Université du Québec en Outaouais **Département d'informatique et d'ingénierie**

Sigle : CYB1003 Gr. 01
Titre : Introduction à la cybersécurité
Session : Hiver 2026 Horaire et local
Professeur : WA ARA LIMANGANA HASSANA

1. Description du cours paraissant à l'annuaire :

Objectifs

Au terme de ce cours, l'étudiant.e sera en mesure de comprendre les défis et enjeux de la cybersécurité et différentes approches permettant de relever ces défis.

Contenu

Définitions et concepts de base de la cybersécurité: triade CID (équilibre entre confidentialité, intégrité et disponibilité). Évolutions du cyberespace (interconnectivité des systèmes, actifs dans le cyberespace, aspects physiques et risques associés). Vulnérabilités logicielles et exploitation. Cadres de référence en cybersécurité (CIS, NIST-CSF, etc.). Moyens de protection (conception sécurisée du cyberespace, analyse, surveillance, contrôle, test, etc.). Sauvegarde et protection des données. Encodage et cryptographie. Cybermenaces, cyberattaques, gestion d'incidents, gouvernance et éthique en cybersécurité. Résolution de problèmes de cybersécurité, issus du monde réel, pour atténuer les cybermenaces.

Descriptif – Annuaire

2. Objectifs spécifiques du cours :

Au terme de cette activité, l'étudiante, l'étudiant(e), doit dégager une compréhension globale et cohérente du domaine de la cybersécurité et être au fait des enjeux, des problématiques et des solutions techniques proposés dans la littérature.

3. Stratégies pédagogiques : le cours est en présentiel

Le cours alterne entre des exposés magistraux interactifs, des démonstrations pratiques et des séances de travaux dirigés (TD) favorisant l'expérimentation des notions abordées.

Chaque séance de cours vise à introduire un thème central de la cybersécurité à l'aide d'exemples concrets et d'études de cas réels.

Les TD permettent d'appliquer ces notions à travers :

– des exercices d'analyse de menaces et vulnérabilités ;

– des manipulations d'outils de sécurité (pare-feux, VPN, chiffrement) dans des environnements simulés ;

– des discussions de groupe sur l'éthique et la gouvernance en cybersécurité.

L'évaluation formative est soutenue par des quiz Moodle et des mini-labs hebdomadaires.

La participation active et la réflexion critique des étudiant.es sont encouragées afin de développer la compréhension globale des enjeux de sécurité.

4. Heures de disponibilité ou modalités pour rendez-vous :

Disponible avant ou après les cours, et sur rendez-vous. Je suis disponible avant le cours et surtout en ligne à partir de 14h.

Courriel : waah01@uqo.ca

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Présentation du plan de cours et des attentes Introduction à la cybersécurité : définitions, enjeux, triade CID (Confidentialité–Intégrité–Disponibilité)	12/01/2026
2	Évolution du cyberespace et des menaces ; typologie d'attaques **TD1**/TP : cartographie des menaces et classification par impact **20/01/2026**	19/01/2026
3	Vulnérabilités logicielles et exploitation ; principes de durcissement **TD2**/TP: analyse d'une faille réelle (CVE) **27/01/2026**	26/01/2026
4	Cadres de référence : CIS, NIST-CSF, ISO 27001	02/02/2026
5	Contrôle d'accès : DAC, MAC, RBAC ; gestion des identités **TD3** : modélisation de rôles et autorisations **10/02/2026**	09/02/2026
6	Cryptographie et encodage : principes de chiffrement et d'authentification **TD4**: démonstration d'outils de hachage et chiffrement symétrique **17/02/2026**	16/02/2026
7	Sécurité des réseaux : pare-feux, IDS/IPS, VPN Gestion d'incidents et continuité des opérations **TD5**/TP : configuration de base d'un pare-feu sur simulateur **24/02/2026**	23/02/2026
8	**Semaine d'études**	2 au 6 mars 2026
9	**Examen de mi-session** **TD6**/TP : étude de cas sur un incident de cybersécurité **10/03/2026**	09/03/2026
10	Gouvernance, politiques et conformité **TD7**/TP: analyse d'une politique de sécurité existante (ISO 27002) **17/03/2026**	16/03/2026
11	Sécurité du stockage et protection des données ;	23/03/2026
12	Sécurité des applications et systèmes d'exploitation	30/03/2026
13	**Congé du lundi de Pâques** **TD8** : Sécurité du cloud et de l'Internet des objets (IoT) **07/04/2026**	06/04/2026
14	Éthique, vie privée et responsabilité numérique	13/04/2026
15	**Examen final**	20/04/2026

