UNIVERSITÉ DU QUÉBEC EN OUTAOUAIS

PROGRAMMES D'ÉTUDES
Version complète

Certificat en réseaux informatiques et cybersécurité - 4666

RESPONSABLE :

Gatineau

Karim El Guemhioui
Directeur de module

Pour de plus amples informations :

Téléphone : 819 595-3900, poste 1620
Courriel : modinfo@uqo.ca

SCOLARITÉ :

30 crédits, Premier cycle

OBJECTIFS :

Cette formation a pour objectif de fournir les connaissances et les compétences nécessaires pour sécuriser des réseaux informatiques, les surveiller activement en vue de prévenir et détecter les cybermenaces ainsi que pour assurer la reprise en cas d'incident.

Au terme de cette formation, l'étudiante ou l'étudiant sera en mesure de savoir comment :

1. Mener des recherches, analyser de l'information, préparer des rapports et des plans pour résoudre les problèmes de la sécurité des réseaux informatiques.
2. Sécuriser le trafic réseau.
3. Mettre en place des mécanismes de cybersécurité pour assurer un fonctionnement sécuritaire du réseau.
4. Diagnostiquer l'état d'un réseau informatique.
5. Identifier les vulnérabilités du réseau et mettre en place les contremesures nécessaires.
6. Assurer la résilience des réseaux informatiques dont il ou elle est responsable.
7. Mettre en place les mesures de reprise en cas d'incidents.
8. Communiquer efficacement sur les aspects de la sécurité des réseaux.

INFORMATIONS SUR L'ADMISSION :

Lieu d'enseignement	Régime	Trimestres d'admission		
		Automne	Hiver	Été
Gatineau	TP	✓	✓	

TP : Temps partiel

CONDITIONS D'ADMISSION :

Base collégiale

Être titulaire d'un diplôme d'études collégiales en informatique, en sciences informatiques et mathématiques ou en sciences de la nature ou l'équivalent;

Les détentrices et détenteurs d'un D.E.C. qui ne comporte pas au moins un cours de mathématiques de niveau collégial québécois, ou l'équivalent, devront réussir le cours d'appoint MAT1023 - Éléments de mathématiques pour l'informatique.

Base études universitaires

Avoir réussi un minimum de 30 crédits dans un programme universitaire, avec une moyenne cumulative de 2,0 sur 4,3 ou l'équivalent;

Les candidates et candidats dont le niveau de préparation en mathématiques ne comporte pas au moins un cours de mathématiques de niveau collégial québécois, ou l'équivalent, devront réussir le cours d'appoint MAT1023 - Éléments de mathématiques pour l'informatique.

Base adulte

Posséder des connaissances appropriées, avoir au moins vingt et un (21) ans et avoir occupé pendant au moins vingt-quatre (24) mois un poste dans les aspects techniques du domaine de l'informatique.

Les candidates et candidats dont le niveau de préparation en mathématiques ne comporte pas au moins un cours de mathématiques de niveau collégial québécois, ou l'équivalent, devront réussir le cours d'appoint MAT1023 - Éléments de mathématiques pour l'informatique.

PLAN DE FORMATION :

Cours obligatoires

CYB1003	Introduction à la cybersécurité
INF4523	Réseaux d'ordinateurs (INF1563 ou INF1653)
INF1653	Introduction à la programmation et aux scripts
CYB1153	Virtualisation des réseaux et cybersécurité
INF1343	Administration des réseaux (INF3803 ou INF4523)
CYB1023	Sécurité des réseaux informatiques (CYB1003 et INF4523)
CYB1133	Sécurité des données et contrôle d'accès au niveau organisationnel (INF1563 ou INF1653)
CYB1143	Sécurité des réseaux mobiles (CYB1003 et INF4523)
	6 crédits optionnels

Cours optionnels

Choisir six (6) crédits parmi la liste de cours optionnels suivante :

COM1193A	English Communication Skills for Science Studies
COM2373	Éthique, technologies de l'information et société
CYB1033	Aspects légaux de la cybersécurité
CYB1043	Audit des systèmes d'information en comptabilité
CYB1053	Audit en cybersécurité et conformité (INF3803 ou INF4523)
CYB1063	Communication et leadership en cybersécurité
CYB1073	Cybersécurité comportementale
CYB1083	Géopolitique du cyberespace
CYB1093	Gestion de projets et cybersécurité (CYB1003)
CYB1103	Gouvernance en cybersécurité et gestion de risque (CYB1003)
CYB1123	Sécurité de l'infonuagique et des services Web (CYB1003 et CYB1133)
INN1003	Projet intégrateur en innovation numérique
	Tout cours offert au baccalauréat en informatique

COM1193A

English Communication Skills for Science Studies

Objectifs : The student will acquire the knowledge and the discipline-specific written and oral communication skills, as required for science and engineering professionnals.

