COMPARAISON DE DIVERSES REPRÉSENTATIONS DE MALWARES POUR L'APPRENTISSAGE AUTOMATIQUE

PROJET DE RECHERCHE

LAURA MONTAGNIER

SOMMAIRE

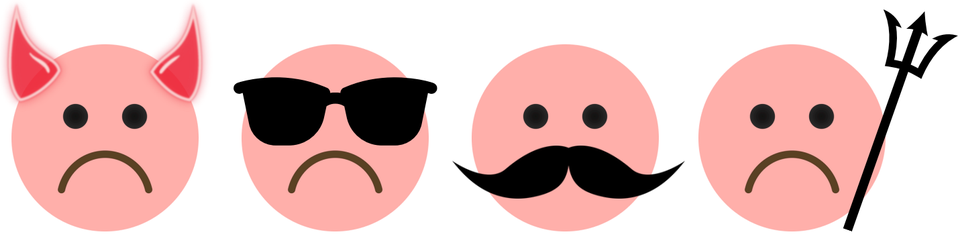
- Notions de base
- Différentes représentations
- Construction d’une API
- Evolution de l’API
- Résultats

3

NOTIONS DE BASE

- Cleanwares

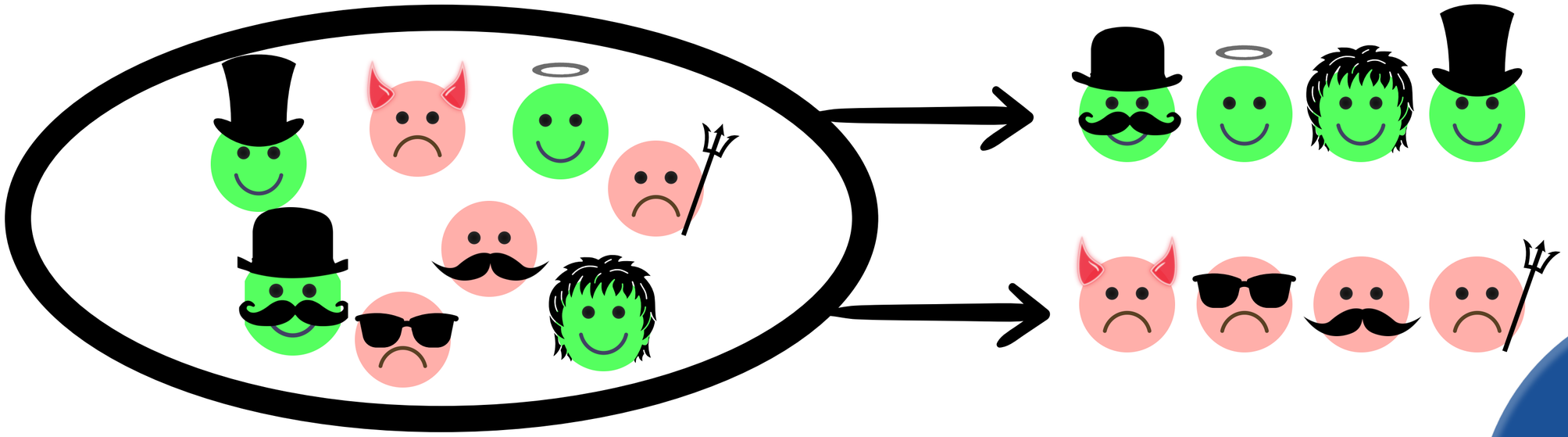
- Malwares



4

NOTIONS DE BASE

