GARR

The Italian Academic & Research Network

www.garr.it

INFN Istituto Nazionale di Fisica Nucleare

Borsa di Studio Orio Carlini

Gestione di una rete locale complessa di un centro di calcolo di grandi dimensioni (in particolare del TIER1 italiano per LHC) con particolare attenzione agli aspetti di monitoring, analisi di flusso ed analisi dei log

Germano Giotta

Borsisti Day, Roma, 16.12.2012

Picchi di attività o di utilizzo delle risorse

- Come trovo la causa?
  - Correlazione
  - Come posso correlarli?

- Come e chi tiene traccia delle possibili cause e condizioni che l'hanno generato?

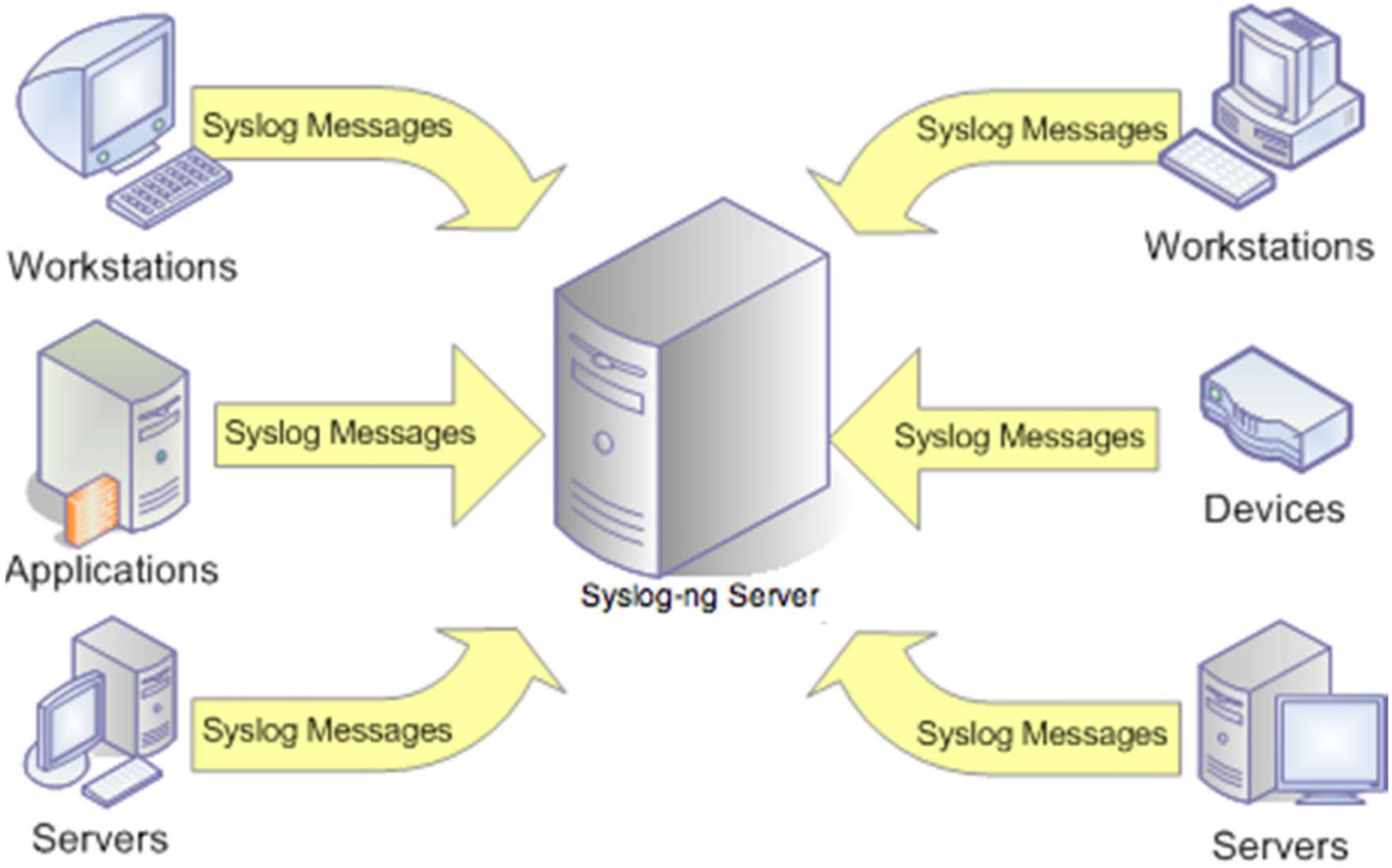
Obiettivi

- Obiettivo 1 : *“Analisi Post-Evento”* scovare le cause
- Obiettivo 2 : “Rilevare Anomalie in Real-Time”
- Obiettivo 3 :”Predisporre delle contromisure” per evitare il ripetersi del problema

Alcune Osservazioni sull'uso dei LOG

- Già previsti e disponibili secondo specifiche disposizioni di legge
  - *D.Lgs 196/03, D.L. 27Lugio 2005,Provvedimenti a carattere generale del garante della privacy 2008*
- Problema di visualizzazione
  - Accesso, ricerca, formulazione dei pattern
- Problema correlazione
- Un'Analisi tardiva spesso è inutile

Syslog-ng

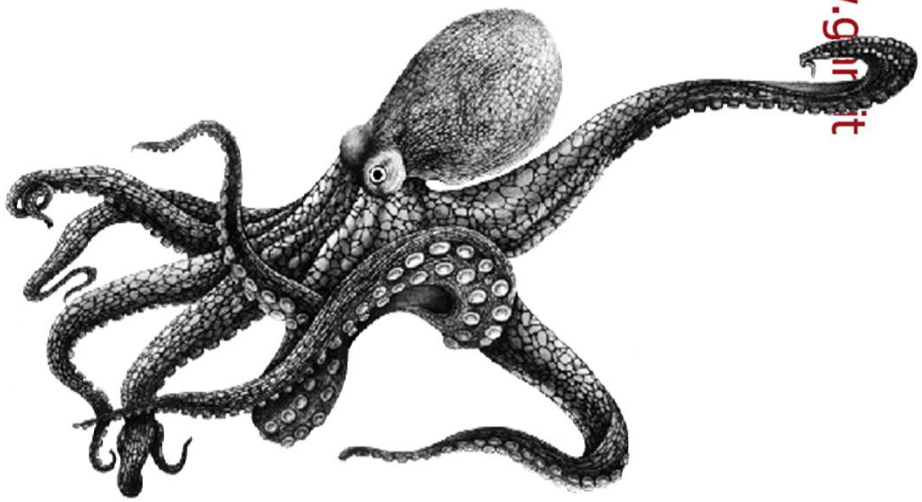


Idea Iniziale : Parsing con Script

- Riutilizzo di script Perl già fatti
  - Numero esiguo di eventi
  - No correlazione
  - Soluzione con Software “Perl Wrapper”
    - Swatch, Wots : demoni scritti in Perl, permettono estensioni, controllo contemp. di più log alert con Nagios e/o mail, rotazione con logrotate, no correlazione