Contenu : The focus of the course will be on appropriate style and format of written documents, such as product, process and project description, proposal and report, and on scientific literature reviews. A closely related oral work will also be done and will enable students to give formal presentations, lead discussions, take part in seminars and conduct meetings.

COM2373

Éthique, technologies de l'information et société

Objectifs : Permettre à l'étudiant de se sensibiliser aux questions et problèmes d'ordre éthique que posent la création, l'utilisation et la diffusion des technologies de l'information.

Contenu : Présentation des principes d'ordre éthique susceptibles de concerner ou de s'appliquer au domaine des technologies de l'information. Étude de politiques, de cadres juridiques et réglementaires et de protocoles divers balisant ce domaine aux niveaux national et international. Impacts social et culturel des nouvelles technologies de l'information. Examen plus approfondi de problèmes touchant aux cadres et aux modes de vie en société : respect de la vie privée et de la réputation, liberté d'expression et *censure+, utilisation et couplage des banques de données informatisées, droit d'auteur, mésinformation et désinformation, commercialisation des informations personnelles, etc.

CYB1003

Introduction à la cybersécurité

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.

CYB1023

Sécurité des réseaux informatiques

Objectifs : Au terme de ce cours, l'étudiant.e aura approfondi par la pratique les techniques d'analyse de vulnérabilités, d'élaboration de scénarios d'attaques et de sécurisation des réseaux informatiques.

Contenu : Rappel sur les architectures de réseaux informatiques et propriétés de sécurité. Anatomie d'une cyberattaque ("Cyber Kill Chain"). Mesures de sécurité (zonage, défense en profondeur, défense active, sécurité du périmètre, gestion des accès, etc). Gestion des vulnérabilités dans les réseaux informatiques. Principaux outils utilisés pour analyser et attaquer un réseau informatique (wireshark, nmap, nessus, metasploit, etc.). Contrôles de sécurité (NIST 800-53). Contre-mesures disponibles pour faire face aux différentes attaques réseau. Techniques de détection et de protection (pare-feux, système de prévention et de détection des intrusions, filtrage de courriels, etc.). Sécurité des réseaux sans fil. Sécurité d'accès à distance (IPSEC, VPN). Résolution de problèmes de sécurité des réseaux informatiques issus du monde réel. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

CYB1033

Aspects légaux de la cybersécurité

Objectifs : Au terme de ce cours, l'étudiant.e aura connaissance de la législation québécoise, de la législation canadienne et des traités internationaux dans le domaine de la cybersécurité, ainsi que des pratiques concernant le sujet.

Contenu : Cadre légal et juridique pour la cybersécurité, la cybercriminalité et les technologies de l'information. Lois constitutionnelles et chartes des droits. Législation canadienne, québécoise et traités internationaux. Le code pénal du Canada et les articles applicables à la cybersécurité et à la cybercriminalité. Autres lois et règlements pertinents, comme la loi sur le pourriel et la loi sur le recyclage de fonds. La juridiction. Législation canadienne et québécoise sur l'accès à l'information, sur les documents électroniques, sur la protection des données et sur la protection de la vie privée.

CYB1043

Audit des systèmes d'information en comptabilité

Objectifs : Au terme de ce cours, l'étudiant.e sera familiarisé.e avec les concepts associés à l'audit sécurisé et au contrôle des systèmes d'information d'un point de vue comptable.

Contenu : Introduction aux Systèmes d'Information Comptables (SIC). Modélisation des données. Documentation des SIC. Processus d'affaire. Contrôle interne des SIC. Fraudes digitales et crimes informatiques comptables. Aspects éthiques et protection de la vie privée affectant l'audit comptable. L'audit intégré. Développement et implantation efficace des SIC. Les progiciels de gestion. Audit et comptabilité en ligne. Projet d'audit d'un SIC.

CYB1053

Audit en cybersécurité et conformité

Objectifs : Au terme de ce cours, l'étudiant.e sera en mesure d'appliquer les méthodes d'audit en cybersécurité à partir de cadres de référence et législatifs, d'évaluer le niveau de risque et de prioriser les actions pour combler les écarts de façon optimale.

