

Visualisation appliquée à la détection d'intrusions

Pierre Chifflier Sébastien Tricaud

INL
101/103 Bvd MacDonald
75019 Paris, France

Paris, OSSIR 2008



Sommaire

- 1 Introduction aux IDS
 - Petit tour de la détection d'intrusions
- 2 Introduction à la visualisation
 - Trois points à retenir
 - Représenter l'information
 - Exemples
- 3 Méthodologie
 - Prérequis
 - Architecture
 - Classification
- 4 Exemple de représentation
- 5 Conclusion

- 1 Introduction aux IDS
 - Petit tour de la détection d'intrusions
- 2 Introduction à la visualisation
 - Trois points à retenir
 - Représenter l'information
 - Exemples
- 3 Méthodologie
 - Prérequis
 - Architecture
 - Classification
- 4 Exemple de représentation
- 5 Conclusion

Qu'est-ce que l'IDS ?

- IDS pour Intrusion Detection System
- Les gens du marketing l'appellent
 - IPS (!!): Système de prévention d'intrusions¹
 - SIEM : Security Information and Event Management
- On préférera le terme IDS

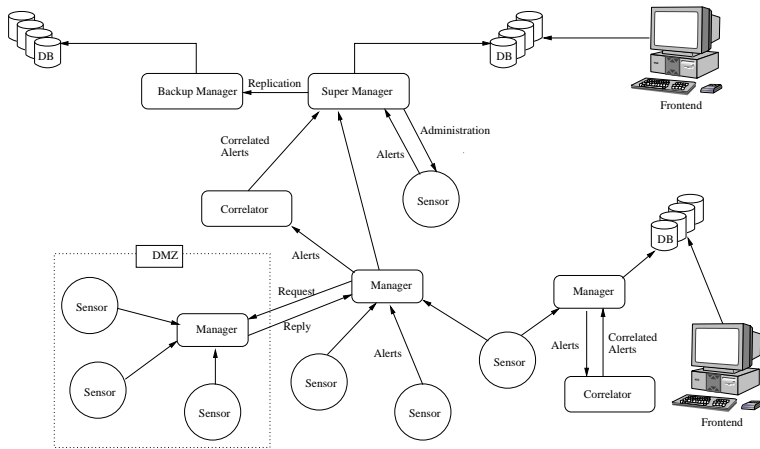
¹ On rappellera que IPS = IDS + contre-mesure

Trois types d'IDS aujourd'hui

- IDS Machines (HIDS) : Peu sensible aux faux positifs
- IDS Réseau (NIDS) : Très sensible aux faux positifs
- IDS Hybride (HbIDS) : Mélange HIDS et NIDS

Petit tour de la détection d'intrusions

Une architecture que l'on aime bien



Différents types de sondes

- Pots de miel : Nepenthes, Honeynet, ..
- Physique : Alarme, ouverture de porte, ..
- Réseau : Snort, Sancp, ..
- Machine : Samhain, Ossec, Prelude LML, ..
- Scanners : Nessus, p0f, nmap, ..

Petit tour de la détection d'intrusions

Prewikka

Prewikka company ltd. Prewikka

Alerts | Heartbeats | Filters admin on

Events

Agents

Tickets

Stats

Users

About

Sensors availability:

31

Filters:
Step:
Tz:
Limit:
2005-04-03 18:36:43
2005-04-03 19:36:43
+01:00

Classification	Source	Target	Sensor
(4024/4065 alerts not shown... expand)			
6 x (spo_bo) Back Orifice Traffic detected			
2 x TFTP GET passed			
5 x WEB-CGI /cgi-bin/ access			
6 x WEB-CGI a1stats a1disp3.cgi directory traversal attempt			
3 x WEB-CGI AltaVista Intranet Search directory traversal attempt			netfilter (avale.prelude-i
3 x WEB-CGI Amaya templates sendtemp.pl directory traversal attempt	62.226.95.44-2788	194.246.202.67-80	snort (avale.prelude-i
7 x WEB-CGI anaconda directory transversal attempt			sshd (avale.prelude-i
3 x WEB-CGI Armada Style Master Index directory traversal			
3 x WEB-CGI auktion.cgi directory traversal attempt			
3 x WEB-CGI calendar_admin.pl arbitrary command execution attempt			
2 x TCP packet dropped (failed)	168.95.5.94-40087	194.246.202.67-80 interface: eth0	netfilter (avale.prelude-i
WEB-MISC robots.txt access (vendor-specific:uri)	64.62.145.13-43750	194.246.202.67-80	snort (avale.prelude-i
DDOS Stacheldraht client check gag (vendor-specific:uri)	192.168.0.1	194.246.202.67	snort (avale.prelude-i
WEB-MISC robots.txt access (vendor-specific:uri)	64.62.145.62-87286	194.246.202.67-80	snort (avale.prelude-i
2 x WEB-MISC robots.txt access	64.242.250.94-83220	194.246.202.67-80	snort (avale.prelude-i
3 x WEB-MISC robots.txt access	65.54.186.94-37895	194.246.202.67-80	snort (avale.prelude-i



