Les limites de l'IA appliquée à la cyber-sécurité

dans un contexte d'évaluation

Frédéric GUIHERY, Responsable R&D, AMOSSYS

AMOSSYS
EXPERT IN CYBERSECURITY

EUROPEAN CYBER WEEK
THE EUROPEAN CYBER DEFENCE AND CYBERSECURITY FORUM

#EuroCyberWeek

PÔLE D'EXCELLENCE CYBER

BRETAGNE DÉVELOPPEMENT INNOVATION

Région Bretagne

Ministère de la Défense

Contexte

Le CESTI Amossys

- Laboratoire d'évaluation agréé par l'ANSSI
- Evaluations de produits de sécurité (Critères Communs / CSPN)

Constats

- **Jusqu'à présent** : évaluation de produits de sécurité « traditionnels » (pare-feu, IDS, chiffreurs, etc.) basés sur des techniques **déterministes**
- **Désormais** : intégration d'algorithmes d'apprentissage et de prise de décision dans certains produits de sécurité

Objectifs

- Adapter les méthodes d'évaluations sur les nouvelles classes de produits de sécurité
- Tirer vers le haut le niveau d'efficacité de ces produits de sécurité

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les usages de l'IA en cybersécurité

Cas d'applications

- Détection d'intrusions
- Filtrage des spams
- Analyse de malware
- Détection d'exfiltration de données
- Authentification biométrique
- Voiture autonome
- …

Méthodes utilisées

- Classification
- Clustering
- Détection d'anomalies
- Régression linéaire et prédictions
- …

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

AMOSSYS
EXPERT IN CYBERSECURITY

Les limites de l'IA en cybersécurité

Les limites de l'IA en cybersécurité

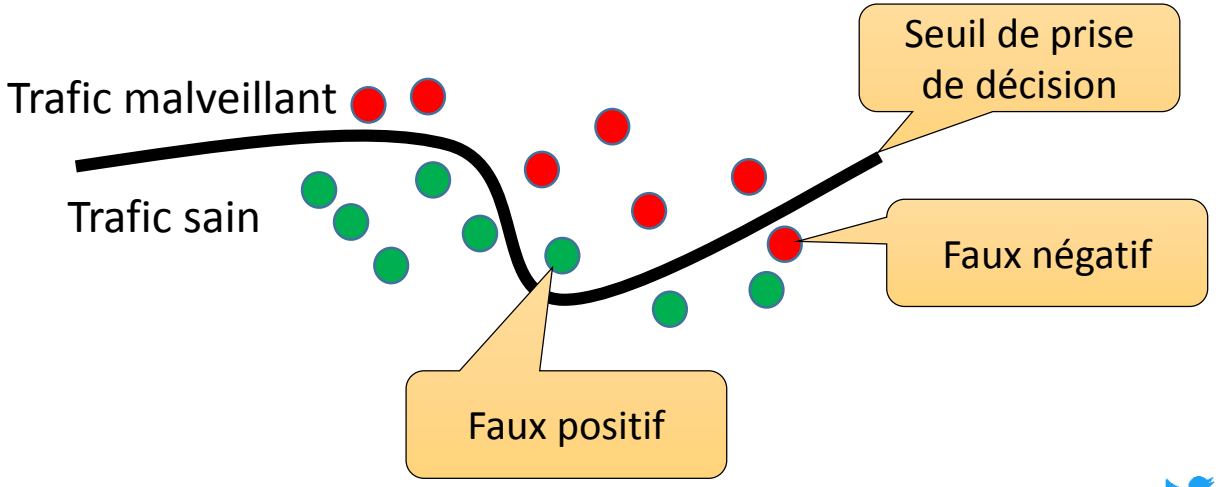
La complexité du paramétrage

- Beaucoup d'algorithmes reposent sur des paramètres
  - Paramètres directs (seuils de décision)
  - Paramètres indirects (nombre de points pour créer un cluster, …)
  - Hyper-paramètres (structure du réseau de neurone, …)
- Importance d'avoir des paramètres précis pour éviter faux négatifs et faux positifs
- Nécessité d'adapter les paramètres au contexte opérationnel
- Nécessité de faire évoluer les paramètres en fonction des modifications du SI

