
Worth1000.com

Inteligencia Operacional :

Del grep al cuadro de mandos

X Foro de Seguridad de RedIRIS

Jordi Guijarro Olivares

jguijarro@cesca.cat

Índice

1. Introducción
2. ENS : Marco Operacional
3. Sistemas de Inteligencia Operacional
   - ¿Busco dentro o fuera?
   - Un, dos, tres...
   - ¿Qué me aportan los flujos?
   - Escenario 1 : OSSEC como SIEM
   - Escenario 2: Splunk como gestor de Logs
   - ¿Qué nos aporta un MIX ?
4. Y más allá...

Detección, detección, detección... directivas de los grandes!

- **Using NetFlow** to support incident response by identifying zero-day malware that has bypassed typical security controls;exposing compromised machines; verifying that connections destined for areas within the enterprise network are expected in accordance with company network and security policies; evaluating firewall access control lists; and detecting covert channels and/or web-based uploads.

- **Taking an analytical approach to detecting APTs** and deploying well-understood computer security incident responses. These include the ability to produce, collect, and query logs; some form of deep packet inspection to cover key network "choke points"; the ability to quickly query network connections or flows through NetFlow or similar services; the development of trust-based, intelligence-sharing relationships with other organizations; and malware analysis.

- **Assigning IDS location variables to make alerts more "human-readable,"** so that security teams can instantly identify and escalate an incident without needing to first decipher the alert.

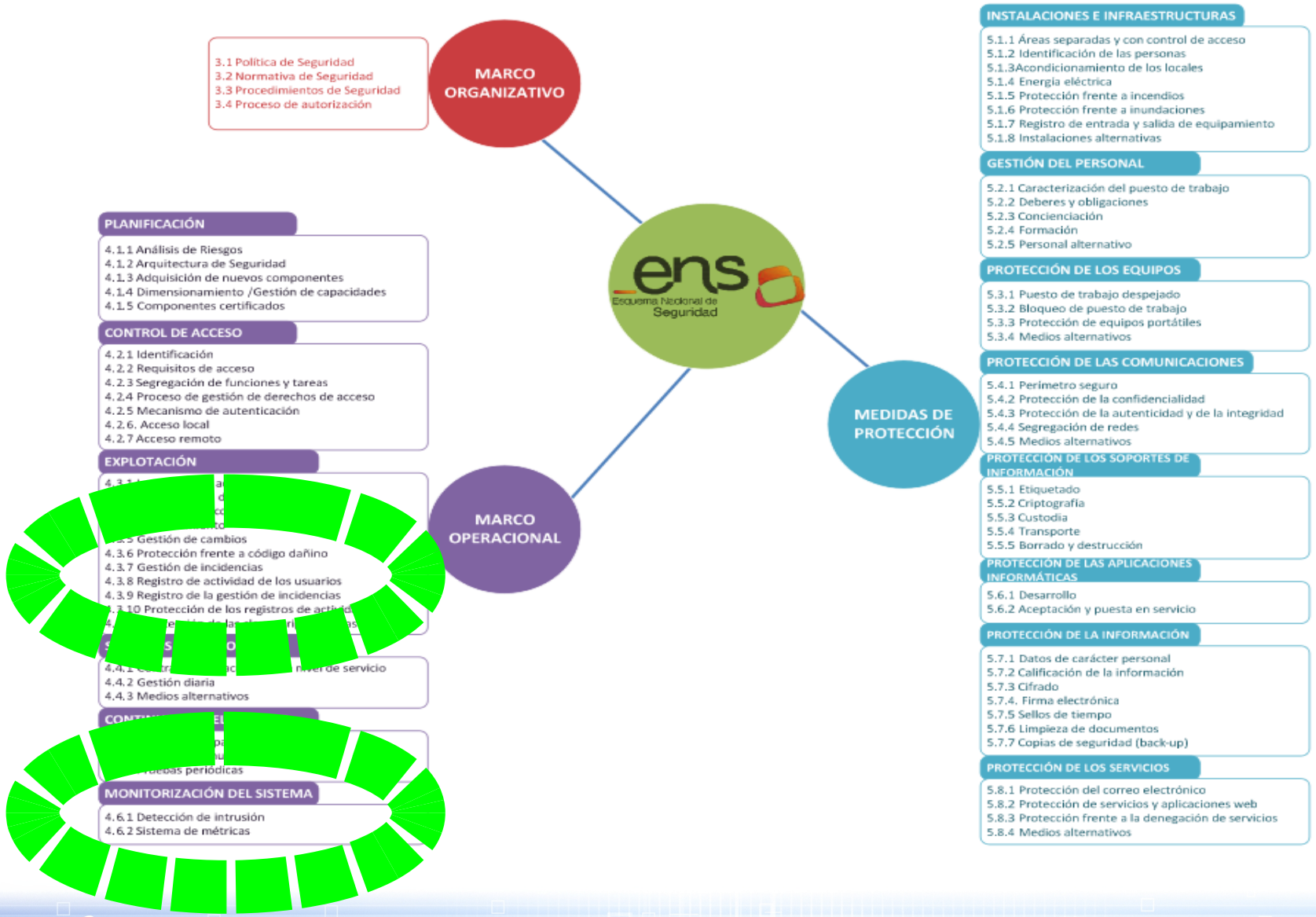
- **Baselining to detect anomalous events.** Approaches include charting infected host count per detection vector, establishing thresholds and trending, or recording the number of IP addresses found per run of each malware report and then looking for deviations from what is expected.

Detección, detección, detección...

Detección, detección, detección...

"The capacity to produce, collect, and query logs—the more the better, but at least the important ones—from a security perspective (e.g., host logs, proxies, and authentication and attribution logs)"

ENS: MARCO OPERACIONAL



4.6.1 Detección de intrusión [op.mon.1]

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

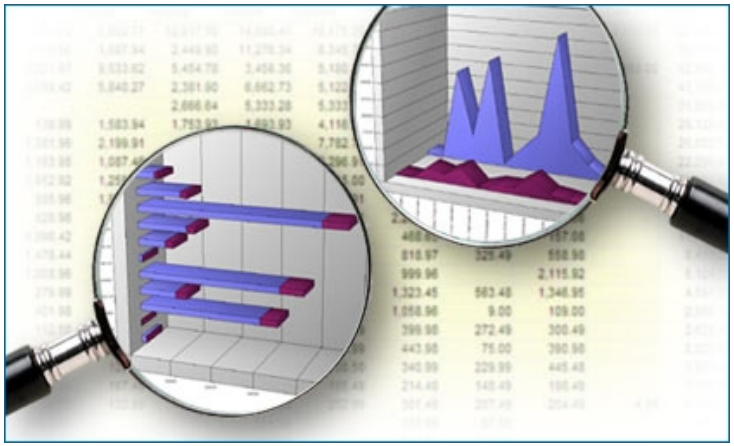
Categoría ALTA

Se dispondrán de herramientas de detección o de prevención de intrusión.

INTELIGENCIA OPERACIONAL

WIKIPEDIA
The Free Encyclopedia

Operational intelligence (OI) is a form of real-time dynamic, business analytics that delivers visibility and insight into business operations.