Contenu : Notions de base de systèmes d'exploitation. Processus d'évaluation et autorisation de sécurité (EAS ou SA&A), obligations légales des organisations, standards et certifications en cybersécurité, analyse du contexte organisationnel et analyse de risque. Audit de plateformes Windows et Linux, de réseaux sans fils et de plateformes mobiles, et évaluation de la robustesse des configurations à l'aide de scripts PowerShell et SCCM. Mesures correctives et conditions minimales d'opération. Stratégies de communication et gestion de l'information. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

CYB1063

Communication et leadership en cybersécurité

Objectifs : Au terme de ce cours, l'étudiant.e sera prêt.e à jouer un rôle central dans une organisation en utilisant des techniques de communication efficaces afin de traduire dans un langage d'affaire les enjeux de cybersécurité.

Contenu : Analyse de risque au niveau organisationnel. Engagement des parties prenantes, techniques de négociation et présentation efficace. Conversion du risque technique en risque organisationnel. Escalade de l'information en réponse aux incidents, échange d'information rapide et efficace (breffage), contrôle et dissémination de l'information et relation avec les médias. Rédaction de rapports techniques en cybersécurité. Transfert de connaissances et formation des utilisateurs aux pratiques responsables en cybersécurité. Résolution de problèmes de communication en cybersécurité issus du monde réel.

CYB1073

Cybersécurité comportementale

Objectifs : Au terme de ce cours, l'étudiant.e sera en mesure de comprendre les principaux facteurs humains de risques en cybersécurité et de décrire différentes techniques d'ingénierie sociale et les mécanismes d'influence sur lesquels ils s'appuient.

Contenu : Éléments de base de cybersécurité. Facteurs humains de risque en cybersécurité : erreurs et négligence, limitations et biais cognitifs. Profilage des cyberattaquants et des cyberdéfenseurs : motivations, comportements. Ingénierie sociale : mécanismes d'influence, tromperie, éléments de théorie des jeux comportementale. Risques liés aux médias sociaux et santé mentale : phénomènes de bulles, désinformation, cyberintimidation, pédo-piégeage. Problématiques psychologiques et sociales liées aux mécanismes d'authentification, choix et réutilisation des mots de passe, acceptabilité sociale de la biométrie. Techniques défensives basées sur le comportement (pots de miel, stéganographie, etc.).

CYB1083

Géopolitique du cyberespace

Objectifs : Au terme de ce cours, l'étudiant.e sera en mesure d'appréhender les enjeux et de comprendre les doctrines géopolitiques dans le cyberespace.

Contenu : Développement d'Internet, du dark web et du cyberespace. Contrôle et régulation du cyberespace. Respect des libertés individuelles dans le cyberespace. Conflits géopolitiques dans le cyberespace (guerre économique, combats militaires, renseignement, politique d'influence diplomatique et culturelle). Cyberconflictualité et cyberterrorisme, groupes APT. Doctrine de cyberdomination. Enjeux de souveraineté numérique et stratégies développées par les États pour renforcer leur contrôle et leur puissance dans le cyberespace.

CYB1093

Gestion de projets et cybersécurité

Objectifs : Au terme de ce cours, l'étudiant.e sera capable d'utiliser des processus, outils et techniques pour intégrer la cybersécurité dans l'ensemble du cycle de vie des projets.

Contenu : Cadres et modèles de gestion: approche DevSecOps, Agile, etc. Sécurité et protection de la vie privée dès la conception. Niveau de préparation technologique et modèles de maturité. Gestion du risque et des opportunités. Modélisation de la menace et plan de contingence. Intégrité de la chaîne d'approvisionnement. Gestion des équipes et procédures de sécurité. Stratégies et meilleures pratiques en gestion de projets de sécurité informatique. Conception et mise en œuvre de projets pour résoudre des problèmes de cybersécurité issus du monde réel. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

CYB1103

Gouvernance en cybersécurité et gestion de risque

Objectifs : Au terme de ce cours, l'étudiant.e sera initié.e aux moyens de gestion de la sécurité informationnelle ainsi qu'aux moyens de régulation des systèmes de sécurité mis en place dans une entreprise pour atteindre ses objectifs.

