

PLACID (PROBABILISTIC GRAPHICAL MODELS AND LOGICS FOR ALARM CORRELATION IN INTRUSION DETECTION)

Philippe Leray^{1,4}, Salem Benferhat², Ludovic Mé³, Karim Tabia¹

¹LITIS (INSA-Rouen), ²CRIL (Univ. Artois), ³SUPELEC, ⁴LINA/COD (Univ. Nantes)
<http://placid.insa-rouen.fr/>

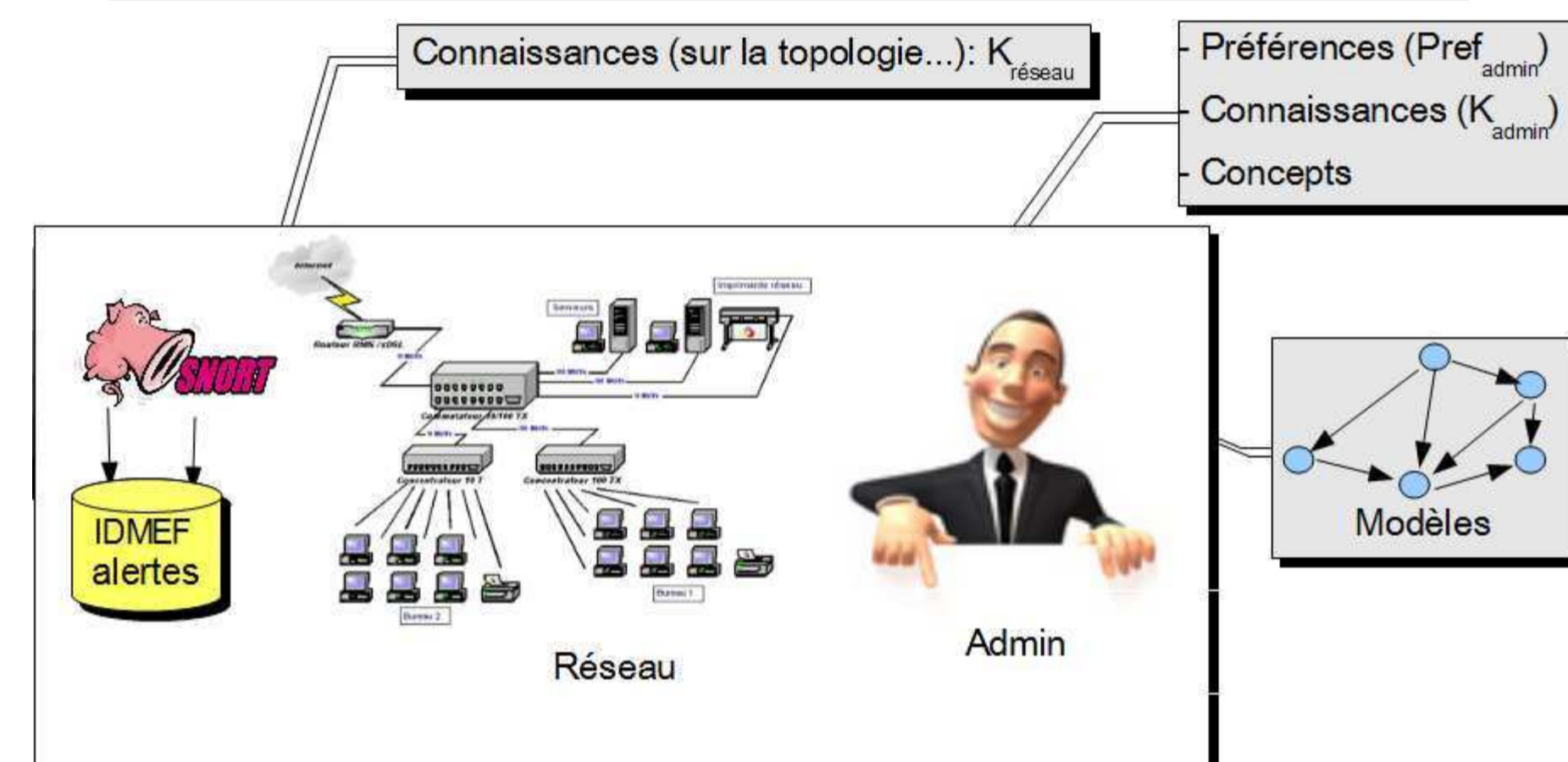


PLACID : VUE GÉNÉRALE