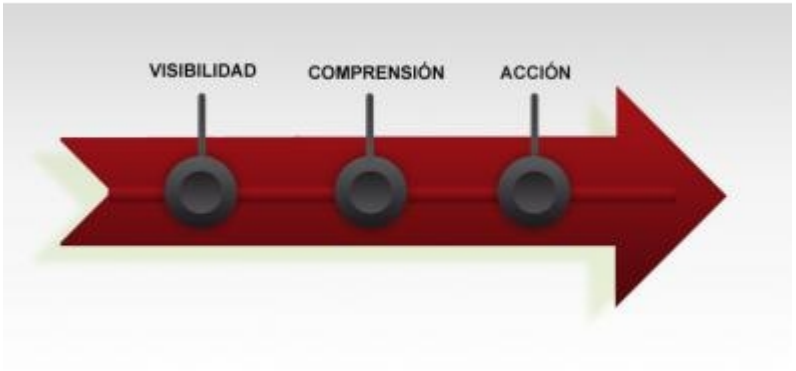


INTELIGENCIA OPERACIONAL

Operational Intellingence consta de dos naturalezas complementarias que permiten alcanzar su máxima potencia analítica:

- Métricas. La inteligencia operacional aporta indicadores y cuadros de mando de negocio vitales para la monitorización en tiempo real de las operaciones y su observación por las personas de la compañía.

- Actuación. Llega a detectar patrones complejos de comportamiento, cruzando en la analítica dimensiones dispares entre sí (tiempo, espacio, recursos, etc.) y permite lanzar acciones correctivas de manera automática, así también como acciones solicitadas por el usuario en base a una alarma o observación del cuadro de mando.

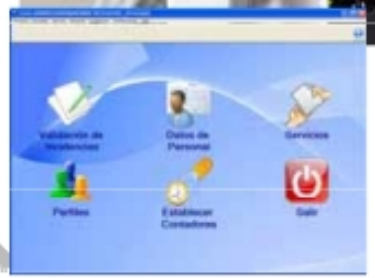


Servicios de Seguridad Informática

PROSEGUR

SEGURIDAD INFORMATICA

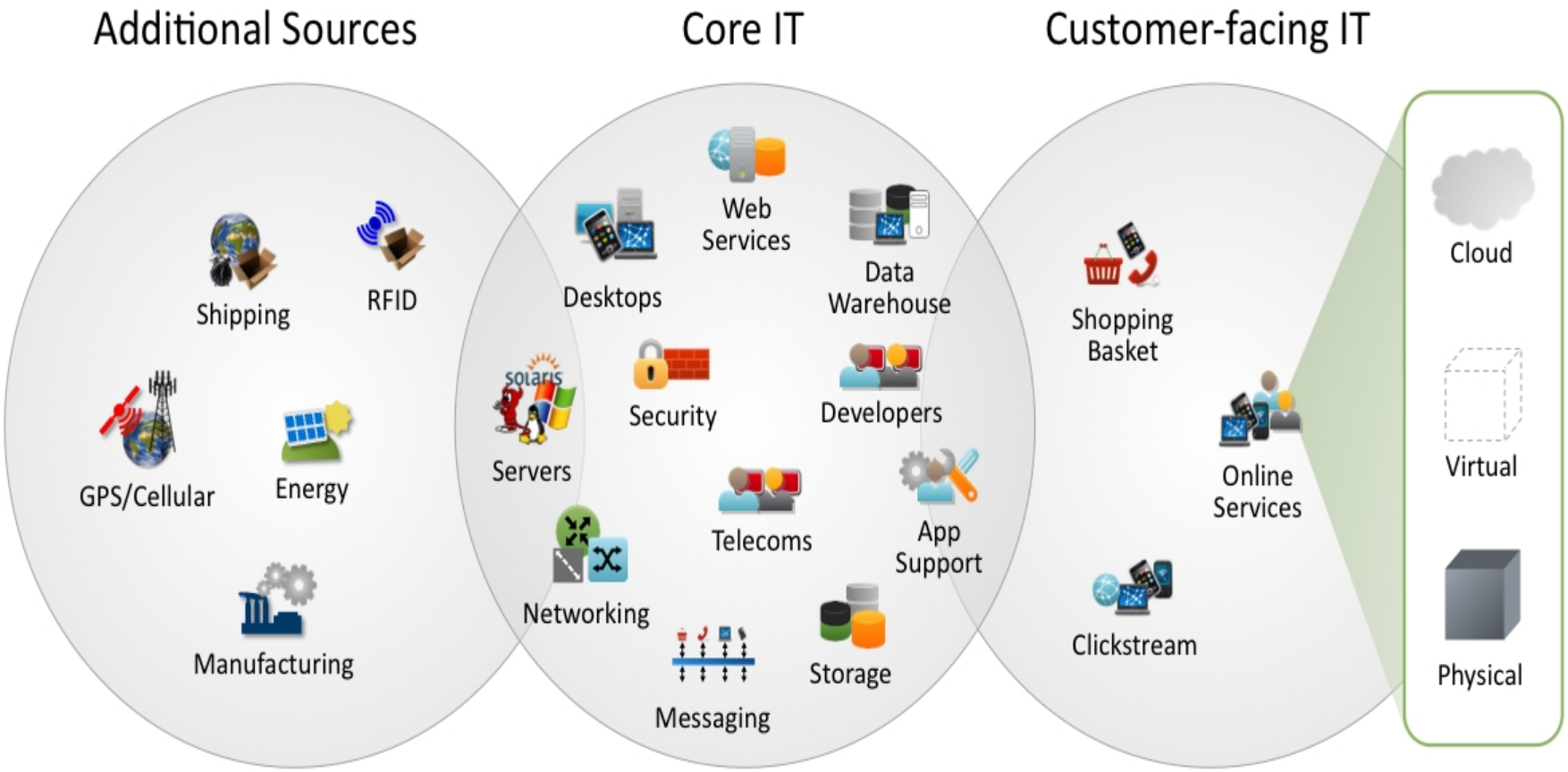
- Control de Accesos a sistemas
- Integridad de sistemas
- Control de comunicaciones



ANALISIS DE LOG Y CORRELACION DE EVENTOS

- Gestión y monitorización de presencia
- Acceso de aplicaciones y sistemas
- Predicción y detección del fraude

¿La información fluye tanto desde dentro como desde fuera?



¿La información fluye tanto desde dentro como desde fuera?

