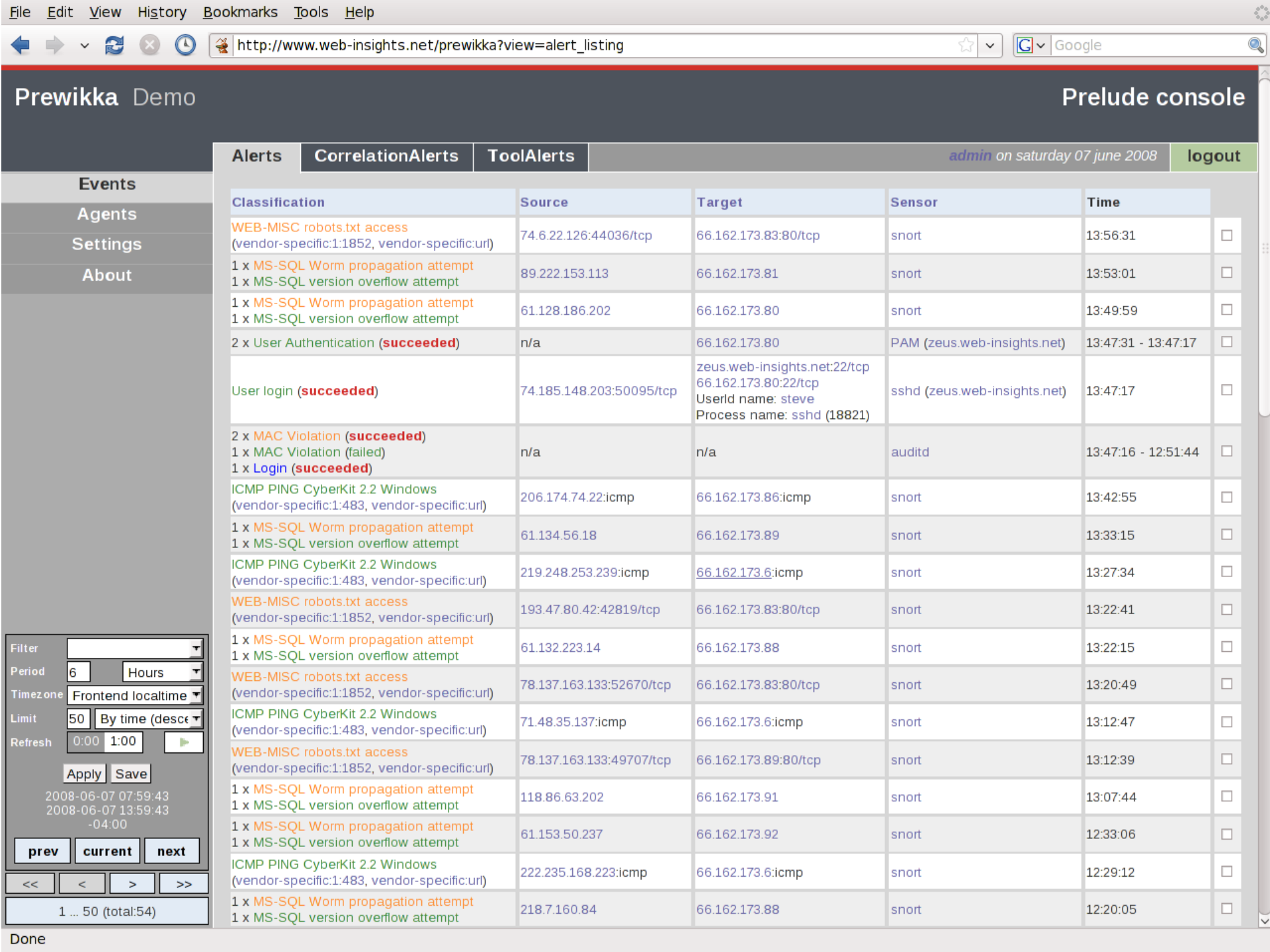
Picviz: logiciel de visualisation des journaux

Sébastien Tricaud

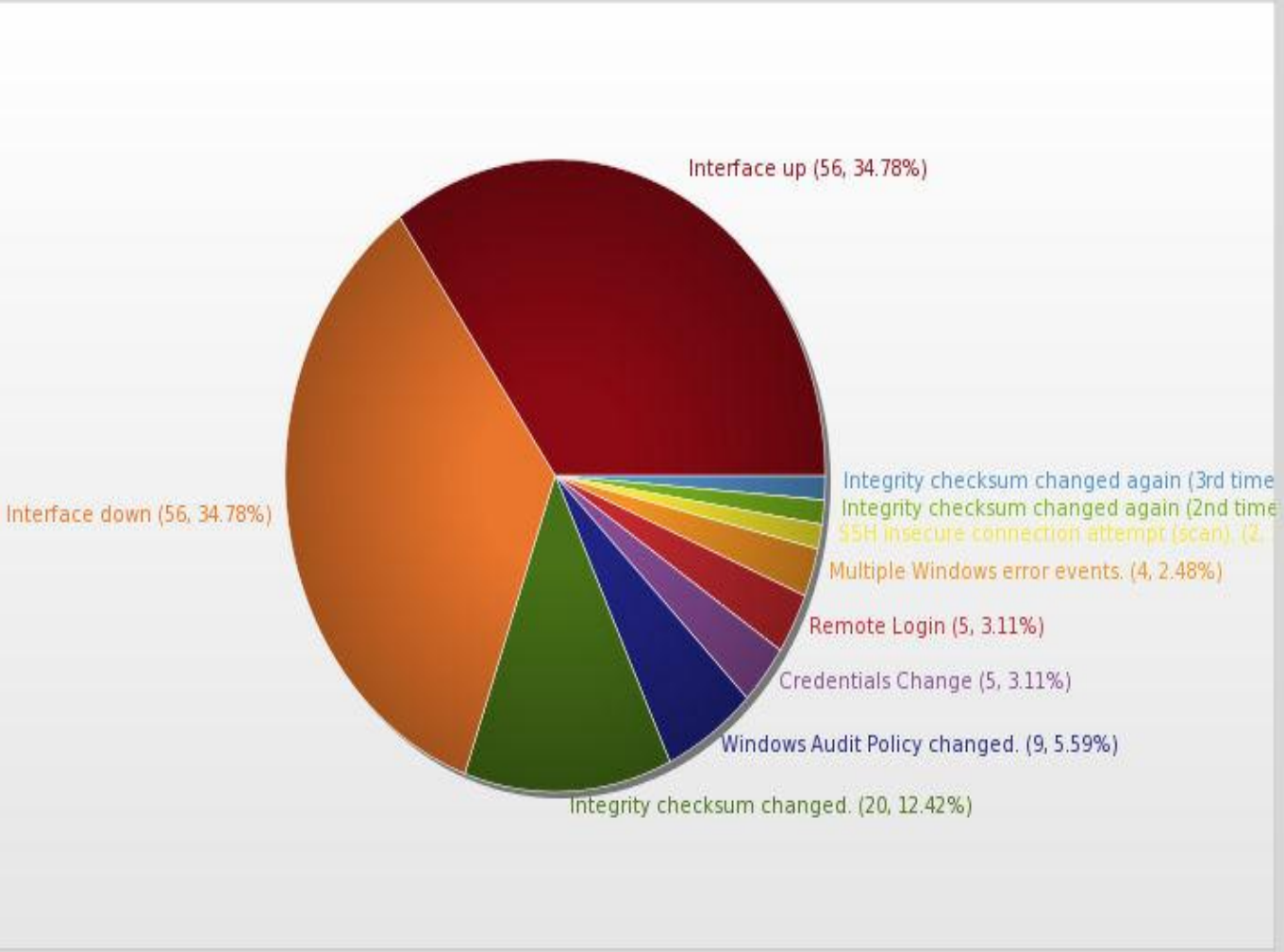

File Edit View History Bookmarks Tools Help
http://www.web-insights.net/prewikka?view=alert_listing
Google
Prewikka Demo
Prelude console
Alerts
CorrelationAlerts
ToolAlerts
admin on saturday 07 june 2008
logout
Events
Agents
Settings
About
Classification
Source
Target
Sensor
Time
WEB-MISC robots.txt access
(vendor-specific:1:1852, vendor-specific:url)
74.6.22.126:44036/tcp
66.162.173.83:80/tcp
snort
13:56:31
1 x MS-SQL Worm propagation attempt
1 x MS-SQL version overflow attempt
89.222.153.113
66.162.173.81
snort
13:53:01
1 x MS-SQL Worm propagation attempt
1 x MS-SQL version overflow attempt
61.128.186.202
66.162.173.80
snort
13:49:59
2 x User Authentication (succeeded)
n/a
66.162.173.80
PAM (zeus.web-insights.net)
13:47:31 - 13:47:17
User login (succeeded)
74.185.148.203:50095/tcp
zeus.web-insights.net:22/tcp
66.162.173.80:22/tcp
Userid name: steve
Process name: sshd (18821)
sshd (zeus.web-insights.net)
13:47:17
2 x MAC Violation (succeeded)
1 x MAC Violation (failed)
1 x Login (succeeded)
n/a
n/a
auditd
13:47:16 - 12:51:44
ICMP PING CyberKit 2.2 Windows
(vendor-specific:1:483, vendor-specific:url)
206.174.74.22:icmp
66.162.173.86:icmp
snort
13:42:55
1 x MS-SQL Worm propagation attempt
1 x MS-SQL version overflow attempt
61.134.56.18
66.162.173.89
snort
13:33:15
ICMP PING CyberKit 2.2 Windows
(vendor-specific:1:483, vendor-specific:url)
219.248.253.239:icmp
66.162.173.6:icmp
snort
13:27:34
WEB-MISC robots.txt access
(vendor-specific:1:1852, vendor-specific:url)
193.47.80.42:42819/tcp
66.162.173.83:80/tcp
snort
13:22:41
1 x MS-SQL Worm propagation attempt
1 x MS-SQL version overflow attempt
61.132.223.14
66.162.173.88
snort
13:22:15
WEB-MISC robots.txt access
(vendor-specific:1:1852, vendor-specific:url)
78.137.163.133:52670/tcp
66.162.173.83:80/tcp
snort
13:20:49
ICMP PING CyberKit 2.2 Windows
(vendor-specific:1:483, vendor-specific:url)
71.48.35.137:icmp
66.162.173.6:icmp
snort
13:12:47
WEB-MISC robots.txt access
(vendor-specific:1:1852, vendor-specific:url)
78.137.163.133:49707/tcp
66.162.173.89:80/tcp
snort
13:12:39
1 x MS-SQL Worm propagation attempt
1 x MS-SQL version overflow attempt
118.86.63.202
66.162.173.91
snort
13:07:44
1 x MS-SQL Worm propagation attempt
1 x MS-SQL version overflow attempt
61.153.50.237
66.162.173.92
snort
12:33:06
ICMP PING CyberKit 2.2 Windows
(vendor-specific:1:483, vendor-specific:url)
222.235.168.223:icmp
66.162.173.6:icmp
snort
12:29:12
1 x MS-SQL Worm propagation attempt
1 x MS-SQL version overflow attempt
218.7.160.84
66.162.173.88
snort
12:20:05
Filter
Period
6
Hours
Timezone
Frontend localtime
Limit
50
By time (desce
Refresh
0:00
1:00
Apply
Save
2008-06-07 07:59:43
2008-06-07 13:59:43
-04:00
prev
current
next
<<
<
>
>>
1 ... 50 (total:54)
Done

Prewikka

Events
Agents
Statistics
Settings
About

Categorizations | Sources | Targets | Analyzers | Timeline

Top 10 Classifications

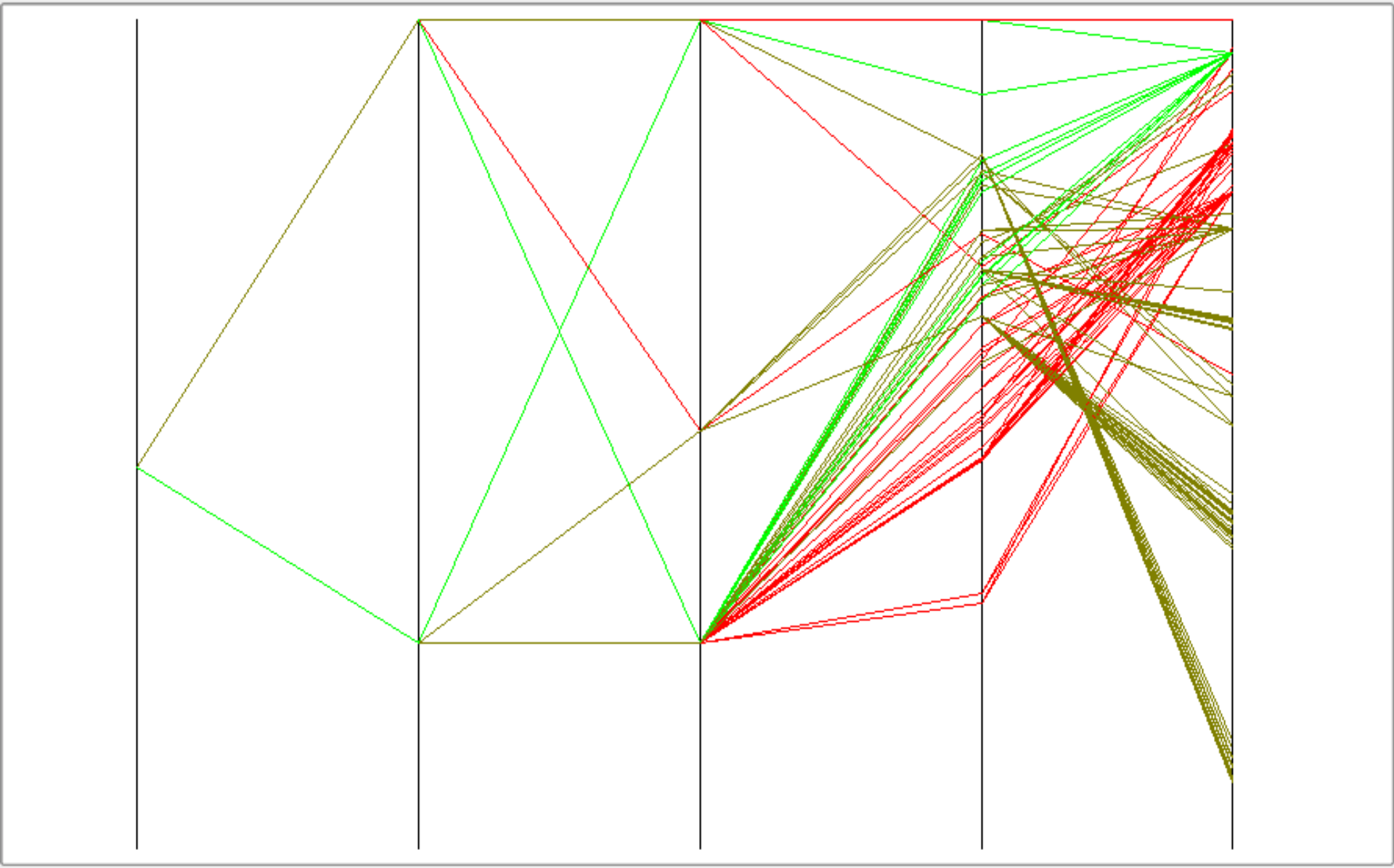



Brute force attack
Multiple failed attempts have been made to login to a user account
Brute force attack
Multiple failed attempts have been made to login to a user account

