Supervision de la sécurité

Benjamin Morin

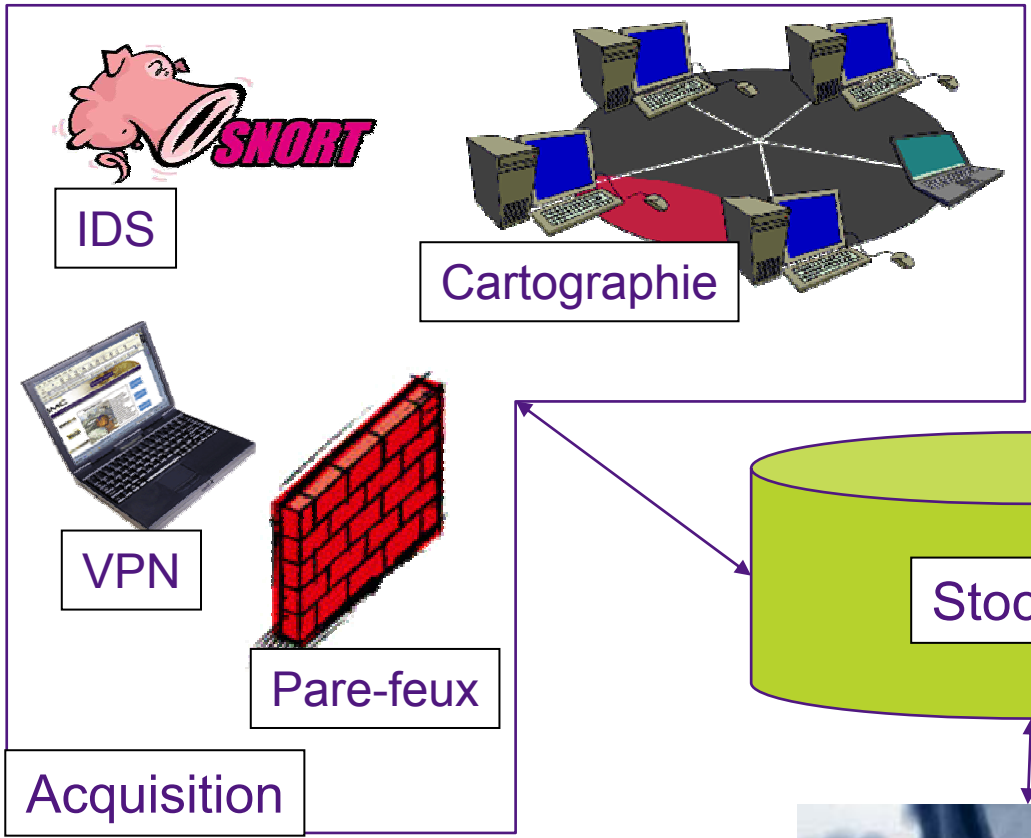
benjamin.morin@francetelecom.com

3 mai 2004

Objectif

- **Equipements de sécurité produisent des événements/alertes**
  - Volume important
  - Formats hétérogènes
- **Nécessiter de développer une infrastructure permettant de**
  - Centraliser
  - Federer
  - Analyser les événements
- **Infrastructure de supervision de la sécurité opérationnelle**
- **Déploiement dans les filiales de France Télécom**

Schéma général



Acquisition d'événements

- **Modules d'acquisition**
  - Systèmes de détection d'intrusions réseau et applicatifs
    - Snort
    - Détection d'intrusion dans les réseaux haut-débit
  - Acquisition de la cartographie de l'environnement surveillé
    - Approche passive
  - Audits de vulnérabilité (Nessus)
  - Logs systèmes, firewalls, concentrateurs VPN
  - Manifestations virales
- **Formatage des événements en IDMEF**
- **Implémentation**
  - Modules d'acquisitions écrits en Perl

Stockage des événements

- **Schéma relationnel permettant**
  - d'effectuer des requêtes
  - de fédérer les informations produites par les sondes
  - de structurer ces informations de manière cohérente
  - de centraliser la configuration des sondes (ex. signatures IDS)
- **Implémentations**
  - Postgresql (open-source)
  - Oracle (performances)
  - Versions futures de MySQL?
- **Optimisations**
  - Requêtes
  - Insertion de données
  - ~ 4 M événements

Corrélation d'alertes

- **PEACE**
  - Peace is an Event and Alarm Correlation Engine
- **Objectifs**
  - Réduction du volume d'alertes (fausses alertes, regroupements)
  - Améliorer la sémantique des alertes (contenu, sévérité)
- **Approches**
  - Logico-temporelles (scénarios)
  - Statistiques (aggrégation, clustering)
  - Knowledge-based
- **Informations utilisées**
  - Propriétés des attaques et des vulnérabilités
  - Informations cartographiques

Présentation des informations

- **Faciliter l'appréhension des événements pour les opérateurs**
- **Contrôle d'accès pour les opérations sur les bases**
  - Consultation
  - Modification
  - Archivage
  - Notions de rôles
- **Visualisation des informations dans un navigateur**
- **Implémentation en PHP**

Future works

- Mise en open source du projet
- Techniques de corrélation d'alertes
- Techniques visualisation

Questions?