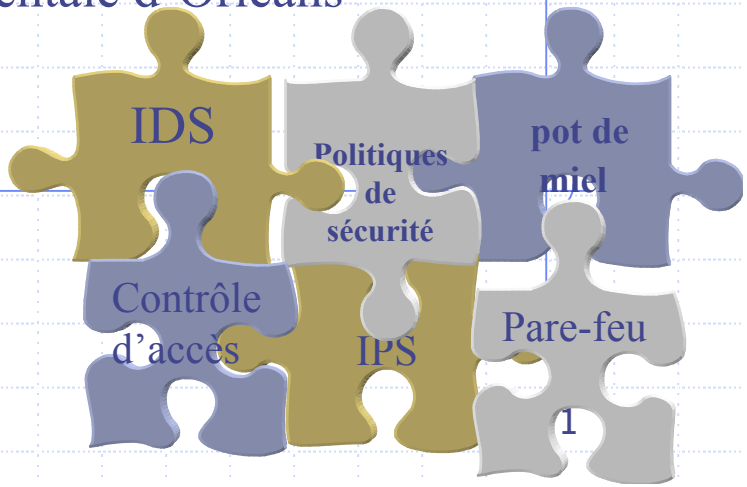
Évaluation des Systèmes de Détection d'Intrusion : *Synthèse et Perspectives*

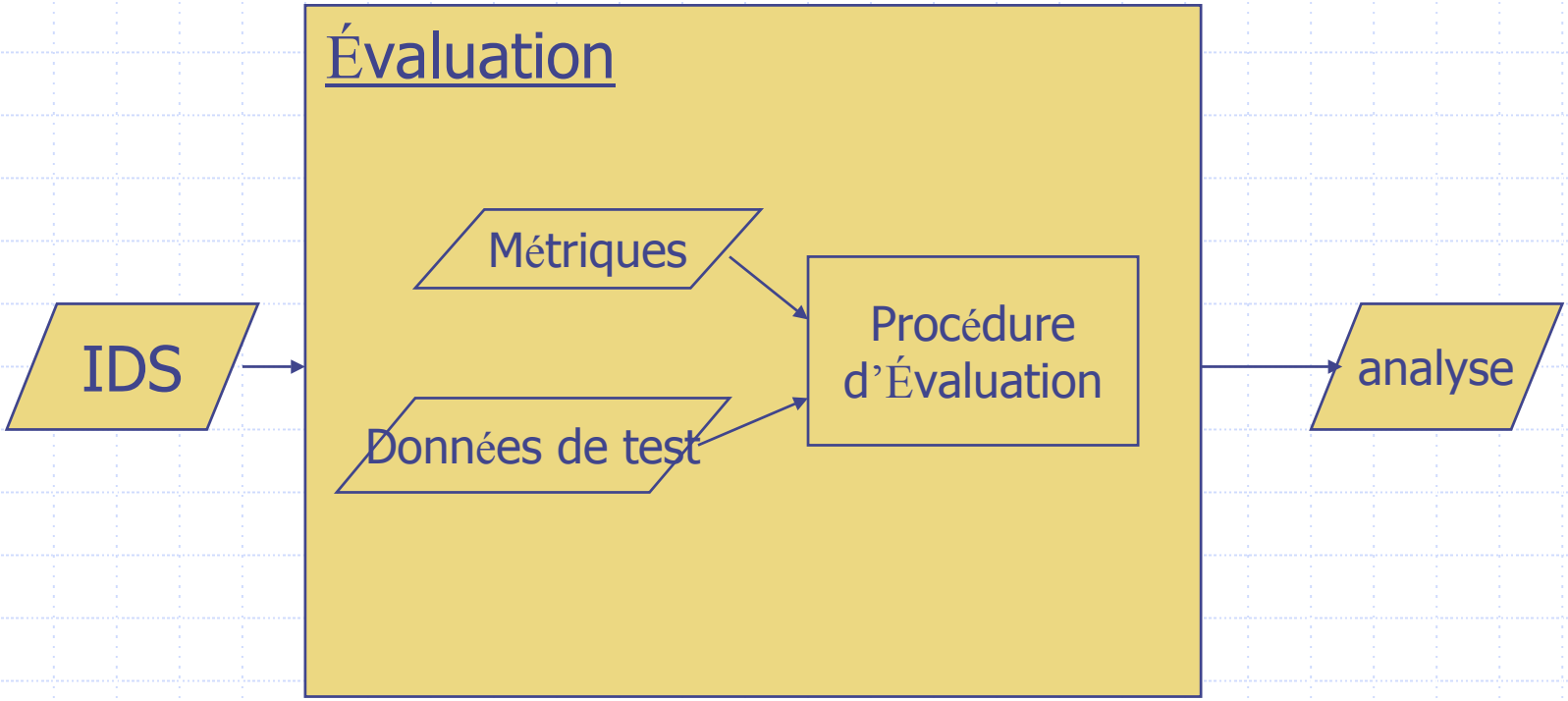
Mohammed GAD EL RAB
Anas ABOU EL KALAM
{Mgad}/{anas.abouelkalam}@ensi-bourges.fr
Laboratoire d'Informatique Fondamentale d'Orléans
LIFO – CNRS



