

Diplôme d'études supérieures spécialisées en cybersécurité - 1454

CRÉDITS :

30 crédits, Deuxième cycle

DIPLÔME :

Diplôme d'études supérieures spécialisées en cybersécurité

OBJECTIFS :

Objectif général

- Développer des compétences avancées en cybersécurité.

Objectifs spécifiques

- Développer une compréhension approfondie des concepts clés en cybersécurité;
- Comprendre les enjeux, les risques et les menaces en cybersécurité;
- Détecter les vulnérabilités des systèmes informatiques;
- Évaluer les besoins essentiels en cybersécurité d'une organisation;
- Acquérir des compétences opérationnelles avancées et des stratégies de sécurité pour se défendre contre les attaques et gérer les risques;
- Concevoir, développer et déployer une architecture de cybersécurité;
- Savoir sécuriser les données, les communications et les dispositifs informatiques;
- Connaître les enjeux techniques, juridiques, politiques, et éthiques liés à la cybersécurité.

INFORMATION SUR L'ADMISSION :

Lieu d'enseignement	Régime	Trimestres d'admission			Étudiants étrangers		
		Aut.	Hiv.	Été	Aut.	Hiv.	Été
Campus de Rimouski	TC	Démarrage par cohorte					
	TP	Démarrage par cohorte					
Campus de Lévis	TC	Démarrage par cohorte					
	TP	Démarrage par cohorte					

TC : Temps complet

TP : Temps partiel

CONDITIONS D'ADMISSION :

Base études universitaires au Québec

La candidate ou le candidat doit être titulaire d'un baccalauréat, ou l'équivalent, en informatique, en informatique de gestion ou en génie informatique, obtenu avec une moyenne cumulative d'au moins 3 sur 4,3 ou l'équivalent.

Compétences linguistiques en français :

La candidate ou le candidat qui ne peut faire la preuve de ses compétences linguistiques en français selon les critères de la "Politique relative à la maîtrise du français" devra transmettre une attestation de réussite à un test de français accepté par l'Université et répondant au seuil de réussite exigé pour que sa demande d'admission puisse être analysée. Si la demande d'admission est validée, il devra alors se soumettre à un examen institutionnel de français lors de son arrivée à l'UQAR, après avoir reçu une convocation à cet effet. En cas d'échec à l'examen, la réussite d'un cours de français sera exigée et l'inscription à ce cours est obligatoire dès le trimestre d'admission.

Base expérience

Posséder les connaissances requises, une formation appropriée et une expérience jugée pertinente.

Les méthodes et les critères de sélection consistent à l'évaluation du dossier scolaire et des lettres de recommandation. Les candidates et les candidats qui présentent une demande sur la base de l'expérience pertinente seront convoqués à une entrevue. Avant d'être admis au programme, la candidate ou le candidat peut être appelé à parfaire sa formation par une propédeutique ou par des cours d'appoint.

Compétences linguistiques en français :

La candidate ou le candidat qui ne peut faire la preuve de ses compétences linguistiques en français selon les critères de la "Politique relative à la maîtrise du français" devra transmettre une attestation de réussite à un test de français accepté par l'Université et répondant au seuil de réussite exigé pour que sa demande d'admission puisse être analysée. Si la demande d'admission est validée, il devra alors se soumettre à un examen institutionnel de français lors de son arrivée à

l'UQAR, après avoir reçu une convocation à cet effet. En cas d'échec à l'examen, la réussite d'un cours de français sera exigée et l'inscription à ce cours est obligatoire dès le trimestre d'admission.

PLAN DE FORMATION :

Bloc 1

Deux (2) cours obligatoires :

INF74022	Introduction à la cybersécurité (3 cr.)
INF74122	Aspects légaux, éthiques et vie privée en cybersécurité (3 cr.)

Cours optionnels

Six (6) cours parmi les blocs 2 et 3.

Bloc 2 Cours de spécialité

Cinq (5) ou six (6) cours parmi les suivants (18 cr.)

INF74222	Contrôle d'accès (3 cr.)
INF74322	Cryptographie (3 cr.)
INF74422	Cryptanalyse (3 cr.)
INF74522	Cybersécurité en Internet des Objets (3 cr.)
INF74622	Détection d'intrusions (3 cr.)
INF74722	Développement, sécurité et opérations - DevSecOps (3 cr.)
INF74822	Gouvernance de la cybersécurité (3 cr.)
INF74922	Investigation numérique (3 cr.)
INF75022	Sécurité des systèmes informatiques et des réseaux des infrastructures critiques et leur résilience (3 cr.)
INF75122	Contrats intelligents, cryptomonnaies et chaînes de blocs (« blockchain ») (3 cr.)
INF75222	Sujets spéciaux en cybersécurité (3 cr.)