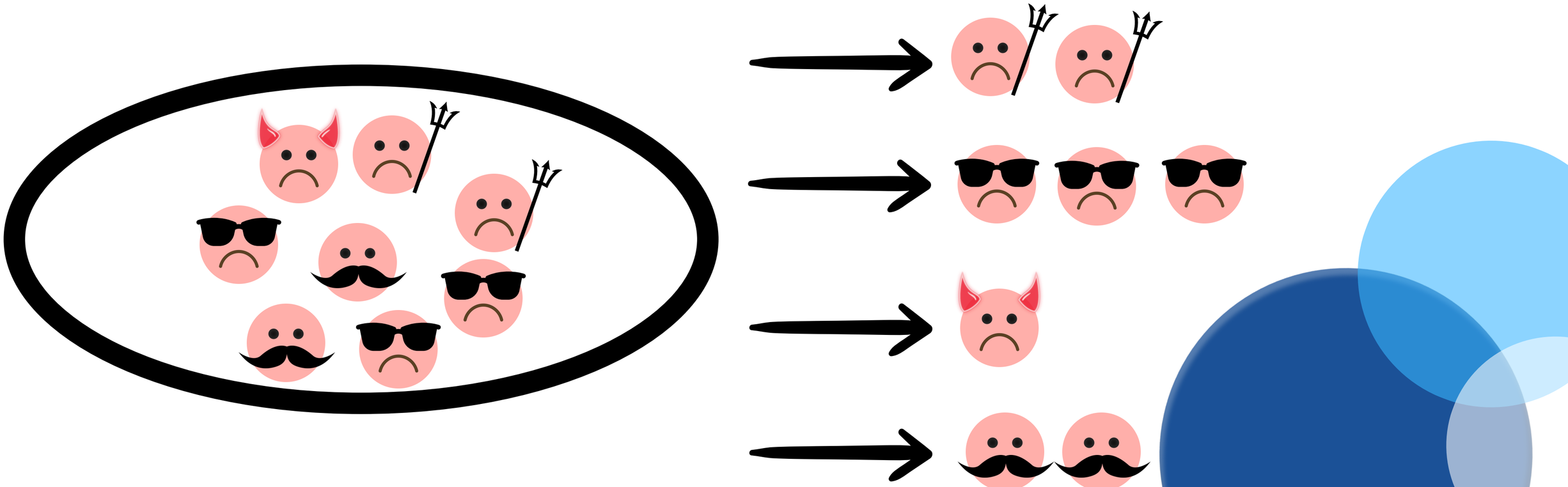
La Détection



5

NOTIONS DE BASE

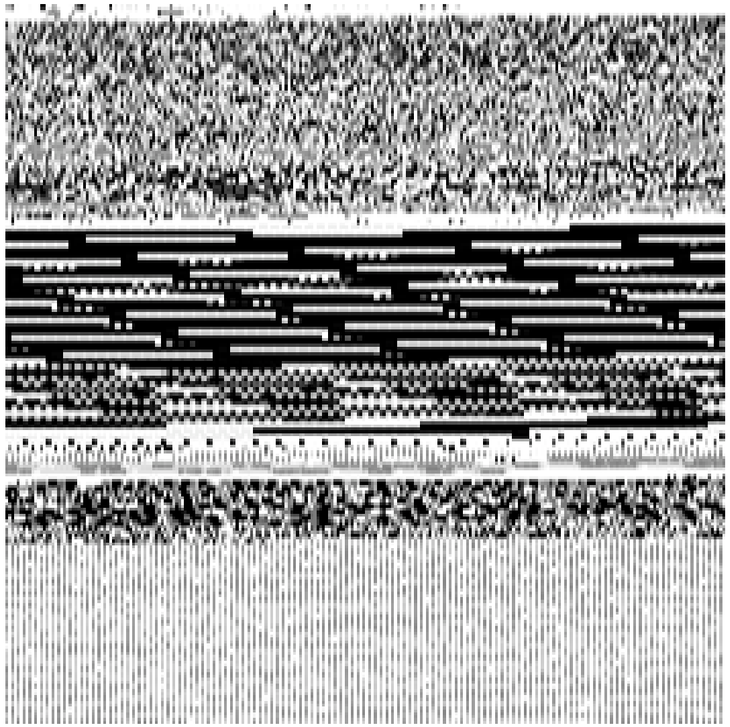
La Classification



6

DIVERSES REPRÉSENTATIONS

- Grayscales
- Graphes d’entropie
- PE_feats
- EMBER

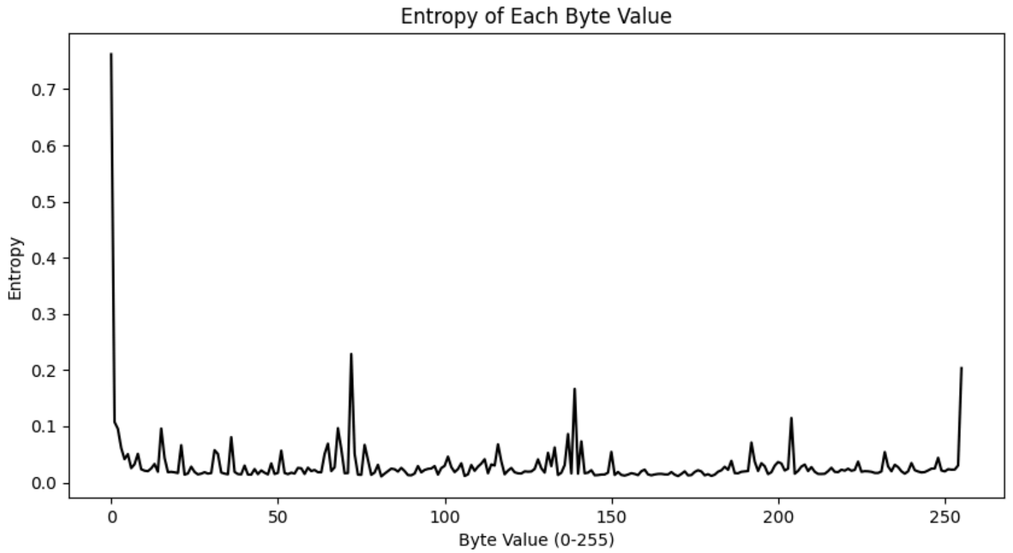


GRAYSCALES

- Statique, une image
- Chaque byte a une couleur qui correspond à sa valeur, 0 pour le noir, 255 pour le blanc

