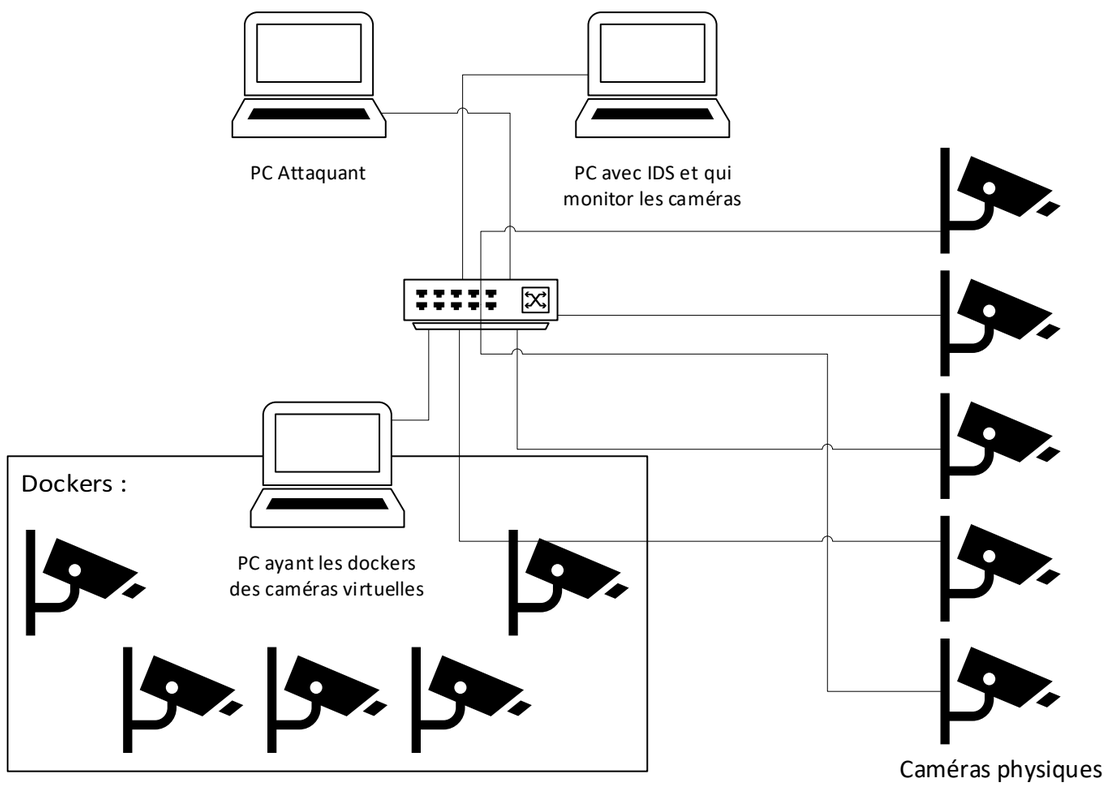
IDS dans le domaine de la sûreté

Auteurs : Jean Vincent - Alexis Camus - Charly Cassese

CONTEXTE ET OBJECTIF

- Aphelio est une startup spécialisée en cybersécurité (outil de sécurité CyberSmartLearn pour ses clients industriels).
- Réaliser un Proof of Concept d'un système de détection d'intrusions dans un réseau de caméras IP en utilisant du Machine Learning.

MÉTHODES ET DÉVELOPPEMENTS



Préparation des données

- Réalisation de cyber-attaques pour obtenir des jeux de données pour entrainer les IA.
- Analyse des données pour en extraire des statistiques pertinentes.
- Développement de différents modèles d'IA pour la détection de comportement anormal et pour la classification des différentes attaques.
- Développement avec le langage Python.
- Utilisation de logiciels pour analyser et extraire le flux réseau.(Wireshark, tshark)

Architecture de l'IDS

Fonctionnement en deux modules :

- Le premier module permet, de différencier du comportement normal d'un comportement anormal grâce à un entrainement.
- Le second modèle permet la classification des différentes attaques lorsque le premier modèle lui a signalé une anomalie dans le flux réseau.

RÉSULTATS ET CONCLUSION

L'IDS est capable de détecter et classifier les attaques suivantes :

- ICMP tunneling : permet l'extraction de données.
- Man in the Middle ARP : interception de trafic réseau.
- TCP flood, ICMP flood : attaque de type Déni de services.
- Scan réseau : découverte de réseaux.

Si une attaque non implémentée à lieu, celle-ci est classée dans la catégorie autre.
L'IDS est capable de détecter un comportement normal.

MOTS-CLÉS : cyber-attaques – machine learning – caméras IP – système de détection d'intrusion