Contenu : La cybersécurité en tant que décision d'affaire. Principes de gouvernance appliqués aux technologies de l'information des entreprises. Survol des TI et de la sécurité en entreprise. Aperçu des référentiels de gouvernance des TI (COBIT et ISO 38500). Alignement stratégique des TI aux affaires. Gestion des risques TI. Cadres de contrôle. Cadre réglementaire

(Conformité). Cadre normatif. Fonctions de surveillance. Pratique d'audit interne. Survol de plateformes de gestion de la gouvernance des risques et de la conformité (GRC). Enjeux et défis rencontrés en gouvernance des TI et de la sécurité en entreprise. Résolution de problèmes de gouvernance et de gestion de risque tirés du monde réel. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

CYB1123

Sécurité de l'infonuagique et des services Web

Objectifs : Au terme de ce cours, l'étudiant.e sera familier.e avec les enjeux de la sécurité dans l'infonuagique et les services web, et sera capable de mettre en œuvre des solutions pour sécuriser les infrastructures infonuagiques et les services Web.

Contenu : Modèles de service (SAAS, PAAS, IAAS) et de déploiements (public, privé, communautaire, hybride) de l'infonuagique. Techniques et outils de virtualisation. Architecture d'une application Web. Éléments de base du langage SQL. Vulnérabilités, attaques et menaces dans le nuage et les services web (brute force, escalade de privilèges, XSS, injection de code, DDoS, etc.). Recommandations de l'OWASP (Open Web Application Security Project). Techniques de protection des données, des infrastructures et des applications dans le nuage (pare-feu, tests, etc.). Méthodologie d'évaluation de la sécurité applicative. Gestion des risques dans le nuage et aspects légaux de la sécurité dans le nuage et les applications Web. Ce cours comporte des séances obligatoires de travaux pratiques (TP).

CYB1133

Sécurité des données et contrôle d'accès au niveau organisationnel

Objectifs : Au terme de ce cours, l'étudiant.e aura acquis une compréhension de la problématique et des solutions pour la protection de données dans les organisations, comme le gouvernement, les banques et le militaire, ainsi qu'une compréhension des modèles abstraits et outils existants à cette fin.

Contenu : Principes généraux et besoins. Secret, confidentialité, intégrité, disponibilité. Besoin de savoir, moindre privilège, conflits d'intérêt, vie privée. Politiques, modèles et administrations. Contrôle d'accès et contrôle de flux de données. Domaines, sessions et flux de travaux. Mise en œuvre de la sécurité des données dans les systèmes d'exploitation. Canaux cachés. Modèles de contrôle d'accès principaux, tels que: matrices de contrôle d'accès, contrôle d'accès discrétionnaire, contrôle d'accès obligatoire, contrôle d'accès basé sur les rôles, contrôle d'accès basé sur les attributs. Windows Active Directory et SE-Linux. Avantages et limitations de chaque modèle, autres modèles pertinents. Vérifications (audits). Ce cours comporte des séances obligatoires de travaux dirigés (TD).

CYB1143

Sécurité des réseaux mobiles

Objectifs : Au terme de ce cours, l'étudiant.e sera initié.e aux enjeux et défis de la cybersécurité dans les réseaux mobiles, sans fil, standards et de nouvelles générations, et sera en mesure de conseiller des usagers à l'emploi sécuritaire de ces réseaux.

Contenu : Rappel sur les réseaux sans fil et la mobilité. Vulnérabilités des réseaux sans fil (Wifi, WiMax, Bluetooth, etc.). Mise en place d'un réseau local sans fil avec infrastructure sécurisée. Mesures de sécurité, outils d'audit et méthodes d'évaluation des risques dans les réseaux locaux sans fil. Réseaux sans fil et leurs impacts sur les entreprises. Mécanismes de sécurités décentralisés. Sécurité du WIFI (gestion d'accès, authentification, WIDS/WIPS, etc.). Sécurité du Bluetooth. Éléments de sécurité des réseaux de capteurs sans-fil avec les normes Zwave et ZigBee. Sécurité des appareils mobiles et des applications téléchargées. Utilisation sécuritaire des appareils mobiles dans des scénario d'entreprises. Introduction à la sécurité des réseaux mobiles 5G.

CYB1153

Virtualisation des réseaux et cybersécurité

Objectifs : À la fin de ce cours, l'étudiant.e comprendra les principes et techniques de virtualisation, leur application en infonuagique, connaîtra les défis de cybersécurité que pose la virtualisation et sera en mesure d'analyser un environnement virtuel en vue d'appliquer des solutions de cybersécurité existantes.