8

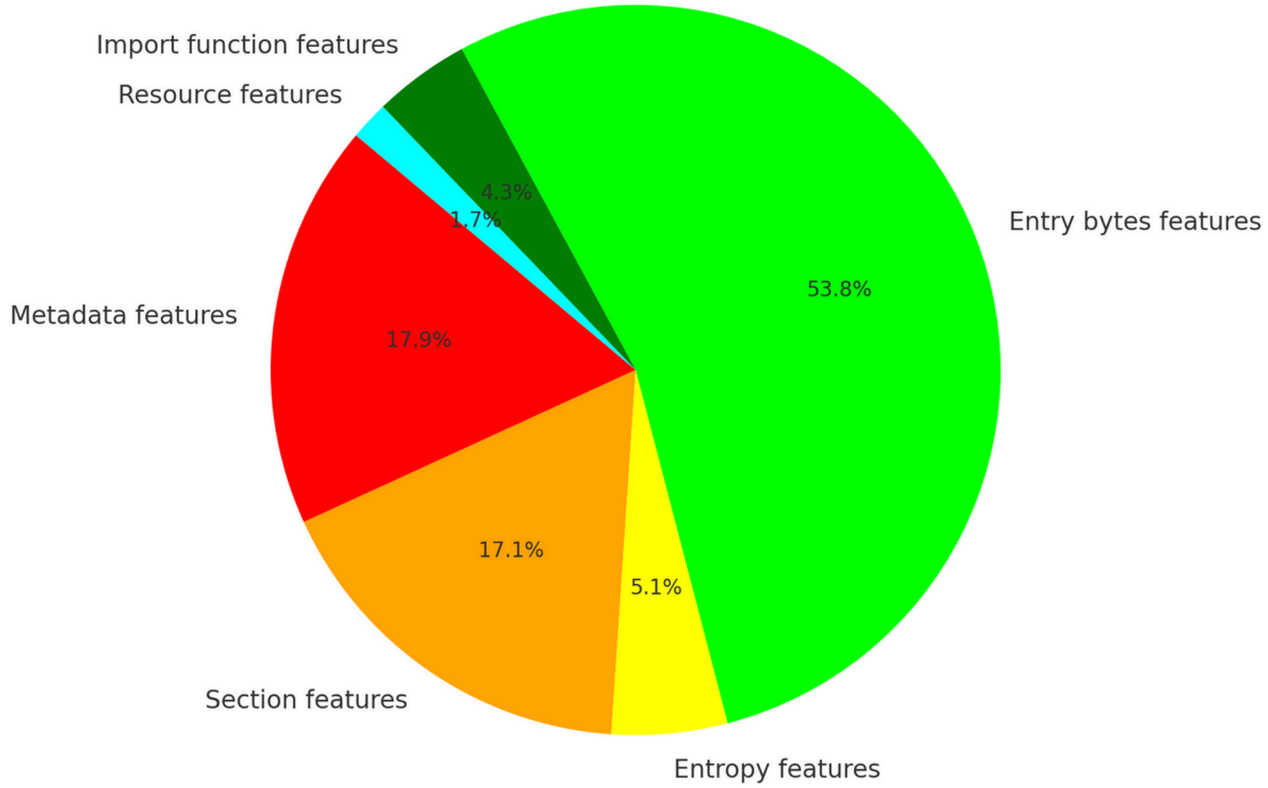
GRAPHES D’ENTROPIE



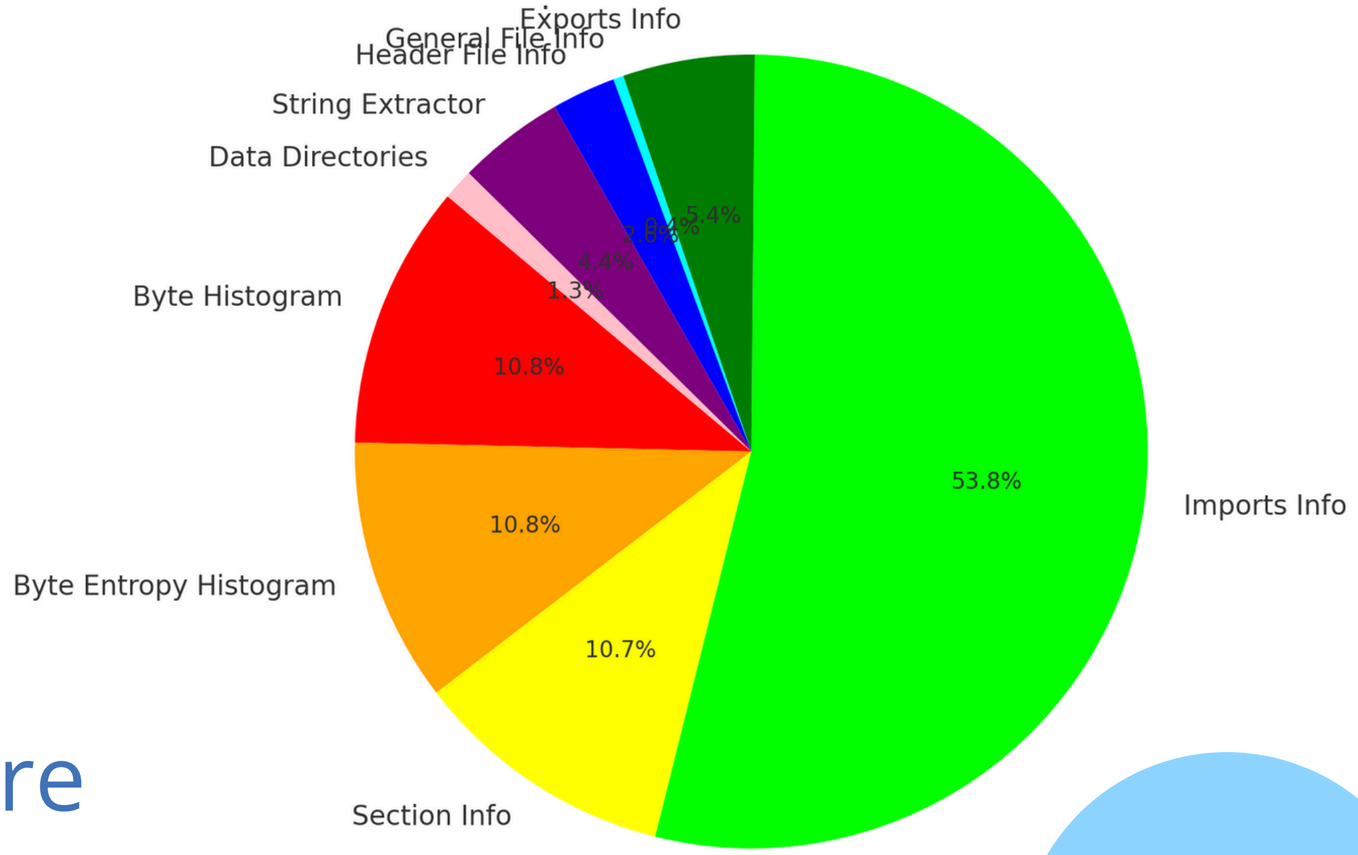
- Statique, une image
- Calcul de l’entropie de chaque *byte*