Bloc 3 Cours d'enrichissement

Zéro (0) ou un (1) cours d'enrichissement pourra être suivi dans un autre programme de deuxième cycle de l'UQAR, sur approbation de la direction du programme.

Bloc 4 Activité finale

Une activité (6 cr.) parmi les suivantes:

INF79222	Stage (6 cr.)
INF79322	Projet (6 cr.)

Programme approuvé par la Commission des études du 4 octobre 2022 (CE-584-7553)

INF74022**Introduction à la cybersécurité**

Objectif : Développer une compréhension approfondie des technologies et méthodes modernes de protection des informations et des systèmes informatiques.

Contenu : Historique et standards de cybersécurité. Cybermenaces. Besoins essentiels en cybersécurité : identification, authentification, confidentialité, autorisation, intégrité, non répudiation. Fondamentaux de la sécurité réseau. Sécurisation des informations et dispositifs personnels. Menaces, vulnérabilités et risques de cybersécurité. Politiques de cybersécurité.

INF74122**Aspects légaux, éthiques et vie privée en cybersécurité**

Objectif : S'initier aux principaux enjeux légaux et éthiques de la cybersécurité.

Contenu : Potentiels défis et enjeux légaux et éthiques de la cybersécurité. Meilleures pratiques éthiques en cybersécurité. Cybersécurité et vie privée. Lois sur la protection des données. Propriété intellectuelle. Cadres légaux pour la protection de données (entre autres : PIPEDA, GDPR, U.S. Privacy Act).

INF74222**Contrôle d'accès**

Objectif : Appliquer les principaux concepts, modèles et politiques du contrôle d'accès.

Contenu : Concepts essentiels en contrôle d'accès. Modèles de contrôle d'accès (entre autres : DAC, MAC, RBAC, ABAC). Médamodèles de contrôle d'accès. Développement de politiques de contrôle d'accès. Principes et fonctionnement d'une machine à politiques de contrôle d'accès et mise en application du contrôle d'accès. Applications du contrôle d'accès : bases de données, systèmes informatiques, applications web, l'infonuagique, Internet des Objets. Cadres et standards de contrôle d'accès (entre autres : XACML, NGAC).

INF74322**Cryptographie**

Objectif : Comprendre le fonctionnement des principaux protocoles et algorithmes cryptographiques et leurs applications.

Contenu : Historique : notions élémentaires de la théorie des nombres et de la théorie de la complexité; cryptologie symétrique et asymétrique; signature électronique, fonctions de hachage à sens unique; protocole d'échange de clés, échange de clés; exemples de librairie dans des langages C et Python; cryptologie quantique; cryptosystèmes à courbes elliptiques. Infrastructures de clés publiques (PKI). Cryptographie dans la technologie du Blockchain.

INF74422**Cryptanalyse**

Objectif : Développer une connaissance approfondie des attaques cryptographiques.

Contenu : Introduction à la cryptanalyse : principes de Kerckhoffs, attaques théoriques et pratiques, modèles d'attaques, cibles d'attaques. Cryptanalyse des chiffrements par blocs, par flux, par hachage. Algorithmes de factorisation. Cryptanalyse algébrique. Cryptanalyse basée sur l'apprentissage automatique. Algorithmes quantiques.

INF74522**Cybersécurité en Internet des Objets**

Objectif : Explorer les concepts, les préoccupations, les politiques, et les pratiques liées à la cybersécurité dans l'Internet des objets.

Contenu : Politiques et pratiques de sécurité de l'Internet des Objets (IoT). Évaluation de la sécurité des systèmes de l'Internet des Objets et détection des vulnérabilités. Architectures des systèmes IoT. Développement et prototypage IoT avec entre autres : Raspberry Pi et Arduino. Utilisation des outils de test de pénétration et de vulnérabilité dans le monde réel tels que Kali Linux. Sécuriser les dispositifs IoT. Mesures d'atténuation de menaces et réduction des risques dans les solutions IoT.

INF74622**Détection d'intrusions**

Objectif : Explorer les concepts fondamentaux des systèmes de détection d'intrusion (IDS).

Contenu : Rôle des IDS dans une stratégie de sécurité globale. Prévention d'intrusions. Détection d'intrusions avec outils : Snort, Types d'IDS (basée sur des règles, le comportement et les modèles d'attaques, basés réseaux et hôte, etc). Inspection de trafic réseau. Méthodes d'évasion de la détection des IDS et contre-mesures. Apprentissage automatique pour la détection d'intrusions. Architectures de systèmes IDS. Installation et configuration d'IDS.

INF74722**Développement, sécurité et opérations - DevSecOps**

Objectif : Apprendre à intégrer et à surveiller la sécurité dans les applications et les conteneurs.

