

## 1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

---

Titre officiel du cours :	<b>INF802 - Planification et prévention en sécurité TI</b>
Nombre de crédits :	3 crédits – 135 heures
Programme :	Microprogramme de 2e cycle en sécurité informatique - volet prévention
Cours préalables ou concomitants :	aucun
Lieu du cours :	Moodle / Adobe Connect (à distance)
Session :	Automne 2023
Date de début :	29 août 2023
Date de fin :	05 décembre 2023
Date limite d'ajout / retrait	15 septembre 2023
Date limite d'abandon :	15 novembre 2023
Rencontres synchrones :	<b>Mardis :</b> 29 août 2023 5-12-19-26 septembre 2023 3-10-17-24-31 octobre 2023 7-14-21-28 novembre 2023 5 décembre 2023
Personne(s)-ressource(s) :	Capt(ret) Steve Waterhouse, CD, CISSP
Courriel(s) :	<a href="mailto:Steve.Waterhouse@USherbrooke.ca">Steve.Waterhouse@USherbrooke.ca</a>

## 2. MISE EN CONTEXTE

---

### DESCRIPTION OFFICIELLE DU COURS

#### **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 des escalades post-incidents (incident/réaction). Intervention dans un environnement mobile, exploration des notions de vie privée et de la protection des renseignements personnels.

### PLACE DU COURS DANS LE PROGRAMME

Cette activité de formation s'inscrit dans le début du microprogramme. Son positionnement permet à l'étudiant d'acquérir les assises d'une gestion des incidents ainsi que l'identification de vulnérabilité en sécurité. L'activité permet de contextualiser les éléments théoriques dans une mise en application terrain de la sécurité TI.

### OBJECTIFS DU MICROPROGRAMME<sup>1</sup>

Le Microprogramme en sécurité informatique - volet prévention permet à l'étudiante ou à l'étudiant de :

- maîtriser les tenants et aboutissants de la sécurité informatique contemporaine;
- maîtriser la nature des surfaces d'attaque exposées par une infrastructure de TI;

---

<sup>1</sup> Extrait de la fiche signalétique



- 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;
- pouvoir critiquer une telle stratégie telle que mise en place dans une organisation, de manière à en corriger les faiblesses.

#### CHARGE DE TRAVAIL

Les trois crédits équivalent à 135 heures, soit 45 heures de rencontres collectives et 90 heures de travail personnel, réparties de la façon suivante : (distinguer le temps de lecture personnelle, le temps de travail sur le site, le temps de réalisation des travaux, etc.)

Enseignement magistral	45 heures
Conférence externe	10 heures
Lecture personnelle	40 heures
Activités de consolidation	40 heures
<b>TOTAL</b>	<b>135 heures</b>

### 3. DÉROULEMENT DU COURS

Module	Description	Enseignant
<p><b>Module 1 :</b> <b>Notions de processus et fonctions informatiques</b> <i>29 août 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Introduction au cours INF 802 et présentation enseignant / étudiants</li> <li>◆ Fondements de la cybersécurité</li> <li>◆ Pyramide de sécurité de l'information</li> <li>◆ Pyramide organisationnelle versus pyramide de la sécurité de l'information</li> <li>◆ Notions de processus</li> <li>◆ Quelques définitions conceptuelles</li> <li>◆ Survol à très haut niveau de COBIT 5</li> <li>◆ Survol à très haut niveau d'ITIL</li> <li>◆ Survol de la norme PCI-DSS v4</li> <li>◆ Facteurs clés de succès de l'implantation des référentiels, normes, etc.</li> <li>◆ Raisons de l'adoption de cadres référentiels, normes, etc.</li> <li>◆ Centre opérationnel de sécurité (SOC)</li> <li>◆ Système de billetterie</li> <li>◆ RFC</li> </ul>	<p>Steve Waterhouse</p>
<p><b>Module 2 :</b> <b>Processus de gestion d'incidents</b> <i>05 septembre 2023</i> <i>12 septembre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Définitions conceptuelles</li> <li>◆ Généralités et quelques statistiques</li> <li>◆ Processus de gestion d'incidents                             <ul style="list-style-type: none"> <li>◆ Cadre référentiel de gestion d'incidents selon le NIST-sp 800-61</li> <li>◆ Objectifs</li> <li>◆ Phase de préparation</li> <li>◆ Phase de détection et analyse</li> <li>◆ Phase de confinement, éradication et recouvrement</li> <li>◆ Phase de revue post-incident (désescalades)</li> <li>◆ Quelques indicateurs (métriques) d'incidents</li> <li>◆ Quelques bonnes pratiques (si possible)</li> <li>◆ Exemples de processus génériques de gestion d'incidents</li> <li>◆ Matrice RACI</li> <li>◆ Quelques lectures suggérées</li> </ul> </li> <li>◆ <b>Travail Pratique#1 – Gestion d'incidents</b></li> </ul>	<p>Steve Waterhouse</p>