- 1 Introduction aux IDS
 - Petit tour de la détection d'intrusions
- 2 Introduction à la visualisation
 - Trois points à retenir
 - Représenter l'information
 - Exemples
- 3 Méthodologie
 - Prérequis
 - Architecture
 - Classification
- 4 Exemple de représentation
- 5 Conclusion

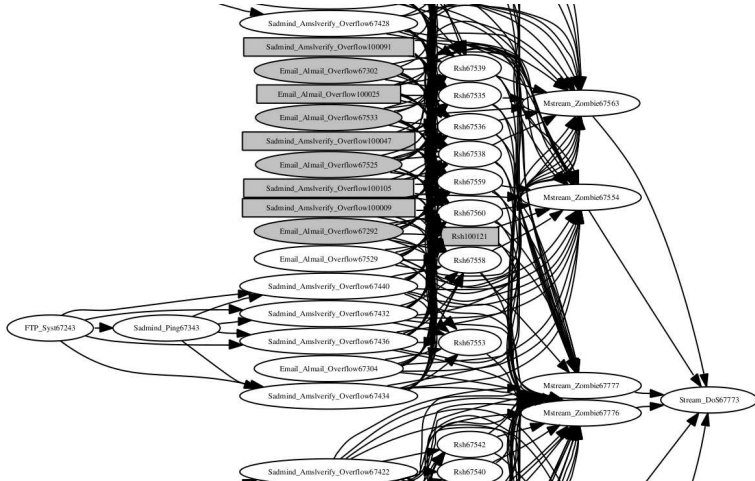
Trois points à retenir

Le visualisation, kesako?

- Un façon (in)utile de représenter l'information
- Permettre l'exploitation de données rapidement
- Se concentrer sur l'essentiel (et se faire avoir sur le détail)

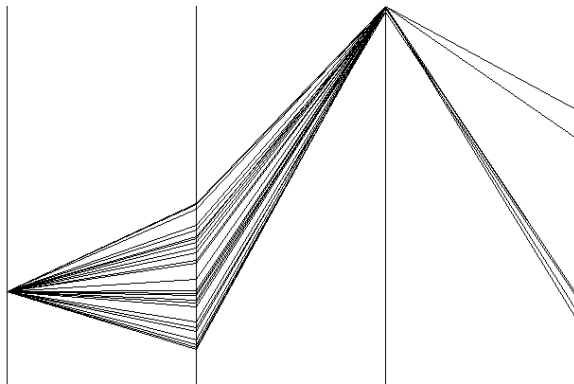
Représenter l'information

LLDOS 1.0 Alert correlation graph



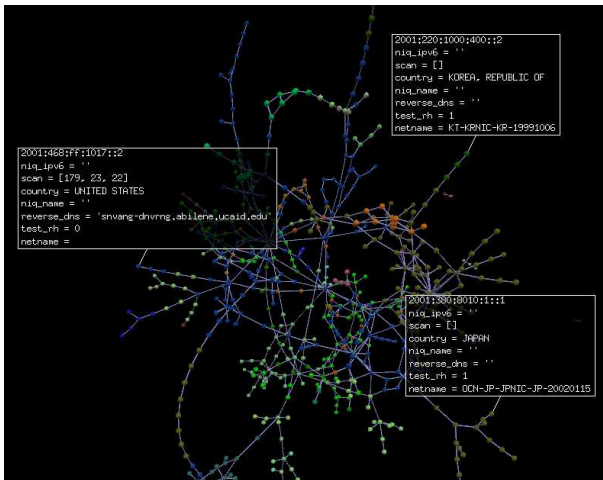
Représenter l'information

SVP



Exemples

IPv6 world



Exemples

Correlation UI

Alert Correlation in a Cooperative Intrusion Detection Framework (Frédéric Cuppens / Alexandre Miège) :

