Security Uses Case

IDS - TEAM N°4

09/12/2026

Yann PATE
Romain PARADA
Baptiste RAUX
Maxim QUÉNEL
Pierre REYNAUD
Enzo POLIZZI

Intrusion detection system

1. Introduction and Problem Statement

Why it is related to AI ?

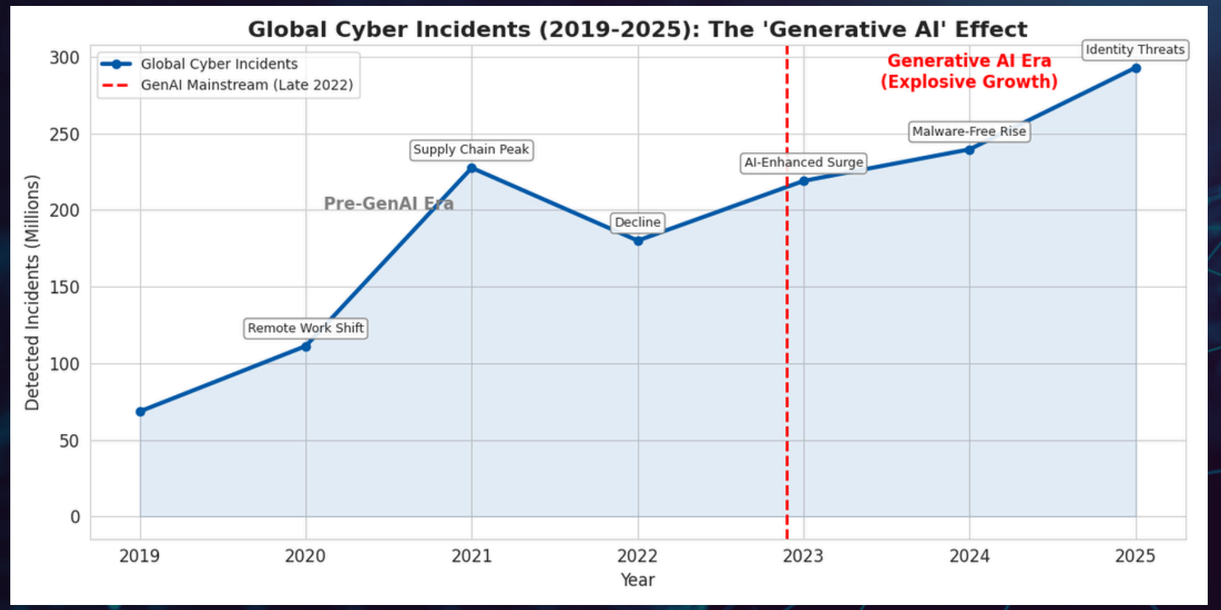
- Attacker increase their capability thanks to AI
- We need to defense oursleves in the same way

What we want to secure ?

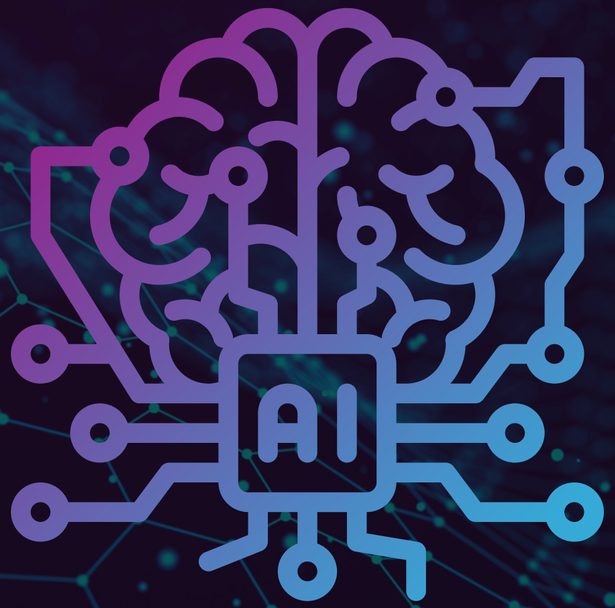
- Secure endpoint that are the gatedoor of apps

What we want to provide ?

- Provide a tool that recognize thanks to AI a cyber threats and this process need to be real quick to handle as many as possible request per seconds

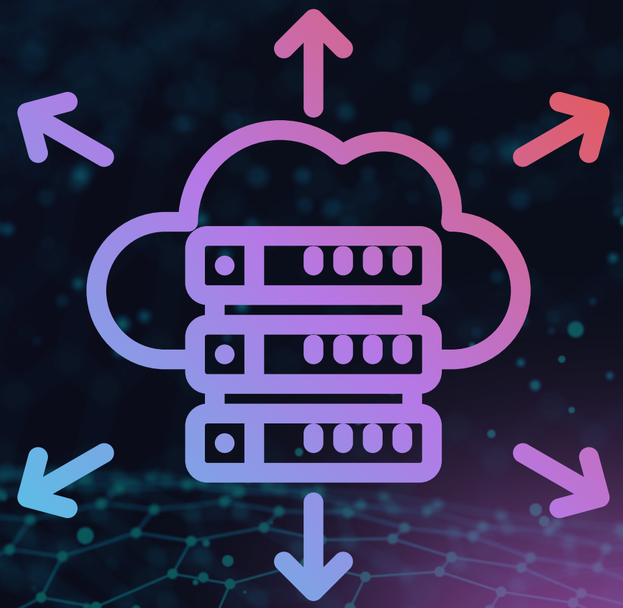


2. Background and Theoretical Foundations



Ai pillar

Cybersecurity pillar



Cloud computing pillar

AI - Background and Theoretical Foundations

Apprentissage Supervisé & Classification Binaire

Objective : Classify Network Traffic (Normal vs Attack)

Model : Gradient Boosting Decision Trees (GBDT)

Implementation : CatBoost (Categorical Boosting)

StandardScaler
Normalization of numerical variables (Mean=0, Var=1)

