Algorithmes d'Intelligence Artificielle en Cybersécurité & Intégration en environnements contraints

Stéphane Morucci[1], Stéphane Davy[2], Nicolas Raux[2], Jérémy Scion[3], Guillaume Lerouge[4], Nathan Rydin[1], Marc Le Nué[1], Dorian Screm[1]

[1] Orange Labs, 4 rue du Clos Courtel, 35510 Cesson Sévigné
[2] Orange Cyber Défense, 9 rue du Chêne Germain, 35510 Cesson Sévigné
[3] Orange Cyber Défense, 54 Place de l'Ellipse, 92000 Nanterre
[4] SoftAtHome, 9 rue du Débarcadère, 92700 Colombes

Résumé

L'Intelligence Artificielle (IA) dans le domaine de la cyber sécurité offre un formidable champ d'exploration et promet pour la première fois la possibilité de détection d'attaques jusqu'alors inconnues. Les promesses de l'IA pour la cyber couvrent également une limitation des ressources opérationnelles nécessaires grâce à un filtrage amont du trafic (moins de flux au niveau des équipements de surveillance, recherches de compromission plus efficace) et des gains de temps pour les exploitants (diminution des faux-positifs, meilleure pertinence des alertes). Par ailleurs, le recours à des solutions non-supervisées permet aussi d'envisager une mise en exploitation très rapide comparée aujourd'hui à plusieurs semaines pour la mise en place d'un SIEM (System Information and Event Management, la pierre angulaire d'une solution de supervision de la sécurité).
Cet article propose de comparer les performances de plusieurs algorithmes de détection d'anomalie sur 2 jeux de données (« datasets »). Travailler sur des datasets de production nécessite en plus la mise en place de techniques de protection de données dont certaines seront exposées avec leurs impacts associés. L'intégration d'algorithmes d'IA dans un environnement de production impose certaines contraintes à différents niveaux. Nous présentons dans cet article 3 types d'intégration : l'intégration dans 2 SIEMs, l'intégration dans une solution Open-Source prometteuse (Apache Metron) et notre vision d'une intégration dans un écosystème d'opérateur Télécom, en particulier au niveau des box ADSL/fibre Grand-Public.

Mots clefs
Cybersecurité, Détection d'anomalie, SIEM, Intégration.