Présentation de différents de nos résultats notamment au sujet de la méthode substitut, de test de robustesse Etc.

Au sujet de la démo :

Il sera préférable d'énoncer les résultats globaux de l'entraînement
L'intérêt de la démo est le cœur du sujet, la présentation des attaques etc
La démo a pour but de se concentrer sur le cœur du sujet : la présentation des modèles, des attaques et leurs résultats.

Pour la présentation :

Il va falloir faire attention à la durée de la présentation, le sommaire est fourni et nécessite donc que nous soyons conscients du temps limité.

Pour la robustesse :

On peut tester l'entrainement du RF que sur les données adverses, les premiers tests semblent montrer qu'une faible amélioration ou pas du tout.
Il est possible d'entrainer à nouveau un RF, peux être que ça risque de prendre un peu de temps pour un dernier jour.
Si on entraine un nouveau modèle, les données adverses sont noyées par les données clean.
Il est préférable d'entrainer à nouveau un modèle déjà entrainé avec uniquement des données adverses.
Fusionné deux Random Forest entrainé sur des types de données différentes ?
Se concentrer sur le recall et les matrices de confusion.
Les Clipping, Clamping, Round, conservent-ils la Cohérence logique ?Oui
Le fait de modifier les attaques adverserial pour les rendres réaliste n'est pas un risque de les rendre Bénignes ? pas forcément.

Retour très positif sur nos échanges durant l'entièreté du projet et notre attitude.

Feedback sur les sujets/ organisations du modules/retour sur les entretiens:

Sujets : Sujets suffisamment variés pour permettre un choix de cœur des projets.
Organisation : Durée devrait être x2, les organisations d'EDT nous ont fait ressentir un fait de 2 semaines. Il pourrait être utile que la période de projet soit plus longue avec mi-temps sur une période pour permettre. Mettre par exemple en parallèle avec la transition des parcours.
Entretiens : toujours très utile et bienveillant.