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

Sigle : CYB1003 Gr. 20
Titre : Introduction à la cybersécurité
Session : Automne 2026 Horaire et local
Professeur.e : Beniiche , Abdeljalil

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 :

L'objectif de cette activité est que l'étudiante ou l'étudiant soit capable de comprendre de manière globale et cohérente le domaine de la cybersécurité, et qu'il ou elle soit au courant des enjeux, des problèmes et des solutions techniques présentés dans la littérature.

3. Stratégies pédagogiques :

Les séances de cours seront présentées sous forme magistrales interactifs, parsemées d'exercices de compréhension. Le matériel pédagogique est accessible à partir de la plateforme Moodle dédiée au cours. Un forum de discussion sera aussi disponible pour poser des questions liées à la matière enseignée.

Des travaux dirigés et pratiques seront également réalisés afin de consolider les concepts présentés durant les séances de cours.

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

Communication par courriel (abdeljalil.beniiche@uqo.ca) et via le forum de discussion.

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Présentation du plan de cours Introduction aux concepts de base de la cybersécurité • Objectifs de la cybersécurité • Triade CID (Confidentialité, intégrité, et disponibilité) • Enjeux, menaces et contrôles de cybersécurité • Normes, cadres de référence en cybersécurité (CIS, NIST-CSF, ISO, etc.) • Métiers, opportunités et certifications en cybersécurité	08 sep. 2026
2	Menaces et vulnérabilités des systèmes • Types de vulnérabilités • Techniques d'exploitation des vulnérabilités • Impact des vulnérabilités • Catégories des menaces	15 sep. 2026

	• Évolutions du cyberespace et risques associés • Cybermenaces, cyberattaques • Modélisation de la menace **TD/TP1 : 16 septembre**	
3	Gestion des menaces et vulnérabilités • Système commun de notation des vulnérabilités (CVSS) • Vulnérabilités courantes et expositions (CVE) • NVD (National Vulnerability Database) • Recensement et classification des actifs informationnels • Classification et protection des données • Cycle de vie des données **TD/TP2 : 23 septembre**	22 sep. 2026
4	Gestion de la cybersécurité et analyse du risque • Analyse de structures organisationnelles • Gestion de la cybersécurité dans les entreprises • Gestion de risque cyber • Méthodes d'analyse de risque • Normes et référentiels **TD/TP3 : 30 septembre**	29 sep. 2026
5	Systèmes GRC : Gouvernance, Risque, et Conformité • Gouvernance, Risque, et Conformité • Outils GRC • Orientation pour la gestion des risques • Traitement des risques • Plan de remédiation **TD/TP4 : 07 octobre**	06 oct. 2026
6	**Semaine d'études**	13 oct. 2026
7	Cryptographie • Cryptographie symétrique et asymétrique • Chiffrement, encryption et hachage • Algorithmiques RSA, DES et triple DES, etc • Sécurité et génération de clés • Certificats et signatures numériques **Révisions pour l'examen de mi-session**	20 oct. 2026 **(Séance en non-présentiel)**
8	**Examen de mi-session**	27 oct. 2026

9	Sécurité et protection des réseaux • Principe de fonctionnement des VPN : Tunneling, routage, filtrage • Protocoles sécurisés: IPsec, SSH, TLS, etc. • Vulnérabilités des réseaux • Segmentation réseautiques • Sécurité des réseaux • Principe de Zéro Trust	03 nov. 2026 **(Séance en non-présentiel)**
10	Systèmes pare-feux (*Firewalls*) • Principe de conception des pare-feu (firewall) • Configuration d'un pare-feu • Règles de filtrage • Architecture de sécurisation par pare-feu • Le « proxy » **TD/TP5 : 11 novembre**	10 nov. 2026
11	Systèmes de contrôle et gestion des identités et des accès • Architecture de contrôle d'accès • Authentification et autorisation • Authentification multifacteur (MFA) • Authentification unique (SSO), Jeton, JIT • Modèles de contrôle d'accès : DAC, MAC, RBAC, etc. **TD/TP6 : 18 novembre**	17 nov. 2026
12	Sécurité des postes de travail • Politique de mots de passe • Mises à jour et patch management • Sécurité physique et verrouillage • Antivirus, EDR, XDR et anti-malware • Outils pour la détection d'intrusion • Guide CIS (Center for Internet Security) **TD/TP7 : 25 novembre** **Énoncé : Travail de session**	24 nov. 2026
13	Journalisation, surveillance et gestion des incidents • Objectif de la journalisation • Source de la journalisation • Type de journaux cybersécurité • SIEM et outils de la journalisation • Sauvegarde et protection des données	01 déc. 2026

14	Révision et récapitulatif du cours Préparation à l'examen final Questions/réponses sur le travail de session	08 déc. 2026 **(Séance en non-présentiel)**
15	**Examen final**	15 déc. 2026

6. Évaluation du cours :

L'évaluation est l'appréciation du niveau d'apprentissage atteint par l'étudiant(e) par rapport aux objectifs des cours et des programmes.

Dans le cas spécifique du cours Introduction à la cybersécurité**,** l'attribution des notes se fera selon la répartition suivante :

- **Examen de mi-session : 30 %**
- **Examen final : 40 %**
- **Travail de session : 30 %**

7. Politiques départementales et institutionnelles :

- Politiques relatives à la tenue des examens
- Note sur le plagiat et les fraudes
- 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. Shoemaker, D., Sigler, K., & Shoemaker, T. (2023). Teaching Cybersecurity: A Handbook for Teaching the Cybersecurity Body of Knowledge in a Conventional Classroom (1st ed.). CRC Press.
10. NIST Cybersecurity Framework (CSF): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

9. Page Web du cours :

http://moodle.uqo.ca