Prelude IDMEF Grapher

File Help

timeline | source(0).node.address(0).address | target(0).node.address(0).address | alert.classification.text | alert.assessment.impact.description



Picviz Opensource

- Présenté à Usenix WASL en décembre 2008

http://www.usenix.org/events/wasl/tech/full_papers/tricaud/tricaud.pdf

- Génère un graphe depuis un language

```
$ pcv -Tpngcairo -Rheatline -rrrra syslogemu.pcv > syslogemu.png
```

```
header {
        title = "Syslog picviz analysis";
}
axes {
        ipv4   SRC [label="Ip source"];
        ipv4   DST [label="IP destination"];
        port   SPT [label="Port source"];
        port   DPT [label="Port destination"];
}
data {
PortIN="",SRC="192.168.1.205",DST="192.168.1.240",SPT="48040",DPT="23";
PortIN="",SRC="192.168.1.205",DST="192.168.1.240",SPT="48040",DPT="113";
PortIN="",SRC="192.168.1.205",DST="192.168.1.240",SPT="48040",DPT="21";
...
}
```


PICVIZ®
LABS

Picviz Inspector

- Normalisation facile des données
  - Binaire
  - Texte
  - Base de données
  - Hadoop
- Visualisation interactive jusqu'au milliard
- Correlation visuelle

Problèmes

- Les machines sont devenues omniprésentes
- Les données sont volumineuses

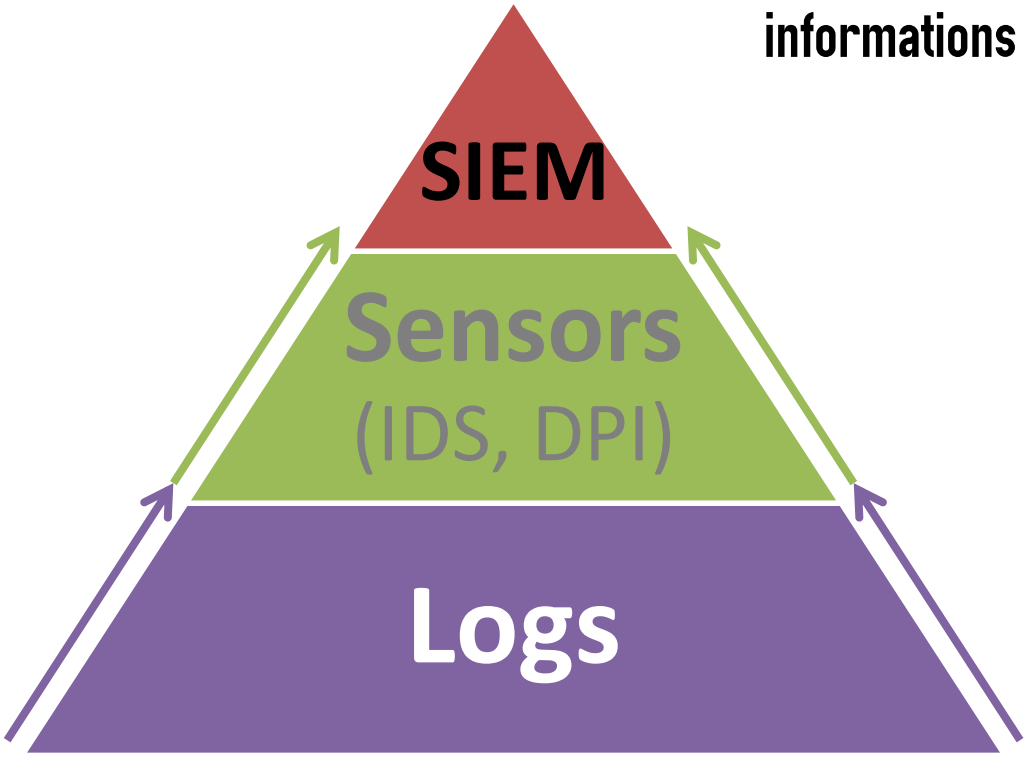
- Un résumé par statistiques, diagrames, camemberts etc. ne suffisent plus
- On a automatisé tout ce que l'on pouvait, on a oublié l'humain derrière

But

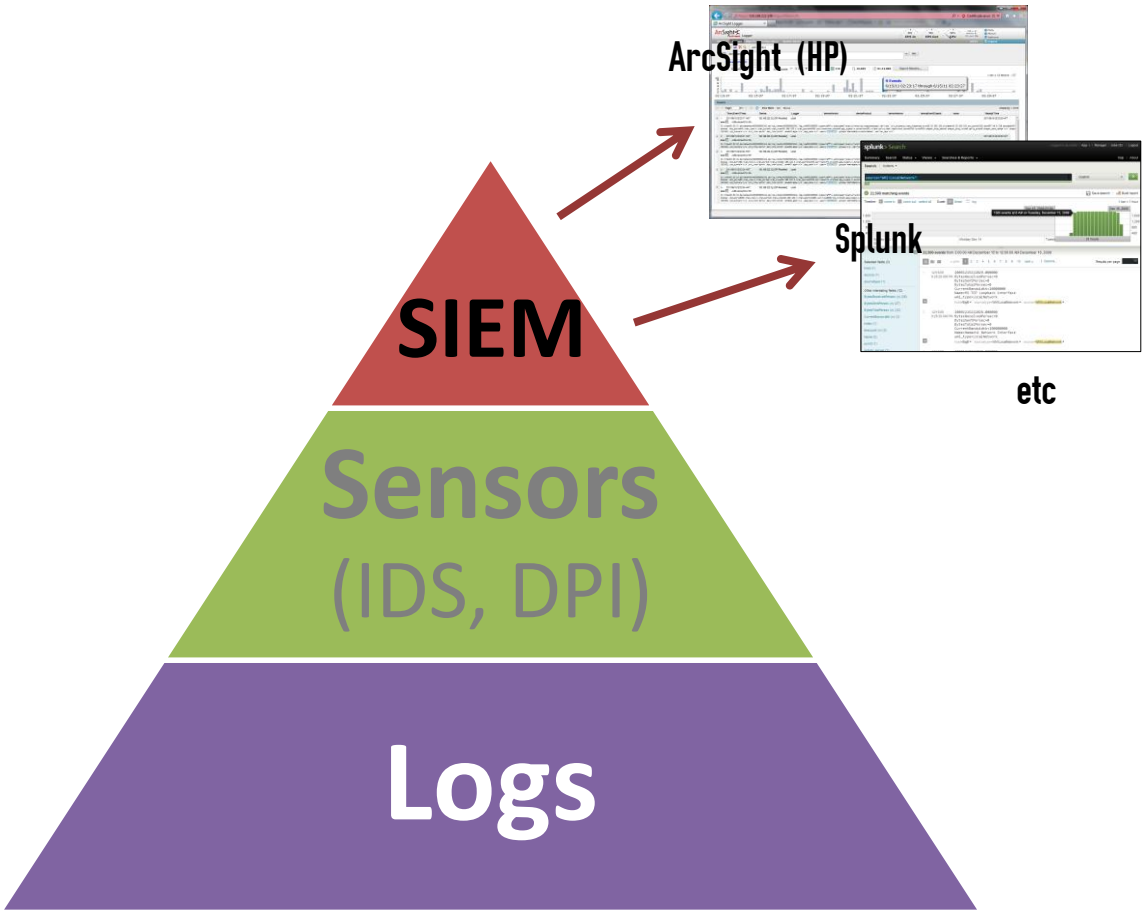
Trouver des attaques inconnues dans une masse de données colossale

LOG MANAGEMENT (aujourd'hui)

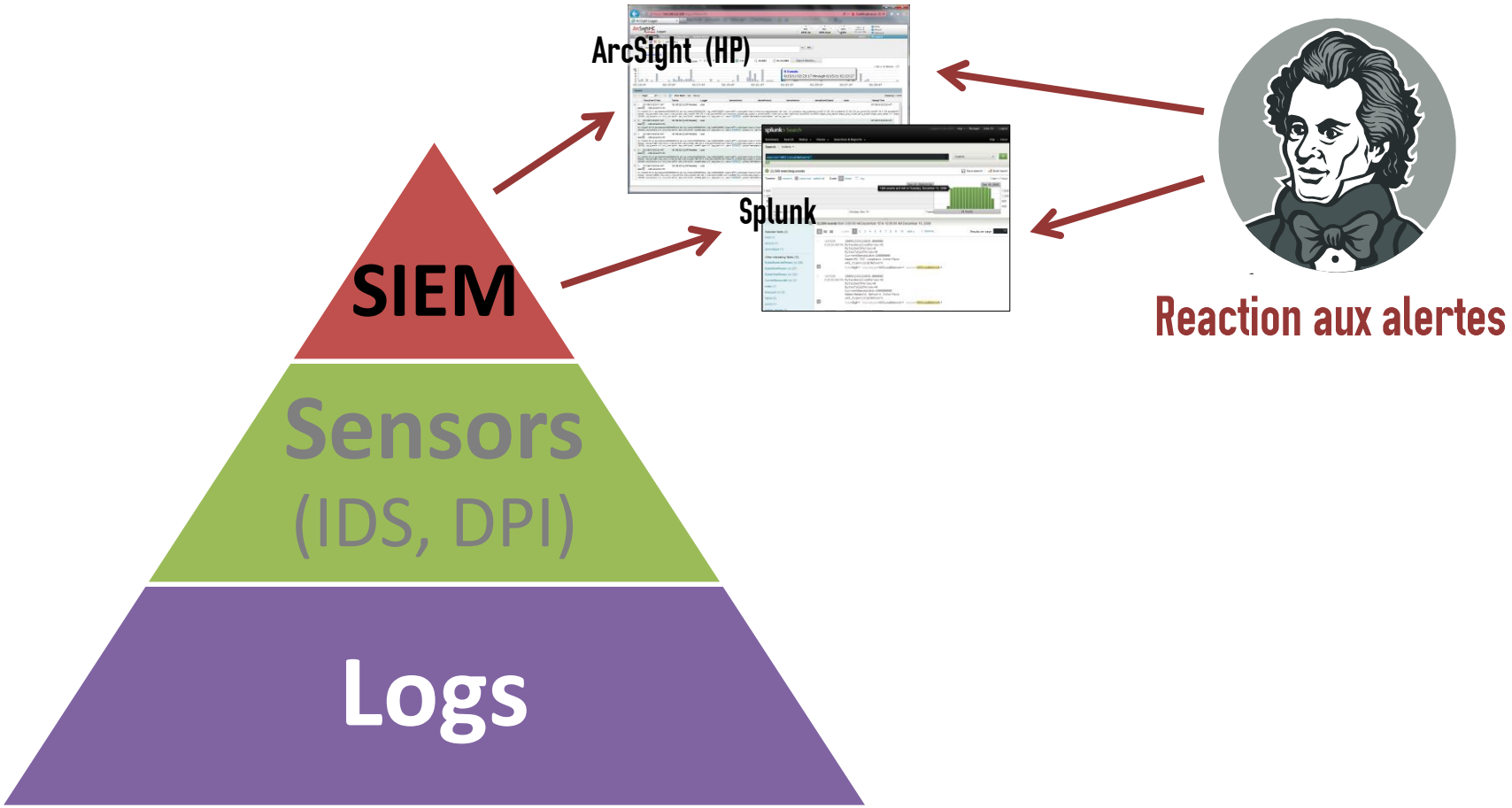
Réduction des données et des informations