Les limites de l'IA en cybersécurité

La complexité du paramétrage

- Beaucoup d'algorithmes reposent sur des paramètres
  - Paramètres directs (seuils de décision)
  - Paramètres indirects (nombre de points pour créer un cluster, …)
  - Hyper-paramètres (structure du réseau de neurone, …)
- Importance d'avoir des paramètres précis pour éviter faux négatifs et faux positifs
- Nécessité d'adapter les paramètres au contexte opérationnel
- Nécessité de faire évoluer les paramètres en fonction des modifications du SI



AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

La complexité du paramétrage

- Beaucoup d'algorithmes reposent sur des paramètres
  - Paramètres directs (seuils de décision)
  - Paramètres indirects (nombre de points pour créer un cluster, …)
  - Hyper-paramètres (structure du réseau de neurone, …)
- Importance d'avoir des paramètres précis pour éviter faux négatifs et faux positifs
- Nécessité d'adapter les paramètres au contexte opérationnel
- Nécessité de faire évoluer les paramètres en fonction des modifications du SI

- Le point de vue de l'évaluateur
  - ➢ Analyser la capacité d'adaptation à l'environnement
  - ➢ Analyser la capacité d'assistance au paramétrage

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau d'efficacité face à des attaques complexes

- Les datasets publics contiennent essentiellement des patterns d'attaques basiques
  - Scan de ports
  - DoS
  - Exploitations unitaires de vulnérabilités
  - …
- Les datasets publics sont généralement trop ciblés
  - PCAP
  - netflow
  - Syslog
  - …

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau d'efficacité face à des attaques complexes

- Les datasets publics contiennent essentiellement des patterns d'attaques basiques
  - Scan de ports
  - DoS
  - Exploitations unitaires de vulnérabilités
  - …
- Les datasets publics sont généralement trop ciblés
  - PCAP
  - netflow
  - Syslog
  - …

- Le point de vue de l'évaluateur
  - ➢ Confronter les produits face à des scénarios d'attaques évolués en termes de TTP
  - ➢ Besoin de simuler un trafic de vie pertinent
  - ➢ Besoin d'avoir des datasets « riches », c'est-à-dire incluant des traces réseau et système cohérentes entre elles

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau d'efficacité face à des techniques d'attaques inconnues

- Obsolescence des datasets utilisés dans le domaine académique
- Limite inhérente à l'apprentissage [SOMMER/PAXSON, 2010]
  - Les systèmes basés sur l'apprentissage supervisé doivent travailler sur des données labellisées de chaque classe (trafic sain ET trafic malveillant)
  - Ces systèmes ne peuvent donc pas s'entrainer sur des attaques « inconnues » et s'avèrent donc peu robustes en phase de test
  - Les systèmes non supervisés semblent plus adaptés à la détection de variations d'attaques connues

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau d'efficacité face à des techniques d'attaques inconnues

- Obsolescence des datasets utilisés dans le domaine académique
- Limite inhérente à l'apprentissage [SOMMER/PAXSON, 2010]
  - Les systèmes basés sur l'apprentissage supervisé doivent travailler sur des données labellisées de chaque classe (trafic sain ET trafic malveillant)
  - Ces systèmes ne peuvent donc pas s'entrainer sur des attaques « inconnues » et s'avèrent donc peu robustes en phase de test
  - Les systèmes non supervisés semblent plus adaptés à la détection de variations d'attaques connues

- Le point de vue de l'évaluateur
  - ➢ Confronter les produits face à des techniques d'attaques modernes
  - ➢ Et face à des variations d'attaques connues