<p><b>Module 3 :</b> <b>Mesures de performances et notions de vie privée</b> <i>19 septembre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Définitions conceptuelles</li> <li>◆ Généralités sur les mesures de performance <ul style="list-style-type: none"> <li>◆ Enjeux</li> <li>◆ Raisons d'utilisation des tableaux de bord</li> <li>◆ Tableau de bord</li> <li>◆ Étapes de réalisation d'un tableau de bord</li> <li>◆ Cascades d'objectifs COBIT 5</li> <li>◆ Objectifs facilitants COBIT 5</li> <li>◆ Quelques métriques de gestion d'incidents selon COBIT 5</li> <li>◆ Quelques métriques d'incidents selon le NIST-sp-800-61</li> </ul> </li> <li>◆ Notion de vie privée <ul style="list-style-type: none"> <li>◆ Respect de la vie privée</li> <li>◆ Dimensions du respect de la vie privée</li> <li>◆ Encadrement vie privée et protection des renseignements personnels (PRP): USA, ONU, Union Européenne, Canada, et Québec</li> <li>◆ Atteinte à la vie privée et quelques conséquences rattachées au non-respect de la PRP</li> <li>◆ Quelques contrôles pouvant aider à réduire les risques d'atteinte à la vie privée</li> </ul> </li> </ul>	<p>Steve Waterhouse</p>
<p><b>Module 4 : notions d'incident majeur et de gestion de crise</b> <i>26 septembre 2023</i> <i>03 octobre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Contexte</li> <li>◆ Définitions conceptuelles <ul style="list-style-type: none"> <li>◆ Anomalie</li> <li>◆ Incident de sécurité mineur</li> <li>◆ Incident de sécurité important</li> <li>◆ Incident de sécurité critique</li> </ul> </li> <li>◆ Notions d'incident majeur <ul style="list-style-type: none"> <li>◆ Délimitation d'incident majeur dans le cadre du module</li> <li>◆ Quelques incidents majeurs : <ul style="list-style-type: none"> <li>◆ Verglas (1998)</li> <li>◆ Y2K (1999)</li> <li>◆ Wannacry / NotPetya (2017)</li> <li>◆ ARC / Equifax (2017)</li> <li>◆ Marriott (2018-2020)</li> <li>◆ Desjardins (2019)</li> <li>◆ Capital One (2019)</li> </ul> </li> </ul> </li> </ul>	<p>Steve Waterhouse</p>

	<ul style="list-style-type: none"> <li>◆ COVID-19 (2020)</li> <li>◆ Gestion de crise <ul style="list-style-type: none"> <li>◆ Généralités</li> <li>◆ Quelques contrôles de gestion d'incident majeur</li> <li>◆ Grandes lignes de gestion de crise selon le NIST-sp 800-61</li> <li>◆ Quelques constantes dans la gestion de crise <ul style="list-style-type: none"> <li>◆ Se préparer avant la crise</li> <li>◆ Durant la crise</li> <li>◆ Réponse à la crise</li> <li>◆ Post-mortem</li> <li>◆ Stratégies de communication</li> </ul> </li> <li>◆ Exemple de communication de crise</li> </ul> </li> </ul>	
<p><b>Module 5 – Savoir évaluer et reconnaître les menaces</b> <i>10 octobre 2023 17 octobre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Définitions</li> <li>◆ Menaces et autres</li> <li>◆ Anticipation de protection envers la menace</li> <li>◆ Menaces et exploits</li> <li>◆ Les acteurs et leurs menaces</li> <li>◆ Attribution – À qui la faute ?</li> </ul> <p><b>Travail pratique #2 – Savoir évaluer et reconnaître les menaces</b></p>	Steve Waterhouse
<p><b>Module 6 : Les centres d'opération de sécurité</b> <i>24 octobre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Définitions</li> <li>◆ Menaces et autres</li> <li>◆ Anticipation de protection envers la menace</li> <li>◆ Menaces et Exploits</li> <li>◆ Les acteurs et leurs menaces</li> <li>◆ Attribution – À qui la faute ?</li> </ul>	Steve Waterhouse
<p><b>Module 7 - Processus de gestion des vulnérabilités</b> <i>31 octobre 2023 07 novembre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Gestion des risques</li> <li>◆ Évaluation des menaces et des risques (ÉMR)</li> <li>◆ Définitions relatives à la gestion des vulnérabilités</li> <li>◆ Élaboration d'une méthodologie d'évaluation des vulnérabilités</li> <li>◆ Outils de référence avec lesquels à travailler</li> </ul> <p>◆ <b>Travail pratique#3 – Gestion des vulnérabilités</b></p>	Steve Waterhouse