Plan

- Introduction
- État de l'art
- Nos objectives
- Notre approche

Introduction



État de l'art

- Évaluations Ad-hoc et non systématiques
  - Données de test mal choisies/générées
  - Métriques insignifiants

    ➢ Résultats non validés voire biaisés

IDSs restent toujours avec :

- Nombre important de Fausses Alertes
- Capacité Faible de détection

Objectives

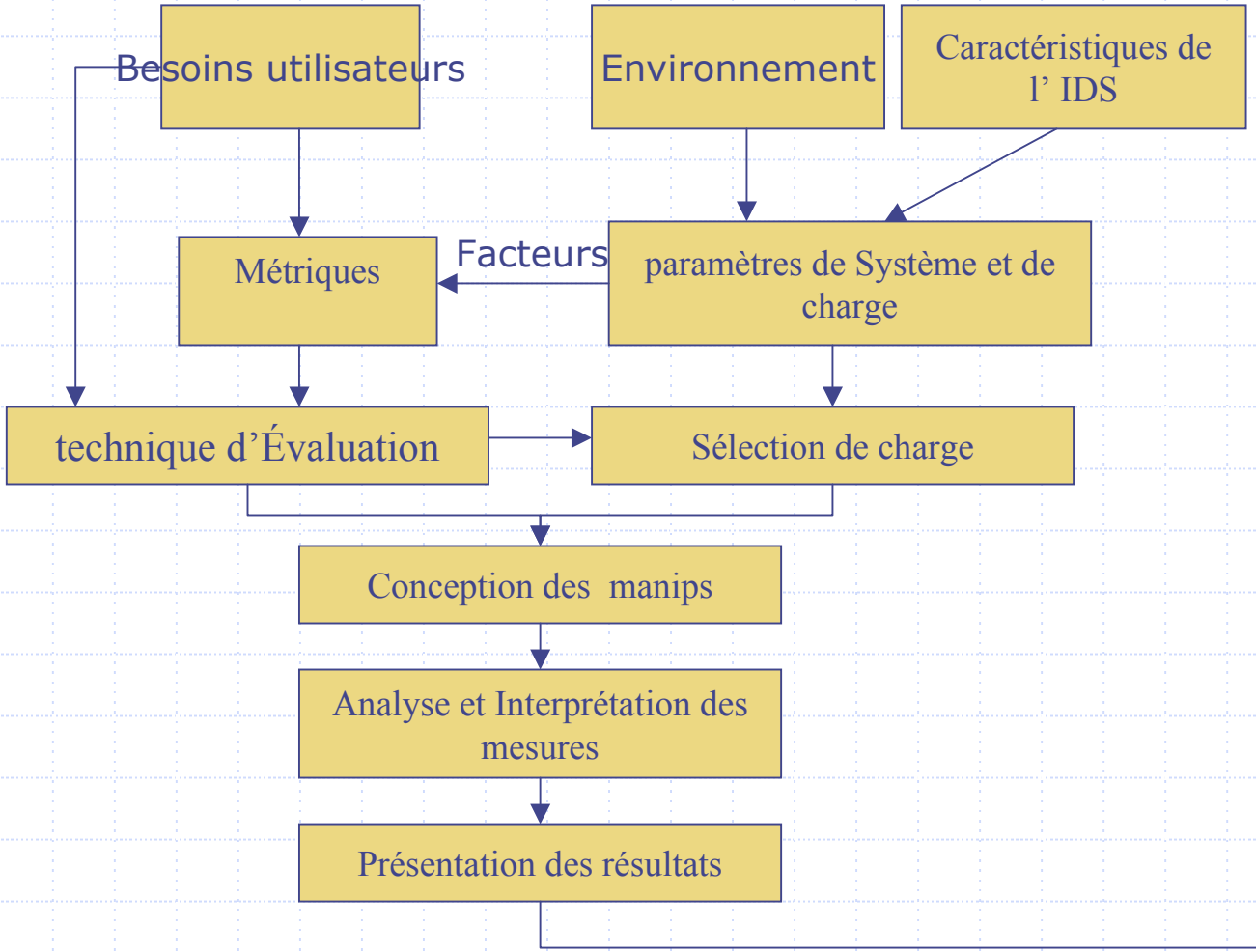
Établir une méthodologie d'évaluation :