OneHotEncoder
Transformation of categorical variables

Boosting Mechanics

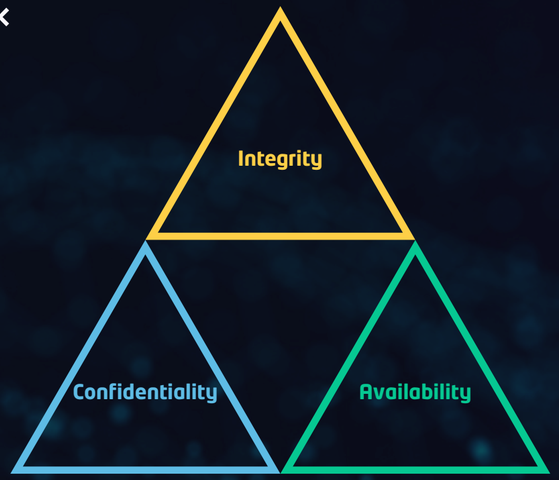
SEQUENTIAL OPTIMIZATION VS BAGGING

Gradient Descent

Each new tree learns from the errors of the previous one.

Minimization of the Loss Function in function space.

Cybersecurity - Background and Theoretical Foundations



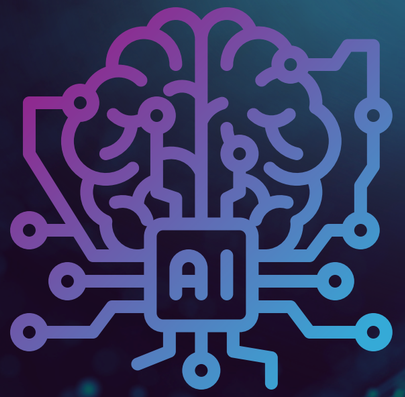
CIA TRIAD

Traditional attack and where they occurs

" When attacks are rare, high accuracy can be misleading "

-

- Accuracy different than Security Quality



AI-Augmented threats

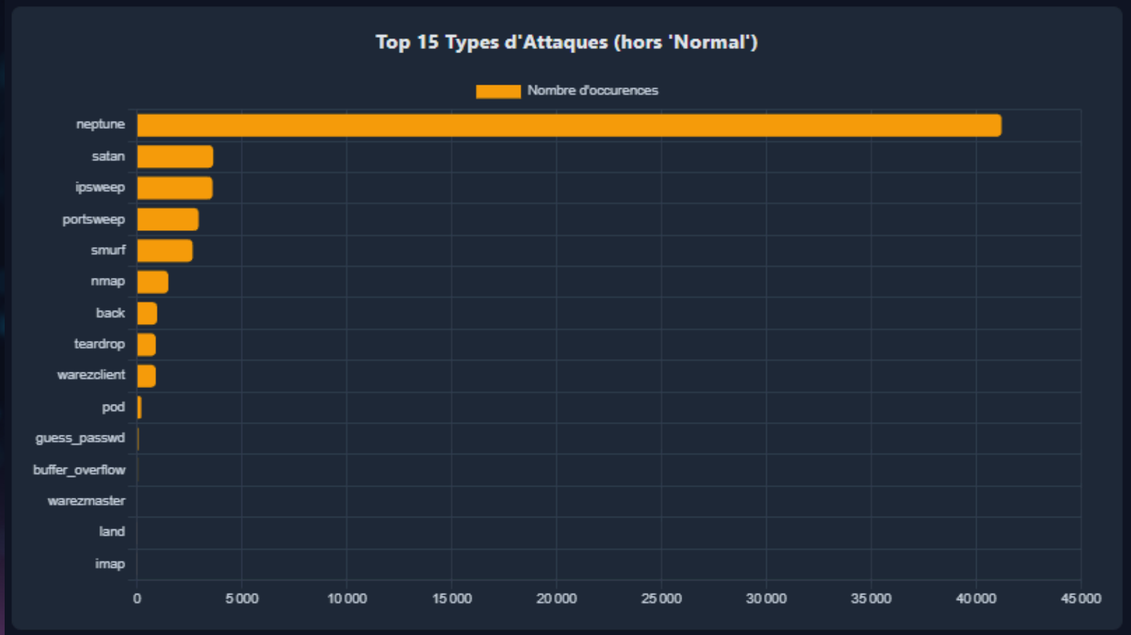
Cloud computing - Background and Theoretical Foundations