- Explosión de grandes volúmenes de datos IT, fuentes y tipos
- 80-95% de datos no estructurados
- Si se almacenan, es de manera distribuida en silos a lo largo de la organización
- Las nuevas tecnologías añaden una alta complejidad (virtualización, cloud, web 2.0, movilidad, SOA…)
- Las Tendencias de Negocio (*ej., disponibilidad 365 horas*) hacen que los datos de IT sean cada vez más valiosos

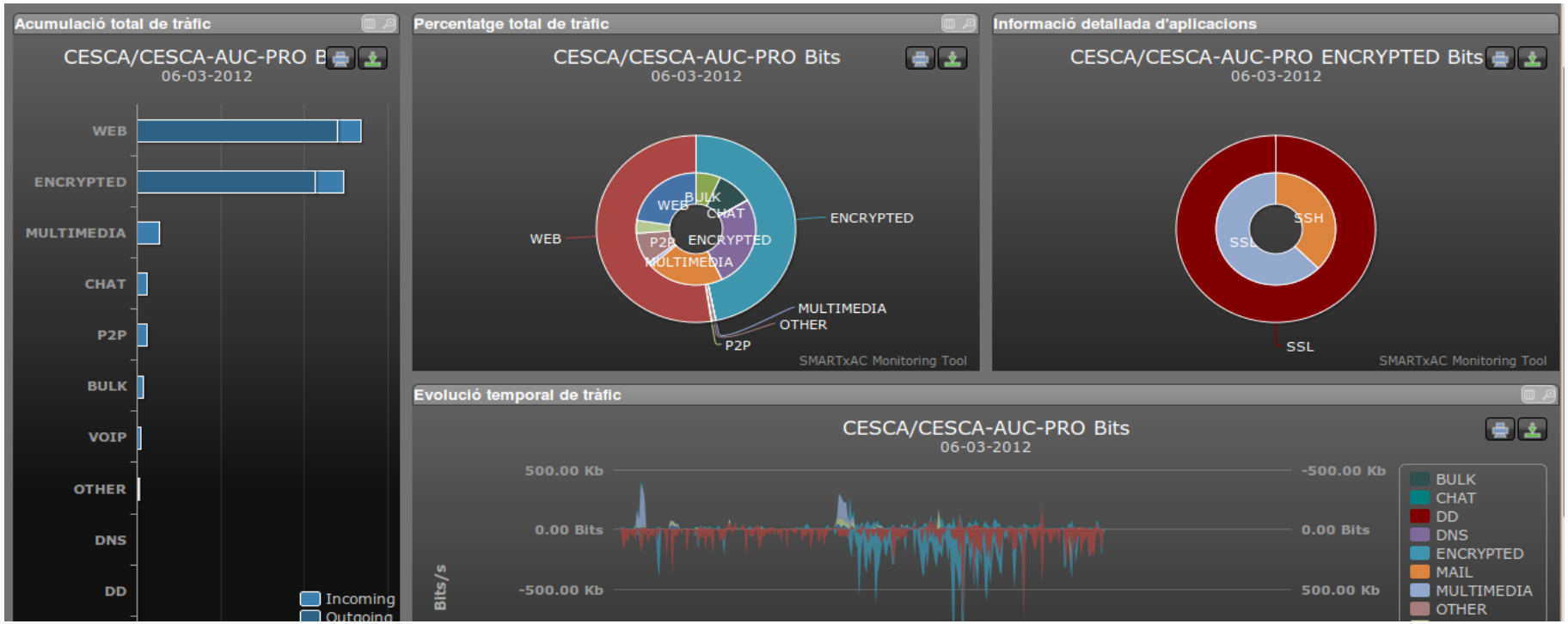
Del grep pasando por egrep y lidiando con SUPER expresiones regulares

egrep '^(0|1)+ [a-zA-Z]+$' syslog.*

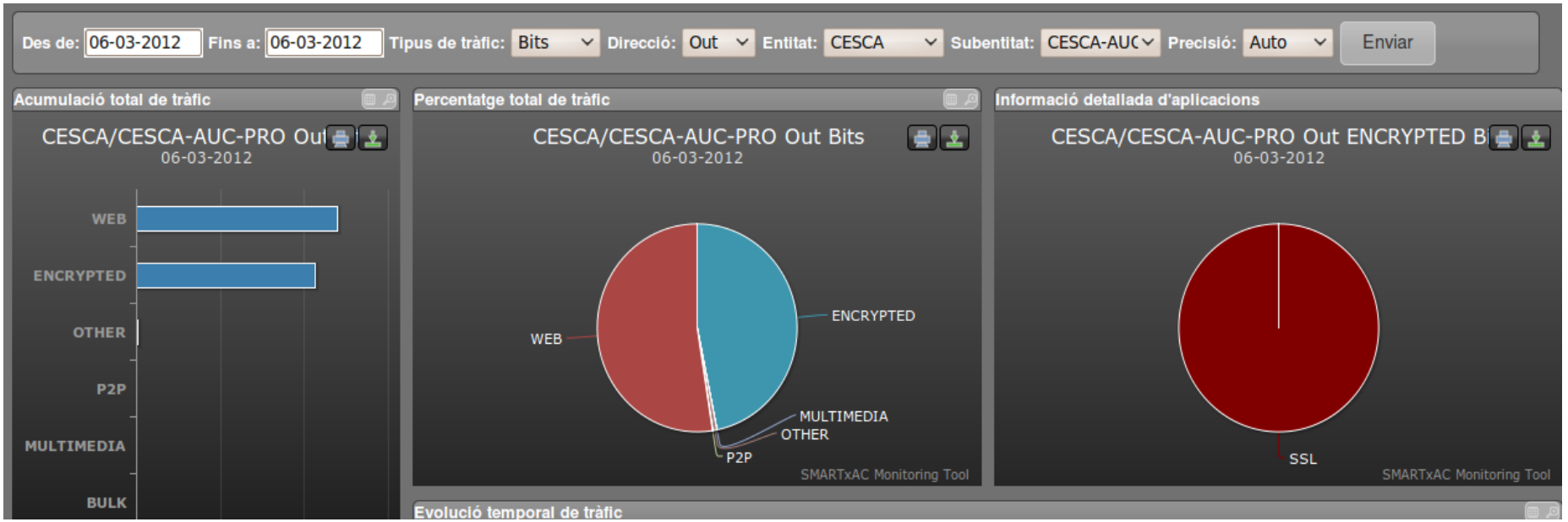
```
(?:(?:\r\n)?[ \t])*(?:(?:(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:\r\n)?[ \t]
)+|\Z|(?=[\["()<>@,;:\\".\[\]]))|"(?:[^\"\r\\]|\\.|(?:(?:\r\n)?[ \t]))*"(?:(?:
\r\n)?[ \t])*)(?:\.(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(
?:\r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|"(?:[^\"\r\\]|\\.|(?:(?:\r\n)?[
\t]))*"(?:(?:\r\n)?[ \t])*))*@(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\0
31]+(?:(?:(?:\r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\
](?:(?:\r\n)?[ \t])*)(?:\.(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031]+
(?:(?:(?:\r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\](?:
(?:\r\n)?[ \t])*))*|(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:\r\n)?[ \t])+|\Z
|(?=[\["()<>@,;:\\".\[\]]))|"(?:[^\"\r\\]|\\.|(?:(?:\r\n)?[ \t]))*"(?:(?:\r\n)
?[ \t])*)*\<(?:(?:\r\n)?[ \t])*(?:@(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:\
r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\](?:(?:\r\n)?[
 \t])*)(?:\.(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:\r\n)
?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\](?:(?:\r\n)?[ \t]
)*))*(?:,@(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:\r\n)?[
 \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\](?:(?:\r\n)?[ \t])*
)(?:\.(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:\r\n)?[ \t]
)+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\](?:(?:\r\n)?[ \t])*))*)
*:(?:(?:\r\n)?[ \t])*)?(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:\r\n)?[ \t])+
|\Z|(?=[\["()<>@,;:\\".\[\]]))|"(?:[^\"\r\\]|\\.|(?:(?:\r\n)?[ \t]))*"(?:(?:\r
\n)?[ \t])*)(?:\.(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?:(?:
\r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|"(?:[^\"\r\\]|\\.|(?:(?:\r\n)?[ \t
]))*"(?:(?:\r\n)?[ \t])*))*@(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031
]+(?:(?:(?:\r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\](
?:(?:\r\n)?[ \t])*)(?:\.(?:(?:\r\n)?[ \t])*(?:[^()<>@,;:\\".\[\] \000-\031]+(?
:(?:(?:\r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|\[([^\[\]\r\\]|\\.)*\](?:(?
:\r\n)?[ \t])*))*\>(?:(?:\r\n)?[ \t])*)|(?:[^()<>@,;:\\".\[\] \000-\031]+(?:(?
:(?:\r\n)?[ \t])+|\Z|(?=[\["()<>@,;:\\".\[\]]))|"(?:[^\"\r\\]|\\.|(?:(?:\r\n)?
[ \t]))*"(?:(?:\r\n)?[ \t])*)*:(?:(?:\r\n)?[ \t])*(?:(?:(?:[^()<>@,;:\\".\[\]
...
```

