

Sigle : CYB1003 Gr. 01**Titre : Introduction à la cybersécurité****Session : Automne 2026 Horaire et local****Professeur : Adi, Kamel****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 cyberspace (interconnectivité des systèmes, actifs dans le cyberspace, aspects physiques et risques associés). Vulnérabilités logicielles et exploitation. Cadres de référence en cybersécurité (CIS, NIST-CSF, etc.). Moyens de protection (conception sécurisée du cyberspace, 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 :

Les séances de cours seront présentées sous forme magistrales, 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, sous la supervision d'un assistant d'enseignement, seront également réalisés afin de consolider les concepts présentés durant les séances de cours. Ces activités s'appuieront notamment sur le cyber range Airbus Cybersecurity, afin de permettre aux étudiants de mettre en pratique les notions étudiées dans un environnement réaliste de cybersécurité.

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

Communication par courriel (Kamel.Adi@uqo.ca) et via le forum de discussion sur la plateforme Moodle

5. Plan détaillé du cours sur 15 semaines :

Semaine	Thèmes	Dates
1	Introduction et concepts de base Enjeux et menaces	08 sept. 2026

	Objectifs de la sécurité informatique	
2	Cryptographie - Historique - Cryptographie classique : mono et poly alphabétique	15 sept. 2026
3	Cryptanalyse - Historique - Classification des attaques - Cryptanalyse par recherche de clés - Cryptanalyse par analyse de fréquence Travail dirigé 1	22 sept. 2026
4	Cryptographie moderne : symétrique et asymétrique Travail pratique 1	29 sept. 2026
5	Les protocoles de communication - Introduction à la réseautique - Protocoles TCP/IP Travail dirigé 2 Révisions pour l'examen de mi-session	6 oct. 2026
6	Semaine d'études	13 oct. 2026
7	Examen de mi-session	20 oct. 2026
8	Vulnérabilités des systèmes - Types de vulnérabilités - Techniques d'exploitation des vulnérabilités Cadres de référence en cybersécurité (CIS, NIST-CSF, etc.) Travail pratique 2	27 oct. 2026
	Systèmes de détection d'intrusion - Approches pour la détection d'intrusion - NIDS et HIDS - Outils pour la détection d'intrusion Travail pratique 3	03 nov. 2026

10	Systèmes pare-feux (<i>Firewalls</i>) • Principe de conception des pare-feu (<i>firewall</i>) • Configuration d'un pare-feu • Règles de filtrage • Architecture de sécurisation par pare-feu • Le « <i>proxy</i> » Travail pratique 4	10 nov. 2026
11	<u>Cours à distance</u> Gestion de la sécurité informatique et analyse du risque • Analyse de structures organisationnelles • Gestion de risque • Méthodes d'analyse de risque ○ La méthode Octave ○ La méthode Mehari Travail pratique 5	17 nov. 2026
12	<u>Cours à distance</u> Les réseaux privés virtuels (VPN) • Principe de fonctionnement des VPN : <i>Tunneling</i>, routage, filtrage • Protocoles : IPsec, etc. • Mise en œuvre d'un VPN Travail pratique 6	24 nov. 2026
13	<u>Cours à distance</u> Systèmes de contrôle d'accès • Architecture de contrôle d'accès • Modèles de contrôle d'accès : DAC, MAC, RBAC, etc. Travail pratique 7	01 dec. 2026
14	Virologie informatique • Contexte et historique • Taxonomie d'infections • Cycle de vie d'un virus • Mécanismes d'infection • Techniques anti-virales	08 déc. 2026

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 CYB1003, 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 :

- 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)

À l'UQO, **les violences à caractère sexuel, c'est tolérance zéro!**

La communauté universitaire s'engage à lutter contre les inconduites, le harcèlement et les violences à caractère sexuel : parce que **le respect, c'est l'affaire de tout le monde!**

N'oubliez pas de faire la formation obligatoire :

uqo.ca/bimi/formation-obligatoire

Pour de plus amples renseignements :

bimi@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 : 2^e 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>