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

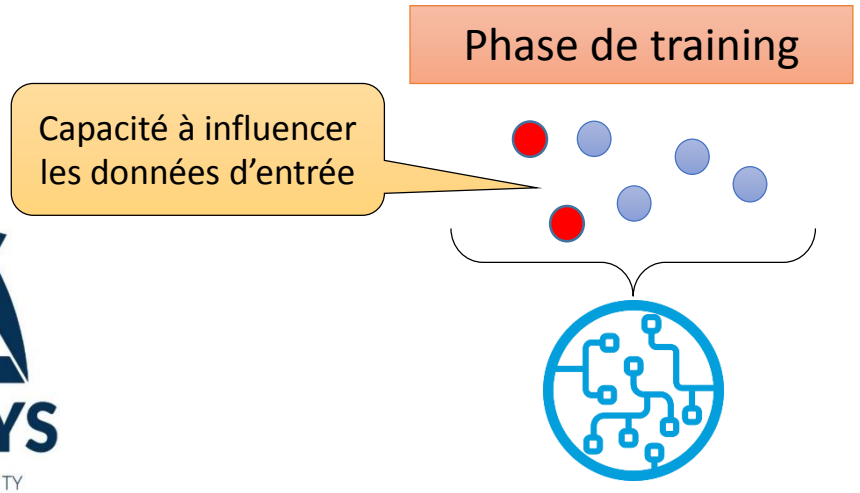
Le niveau de robustesse des algorithmes

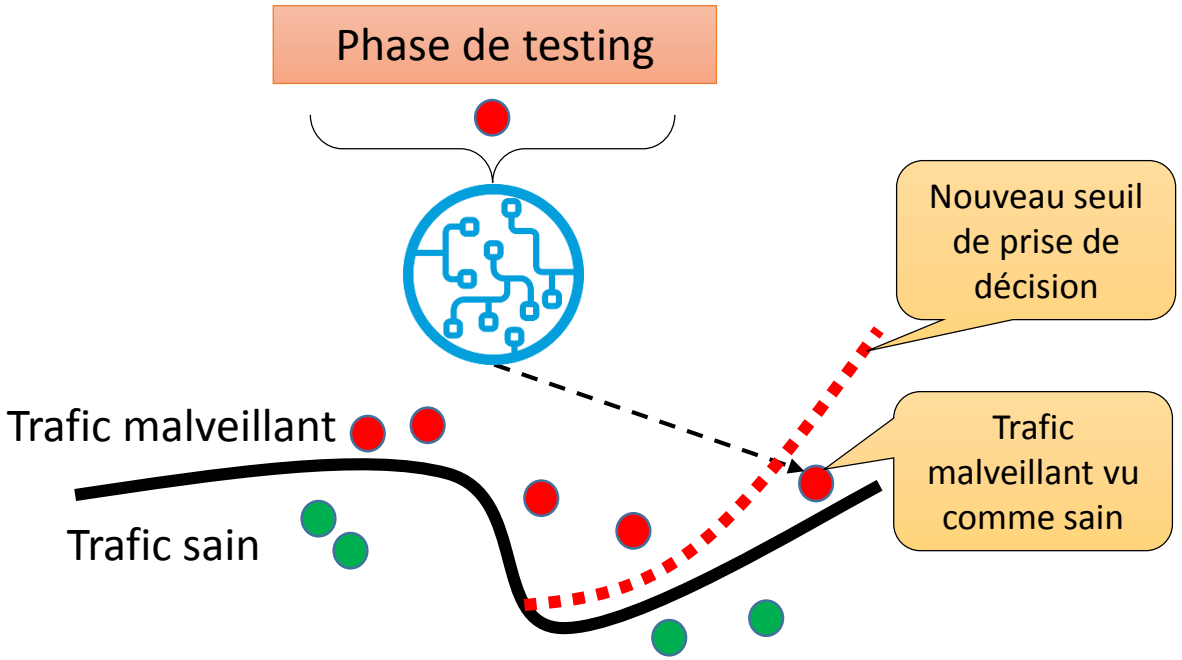
- Empoisonnement des données d'entrainement

Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement





AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test

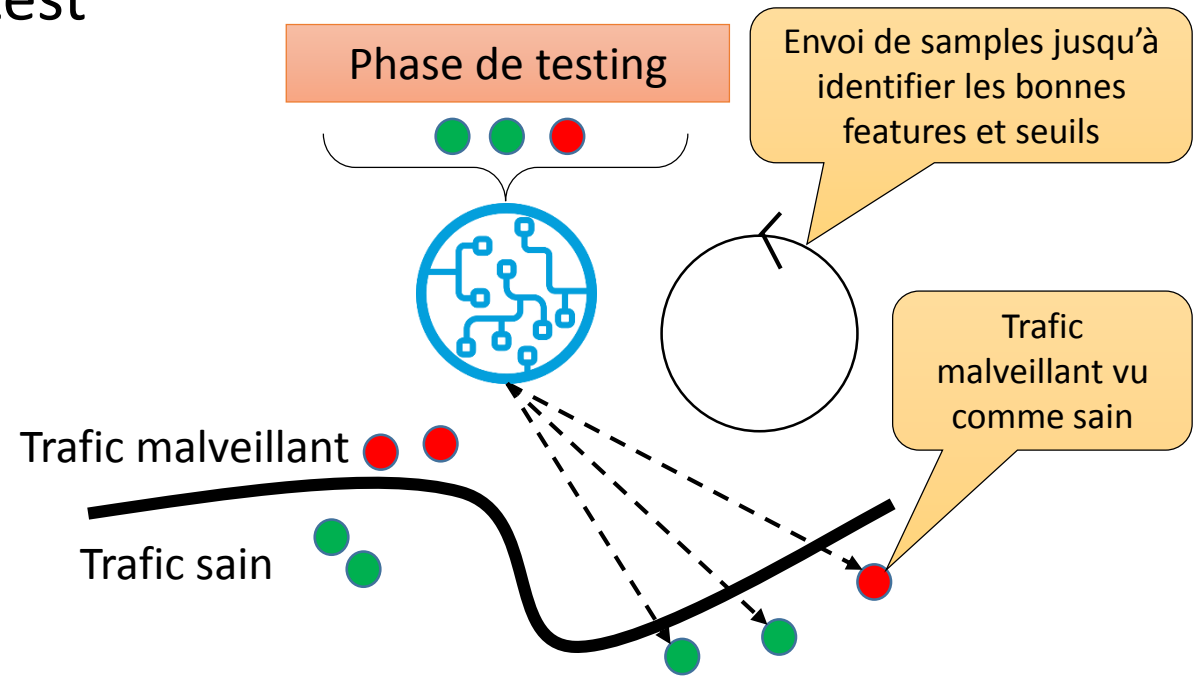
AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test



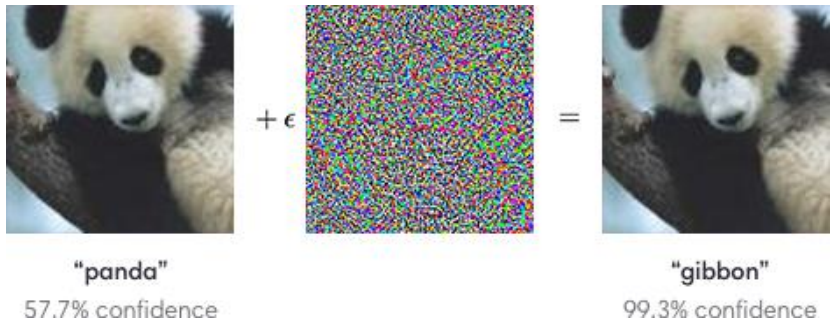
AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