The screenshot displays a software interface for alert correlation. It is divided into several panes:

- File / Option:** Lists various alert sources and their details, such as 'IP: 194.90.104.90 - 2001/12/18-233' and 'GASSATA: 180.9.190.188.9.180-2001-12-18T18:48:36Z-17'.
- Alerts list:** A table of alerts with columns for ID, source, and time. For example: '1 | CRIM-04189-134.212.230.82-6 | MIRA-0072'.
- Alerts list (continued):** Another table showing related alerts, such as '1 | CRIM-04189-134.212.230.82-7 | MIRA-0182'.
- Alerts list (continued):** A third table showing alerts with a 'niveau' (level) of 10, such as '1 | CRIM-04189-134.212.230.82-17 | MIRA-0187'.
- Alerts list (continued):** A fourth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-19 | MIRA-0188'.
- Alerts list (continued):** A fifth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-21 | MIRA-0189'.
- Alerts list (continued):** A sixth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-23 | MIRA-0190'.
- Alerts list (continued):** A seventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-24 | MIRA-0191'.
- Alerts list (continued):** An eighth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-25 | MIRA-0192'.
- Alerts list (continued):** A ninth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-26 | MIRA-0193'.
- Alerts list (continued):** A tenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-27 | MIRA-0194'.
- Alerts list (continued):** An eleventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-28 | MIRA-0195'.
- Alerts list (continued):** A twelfth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-29 | MIRA-0196'.
- Alerts list (continued):** A thirteenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-30 | MIRA-0197'.
- Alerts list (continued):** A fourteenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-31 | MIRA-0198'.
- Alerts list (continued):** A fifteenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-32 | MIRA-0199'.
- Alerts list (continued):** A sixteenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-33 | MIRA-0200'.
- Alerts list (continued):** A seventeenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-34 | MIRA-0201'.
- Alerts list (continued):** An eighteenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-35 | MIRA-0202'.
- Alerts list (continued):** A nineteenth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-36 | MIRA-0203'.
- Alerts list (continued):** A twentieth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-37 | MIRA-0204'.
- Alerts list (continued):** A twenty-first table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-38 | MIRA-0205'.
- Alerts list (continued):** A twenty-second table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-39 | MIRA-0206'.
- Alerts list (continued):** A twenty-third table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-40 | MIRA-0207'.
- Alerts list (continued):** A twenty-fourth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-41 | MIRA-0208'.
- Alerts list (continued):** A twenty-fifth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-42 | MIRA-0209'.
- Alerts list (continued):** A twenty-sixth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-43 | MIRA-0210'.
- Alerts list (continued):** A twenty-seventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-44 | MIRA-0211'.
- Alerts list (continued):** A twenty-eighth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-45 | MIRA-0212'.
- Alerts list (continued):** A twenty-ninth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-46 | MIRA-0213'.
- Alerts list (continued):** A thirtieth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-47 | MIRA-0214'.
- Alerts list (continued):** A thirty-first table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-48 | MIRA-0215'.
- Alerts list (continued):** A thirty-second table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-49 | MIRA-0216'.
- Alerts list (continued):** A thirty-third table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-50 | MIRA-0217'.
- Alerts list (continued):** A thirty-fourth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-51 | MIRA-0218'.
- Alerts list (continued):** A thirty-fifth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-52 | MIRA-0219'.
- Alerts list (continued):** A thirty-sixth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-53 | MIRA-0220'.
- Alerts list (continued):** A thirty-seventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-54 | MIRA-0221'.
- Alerts list (continued):** A thirty-eighth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-55 | MIRA-0222'.
- Alerts list (continued):** A thirty-ninth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-56 | MIRA-0223'.
- Alerts list (continued):** A fortieth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-57 | MIRA-0224'.
- Alerts list (continued):** A forty-first table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-58 | MIRA-0225'.
