fácil de tratar que los paquetes de red
- Generación y almacenage centralizado de alertas, no de logs.
- Arquitectura basada en agentes (Via conexiones seguras)
- Fácil de instalar, configurar y ampliar.
- Multiplataforma (Windows, Solaris, Linux, BSD, etc.)

Que ofrece OSSEC I

- Revisión de la **Integridad a nivel de archivos**
- Revisión de la **Integridad del Registro (Win)**
- Detección **de anomalías** a nivel de HOST (detección de rootkits)
- Alertas en **tiempo real** y respuesta **Activa**
- Análisis de Logs (**Variedad destacada** de tipo de logs soportados)

Que ofrece OSSEC II

- OSSEC se puede configurar para controlar cualquier log que pueda tener acceso

- Logs de aplicaciones soportados por defecto como:

  - Syslog, Unix Pam, sshd (OpenSSH), Solaris telnetd, Samba, Su, Sudo, Proftpd,Pure-ftpd, vsftpd, Microsoft FTP server, Solaris ftpd, Imapd, Postfix, Sendmail, vpopmail, Microsoft Exchange, Apache, IIS5, IIS6, Horde IMP, Iptables, IPF. PF, Netscreen, Cisco PIX/ASA/FWSM, Snort, Cisco IOS, Nmap, Symantec AV, Arpwatch, Named, Squid, Windows event logs, etc

Modos de funcionamiento

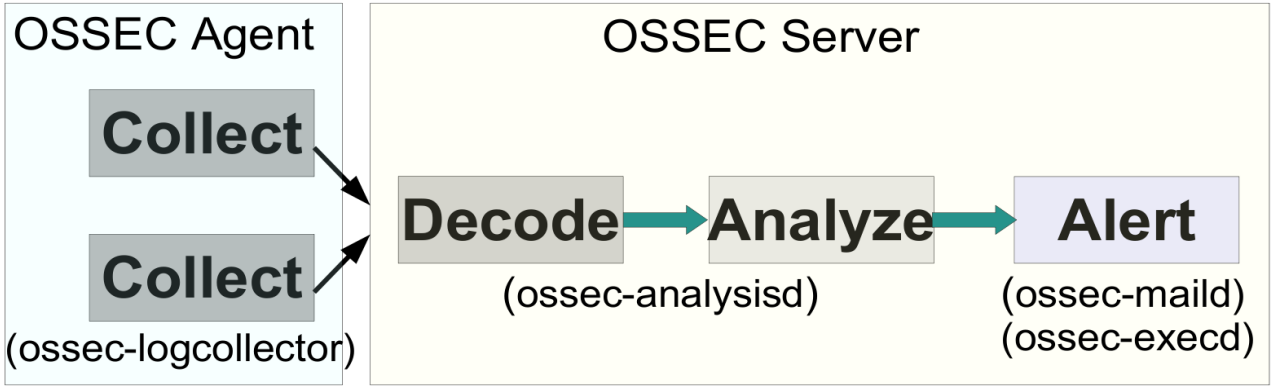
- 2 modos
  - Local: Solo un equipo a monitorizar
  - Client/Server: Monitorización centralizada basada en agentes

- Espacio de archivos
  - Por defecto: /var/ossec
  - Configuración: /var/ossec/etc/ossec.conf
  - Reglas: /var/ossec/rules/*.xml
  - Log de alertas: /var/ossec/logs/alerts.log
  - Binarios: /var/ossec/bin/
  - Decodificadores: /var/ossec/etc/decoders.xml

OSSEC Network Communication

UDP port 1514 (Compressed & encryption)

Flujo de datos



OSSEC Decoders

- OSSEC utiliza decodificadores para parsear los logs
- Los decodificadores estan escritos en XML
- Extrae campos de información útil de las de las entradas de los logs
  - Source IP and/or port
  - Destination IP and/or port
  - Program name or user name
  - Time, Match and more
- Luego se utilizarán para las reglas y para alertar

OSSEC Rules & Rule Format

- Las reglas son asignadas en niveles de prioridad: del 1 al 15
- Rules trigger basados en:
  - Pattern matching in strings
  - Timing between matches (x hits on rule y in z interval)
  - Dependence on other rules (x rule already fired)
  - Time of day
  - Hostnames
  - Applications
- Crear alertas customizadas es fácil

Alertas OSSEC

- Configuración por defecto incluye alertas como:
  - Web attacks
  - SSH brute force
  - Buffer overflows and program crashes
  - Firewall events
  - Users using sudo
  - Muchos más...

Ejemplo de alertas

OSSEC HIDS Notification.

2011 May 27 15:18:53 Rule Id: 5503 level: 5

Location: (engima1) 192.168.X.Y->/var/log/auth.log

Src IP: 22.22.22.22

User login failed.

May 27 15:18:52 s_sys@maquina1 sshd[10227]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=22.22.22.22 user=usuario1

Ejemplo de alertas

OSSEC HIDS Notification.

2011 May 27 16:41:17 Rule Id: 5712 level: 10

Location: (maquina1) 192.168.X.Y->/var/log/auth.log

Src IP: 148.208.X.Y

SSHD brute force trying to get access to the system.