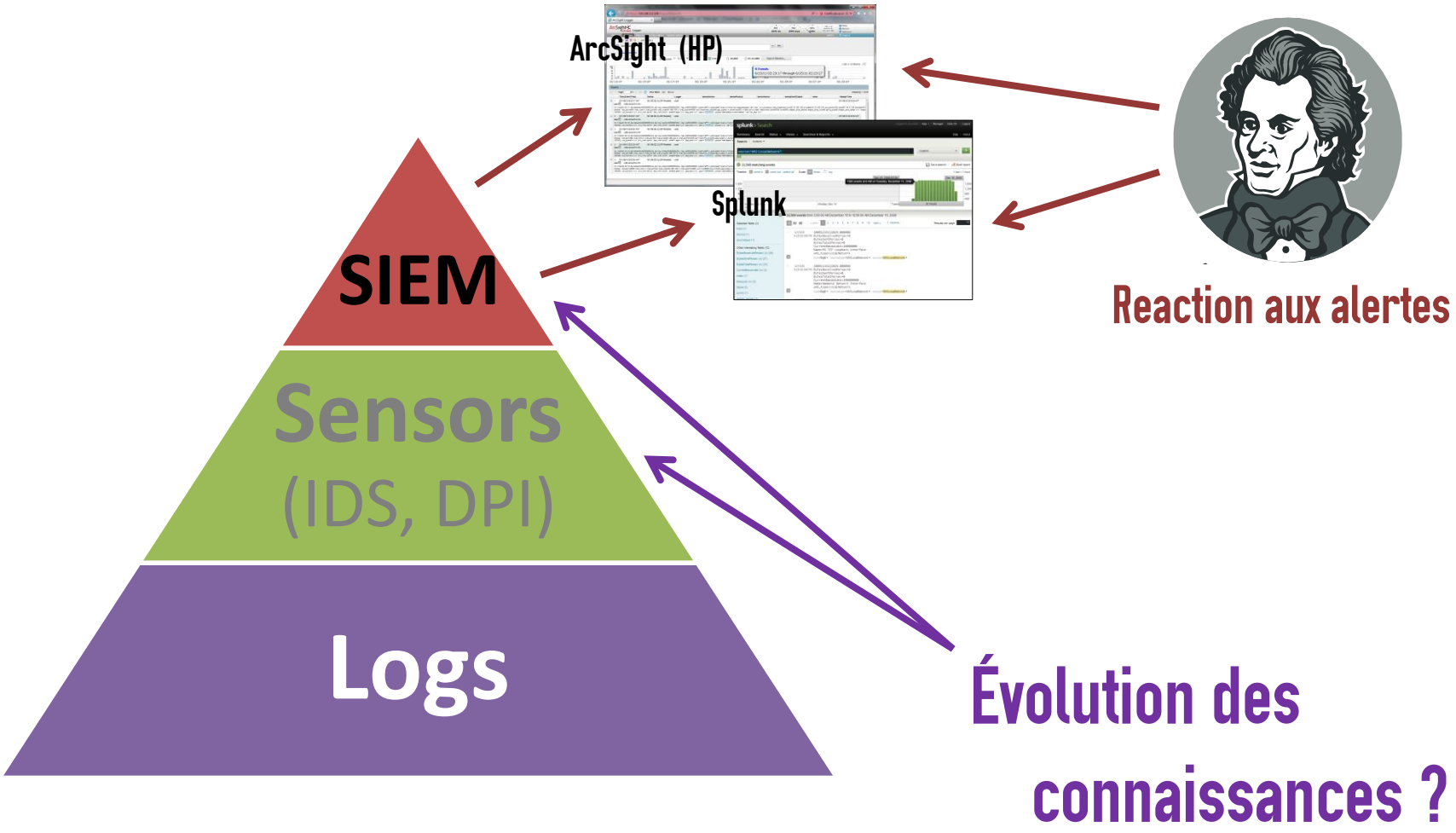
LOG MANAGEMENT (aujourd'hui)



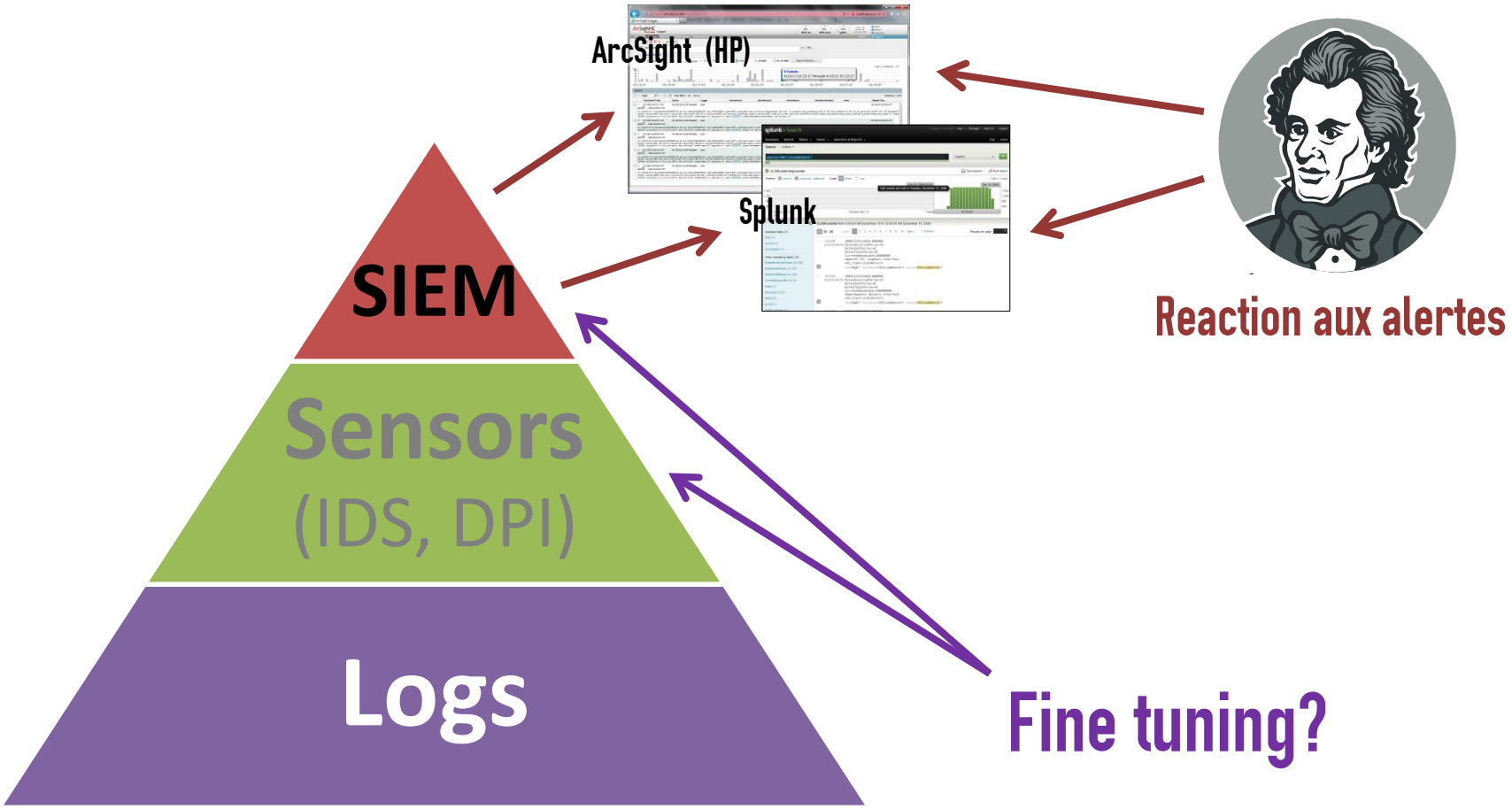
LOG MANAGEMENT (aujourd'hui)



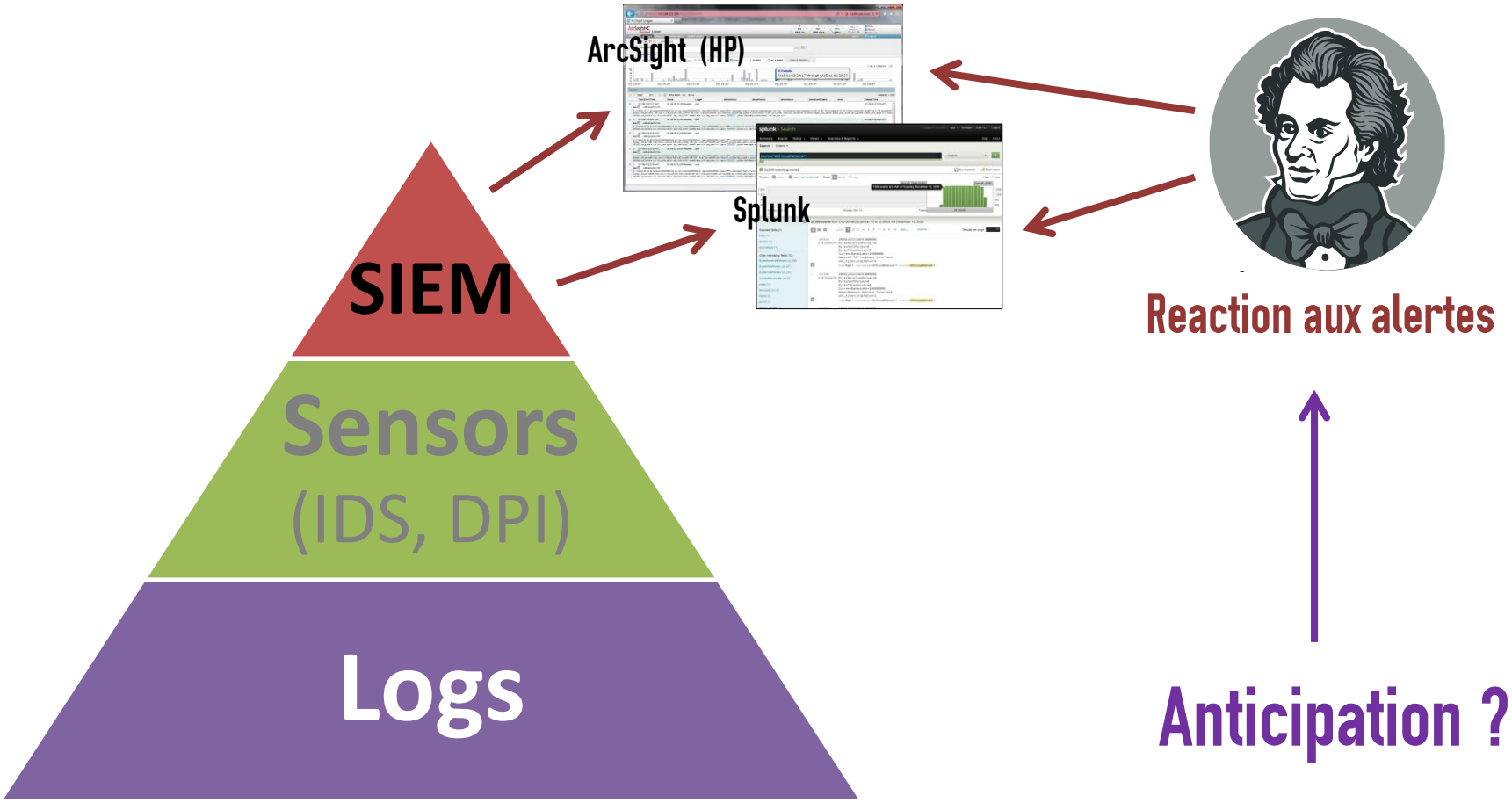
LOG MANAGEMENT (aujourd'hui)



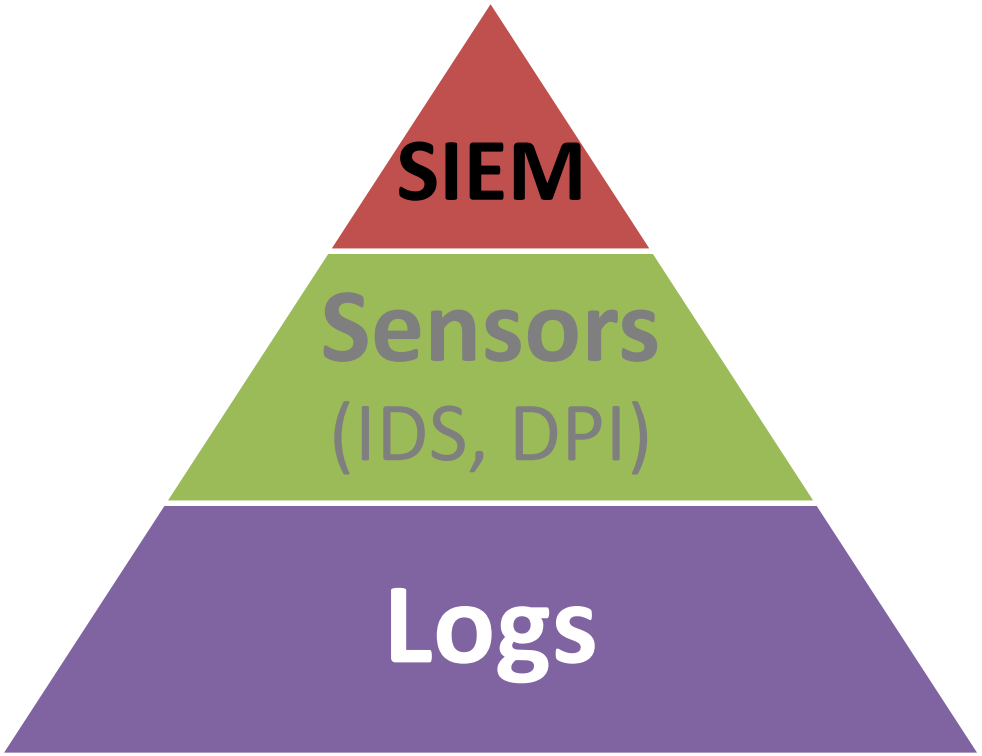
LOG MANAGEMENT (aujourd'hui)



LOG MANAGEMENT (aujourd'hui)