- Alerts list (continued):** A forty-second table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-59 | MIRA-0226'.
- Alerts list (continued):** A forty-third table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-60 | MIRA-0227'.
- Alerts list (continued):** A forty-fourth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-61 | MIRA-0228'.
- Alerts list (continued):** A forty-fifth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-62 | MIRA-0229'.
- Alerts list (continued):** A forty-sixth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-63 | MIRA-0230'.
- Alerts list (continued):** A forty-seventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-64 | MIRA-0231'.
- Alerts list (continued):** A forty-eighth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-65 | MIRA-0232'.
- Alerts list (continued):** A forty-ninth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-66 | MIRA-0233'.
- Alerts list (continued):** A fiftieth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-67 | MIRA-0234'.
- Alerts list (continued):** A fifty-first table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-68 | MIRA-0235'.
- Alerts list (continued):** A fifty-second table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-69 | MIRA-0236'.
- Alerts list (continued):** A fifty-third table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-70 | MIRA-0237'.
- Alerts list (continued):** A fifty-fourth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-71 | MIRA-0238'.
- Alerts list (continued):** A fifty-fifth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-72 | MIRA-0239'.
- Alerts list (continued):** A fifty-sixth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-73 | MIRA-0240'.
- Alerts list (continued):** A fifty-seventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-74 | MIRA-0241'.
- Alerts list (continued):** A fifty-eighth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-75 | MIRA-0242'.
- Alerts list (continued):** A fifty-ninth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-76 | MIRA-0243'.
- Alerts list (continued):** A sixtieth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-77 | MIRA-0244'.
- Alerts list (continued):** A sixty-first table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-78 | MIRA-0245'.
- Alerts list (continued):** A sixty-second table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-79 | MIRA-0246'.
- Alerts list (continued):** A sixty-third table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-80 | MIRA-0247'.
- Alerts list (continued):** A sixty-fourth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-81 | MIRA-0248'.
- Alerts list (continued):** A sixty-fifth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-82 | MIRA-0249'.
- Alerts list (continued):** A sixty-sixth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-83 | MIRA-0250'.
- Alerts list (continued):** A sixty-seventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-84 | MIRA-0251'.
- Alerts list (continued):** A sixty-eighth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-85 | MIRA-0252'.
- Alerts list (continued):** A sixty-ninth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-86 | MIRA-0253'.
- Alerts list (continued):** A seventieth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-87 | MIRA-0254'.
- Alerts list (continued):** A seventy-first table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-88 | MIRA-0255'.
- Alerts list (continued):** A seventy-second table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-89 | MIRA-0256'.
- Alerts list (continued):** A seventy-third table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-90 | MIRA-0257'.
- Alerts list (continued):** A seventy-fourth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-91 | MIRA-0258'.
- Alerts list (continued):** A seventy-fifth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-92 | MIRA-0259'.
- Alerts list (continued):** A seventy-sixth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-93 | MIRA-0260'.
- Alerts list (continued):** A seventy-seventh table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-94 | MIRA-0261'.
- Alerts list (continued):** A seventy-eighth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-95 | MIRA-0262'.
- Alerts list (continued):** A seventy-ninth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-96 | MIRA-0263'.
- Alerts list (continued):** An eightyth table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-97 | MIRA-0264'.
- Alerts list (continued):** An eighty-first table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-98 | MIRA-0265'.
- Alerts list (continued):** An eighty-second table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-99 | MIRA-0266'.
- Alerts list (continued):** An eighty-third table showing alerts with a 'niveau' of 10, such as '1 | CRIM-04189-134.212.230.82-100 | MIRA-0267'.