May 27 16:41:17 s_sys@maqu1 sshd[24754]: Invalid user webmaster from 148.208.X.Y

May 27 16:41:14 s_sys@maqu1 sshd[24744]: Failed password for invalid user guest from 148.208.C.Y port 51014 ssh2

May 27 16:41:12 s_sys@maqu1 sshd[24744]: Invalid user guest from 148.208.X.Y

May 27 16:41:12 s_sys@maqu1 sshd[24744]: Invalid user guest from 148.208.X.Y

May 27 16:41:09 s_sys@maqu1 sshd[24724]: Failed password for invalid user admin from 148.208.X.Y port 50612 ssh2

May 27 16:41:07 s_sys@maqu1 sshd[24724]: Invalid user admin from 148.208.X.Y

May 27 16:41:09 s_sys@maqu1 sshd[24724]: Failed password for invalid user admin from 148.208.X.Y port 50612 ssh2

Ejemplos de alertas

OSSEC HIDS Notification.

2011 Oct 08 03:29:08

Received From: (maquina.cesca.cat) 192.168.X.Y->/var/log/messages

Rule: 100130 fired (level 10) -> "Accounting access outside of regular business hours."

Portion of the log(s):

Oct 8 03:29:25 maquina1 sshd[554254]: Accepted keyboard-interactive/pam for usuario02 from 108.28.X.Y port 35098 ssh2

Ejemplo alerta

OSSEC HIDS Notification.

2011 Oct 11 11:06:08

Received From: (cloudcop) 192.168.X.Y->/var/log/syslog

Rule: 7202 fired (level 9) -> "Arpwatch "flip flop" message. IP address/MAC relation changing too often."

Portion of the log(s):

Oct 11 11:18:29 cloudcop arpwatch: flip flop 84.89.X.Y 02:00:54:59:00:74 (02:00:54:59:00:76) eth0

Ejemplo de alertas

OSSEC HIDS Notification.

2010 Aug 04 12:10:08

Received From: webdev->/var/log/httpd/access_log

Rule: 31106 fired (level 12) -> "A web attack returned code 200 (success)."

Portion of the log(s):

172.16.46.X - - [04/Aug/2010:12:10:07 -0400] "GET /drupal-4.7.11/?q=user/autocomplete/%3Cscript%3Ealert(%27title%27)%3B%3C%2Fscript%3E HTTP/1.1" 200 140 "http://172.16.46.129/drupal-4.7.11/?q=node/add/page" "Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.11) Gecko/20100723 Fedora/3.5.11-1.fc12 Firefox/3.5.11"

Ejemplo de reglas

```
<rule id=”100130” level=”12”>
    <if_sid> 5700 </if_sid>
    <time> 8:00pm – 6.00am </time>
    <description> Accounting access outside of regular business hours. </description>
    <user> empleado1 </user>
    <group> policy_violation </group>
    <hostname> maquina01 </hostname>
</rule>


  <rule id="5700" level="0" noalert="1">
     <decoded_as>sshd</decoded_as>
     <description>SSHD messages grouped.</description>
  </rule>
```

Respuesta activa

```
  <command>
     <name>mail-test</name>
     <executable>mail-test.sh</executable>
     <timeout_allowed>no</timeout_allowed>
     <expect />
  </command>

<active-response>
    <command>mail-test</command>
    <location>server</location>
    <rules_id>100130</rules_id>
</active-response>
```

OSSEC WUI

Main | Search | Integrity checking | Stats | About

PayPal DONATE

October 11th 2011 07:21:44 PM

Available agents:

(127.0.0.1)
(192.168.29.70)
(192.168.29.54)
web (192.168.33.100)
(192.168.29.62)

Latest modified files:

+/usr/sbin/sshd
+/etc/pam.d/sshd
+/etc/ssh/sshd_config
+/etc/rc.d/rc5.d/S55sshd
+/etc/rc.d/rc0.d/K25sshd

