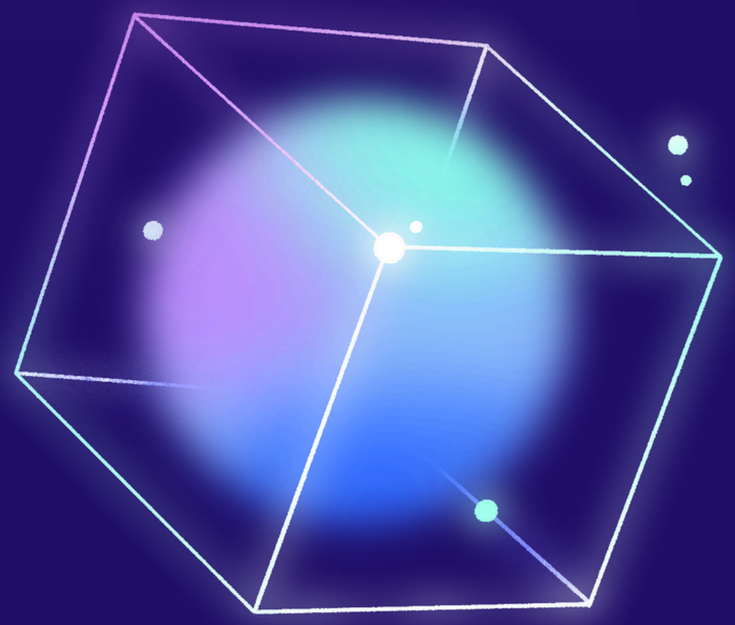
PLAN

CONTEXTE GÉNÉRAL

PROBLÉMATIQUE DE SÉCURITÉ

- Hausse exponentielle des cyberattaques (+67% en 2023)
- Limites des systèmes traditionnels (ex: règles statiques)
- Nécessité de systèmes NIDS (Network Intrusion Detection) précis et rapides.

CONTEXTE GÉNÉRAL



OBJECTIFS DU PROJET

Concevoir, évaluer et optimiser un système de détection d'intrusions réseau (NIDS) en utilisant des techniques de machine learning supervisé.

Comparer les performances de trois modèles classiques (XGBoost, Random Forest, MLP) sur les jeux de données NSL-KDD , afin d’identifier le modèle le plus efficace pour détecter à la fois les attaques fréquentes (DoS, Probe) et les attaques rares (R2L, U2R)

DATASET

NSL-KDD : JEU D’ENTRAÎNEMENT ET DE TEST

Pourquoi ce dataset ?

Structure multi-classe bien adaptée

- Il contient plusieurs types d’attaques : DoS, Probe, R2L, U2R, et Normal.

Challenge de déséquilibre des classes

- Idéal pour tester à la fois la capacité d’un modèle à détecter des attaques fréquentes (DoS) et rares (U2R)

Données tabulaires structurées:

- Facilement exploitable sans nécessité de traitement lourd comme pour des fichiers pcap bruts.
- Les 36 features sont déjà préformatées en caractéristiques numériques ou catégoriques .

DATASET

NSL-KDD : JEU D'ENTRAÎNEMENT ET DE TEST

La structure de dataset :

Le dataset NSL-KDD est structuré en 2 parties distinctes :

Fichier	Usage	Nombre d'échantillons	catégories Attaques
KDDTrain+	**Entraînement**	~4 000	Normal, DoS, Probe, R2L,U2R
KDDTest+	**Test**	~22 500	mailbomb, apache2, udpstorm, xterm, ps, sqlattack ...etc

Note: KDDTrain+ est un sous-ensemble équilibré (4K échantillons) pour éviter le biais de classe, tandis que KDDTest+ (22K) conserve la distribution déséquilibrée réelle du trafic réseau pour une évaluation réaliste.