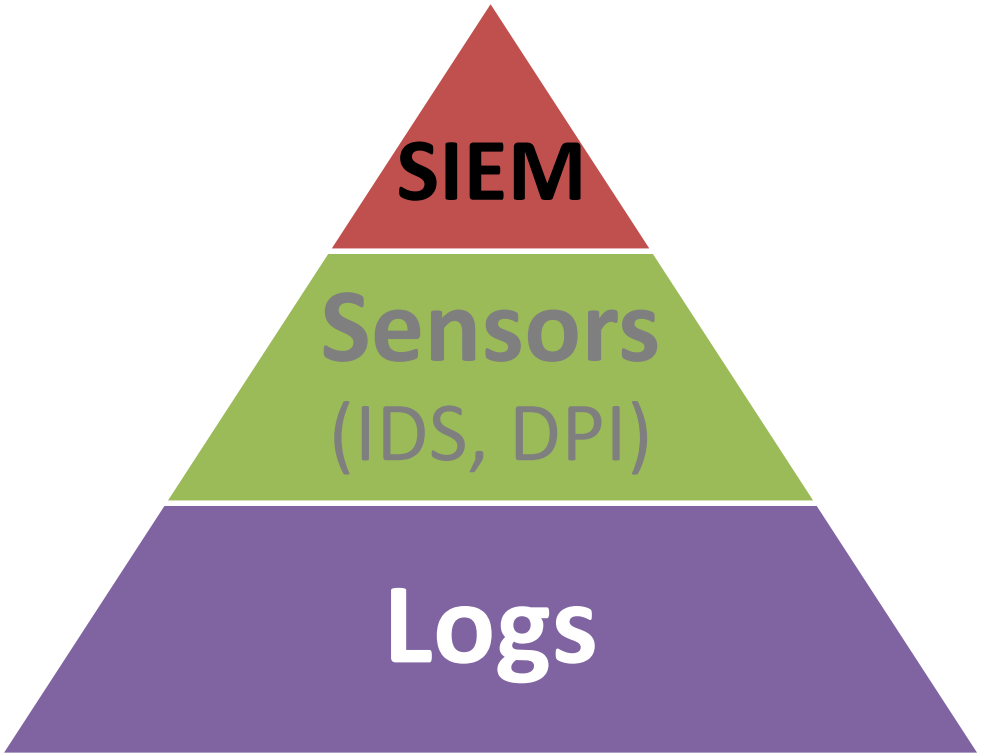


LOG MANAGEMENT (aujourd'hui)



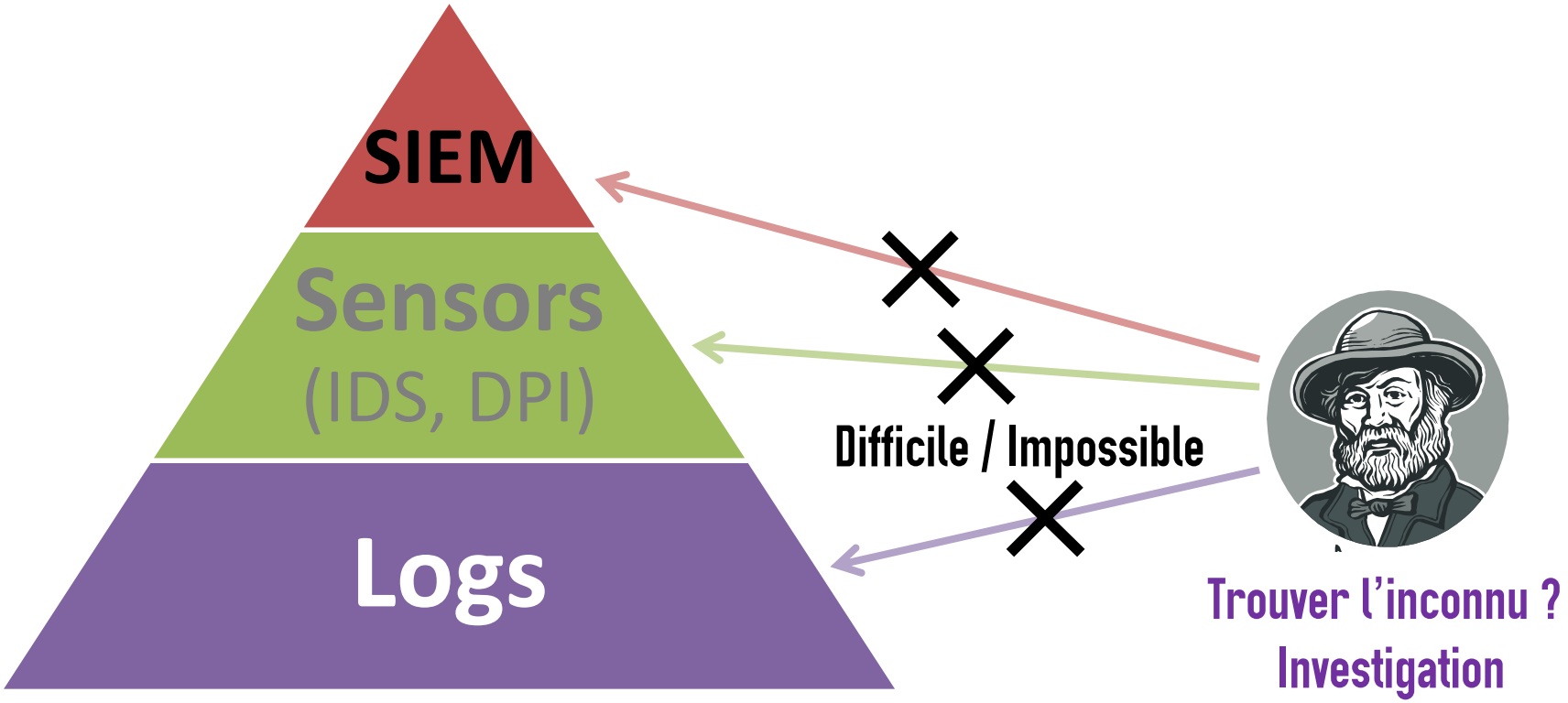
Trouver l'inconnu ?

LOG MANAGEMENT (aujourd'hui)

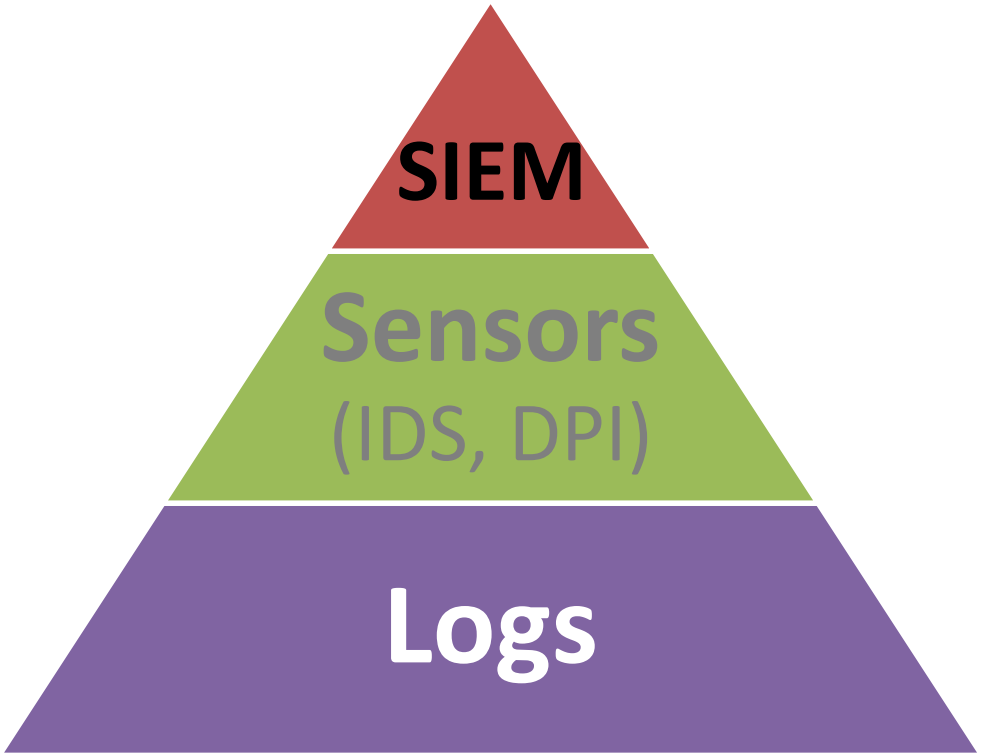


Trouver l'inconnu ?
Investigation

LOG MANAGEMENT (aujourd'hui)

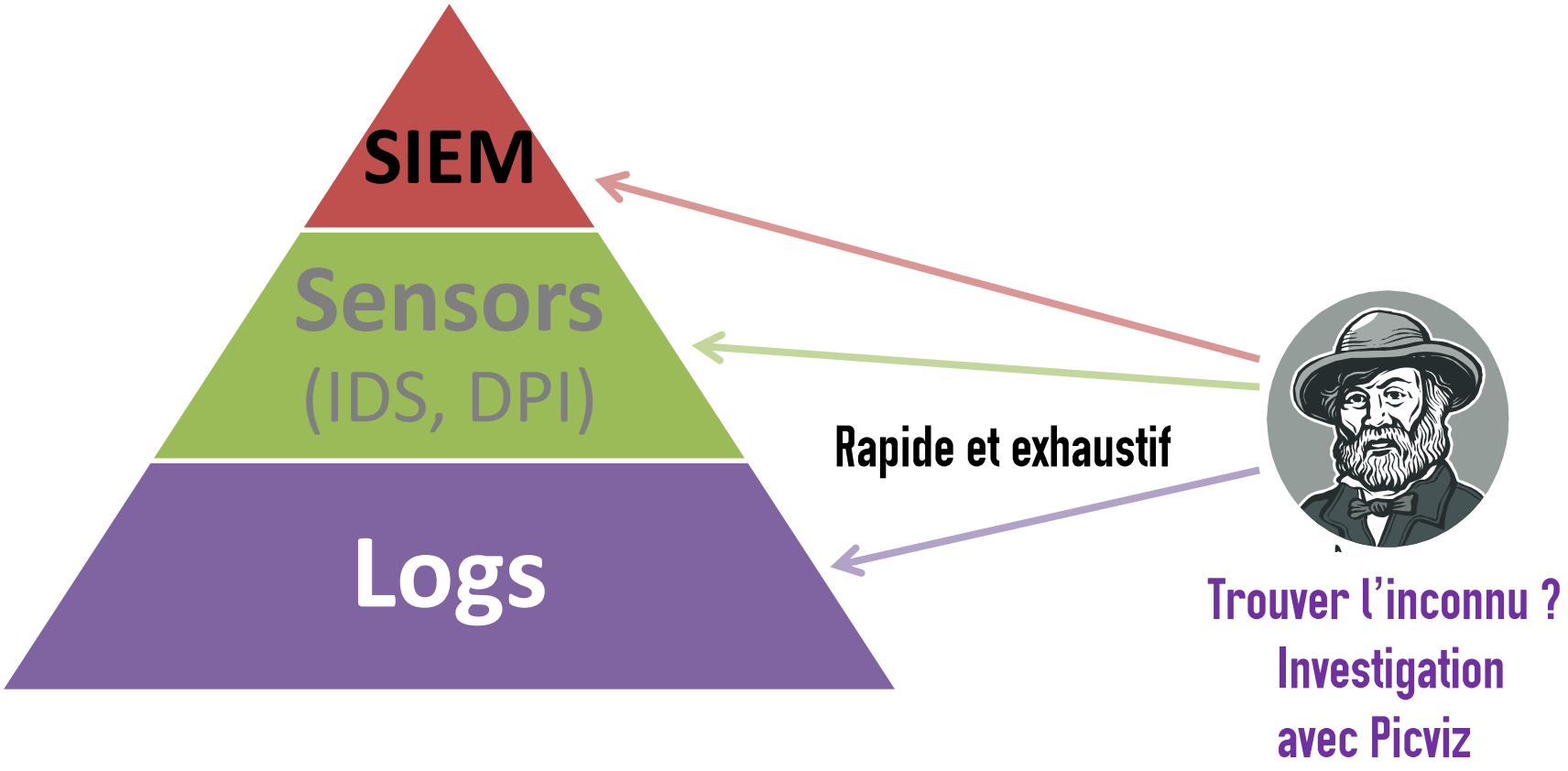


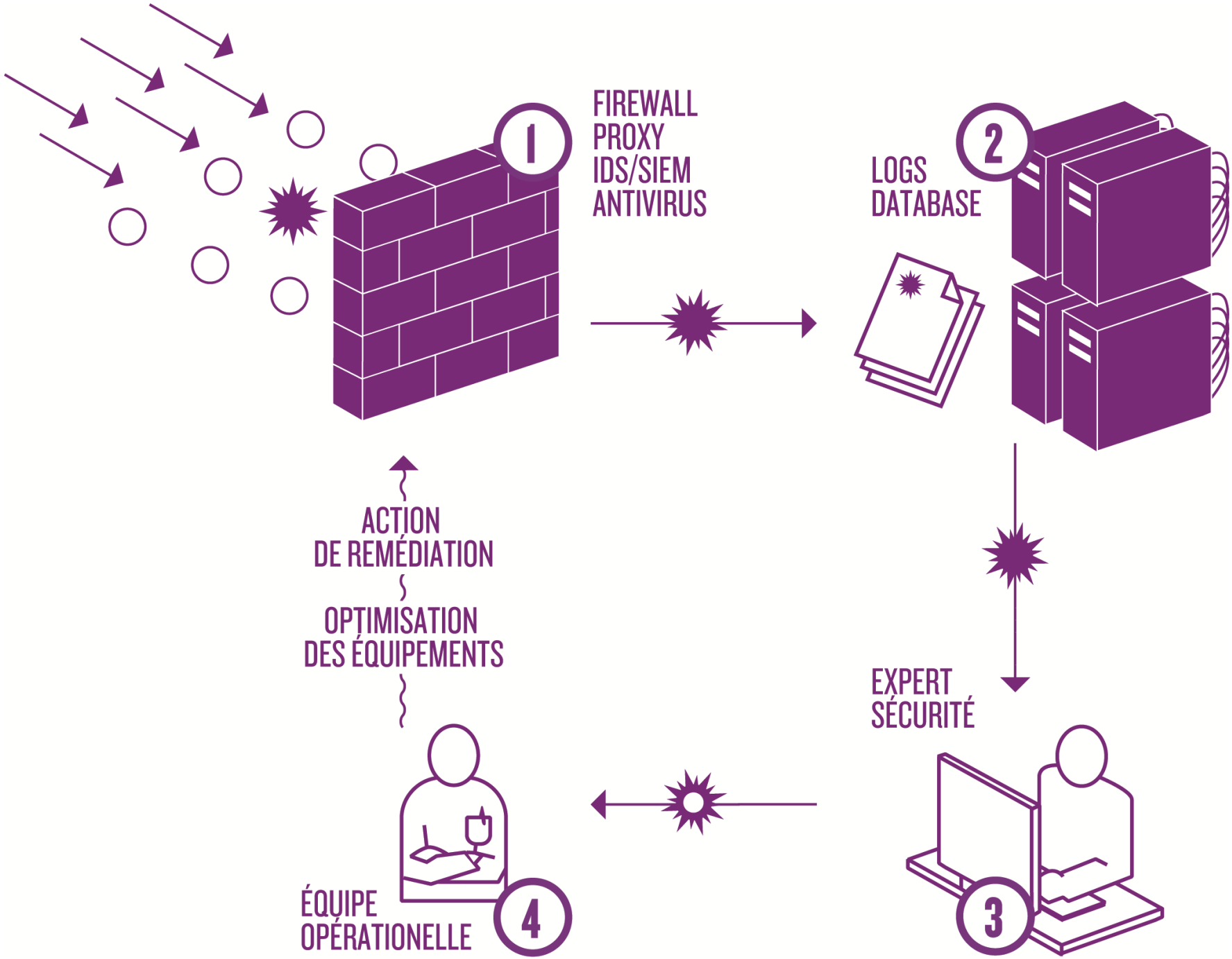
LOG MANAGEMENT (aujourd'hui)