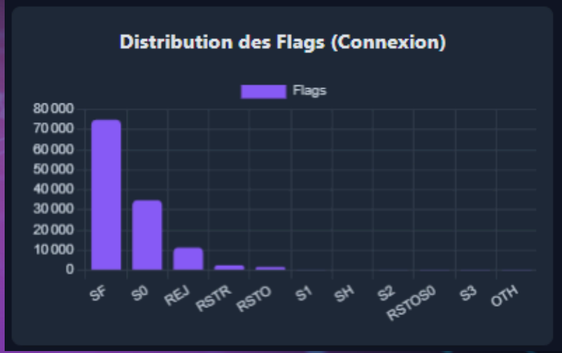
Orchestrator

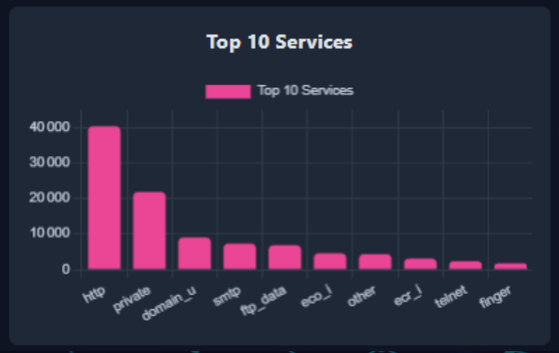
Image/ Container

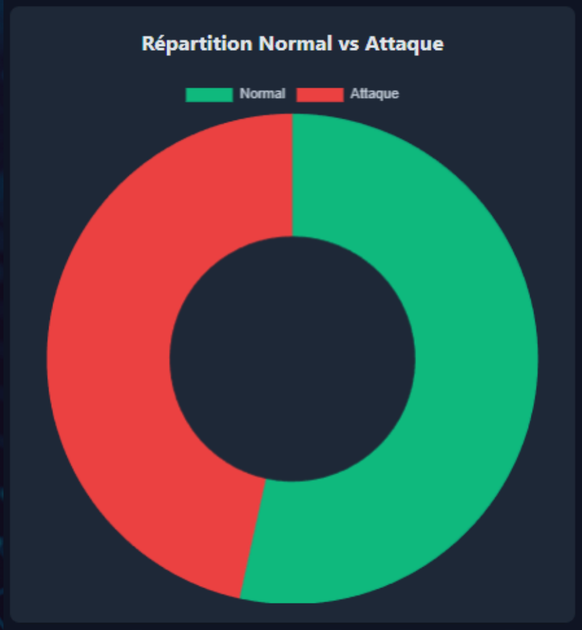
Request

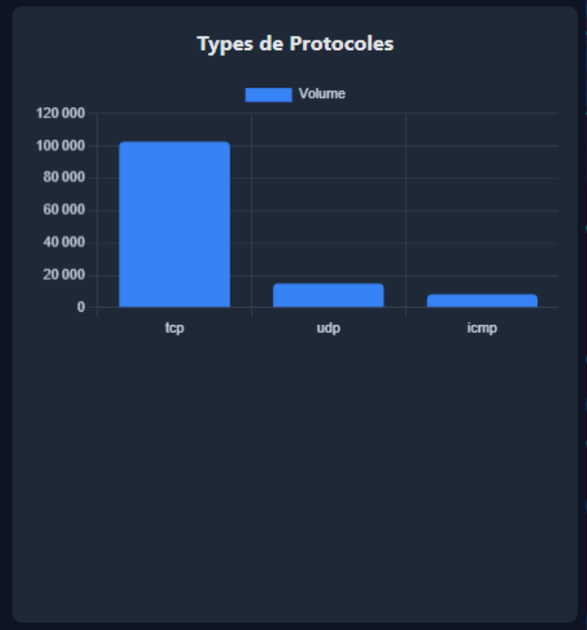
3. Dataset: Selection, Preprocessing and Challenges - Training dataset