PE_FEATS

- Statique et tabulaire
- 119 features

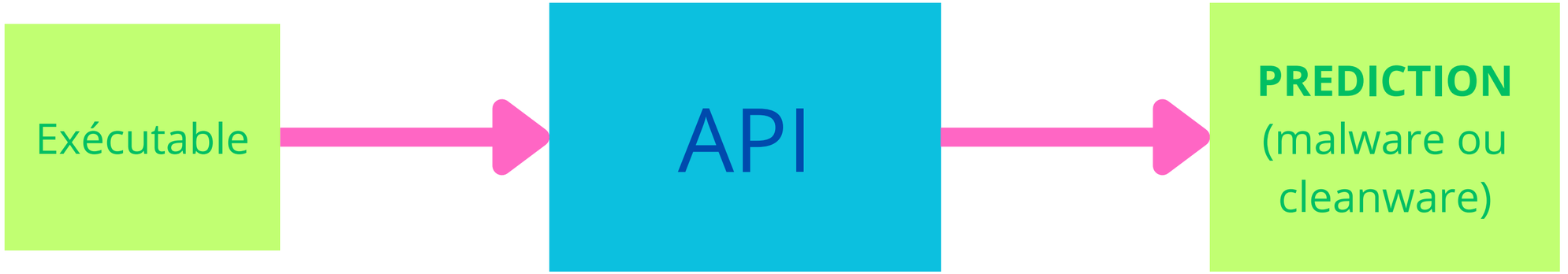


EMBER



- Statique et tabulaire
- *2381 features*
- 9 groupes de features

DÉTECTION

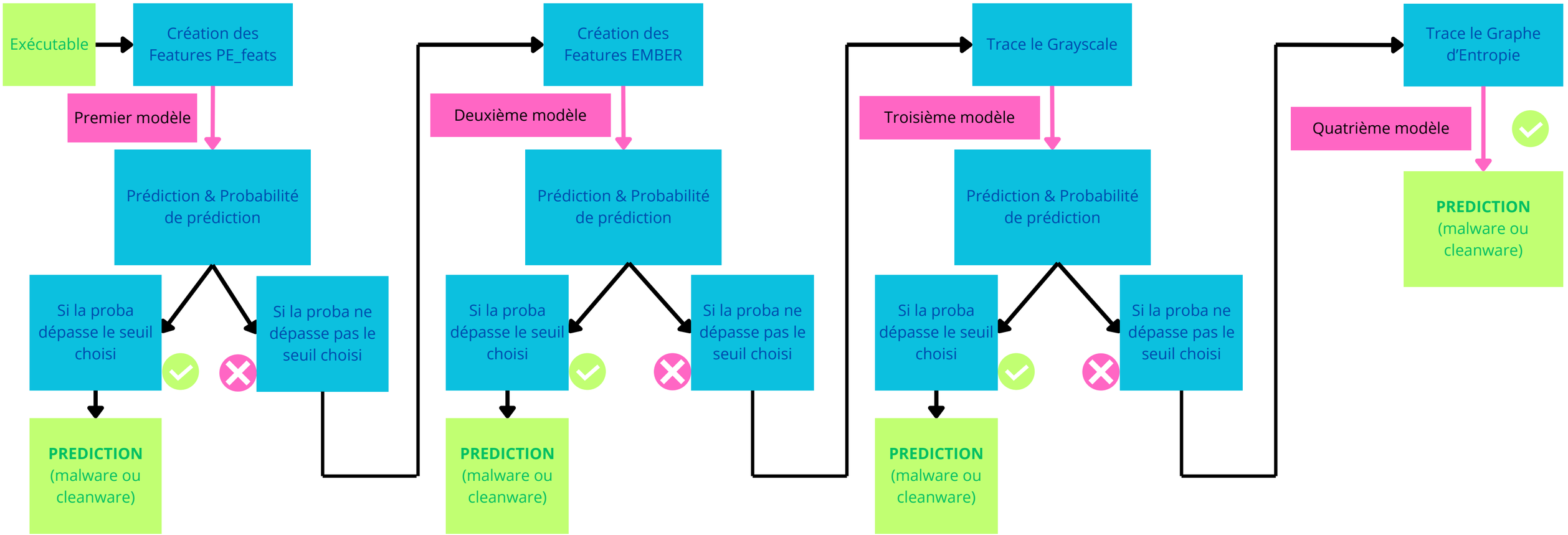


API la plus précise possible

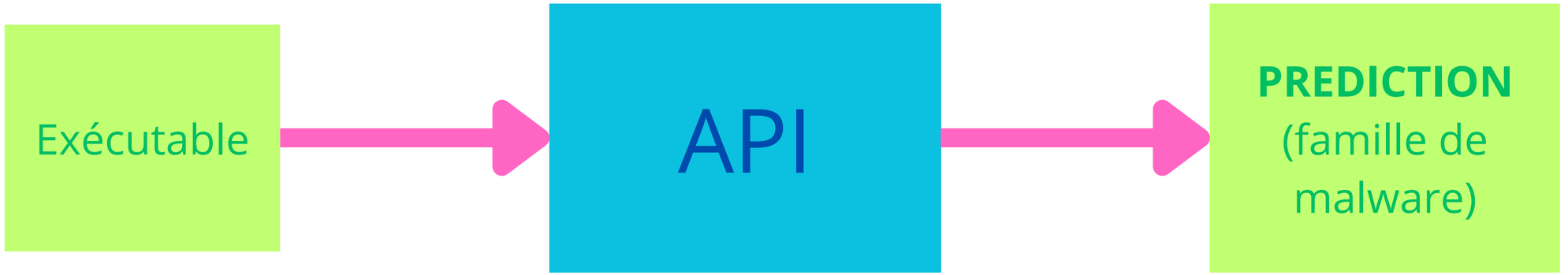
API la moins coûteuse en temps possible

12

API POUR LA DÉTECTION