MODELES

SELECTION DES DES MODÈLES NIDS

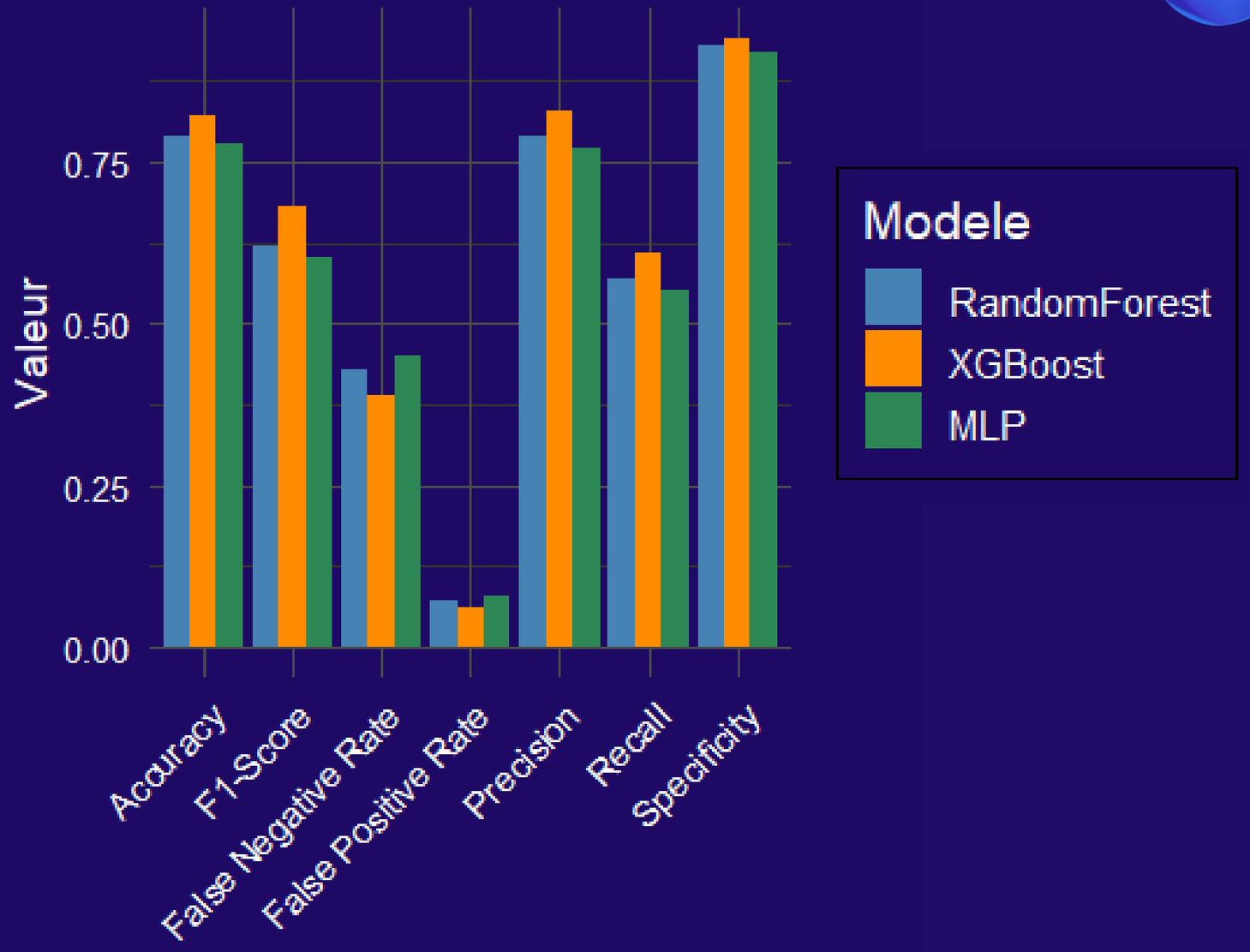
Modèle	Type	Principes clés	Avantages	Inconvénients
Random Forest	Ensemble d’arbres	Plusieurs arbres de décision construits sur des sous-échantillons aléatoires	Robuste au surapprentissage, facile à utiliser	Peut être lent avec beaucoup d’arbres, sensible au déséquilibre
XGBoost	Gradient Boosting	Arbres construits séquentiellement en corrigeant les erreurs précédentes	Haute précision, rapide, bon sur déséquilibre	Nécessite tuning fin des hyperparamètres
MLP (Perceptron multi-couches)	Réseau de neurones	Couches entièrement connectées avec non-linéarités	Modélisation des relations complexes	Sensible aux paramètres, plus coûteux en calcul

MODELES

XGBoost montre une bonne performance générale.

