8a avenue Maistriau
7000 Mons

www.heh.be

Intitulé de l'UE	Machine learning appliqué à la cybersécurité
Section(s)	- **(3 ECTS)** Master en sciences de l'Ingénieur industriel / Finalité Informatique / Cycle 2 Bloc 2 option Réseaux et Sécurité

Responsable(s)	Heures	Période
Jean-Sébastien LERAT	45	**Quad 1**

Activités d'apprentissage	Heures	Enseignant(s)
Data Mining	20h	**Jean-Sébastien LERAT**
Machine learning	25h	**Jean-Sébastien LERAT**

Prérequis	Corequis
- Cryptologie	- Sécurité des systèmes informatiques

Répartition des heures
Data Mining : 10h de théorie, 10h de travaux
Machine learning : 10h de théorie, 15h de travaux

Langue d'enseignement
Data Mining : Français, Anglais
Machine learning : Français, Anglais

Connaissances et compétences préalables
Maîtrise des concepts de programmations Maîtrises de concepts mathématiques du bachelier

Objectifs par rapport au référentiel de compétences ARES

Cette UE contribue au développement des compétences suivantes

- Master en Sciences de l'ingénieur industriel :

- Identifier, conceptualiser et résoudre des problèmes complexes
  - Intégrer les savoirs scientifiques et technologiques afin de faire face à la diversité et à la complexité des problèmes rencontrés
  - Concevoir, développer et améliorer des produits, processus et systèmes techniques
  - Sélectionner et exploiter les logiciels et outils conceptuels les plus appropriés pour résoudre une tâche spécifique
  - Établir ou concevoir un protocole de tests, de contrôles et de mesures.

- Concevoir et gérer des projets de recherche appliquée
    - Réunir les informations nécessaires au développement de projets de recherche
    - Valider les performances et certifier les résultats en fonction des objectifs attendus
    - Exploiter les résultats de recherche
- S'intégrer et contribuer au développement de son milieu professionnel
    - Travailler en autonomie et en équipe dans le respect de la culture d'entreprise
- S'engager dans une démarche de développement professionnel
    - Actualiser ses connaissances et s'engager dans les formations complémentaires adéquates

- Master en Sciences de l'ingénieur industriel en Informatique :

Acquis d'apprentissage spécifiques

Comprendre les algorithmes de machine learning (principalement data mining et deep learning)
Mettre en place une solution de machine learning (principalement data mining et deep learning)
Justifier les choix de conception d'une solution de machine learning
Concevoir et mettre en oeuvre une solution de machine learning en réponse à un problème de cybersécurité

Contenu de l'AA Data Mining

- Notions de Data mining : classification, clustering, association, apprentissage (non-)supervié, on/offline, évaluation de l'apprentissage
- Apprentissage par renforcement
- Apprentissage profond : ANN, CNN, RNN, LSTM, GRU
- Détection de signature
- Détection d'anomalies
- IDS (intrusion detection system) intelligent
- Détection de profil d'utilisation de réseau
- Détection de menaces

Contenu de l'AA Machine learning

- Notions de Machine Learning (apprentissage par renforcement, métaheuristique, apprentissage profond ...)
- Modèle : théorie des jeux, modèles basé sur les chaînes de markov, probabiliste, logique floue, ...
- Détection de signature
- Détection d'anomalies
- IDS (intrusion detection system) intelligent
- Détection de profil d'utilisation de réseau
- Détection de menaces

Méthodes d'enseignement

Data Mining : cours magistral, travaux de groupes, approche par projets, approche avec TIC

Machine learning : cours magistral, travaux de groupes, approche par projets, approche avec TIC

Supports

Data Mining : copies des présentations

Machine learning : copies des présentations

Ressources bibliographiques de l'AA Data Mining

Dua, S. & Du, X. (2016). *Data Mining and Machine Learning in Cybersecurity.* CRC Press

Talbi, E.G. (2009). *Metaheuristics: From Design to Implementation.* Wiley

Shoham, Y. & Leyton-Brown, K. (2008). *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations.* Cambridge University Press