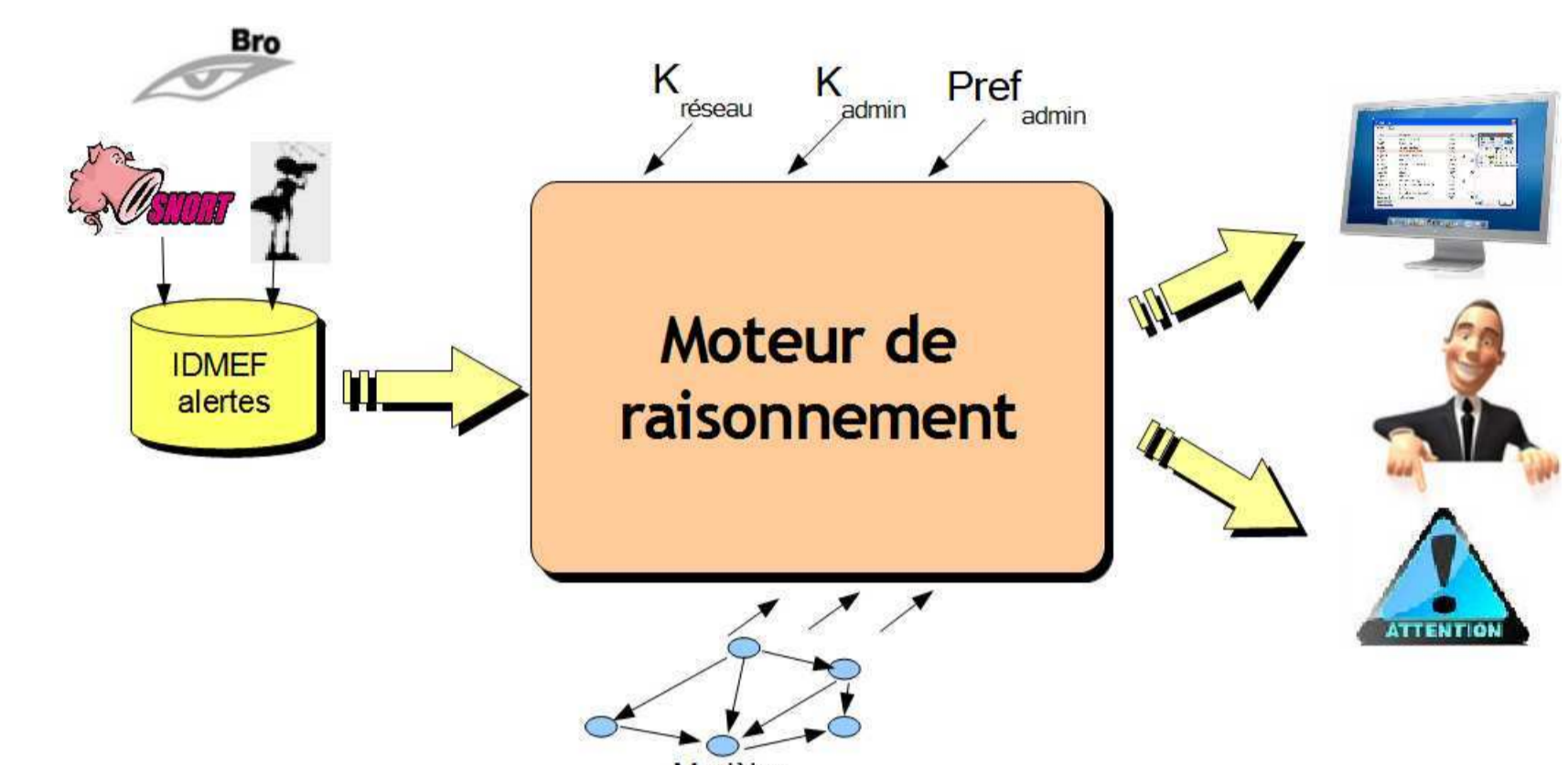
Synoptique

- ◇ **Type du projet** : ANR SETIN 2006
- ◇ **Date début** : Janvier 2007
- ◇ **Date fin** : Janvier 2011
- ◇ **Partenaires** : LITIS, CRIL, SUPELEC
- ◇ **Objectifs** : Filtrage & Prioritarisation & Corrélation d'alertes
- ◇ **Approches** : Logiques & Probabilistes
- ◇ **Contact** : philippe.Leray@univ-nantes.fr

