# IA en cyber-sécurité

Chauvin Stéphane, stephane.Chauvin@mydataball.com, R2C system, Niort

Résumé : *dans le cadre des projets que nous réalisons quant à la mise en place de solution de data analytics et d'IA industrielles, nous présentons une mise en place de la solution MyDataBall pour le sujet de la cybersécurité. Lauréat de la solution, notre intervention se concentre sur le calcul dans les graphes d'IP et AS d'indicateurs comportementaux des flux de données et le calcul de la vulnérabilité d'une entreprise.*

Mots clés : *data modélisation by graph, knowledge discovery in graph, machine learning, datamining industriel et IA*

## 1. Introduction

Le sujet de la cyber-sécurité est prégnant à l'aune des attaques que la France a subi en 2020. Les sujets actuels d'attaques des entreprises ne sont qu'une première étape. Les projets de smartbuilding et de smartcity sont aussi au cœur du besoin de mesurer et d'anticiper des mouvements à fort risques. Notre principe est de collecter les éléments entrants et sortants d'une entité (entreprises, collectivités, associations, organismes, …) et de mesurer les relations profondes de connexion. Notre référentiel d'information mondial des IP et AS, nous sommes en mesure de calculer des indicateurs sur les graphes des relations si des perturbations annoncent des anomalies de trafics et des comportements à risques.

## 2. Méthodologie

Au quotidien sont rafraîchis les données des relations IP et AS par TRACEROUTE. Au quotidien, pour chaque IP (quelques millions) et les AS (quelques dizaines de milliers), on reconstitue les graphes de relation. Une batterie de 17 indicateurs mesure les perturbations et les sauts topologiques des graphes. Ils présupposent des mouvements de hacking et de captation de flux dans un but d'agression et de malveillance.

Notre propos est de revenir sur le calcul des indicateurs sur ces graphes qui sont gourmands en temps de calcul. Nous montrons que, en mettant les graphes sous forme d'une collection d'arbres, la fourniture des indicateurs devient raisonnable. L'ensemble de ces mesures consolide une note de vulnérabilité et d'exposition au risque. En outre, ce résultat contribue à accélérer les points d'amélioration pour être ISO 27001 et ISO 27005 pour toute entreprise et entité qui souhaite un plan d'action pour sa sécurité numérique.

Nous donnerons des exemples qui montrent les fluctuations et les prémisses de ces fluctuations.

## 3. Originalité / perspective

Notre collection de mesure au quotidien nous permet d'engager la mise en place de machine learning pour en déduire des prédictions à J+1 d'alertes selon le degré de

vraisemblance, de véracité et de prise de décision pour une action préventive.