The bottom right pane, titled 'diagramme de corrélation', shows a flow diagram with nodes representing alerts and their relationships. Nodes include '2', '5', '7', '10', 'Alert_1', 'Alert', and '23'. Arrows indicate the flow of information between these nodes, showing how individual alerts are correlated into a larger context.

Brouette

Notification pour l'administrateur



- 1 Introduction aux IDS
 - Petit tour de la détection d'intrusions
- 2 Introduction à la visualisation
 - Trois points à retenir
 - Représenter l'information
 - Exemples
- 3 Méthodologie**
 - Prérequis
 - Architecture
 - Classification
- 4 Exemple de représentation
- 5 Conclusion

Comprendre une attaque

Objectifs :

- Reconstruire la séquence d'événements
- Reconnaître les cibles, protocoles, outils, ...
- Adapter la sévérité
- Supprimer des faux positifs
- Préparer pour une éventuelle contre-mesure
- Vérifier l'application de la politique de sécurité

Comprendre une attaque

Objectifs :

- Reconstruire la séquence d'événements
- Reconnaître les cibles, protocoles, outils, ...
- Adapter la sévérité
- Supprimer des faux positifs
- Préparer pour une éventuelle contre-mesure
- Vérifier l'application de la politique de sécurité

Outils :

- Normalisation, Centralisation
- Corrélation
- Aperçu graphique

Prérequis

- Sources multiples
- Normalisation des évènements/alertes
- Centralisation
- Format d'échange standard

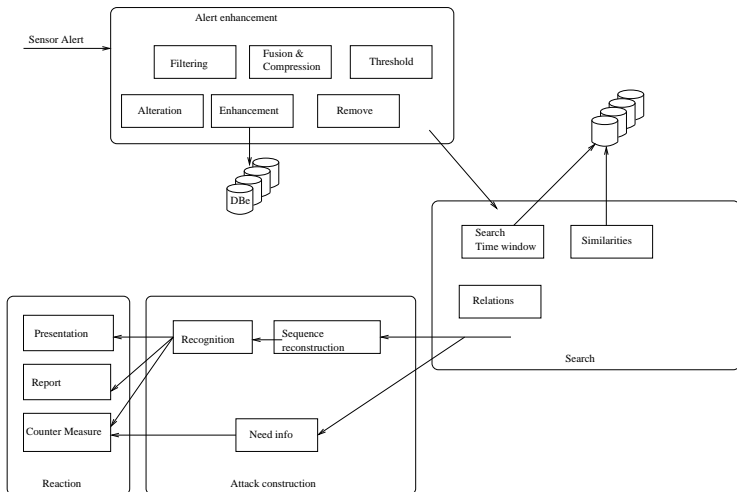
⇒ IDMEF (RFC 4765)

`http://www.rfc-editor.org/rfc/rfc4765.txt`

Données intéressantes d'un message IDMEF

- **Source** : alert.source(0).node.address(0).address
- **Destination** : alert.target(0).node.address(0).address
- **Impact** : alert.assessment.impact.severity
- **Complétion** : assessment.impact.completion
- **Vecteur d'attaque** : alert.classification.text
- **Type d'analyseur** : analyzer(0).class
- ...

Architecture



Une attaque devient corrélable lorsque :

- On a une alerte
- On a les informations complémentaires (OS, CVE...)
- On a rangé l'alerte dans une catégorie connue

Attaques :

- 1 Prospector
- 2 Pénétrer
- 3 Perdurer
- 4 Propager
- 5 Paralyser

Alertes :

- Prelude LML: Mar 8 17:30:30 prelude
sshd[19529]: (pam_unix) session opened for
user root by root(uid=0)
- Snort: BLEEDING-EDGE SCAN NMAP -f -sS
- ClamAV: Eicar-Test-Signature (succeeded)
- Auditd: App Abnormal Termination

Mettre l'alerte dans une catégorie connue :

● Authentication

- Local user
- System user
- Admin user
- Other

● Probe

- Protocol
- Scan
- Sniff
- Users
- Other

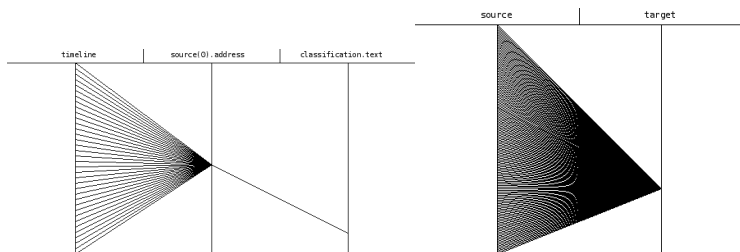
● Corruption

- File
- Application
- Other

● Availability

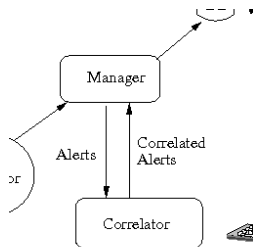
Classification

Visualisation d'attaques



- 1 Introduction aux IDS
 - Petit tour de la détection d'intrusions
- 2 Introduction à la visualisation
 - Trois points à retenir
 - Représenter l'information
 - Exemples
- 3 Méthodologie
 - Prérequis
 - Architecture
 - Classification
- 4 Exemple de représentation
- 5 Conclusion