Trouver l'inconnu ?
Investigation
avec Picviz

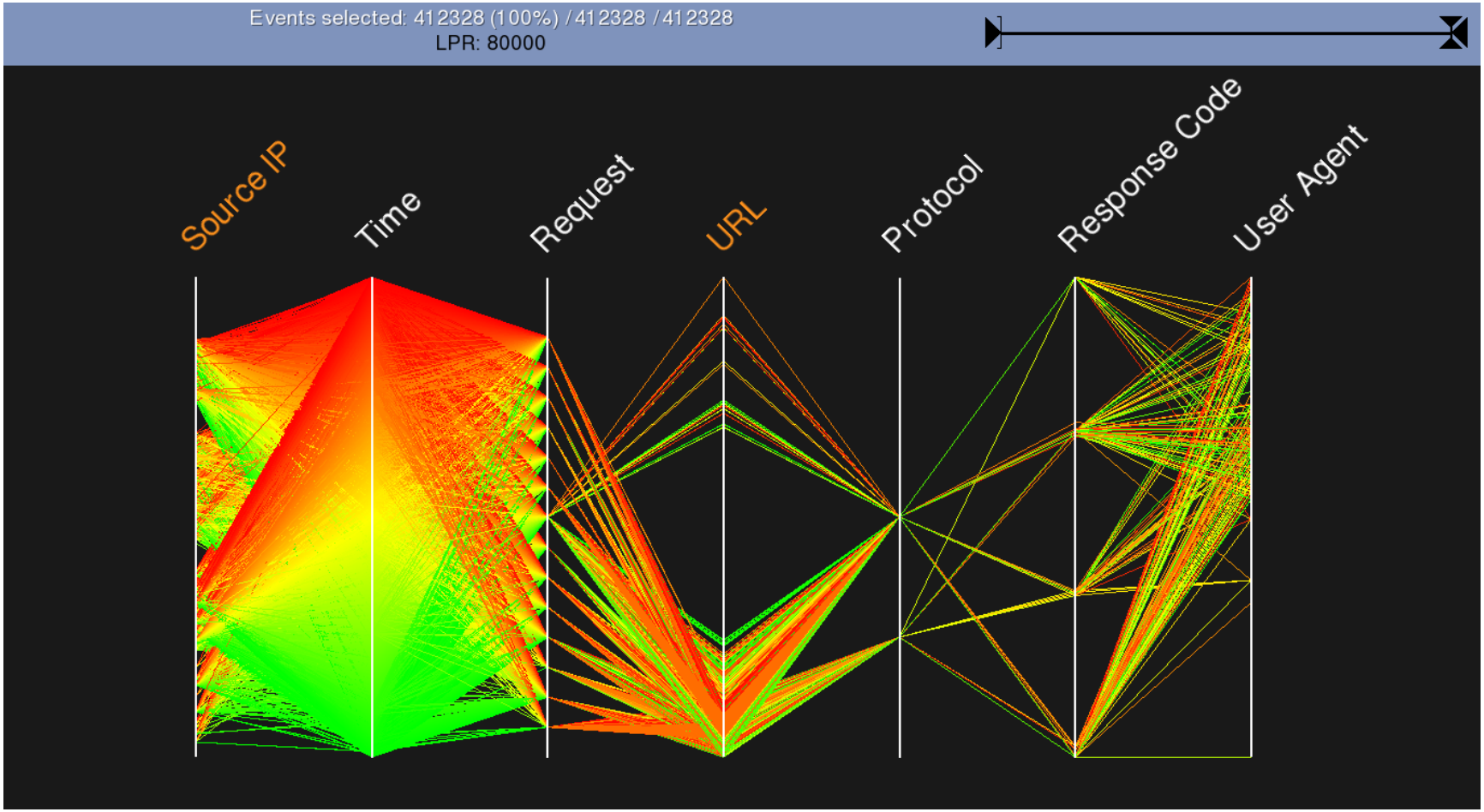
LOG MANAGEMENT (aujourd'hui)




1
FIREWALL
PROXY
IDS/SIEM
ANTIVIRUS
2
LOGS
DATABASE
EXPERT
SÉCURITÉ
3
ÉQUIPE
OPÉRATIONELLE
4
OPTIMISATION
DES ÉQUIPEMENTS
ACTION
DE REMÉDIATION

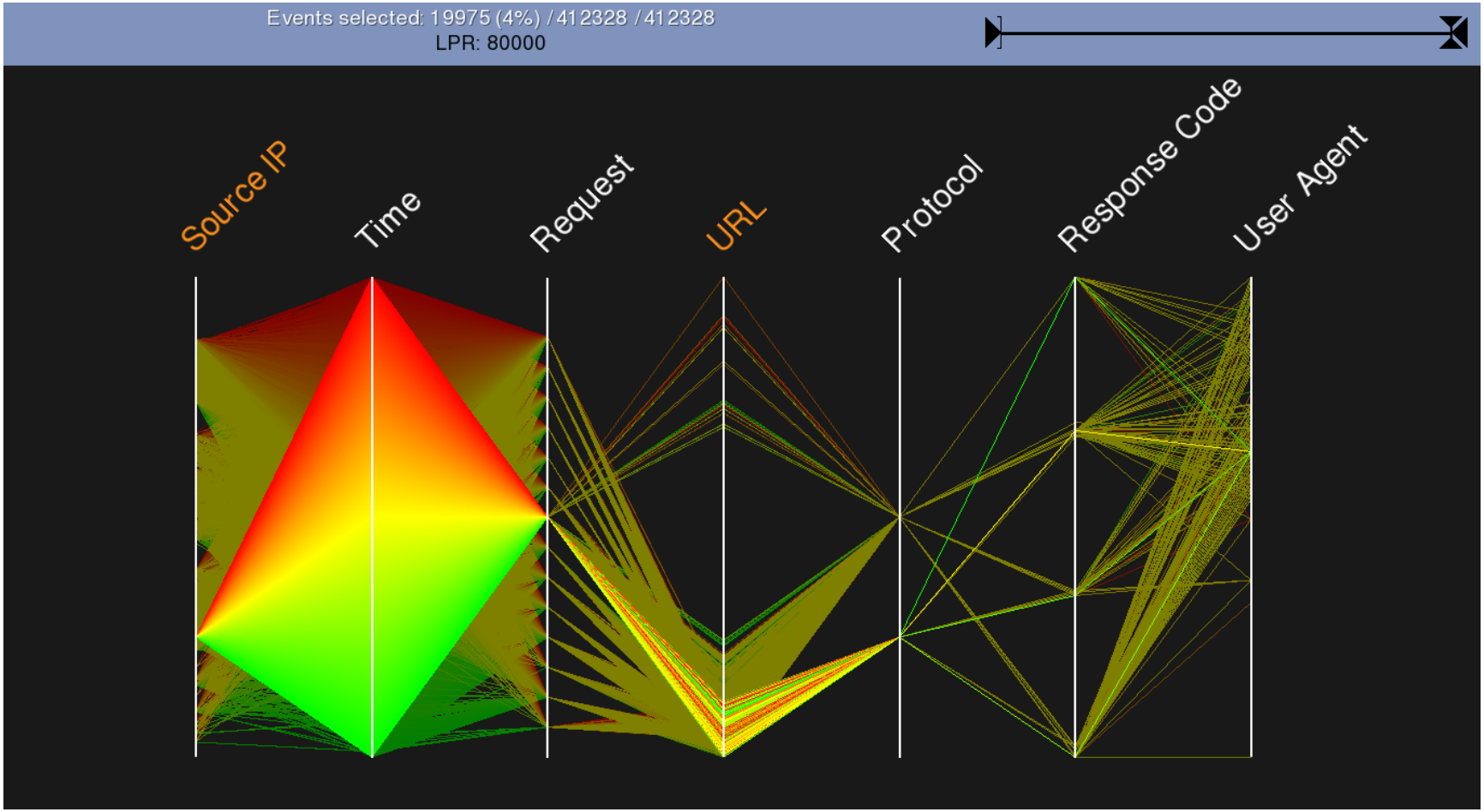
Fichier de log d'un serveur Apache

Vue globale ...



