Université de Sherbrooke

FACULTÉ DES SCIENCES

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Les sections *Présentation*, *Structure du programme* et *Admission et exigences* (à l'exception de la rubrique intitulée « Document(s) requis pour l'admission ») constituent la version officielle de ce programme. La dernière mise à jour a été faite le 18 juin 2026. L'Université se réserve le droit de modifier ses programmes sans préavis.

PRÉSENTATION

Sommaire*

*IMPORTANT : Certains de ces renseignements peuvent varier selon les cheminements ou concentrations. Consultez les sections *Structure du programme* et *Admission et exigences* pour connaitre les spécificités d'admission par cheminements, trimestres d'admission, régimes ou lieux offerts.

CYCLE
2e cycle

RÉGIME DES ÉTUDES
Régulier

CRÉDITS
30 crédits

RÉGIMES D'INSCRIPTION
Temps complet, Temps partiel

TRIMESTRES D'ADMISSION
Automne, Hiver

LIEU
Formation à distance - Campus Longueuil

Renseignements

- 1 888 463-1835 poste 61715
- 450 463-1835 poste 61715
- ti@usherbrooke.ca
- Site Internet

Objectif(s) général(aux)

Permettre à l'étudiante ou à l'étudiant :

- de maîtriser les tenants et aboutissants de la sécurité informatique contemporaine;
- de maîtriser la nature des surfaces d'attaque exposées par une infrastructure de TI;
- de savoir concevoir, mettre en œuvre et documenter une stratégie efficace pour protéger et défendre ces surfaces d'attaque, en tenant compte d'un budget de ressources donné;
- de pouvoir critiquer une telle stratégie telle que mise en place dans une organisation, de manière à en corriger les faiblesses;
- de maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure;

- de savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale;
- de savoir dresser et exécuter un plan d'intervention en cas d'incident et de brèche de données, de manière à trouver le meilleur compromis entre la minimisation des dommages et l'interruption des activités de l'organisation.

STRUCTURE DU PROGRAMME

Activités pédagogiques obligatoires - 24 crédits

Code de l'activité pédagogique	Titre de l'activité pédagogique et nombre de crédits
INF801	Concepts de base de la sécurité en TI - 3 crédits
INF802	Planification et prévention en sécurité des TI - 3 crédits
INF803	Sécurité des systèmes - 3 crédits
INF805	Introduction aux attaques informatiques - 3 crédits
INF807	Criminalistique en sécurité des TI - 3 crédits
INF808	Réaction aux attaques et analyses des attaques - 3 crédits
INF810	Projet en sécurité 1 - 3 crédits
INF811	Projet en sécurité 2 - 3 crédits

Activités pédagogiques à option - 6 crédits

Deux activités pédagogiques choisies parmi les suivantes :

Code de l'activité pédagogique	Titre de l'activité pédagogique et nombre de crédits
INF804	Sécurité des logiciels - 3 crédits
INF806	Système et réseau - 3 crédits
INF809	Architecture de sécurité - 3 crédits
INF815	Veille en technologie, fraude et cybersécurité - 3 crédits

ADMISSION ET EXIGENCES

LIEU(X) DE FORMATION ET TRIMESTRE(S) D'ADMISSION

Formation à distance : admission aux trimestres d’automne et d'hiver

Condition(s) générale(s)

Condition générale d’admission aux programmes de 2e cycle de l’Université (cf. *Règlement des études*)

Condition(s) particulière(s)

Détenir un grade de 1er cycle comportant au moins trois années d'études ou l’équivalent en informatique, en informatique de gestion, en génie informatique ou en génie logiciel, ou tout autre diplôme jugé équivalent.

Avoir obtenu une moyenne cumulative d'au moins 2,7 dans un système où la note maximale est de 4,3 (ou environ 12 sur 20 dans les matières en sciences) ou avoir obtenu des résultats scolaires jugés équivalents.

Avoir au moins deux ans d’expérience professionnelle jugée pertinente en technologies de l’information et en sécurité informatique, et incluant, au plus, une année de stage.

Critère(s) de sélection

La sélection des candidates et candidats se fait sur la base d'une liste d'excellence. Pour établir cette liste, la qualité du dossier scolaire, l’expérience professionnelle et les résultats de l'entrevue d'admission sont pris en considération.

La Faculté peut néanmoins admettre une candidate ou un candidat ne satisfaisant pas aux conditions particulières d'admission. Dans un tel cas, la Faculté peut, conformément au *Règlement des études*, imposer à l'étudiante ou à l'étudiant des activités pédagogiques d'appoint.

Document(s) requis pour l’admission

Se présenter à une entrevue d’admission.