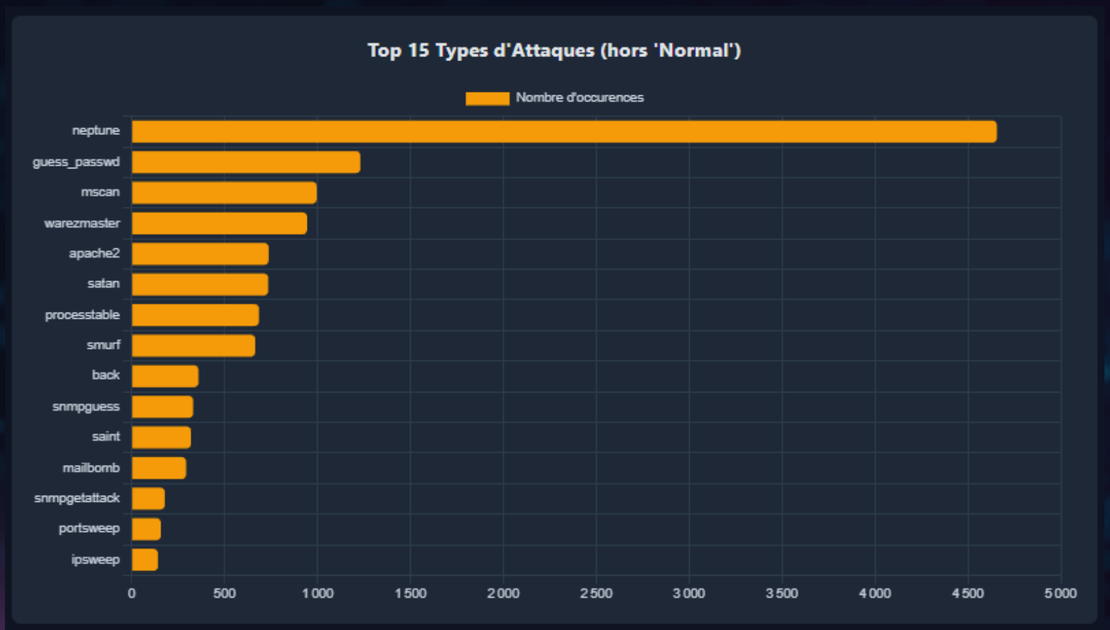


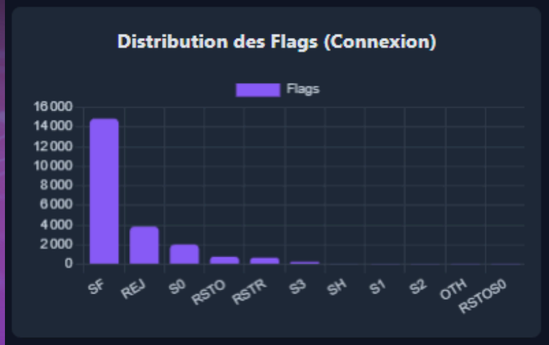


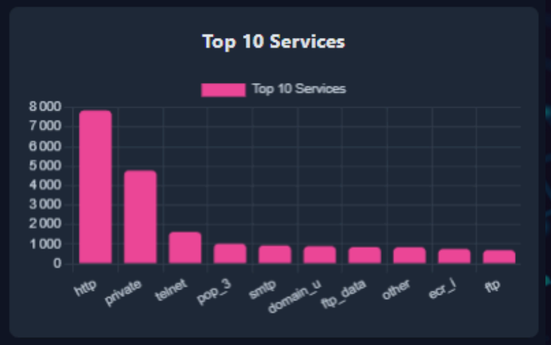


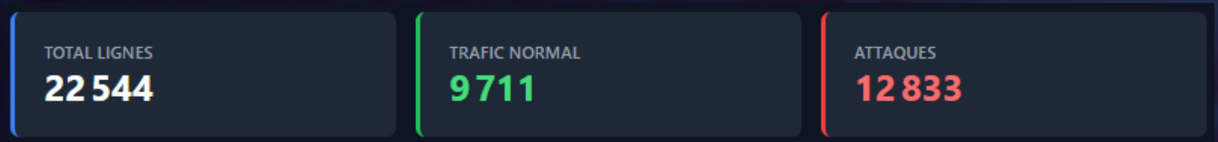


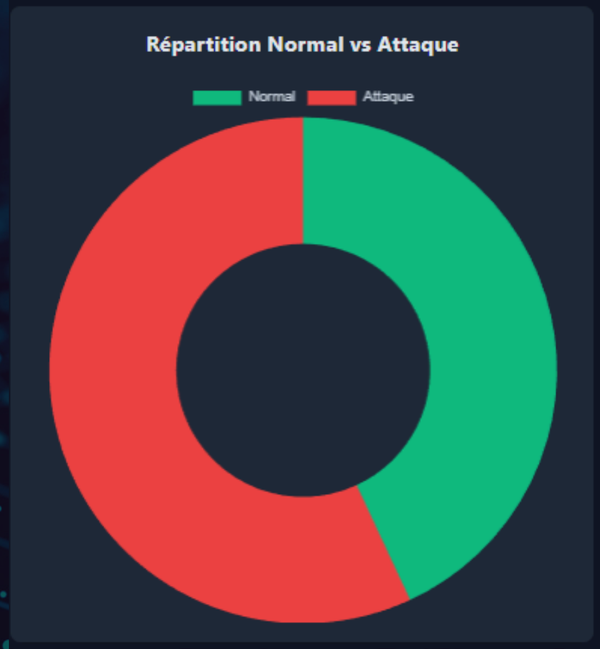
3. Dataset: Selection, Preprocessing and Challenges - Testing dataset