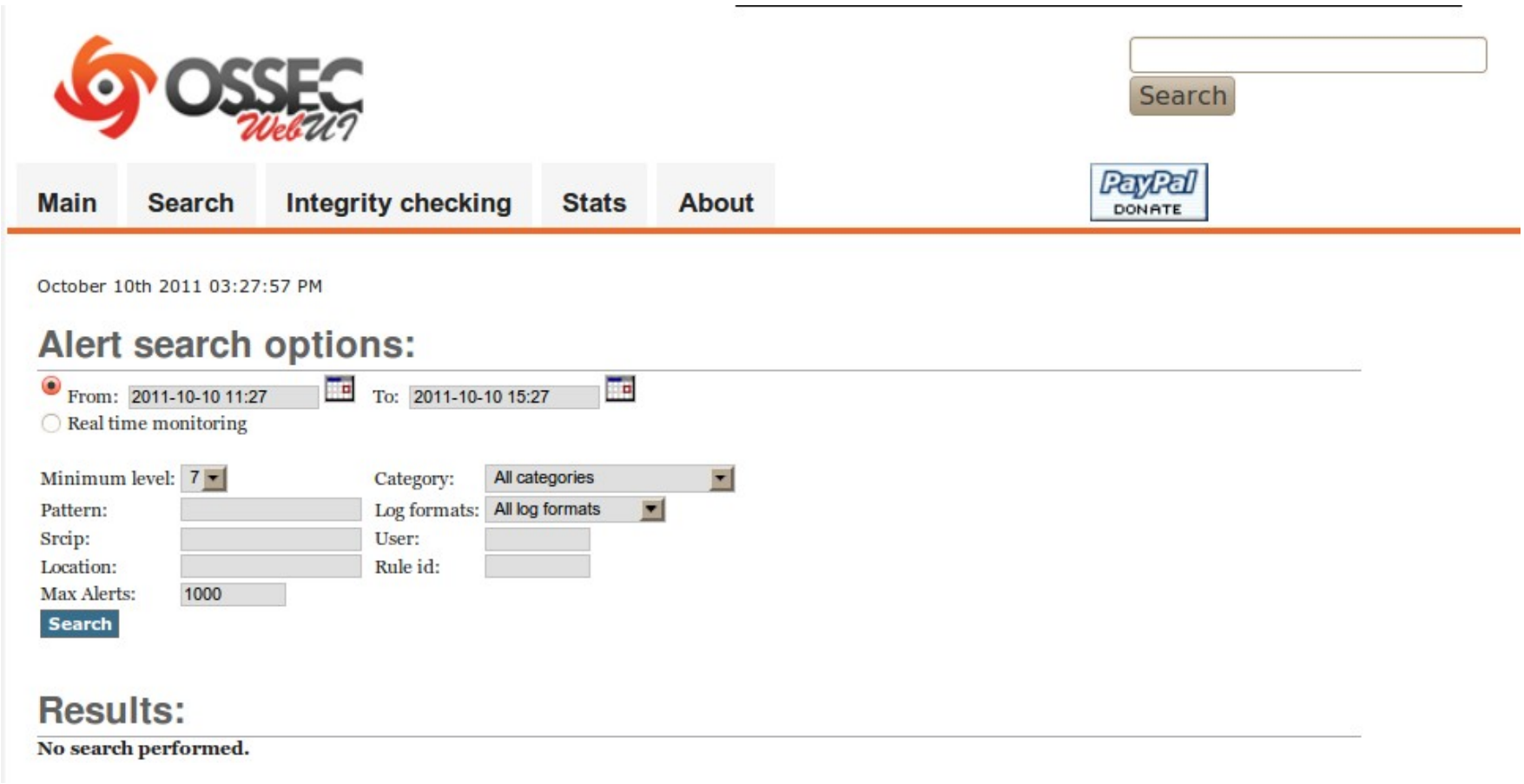
Latest events

2011 Oct 10 15:27:22 Rule Id: 5715 level: 3
Location: >/var/log/messages
Src IP:
SSHD authentication success.
Oct 10 15:27:22 sshd[21483]: Accepted keyboard-interactive/pam for from port 34500 ssh2

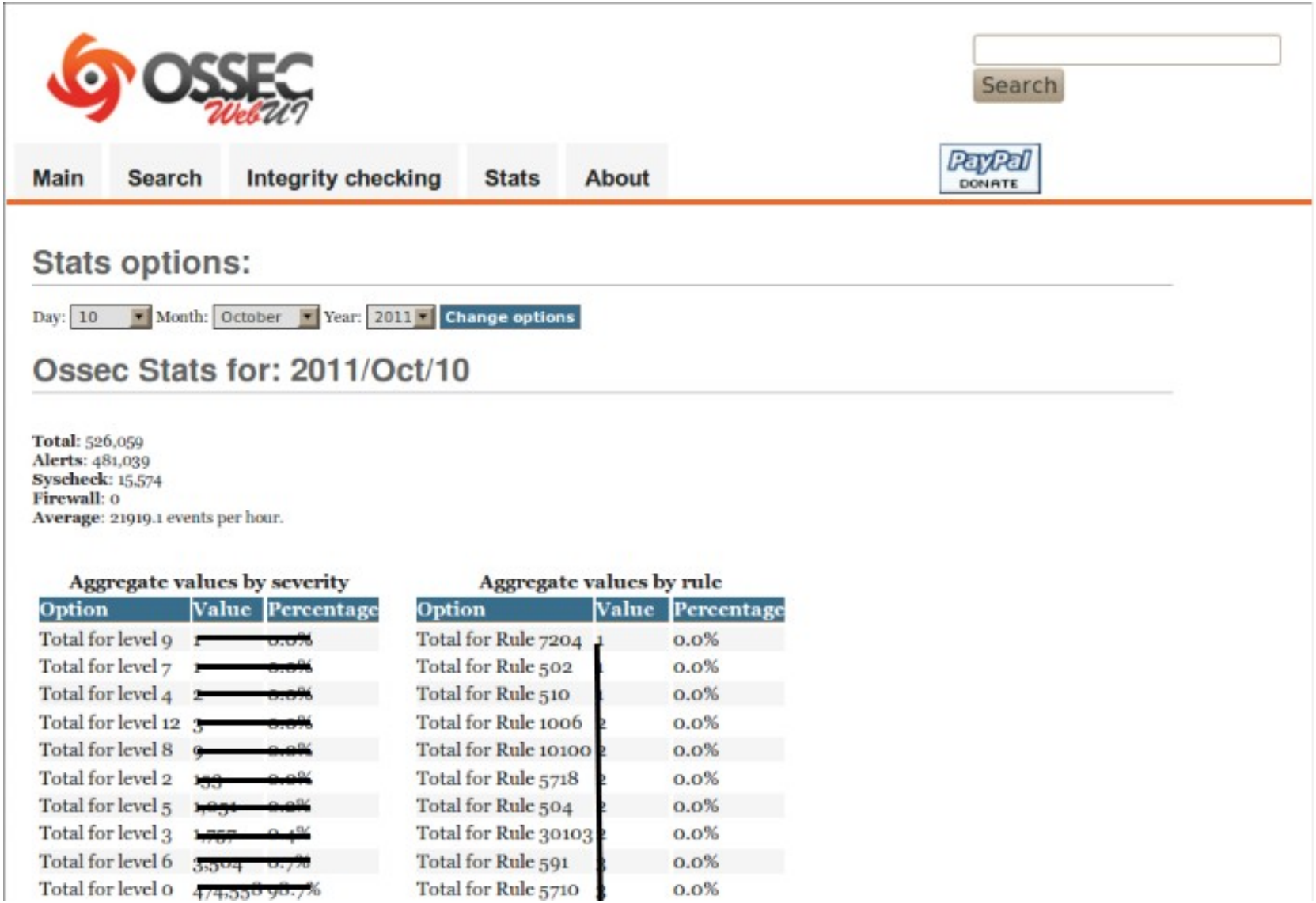
2011 Oct 10 15:27:22 Rule Id: 5706 level: 6
Location: >/var/log/messages
Src IP:
SSH insecure connection attempt (scan).
Oct 10 15:27:21 sshd[24992]: Did not receive identification string from