<p><b>Module 8 - Processus de gestion des mises à jour</b> <i>14 novembre 2023 21 novembre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Définition de l'importance du processus des mises à jour</li> <li>◆ Mises à jour PME</li> <li>◆ Mises à jour GE</li> <li>◆ Les exceptions (IoT, ICS/SCADA)</li> <li>◆ Élaboration d'une méthodologie d'évaluation des mises à jour</li> <li>◆ Problèmes anticipés</li> <li>◆ Outils</li> </ul> <p>◆ <b>Travail pratique#4 – Gestion des mises à jour</b></p>	<p>Steve Waterhouse</p>
<p><b>Module 9 - Prévention de l'hameçonnage</b> <i>28 novembre 2023 05 décembre 2023</i></p>	<ul style="list-style-type: none"> <li>◆ Définition de ce qu'est l'hameçonnage</li> <li>◆ Faits vécus</li> <li>◆ Prévention de l'hameçonnage</li> <li>◆ Logiciel d'extorsion ou rançongiciel (ransomware)</li> <li>◆ Intervention d'une équipe de sécurité (développeurs et administrateurs de système)</li> <li>◆ Prévention, réaction et introduction de mesure de désescalades post incident (incident/réaction)</li> </ul> <p>◆ <b>Administration de fin de cours</b></p>	<p>Steve Waterhouse</p>

### a. CONSIDÉRATIONS MÉTHODOLOGIQUES

#### APPROCHES MÉTHODOLOGIQUE ET PÉDAGOGIQUE

Le cours INF802 privilégie une diversité de méthodes pédagogiques, dont la pratique réflexive, les groupes de discussion, l'apprentissage par problèmes, la méthode des cas et l'apprentissage par projet. Il est attendu que chaque individu participant au cours s'engage de manière active et régulière en intervenant dans les séances AdobeConnect et les forums de discussion, **valant 10%** de la note finale.

Puisqu'il s'agit d'un cours en ligne, toutes les ressources et les consignes sont disponibles sur Moodle 2: <http://www.usherbrooke.ca/moodle2-cours/>.

## ÉVALUATION DES APPRENTISSAGES

### ÉVALUATION N° 1:

#### Travail pratique #1 – Analyse de gestion des incidents

- **Compétence mobilisée :** Comprendre et mettre en place un processus de gestion des incidents (C1)  
Établir des métriques d'évaluation de la sécurité (C3)
- **Description :**
  - À la suite d'une démonstration de l'enseignant, demander à l'étudiant une analyse de la gestion d'incidents basée sur un cas déposé dans Moodle
  - Travail à compléter individuellement
  - Voir grille déposée dans Moodle
- **Critères d'évaluation** Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle.
- **Notation:** Note sur 100, 20 % de la note finale
- **Date de remise :** Le travail est à remettre dans Moodle au plus tard le **lundi 18 septembre 2023, 23h59 HAE**. Le format à recevoir sera sous PDF avec comme nomenclature :  
INF802IFT505-A23-TP1-<nomdefamille.initialprénom>.pdf

### ÉVALUATION N° 2 :

#### QUIZ (Total de 1)

- **Compétence mobilisée :**
  - Comprendre et mettre en place un processus de gestion des incidents (C1)
  - Gérer les vulnérabilités et appliquer une approche proactive contre les cyberattaques (C2)
- **Description :**
  - Un quiz individuels à compléter dans Moodle en 45 minutes les les notions des modules 1-6
- **Critères d'évaluation** Chaque quiz est composé de questions à choix de réponses sur les éléments présentés dans le module.
- **Notation :** Chaque quiz compte pour 10 % de la note finale
- **Date de remise :** Date à confirmer