Mail::RFC822::Address-0.4

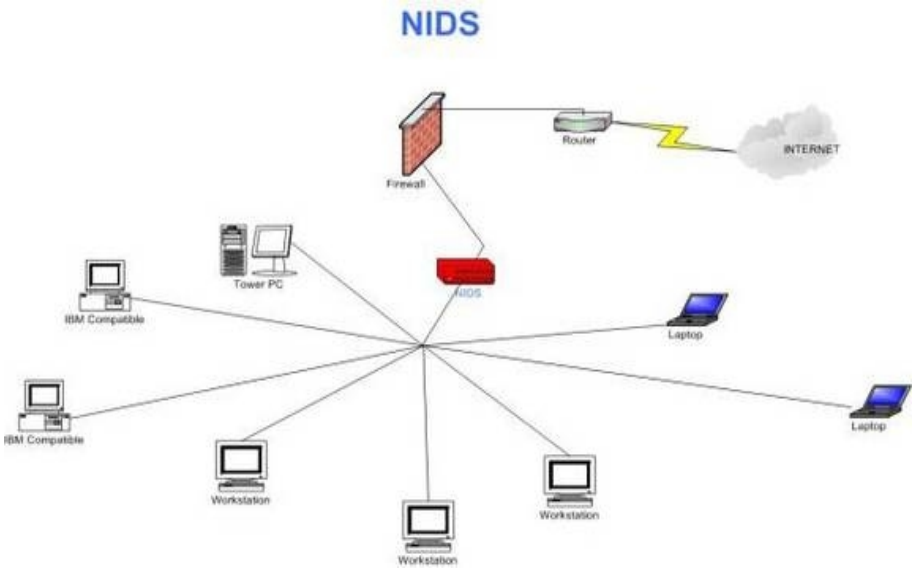
¿Qué me aportan los flujos?

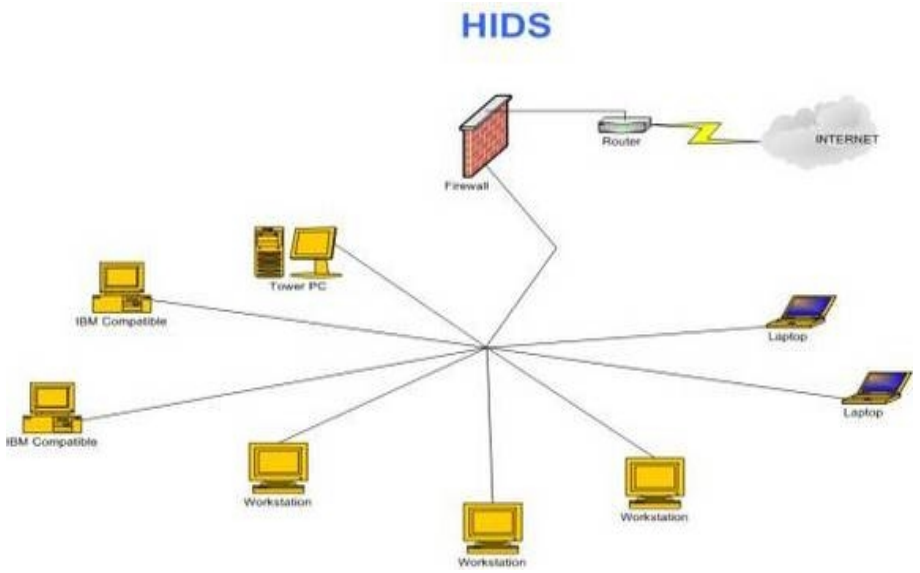


¿Qué me aportan los flujos?



