Comment améliorer la résilience aux cyberattaques des systèmes hyperconnectés du futur : retour d'expérience

Pilotage technique : **Nada Essaouini**, Ingénieur de recherche - analyste des technologies de cybersécurité, IRT SystemX.

Grâce à l'initiative START@SystemX Cybersécurité, la start-up craft ai, lauréate de la saison 1, a pu expérimenter les performances de sa solution d'intelligence artificielle dans le contexte de la détection d'intrusions (piratage informatique) par une approche d'analyse comportementale. L'évaluation des modèles prédictifs générés par craft ai s'est établie sur une méthodologie d'évaluation et de comparaison des systèmes de détection d'intrusions (IDSs) développée au sein du projet EIC (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité) de l'IRT SystemX. Elle s'est faite en collaboration avec Airbus CyberSecurity et Thales Services.

Dans les activités d'évaluation ou d'analyse comparative des IDSs, trois axes sont explorés : les méthodes de génération des données de tests, les métriques et les méthodologies de mesures. Une méthodologie de mesure consiste donc à spécifier les propriétés de l'IDS et à déterminer les données de tests et les métriques utilisées pour l'évaluation de ces propriétés.

Dans notre expérience, deux propriétés ont été plus particulièrement analysées : la précision de la détection d'attaque et l'*actionnabilité*. La précision de la détection des attaques consiste à évaluer conjointement le taux des faux positifs (évènement/comportement évalué hostile à tort) et le taux des vrais positifs (évènement/comportement évalué hostile à raison). L'actionnabilité mesure la pertinence des informations rapportées dans les alertes des IDSs et leurs impacts sur les stratégies d'atténuation à adopter. En particulier l'évaluation de l'actionnabilité présente un grand challenge pour les IDSs à base d'apprentissage automatique contrairement aux IDSs à base de signature. En effet, une alerte émise par un IDS à base de signature contient un identifiant de la signature qui l'a déclenchée. Ainsi, évaluer l'actionnabilité d'un IDS à base de signature revient à savoir si la signature qui déclenche l'alerte renvoie une information pertinente sur l'attaque jouée dans les données de test. Plus l'information est exacte, plus la stratégie d'atténuation à adopter devient claire et efficace. La difficulté d'évaluer les IDSs à base d'apprentissage automatique provient du fait que leurs résultats sont souvent présentés sous forme de scores décrivant les degrés d'anomalies et non sous forme d'information claire sur la nature de l'attaque.

Dans notre projet, l'évaluation de l'actionnabilité s'appuie sur des mécanismes de corrélation et des données de tests décrivant un scénario complet d'attaque. Si la corrélation, alimentée par les sorties de l'IA, retrouve le scénario d'attaque du test, alors l'IDS est considéré complètement actionnable.

Pour l'expérimentation, nous avons utilisé des données de tests fournies par Airbus CyberSecurity. Ces données présentent un scénario complet d'attaques étalées dans le temps et proche de techniques d'attaques réelles. Un individu y effectue un criblage et un ciblage avec l'aide des réseaux sociaux puis usurpe l'identité d'un individu référent. Il adresse alors à plusieurs employés un courriel comprenant une pièce jointe malveillante (première incongruité). Cette dernière est activée par un employé imprudent. Elle effectue alors un balayage de ports (seconde incongruité) vers des équipements réseau (reconnaissance du système visé). L'un d'eux présente une vulnérabilité qui peut alors être exploitée (troisième incongruité) par l'attaquant afin de compromettre et/ou dérober des informations sensibles de l'entreprise présente sur son système d'information.

Concernant le mécanisme de corrélation, Airbus CyberSecurity a fourni un procédé novateur de corrélation qui, alimenté par les sorties de l'IA, a produit en sortie des graphes dont la pertinence a été quantifiée.

Finalement pour mener cette analyse comparative, un module d'évaluation implémenté grâce aux modèles prédictifs de craft ai a été comparé à un IDS à base d'apprentissage automatique industriel. En appliquant l'outil de corrélation sur les sorties de l'IDS industriel, le scénario d'attaque a été complètement reconstruit, les trois incongruités ayant été clairement identifiées. Aucun résultat concluant n'a cependant pu être obtenu en combinant le module d'évaluation de craft ai et le module de corrélation d'Airbus.

Au niveau de la précision dans la détection d'attaque, la métrique de mesure utilisée est la capacité de détection. La métrique de capacité de détection mesure la quantité d'information partagée entre les données d'entrée d'un IDS et ses sorties (c.-à-d. l'information mutuelle). Plus l'information mutuelle entre ces données est grande, moins il y a d'incertitude sur les données d'entrées de l'IDS en observant les alertes produites, et par conséquent plus la précision de détection de l'IDS est grande.

Comparé à l'IDS industriel, craft ai a montré une capacité de détection plus élevée que celle de l'IDS industriel ce qui nous mène à la conclusion que craft ai est plus précis dans la détection d'attaque. Ce résultat est dû au fait que les modèles de craft ai émettent beaucoup moins de faux positifs que l'IDS industriel sur ce cas.

Cette collaboration a été bénéfique pour valider notre méthodologie et à nos partenaires industriels, notamment sur des aspects liés au partage des données, des technologies et des connaissances métiers des différents participants.

Voici quelques témoignages :

« *Notre collaboration avec Thalès et Airbus, ainsi qu'avec les chercheurs de l'IRT SystemX, nous a permis de démontrer la valeur de la technologie de craft ai sur le sujet de la cybersécurité. Grâce à l'expertise métier de nos partenaires, nous avons pu déterminer les enjeux d'application de craft ai pour la détection d'intrusions par analyse comportementale et cadrer les prochaines étapes de cette collaboration fructueuse* ». **Caroline Chopinaud**, Chief Business Development Officer chez craft ai.

« *Airbus CyberSecurity se félicite du projet START@SystemX Cybersécurité, basé sur une collaboration quadripartite avec l'IRT SytemX, craft ai et Thalès. La richesse des concepts mis en œuvre ainsi que la non uniformité et la diversité des approches adoptées par les différentes parties ont été une réelle source de progrès, autant sur le plan des avancées technologiques que sur la manière de les gérer et de les orienter* ». **Jean Philippe Fauvelle**, Architecte Technique et Solution en cyber-sécurité, IA, cloud, big-data chez Airbus Defence and Space CyberSecurity.

« *Le bilan de la participation de craft ai à la thématique cybersécurité de START@SystemX est positif à plusieurs égards. L'implication continue et la disponibilité de l'équipe de craft ai ont permis une compréhension de nos intérêts mutuels impossible autrement. La start-up craft ai a ainsi su démontrer sa capacité à appréhender les enjeux de la cybersécurité et de ses nombreux acteurs, afin d'identifier les avantages et inconvénients de leur solution. Les résultats concrets sortis de cette phase d'expérimentation ont mis en évidence que l'évaluation opérationnelle de ce type de technologies implique de se placer dans des contextes applicatifs précis, ce qui a été rendu possible grâce à la collaboration d'Airbus et de Thalès. L'analyse de ces résultats par l'IRT SystemX a permis de confirmer la nécessité pour ces technologies d'IA de disposer de données en nombre, suffisamment représentatives de la réalité d'un système d'information récent, mais également d'une connaissance fine des invariants du système, afin de produire des résultats exploitables.* », **Olivier Bettan**, Head of Cyber Security Lab chez Thales Solutions de Sécurité & Services et **Jérome Kodjabachian**, Expert Thales, Responsable Technique au laboratoire ThereSIS de Thales à Palaiseau.