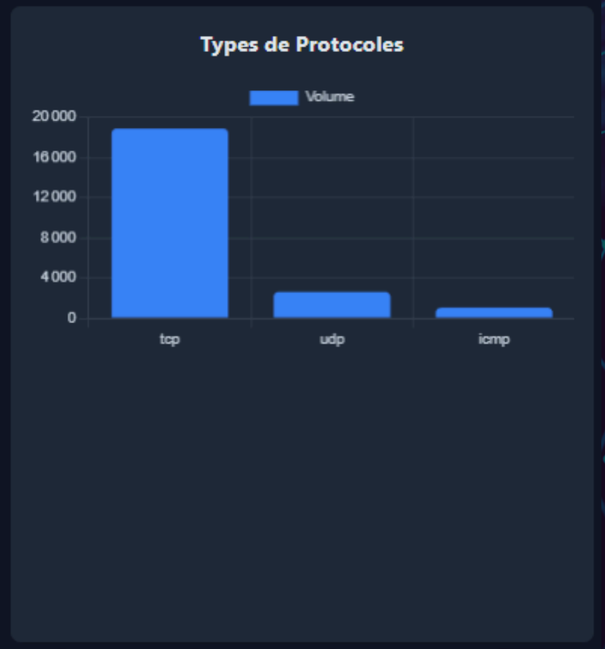








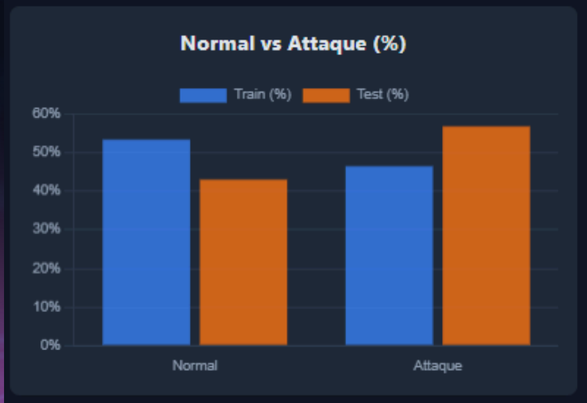


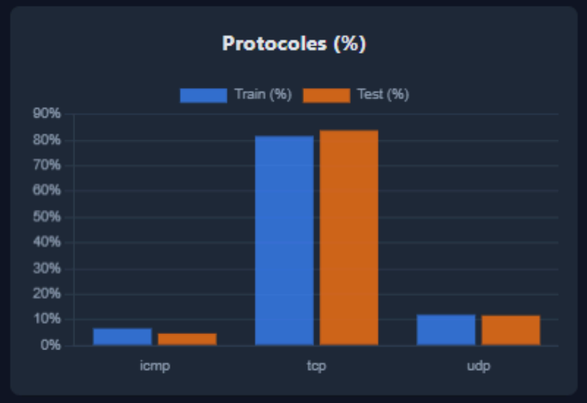


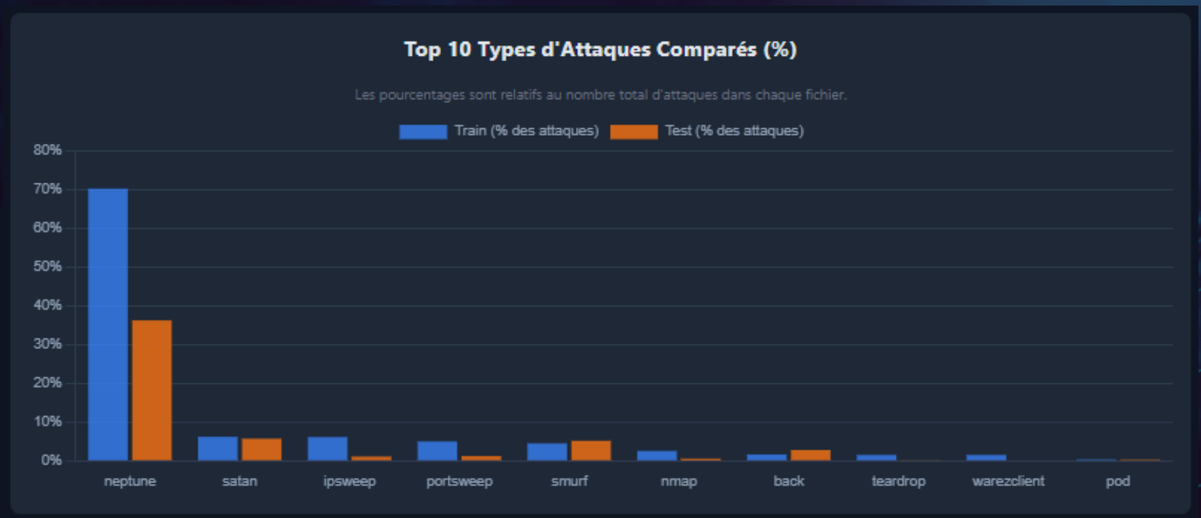
3. Dataset: Selection, Preprocessing and Challenges