RÉSULTATS SUR LE JEU DE TEST

Performance Globale (Test Set)



MODELES

XGBoost

Excellente détection des attaques DoS (89%) et Probe (83%).

MLP

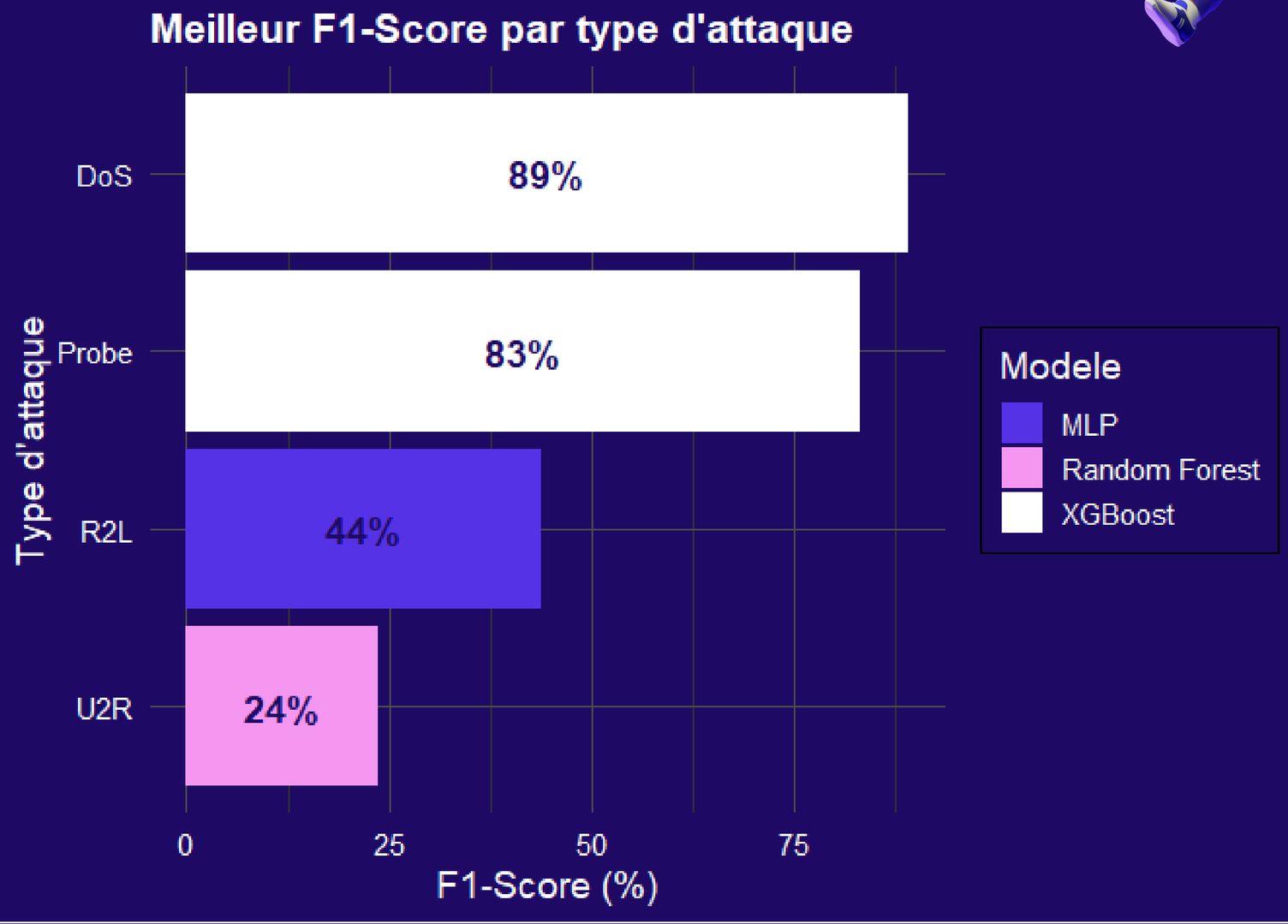
détecte mieux R2L que les autres modèles (reste insuffisante)