CLASSIFICATION

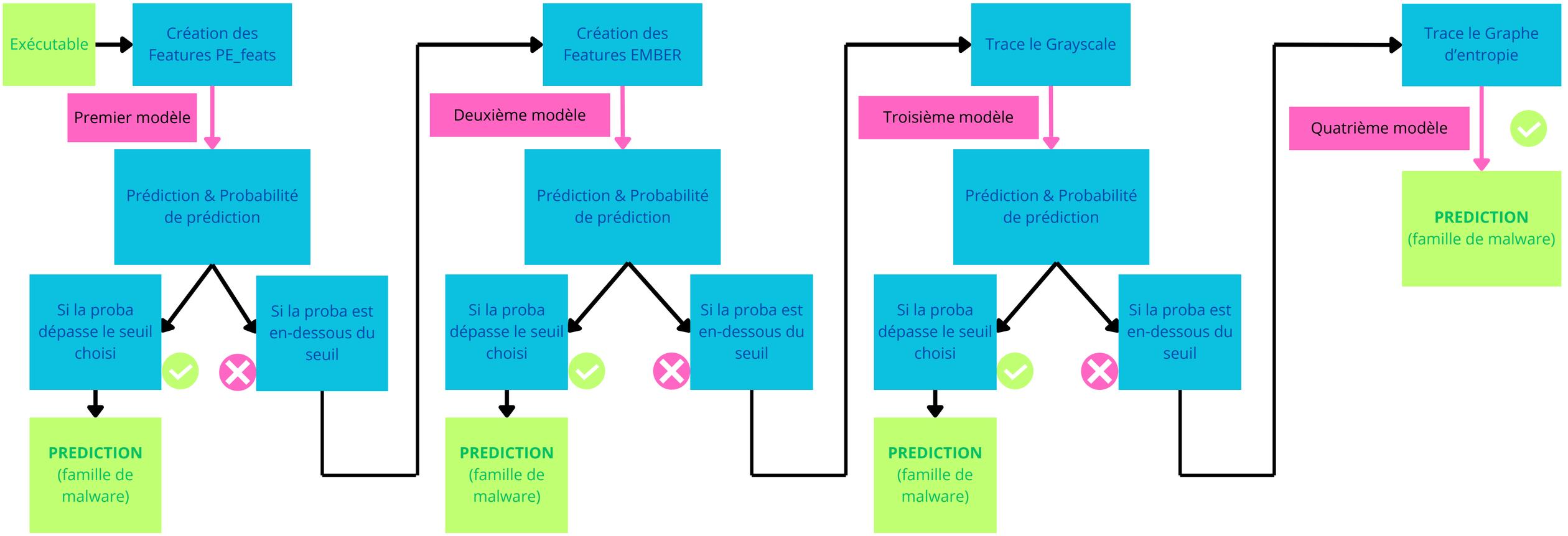


API la plus précise possible

API la moins coûteuse en temps possible

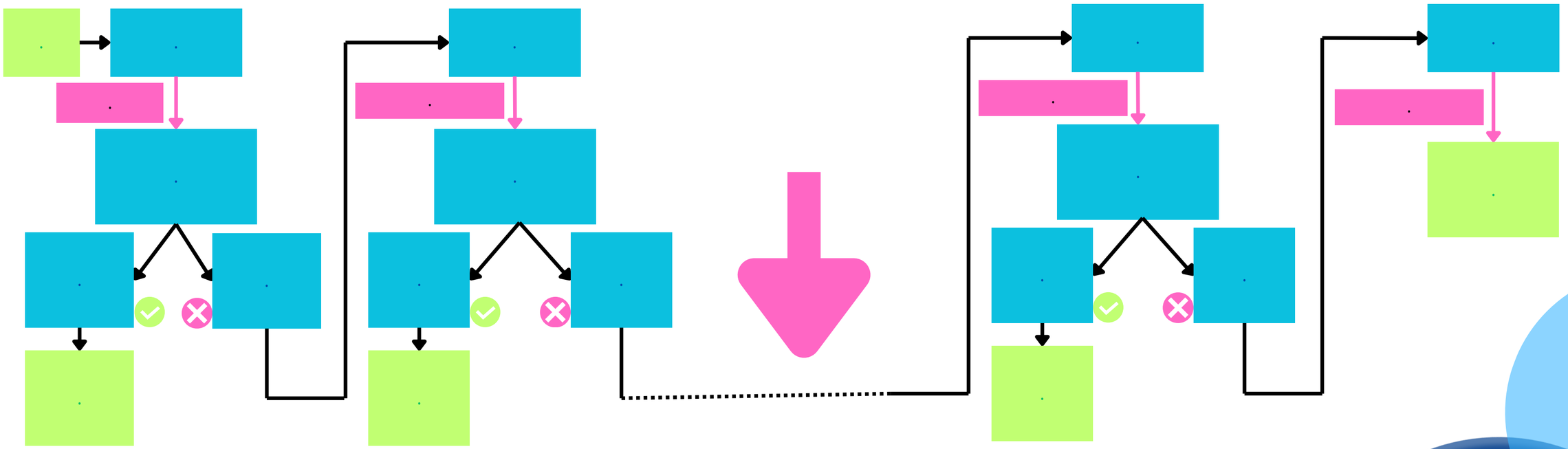
14

API POUR LA CLASSIFICATION

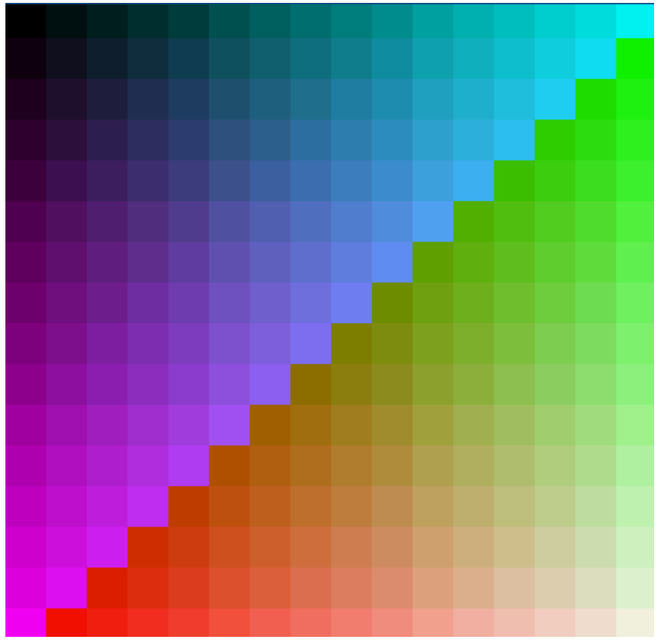


EVOLUTION DE L'API

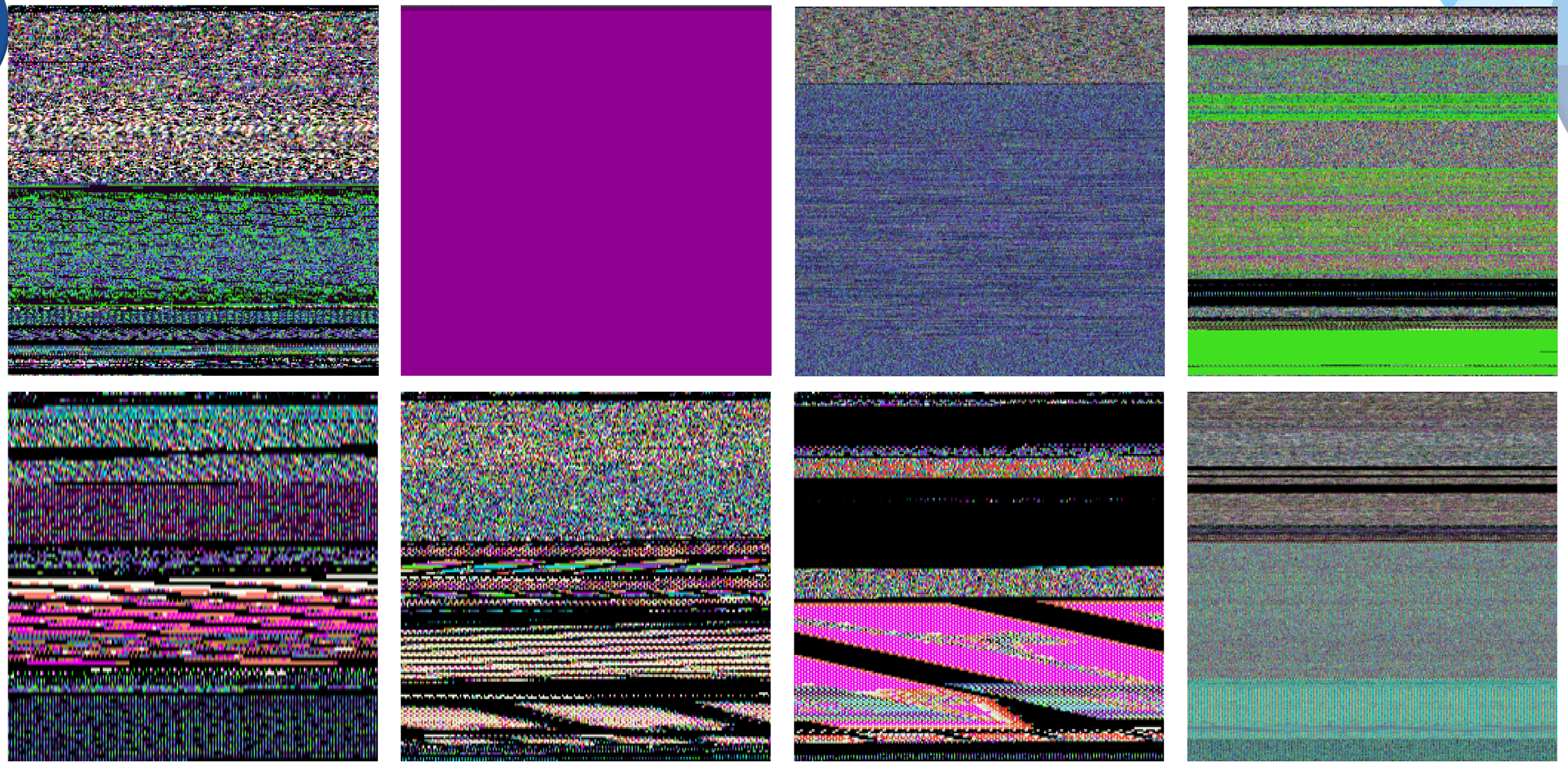
Nouveau Modèle



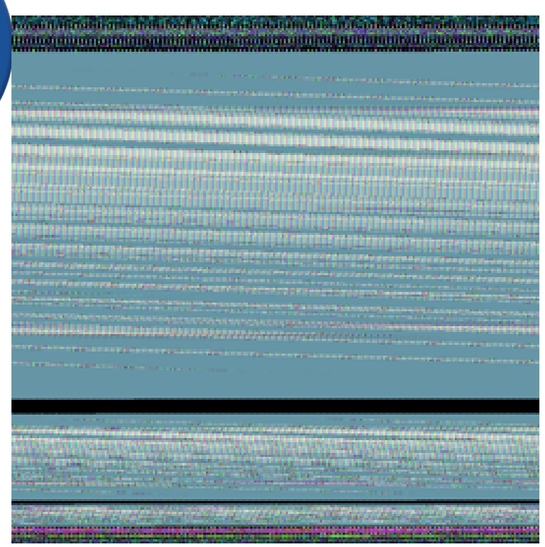