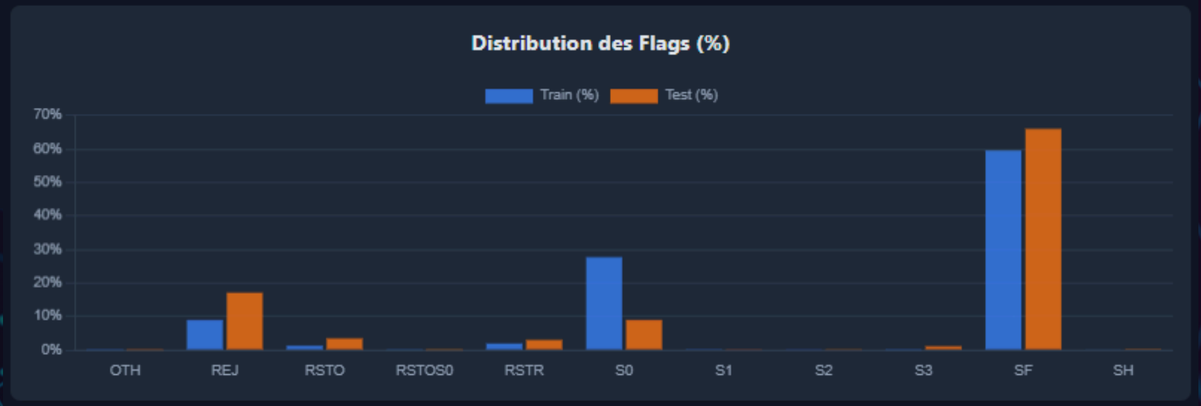
TAUX D'ATTAQUE (TRAIN)
46.5%

TAUX D'ATTAQUE (TEST)
56.9%



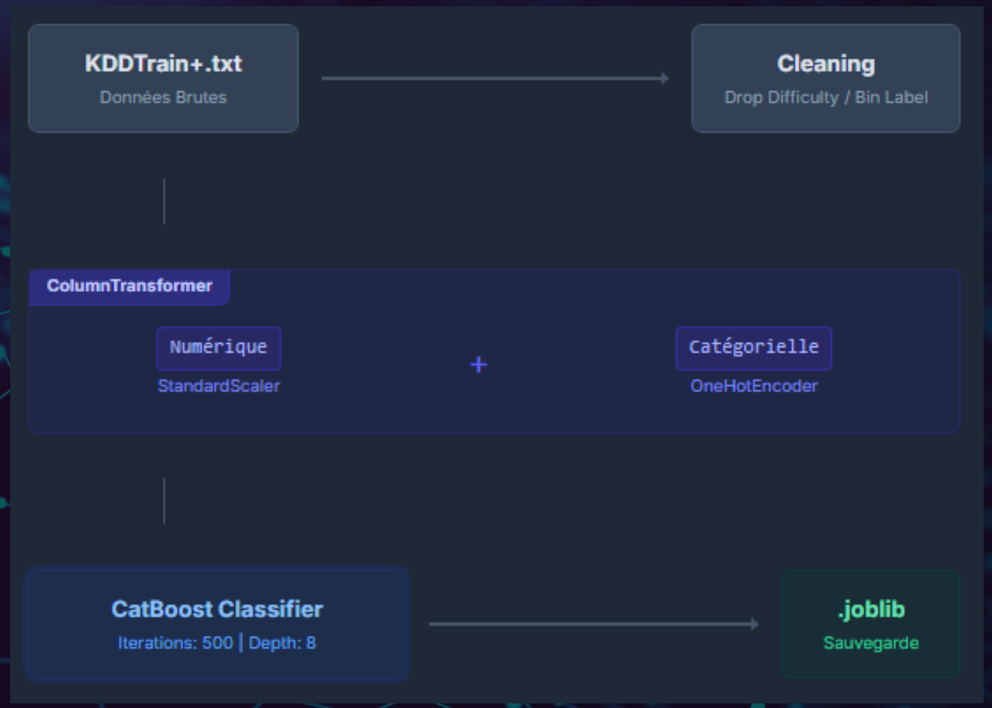


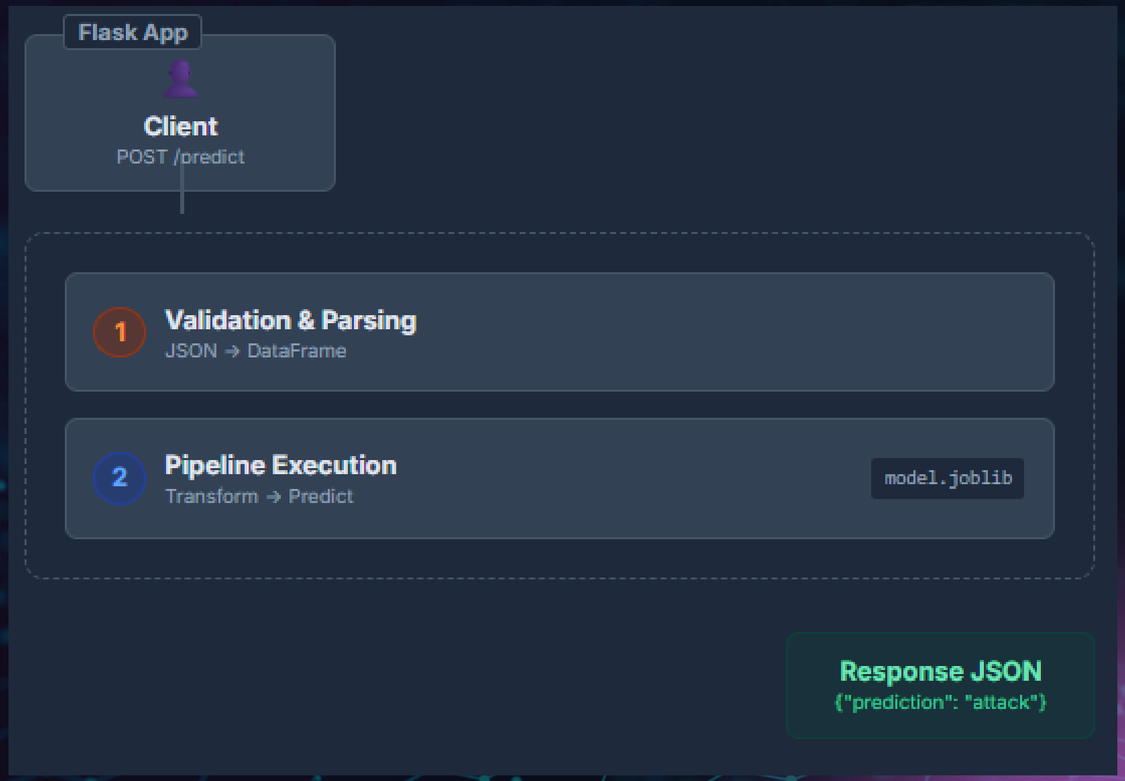




[Source Kaggle dataset NSL-KDD]