<b>ÉVALUATION NO 3:</b>	<b>Travail pratique #2</b>
▪ <b>Compétence mobilisée :</b>	Savoir évaluer et reconnaître les menaces
▪ <b>Description :</b>	<ul style="list-style-type: none"><li>▪ Selon un scénario présenté, appliquer les meilleures pratiques vues en classe en lien avec les références</li><li>▪ Ceci est un travail individuel</li></ul>
▪ <b>Critères d'évaluation</b>	Le travail devra être d'un maximum de 5 pages en prenant soin de citer les références. Un retour global sera fait le mardi suivant la remise du travail.
▪ <b>Notation :</b>	Note sur 100, 20 % de la note finale
▪ <b>Date de remise:</b>	Le travail est à remettre dans Moodle au plus tard <b>le lundi 23 octobre 2023, 23h59 HAE</b> . Le format à recevoir sera sous PDF avec comme nomenclature : INF802IFT505-A23-<nomdefamille.initialprénom>.pdf
<b>ÉVALUATION N° 4 :</b>	<b>Travail pratique #3</b>
▪ <b>Compétence mobilisée :</b>	Gestion des vulnérabilités
▪ <b>Description :</b>	Selon un scénario présenté, appliquer les meilleures pratiques vues en classe en lien avec les références. Ceci est un travail individuel.
▪ <b>Critères d'évaluation</b>	Le travail au total devra être d'un maximum de 5 pages en prenant soin de citer les références. Un retour global sera fait le mardi suivant la remise du travail.
▪ <b>Notation :</b>	Note sur 100, 20 % de la note finale
▪ <b>Date de remise :</b>	Le travail est à remettre dans Moodle au plus tard le <b>lundi 13 novembre 2023, 23h59 HNE</b> . Le format à recevoir sera sous PDF avec comme nomenclature : INF802IFT505-A23-TP3-<nomdefamille.initialprénom>.pdf
<b>ÉVALUATION NO 5 :</b>	<b>Travail pratique #4</b>
▪ <b>Compétence mobilisée :</b>	Gestion des mises à jour



- **Description :** À partir de références travaillées en classe, répondre aux questions. Ceci est un travail individuel.
- **Critères d'évaluation** Le travail devra être d'un maximum de 5 pages en prenant soin de citer les références. Un retour global sera fait le mardi suivant la remise du travail.
- **Notation :** Note sur 100, 20 % de la note finale
- **Date de remise :** Le travail est à remettre dans Moodle au plus tard le **lundi 27 novembre 2023, 23h59 HNE**. Le format à recevoir sera sous PDF avec comme nomenclature :  
INF802IFT505-A23-TP4-<nomdefamille.initialprénom>. pdf

#### 4. RÈGLEMENTS ET AUTRES

---

##### PROMOTION DE LA QUALITÉ DE LA LANGUE

Pour promouvoir la qualité du français, les fautes d'orthographe, de lexique et de syntaxe sont prises en considération. Dans tous les travaux, elles seront comptabilisées comme suit : 0,25 pour chaque faute jusqu'à concurrence de 10 % de la note maximale pour chaque objet d'évaluation.

Vous êtes fortement encouragés à effectuer une relecture attentive des travaux avant leur remise officielle et à utiliser les outils de correction disponibles.

##### PRÉSENTATION DES TRAVAUX

Les travaux doivent obligatoirement être soumis sur le site Moodle du cours à la date d'échéance prévue.

Les fichiers électroniques doivent obligatoirement être soumis en format PDF pour faciliter l'insertion de commentaires.

L'intitulé du fichier doit comprendre le numéro du travail, votre nom et vos initiales<sup>SEP</sup> (exemple: pour le travail 1: INF802IFT505-A23-TP1-Jacques.PJ.PDF).

##### DÉLITS RELATIFS AUX ÉTUDES<sup>2</sup>

---

<sup>2</sup> Extrait du [Règlement des études 2017-2018](#)



Le terme « délit » désigne toute infraction ou toute tentative de commettre une infraction, ainsi que toute participation à une infraction ou à une tentative de commettre une infraction, par une personne assujettie à une règle qui lui est applicable en raison de son statut.

Outre la contravention à toute règle applicable à la personne assujettie en vertu d'une source autre que le Règlement des études (Règlement 2575-009), l'Université considère trois (3) types de délits : les délits relatifs aux études, les délits relatifs à l'Université ou aux membres de la communauté universitaire et les délits relatifs aux activités de stage. Ces délits sont présentés aux articles suivants :

Un délit relatif aux études désigne tout acte trompeur ou toute tentative de commettre un tel acte, quant au rendement scolaire ou une exigence relative à une activité pédagogique, à un programme d'études ou à un parcours libre. Sont notamment considérés comme un délit relatif aux études les faits suivants :

- a) commettre un plagiat, soit faire passer ou tenter de faire passer pour sien, dans une production évaluée, le travail d'une autre personne ou des passages ou idées tirés de l'œuvre d'autrui (ce qui inclut notamment le fait de ne pas indiquer la source d'une production, d'un passage ou d'une idée tirés de l'œuvre d'autrui);
- b) commettre un autoplgiat, soit soumettre, sans autorisation préalable, une même production, en tout ou en partie, à plus d'une activité pédagogique ou dans une même activité pédagogique (notamment en cas de reprise);
- c) usurper l'identité d'une autre personne ou ne procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
- d) fournir ou obtenir toute aide non autorisée, qu'elle soit collective ou individuelle, pour une production faisant l'objet d'une évaluation;
- e) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique.

