Génération automatisée de graphes de connaissances CTI et de graphes d'attaques pour la gestion Continue des risques cybersécuritaires

Numéro de la fiche : OPR-1265

Sommaire

DIRECTION DE RECHERCHE

Amine Trabelsi, Professeur - Département d'informatique

RENSEIGNEMENTS

amine.trabelsi@usherbrooke.ca

UNITÉ(S) ADMINISTRATIVE(S)

Faculté des sciences
Département d'informatique

CYCLE(S)

3e cycle

LIEU(X)

Université de Sherbrooke, campus principal

Description du projet

Dans un contexte où les cybermenaces évoluent à un rythme effréné, la gestion traditionnelle des risques cybersécuritaires montre ses limites face à la complexité et à la diversité des attaques modernes. Ce projet de recherche propose une approche novatrice basée sur l'intelligence artificielle pour automatiser et optimiser la compréhension du paysage des menaces cyber en temps réel.
L'objectif central consiste à développer un système de Graphes de Connaissances CTI (Cyber Threat Intelligence) continuellement alimenté et mis à jour, capable d'intégrer l'intelligence des menaces extraite automatiquement depuis des flux d'informations hétérogènes et des rapports cybersécuritaires. Cette plateforme s'appuiera sur des techniques avancées de traitement du langage naturel et d'apprentissage automatique pour identifier, extraire et structurer les informations pertinentes concernant les menaces, vulnérabilités, indicateurs de compromission et tactiques d'attaque.
Le projet développera parallèlement un pipeline systématique de construction de graphes d'attaques, établissant des liens intelligents entre le graphe de connaissances CTI et les référentiels externes reconnus tels que MITRE ATT&CK et CAPEC. Cette intégration permettra de créer des modèles d'attaques sophistiqués offrant une vision holistique des scénarios de menaces et de leurs interconnexions complexes.
L'architecture proposée intégrera des mécanismes d'apprentissage adaptatif permettant au système d'évoluer automatiquement avec l'émergence de nouvelles menaces. Les graphes seront enrichis par des algorithmes de raisonnement capables d'identifier des patterns cachés, de prédire l'évolution des menaces et de suggérer des mesures de mitigation proactives.
Cette recherche produira des datasets réutilisables et des modèles affinés mis à disposition de la communauté scientifique, garantissant la reproductibilité et encourageant les développements futurs dans ce domaine critique pour la sécurité numérique.

Discipline(s) par secteur

Sciences naturelles et génie

Informatique

Financement offert

Oui

Montant annuel : 30 000$

La dernière mise à jour a été faite le 26 August 2025. L’Université se réserve le droit de modifier ses projets sans préavis.