4. AI Methodology and Workflow





4. Methodology and Workflow

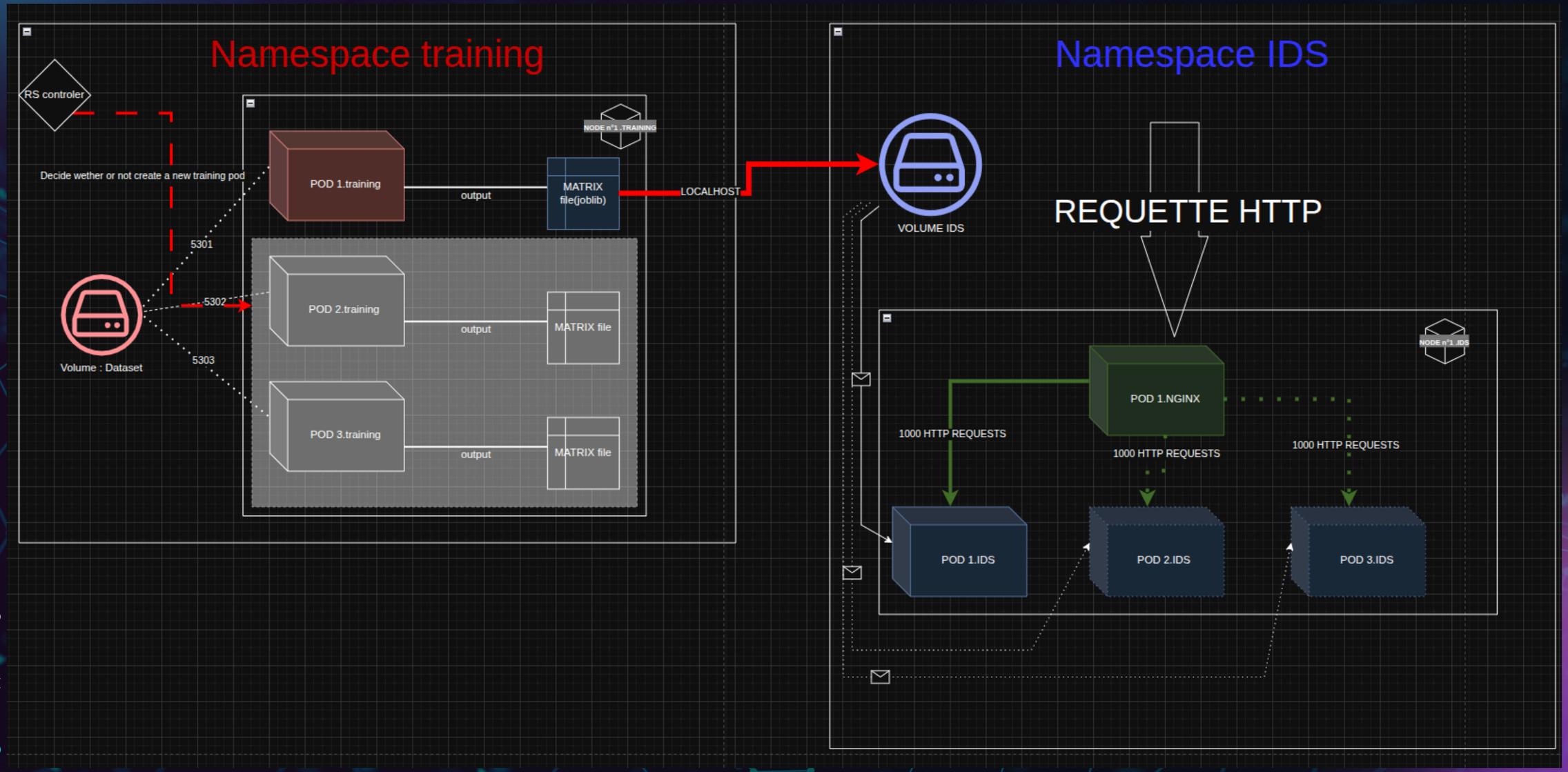
Performance Summary

Metric comparison by model

FINAL ANALYSIS

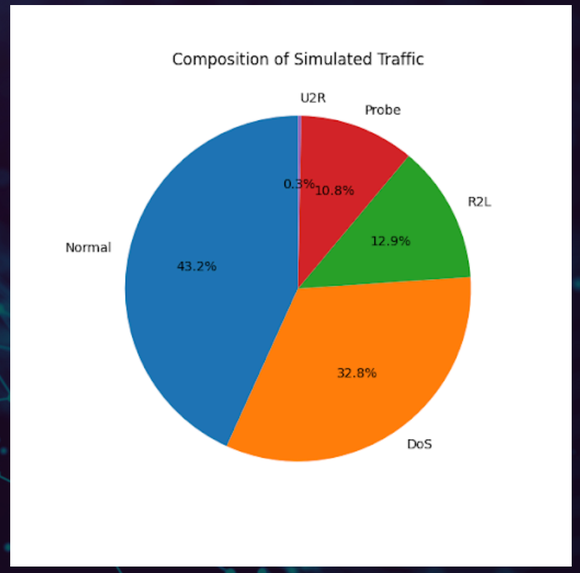
MODEL	ACCURACY	PRECISION	RECALL	F1-SCORE	ROC-AUC
VotingClassifier	0.799	0.968	0.661	0.791	0.972
LightGBM (Optimized)	0.805	0.970	0.680	0.804	0.970
ForestRegressor	0.781	**0.970**	0.640	0.780	0.970
CatBoost	**0.889**	0.960	**0.840**	**0.896**	0.970
XGBoost	0.851	0.968	0.762	0.853	**0.974**

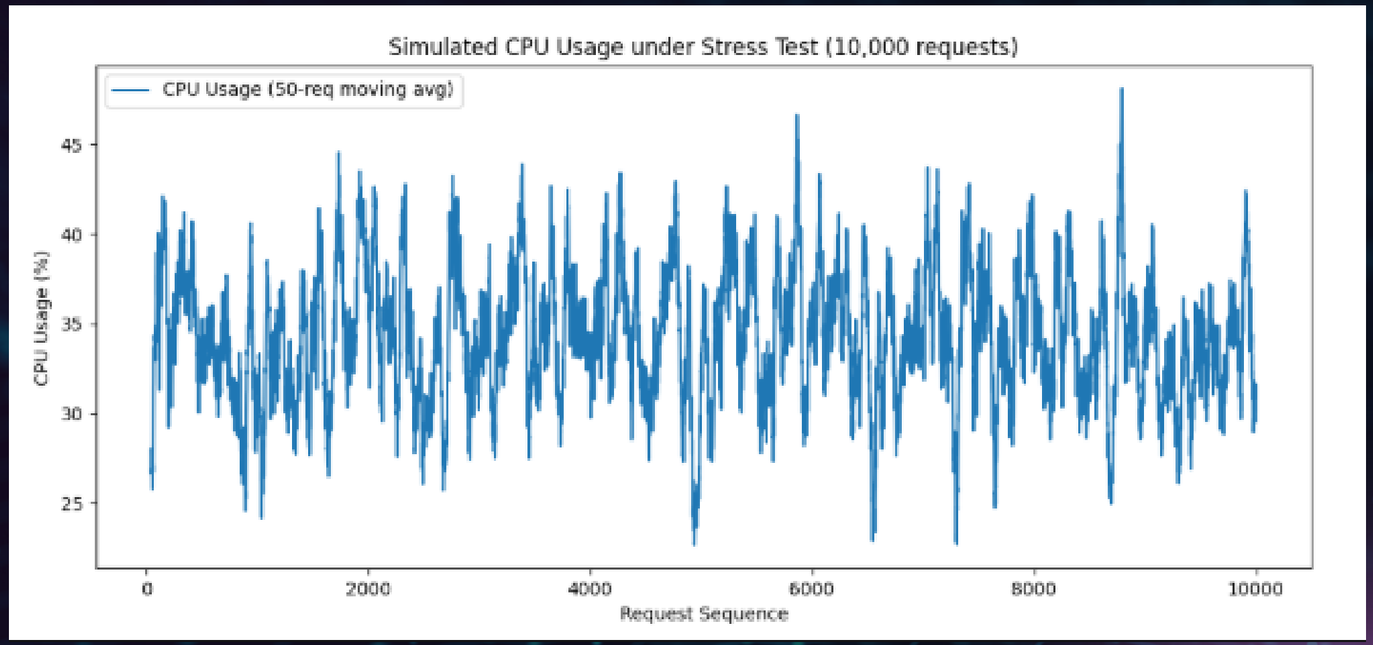
4. Methodology and Workflow



4. Workflow - Stress test

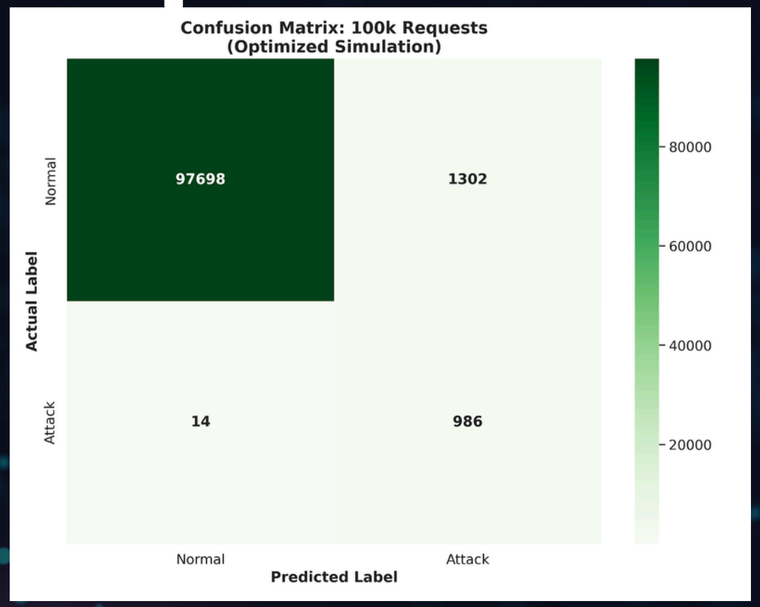
- Stress Test before optimization with **10,000 requests to see ressources limits**