2011 Oct 10 15:27:19 Rule Id: 5706 level: 6
Location: ->/var/log/messages
Src IP:
SSH insecure connection attempt (scan).

OSSEC WUI


OSSEC WebUI
Search
Main
Search
Integrity checking
Stats
About
PayPal DONATE
October 10th 2011 03:27:57 PM
Alert search options:
From: 2011-10-10 11:27
To: 2011-10-10 15:27
Real time monitoring
Minimum level: 7
Category: All categories
Pattern:
Log formats: All log formats
Srcip:
User:
Location:
Rule id:
Max Alerts: 1000
Search
Results:
No search performed.

OSSEC WUI


OSSEC WebUI
Search
Main
Search
Integrity checking
Stats
About
PayPal DONATE
Stats options:
Day: 10 Month: October Year: 2011 Change options
Ossec Stats for: 2011/Oct/10
Total: 526,059
Alerts: 481,039
Syscheck: 15,574
Firewall: 0
Average: 21919.1 events per hour.
Aggregate values by severity
Option Value Percentage
Total for level 9
Total for level 7
Total for level 4
Total for level 12
Total for level 8
Total for level 2
Total for level 5
Total for level 3
Total for level 6
Total for level 0
Aggregate values by rule
Option Value Percentage
Total for Rule 7204 0.0%
Total for Rule 502 0.0%
Total for Rule 510 0.0%
Total for Rule 1006 0.0%
Total for Rule 10100 0.0%
Total for Rule 5718 0.0%
Total for Rule 504 0.0%
Total for Rule 30103 0.0%
Total for Rule 591 0.0%
Total for Rule 5710 0.0%

Inconvenientes OSSEC

- Dificultad de actualizar entre versiones
- Coordinación de las pre-shared keys puede ser problemático
- Algunas veces agentes pueden no responder
- Gran volumen de alertas
- OSSEC es bueno para alertas tempranas pero no es bueno en una situación de compromiso posterior
- Tenga mucho cuidado con la respuesta activa para evitar la auto-negación de servicio