Software per gestione/controllo dei Log (1)

- Octopussy
  - Multipiattaforma
  - Parsing Real-Time
  - Sviluppo lento



- Alternative a Pagamento :
  - Logzilla (ex php-syslog)
  - Splunk

LOGZILLA

splunkbase

Software per gestione/controllo dei Log (2)

- GrayLog2
  - Opensource
  - Log su MongoDB (NoSQL) per statistiche e grafici
  - Struttura dati con Elastic Search

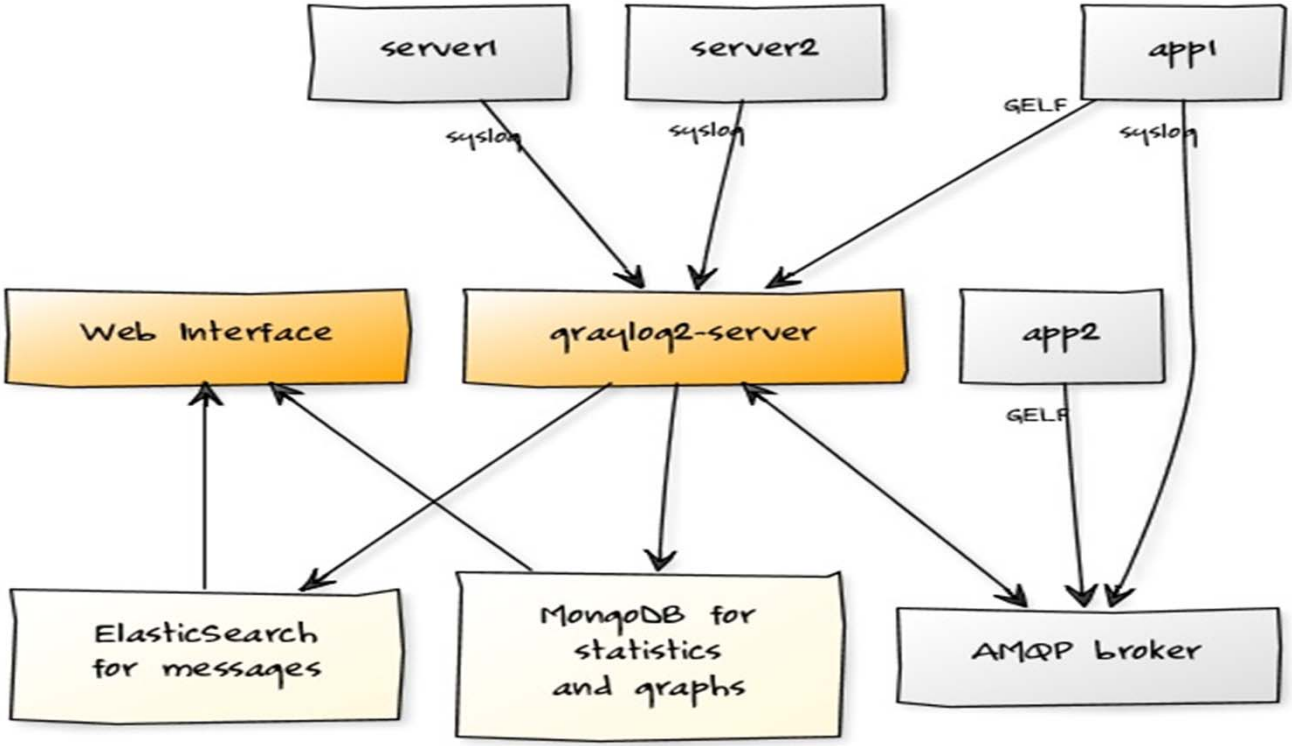
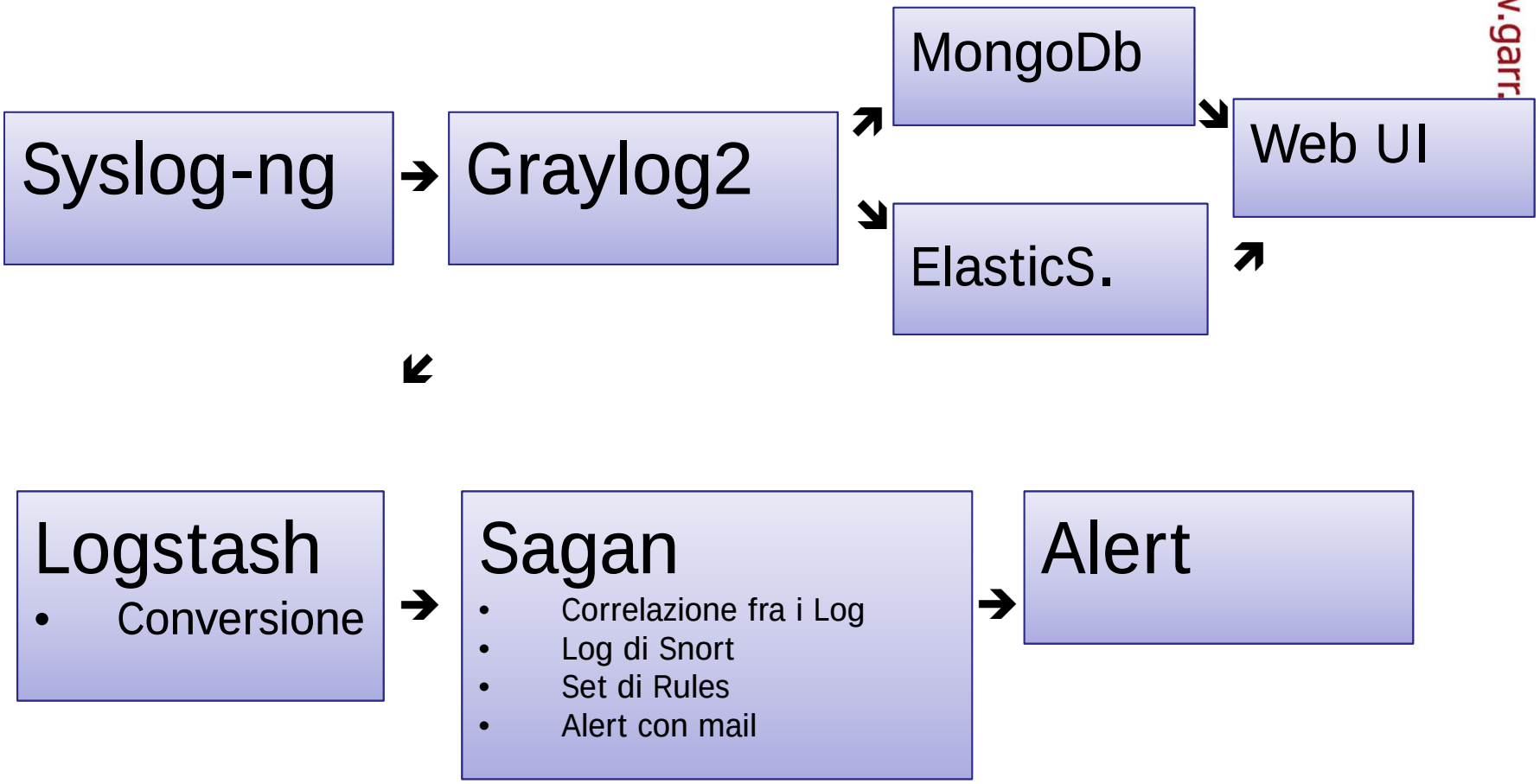
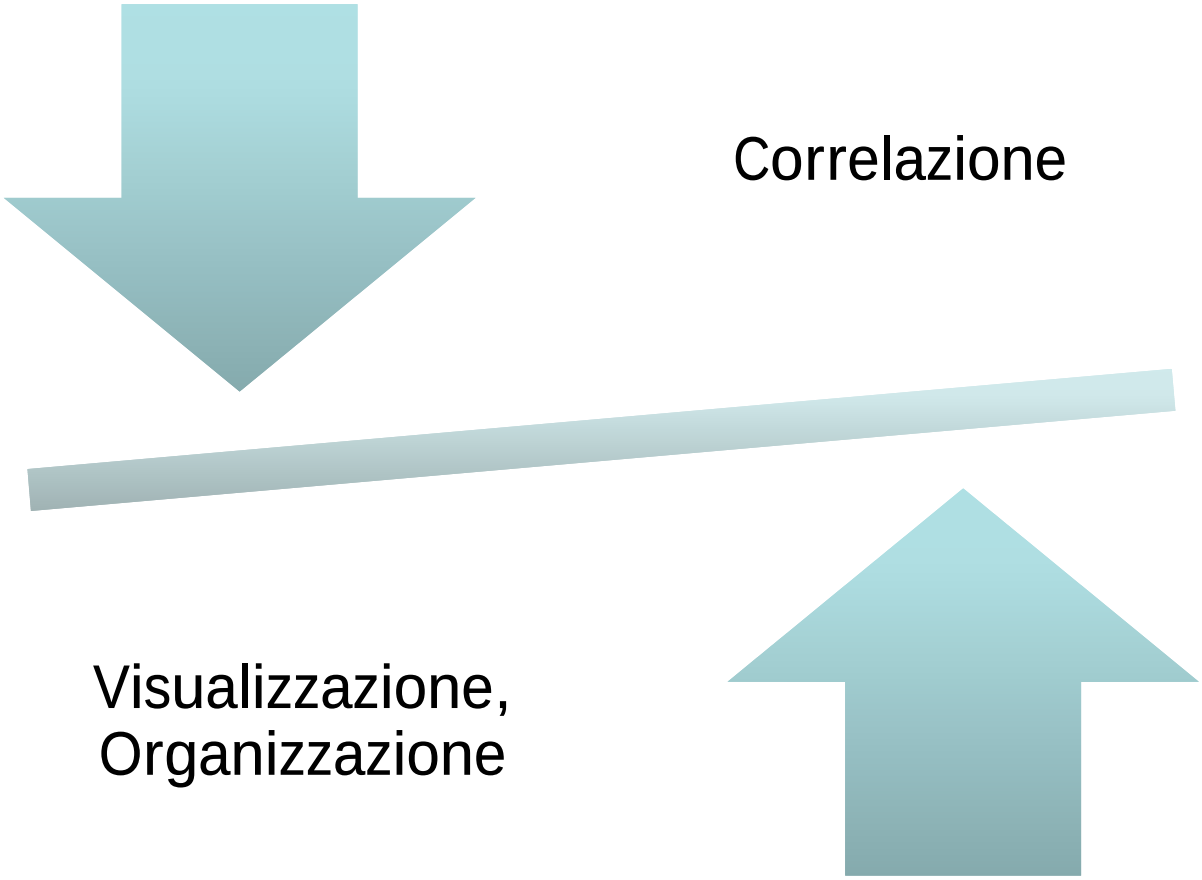


