Avis de Soutenance

Monsieur AMINE TELLACHE

Spécialité : Informatique et Applications

Soutiendra publiquement ses travaux de thèse intitulés

« Cybersécurité de nouvelle génération fondée sur l'intelligence artificielle : de la détection collaborative des intrusions à la réponse automatisée aux incidents »

dirigés par Monsieur Yacine GHAMRI DOUDANE

Soutenance prévue le **vendredi 16 janvier 2026** à 14h00

Lieu : La Rochelle Université – Pôle Communication
Amphiheatre Michel Crépeau
44 Avenue Albert Einstein 17000 La Rochelle

Composition du jury proposé

M. Yacine GHAMRI DOUDANE	La Rochelle Université	Directeur de thèse
Mme Leila MERGHEM-BOULAHIA	Université de Technologie de Troyes	Rapporteure
Mme Samiha AYED	IMT Atlantique	Rapporteure
M. Ronan CHAMPAGNAT	La Rochelle Université	Examinateur
Mme Kandaraj PIAMRAT LEREBOURS	Nantes Université	Examinatrice
Mme Selma BOUMERDASSI	Université Paris 8	Examinatrice
M. Mokhtari AMDJED	OODRIVE	Co-encadrant de thèse
M. Abdelaziz AMARA KORBA	German University of Technology in Oman (GUtech)	Co-encadrant de thèse
M. Horea MOLDOVAN	OODRIVE	Invité

Résumé :

L'intelligence artificielle (IA) s'impose aujourd'hui comme un levier majeur dans l'évolution de la cybersécurité, en apportant des avancées décisives dans la protection contre des menaces toujours plus sophistiquées. Deux domaines s'avèrent particulièrement critiques dans ce contexte : la détection d'intrusions et la réponse aux incidents. La première constitue le point d'entrée indispensable pour identifier les attaques, tandis que la seconde en assure le traitement et la neutralisation. Ensemble, elles forment le pilier essentiel de la défense numérique contemporaine. Les systèmes traditionnels de détection d'intrusions (IDS) révèlent rapidement leurs limites face à l'évolution continue des menaces. Leur efficacité se trouve compromise par un taux élevé de faux positifs, ainsi que par l'utilisation de jeux de données souvent déséquilibrés et peu représentatifs de la diversité réelle des menaces. Pour dépasser ces obstacles, la recherche s'oriente vers des approches plus intelligentes, capables de tirer parti d'analyses collaboratives et distribuées. Ces modèles visent à mutualiser l'expérience et les connaissances de plusieurs organisations afin d'améliorer la détection, tout en soulevant de nouveaux défis liés à l'hétérogénéité des données et à la préservation de la confidentialité. Parallèlement, les processus de réponse aux incidents sont paralysés par une avalanche d'alertes, la fragmentation et l'hétérogénéité des informations issues des renseignements sur les menaces cyber (CTI). Leur traitement, encore largement manuel, demeure chronophage, coûteux et passe difficilement à l'échelle. Ces contraintes révèlent l'importance de concevoir des solutions intelligentes, automatisées et adaptatives, capables de fonctionner efficacement dans des environnements cloud dynamiques. Dans cette thèse, nous apportons quatre contributions principales visant à renforcer les capacités de cybersécurité de bout en bout. Premièrement, nous introduisons MARL IDS, une architecture de détection d'intrusions basée sur l'apprentissage par renforcement multi-agent, qui améliore la précision et l'adaptabilité en combinant des agents spécialisés par type d'attaque et un agent décisionnel global qui consolide leurs résultats. Deuxièmement, nous proposons FMARL IDS, une extension fédérée de cette approche permettant la collaboration inter-organisationnelle tout en préservant la confidentialité des données. Ce modèle traite efficacement les problèmes liés à l'hétérogénéité des données (non-IID) et démontre une grande robustesse avec un faible taux de faux positifs. Côté réponse aux incidents, nous présentons AI2R, un cadre basé sur la génération augmentée de récupération (RAG) qui intègre les grands modèles de langage (LLMs) avec une CTI dynamique afin d'automatiser et d'accélérer la génération de réponses contextuelles et actionnables, réduisant ainsi la charge des analystes et les délais de réaction. Enfin, nous proposons CoT AI2R, une extension guidée par le raisonnement par chaine (CoT), qui structure le processus décisionnel des LLMs en étapes alignées avec les pratiques réelles des différentes équipes de cybersécurité. Cette approche améliore la fiabilité, l'explicabilité et la pertinence opérationnelle des recommandations générées. Dans l'ensemble, ces contributions montrent que l'IA peut considérablement renforcer la défense en cybersécurité, en améliorant à la fois la précision et la collaboration dans la détection d'intrusions, ainsi que la rapidité, la cohérence et la contextualisation dans la réponse aux incidents. Au-delà de ces avancées techniques, cette thèse ouvre la voie à une nouvelle génération de systèmes de défense intelligents, adaptatifs, fiables, capables de fonctionner de manière autonome dans des environnements cloud dynamiques et hétérogènes.