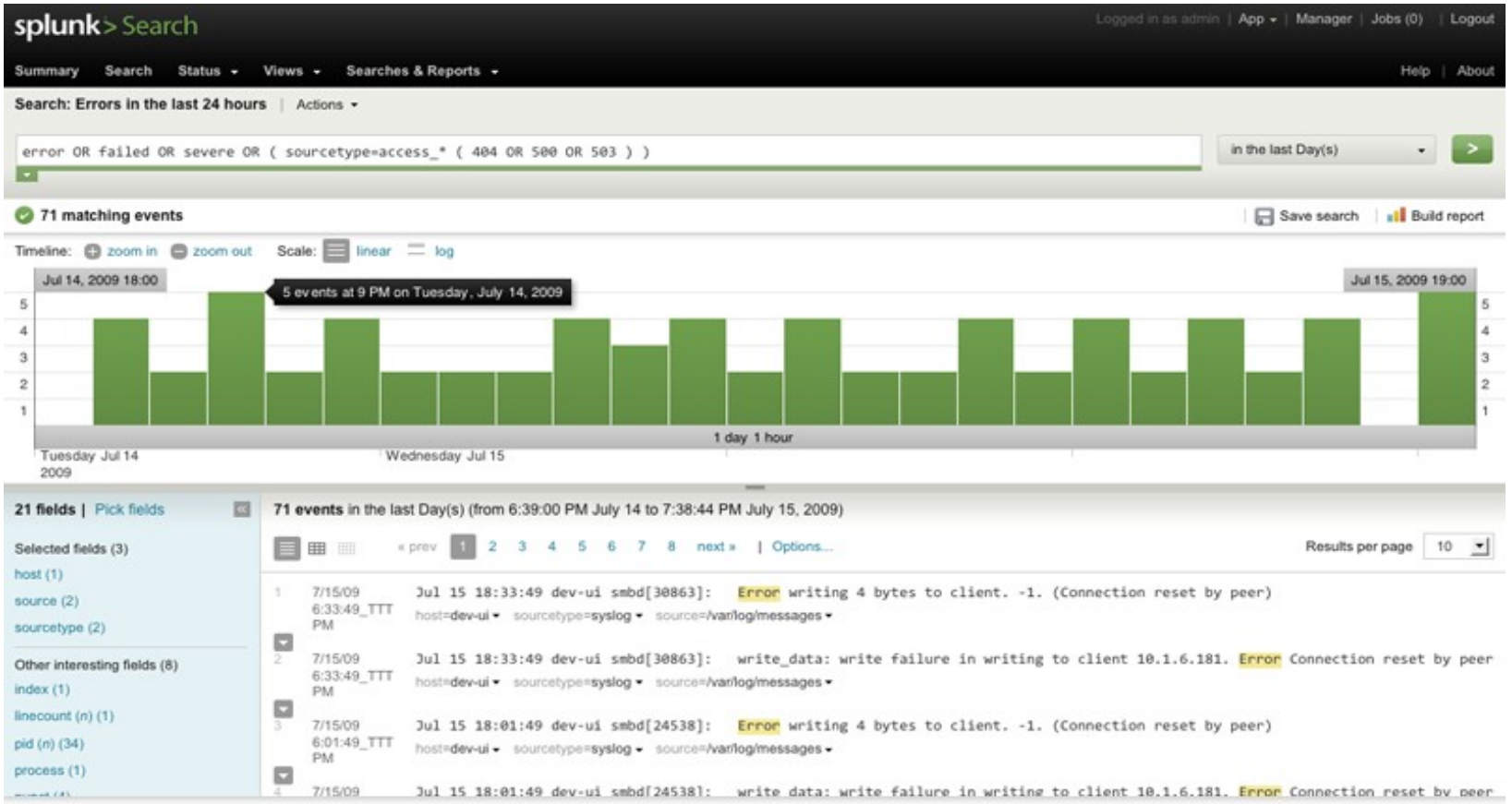
1. Sistemas de detección de intrusos (IDS)
   - NIDS
   - HIDS

2. Caso de uso mediante OSSEC
   - Introducción
   - Reglas y ejemplos
   - OSSEC WUI

3. Integración con sistemas de inteligencia operacional
   - Splunk
   - OSSEC for Splunk

3.1 Splunk

- Motor de análisis y busqueda
- Monitoriza y hace reporting
- Muchos usos fuera de la seguridad



Versiones

- Gratis
  - 500MB/día
  - Reporting
  - Ad-hoc search
- Enterprise
  - Más de 500MB/día
  - Control de acceso
  - Búsquedas distribuidas, Load Balancing
  - Monitoring & Alertas
- SO soportados
  - Windows, Linux, Solaris, OSX, FreeBSD, AIX, HP-UX

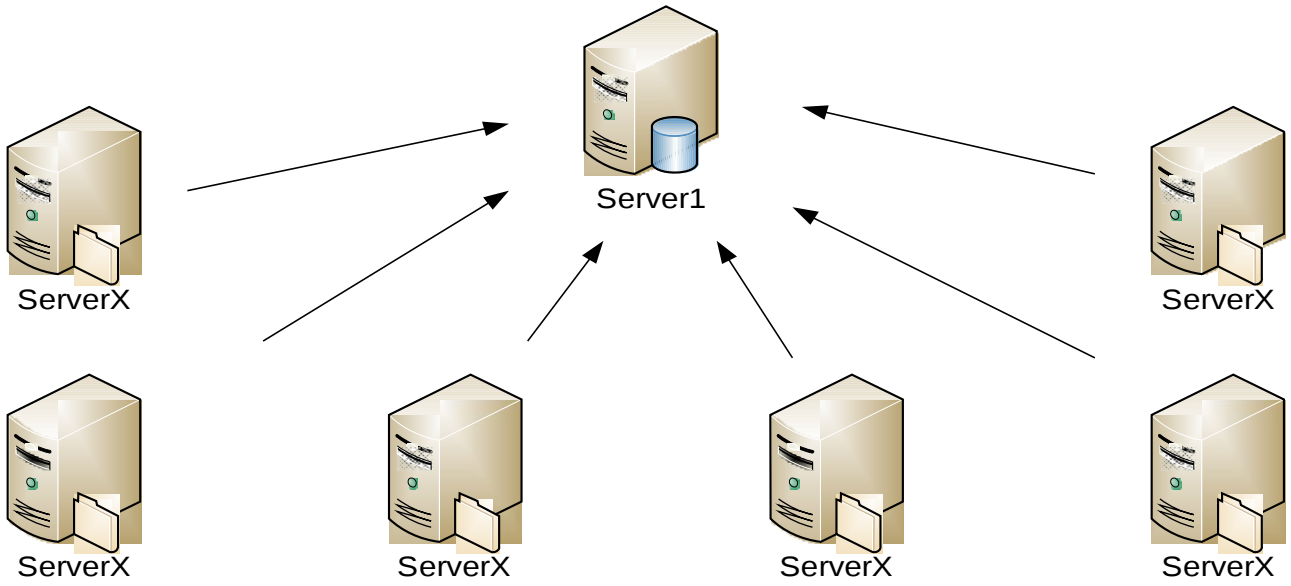
Data Sources

Splunk tiene 2 partes

- Splunkd
  - Hace el trabajo de procesamiento
  - Indexa todos los ficheros
  - Controles de accesos a la información
  - Componente básico
- SplunkWeb
  - Interfaz de usuario hacia la información