Sistemas de detección de Intrusos : En busca del SIEM





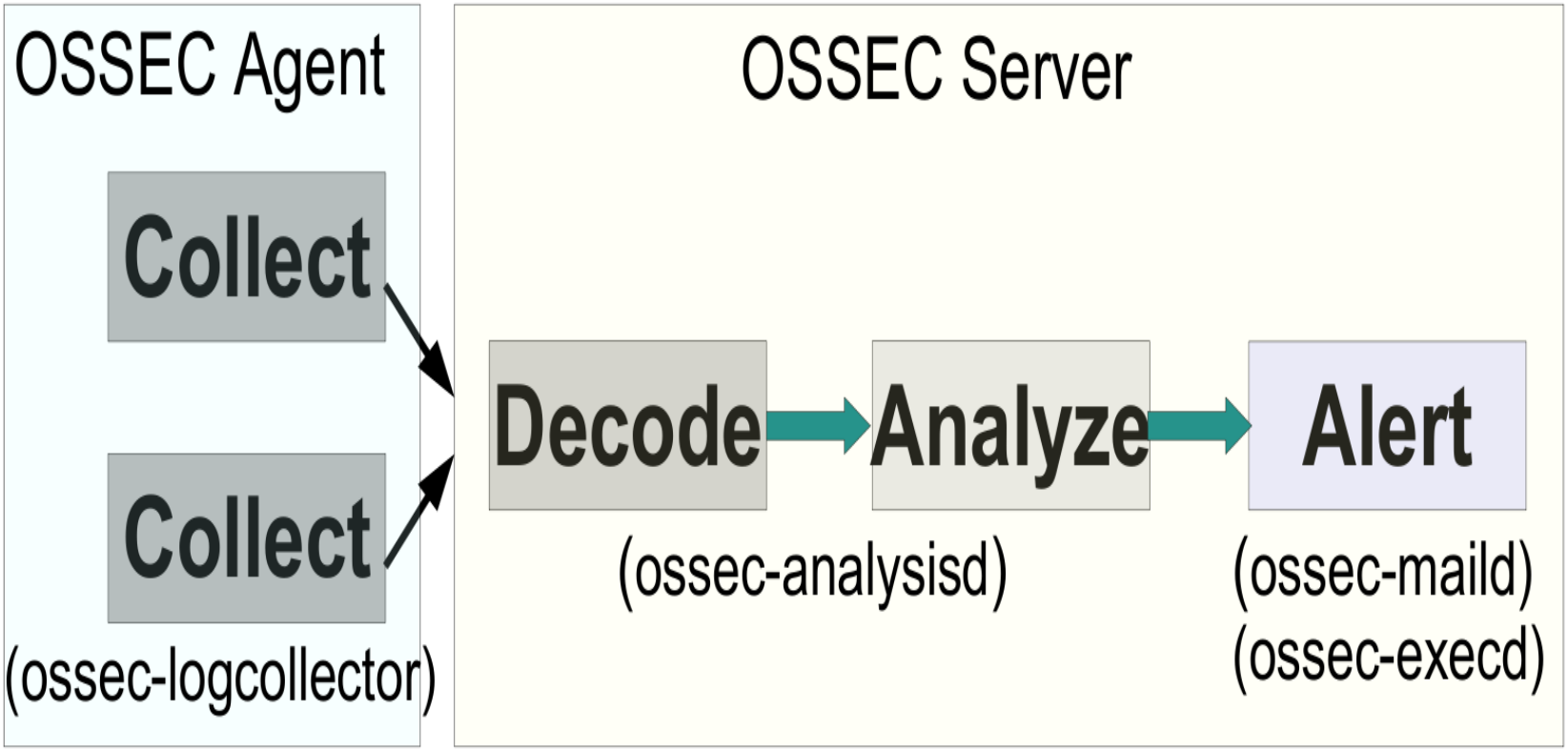
Los HIDS's como complemento estratégico

- Fácil implementación
- Pocos requisitos de Hardware i “pocos” falsos positivos
- Alta visibilidad
- Visibilidad en la actividad del sistema (kernel, comportamiento de usuarios, etc.)
- Requieren centralización y agentes en los clientes
- Basados en el tratamiento de logs / correlación.
- Complemento claro de la detección a nivel de red.

¿Qué nos ofrece OSSEC?

- Revisión de la **Integridad a nivel de ficheros**
- Detección **de problemas** a nivel de HOST (detección de rootkits)
- Alertas en **tiempo real y capacidad de respuesta Activa**
- Análisis y correlación de Logs (Multitud de logs soportados)
- ...

Tratamiento de la información



La Configuración por defecto incluye alertas del tipo:

- Web attacks
- SSH brute force
- Buffer overflows and program crashes
- Firewall events
- Users using sudo
- Y 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 II

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

Ejemplo de Alertas III

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 de Alertas IV

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 V

OSSEC HIDS Notification.

2010 Aug 04 12:10:08

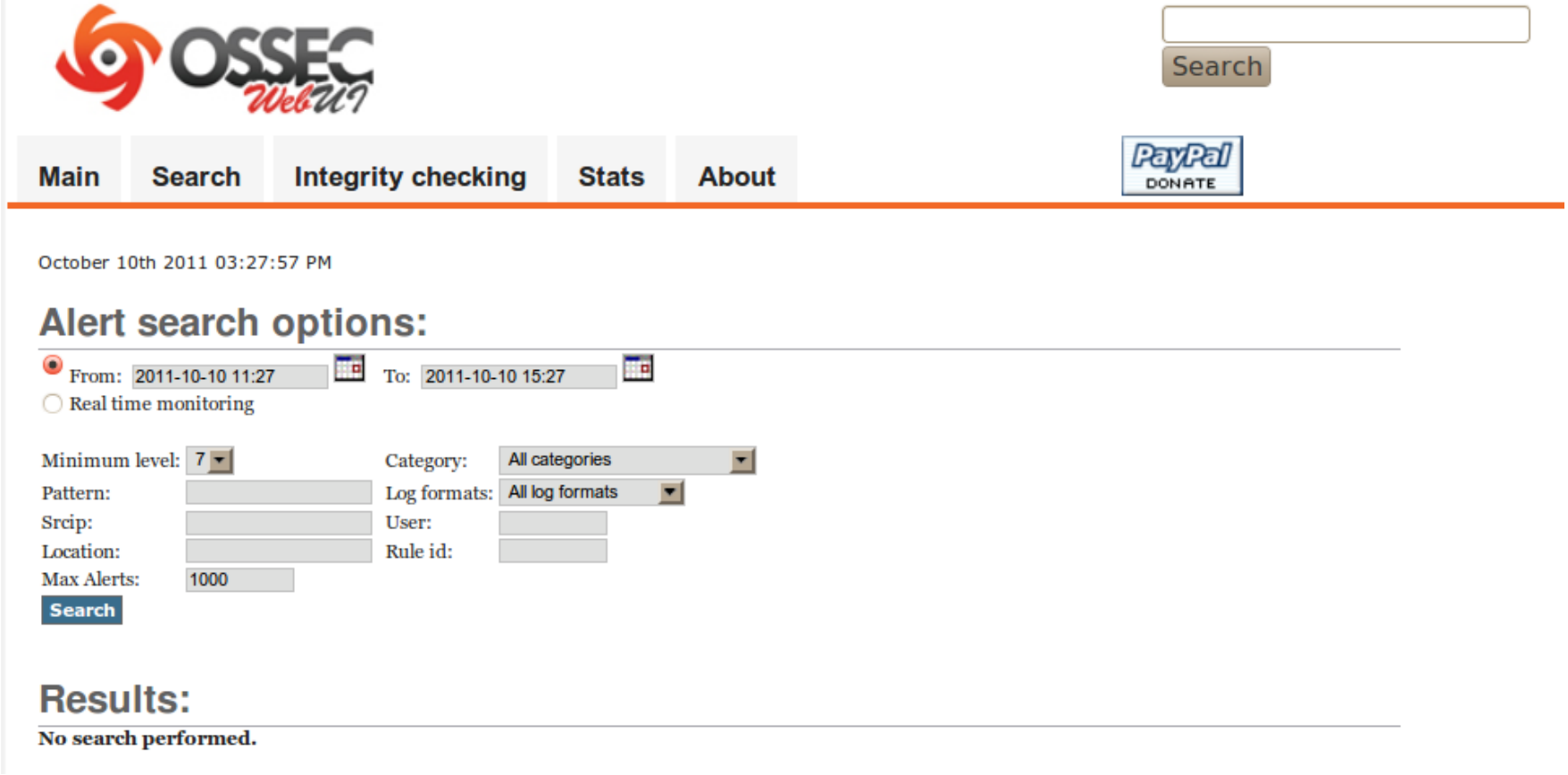
Received From: webdev->/var/log/httpd/access_log

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"

