Reinforced Autonomous Agents with Attack-Defense Exercises in Realistic Environments

Frédéric Guihery[1], Georges Bossert[2], Damien Crémilleux[1], Olivier Tétard[2], Gildas Jeantet[2]

[1] *AMOSSYS, prenom.nom@amossys.fr*
[2] *SEKOIA, prenom.nom@sekoia.fr*

Mots clés / Keywords

Apprentissage par renforcement, APT simulation, infrastructure d'attaque, TTP, XDR, remédiation, course of action

Résumé

La tendance actuelle est à l'automatisation des opérations d'un centre opérationnel de la sécurité (SOC, Security Operations Center), en particulier sur le volet remédiation. Cependant, la mise en œuvre de playbooks de remédiation doit être qualifiée en termes d'impact sur le service protégé, afin d'éviter des pertes de disponibilité. Nous proposons une démarche visant à automatiser l'exécution de modes opératoires d'attaquants vis-à-vis d'un système d'information, afin d'apprendre les meilleures contre-mesures à appliquer. Cette démarche s'appuie sur un environnement d'exercice automatisant l'attaque et la défense, dans une optique d'apprentissage. Nous présentons ici les contributions suivantes :

- une plateforme de simulation afin de tester et entraîner un agent autonome, dans un environnement maîtrisé, face à des scénarios d'attaque représentatifs de modes opératoires de groupes d'attaquants ;
- un agent autonome capable de réagir rapidement et compléter voire suppléer les opérateurs humains via une réponse adaptée à une posture de sécurité définie tout en permettant d'interagir avec eux pour une remédiation complète.

L'automatisation de l'attaque repose sur la simulation de modes opératoires de groupes d'attaquants et d'infrastructures d'attaque. En défense, il est effectué un apprentissage automatisé des séquences d'actions de remédiations les plus adaptées à la protection d'un système d'information (SI). Cette plateforme a pour ambition de devenir un cadre de gamification de l'attaque-défense permettant d'évaluer l'efficacité d'architectures de lutte informatique défensive.

Résultats

La présentation détaillera les résultats obtenus par la plateforme DALID qui permet d'observer le comportement d'agents autonomes d'attaques et de défenses au cours d'exercices répétés afin de constituer automatiquement les meilleures stratégies de remédiations pour des équipes SOC. L'ensemble des résultats est détaillé dans l'article et la présentation donnée lors de la conférence C&ESAR 2021 : https://ceur-ws.org/Vol-3056/paper-12.pdf

Notes

Ces travaux ont été réalisés au sein du projet DALID (Démonstrateur Automatisé de Lutte Informatique Défensive), dans le cadre du dispositif RAPID de DGA-MI et de l'Agence de l'Innovation de Défense. Il s'agit d'un projet de 2 ans (2020/2022), réalisé en collaboration entre les

entreprises SEKOIA et AMOSSYS. DALID a été présenté comme "Démarrage de projet" lors de RESSI 2020.