### RESPECT DES DÉLAIS<sup>3</sup>

Tout défaut de remplir les exigences d'évaluation prévues sur le plan de l'activité pédagogique, par exemple pour une production attendue ou un examen, entraîne la **valeur zéro (0)**, à moins que les raisons et les preuves fournies par l'étudiante ou l'étudiant n'aient été acceptées par la faculté ou le centre universitaire de formation.

L'étudiante ou l'étudiant doit **justifier par écrit** son défaut de se soumettre à une évaluation auprès de la faculté ou du centre universitaire de formation. Cette justification doit être **déposée**

---

<sup>3</sup> Extrait du [Règlement des études 2017-2018](#)

**dans le respect du délai** déterminé au règlement complémentaire de la faculté ou du centre universitaire de formation.

Le cas échéant, la faculté ou le centre universitaire de formation peut accorder un délai pour la présentation d'une production, soumettre l'étudiante ou l'étudiant à un examen supplémentaire, apporter des modifications aux exigences de stage ou ne pas tenir compte de cet élément d'évaluation dans l'attribution de la note finale.

## 5. NOTATION

---

Comment une cote est évaluée au CeFTI ?

L'attribution d'une cote au CeFTI n'a rien du hasard. Les enseignants doivent identifier les frontières de cote en fonction d'un modèle basé sur la loi de probabilité de Laplace-Gauss. Voici les règles d'attribution en vigueur au CeFTI.

1. Identification d'une moyenne cible pour l'activité par la direction

- Début de programme : [2,6..3,0]
- Milieu de programme : [2,9..3,3]
- Fin de programme : [3.2..3,7]

2. L'enseignant propose des coupures en conformité avec le règlement des études de l'Université, <https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/>

- A+, A, A- : Excellent
- B+, B, B- : Très bien
- C+, C, C- : Bien
- D+, D : Passable
- E : Échec

3. Les cotes sont transmises à la direction du CeFTI avant d'être officialisées.

L'avantage d'un tel système est la transposition du rendement de l'étudiant en fonction du groupe dans lequel il évolue.

L'évaluation reste équitable entre les cohortes.

L'enseignant a la liberté de proposer une répartition qui déroge de la règle, lorsqu'il juge avoir un groupe particulier.

Ce processus a été discuté et approuvé par le comité de programme au CeFTI le 25 mai 2017.

#### RÉVISION D'UNE NOTE<sup>4</sup>

L'Université reconnaît à toute étudiante ou étudiant le droit à une révision de la note finale sous forme de lettre qui lui est attribuée pour une activité pédagogique ou le test institutionnel de français (TIF), à la condition qu'elle ou qu'il en fasse la demande au moyen du formulaire institutionnel **au plus tard vingt (20) jours ouvrables** après que la note confirmée par la faculté ou le centre universitaire de formation apparaît à son dossier.

## 6. RÉFÉRENCES BIBLIOGRAPHIQUES

---

- ◆ [COBIT 5](#): Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise, ISBN 978-1-60420-436-0;
- ◆ ISO 27001:2018
- ◆ TOGAF
- ◆ SABSA
- ◆ [PCI-DSS version 4 \(français\)](#)
- ◆ NIST Framework Documents - Cybersecurity Framework Version 1.1 (<https://www.nist.gov/cyberframework/framework>);
  - ◆ Version française - Cadre pour l'amélioration de la Cybersécurité des infrastructures critiques  
<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018fr.pdf>
- ◆ NIST SP 800-61 - Computer Security Incident Handling Guide (<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>);
- ◆ NIST SP 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS) [https://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=901146](https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901146)
- ◆ SANS – Incident Handler's Handbook – Patrik Kral
- ◆ [NIST 800-40r4 - Guide to Enterprise Patch Management Technologies](#)
- ◆ [SANS Framework for building a Comprehensive Enterprise Security Patch Management Program](#)
- ◆ [GC - ITSM-10-096 - Les 10 mesures de sécurité des TI : No 2, Appliquer les correctifs aux systèmes d'exploitation et aux applications](#)
- ◆ [SANS A Practical Methodology for Implementing a Patch management Process](#)
- ◆ [CST/GRC - Méthodologie harmonisée d'évaluation des menaces et des risques](#)

---

<sup>4</sup> Extrait du [Règlement des études 2017-2018](#)