Interfaz Web - OSSEC



- ✓ ¿Qué és Splunk?
  - Un software que permite monitorizar, analizar y generar informes a partir de logs generados por las aplicaciones, sistemas,...
- ✓ ¿Qué permite hacer que no haga un gestor de logs convencional?
  - Permite que los usuarios hagan búsquedas, que puedan analizar en tiempo real la información de manera sencilla y ágil.
  - Identificar patrones, proporcionar métricas, diagnosticar problemas i en general proporcionar capacidad de decisión (*bussiness intelligence*)
- ✓ Origen del nombre “Splunk” (Fuente: Wikipedia)
  - “Splunk is a reference to exploring caves, as in spelunking”

‘Masticar y Digerir’

Recolecta, indexa y digiere los datos generados por

nuestra infraestructura IT, de cara a identificar problemas, riesgos y oportunidades, permitiendo

dirigir de la mejor manera las decisiones de IT y de

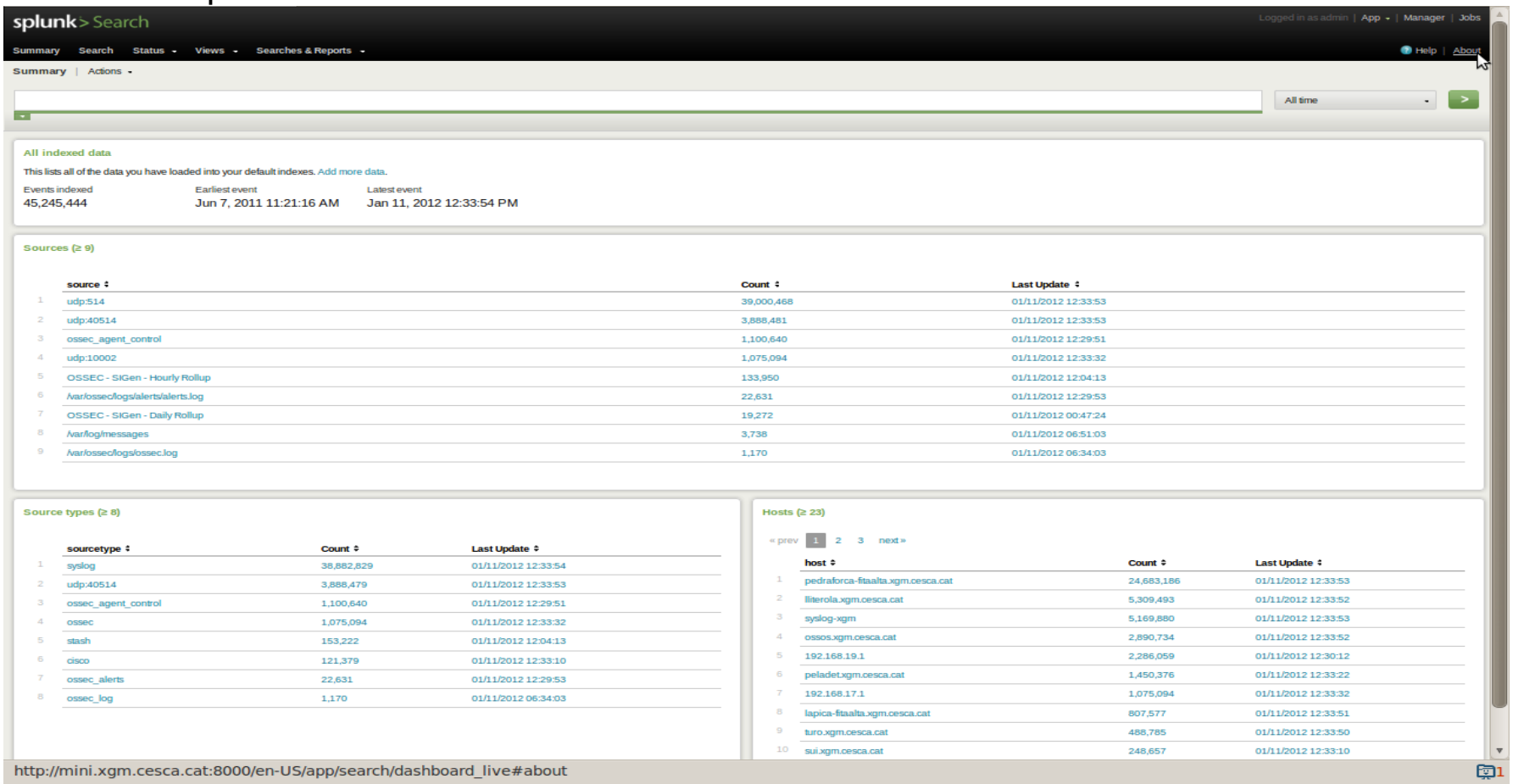
negocio...

Datos indexados....