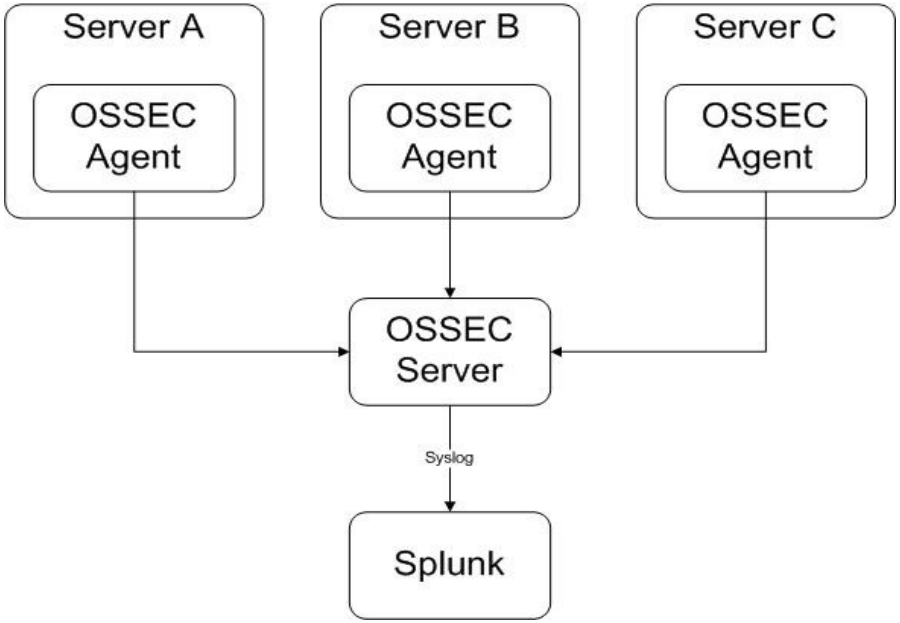
Arquitectura

- Server1
  - Splunkd y SplunkWeb
- ServerX
  - Splunkd o envía syslog 514



3.2. Splunk for OSSEC

- El package contiene parsing lógico, búsquedas guardadas y monitorización para el OSSEC
- Sistema de detección via Splunk