RÉGIME(S) DES ÉTUDES ET D'INSCRIPTION

Régime régulier à temps complet ou à temps partiel

INDEX DES ACTIVITÉS PÉDAGOGIQUES

INF801 - Concepts de base de la sécurité en TI

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Comprendre les fondements de la sécurité informatique, dont la cryptologie, la cybersécurité et l'authentification. Comprendre et maîtriser les technologies de la sécurité.

Contenu

La sécurité en TI aujourd'hui; sécurisation de la base avant les attaques trop avancées; analyse et gestion de la sécurité et du risque; authentification. Sécurité dans le développement logiciel, sensibilisation à l'hameçonnage et à l'ingénierie sociale téléphonique; notions de système d'exploitation et de réseau; les vulnérabilités et les menaces communes, les attaques communes, les bonnes pratiques de base pour l'authentification, la segmentation réseau; introduction à la cryptographie; sécurité des mobiles; sécurité dans l'approche « prenez vos appareils personnels » (PAP) (*bring your own device*); sécurité des systèmes opérationnels (OT); sécurité des systèmes de contrôle industriels (ICS); modélisation de menaces.

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Microprogramme de 2e cycle en sécurité informatique - volet prévention

INF802 - Planification et prévention en sécurité des TI

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Comprendre et mettre en place un processus de gestion des incidents. Gérer des vulnérabilités et appliquer une approche proactive contre les cyberattaques. Établir des métriques d'évaluation de la sécurité.

Contenu

Introduction au concept d'incident/réaction, à la communication et à l'importance d'avoir un plan préétabli; gestion des incidents (plan d'action et de communication); gestion des mises à jour : pourquoi, comment, outils; détection et journaux : comment mettre en place une solution efficace, mais aussi comprendre les outils, leur détection par signatures et comportement réseau ou hôte; suivi et trace d'une intrusion; gestion de risques : niveaux de service, rapports et métriques pour l'évaluation d'une stratégie de gestion des incidents. Prévention de l'hameçonnage; logiciel d'extorsion ou rançongiciel (*ransomware*); intervention d'une équipe de sécurité (développeurs et administrateurs de système); prévention, réaction et introduction de mesure de désescalades postincident (incident/réaction); intervention dans un environnement mobile.

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en génie logiciel

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Diplôme d'études supérieures spécialisées de 2e cycle en technologies de l'information

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet prévention

INF803 - Sécurité des systèmes

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Connaître et maîtriser les principaux systèmes d'exploitation disponibles sur le marché. Savoir renforcer la sécurité de ces systèmes. Comprendre les enjeux de sécurité entourant la virtualisation et les systèmes mobiles.

Contenu

Sécurisation des réseaux. Sécurisation des systèmes d'exploitation. Sécurisation du Web et du nuage. Cryptographie. Sécurité des systèmes mobiles.

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet prévention

INF804 - Sécurité des logiciels

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Comprendre le cycle de vie de développement sécuritaire. Comprendre la sécurité applicative et les concepts de base qui s'y rapportent.

Contenu

Programmation sécuritaire. Les tests de pénétration. Le contrôle des accès. La sécurité sur mobile : analyses d'applications iOS et Android.

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en génie logiciel

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet prévention

Microprogramme de 2e cycle en sécurité informatique - volet réaction

INF805 - Introduction aux attaques informatiques

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Comprendre les étapes d'une cyberattaque. Faire la recherche d'informations sur une cible d'attaque. Différencier les types d'attaques. Utiliser des trousses et outils de piratage de façon éthique. Connaitre les techniques pour détecter des cyberattaques.

Contenu

Analyse d'attaque; montage et préparation des attaques. Les vulnérabilités et leur exploitation; vulnérabilités logicielles, exploitation et construction de maliciel. Introduction et test d'intrusion; OWASP + Guide de tests d'intrusion (*pentest*) OWASP : atelier ou projet de tests d'intrusion Web; tests d'intrusion serveur : exploit, pivot, « metasploit » et Armitage. Analyse des attaques d'hameçonnage : trace réseau, analyse des postes, détection de l'attaquant. Tests d'intrusion (*pentest*) comme méthode d'attaque. Détection de cyberattaques : par extraction des fichiers, par signatures, par anomalies, par analyse de journaux, analyse de flux.

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Diplôme d'études supérieures spécialisées de 2e cycle en technologies de l'information

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet réaction

INF806 - Système et réseau

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Connaitre les caractéristiques de l'architecture des composantes des réseaux informatiques dans un contexte de sécurité. Comprendre les principes d'architecture réseau et de sécurité.

Contenu

Réseau : postes de travail, serveurs, applications Web, SGDBD, routeurs, commutateurs, point d'accès sans fil, pare-feu, serveur mandataire (Proxy), antivirus, courriels, filtrage de contenu, authentification, surveillance réseau. Détection de logiciels malveillants. Services de base en réseautique, virtualisation. Principes d'architecture réseau et de sécurité : OSI, TCP/IP, zonage ou segmentation réseau, flots de trafic, sécurité interzone; attaque réseau, *honeytoken*, détection des pivots. Système : bac à sable (*sandbox*), *cuckoosandbox*, principes de base. Analyse des cas de type C&C irc, twitter, zeus. Cryptologie.