- Systématique
- Validée
- Non biaisée

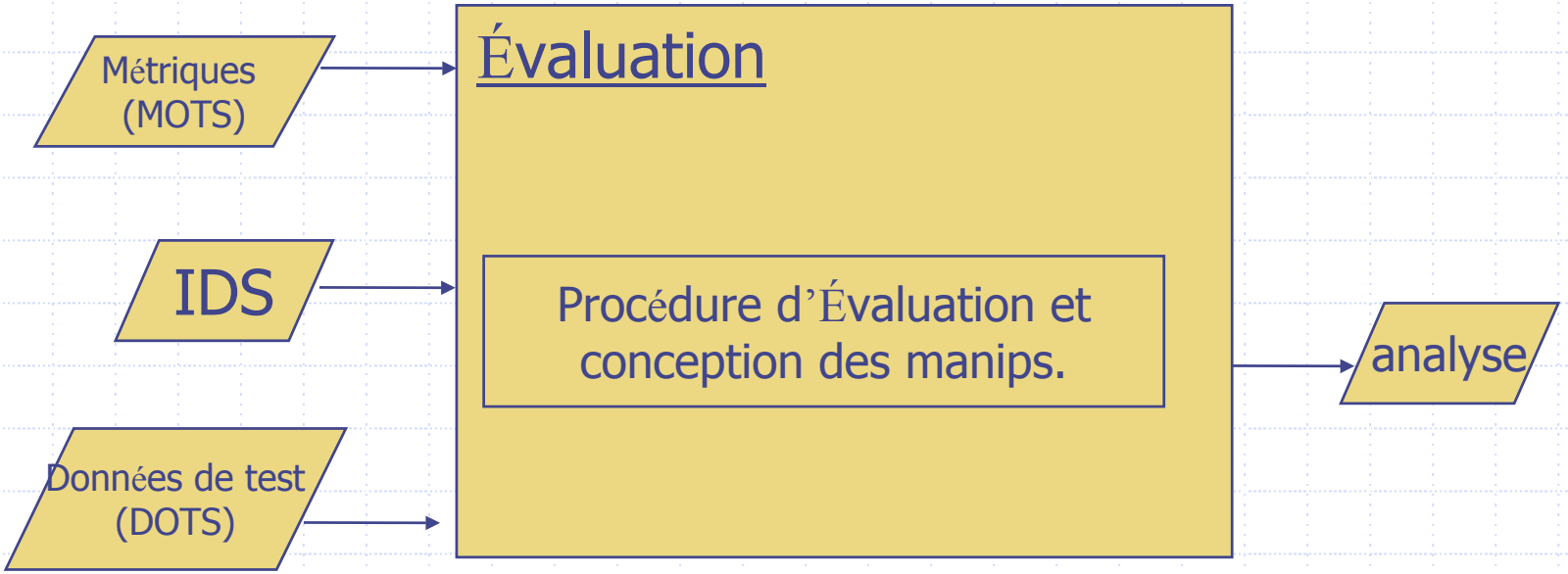
Principales étapes

- Données de test bien générées
- Métriques utiles
- Validation des résultats

Notre Approche (1)