Corrélateur visuel



Code 1/3

- Basé sur Prelude IDS
- Langage de haut niveau
- Le code sera python + Prelude Easy bindings

```
svn co http://svn.prelude-ids.org/libprelude/  
branches/libprelude-easy-bindings
```

Code 2/3

Initialisation

```
import PreludeEasy  
  
client = PreludeEasy.Client("IdmefGraph")  
client.Init()  
client.PoolInit("192.168.33.215", 1)
```

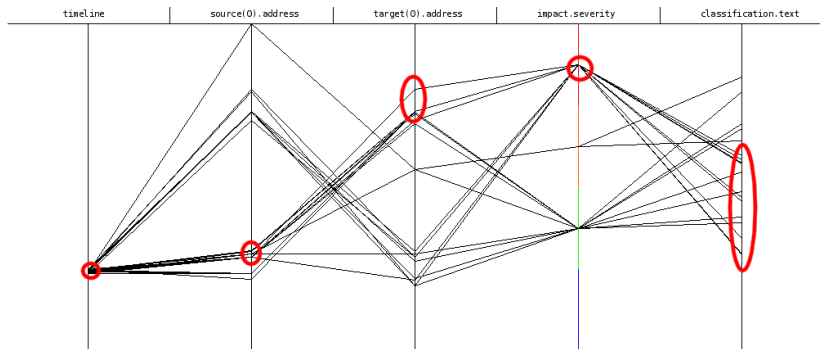
Code 3/3

Récupération et utilisation des objets

```
idmef = client.ReadIDMEF(1)
if idmef:
    severity =
        idmef.Get("alert.assessment.impact.severity")

    if severity == "high":
        print "Attaque importante"
```

Corrélateur visuel



Directions futures

- Choix de vues adaptées, interprétations
- Porter plus de sondes à Prelude
- Règles de corrélations
- Agents passifs de collecte d'information

- Merci de votre attention
- Questions ?

Informations complémentaires



Exemple de sonde : NuFW (<http://www.nufw.org>)

- Pare-feu **authentifiant**, basé sur l'utilisateur
- Fournit un module de log Prelude natif
- Ajoute l'information utilisateur sur chaque connexion
- Ajoute des critères utiles pour la corrélation
- Permet d'appliquer strictement la politique de sécurité

Exemple d'alerte NuFW (1)

```
messageid: 5478076470
analyzer(1):
  analyzerid: 2334565015741136
  name: nufw
  manufacturer: http://www.nufw.org/
  model: NuFW
  version: 2.3.0 ($Revision: 3475 $)
  class: Firewall
  ostype: Linux
  osversion: 2.6.20-15-386
  process:
    name:
    pid: 15197
```

Exemple d'alerte NuFW (2)

```
create_time: 29/06/2007 11:26:24.0 +02:00
classification:
  text: Connection opened
detect_time: 29/06/2007 11:32:56.0 +02:00
analyzer_time: 29/06/2007 11:32:56.642005 +02:00
source(0):
  spoofed: unknown (0)
  node:
    category: unknown (0)
    address(0):
      category: ipv4-addr (7)
      address: 192.168.0.2
  user:
    category: application (1)
    user_id(0):
      type: current-user (1)
      name: pollux
      number: 1000
  process:
    name: firefox
    path: /usr/bin/firefox
  service:
    iana_protocol_number: 6
    iana_protocol_name: tcp
    port: 3489
```

Exemple d'alerte NuFW (3)

```
target(0):
  decoy: unknown (0)
  node:
    category: unknown (0)
    address(0):
      category: ipv4-addr (7)
      address: 82.165.85.221
    service:
      iana_protocol_number: 6
      iana_protocol_name: tcp
      port: 80
  assessment:
    impact:
      severity: low (2)
      type: user (5)
      description: Connection state changed
```