Contenu : Introduction des concepts de base pour l'intégration et l'automatisation de la sécurité dans un pipeline DevOps. Approches DevSecOps. Identification et résolution de vulnérabilités dans les dépendances, Dockerfile, images, ressources K8S. Intégration/déplacement la sécurité vers la gauche dans le pipeline DevOps. Test de sécurité des applications statiques et dynamiques. DevSecOps et les services de sécurité AWS, CI/CD sécurisés.

INF74822**Gouvernance de la cybersécurité**

Objectif : Sensibiliser aux enjeux et aux bonnes pratiques de la gouvernance de la cybersécurité.

Contenu : Importance de la gouvernance de la cybersécurité. Principaux objectifs de la gouvernance de la cybersécurité. Cadre de gouvernance de la cybersécurité. Évaluation de maturité. Modèle RASCI pour définir les rôles et responsabilités. Cadre de contrôle pour la cybersécurité. Défis de la gouvernance de cybersécurité.

INF74922**Investigation numérique**

Objectif : Initier aux outils techniques, et aux méthodologies utilisées dans le domaine de l'investigation numérique.

Contenu : Cybercriminalité et investigation numérique. Types d'évidences digitales. Identification, récupération, analyse, évaluation et évaluation d'éléments de preuves digitaux. Identification des faiblesses dans les preuves digitales; processus en cause pour leur obtention. Assurance de l'intégrité des preuves. Types d'investigations : investigations des dispositifs intelligents, web et réseaux sociaux. Rapport d'enquête. Aspects juridiques.

INF75022**Sécurité des systèmes informatiques et des réseaux des infrastructures critiques et leur résilience**

Objectif : Développer des connaissances de base des infrastructures critiques en général et des infrastructures d'information critiques en particulier.

Contenu : Infrastructures critiques. Acteurs et agents de menace pour les infrastructures critiques. Systèmes cyberphysiques et leur sécurité. Sécurité des systèmes de contrôle. Cadre NIST pour la cybersécurité des infrastructures. Types de résiliences organisationnelles : opérationnelle, informationnelle, chaîne d'approvisionnement. Stratégies, méthodologies et cadres de cybersécurité protégeant les actifs numériques des organisations et assurant leur résilience. Prévention de et reprise après incidents et sinistres numériques. Cybersécurité pour réseaux électriques, réseau de la santé, et systèmes de communication. Sensibilisation à la résilience numérique pour une continuité et reprise après un incident de cybersécurité.

INF75122**Contrats intelligents, cryptomonnaies et chaînes de blocs (« blockchain »)**

Objectif : Introduire la chaîne de blocs, les contrats intelligents, les cryptomonnaies et leur sécurité.

Contenu : Chaîne de blocs, contrats intelligents et cryptomonnaies. Aperçu historique de l'évolution de la chaîne de blocs. Types de consensus, de minage et génération/distribution de jetons. Aspects pratiques et intégration de la chaîne de blocs et des contrats intelligents dans les affaires.

Vulnérabilités et défis en cybersécurité de la chaîne de blocs et des contrats intelligents (entre autres : contrats, nœuds, clés). Outils pour le déploiement, l'audit et l'utilisation des actifs de la chaîne de blocs et les contrats intelligents. Implications juridiques et réglementaires de l'utilisation de la chaîne de blocs, des contrats intelligents et des cryptomonnaies.

INF75222**Sujets spéciaux en cybersécurité**

Objectif : Favoriser l'accès à divers domaines spécialisés ou nouveaux en cybersécurité.

Contenu : Le contenu est variable selon les besoins des étudiantes et des étudiants, de l'expertise professorale disponible et du domaine de spécialisation couvert.

INF79222**Stage (15 crédits du programme doivent être réussis)**

Objectif : Se familiariser avec des problèmes concrets en cybersécurité dans un milieu professionnel.

Contenu : Stage en cybersécurité à temps plein dans un milieu professionnel d'une durée de 4 à 6 mois répartis sur un ou deux trimestres, équivalent à 525 heures de travail. Complément pratique à la formation des étudiantes et des étudiants. Contenu précis déterminé en fonction des milieux professionnels.

INF79322**Projet (15 crédits du programme doivent être réussis)**

Objectif : Intégrer les connaissances théoriques et pratiques acquises dans la réalisation d'un projet en cybersécurité.

Contenu : Projet en cybersécurité à temps plein à l'université d'une durée de 4 à 6 mois répartis sur un ou deux trimestres, équivalent à 525 heures de travail. Complément pratique à la formation des étudiantes et des étudiants. Résolution de problème en cybersécurité. Analyse des différents aspects techniques et économiques du problème soumis. Évaluation des différentes solutions et justification de celle retenue. Conception et implantation de la solution choisie. Contenu précis déterminé en fonction du projet proposé.