RF

Précision U2R légèrement meilleure que les autres modèles.

ANALYSE DES RÉSULTATS PAR CLASS

Détection par Type d'Attaque



MODELES

ANALYSE DES RÉSULTATS PAR CLASS

les points clés observés pour chaque modèle

XGBOOST

Forces	Faiblesses
Meilleure accuracy globale (0.82).	Performance moyenne sur les attaques **R2L** (F1: 44%).
Meilleure F1-Score globale (0.68).	Complexité de réglage des hyperparamètres.
Excellente détection des attaques DoS (89%) et Probe (83%).	
Taux de faux positifs et faux négatifs les plus bas.	

MODELES

RÉSULTATS ET ANALYSE

les points clés observés pour chaque modèle

RANDOM FOREST

Forces	Faiblesses
◆ Très bon score de **Spécificité** (0.93) → détecte bien le trafic normal.	◆ **Recall faible** (0.57) → beaucoup d'attaques passent inaperçues.
◆ Faible **taux de faux positifs** (0.07).	◆ Mauvaise détection des attaques **U2R** (F1-score 24%).
◆ Bonne performance sur **DoS** et **Probe**.	◆ Faible **F1-Score global** (0.62) par rapport à XGBoost.

MODELES

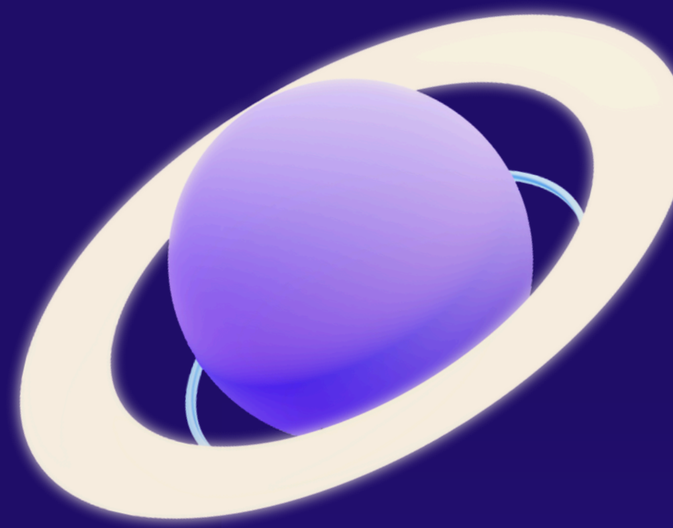
RÉSULTATS ET ANALYSE

les points clés observés pour chaque modèle

MLP

Forces	Faiblesses
◆ Bonne détection des **attaques R2L** (F1-score 44%) – comparable à XGBoost.	◆ **F1-Score le plus faible globalement** (0.60).
◆ Réseau efficace sur les classes minoritaires (relativement).	◆ Mauvaise détection des **U2R** (24%) et **Recall** global le plus faible (0.55).
	◆ Plus sensible aux réglages et nécessite plus de données pour généraliser.

CONCLUSION



XGBoost est globalement le modèle le plus performant.
Les classes rares (U2R, R2L) restent difficiles à détecter.

Future Work :
Pour améliorer la détection des attaques rares (U2R/R2L),
nous envisageons une approche hybride combinant XGBoost
avec des modèles d'anomalies (Isolation Forest)