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet prévention

Microprogramme de 2e cycle en sécurité informatique - volet réaction

INF807 - Criminalistique en sécurité des TI

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Comprendre les différentes étapes d'une enquête de piratage. Faire l'analyse de mémoire vive. Utiliser des outils de diagnostic pour repérer du code malveillant.

Contenu

Principes de base de la criminalistique. Introduction aux outils de criminalistique en cours d'opération *(forensic live)*, mémoire et statique des disques durs. Ingénierie inverse.

---

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Diplôme d'études supérieures spécialisées de 2e cycle en technologies de l'information

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet réaction

---

INF808 - Réaction aux attaques et analyses des attaques

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Apprendre à caractériser différents types de cyberattaques. Apprendre la gestion d'incidents suite à une attaque.

Contenu

Analyse d'attaque. Gestion des incidents. Analyse des attaques d'hameçonnage; trace réseau; analyse des postes; comment détecter l'attaquant. Outils et techniques d'analyse de journaux. Journalisation des serveurs Web; détection d'indices généraux d'activités suspectes. Balayages de vulnérabilités. Attaques de contournement. Attaques de sessions. Attaques par injection. Attaque de déni de service. Analyses d'attaque de serveurs Web. Désescalade postincident.

Préalable(s)

INF805

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet réaction

---

INF809 - Architecture de sécurité

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Comprendre les modèles (référence) d'architecture. Appliquer les standards d'architecture dans un contexte d'entreprise. Formuler une architecture pour les besoins de sécurité d'une entreprise. Faire l'analyse et l'évaluation d'un document d'architecture de sécurité (AS).

Contenu

Contexte : besoins, marché et tendances, définitions. Modèle de sécurité : place de l'AS dans l'architecture d'affaires, applicative, matérielle et de données. Principes d'architecture (se traduisent comment dans la pratique) : *zero-trust*, modèle d'accès, isolation, DICAI. Modèle de référence : standard TOGAF et Archimate, des objets réutilisables. Niveaux d'architecture : AS au niveau affaires, AS au niveau applicatif, AS au niveau technologique, AS au niveau des données. Vues : mise en pratique; outils. Projet (tel que Archimatetool).

---

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en génie logiciel

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Doctorat en informatique

Maîtrise en génie logiciel

Maîtrise en informatique

Microprogramme de 2e cycle en sécurité informatique - volet prévention

Microprogramme de 2e cycle en sécurité informatique - volet réaction

---

INF810 - Projet en sécurité 1

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Intégrer les connaissances du domaine de la prévention en sécurité informatique par l'élaboration d'un projet relié à la sécurité en TI. Démontrer ses habiletés à faire une évaluation de la posture de sécurité d'un environnement IT et OT à l'aide d'outils de test de pénétration (analyse dynamique) et

d'analyse statique (revue architecture selon un standard).

Contenu

Élaboration d'un projet qui devra porter sur les tests d'intrusion (pentest) ou l'analyse d'un iot/scada. Le contenu exact du projet sera déterminé à chaque trimestre en collaboration avec l'équipe enseignante responsable de l'activité.

---

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Microprogramme de 2e cycle en sécurité informatique - volet prévention

---

INF811 - Projet en sécurité 2

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

Cible(s) de formation

Intégrer les connaissances en sécurité informatique par l'élaboration d'une architecture de sécurité ou par l'analyse d'un problème de sécurité.

Contenu

Élaboration d'un projet qui devra porter sur un sujet au choix en sécurité informatique. Le sujet exact sera déterminé à chaque trimestre en collaboration avec l'équipe enseignante responsable de l'activité.

---

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Microprogramme de 2e cycle en sécurité informatique - volet réaction

---

INF815 - Veille en technologie, fraude et cybersécurité

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ OU CENTRE

Faculté des sciences

RÉPARTITION DE LA CHARGE DE TRAVAIL

3-0-6

Cible(s) de formation

Acquérir une vision de l'avenir technique du domaine des technologies en général et de celui de la cybersécurité en particulier par l'intermédiaire de conférences, d'ateliers et de classes de maître, portant sur des sujets à la fine pointe de l'actualité du domaine.

Contenu

Veille technologique; conférences techniques; ateliers; classes de maître.

---

* Sujet à changement

Programmes offrant cette activité pédagogique (cours)

Diplôme d'études supérieures spécialisées de 2e cycle en génie logiciel

Diplôme d'études supérieures spécialisées de 2e cycle en sécurité informatique

Diplôme d'études supérieures spécialisées de 2e cycle en technologies de l'information

Maîtrise en génie logiciel

Maîtrise en informatique