OSSIM
Open Source Security Information Management

Michaël BLANC
EFREI – M2 - SI 1

Le 6 Décembre 2007 :

Les systèmes informatiques de laboratoires scientifiques américains ont été les cibles d'attaques sophistiquées ayant permis une intrusion. (Oak Ridge National Laboratory et Los Alamos National Laboratory)

Après avoir a priori pénétré une base de données contenant des informations personnelles sur les chercheurs, les pirates ont pu concevoir des emails de phishing accompagnés de programmes malveillants, vraisemblablement des chevaux de Troie.

Source : crn.com

Présentation de la solution OSSIM

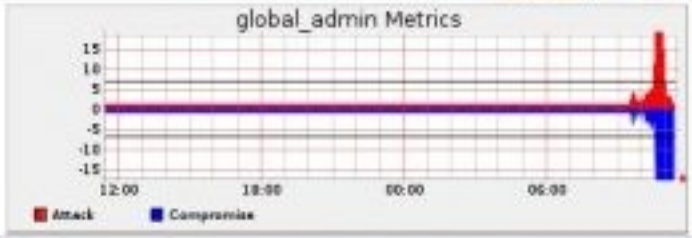
- OSSIM :
  - Gestion des incidents opérationnels de sécurité
  - Collection d'outils visant à aider les administrateurs réseau à la sécurité informatique, la détection d'intrusion et de prévention.
  - Identifier la nature des risques et limiter leurs fréquences et leurs conséquences
- Avantage :
  - Prix (Open source - Licence BSD)
  - Non-intrusif
  - Information organisationnelles
- Concurrents :
  - Micromuse, NetForensics, Self-Defending Network

- Composants d'OSSIM :
  - P0f, détection et l'analyse des changement des OS
  - Arpwatch, détection des anomalies (adresse MAC)
  - Ntop, base de données de comportement
  - Pads, détection des anomalies de service
  - Nessus, évaluation de la vulnérabilité
  - Snort, détection d'intrusion (IDS)
  - Osiris, détection d'intrusion (HIDS)
  - Tcptrack, corrélation des données de session
  - Spade, statistiques de détection des anomalies
  - Nagios, surveillance de la disponibilité des services
  - Moteur de corrélation et règles séquentielles

Les alertes

OSSIM

[Last Day][Last Week][Last Month][Last Year]



Global

Global	Max C date	Max C	Current C
GLOBAL SCORE	2005-03-07 10:45:00	576	499

Global	Max A date	Max A	Current A
GLOBAL SCORE	2005-03-07 10:40:00	103	4

Networks

Network	Max C date	Max C	Current C
desarrollo	2005-03-07 11:20:00	0	0
dmz	2005-03-07 11:20:00	0	0
interna	2005-03-07 10:45:00	575	521
ossim	2005-03-07 10:45:00	570	495

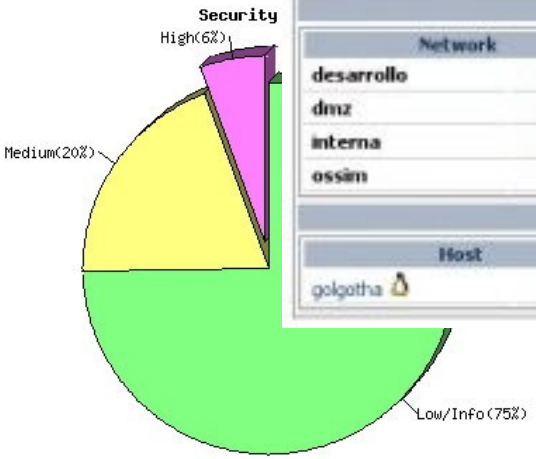
Network	Max A date	Max A	Current A
desarrollo	2005-03-07 11:20:00	0	0
dmz	2005-03-07 11:20:00	0	0
interna	2005-03-07 10:45:00	40	0
ossim	2005-03-07 10:45:00	39	0