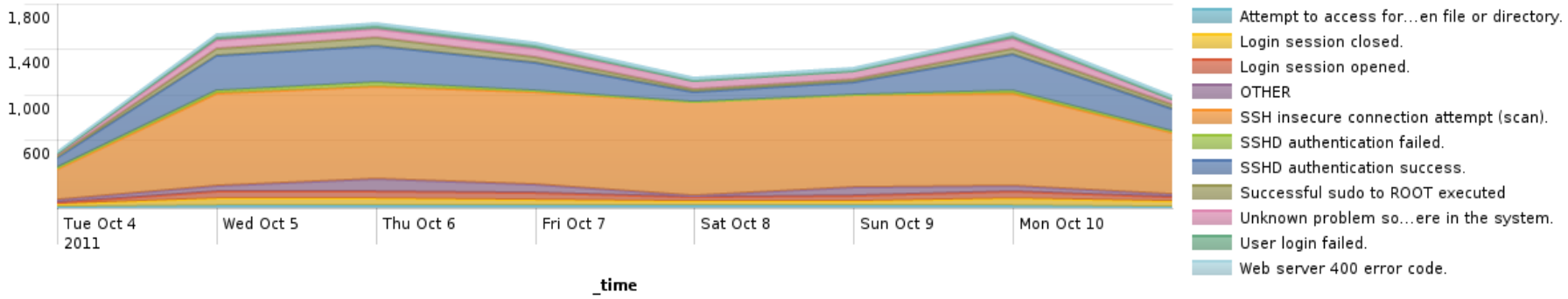
4. Splunk for OSSEC

OSSEC Dashboard (Summarized) | Actions

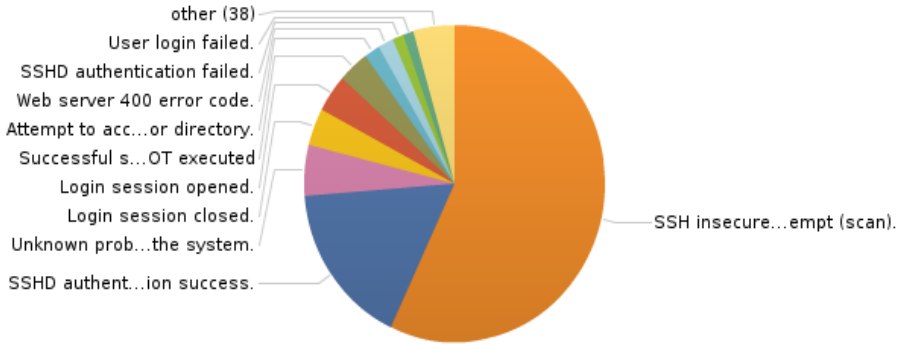
OSSEC Server: All OSSEC Servers

Hourly Summarization | Last 7 days

OSSEC - Top Signatures Over Time



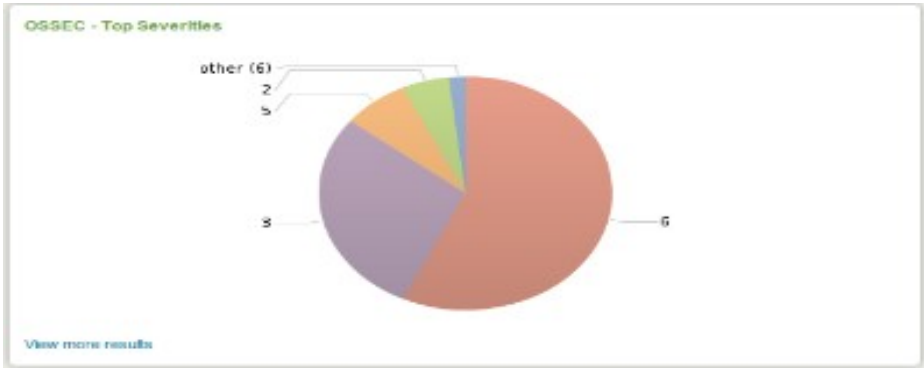
OSSEC - Top Signatures



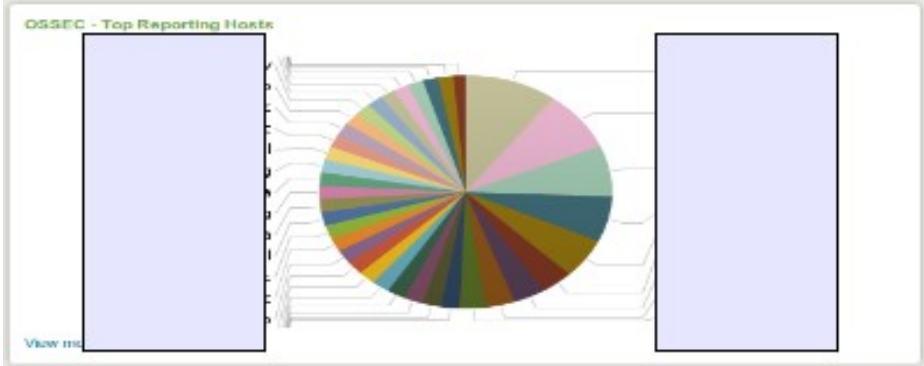
View more results

	signature	count
1	SSH insecure connection attempt (scan).	5699
2	SSHD authentication success.	1680
3	Unknown problem somewhere in the system.	518
4	Login session closed.	383
5	Login session opened.	379
6	Successful sudo to ROOT executed	336
7	Attempt to access forbidden file or directory.	168
8	Web server 400 error code.	168
9	SSHD authentication failed.	120
10	User login failed.	113

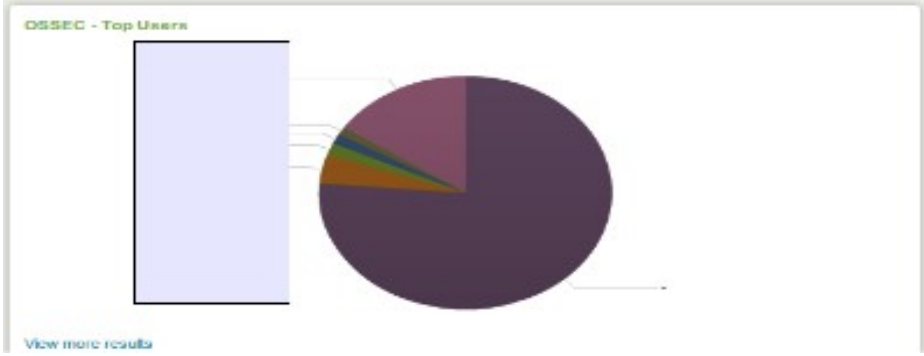
4. Splunk for OSSEC



	severity	count
1	6	5699
2	3	2867
3	5	734
4	2	519
5	12	95
6	4	31
7	10	27
8	7	25
9	8	5
10	9	4

