## **Compétences fondamentales**

| **Num ID** | **Compétences** | **Meet/Missing** |
| --- | --- | --- |
| **Compréhension du problème et des données** |  |  |
| 01.01.A01 | A démontré une compréhension approfondie du contexte cybersécurité et des enjeux de la détection de malware |  |
| 01.01.A02 | A maîtrisé les concepts de graphes de flux de contrôle (CFG) et leur interprétation |  |
| 01.01.A03 | A interprété correctement les instructions assembleur x86/x64 |  |
| 01.01.A04 | A identifié les != types de comportements malveillants (injection, C&C, obf...) |  |
| **Prétraitement et ingénierie des caractéristiques** |  |  |
| 02.01.A01 | A implémenté un parsing efficace des fichiers Digraph (extraction des nœuds et arêtes) |  |
| 02.01.A02 | A conçu des caractéristiques pertinentes à partir des graphes CFG |  |
| 02.01.A03 | A extrait des patterns d'instructions significatifs pour la détection |  |
| 02.01.A04 | A implémenté des méthodes de réduction de dimensionnalité appropriées |  |
| 02.01.A05 | A normalisé et équilibré les données pour éviter les biais d'apprentissage |  |
| **Modélisation et apprentissage** |  |  |
| 03.01.A01 | A sélectionné et justifié l'architecture du modèle de classification multi-labels de façon pertinente |  |
| 03.01.A02 | A paramétré correctement les hyperparamètres avec validation croisée |  |
| 03.01.A03 | A évalué rigoureusement les performances avec la métrique Macro F1 |  |
| 03.01.A04 | A analysé les erreurs de classification et proposé des améliorations |  |
| 03.01.A05 | A mis en œuvre des stratégies pour gérer le déséquilibre des classes |  |

## **Compétences spécifiques à l'explicabilité**

| **Num ID** | **Compétences** | **Meet/Missing** |
| --- | --- | --- |
| **Sélection et justification des méthodes d'explicabilité** |  |  |
| 04.01.A01 | A choisi les méthodes d'explicabilité adaptées au modèle implémenté |  |
| 04.01.A02 | A justifié rigoureusement le choix des méthodes d'explicabilité retenues |  |
| 04.01.A03 | A démontré une compréhension approfondie des méthodes choisies |  |
| 04.01.A04 | A identifié les forces et limites des méthodes sélectionnées |  |
| 04.01.A05 | A proposé une stratégie d'explicabilité cohérente avec les objectifs du projet |  |
| **Méthodes d'explicabilité globale** |  |  |
| 05.01.A01 | A implémenté et interprété des méthodes d'importance globale des caractéristiques |  |
| 05.01.A02 | A mis en œuvre des techniques de visualisation des relations entre variables et prédictions |  |
| 05.01.A03 | A créé des représentations des interactions entre caractéristiques |  |
| 05.01.A04 | A analysé la sensibilité du modèle aux variations des caractéristiques d'entrée |  |
| 05.01.A05 | A extrait et communiqué les règles de décision globales du modèle |  |
| **Méthodes d'explicabilité locale** |  |  |
| 06.01.A01 | A implémenté des techniques d'attribution adaptées au modèle choisi |  |
| 06.01.A02 | A visualisé efficacement les caractéristiques influençant les prédictions individuelles |  |
| 06.01.A03 | A généré des explications alternatives ou contrefactuelles |  |
| 06.01.A04 | A adapté les méthodes d'explication au contexte des malwares et CFG |  |
| 06.01.A05 | A produit des explications locales intelligibles pour les analystes |  |
| **Évaluation et communication des explications** |  |  |
| 07.01.A01 | A vérifié la fidélité des explications par rapport au modèle original |  |
| 07.01.A02 | A mesuré la stabilité des explications face à des variations des entrées |  |
| 07.01.A03 | A évalué la pertinence des explications pour des analystes en cybersécurité |  |
| 07.01.A04 | A comparé objectivement différentes approches d'explicabilité |  |
| 07.01.A05 | A traduit les explications techniques en insights exploitables |  |

## **Compétences techniques et implémentation**

| **Num ID** | **Compétences** | **Meet/Missing** |
| --- | --- | --- |
| **Programmation et environnement technique** |  |  |
| 08.01.A01 | A structuré un code modulaire, propre et bien documenté |  |
| 08.01.A02 | A utilisé efficacement les bib d'analyse de graphes (NetworkX, DGL, PyG) |  |
| 08.01.A03 | A maîtrisé les frameworks d'explicabilité (SHAP, LIME, Captum, Alibi) |  |
| 08.01.A04 | A optimisé le pipeline pour gérer le volume de données (20 000 binaires) |  |
| 08.01.A05 | A géré correctement les versions du code (Git) et assuré la reproductibilité |  |
| **Visualisation et communication** |  |  |
| 09.01.A01 | A créé des visualisations pertinentes des CFG et des patterns malveillants |  |
| 09.01.A02 | A conçu des visualisations efficaces des explications (heatmaps, graphes colorés) |  |
| 09.01.A03 | A adapté le niveau de détail des explications selon l'audience |  |
| 09.01.A04 | A présenté clairement la méthodologie et les résultats (rapport et soutenance) |  |
| 09.01.A05 | A répondu de manière pertinente aux questions techniques lors de la soutenance |  |

## **Compétences analytiques et critiques**

| **Num ID** | **Compétences** | **Meet/Missing** |
| --- | --- | --- |
| **Analyse critique et résultats** |  |  |
| 10.01.A01 | A identifié les limites de l'approche mise en œuvre |  |
| 10.01.A02 | A évalué l'impact des choix méthodologiques sur les résultats |  |
| 10.01.A03 | A détecté et prévenu les biais potentiels dans le modèle et les explications |  |
| 10.01.A04 | A proposé des améliorations pertinentes pour de futures itérations |  |
| 10.01.A05 | A contextualisé les résultats dans le domaine de la cybersécurité |  |
| **Application à la cybersécurité** |  |  |
| 11.01.A01 | A traduit les explications techniques en insights opérationnels pour les analystes |  |
| 11.01.A02 | A relié les patterns identifiés à des comportements malveillants connus |  |
| 11.01.A03 | A proposé des contre-mesures basées sur les comportements détectés |  |
| 11.01.A04 | A analysé la robustesse du modèle face à l'évolution des techniques malveillantes |  |
| 11.01.A05 | A démontré la valeur ajoutée de l'explicabilité pour la détection de malware |  |

## 

## **Critères d'excellence**

| **Num ID** | **Compétences** | **Meet/Missing** |
| --- | --- | --- |
| **Innovation et originalité** |  |  |
| 12.01.A01 | A proposé une approche originale pour la représentation des CFG |  |
| 12.01.A02 | A développé des méthodes d'explicabilité adaptées spécifiquement aux malwares |  |
| 12.01.A03 | A combiné de manière innovante plusieurs techniques d'explicabilité |  |
| 12.01.A04 | A créé des visualisations novatrices pour les explications de comportements malveillants |  |
| 12.01.A05 | A exploré des approches alternatives aux méthodes classiques de détection |  |
| **Dépassement des attentes** |  |  |
| 13.01.A01 | A atteint des performances supérieures à l'état de l'art sur des tâches similaires |  |
| 13.01.A02 | A fourni des explications particulièrement détaillées et exploitables |  |
| 13.01.A03 | A mis en œuvre des méthodes avancées d'évaluation de l'explicabilité |  |
| 13.01.A04 | A développé des outils réutilisables pour la communauté |  |
| 13.01.A05 | A proposé une réflexion approfondie sur les aspects éthiques de la détection de malware |  |