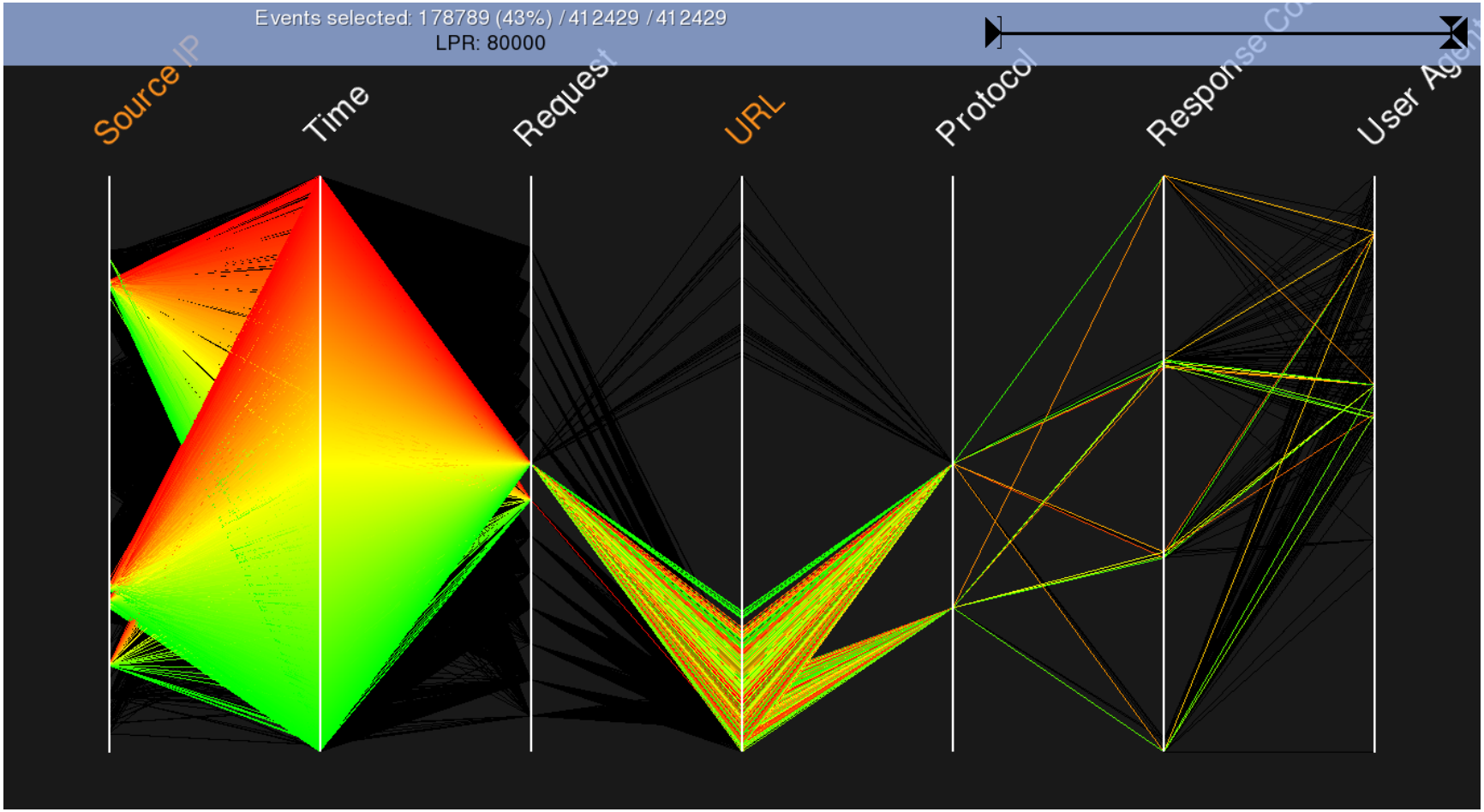
Fichier de log d'un serveur Apache

Robot Twiceler



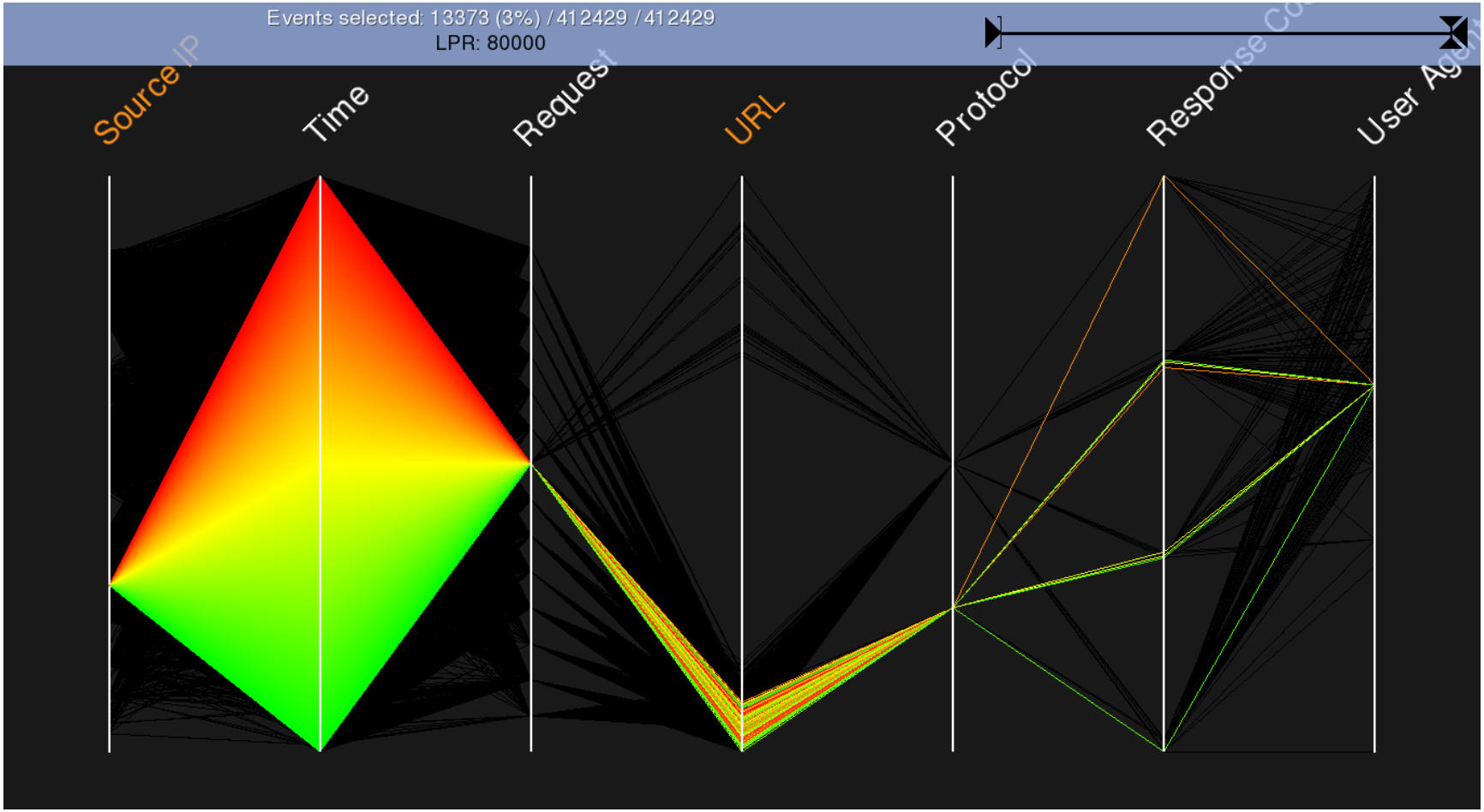
Fichier de log d'un serveur Apache

Trouver les robots automatiquement depuis l'User Agent



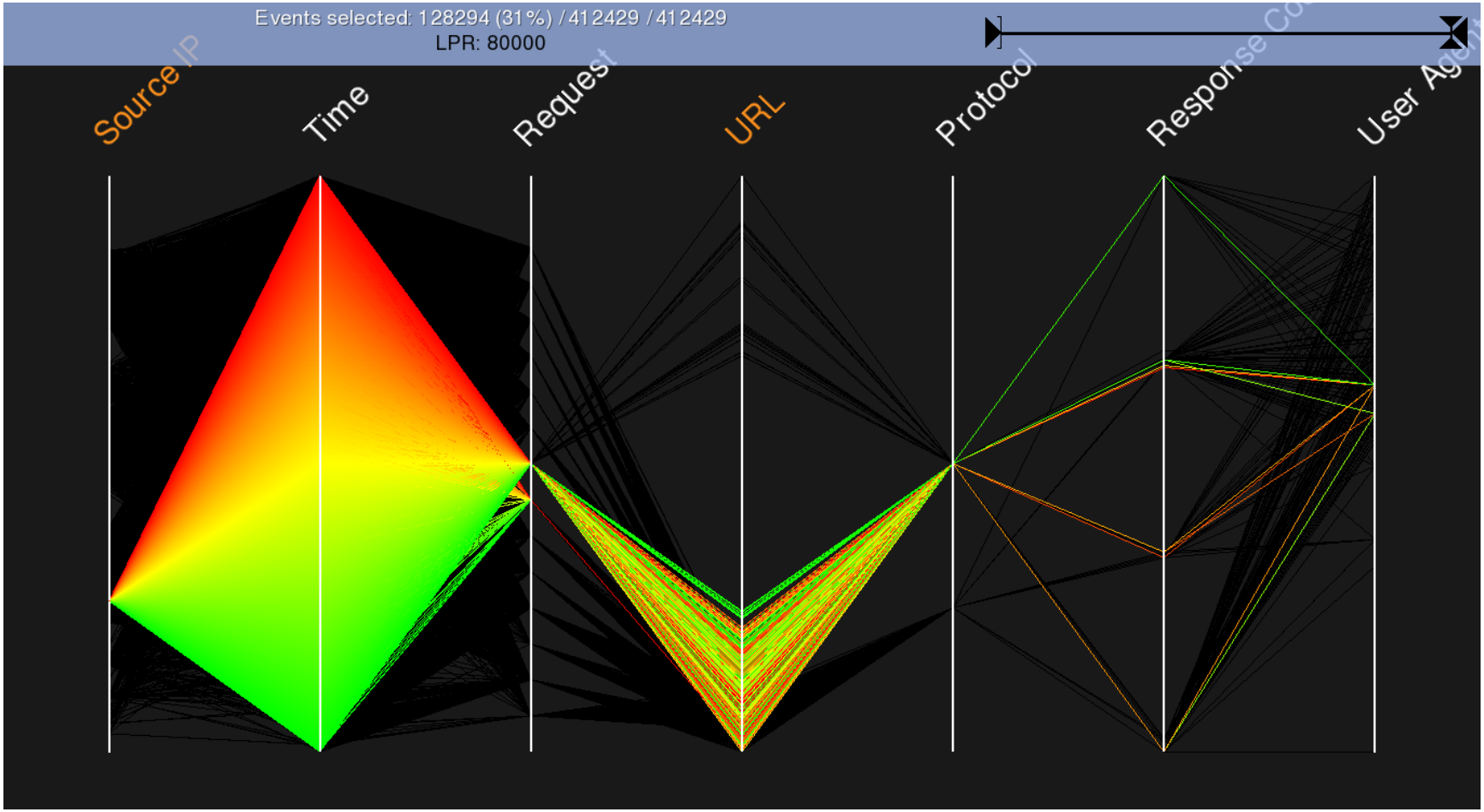
Fichier de log d'un serveur Apache

Yahoo



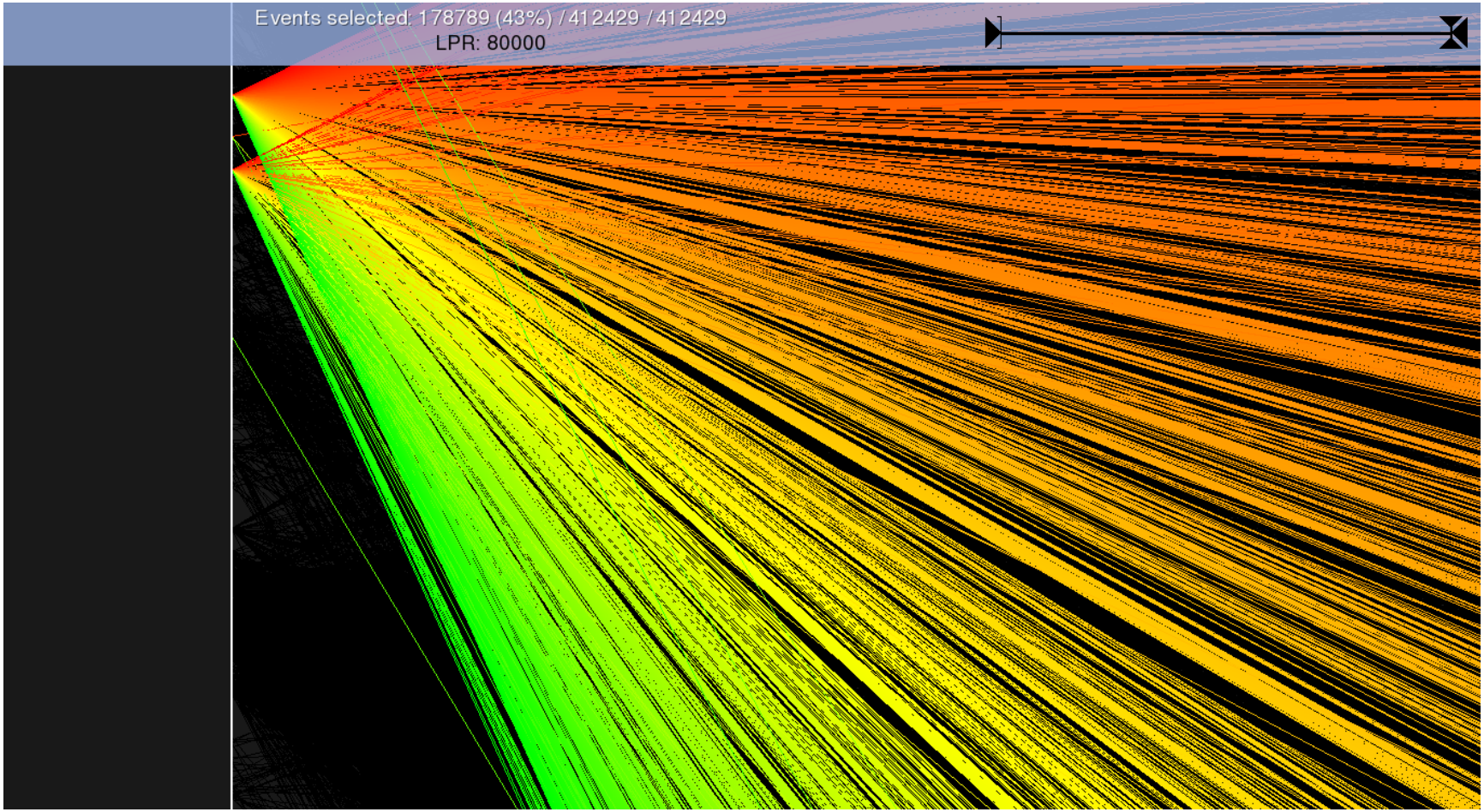
Fichier de log d'un serveur Apache

Google



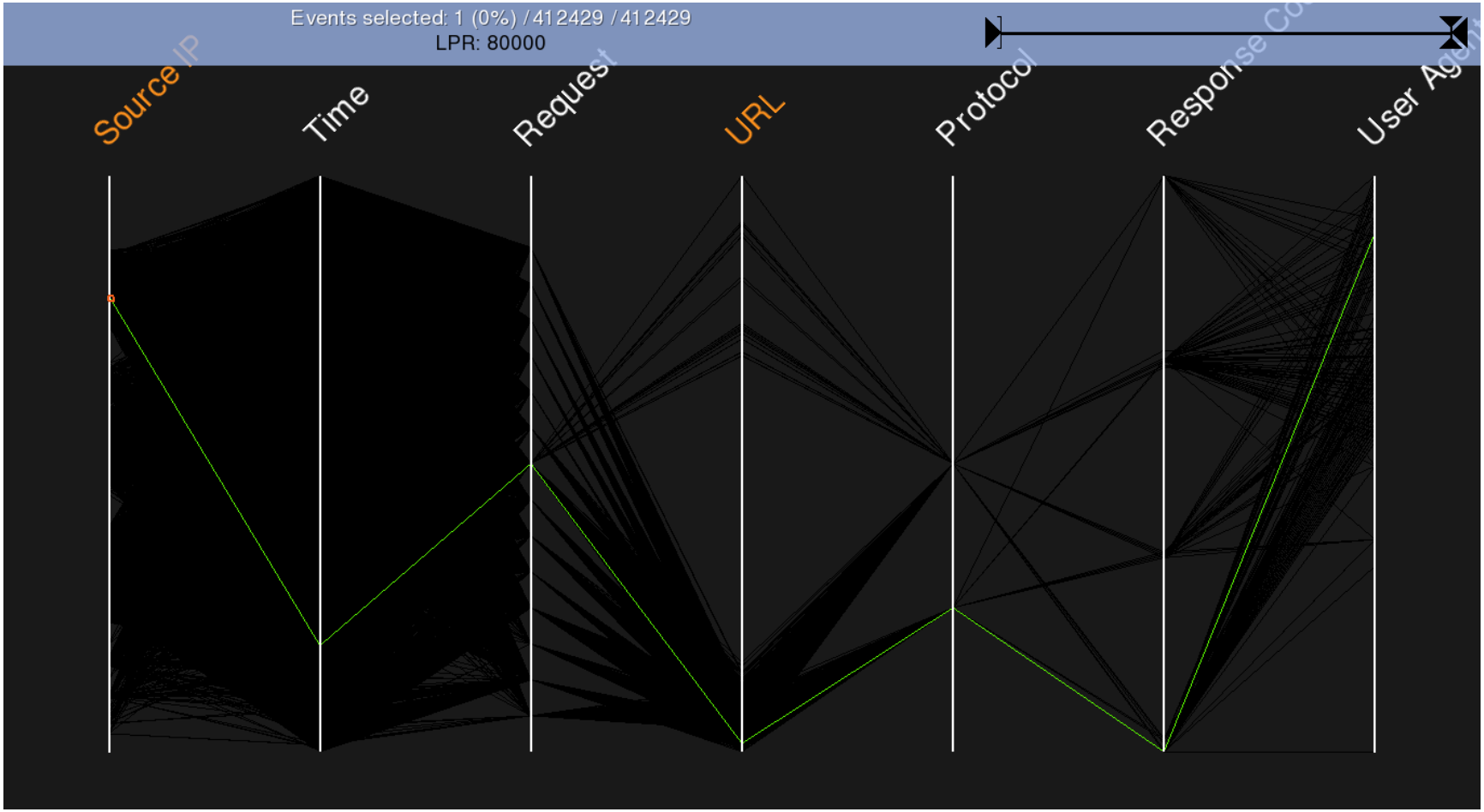
Fichier de log d'un serveur Apache

Zoomer sur l'IP Source ...