Contenu : Rappel sur la structure interne et fonctionnement des ordinateurs. Abstraction du matériel (commutation de contexte, synchronisation, manipulation des interruptions, manipulation de l'horloge système, gestion mémoire, etc.) et architectures des Hyperviseurs (Type 1, Type 2, etc.). Systèmes d'exploitation et logiciels portables. Principes généraux de la virtualisation (partitionnement, isolation et conteneurs et/ou partage des ressources physiques et/ou logicielles, images manipulables). Virtualisation des fonctions réseau (NFV). Commutation et routage définis par logiciel. Création des réseaux virtuels composés de machines virtuelles. Centre de données défini par logiciel. Exigences de monitoring et de gestion de la sécurité NFV, synergie entre SDN et NFV. Quelques outils de virtualisations (VmWare vSphere, Microsoft Hyper V, KVM, Virtual Box, QEMU). Virtualisation et modèles de services (IaaS, PaaS, SaaS) et de déploiement (publique, privé, hybride, multi-cloud) infonuagiques. Vulnérabilités et attaques des hyperviseurs et de l'infonuagique. Introduction aux solutions de cybersécurité des réseaux virtuels (protection des hyperviseurs, protection des conteneurs, des fonctions réseau définis par logiciel). Ce cours comporte des séances de TP.

INF1343

Administration des réseaux

Objectifs : Initier l'étudiant aux principes et méthodologies de l'administration des réseaux informatiques. Lui présenter les outils de gestion de réseau en le sensibilisant aux aspects d'organisation, de performance et de sécurité.

Contenu : Responsabilités d'un administrateur réseau. Comparaison entre divers systèmes d'exploitation réseau. Installation d'un réseau local et interconnexion des réseaux. Mise en place des applications. Allocation, partage et gestion de ressources. Gestion de la performance. Gestion de la sécurité. Configuration de serveurs. Configuration des postes de travail. Aspects légaux. Ce cours comporte des séances obligatoires de travaux dirigés (TD) de deux heures par semaine.

INF1653

Introduction à la programmation et aux scripts

Objectifs : Au terme de ce cours, l'étudiant.e sera initié.e à la programmation structurée et sera en mesure de créer des scripts pour automatiser des tâches informatiques.

Contenu : Survol des paradigmes de programmation. Introduction à la résolution de problèmes avec Python. Éléments de programmation procédurale : instructions, expressions, types de données, flux de contrôle (conditionnels, boucles de répétitions). Survol des concepts de bases des langages de script. Automatisation des tâches utilisant des commandes scripts. Bonnes pratiques de programmation.

INF4523

Réseaux d'ordinateurs

Objectifs : Au terme de cette activité, l'étudiant(e) sera en mesure : de mettre en pratique les concepts et caractéristiques généraux des réseaux locaux.

Contenu : Présentation des modèles et standards d'architecture de réseaux (TCP/IP et OSI). Techniques de transmission des données : (codage et transmission, synchronisation et multiplexage). Éléments des réseaux locaux (LAN) et réseaux étendus (WAN). Simulateurs de réseaux. Technologies de réseaux : réseaux sans fil et réseaux mobiles, ATM, VPN et VoIP. Sécurité dans les réseaux, les protocoles sécuritaires. Ce cours comporte des séances obligatoires de travaux pratiques (TP) de trois heures par semaine.

INN1003

Projet intégrateur en innovation numérique

Objectifs : À la fin de cette activité, la personne étudiante sera en mesure de : s'initier à l'ensemble des étapes de planification et de réalisation d'un projet professionnel, d'intégrer les connaissances acquises sur un sujet interdisciplinaire, de mettre en lumière une problématique rattachée à ce sujet et de mettre en pratique les notions théoriques vues en classe par l'entremise d'un projet intégrateur spécifique à l'innovation numérique.

Contenu : Ce cours permet à l'étudiant(e) une immersion dans la réalisation d'un projet intégrateur d'envergure. La personne étudiante doit démontrer un grand niveau d'autonomie, de savoir-faire technique et de professionnalisme lors de la réalisation du mandat. La personne étudiante y approfondira notamment son porte-folio professionnel en développant des partenariats avec les acteurs du milieu. Ce projet intégrateur permettra d'assurer un ancrage de la formation dans la pratique. Les personnes étudiantes pourront s'impliquer dans différentes initiatives telles que l'organisation d'évènements, le développement de projets, la création d'une entreprise innovante, la réalisation d'une étude de cas, etc.