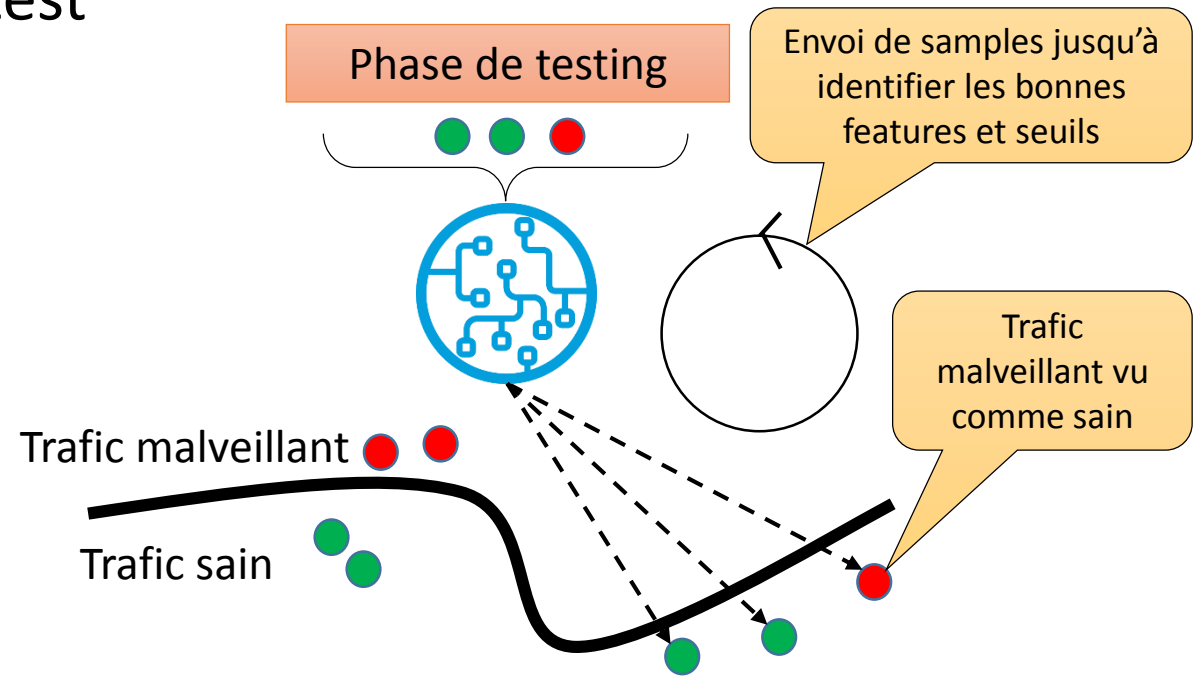
Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test



Source : 2014arXiv1412.6572G



AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test
- Inversion du modèle (i.e. extraction de données d'entrée)

