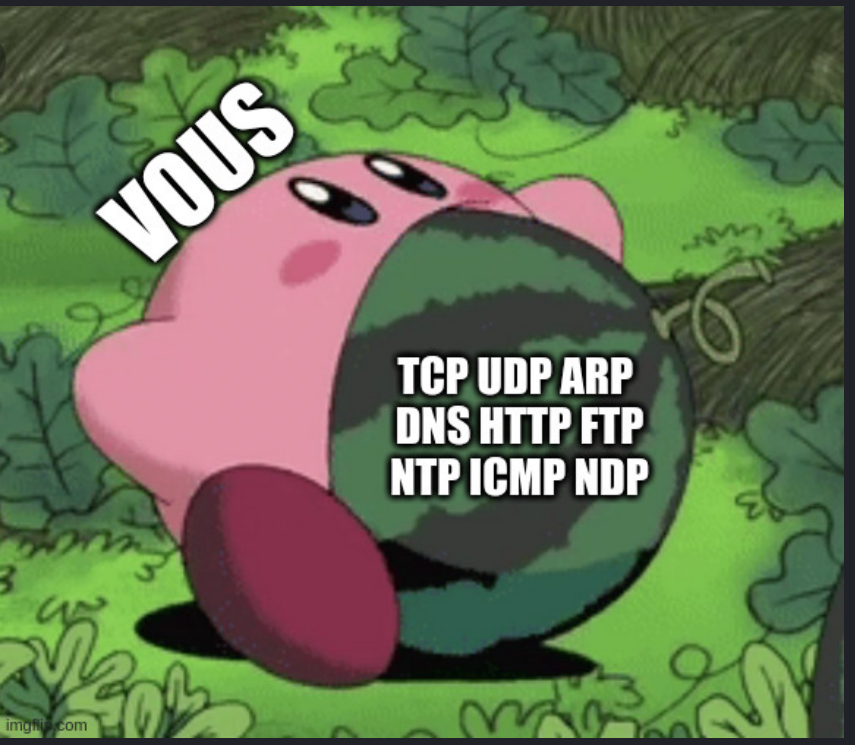
Projet Cyber/IA

Détection de trafic réseau malveillant par Intelligence Artificielle

Pablo Bondia-Luttiau

Problématique

- Trop de trafic pour tout journaliser
- Peu de visibilité sur les menaces de bas niveau
- Détecter au plus tôt les flux malveillants



Qui est visé ?

- Curieux de découvrir la Cyber
- Appétence pour le réseau

Quoi ?

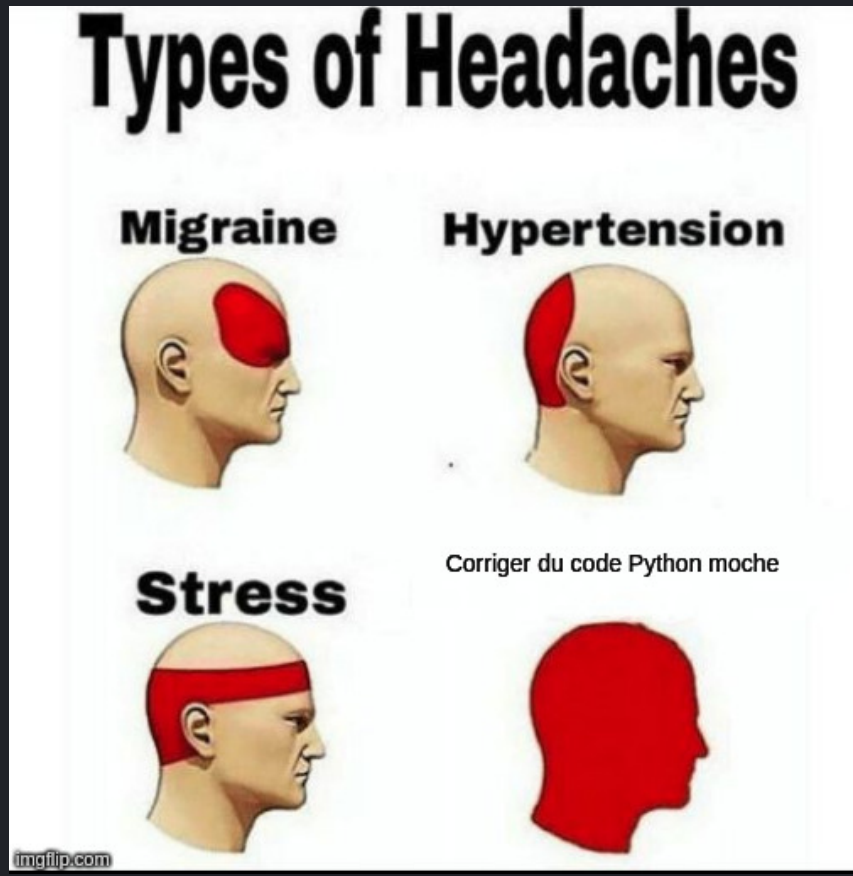
- Détection d'attaques potentielles
- (D)Dos, Reverse Shell, DNS Tunnelling, exfiltration de données...
- Analyse :
    1. En offline avec fichier
    2. En live (bonus)
    3. Dans le Kernel (bonus++)

Comment ?

- Python (Pytorch, TF, etc. autorisés)
- Git avec bonne gestion des branches
- Wireshark
- Le reste est à vous de voir !

Attendus

- Gestion de projet et découpage des tâches
- Code propre
- Compte-rendus réguliers
- Tests de l'IA avec des flux d'un serveur de production



Points importants

- Points d'avancement != Surveillance de masse
- Idées supplémentaires != Lèche-c...arotte
- Soutenance != Cassage de rotules

Amusez-vous

P.S

Les 16 cartes Nvidia A100 de GLiCID devraient vous aider à entraîner votre modèle d'IA ;)

Contact pour questions

Pablo Bondia-Luttiau
Responsable sécurité et Admin Sys/Réseau GLiCID
Bureau T126
pablo.bondia-luttiau@ec-nantes.fr