Diagramma di funzionamento



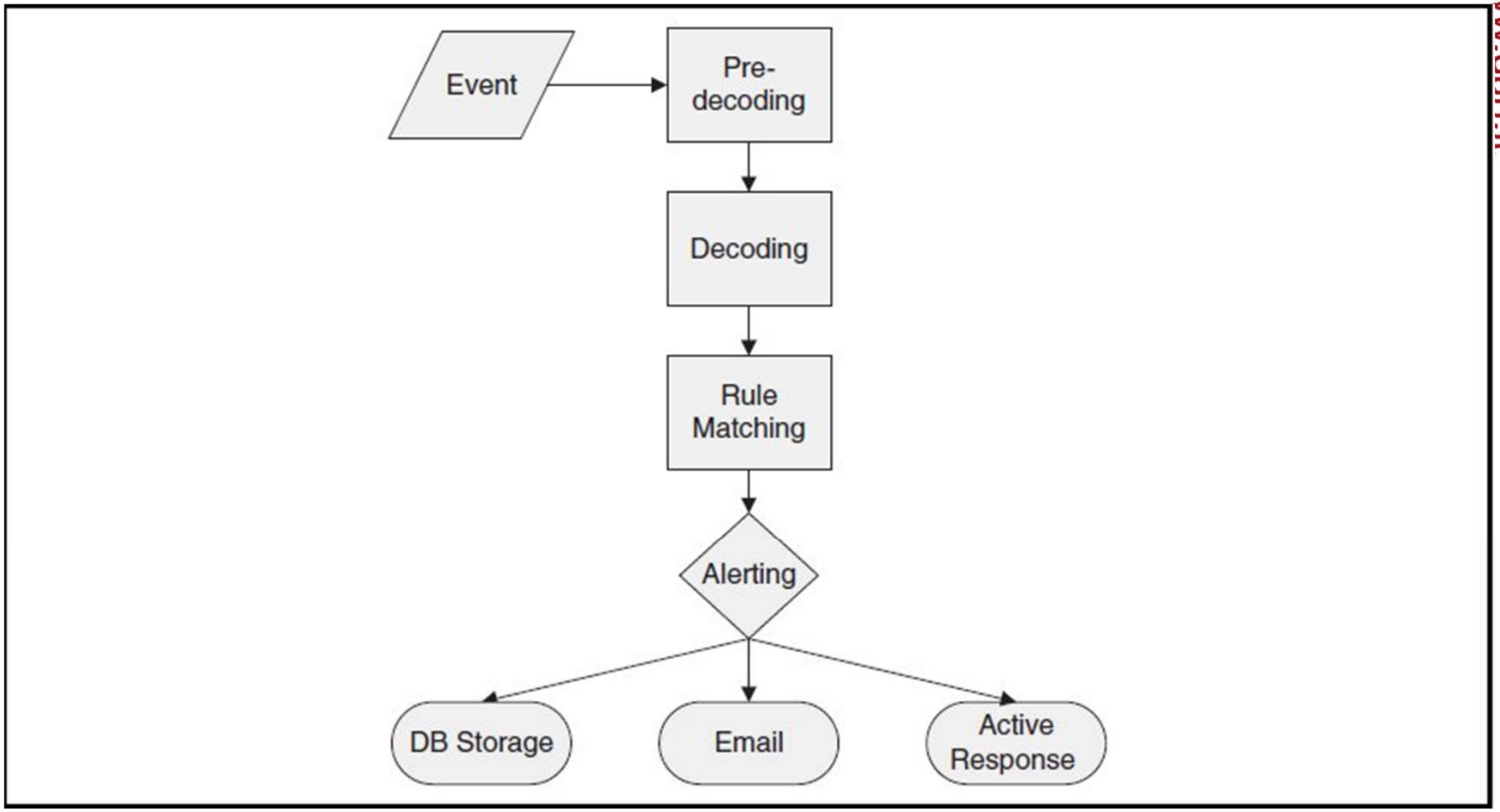
Compromesso



Scelta finale : OSSEC

- OpenSurce, multipiattaforma, sufficiente documentazione
- Controllo dei Log in Real-Time
- System Integrity
- Rootkit Engine
- Sistema di Alert
- Interfaccia Grafica
- Modalità installazione Agent/Server/Local
- Non è un tool di gestione dei Log (gli elabora ma non gli memorizza)

Diagramma di flusso di funzionamento



Ambiente di Virtualizzazione

- Scelta e messa in opera di una infrastruttura per ambienti virtualizzati per i test :
  - VirtualBox + Addition
  - VmWare + Addition
  - KVM (con IntelVT)
  - SCL / CentOS

Individuazione delle modalità operative per l'acquisizione dei Log

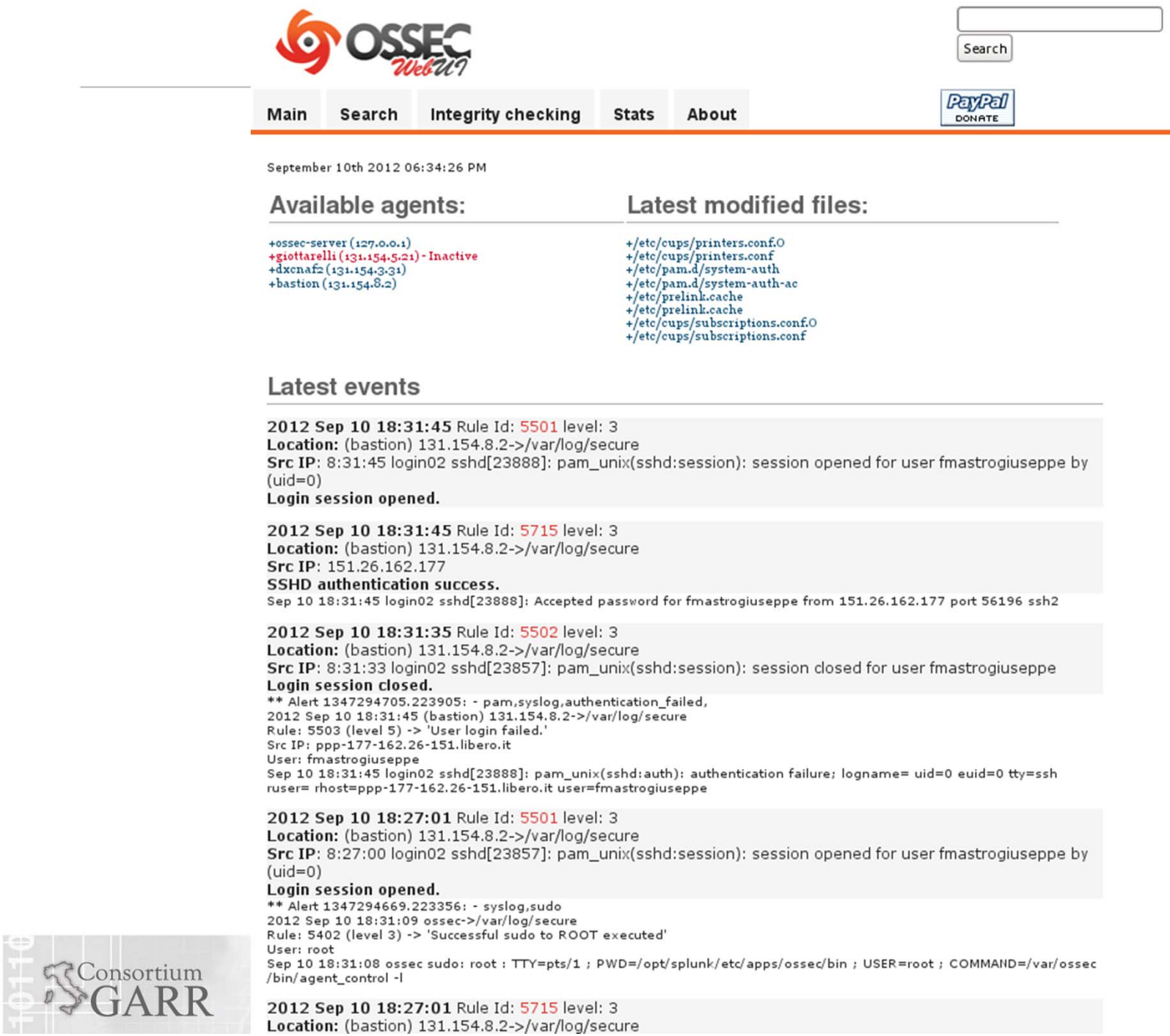
- Saturazione dei Buffer
  - Controllo con netstat, vmstat, top...
- Copia con scp
  - Garantisce sicurezza e connection-oriented
  - Problema dei Log in Append, meglio un Backup differenziale
- Rsync
  - Supporto ssh
  - Compressione dei dati
  - Possibilità di instaurare 1 sola connessione