Notre Approche (2)



(MOTS): Metrics On The Shelf

(DOTS): Dataset On The Shelf

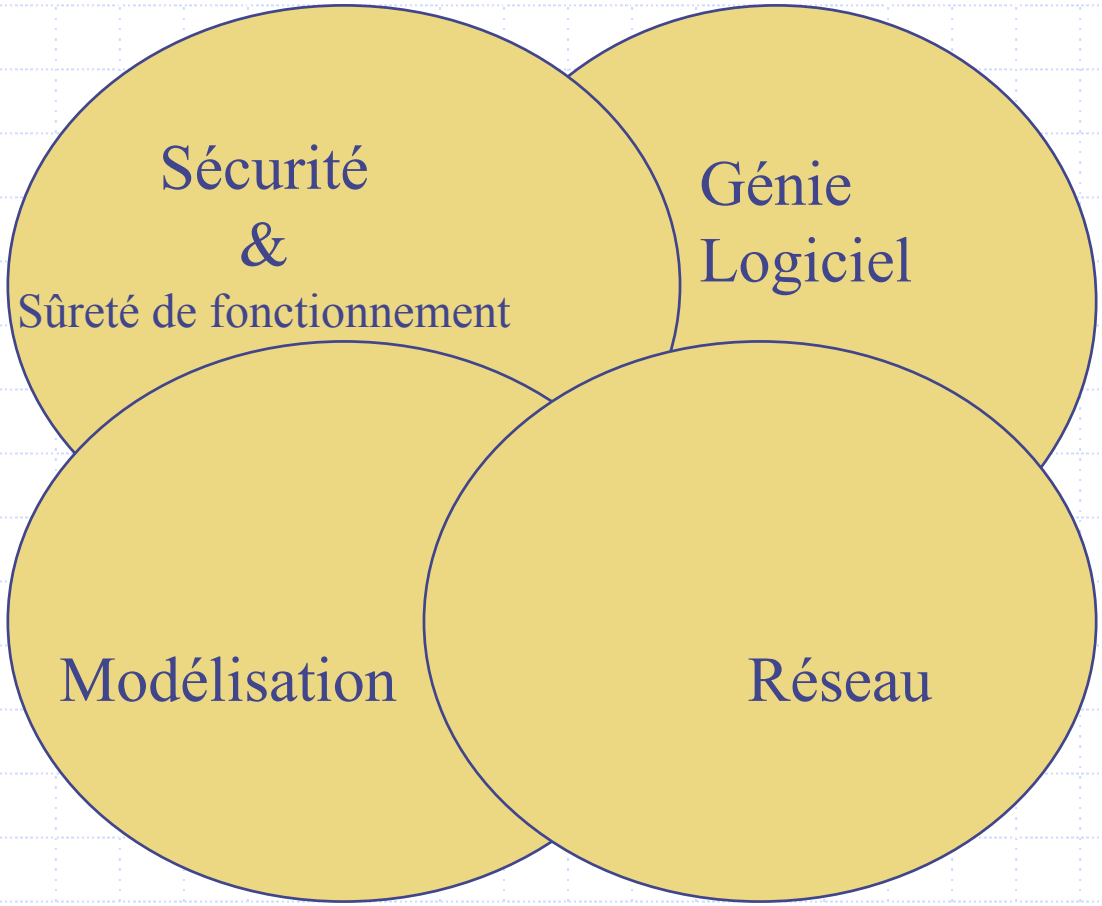
Notre Approche (3)

Couplage évaluation

- *par test &*
- *par analyse du modèle*

  - Valider l'évaluation par test
  - Comprendre le comportement de l'IDS

Conclusion


Sécurité
&
Sûreté de fonctionnement
Génie
Logiciel
Modélisation
Réseau

Questions