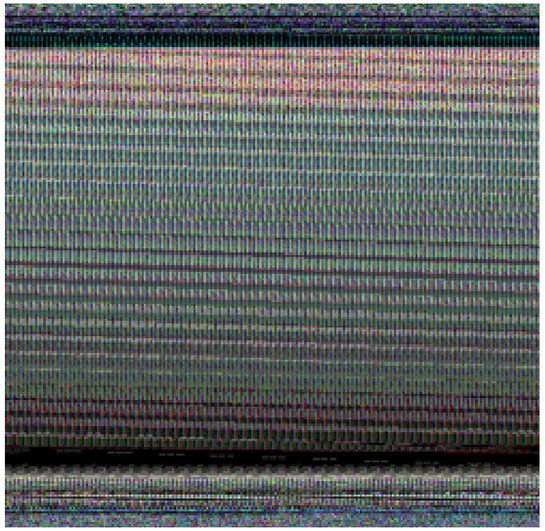
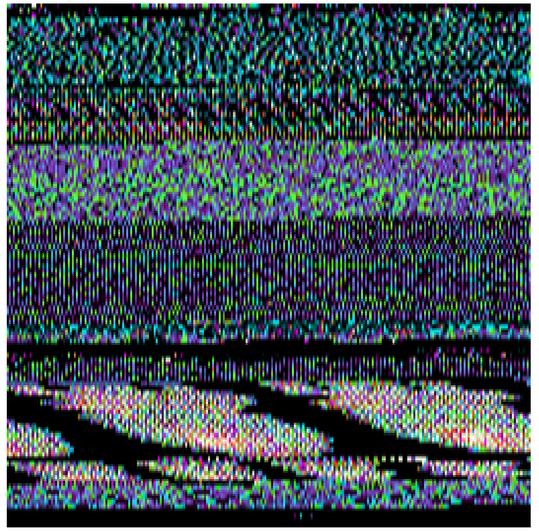
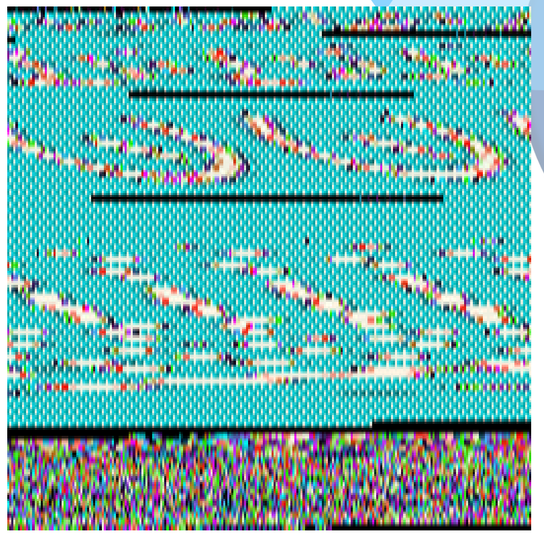
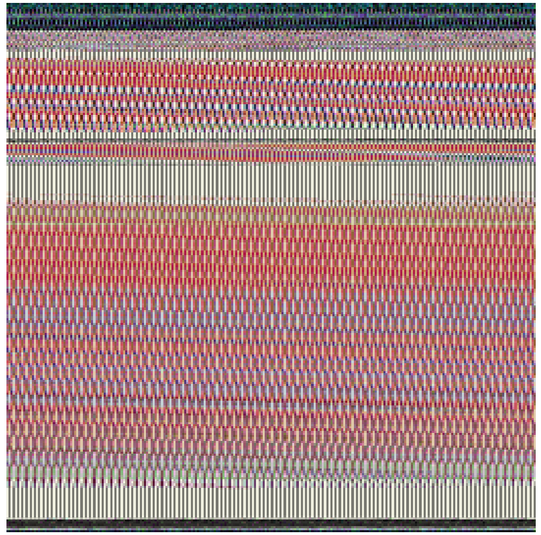
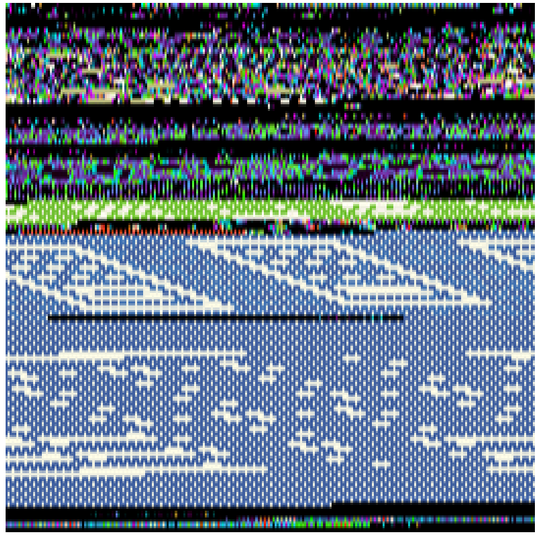
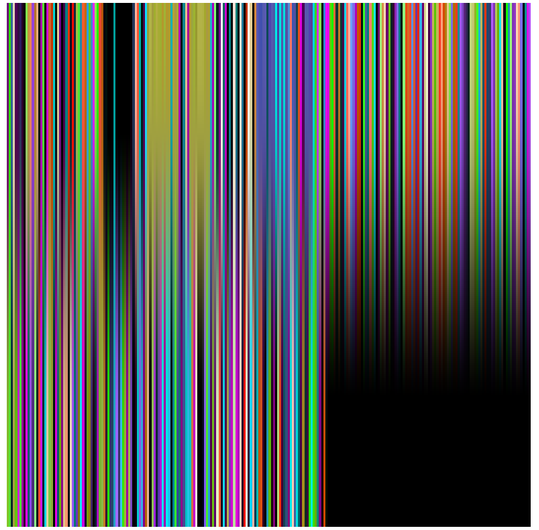
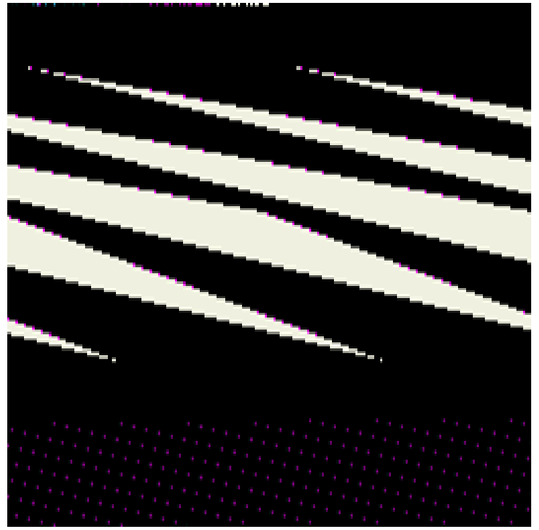
REPRÉSENTATION COLORÉE



- séparer le byte en deux *“nibbles”*
- les utiliser comme coordonnées
- lui donner la couleur de cet endroit sur la colormap



MALWARES

CLEANWARES

RÉSULTATS : DÉTECTION

	Accuracy	Precision	F1 score	Recall
PE_feats	99,2%	99,2%	99,2%	99,2%
Ember	100%	100%	100%	100%
Couleur	95,7%	96,0%	95,7%	95,7%
Grayscale	95,6%	95,7%	95,6%	95,6%
Entropie	93,4%	94,2%	93,5%	93,4%
API	100%	100%	100%	100%

