

# Détection d'intrusions avec Prelude

Pierre Chifflier / INL  
Sebastien Tricaud / Wengo



# NIDS

- Avantages :
  - Détecte les attaques depuis le réseau
  - Temps réel
- Inconvénients :
  - Faux positifs
  - Peut être la cible d'une attaque
- Exemples : Snort, Bro, ...

# HIDS

- Avantages :
  - Filtre les logs pour en déduire des alertes
  - Peu de faux positifs
- Inconvénients :
  - Système à configurer
  - Un par poste
- Exemples : Samhain, LML, ...

# IDS Hybride

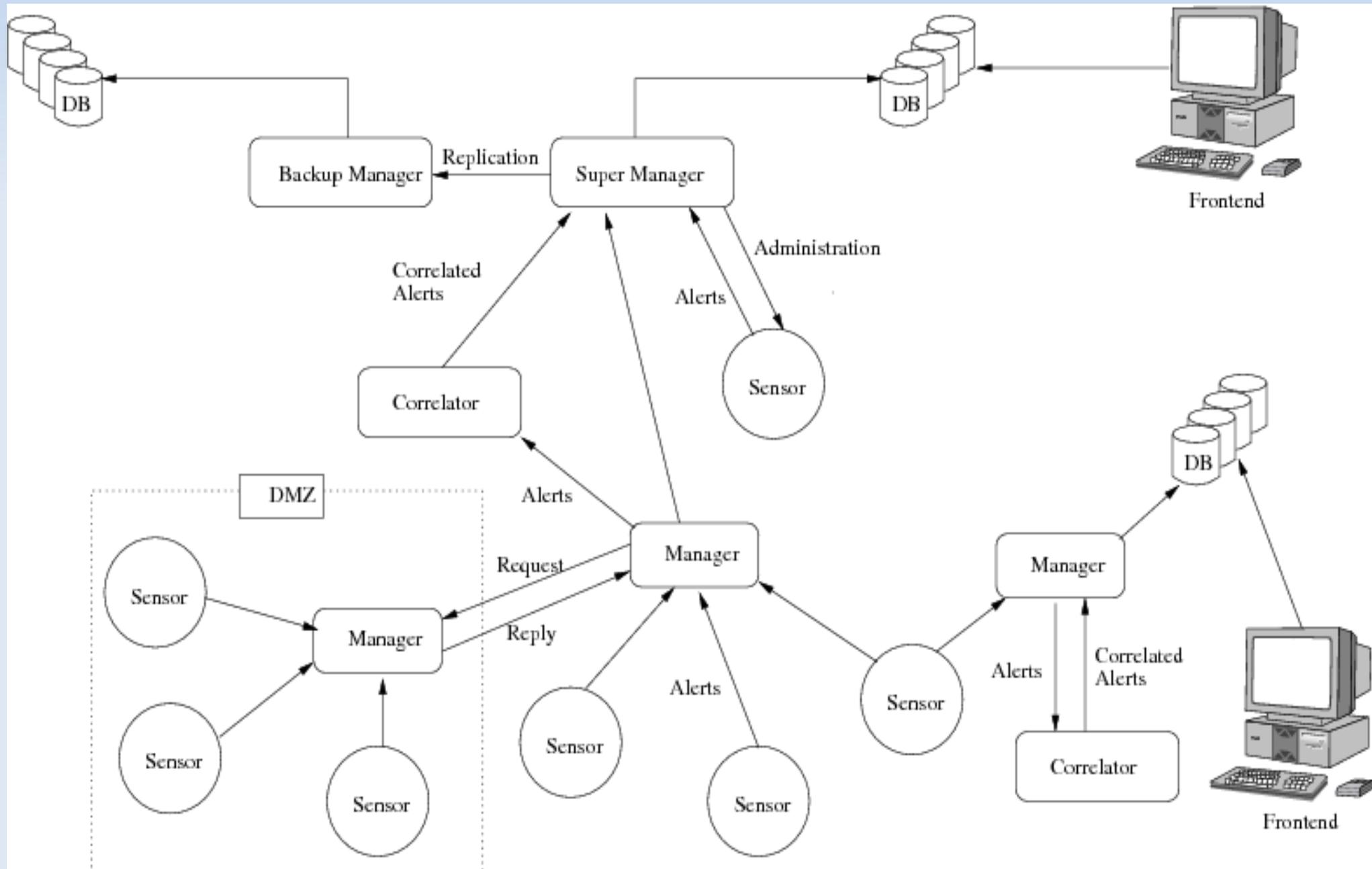
- Avantages des NIDS & HIDS sans les inconvénients
- Normalisation des formats
- Centralisation des événements



# Histoire du projet

- Initié en 1998 par Yoann Vandoorselaere
- Parti d'un NIDS avec reporting distant
- Intégration de HIDS au reporting
- Normalisation des alertes via IDMEF (RFC 4765)
- NIDS remplacé par Snort
- Sondes avec support Prelude : PAM, samhain, NuFW, nessus, nepenthes, libsafe, scancp, ...
- Support de la corrélation

# Architecture distribuée

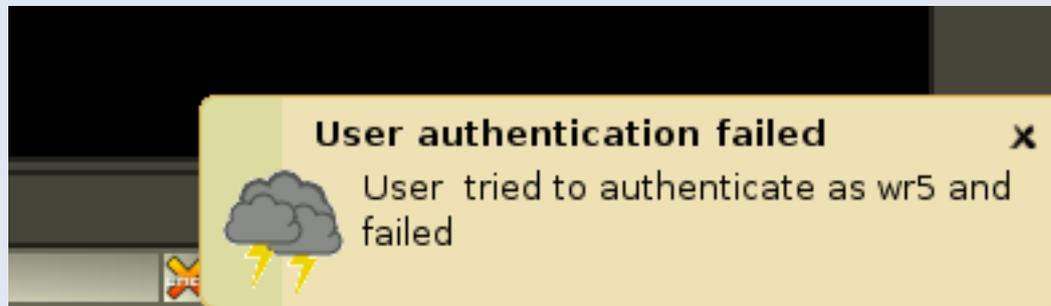


# Architecture Hybride

- Collecter : Sondes, syslog, syslog-ng
- Normaliser : format hétérogène IDMEF
- Centraliser
- Analyse : données collectées, corrélation
- Présentation : UI prewikka, brouette

# Brouette

- Collecteur d'événements pour Prelude IDS
- `$ brouette <IP_manager>`
- Affiche impact + description



# Brouette : themes

## User authentication successful



User authenticated to rph successfully

## Brute force attack



Multiple failed attempts have been made to login to a user account

## User login failed with an invalid user



Someone tried to login with the invalid user "oubiwann" from 80.244.128.37

## SUDO Command Executed



User wr5 successfully executed the command './etc/init.d/rtmpd.sh status' as root.

## SUDO Command Executed



User wr5 successfully executed the command './etc/init.d/rtmpd.sh status' as root.

# Correlation

Définition : aider la couche présentation, infos pertinentes

- Avantages :
  - Détecter des méta-attaques
  - Réduit les faux positifs
  - Détecte une séquence (ex. heure de connection)
- Inconvénient :
  - N'est pas une source unique de confiance

# Futur

- Amélioration de la fiabilité des sondes avec la corrélation
- Contres-mesures
- Paquets Debian ;-)

# Questions ?