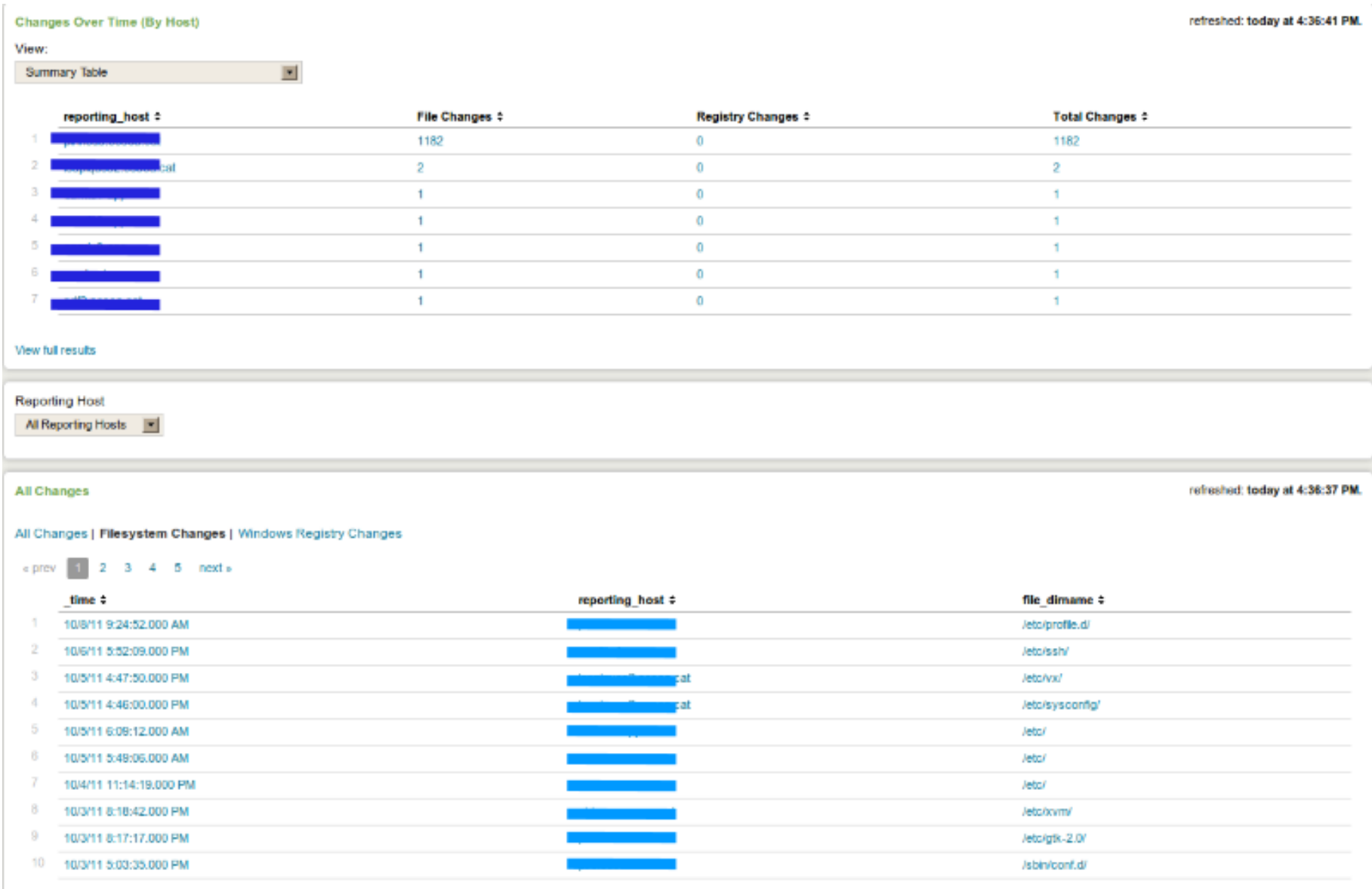


	reporting_host	count
1		1024
2		838
3		809
4		635
5		552
6		356
7		352
8		322
9		280
10		207



	user	count
1		7835
2		400
3		168
4		138
5		110
6		87
7		81
8		71
9		45
10		41

4. Splunk for OSSEC



Changes Over Time (By Host)

refreshed: today at 4:36:41 PM.

View:

Summary Table

	reporting_host	File Changes	Registry Changes	Total Changes
1	[redacted]	1182	0	1182
2	[redacted]	2	0	2
3	[redacted]	1	0	1
4	[redacted]	1	0	1
5	[redacted]	1	0	1
6	[redacted]	1	0	1
7	[redacted]	1	0	1

View full results

Reporting Host

All Reporting Hosts

All Changes

refreshed: today at 4:36:37 PM.

All Changes | **Filesystem Changes** | Windows Registry Changes

« prev 1 2 3 4 5 next »

	_time	reporting_host	file_dirname
1	10/6/11 9:24:52.000 AM	[redacted]	/etc/profile.d/
2	10/6/11 5:52:09.000 PM	[redacted]	/etc/ssh/
3	10/5/11 4:47:50.000 PM	[redacted]	/etc/vx/
4	10/5/11 4:46:00.000 PM	[redacted]	/etc/sysconfig/
5	10/5/11 6:09:12.000 AM	[redacted]	/etc/
6	10/5/11 5:49:06.000 AM	[redacted]	/etc/
7	10/4/11 11:14:19.000 PM	[redacted]	/etc/
8	10/3/11 8:18:42.000 PM	[redacted]	/etc/xvm/
9	10/3/11 8:17:17.000 PM	[redacted]	/etc/gtk-2.0/
10	10/3/11 5:03:35.000 PM	[redacted]	/sbin/conf.d/

Muchas gracias!

avaque@cesca.cat