6. Évaluation du cours :

Les évaluations sont alignées avec les objectifs du cours et favorisent la compréhension appliquée des concepts :
– Examen de mi-session : 30 %
– Examen final : 40 %
– Travail de session / étude de cas : 30 %
Le travail de session consiste à analyser un scénario d'incident et à proposer des mesures de prévention, de détection et de réponse.
Des quiz formatifs sont proposés sur Moodle pour soutenir l'apprentissage continu.

7. Politiques départementales et institutionnelles :

- Politique du département d'informatique et d'ingénierie relative à la tenue des examens
- Note sur le plagiat et sur la fraude
- Politique relative à la qualité de l'expression française écrite chez les étudiants et les étudiantes de premier cycle à l'UQO
- Absence aux examens : cadre de gestion, demande de reprise d'examen (formulaire)

Tolérance ZÉRO en matière de violence à caractère sexuel.

Le Bureau d'intervention et de prévention en matière de harcèlement (BIPH) a pour mission d'accueillir, soutenir et guider toute personne vivant une situation de harcèlement, de discrimination ou de violence à caractère sexuel. Le BIPH oriente ses actions afin de prévenir les violences à caractère sexuel pour que nous puissions étudier, travailler et s'épanouir dans un milieu sain et sécuritaire.
Vous vivez ou êtes une personne témoin d'une situation de violence à caractère sexuel ? Vous êtes une personne membre de la communauté étudiante ou une personne membre du personnel, autant à Gatineau qu'à Ripon et St-Jérôme, l'équipe du BIPH est là pour vous, sans jugement et en toute confidentialité.
Ensemble, participons à une culture de respect.
Pour de plus amples renseignements consultez UQO.ca/biph ou écrivez-nous au Biph@uqo.ca

8. Principales références :

1. Marion AGÉ, Franck EBEL, Raphaël RAULT, Sébastien BAUDRU, Robert CROCFER, David PUCHE, Jérôme HENNECART, Sébastien LASSON , « Sécurité informatique, Ethical Hacking », ISBN : 978-2-7460-6248-1, ENI; Édition : 2e édition, 2011
2. Michael T. Goodrich. Roberto Tamassia, "Introduction to computer security", ISBN-10 : 0-321-51294-4, Pearson Education, 2011
3. Raymond Panko, « Sécurité des systèmes d'information et des réseaux », ISBN : 2-7440-7054-8, Pearson Education, (version traduite de l'anglais), 2004
4. Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing", ISBN-10 : 0-13-035548-8, Prentice Hall, Third Edition, December 02, 2002
5. William Stallings, "Network Security Essentials: Applications and Standards", ISBN : 0132380331, Prentice Hall; 3rd Edition (July 19, 2006)
6. Dieter Gollmann, "Computer Security", ISBN : 0470862939, John Wiley & Sons; 2nd Edition (January 18, 2006)
7. Raymond Panko, "Corporate Computer and Network Security",ISBN : 0130384712, Prentice Hall; United States Edition (March 17, 2003)
8. Matt Bishop, "Introduction to Computer Security", ISBN : 0-321-24744-2, Addison-Wesley, 3rd Edition (October 2006)

9. Page Web du cours :

http://moodle.uqo.ca