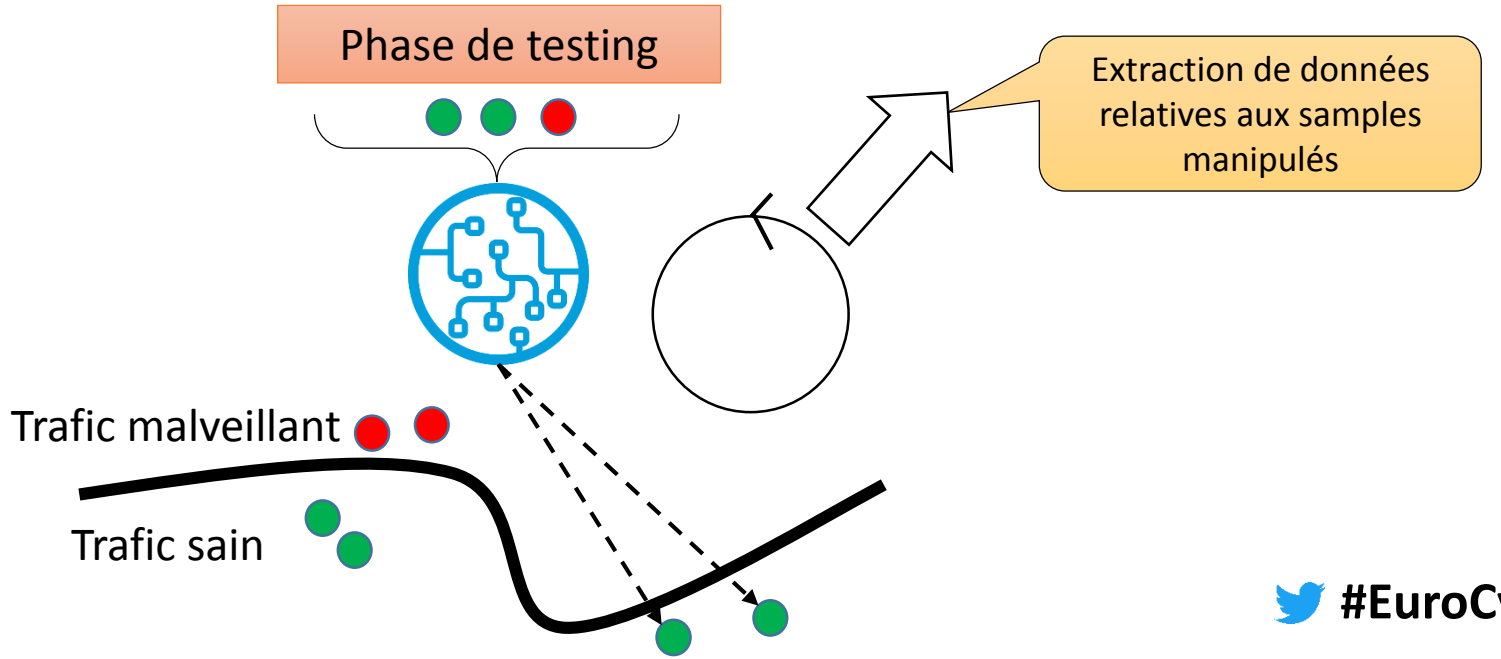
AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test
- Inversion du modèle (i.e. extraction de données d'entrée)



AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test
- Inversion du modèle (i.e. extraction de données d'entrée)
- Extraction du modèle et de ses paramètres/seuils