Rsync

- #!/bin/bash
- while true ;
- do
- cd /var/log/HOSTS/ && find wn-206-01-3*/$(date +%Y/%m/%d/%d) -type f -fprint "${HOME}/elenco"
- rsync -Pztv -e ssh --files-from "${HOME}/elenco" /var/log/HOSTS/ root@131.154.5.54:/var/log/ossec-log/
- echo "copia terminata alle `date` " >> "${HOME}/miolog.txt"
- sleep 10 # or however many seconds you like
- done

Alcuni Cenni sulla configurazione Adottata

- Piattaforma Lamp
  - Apache Web Server
  - MySql database management system
  - Perl, PHP
- Server Relay SMTPAuth con Postfix
- Esclusione dei Log con dimensioni > 100 Mb
  - Escludere server con log prodotti a fine di debug
  - Evitare l'eccessiva durata dello script (basso refresh)


OSSEC WebUI
Search
Main
Search
Integrity checking
Stats
About
PayPal DONATE
September 10th 2012 06:34:26 PM
Available agents:
+ossec-server (127.0.0.1)
+giottarelli (131.154.5.21) - Inactive
+dxcnaf2 (131.154.3.31)
+bastion (131.154.8.2)
Latest modified files:
+/etc/cups/printers.conf.O
+/etc/cups/printers.conf
+/etc/pam.d/system-auth
+/etc/pam.d/system-auth-ac
+/etc/prelink.cache
+/etc/prelink.cache
+/etc/cups/subscriptions.conf.O
+/etc/cups/subscriptions.conf
Latest events
2012 Sep 10 18:31:45 Rule Id: 5501 level: 3
Location: (bastion) 131.154.8.2->/var/log/secure
Src IP: 8:31:45 login02 sshd[23888]: pam_unix(sshd:session): session opened for user fmastrogiuseppe by (uid=0)
Login session opened.
2012 Sep 10 18:31:45 Rule Id: 5715 level: 3
Location: (bastion) 131.154.8.2->/var/log/secure
Src IP: 151.26.162.177
SSHD authentication success.
Sep 10 18:31:45 login02 sshd[23888]: Accepted password for fmastrogiuseppe from 151.26.162.177 port 56196 ssh2
2012 Sep 10 18:31:35 Rule Id: 5502 level: 3
Location: (bastion) 131.154.8.2->/var/log/secure
Src IP: 8:31:33 login02 sshd[23857]: pam_unix(sshd:session): session closed for user fmastrogiuseppe
Login session closed.
** Alert 1347294705.223905: - pam,syslog,authentication_failed,
2012 Sep 10 18:31:45 (bastion) 131.154.8.2->/var/log/secure
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: ppp-177-162.26-151.libero.it
User: fmastrogiuseppe
Sep 10 18:31:45 login02 sshd[23888]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=ppp-177-162.26-151.libero.it user=fmastrogiuseppe
2012 Sep 10 18:27:01 Rule Id: 5501 level: 3
Location: (bastion) 131.154.8.2->/var/log/secure
Src IP: 8:27:00 login02 sshd[23857]: pam_unix(sshd:session): session opened for user fmastrogiuseppe by (uid=0)
Login session opened.
** Alert 1347294669.223356: - syslog,sudo
2012 Sep 10 18:31:09 ossec->/var/log/secure
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'
User: root
Sep 10 18:31:08 ossec sudo: root : TTY=pts/1 ; PWD=/opt/splunk/etc/apps/ossec/bin ; USER=root ; COMMAND=/var/ossec/bin/agent_control -l
2012 Sep 10 18:27:01 Rule Id: 5715 level: 3
Location: (bastion) 131.154.8.2->/var/log/secure

OSSEC WebUI

Search

Main | Search | Integrity checking | Stats | About

PayPal DONATE

Stats options:

Day: 10 Month: September Year: 2012 Change options

Ossec Stats for: 2012/Sep/10

Total: 64,896
Alerts: 61,965
Syscheck: 1
Firewall: 0
Average: 27040 events per hour.

Aggregate values by severity

Option	Value	Percentage
Total for level 4	4	0.0%
Total for level 5	142	0.2%
Total for level 0	470	0.8%
Total for level 3	576	0.9%
Total for level 2	60,773	98.1%
Total for all levels	61,965	100%

Aggregate values by rule

Option	Value	Percentage
Total for Rule 31102	1	0.0%
Total for Rule 30112	1	0.0%
Total for Rule 1006	1	0.0%
Total for Rule 5709	2	0.0%
Total for Rule 5523	2	0.0%
Total for Rule 31101	2	0.0%
Total for Rule 5710	3	0.0%
Total for Rule 10100	4	0.0%
Total for Rule 5722	4	0.0%
Total for Rule 31100	5	0.0%
Total for Rule 2501	6	0.0%
Total for Rule 5716	7	0.0%
Total for Rule 5711	8	0.0%
Total for Rule 509	9	0.0%
Total for Rule 5702	20	0.0%
Total for Rule 3320	28	0.0%
Total for Rule 5721	43	0.1%
Total for Rule 5503	103	0.2%
Total for Rule 5715	109	0.2%
Total for Rule 5502	119	0.2%
Total for Rule 5501	132	0.2%
Total for Rule 5402	216	0.3%
Total for Rule 31108	367	0.6%
Total for Rule 1002	60,773	98.1%
Total for all rules	61,965	100%

Total values per hour

Hour	Alerts	Alerts %	Syscheck	Syscheck %	Firewall	Firewall %	Total	Total %
Hour 0	3,365	5.4%	0	0.0%	0	0.0%	3,513	5.4%
Hour 1	3,339	5.4%	0	0.0%	0	0.0%	3,486	5.4%
Hour 2	3,369	5.4%	0	0.0%	0	0.0%	3,513	5.4%
Hour 3	3,369	5.4%	0	0.0%	0	0.0%	3,512	5.4%
Hour 4	3,383	5.5%	0	0.0%	0	0.0%	3,528	5.4%
Hour 5	3,307	5.3%	0	0.0%	0	0.0%	3,451	5.3%
Hour 6	3,334	5.4%	0	0.0%	0	0.0%	3,477	5.4%
Hour 7	3,371	5.4%	0	0.0%	0	0.0%	3,514	5.4%
Hour 8	3,423	5.5%	0	0.0%	0	0.0%	3,574	5.5%
Hour 9	3,435	5.5%	0	0.0%	0	0.0%	3,593	5.5%

