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, ...

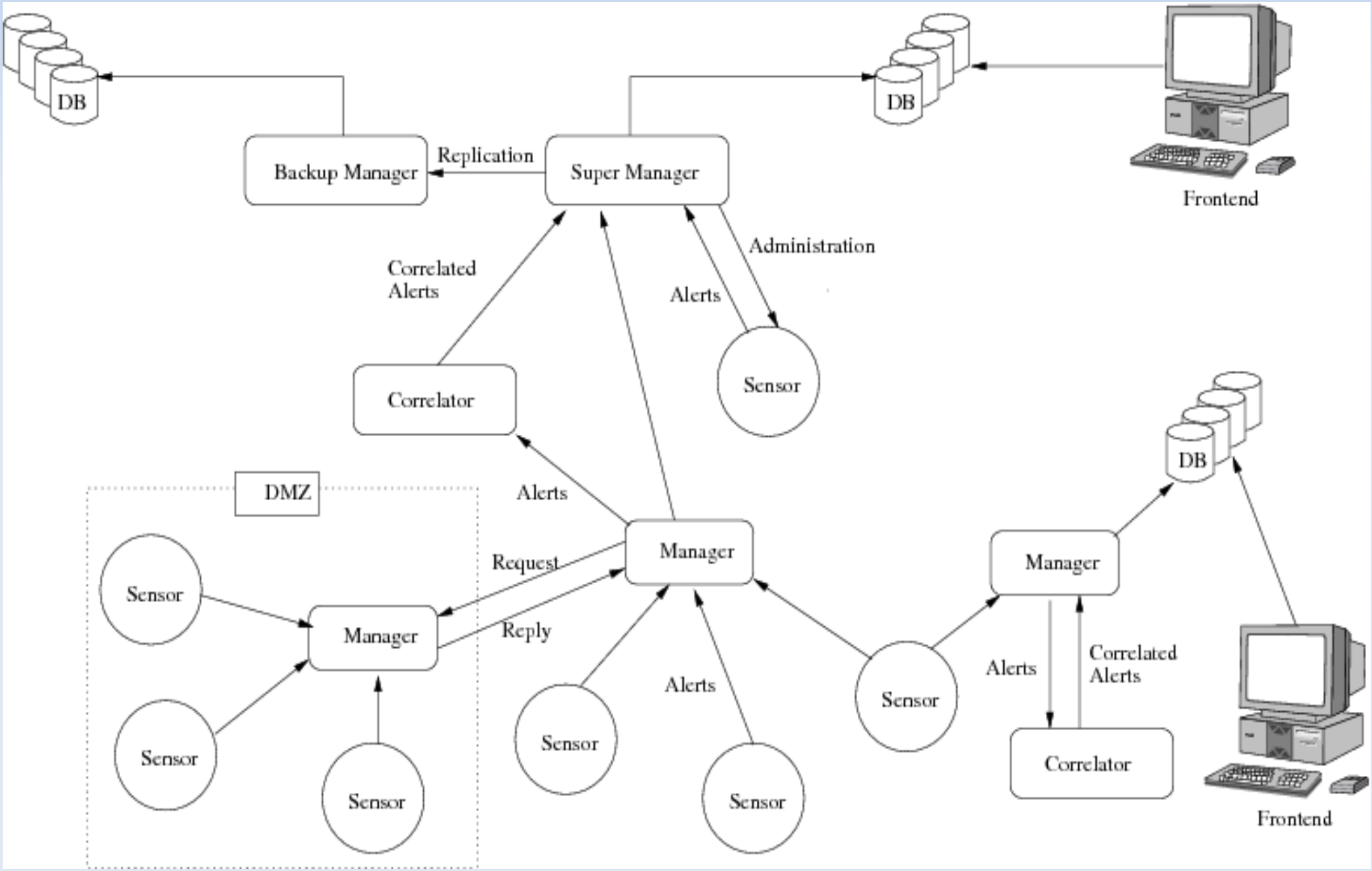
IDS Hybride

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

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 correlation

Architecture distribuée

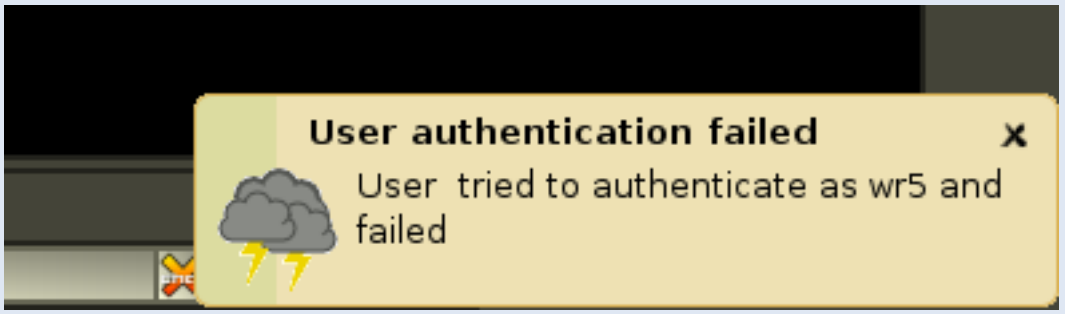


Architecture Hybride

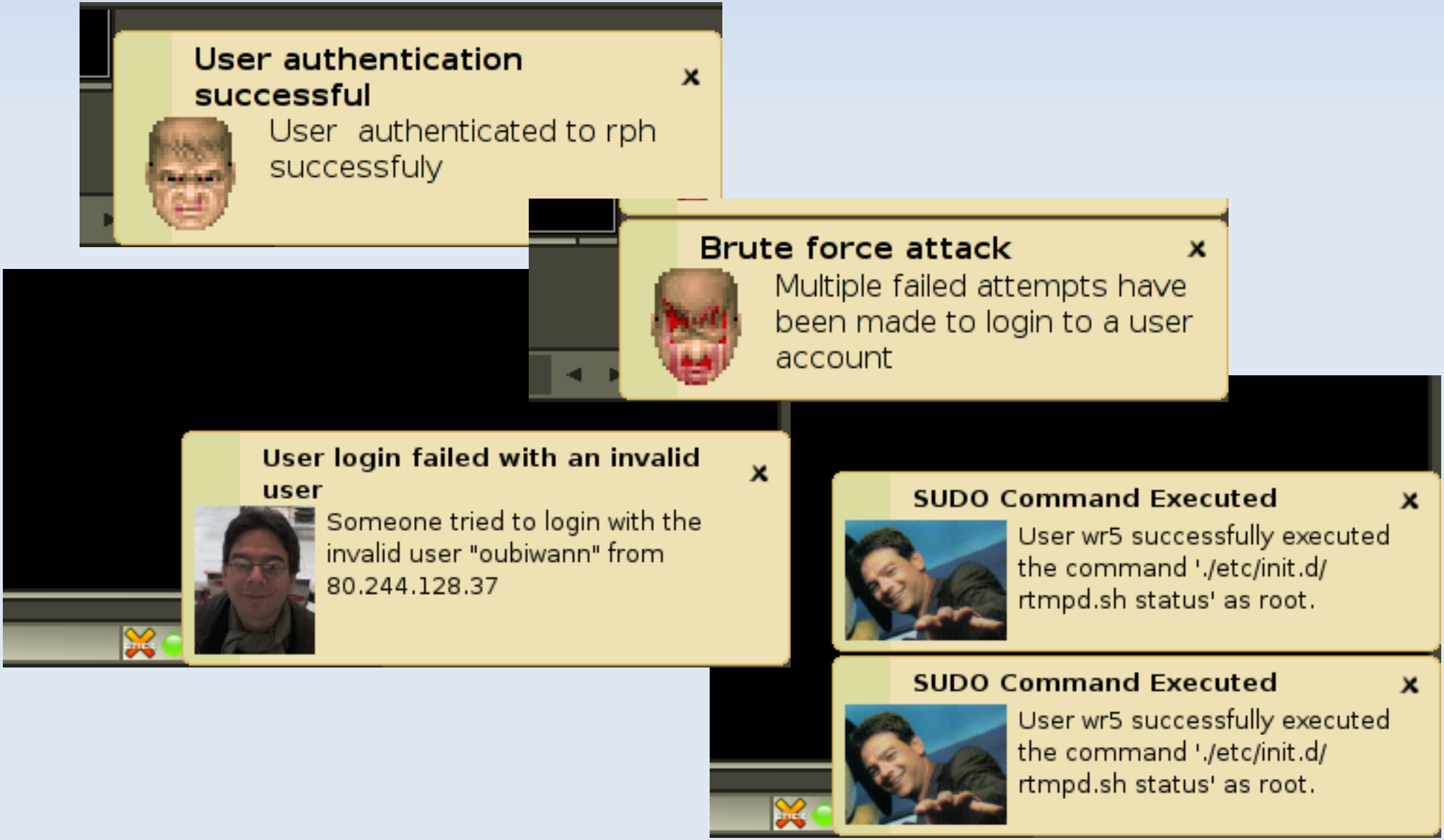
- Collecter : Sondes, syslog, syslog-ng
- Normaliser : format hétérogène IDMEF
- Centraliser
- Analyse : données collectées, correlation
- Présentation : UI prewikka, brouette

Brouette

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



Brouette : themes



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 correlation
- Contres-mesures
- Paquets Debian ;-)

Questions ?