Fuentes de información

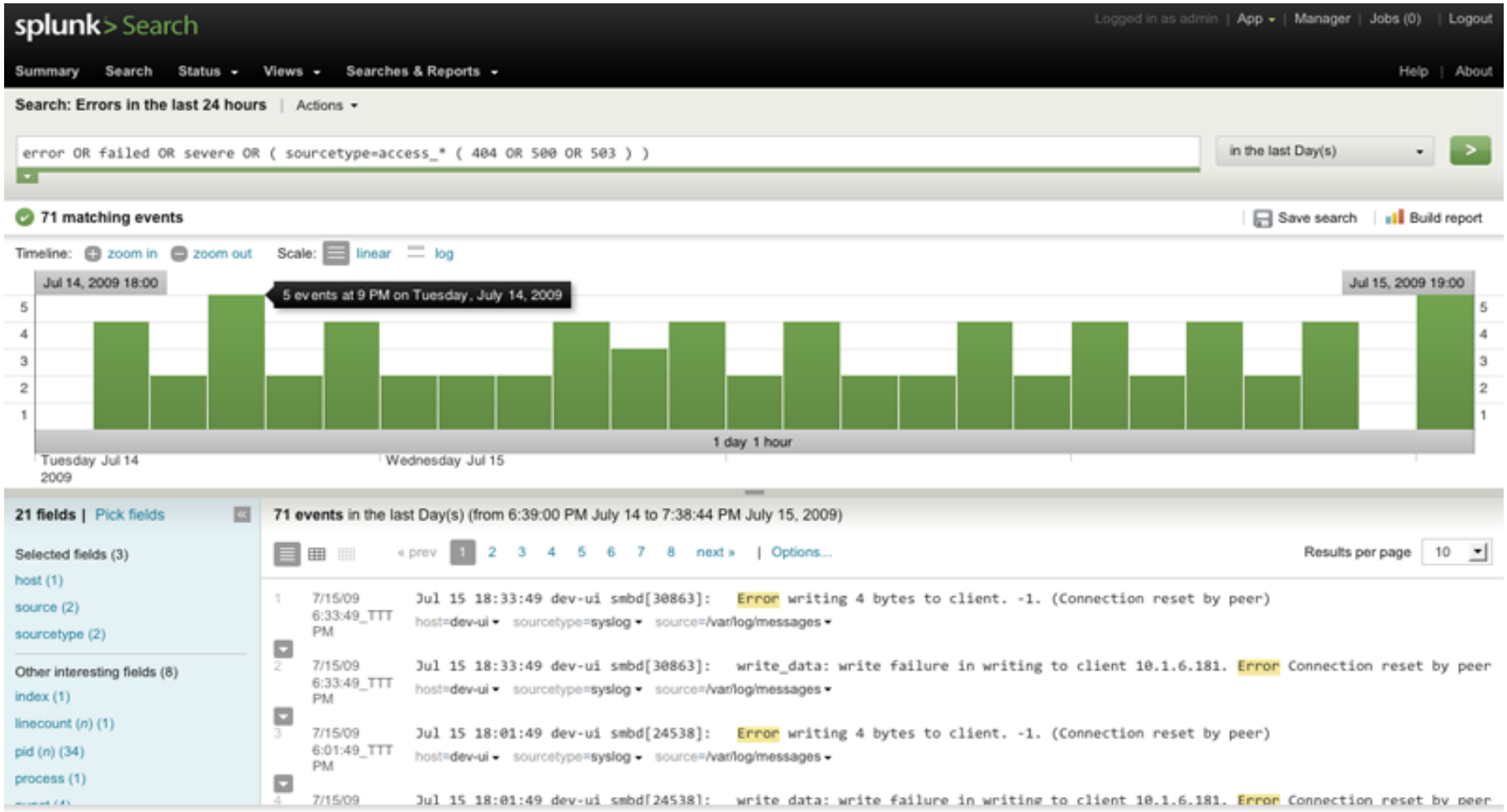
Interfaz Web I

- ✓ Acceso a la aplicación principal
  - Resumen de la información indexada
  - Sources, Hosts, Source Types
  - Búsqueda



Interfaz Web II (Pantalla de Búsqueda)

- ✓ Búsqueda basada en
  - Palabras clave
  - Expresiones regulares



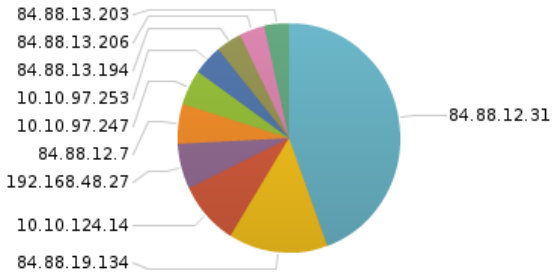
Ejemplos

- ✓ Búsqueda de comandos introducidos por el usuario
  - sourcetype="syslog" command | rex "User:(?<USUARI>[\S]*)" | rex "command:(?<COMANDA>[^\$]*)" | rex "\s[\d]*:\s(?<SEQUENCIA>[\d]*)“
- ✓ Cambio de estado de una interfaz [conectada/no conectada]
  - sourcetype="syslog" changed state to | rex "Interface\s(?<INTERFACE>(?<media>[^\d]+)(?<slot>\d+)\/(?<port>\d+))\,\schanged\sstate\sto\s(?<PORT_STATUS>up|down)”
- ✓ Usuarios que fallan más la introducción de contraseñas...
  - "failed password" src_ip=192.168.1* | top user
- ✓ Clasificación de los usuarios anteriores por máquina i número de errores
  - "failed password" src_ip=192.168.1* | stats count by user,reporting_ip | sort count desc

Paneles de Control en tiempo real

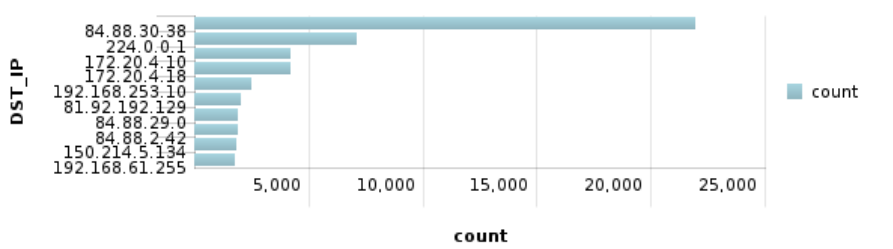
XAVI-PROVA | Actions

TOP10_SRCIP_Filtrades_24h — refreshed: today at 4:04:07 PM.



View results

TOP10_DSTIP_Filtrades_24h — refreshed: today at 4:04:08 PM.



View results

PortFlapping — refreshed: today at 4:04:08 PM.

	interface	host	port_status	count
1	GigabitEthernet0/15		down	28
2	GigabitEthernet0/15		up	28
3	GigabitEthernet0/15		down	6
4	GigabitEthernet0/15		up	6
5	GigabitEthernet0/11		up	1
6	GigabitEthernet0/16		down	1
7	GigabitEthernet0/16		up	1
8	GigabitEthernet0/6		down	1
9	GigabitEthernet0/6		up	1

View results

CaigudesBGP — refreshed: today at 4:04:08 PM.

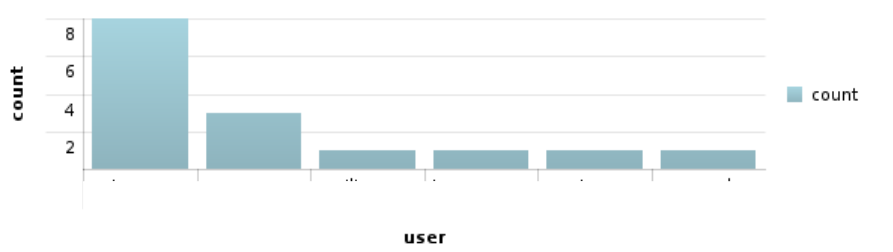
	_time	host	index	linecount	ossec_server	source	sourcetype
1	1/12/12 7:30:12.000 AM		main	1		udp:514	syslog
2	1/12/12 7:29:44.000 AM		main	1		udp:514	syslog
3	1/12/12 7:23:02.000 AM		main	1		udp:514	syslog
4	1/12/12 7:22:32.000 AM		main	1		udp:514	syslog
5	1/11/12 11:06:40.000 PM		main	1		udp:514	syslog
6	1/11/12 11:06:35.000 PM		main	1		udp:514	syslog
7	1/11/12 11:06:29.000 PM		main	1		udp:514	syslog
8	1/11/12 11:06:19.000 PM		main	1		udp:514	syslog
9	1/11/12 11:01:18.000 AM		main	1		udp:514	syslog
10	1/11/12 11:00:26.000 AM		main	1		udp:514	syslog