Search

Main | Search | Integrity checking | Stats | About

PayPal DONATE

September 10th 2012 06:35:30 PM

Alert search options:

From: 2012-09-10 14:35 To: 2012-09-10 18:35

Real time monitoring

Minimum level:	7	Category:	All categories
Pattern:		Log formats:	All log formats
Srcip:		User:	
Location:		Rule id:	
Max Alerts:	1000		

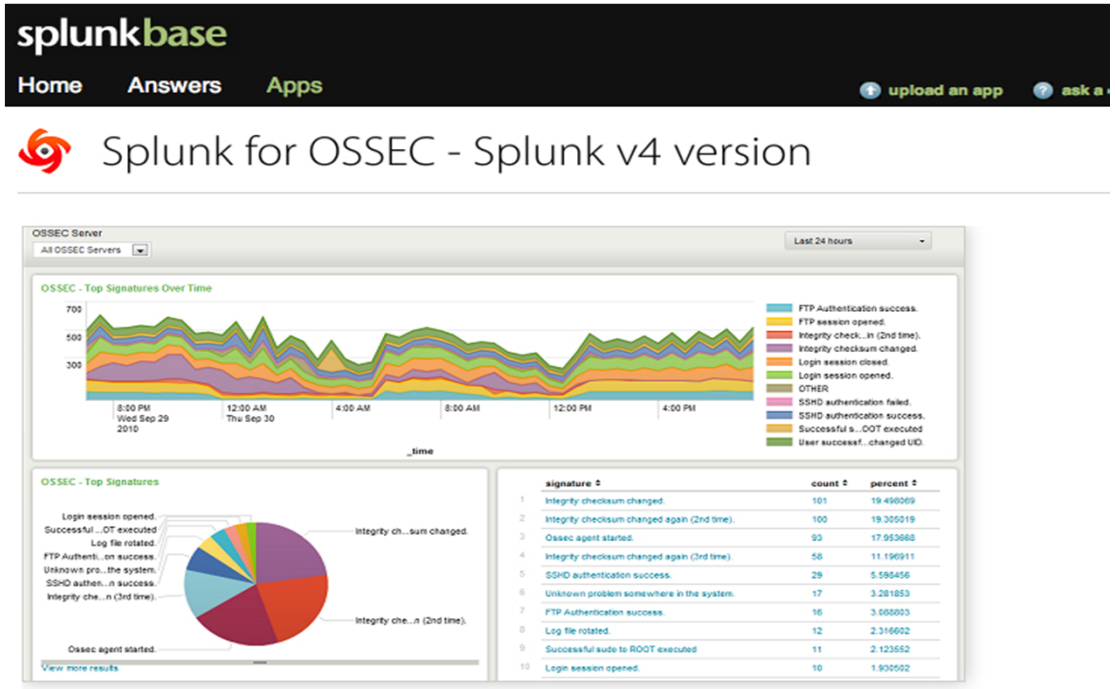
Search

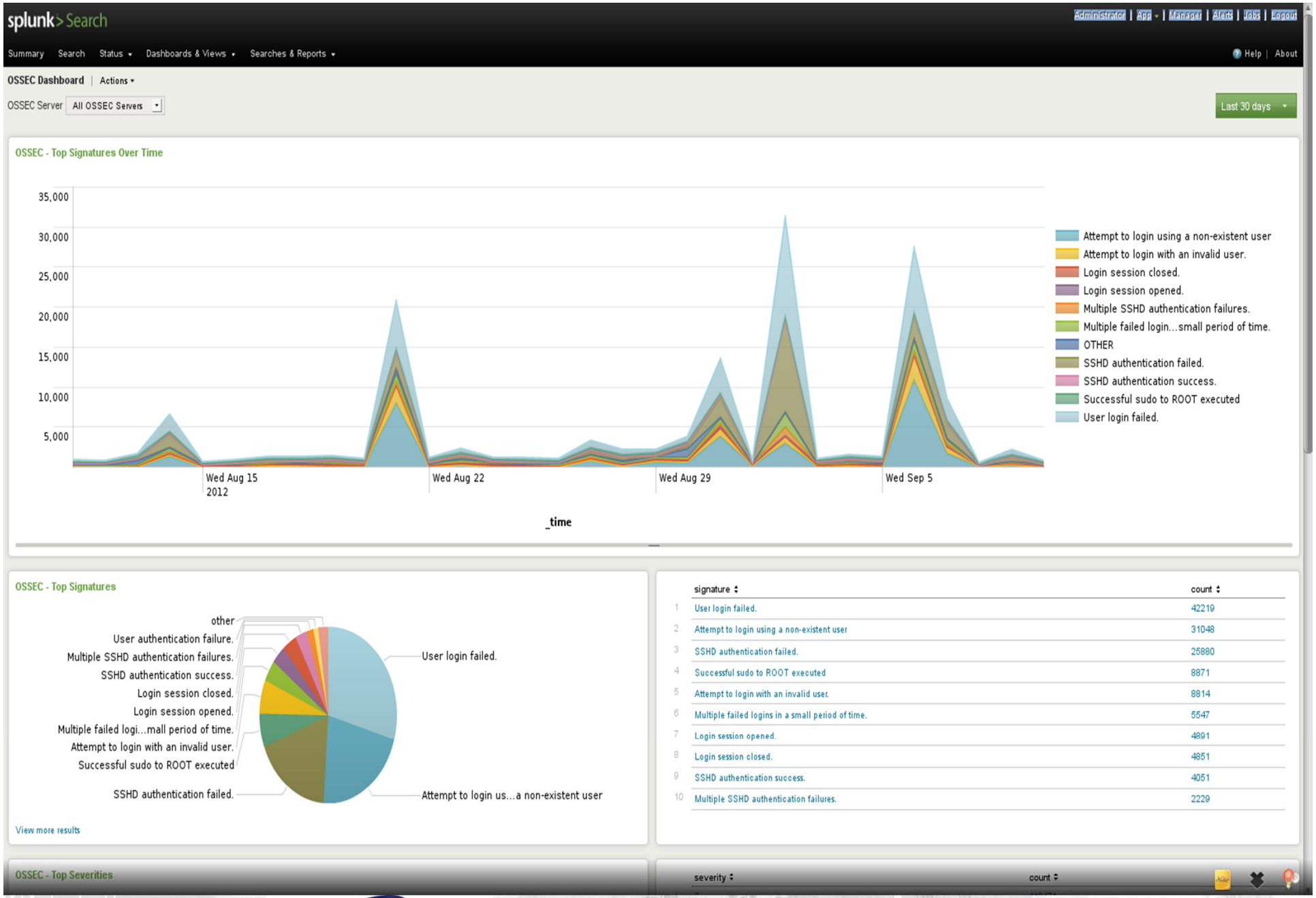
Results:

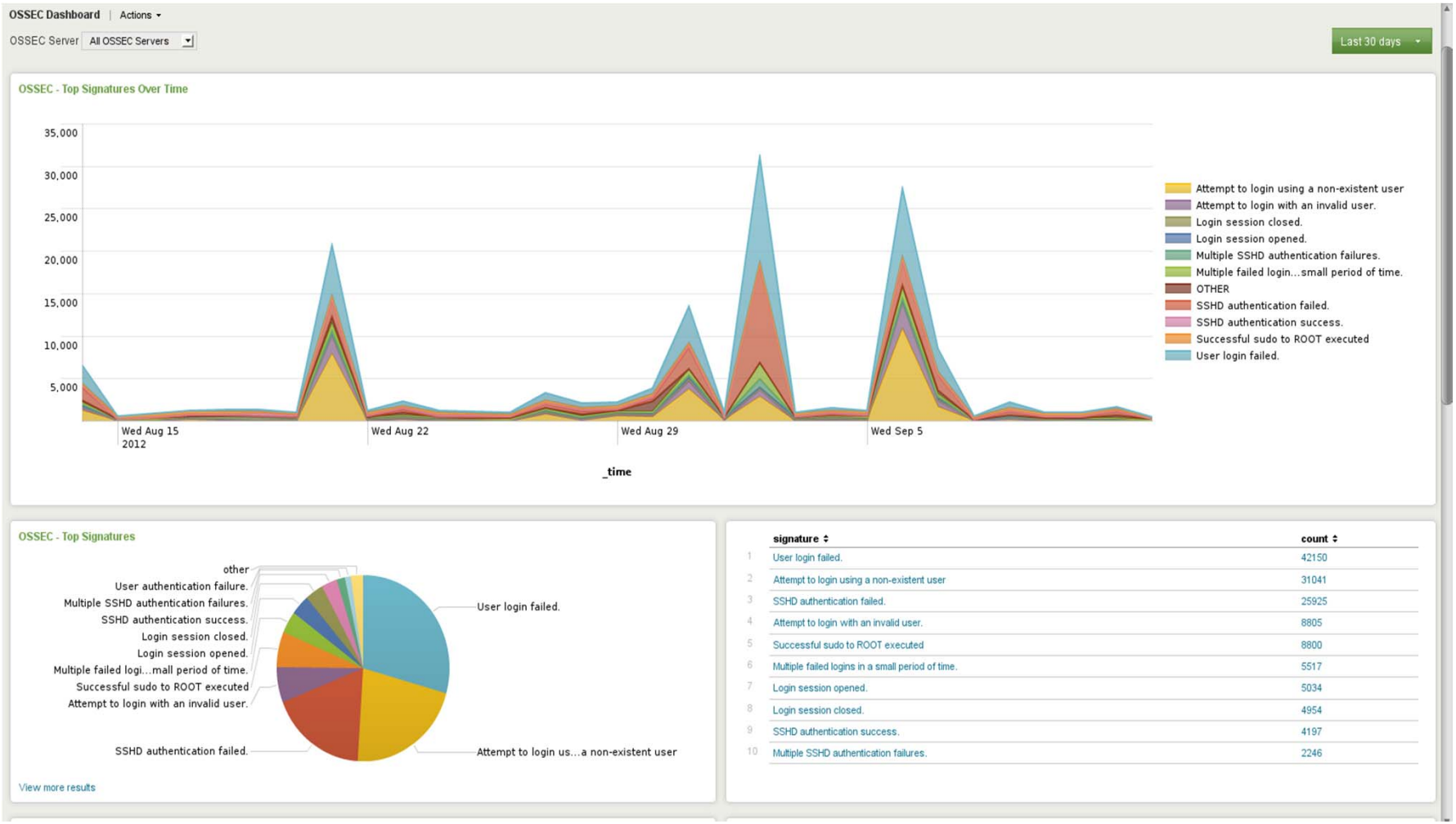
No search performed.

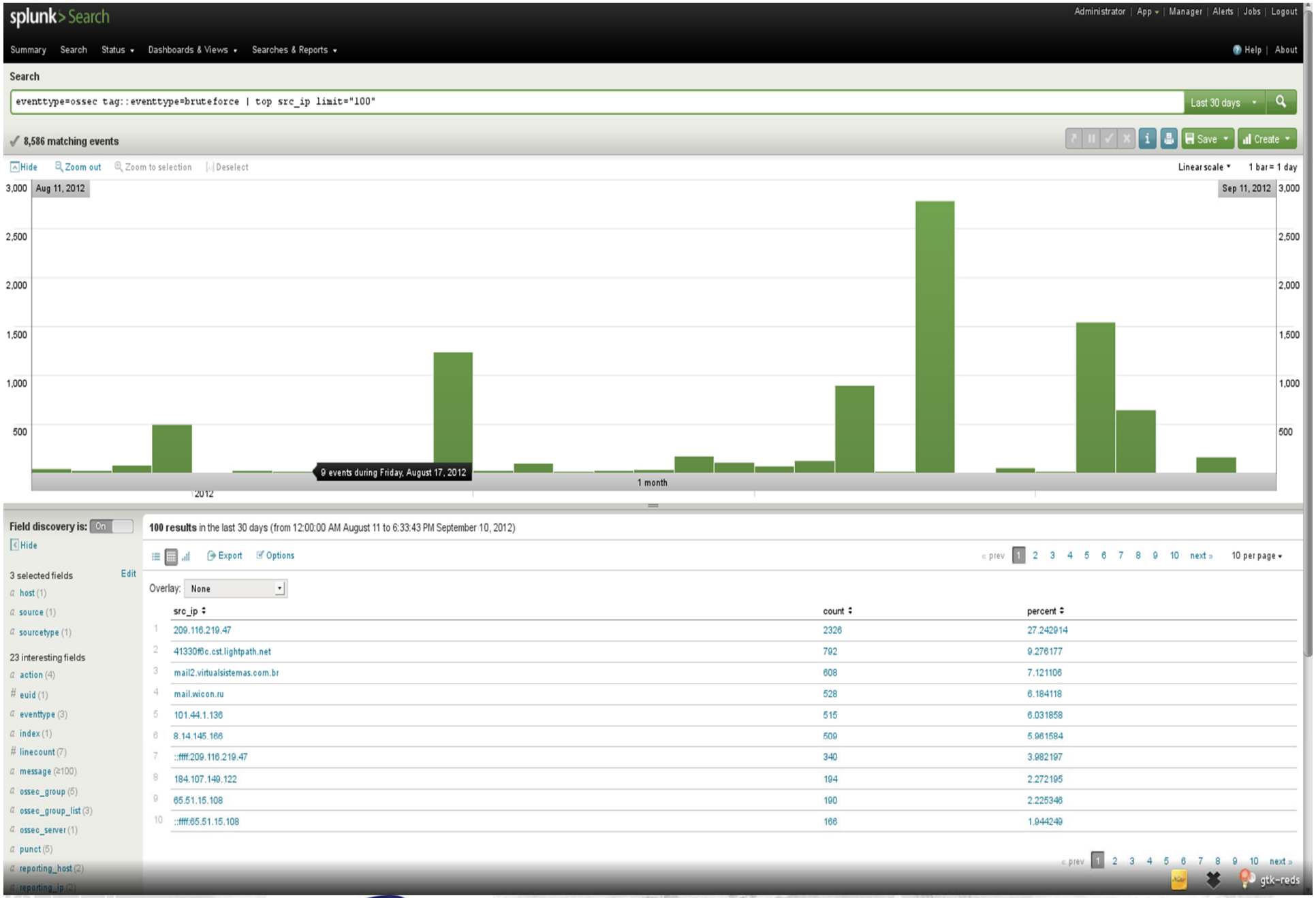
Ricerca di una Interfaccia più esaustiva