Phase 1 : Formalisation des connaissances & Préférences

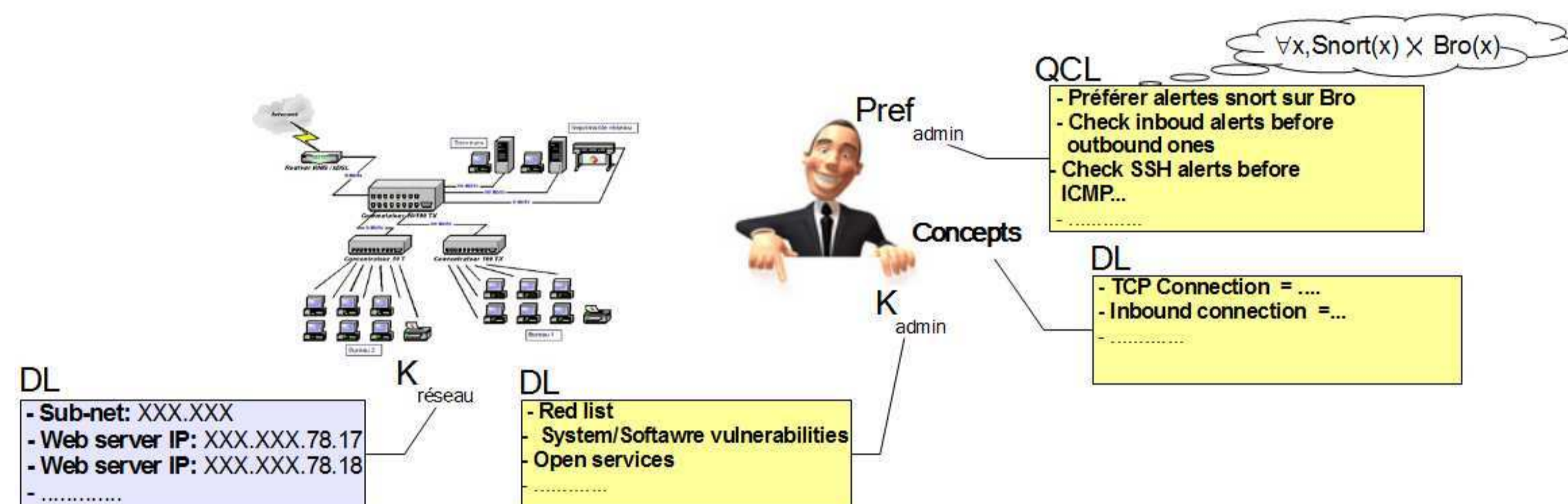


Phase 2 : Déploiement

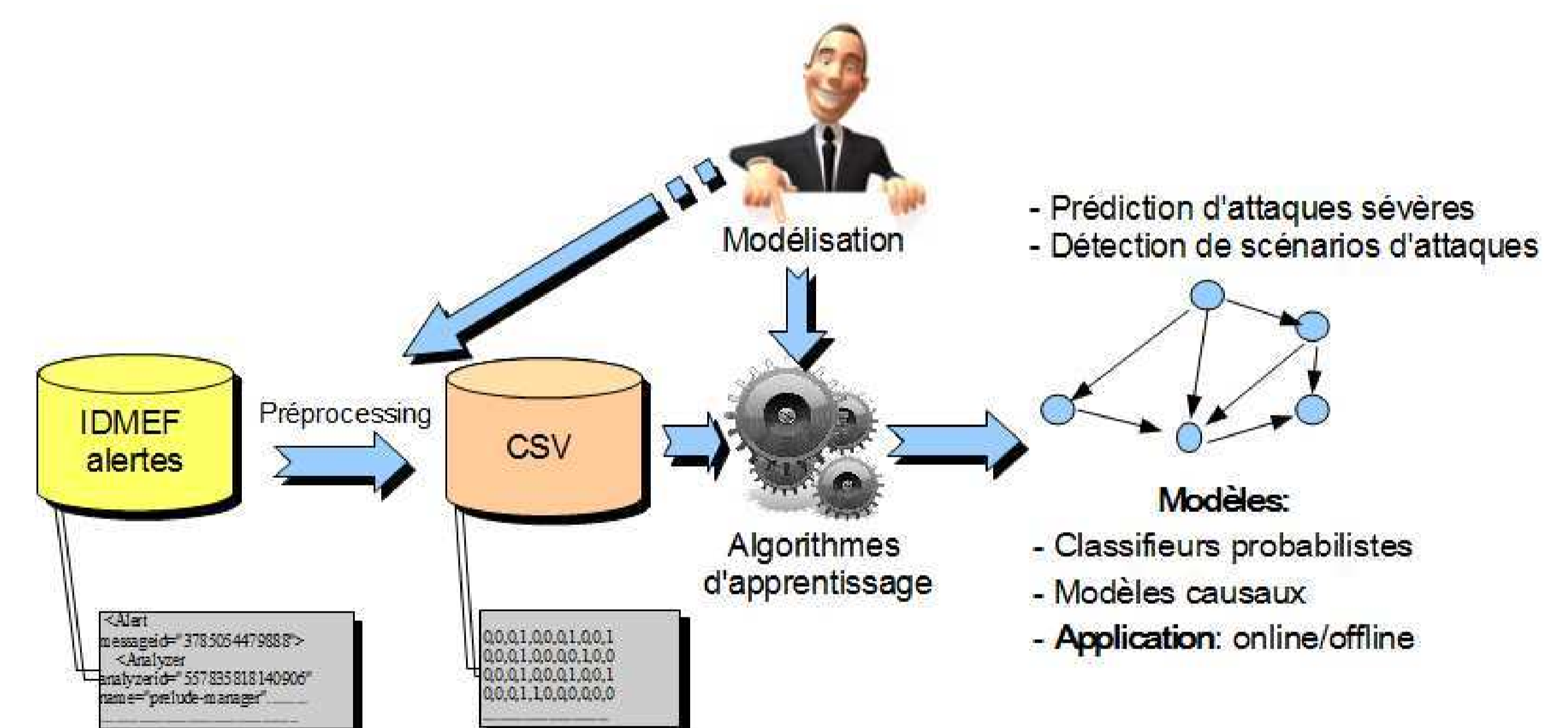


Phase 1 : FORMALISATION DES CONNAISSANCES & PRÉFÉRENCES

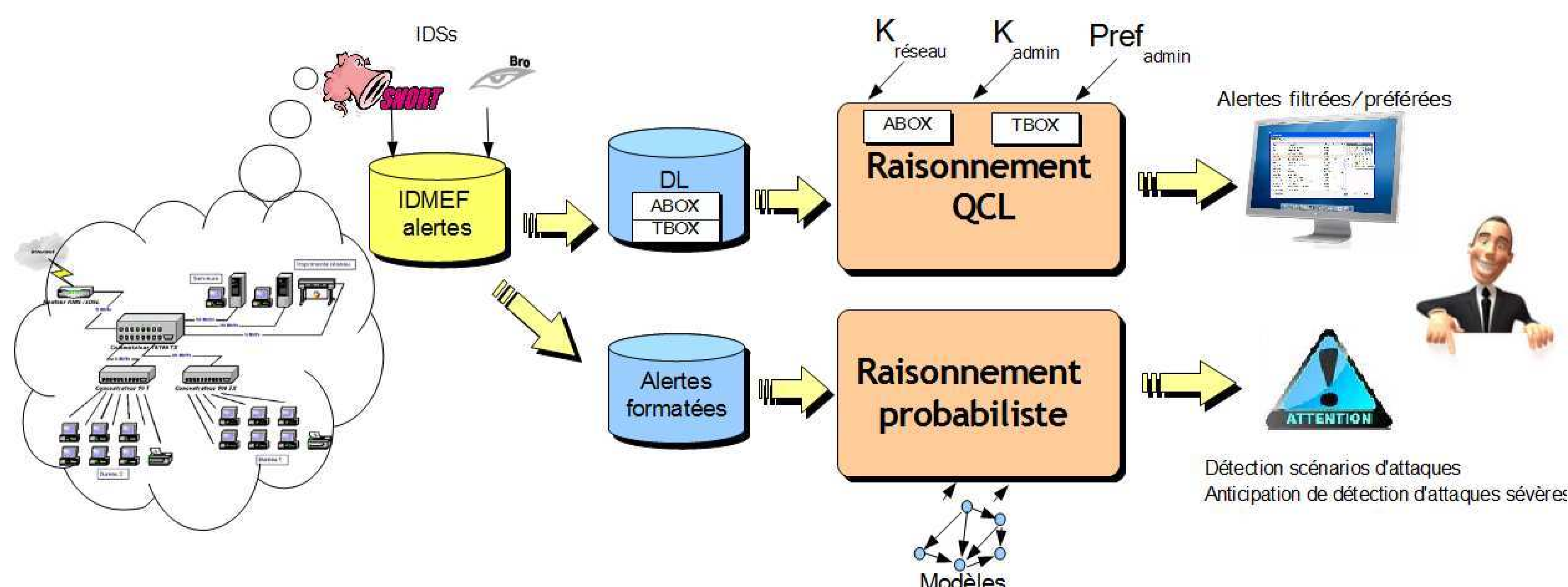
Formalisation des connaissances & Préférences



Constructions de modèles prédictifs



Phase 2 : DÉPLOIEMENT



Résultats & réalisations

- Transformation IDMEF et M4D4 en DL
 - Modélisation des préférences d'un opérateur de sécurité en QCL
 - Détection d'attaques sévères et coordonnées
 - Outils réalisés :
 - Outil pour la gestion de préférences à base des variantes de QCL, évalué sur la base d'alertes
 - Implémentation d'algorithmes d'apprentissage de structures de réseaux Bayésiens basés sur la librairie ProBT
 - Outil d'anonymisation d'alertes IDMEF et
 - Outil de formatage d'alertes IDMEF anonymisées
- Liste des publications sur :
<http://placid.insa-rouen.fr/>

Travaux en cours

1. Formalisation des connaissances & préférences :
 - Logique de description pour la formalisation des concepts
 - Interface pour la formalisation des concepts/connaissances/préférences
 - Implémentation du moteur d'inférence QCL
2. Modèles prédictifs :
 - Développement de nouveaux algorithmes d'estimation de densité
 - Amélioration des modèles Bayésiens/causaux
 - Développement d'une plateforme complète d'acquisition/anonymisation/benchmarking d'alertes IDMEF