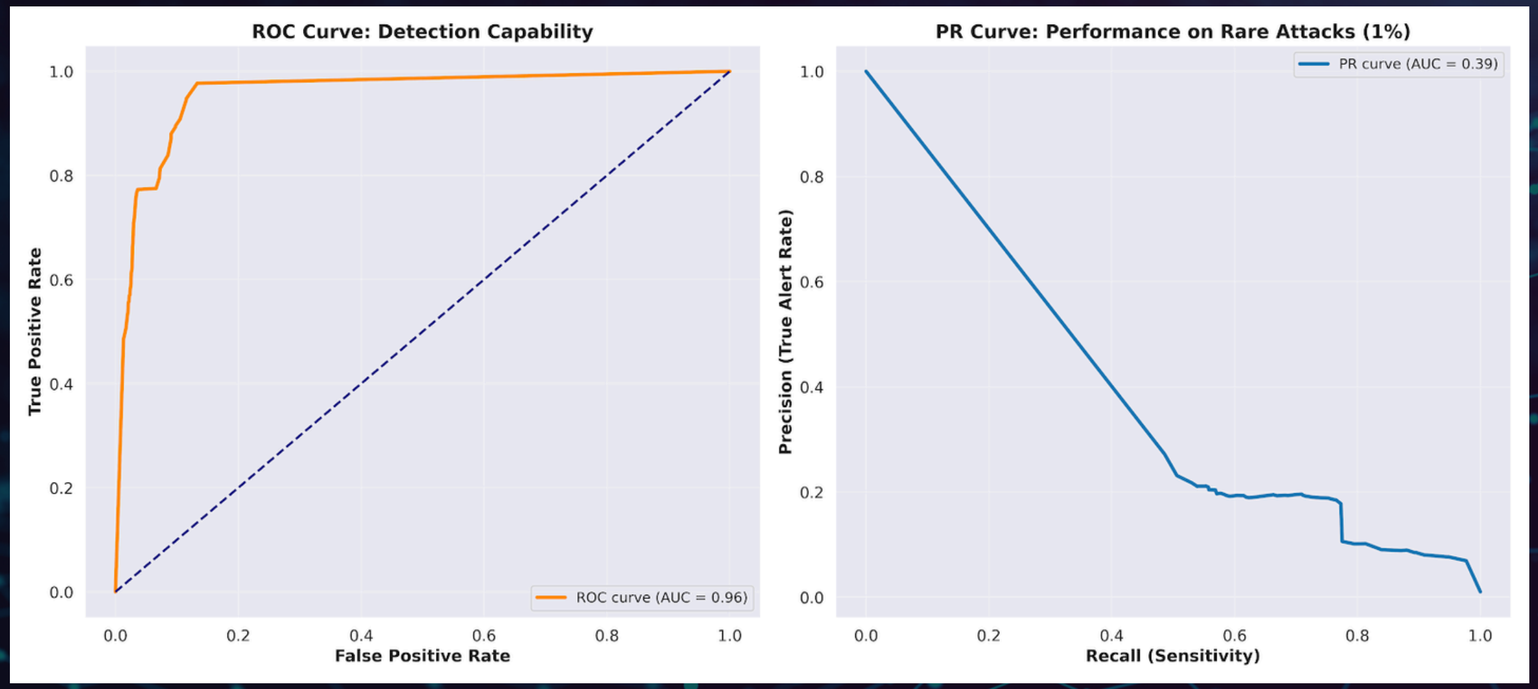


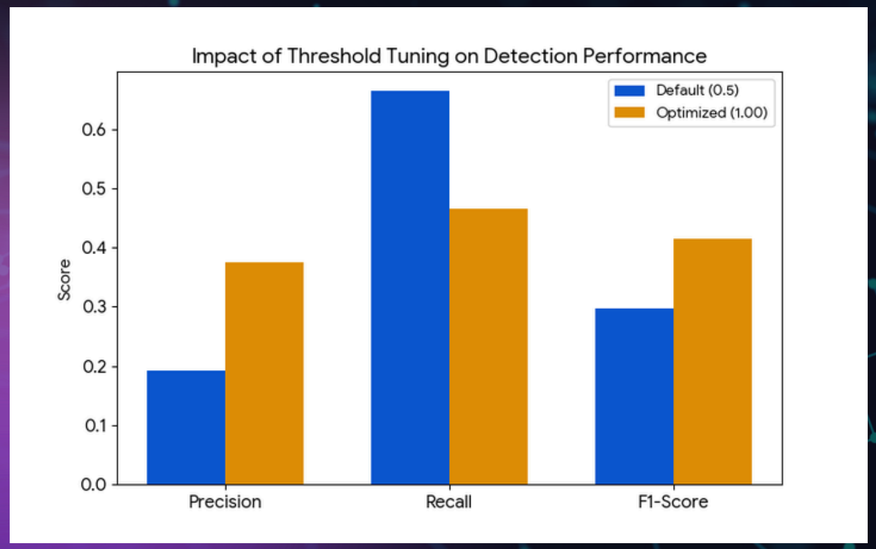


- Configure a **Horizontal Pod Autoscaler** to trigger when CPU usage **exceeds 70%**, ensuring the system **stays responsive** during the attack spikes identified in this report.

5. Results and Analysis Present 100 000 requets







6. Group Organisation and Project Management

Agile management with Jira

Meeting every 2 weeks

- Docker group - Yann / Pierre
- Kubernetes group - Romain / Baptiste
- AI group - Maxim
- Agile product manager - Enzo

Repository with branch rules

3 main issues

7.Conclusions and Perspectives

Key Points & Achievements

Automated & Scalable IDS

Creation of an intrusion detection system capable of automated scaling to handle load.

Plug-and-Play Solution

Modular design allowing for instant deployment and seamless integration into existing infrastructure.

Documented Architecture

Comprehensive technical documentation of the architecture to facilitate maintenance and handover.

Architecture & Security

1. **Container Hardening**
   Transitioning from standard images to **private Docker images** to minimize the attack surface.
2. **Advanced Orchestration**
   Fine-tuning **Pod management** for increased resource isolation and resilience.

Goal: Infrastructure Robustness

Data & Modeling

1. **Dataset Balancing**
   Correcting **class disparity** in the dataset to avoid bias towards majority attacks.
2. **Generalization (Zero-day)**
   Improving detection of novel threats present in **testing** but absent from training.

Goal: Predictive Reliability

THANK YOU!

Yann PATE
Romain PARRADA
Baptise RAUX
Maxim QUÉNEL
Pierre REYNAUD
Enzo POLIZZI

TEAM N°4