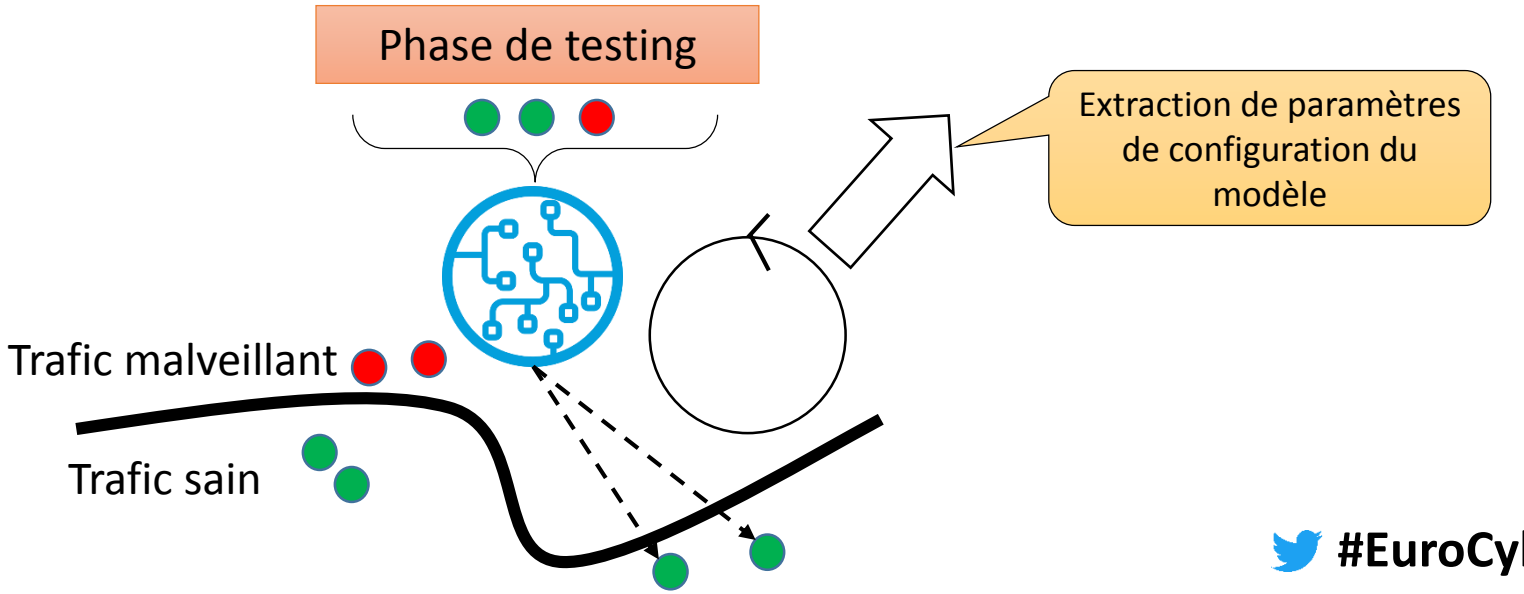
AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test
- Inversion du modèle (i.e. extraction de données d'entrée)
- Extraction du modèle et de ses paramètres/seuils



Les limites de l'IA en cybersécurité

Le niveau de robustesse des algorithmes

- Empoisonnement des données d'entrainement
- Evasion du moteur de test
- Inversion du modèle (i.e. extraction de données d'entrée)
- Extraction du modèle et de ses paramètres/seuils

- Le point de vue de l'évaluateur
  - ➢ Identifier le modèle de menace (exposé à l'empoisonnement, intérêt à évader le mécanisme, confidentialité des inputs, …)
  - ➢ Identifier le niveau de prise en compte de l'adversaire
    - Utilisation d'algorithmes préservant la confidentialité du modèle
    - Capacité à épurer les données d'entrée
    - Combinaison de multiples classifieurs
    - …

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

AMOSSYS
EXPERT IN CYBERSECURITY

Conclusion

Synthèse des limitations

Limites opérationnelles

- Complexité du paramétrage
- Prise en compte du modèle de menace
- …

Limites d'efficacité des algorithmes

- Face aux attaques complexes
- Face aux attaques nouvelles
- …

Limites de robustesse des algorithmes

- Résistance à l'empoisonnement
- Résistance à l'évasion
- …

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

L'évaluation de l'IA chez Amossys

- Démarche d'évaluation reposant sur :
  - L'analyse du modèle de menace du produit
  - L'analyse de l'adaptabilité du produit à l'environnement
  - L'analyse de l'efficacité du produit dans un environnement réaliste
    - Utilisation d'une plateforme Cyber Range générant du trafic d'attaque et du trafic de vie
    - Confrontation face à un catalogue d'attaques
    - Construction de scénarios réalistes et variés
  - L'analyse de la robustesse des algorithmes retenus

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION

Notre présence sur le web

- Site www.amossys.fr
- Twitter twitter.com/Amossys
- Blog blog.amossys.fr
- Github github.com/amossys
- Publications www.amossys.fr/publications.php
- Linkedin linkedin.com/company/amossys

AMOSSYS
EXPERT IN CYBERSECURITY

BRETAGNE DÉVELOPPEMENT INNOVATION