Hosts

Host	Max C date	Max C	Current C
golgotha	2005-03-07 10:45:00	579	495

Host	Max A date	Max A	Current A

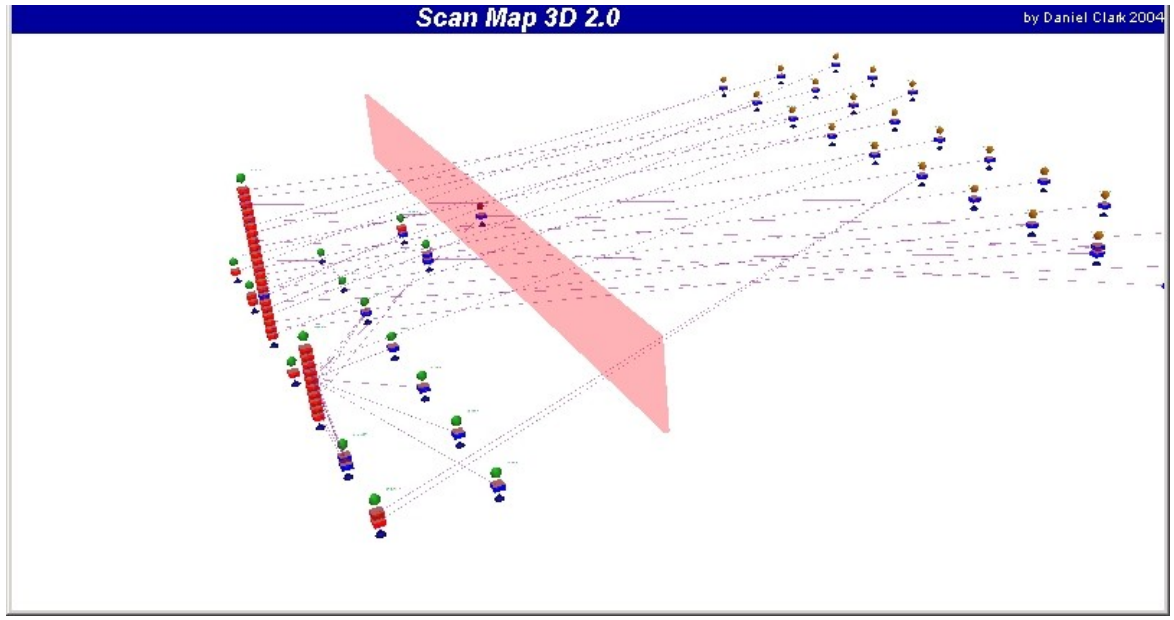
Repartition of the level of th



[Next host : 192.168.2.203]

List of open ports :

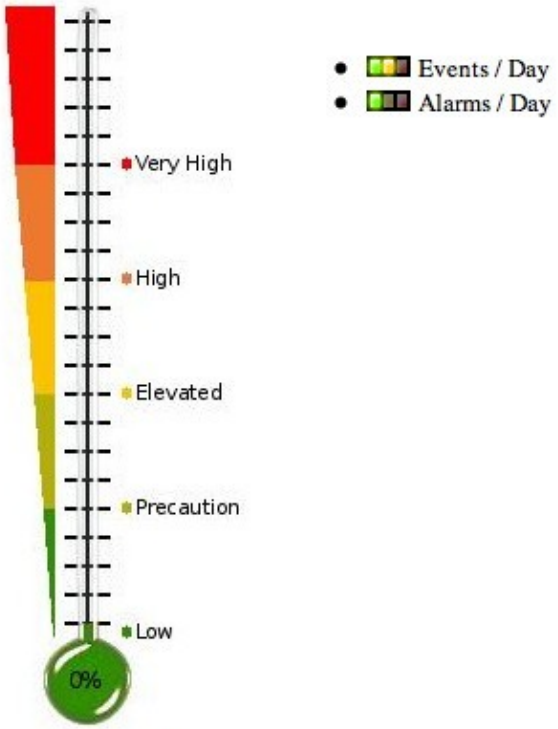
- http (80/tcp) (Security hole found)
- ppp (3000/tcp) (Security warnings found)
- rda (630/tcp) (Security hole found)
- general/udp (Security notes found)
- general/icmp (Security warnings found)
- unknown (33100/udp) (Security warnings found)
- ssh (22/tcp) (Security notes found)
- general/tcp (Security warnings found)
- ftp (21/tcp) (Security notes found)
- shilp (2049/udp) (Security warnings found)
- rda (630/udp) (Security notes found)
- sunrpc (111/udp) (Security notes found)
- unknown (32892/tcp) (Security notes found)
- nfs (2049/tcp) (Security warnings found)
- servstat (633/tcp) (Security notes found)
- rpcbind (111/tcp) (Security notes found)