View results

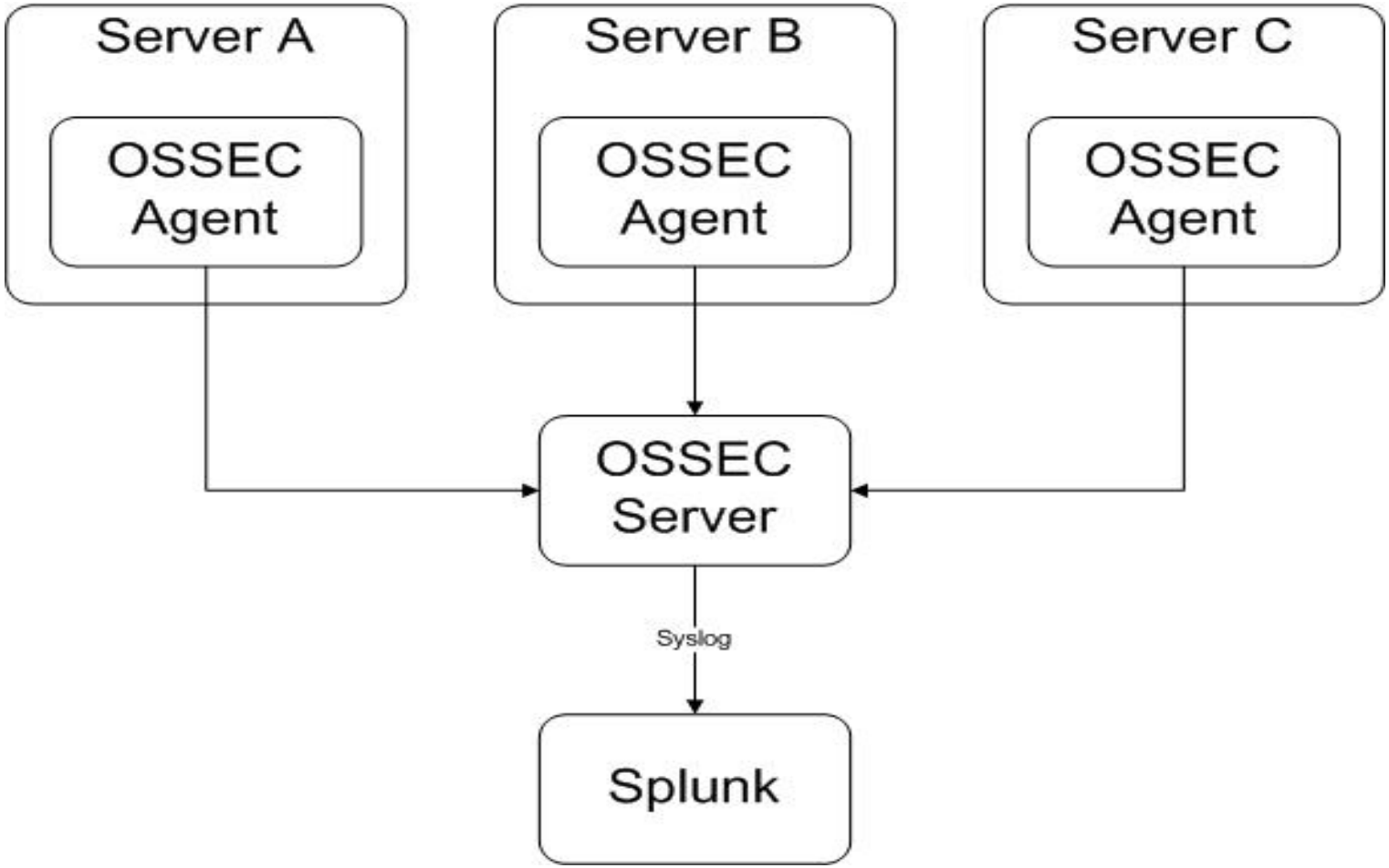
ComandesIntroduides — refreshed: today at 4:04:07 PM.

	_time	host	index	linecount	ossec_server	source	sourcetype	splunk_server
1	1/12/12 4:07:59.000 PM		main	1		udp:514	syslog	syslog-xgm
2	1/12/12 2:01:31.000 PM		main	1		udp:514	syslog	syslog-xgm
3	1/12/12 1:30:12.000 PM		main	1		udp:514	syslog	syslog-xgm
4	1/12/12 1:22:30.000 PM		main	1		udp:514	syslog	syslog-xgm
5	1/12/12 12:26:16.000 PM		main	1		udp:514	syslog	syslog-xgm
6	1/12/12 11:51:18.000 AM		main	1		udp:514	syslog	syslog-xgm
7	1/12/12 10:56:06.000 AM		main	1		udp:514	syslog	syslog-xgm
8	1/12/12 10:56:02.000 AM		main	1		udp:514	syslog	syslog-xgm

Fallades_Password_Ultimes_24h — refreshed: today at 4:04:08 PM.



Y si hacemos un MIX!



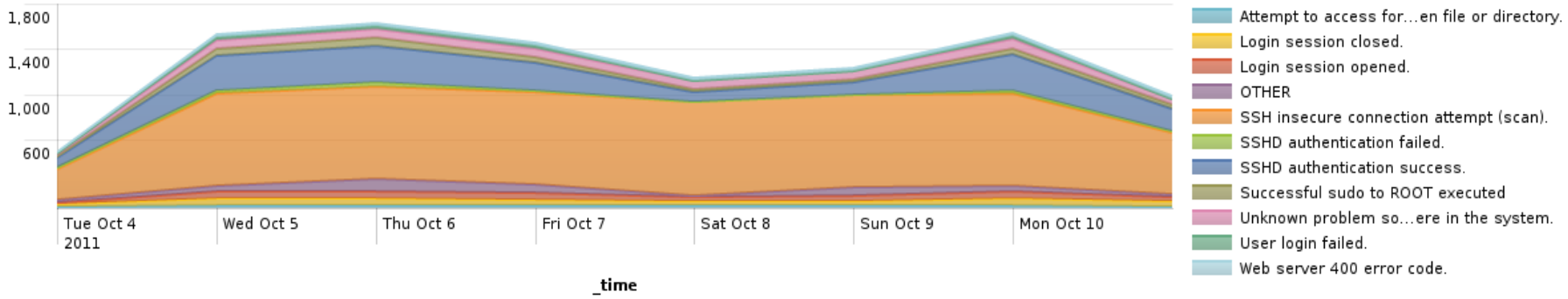
Splunk for OSSEC

OSSEC Dashboard (Summarized) | Actions

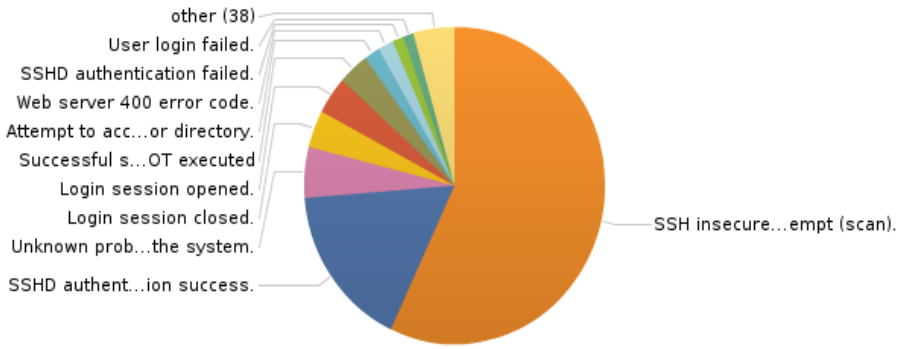
OSSEC Server: All OSSEC Servers

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

¿ Únicamente para temas de Seguridad ?