

FACULTÉ DES SCIENCES

Microprogramme de 2e cycle en sécurité informatique - volet réaction

Les sections *Présentation*, *Structure du programme* et *Admission et exigences* constituent la version officielle de ce programme. La dernière mise à jour a été faite le 7 mai 2019. 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 connaître les spécificités d'admission par cheminements, trimestres d'admission, régimes ou lieux offerts.

CYCLE

2e cycle

CRÉDITS

15 crédits

TRIMESTRE(S) D'ADMISSION

Automne

RÉGIME DES ÉTUDES

Régulier

RÉGIME D'INSCRIPTION

Temps partiel

LIEU

Formation à distance - Campus Longueuil

PARTICULARITÉ*

Ouvert aux étudiants internationaux en régime régulier

* Peut varier pour certains cheminements ou concentrations.

RENSEIGNEMENTS

450 463-1835 poste 61715
1 888 463-1835 poste 61715
[Site Internet](#)
ti@usherbrooke.ca

Objectif(s) général(aux)

Permettre à l'étudiante ou à l'étudiant de :

- maîtriser la nature, le rythme et les outils des cyberattaques contre divers types d'infrastructure;
- savoir détecter les signes et artefacts d'une intrusion, pouvoir mesurer son ampleur et pouvoir en déterminer la chaîne causale;
- 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

INF805	Introduction aux attaques informatiques - 3 crédits
INF807	Criminalistique en sécurité TI - 3 crédits
INF808	Réaction aux attaques et analyses des attaques - 3 crédits
INF811	Projet en sécurité 2 - 3 crédits

Activités pédagogiques à option - à 3 crédits

Une activité pédagogique choisie parmi les suivantes :

INF804	Sécurité des logiciels - 3 crédits
INF806	Système et réseau - 3 crédits
INF809	Architecture de sécurité - 3 crédits

ADMISSION ET EXIGENCES

Lieu(x) de formation et trimestre(s) d'admission

Formation à distance : admission au trimestre d'automne seulement

Condition(s) générale(s)

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

Condition(s) particulière(s)

Détenir un grade de 1^{er} cycle en informatique, en informatique de gestion, en génie informatique, 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 avoir obtenu des résultats scolaires jugés équivalents.

Exigence(s) d'admission

Se présenter à une entrevue d'admission.

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.

Régime(s) des études et d'inscription

Régime régulier à temps partiel

INDEX DES ACTIVITÉS PÉDAGOGIQUES

INF804 - Sécurité des logiciels

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ/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.

INF805 - Introduction aux attaques informatiques

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ/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 trousseaux et outils de piratage de façon éthique. Connaître les techniques pour détecter

Usherbrooke.ca/admission

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.

INF806 - Système et réseau

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ/CENTRE

Faculté des sciences

Cible(s) de formation

Connaître 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, *honeypot*,

détection des pivots. Système : bac à sable (*sandbox*), *cuckoosandbox*, principes de base. Analyse des cas de type C&C irc, twitter, zeus. Cryptologie.

INF807 - Criminalistique en sécurité TI

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ/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.

INF808 - Réaction aux attaques et analyses des attaques

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ/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.

INF809 - Architecture de sécurité

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ/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, DICA. 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).

INF811 - Projet en sécurité 2

Sommaire

CYCLE

2e cycle

CRÉDITS

3 crédits

FACULTÉ/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.