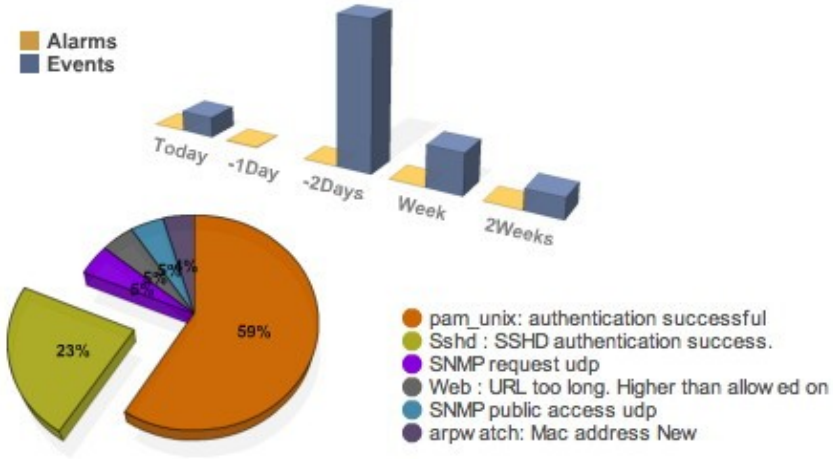
Reporting

OSSIM

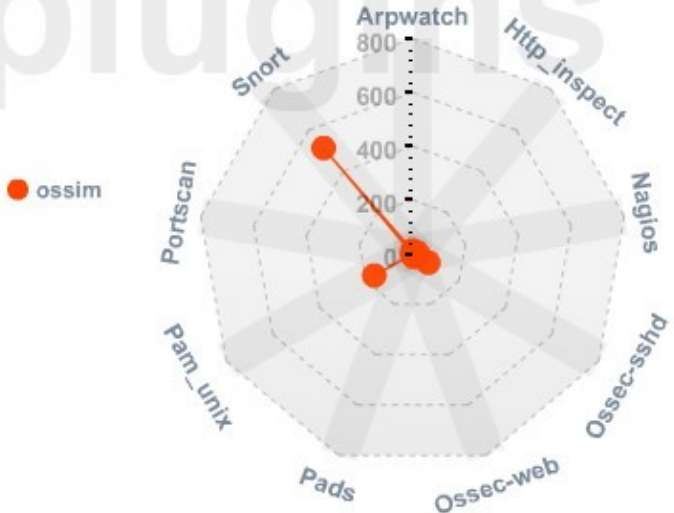
Service Level



Alarms / Events



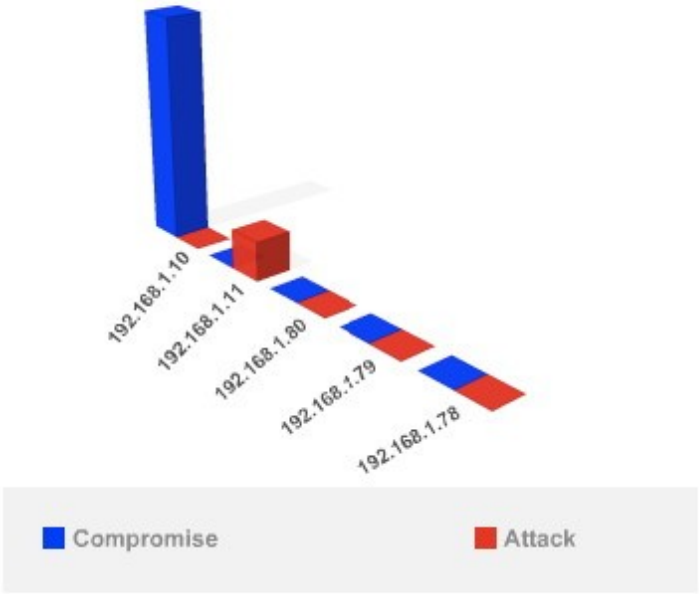
Events by Sensor/Plugin



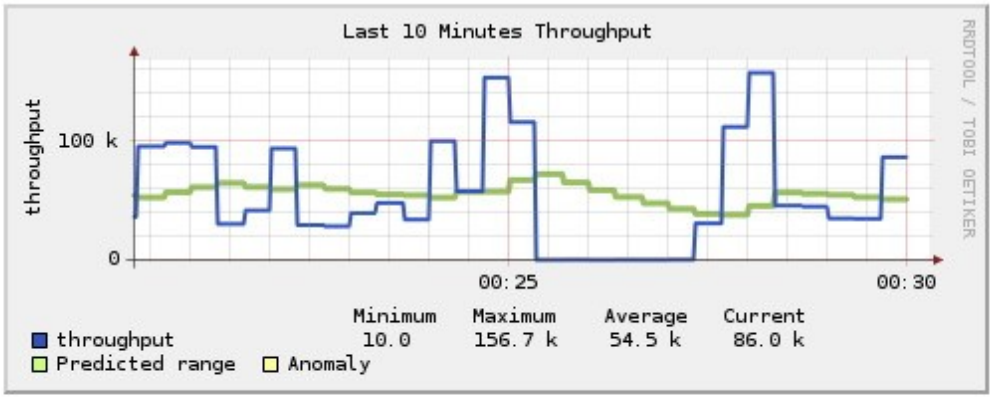
Availability

*Note: Please, configure Nagios and update this panel to view a snapshot of your network.

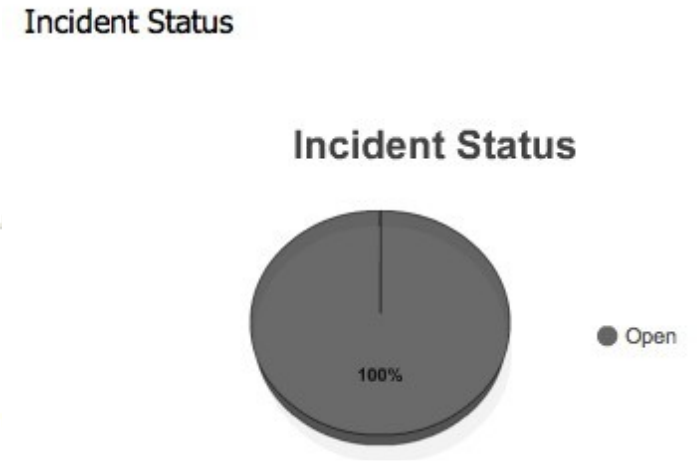
Top 10 hosts risk



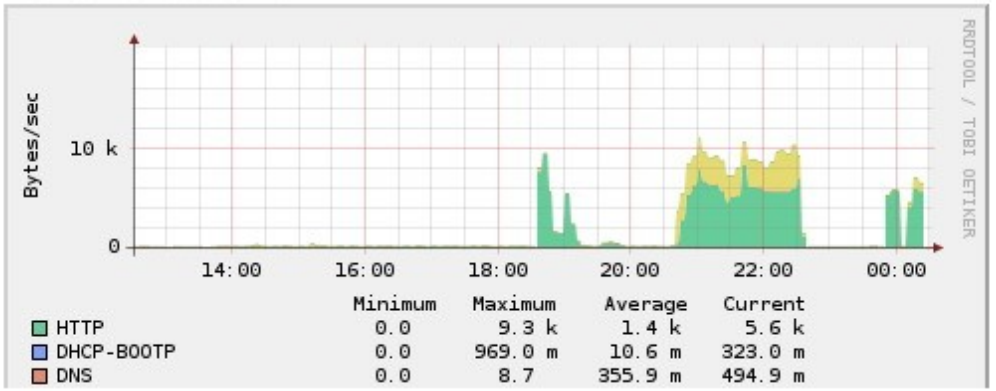
Throughput



Incident Status



Backbone net traffic 12h



Exemple : SFR

- Problèmatique :
  - Cartographie de la malveillance
  - Qualification des impacts potentiels ou avérés
  - Infrastructure complexe (20 000 équipements)
  - Taille des fichiers de journalisation
- Résultats :
  - 10 000 000 d'évenement -> 10 alertes à traiter
  - Corrélations multiples avec des règles séquentielles
  - Repporting et amélioration du tableau de bord
- Evolutions :
  - Logs d'antivirus
  - Logs de logiciels de filtrage
  - Autre moteur de correlation (Data mining)

Source : 01 Réseaux

Merci de votre attention