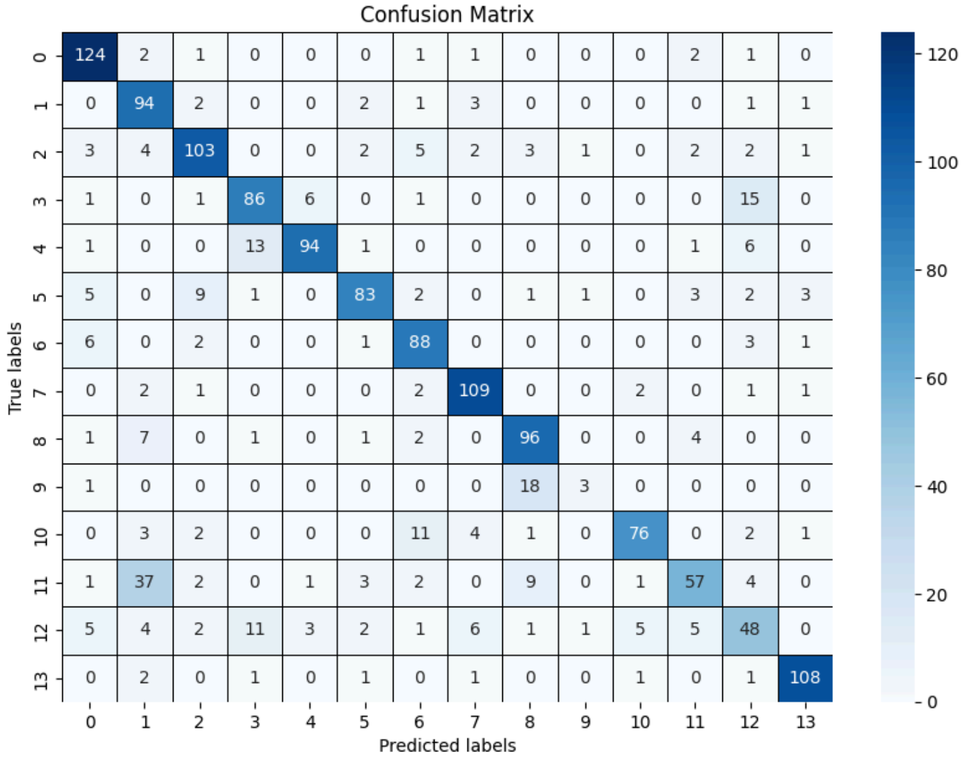
Seuil de confiance : 95 %

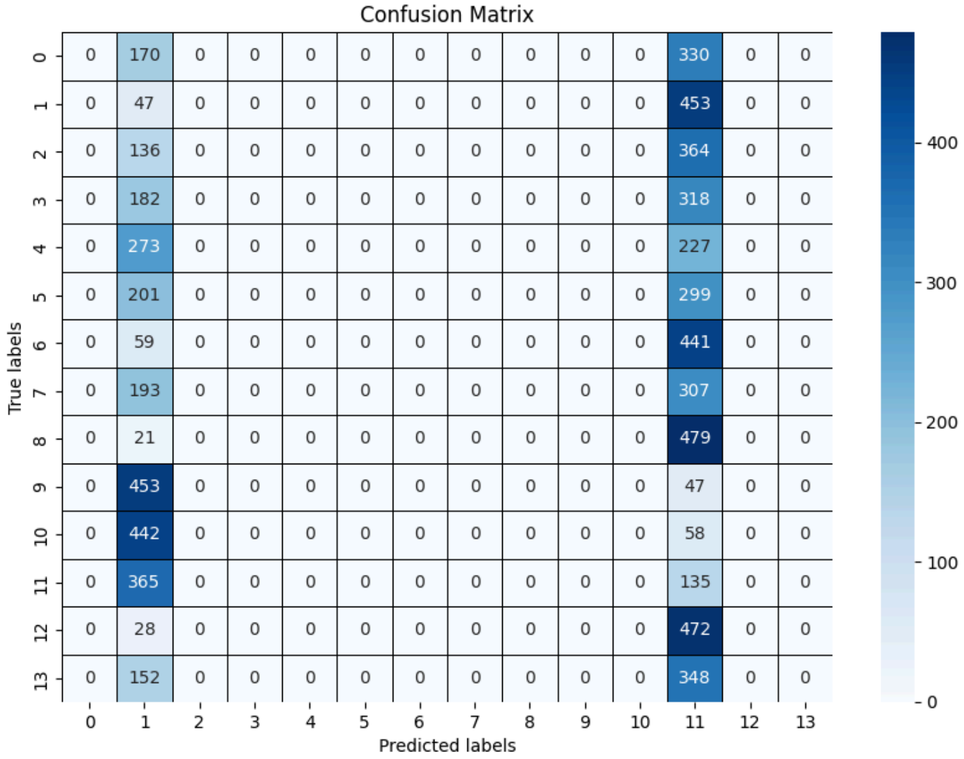
RÉSULTATS : CLASSIFICATION

	Accuracy
PE_feats	85,7%
Ember	97.1%
Couleur	83.2%
Grayscale	79.0%
Entropie	91.0%
API	69.21%

Seuil de confiance : 85%

EXEMPLE DES GRAYSCALES





ALERTE : OVERFITTING !

RÉSULTATS : CLASSIFICATION

	Accuracy	Vraie accuracy
PE_feats	95.2%	85.7%
Ember	97.1%	86.4%
Couleur	83.2%	13.1%
Grayscale	79.0%	2.6%
Entropie	91.0%	11.8%
API	69.21%	69.21%

Seuil de confiance : 85%

RÉSULTATS : CLASSIFICATION ÉVALUATION DE L'API

Seuil de confiance	Accuracy
75 %	84.99%
85 %	69.21%
95 %	77.27%

RÉSULTATS : CLASSIFICATION EMBER ET PE_FEATS

86.8 %

d’accuracy

Seuil de confiance : 85%

CONCLUSION

- Tabulaire vs Images
- Statique et dynamique
- La confiance des modèles