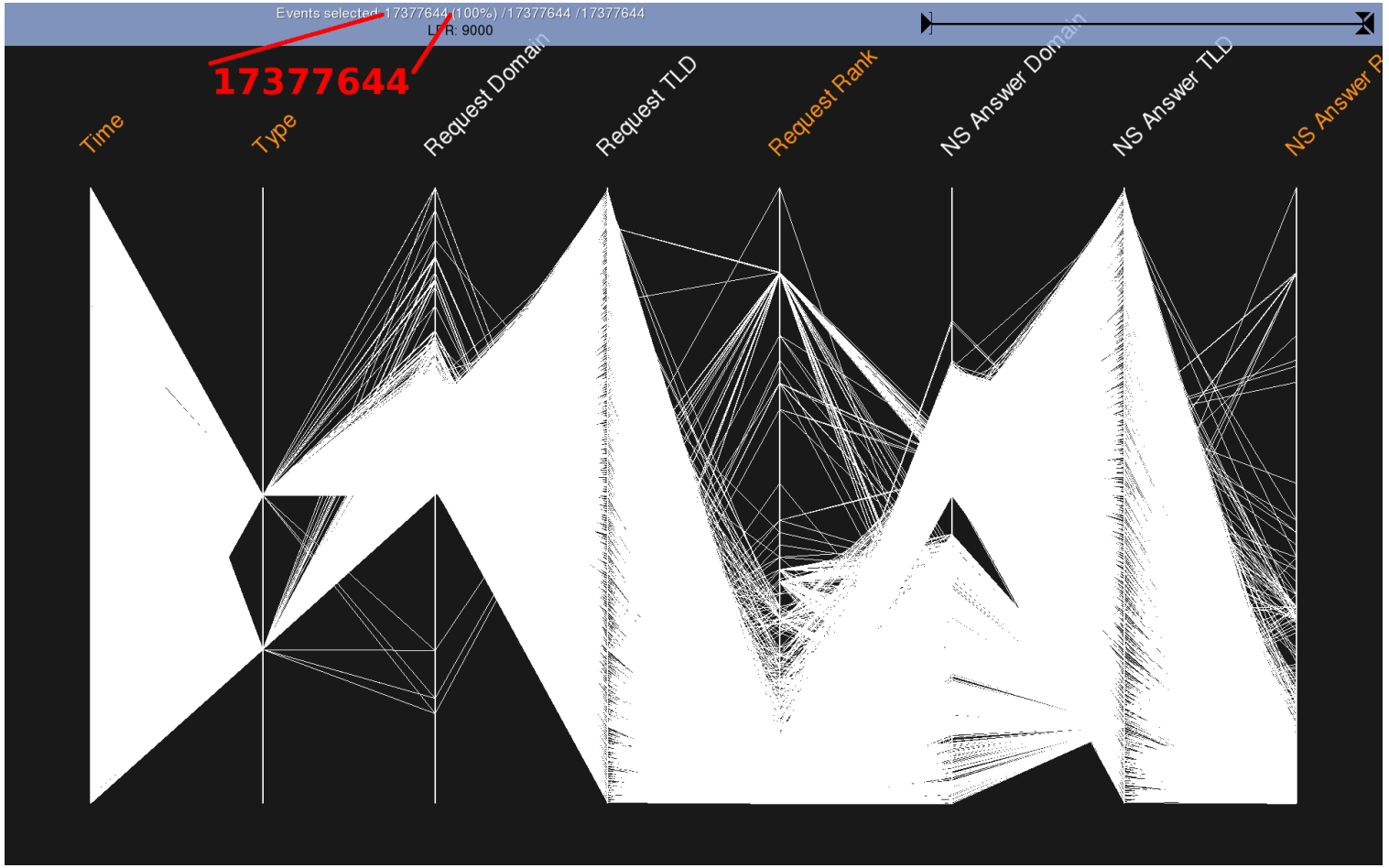
Fichier de log d'un serveur Apache

202.96.51.149 22/Jun/2007:04:25:14 GET /files/gvglue.py HTTP/1.0 200 msnbot/1.0 (+http://search.msn.com/msnbot.htm)



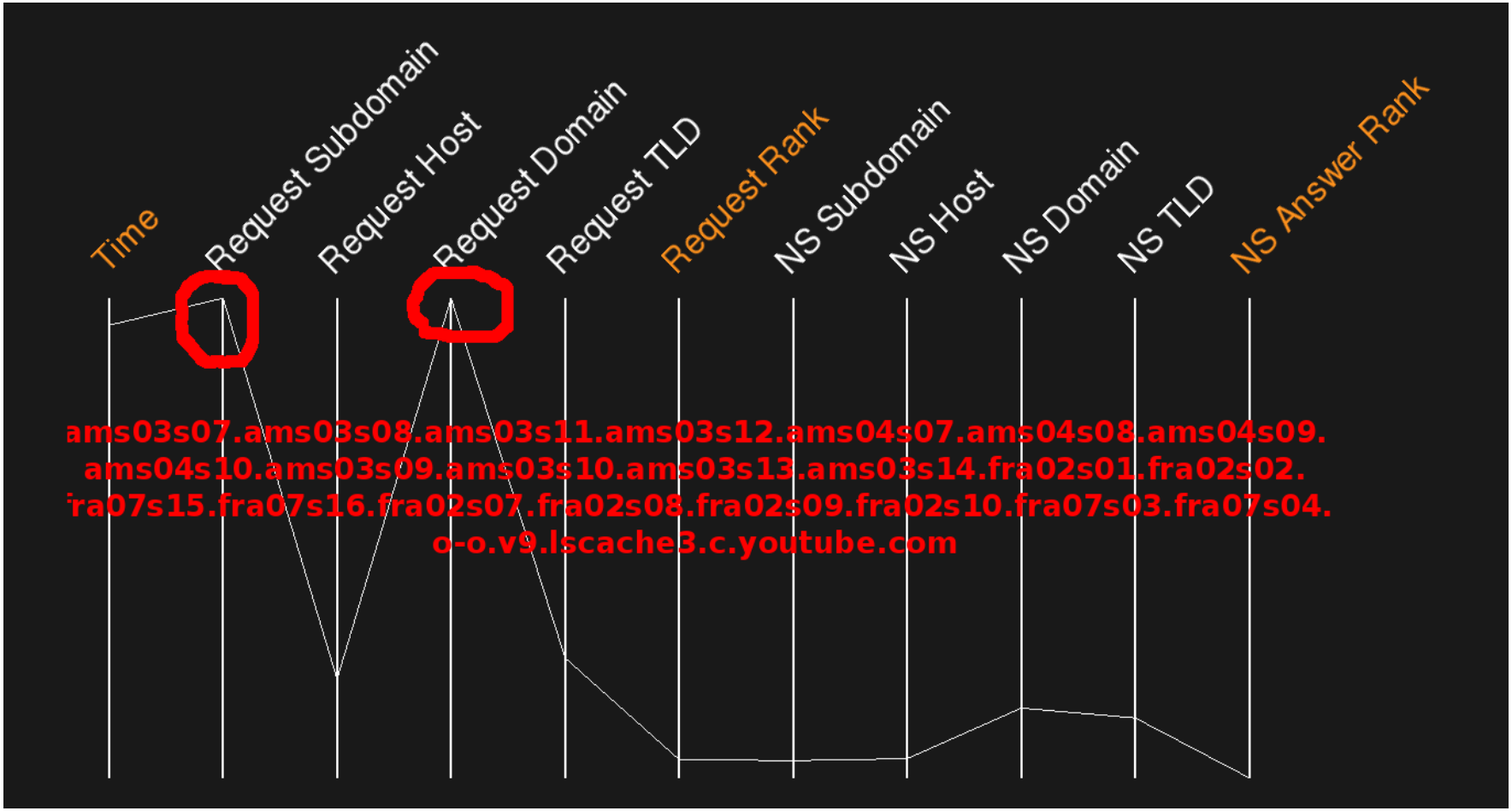
Passive DNS du Luxembourg

Vue globale ...



Passive DNS du Luxembourg

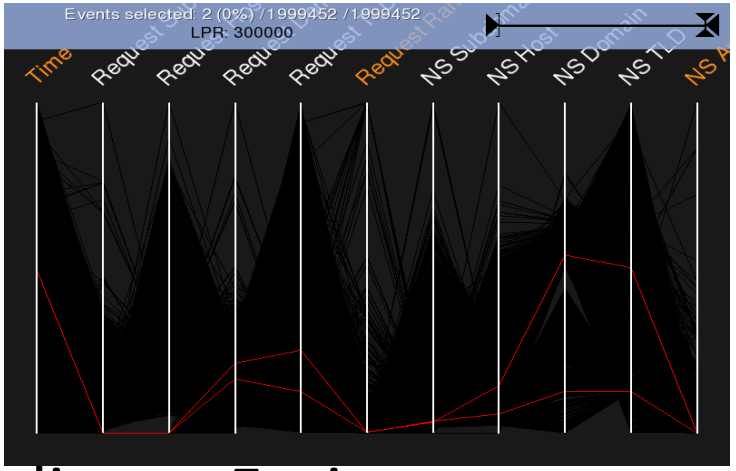
Problème DNS avec Youtube?



Chercher ZEUS

- Utiliser la regex du CERT PL

[a-z0-9]{32,48}\.(ru|com|biz|info|org|net)



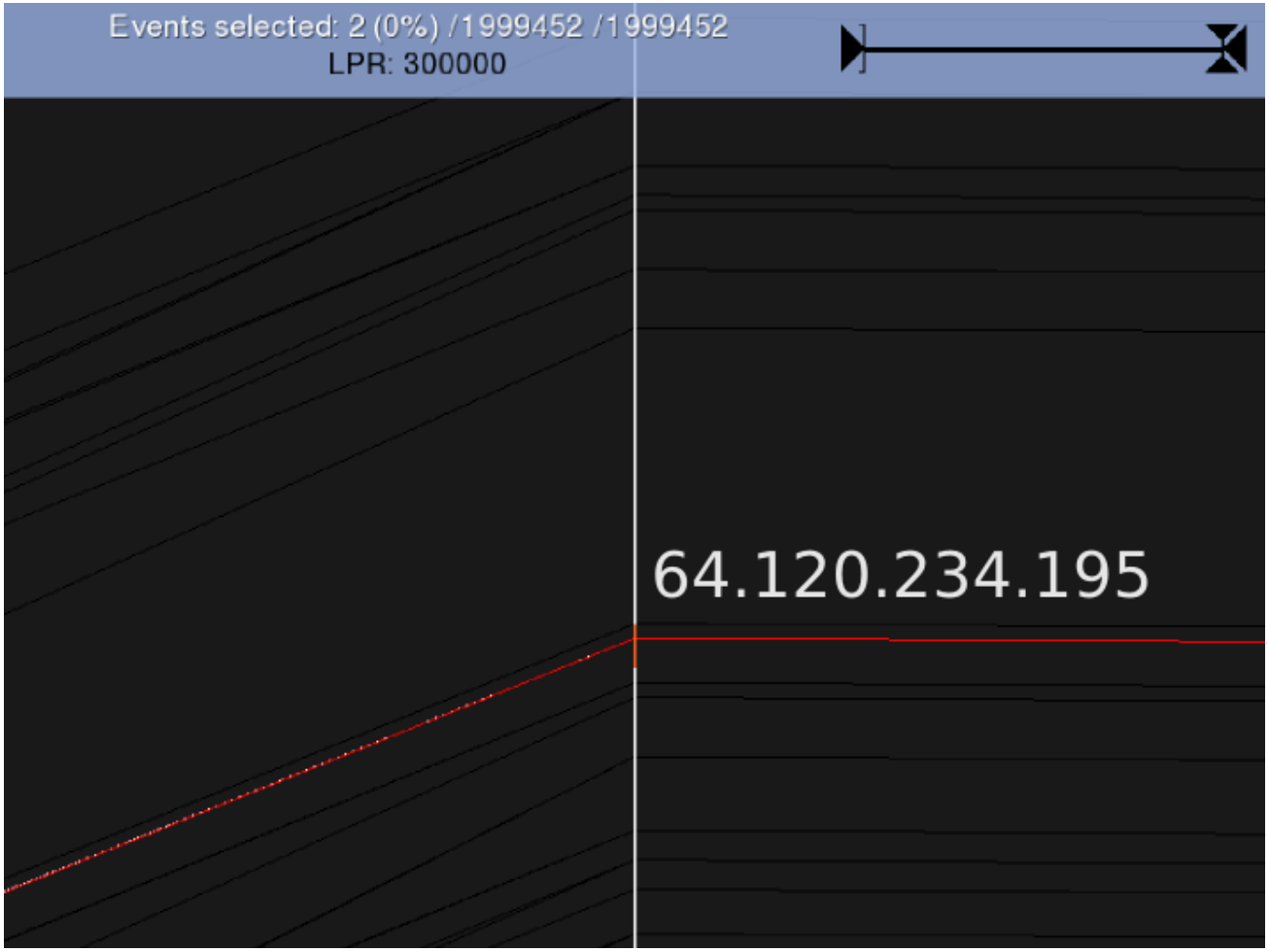
- On récupère des domaines supers:

cg79wo20kl92doowfn01oqpo9mdieowv5tyj.com

eef795a4eddaf1e7bd79212acc9dde16.net

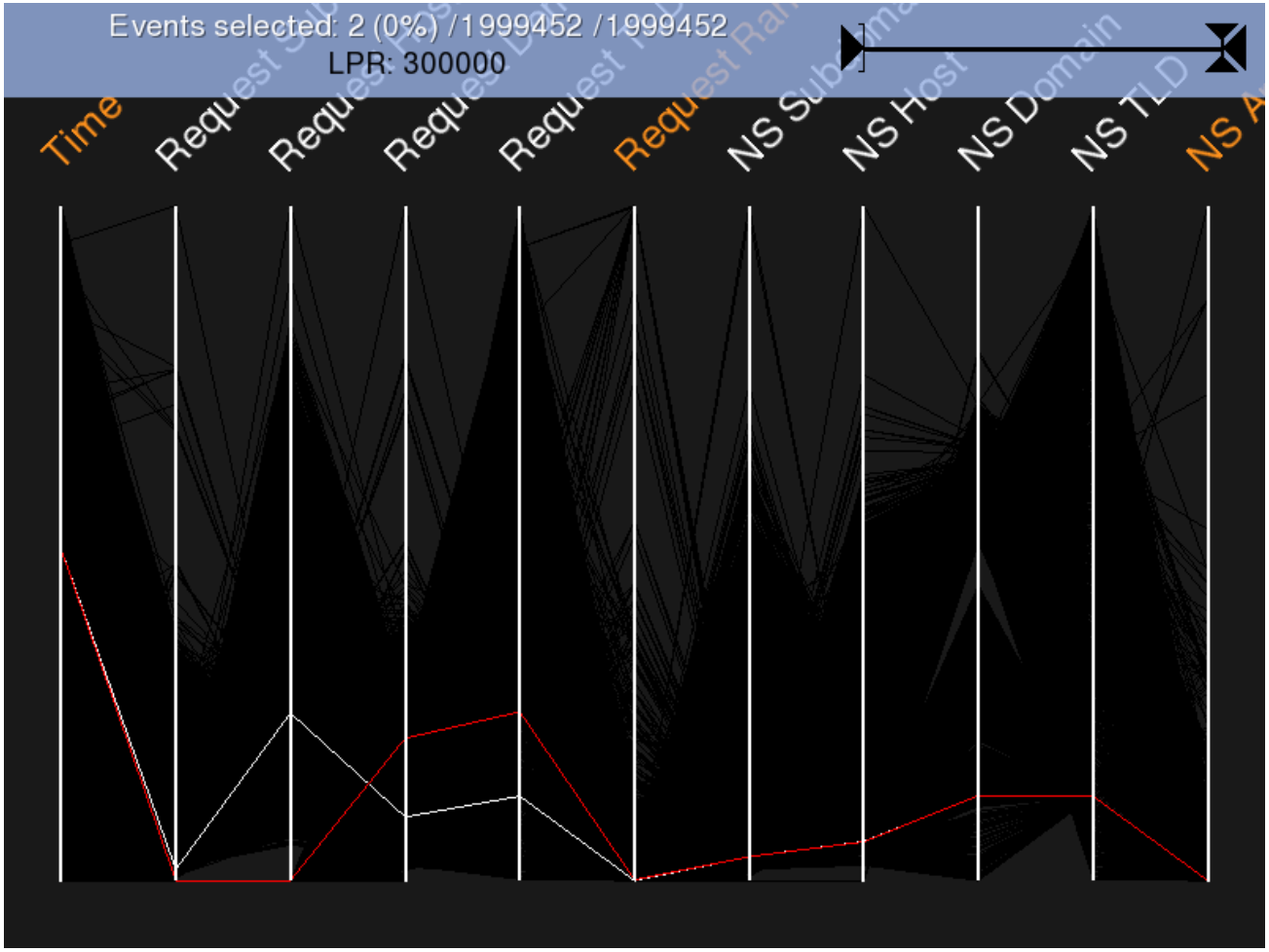
- Mieux : on a le profile visuel nous permettant de trouver ceux qui ne correspondent pas à la regex!

Zoom sur NS answer domain



Revenir à la vue globale

Domaine pour la requête : ns2.speed-tube.net



Investigation de ns2.speed-tube.net

- On récupère des domaines non rankés :

  adsforadsense.co.cc;1.0;ns2.speed-tube.net;1.0

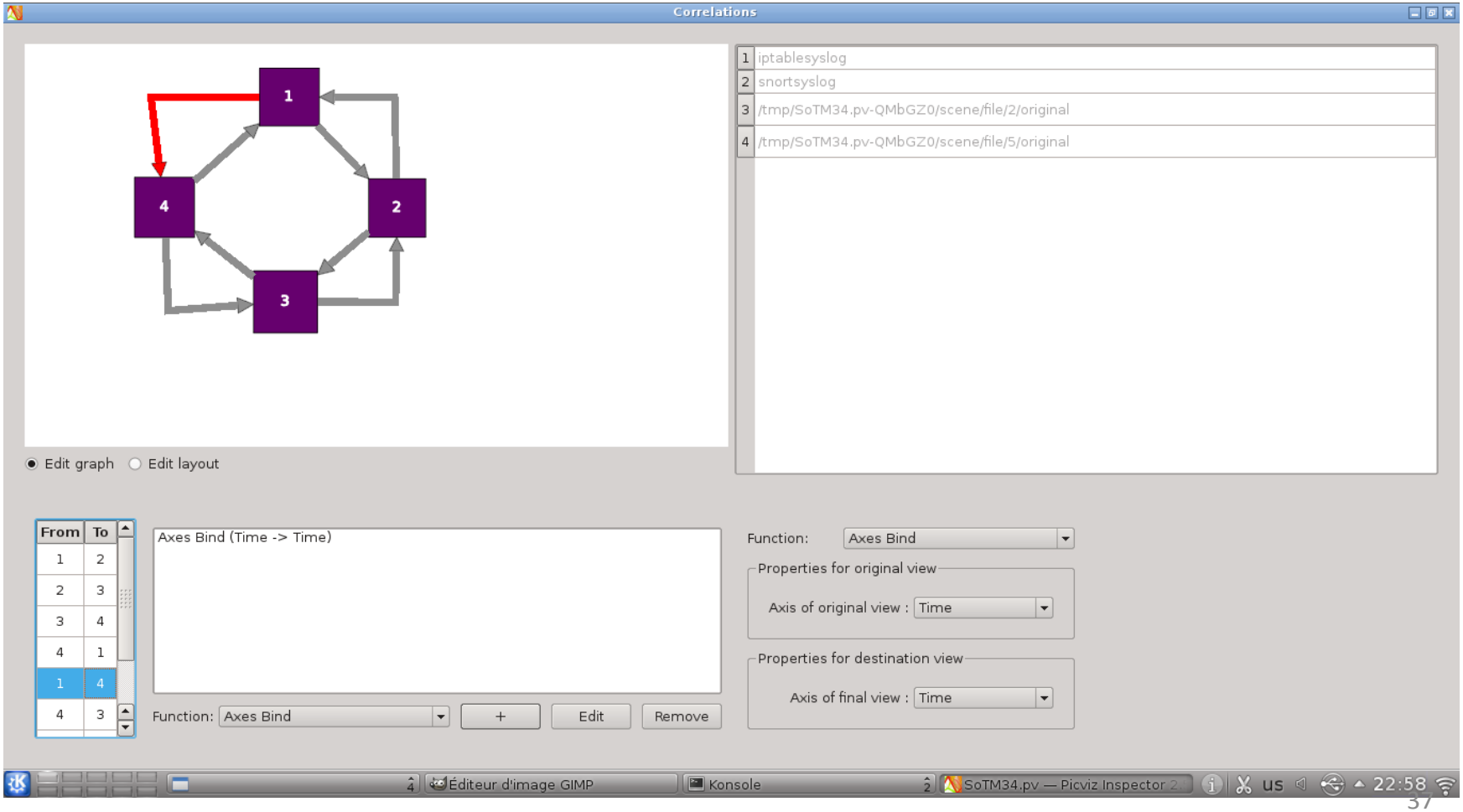
  extra-tube.net;1.0001125221;ns2.speed-tube.net;1.0 ...

- Site malicieux récurrent (reactivé ou en cache) :

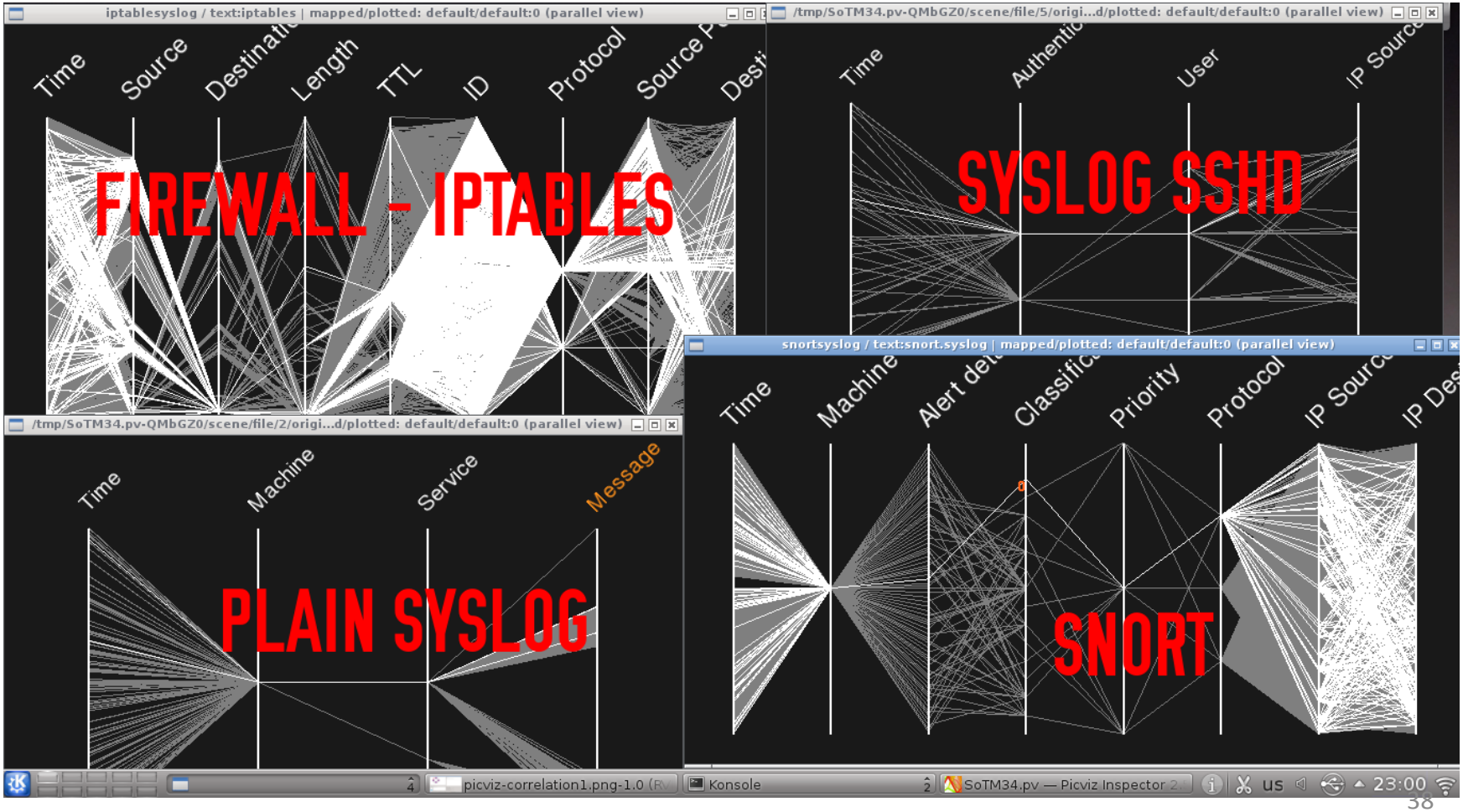
  adsforadsense.co.cc rogue safebrowsing.clients.google.com

  20110315 20110125

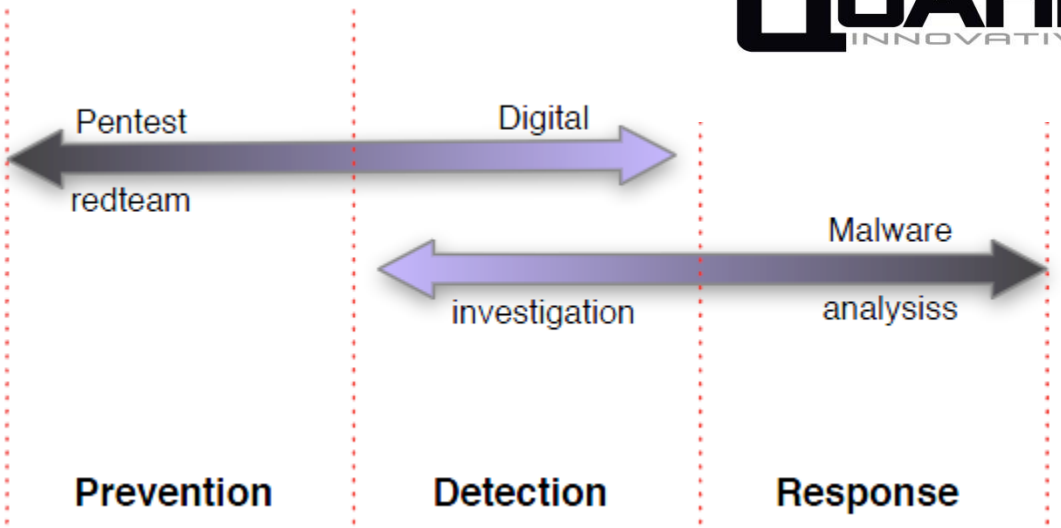
Corrélation Multi-Sources



Corrélation Multi-Sources



Collaboration



Quarkslab

In depth pentesting

Usual services

Automatic pentest
Automatic detection

Picviz Labs

In depth detection

Eve : un scanner des origines

- Synthèse massive factuelle des surfaces d'attaque
- Un scanner scalable
  - Conçu pour scanner un pays
  - Sépare le scan de l'analyse
- Vision temporelle

QUARKSLAB
INNOVATIVE SECURITY

Questions ?