Nowak, M.A. (2006). *Evolutionary Dynamics.* Harvard University Press

Osborne, M.J. (2009). *An Introduction to Game Theory.* Oxford University Press

Borne, P., Benrejeb, M. & Haggège, J. (2007). *Les réseaux de neurones: présentation et applications.* Éditions Technip

Sutton, R.S. (2012). *Reinforcement Learning.* Springer US

Lin, C.T. & Lee, C.S.G. (1996). *Neural Fuzzy Systems: A Neuro-fuzzy Synergism to Intelligent Systems.* Prentice Hall PTR

Conway, D., & White, J. M. (2012). Machine learning for hackers: Case studies and algorithms to get you started. O'Reilly Media.

Dua, S., & Du, X. (2011). Data mining and machine learning in cybersecurity. Auerbach Publications.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning (adaptive computation and machine learning series). The MIT Press.

Machine learning in cyber trust: Security, privacy, and reliability. (2009). Springer.

Patterson, J., & Gibson, A. (2017). Deep learning: A practitioner's approach. O'Reilly Media.

Ressources bibliographiques de l'AA Machine learning

Dua, S. & Du, X. (2016). *Data Mining and Machine Learning in Cybersecurity.* CRC Press

Talbi, E.G. (2009). *Metaheuristics: From Design to Implementation.* Wiley

Shoham, Y. & Leyton-Brown, K. (2008). *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations.* Cambridge University Press

Nowak, M.A. (2006). *Evolutionary Dynamics.* Harvard University Press

Osborne, M.J. (2009). *An Introduction to Game Theory.* Oxford University Press

Borne, P., Benrejeb, M. & Haggège, J. (2007). *Les réseaux de neurones: présentation et applications.* Éditions Technip

Sutton, R.S. (2012). *Reinforcement Learning.* Springer US

Lin, C.T. & Lee, C.S.G. (1996). *Neural Fuzzy Systems: A Neuro-fuzzy Synergism to Intelligent Systems.* Prentice Hall PTR

Conway, D., & White, J. M. (2012). Machine learning for hackers: Case studies and algorithms to get you started. O'Reilly Media.

Dua, S., & Du, X. (2011). Data mining and machine learning in cybersecurity. Auerbach Publications.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning (adaptive computation and machine learning series). The MIT Press.

Machine learning in cyber trust: Security, privacy, and reliability. (2009). Springer.

Patterson, J., & Gibson, A. (2017). Deep learning: A practitioner's approach. O'Reilly Media.

Évaluations et pondérations	
Évaluation	Note globale à l'UE
Langue(s) d'évaluation	Français, Anglais
Méthode d'évaluation	20% de travaux et d'évaluation continue, 80% examen oral dont défense de projet. Les 20% de travaux et d'évaluation continue correspondent à la manière dont l'étudiant s'implique dans la réalisation des exercices présentés en cours. Les 80% d'exame consiste en la réalisation d'un projet d'apprentissage automatique liée à la sécurité informatique. Les étudiants doivent concevoir et implémenter la solution choisie. Ils doivent remettre le travail ainsi qu'un rapport présenté sous la forme d'un article scientifique. Celui-ci fera l'objet d'une présentation orale. Lors de la défense de projet, l'étudiant sera amené à confronter ses arguments scientifiques de par ses connaissances acquises au cours. Les supports de cours sont anglais mais le cours est enseigné en Français. Attention : les étudiants de l'option doivent réaliser un travail dans le cadre des AA "Machine Learning" et le présenter. Les étudiants présents (non-Erasmus+) s'entraîneront également afin de participer au Cybersecurity Challenge (CSC, https://www.cybersecuritychallenge.be/). Cela signifient qu'ils s'engagent à y participer durant le second quadrimestre. Les étudiants qui doivent réaliser un stage doivent contacter le responsable de stage afin d'intégrer la participation au CSC dans la convention de stage.
Report de note d'une année à l'autre pour l'AA réussie en cas d'échec à l'UE	
Data Mining : **non** Machine learning : **non**	

Année académique : **2021 - 2022**