- Senza la necessità di riconvertire i Log
- Consenta la Visualizzazione degli Alert prodotti




splunk> Search
Administrator | App | Manage | Alerts | Jobs | Logout
Summary Search Status Dashboards & Views Searches & Reports
Help | About
OSSEC Dashboard | Actions
OSSEC Server All OSSEC Servers
Last 30 days
OSSEC - Top Signatures Over Time
35,000
30,000
25,000
20,000
15,000
10,000
5,000
Wed Aug 15 2012
Wed Aug 22
Wed Aug 29
Wed Sep 5
_time
Attempt to login using a non-existent user
Attempt to login with an invalid user.
Login session closed.
Login session opened.
Multiple SSHD authentication failures.
Multiple failed login...small period of time.
OTHER
SSHD authentication failed.
SSHD authentication success.
Successful sudo to ROOT executed
User login failed.
OSSEC - Top Signatures
other
User authentication failure.
Multiple SSHD authentication failures.
SSHD authentication success.
Login session closed.
Login session opened.
Multiple failed logi...mall period of time.
Attempt to login with an invalid user.
Successful sudo to ROOT executed
SSHD authentication failed.
User login failed.
Attempt to login us...a non-existent user
View more results
signature
count
1 User login failed. 42219
2 Attempt to login using a non-existent user 31048
3 SSHD authentication failed. 25880
4 Successful sudo to ROOT executed 8871
5 Attempt to login with an invalid user. 8814
6 Multiple failed logins in a small period of time. 5547
7 Login session opened. 4891
8 Login session closed. 4851
9 SSHD authentication success. 4051
10 Multiple SSHD authentication failures. 2229
OSSEC - Top Severities
severity
count


OSSEC Dashboard | Actions
OSSEC Server All OSSEC Servers
Last 30 days
OSSEC - Top Signatures Over Time
35,000
30,000
25,000
20,000
15,000
10,000
5,000
Wed Aug 15 2012
Wed Aug 22
Wed Aug 29
Wed Sep 5
_time
Attempt to login using a non-existent user
Attempt to login with an invalid user.
Login session closed.
Login session opened.
Multiple SSHD authentication failures.
Multiple failed login...small period of time.
OTHER
SSHD authentication failed.
SSHD authentication success.
Successful sudo to ROOT executed
User login failed.
OSSEC - Top Signatures
other
User authentication failure.
Multiple SSHD authentication failures.
SSHD authentication success.
Login session closed.
Login session opened.
Multiple failed logi...mall period of time.
Successful sudo to ROOT executed
Attempt to login with an invalid user.
SSHD authentication failed.
User login failed.
Attempt to login us...a non-existent user
View more results
signature
count
1 User login failed. 42150
2 Attempt to login using a non-existent user 31041
3 SSHD authentication failed. 25925
4 Attempt to login with an invalid user. 8805
5 Successful sudo to ROOT executed 8800
6 Multiple failed logins in a small period of time. 5517
7 Login session opened. 5034
8 Login session closed. 4954
9 SSHD authentication success. 4197
10 Multiple SSHD authentication failures. 2246


splunk> Search
Administrator | App | Manager | Alerts | Jobs | Logout
Summary Search Status Dashboards & Views Searches & Reports
Help | About
Search
eventtype=ossec tag::eventtype=bruteforce | top src_ip limit="100"
Last 30 days
8,586 matching events
Save
Create
Hide
Zoom out
Zoom to selection
Deselect
Linear scale
1 bar = 1 day
3,000
2,500
2,000
1,500
1,000
500
Aug 11, 2012
Sep 11, 2012
9 events during Friday, August 17, 2012
1 month
2012
Field discovery is: On
Hide
3 selected fields
Edit
host (1)
source (1)
sourcetype (1)
23 interesting fields
action (4)
euid (1)
eventtype (3)
index (1)
linecount (7)
message (≥100)
ossec_group (5)
ossec_group_list (3)
ossec_server (1)
punct (5)
reporting_host (2)
reporting_ip (2)
100 results in the last 30 days (from 12:00:00 AM August 11 to 6:33:43 PM September 10, 2012)
Export
Options
« prev 1 2 3 4 5 6 7 8 9 10 next »
10 per page
Overlay: None
src_ip
count
percent
1 209.116.219.47 2326 27.242914
2 41330f8c.cst.lightpath.net 792 9.276177
3 mail2.virtualsistemas.com.br 608 7.121106
4 mail.wicon.ru 528 6.184118
5 101.44.1.136 515 6.031858
6 8.14.145.166 509 5.961584
7 ::ffff:209.116.219.47 340 3.982197
8 184.107.149.122 194 2.272195
9 65.51.15.108 190 2.225346
10 ::ffff:65.51.15.108 166 1.944249
« prev 1 2 3 4 5 6 7 8 9 10 next »
gtk-reds

Conclusioni

- Istituire un sistema di gestione dei Log offre in ogni caso altri vantaggi, oltre a quello di soddisfare le disposizioni normative.
- Ricavare sempre più informazioni dai log disponibili consente non solo ottimizzazione dal punto di vista della sicurezza ma anche utili per scovare bug software o anomalie nell'uso di risorse
- L'esperienza dal punto di vista formativo

Fine

www.garr.it

Grazie per l'attenzione