UNIVERSITÉ DE SHERBROOKE

1. IDENTIFICATION ET RENSEIGNEMENTS GÉNÉRAUX

Titre officiel du cours :	**INF802 - Planification et prévention en sécurité TI**
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
Session :	Automne 2021
Date de début :	31 août 2021
Date de fin :	07 décembre 2021
Date limite de retrait	15 septembre 2021
Date limite d'abandon :	15 novembre 2021
Rencontres synchrones :	**Mardis :** 31 août 2021 7-14-21-28 septembre 2021 5-12-19-26 octobre 2021 2-9-16-23-30 novembre 2021 7 décembre 2021
Personne(s)-ressource(s) :	Steve Waterhouse
Courriel(s) :	Steve.Waterhouse@USherbrooke.ca

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[1]

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;
- 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.

[1] Extrait de la fiche signalétique

UNIVERSITÉ DE SHERBROOKE

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
TOTAL	135 heures

3. DÉROULEMENT DU COURS

Module	Description	Enseignant
Module 1 : Notions de processus et fonctions informatiques *31 août 2021*	♦ Introduction au cours INF 802 et présentation enseignant / étudiants ♦ Fondements de la cybersécurité ♦ Pyramide de sécurité de l'information ♦ Pyramide organisationnelle versus pyramide de la sécurité de l'information ♦ Notions de processus ♦ Quelques définitions conceptuelles ♦ Survol à très haut niveau de COBIT 5 ♦ Survol à très haut niveau d'ITIL ♦ Facteurs clés de succès de l'implantation des référentiels, normes, etc. ♦ Raisons de l'adoption de cadres référentiels, normes, etc. ♦ Centre opérationnel de sécurité (SOC) ♦ Système de billetterie ♦ RFC	Steve Waterhouse

Module 2 : Processus de gestion d'incidents
07 septembre 2021
14 septembre 2021
	♦ Contexte
	♦ Définitions conceptuelles
	♦ Généralités et quelques statistiques
	♦ Processus de gestion d'incidents
	  ♦ Cadre référentiel de gestion d'incidents selon le NIST-sp 800-61
	  ♦ Objectifs
	  ♦ Phase de préparation
	  ♦ Phase de détection et analyse
	  ♦ Phase de confinement, éradication et recouvrement
	  ♦ Phase de revue post-incident (désescalades)
	  ♦ Quelques indicateurs (métriques) d'incidents
	  ♦ Quelques bonnes pratiques (si possible)
	  ♦ Exemples de processus génériques de gestion d'incidents
	  ♦ Matrice RACI
	  ♦ Quelques lectures suggérées
	
	  ♦ **Travail Pratique#1 – Gestion d'incidents**
		Steve Waterhouse

Module 3 : **Mesures de performances et notions de vie privée** 21 *septembre 2021*	♦ Définitions conceptuelles ♦ Généralités sur les mesures de performance ♦ Enjeux ♦ Raisons d'utilisation des tableaux de bord ♦ Tableau de bord ♦ Étapes de réalisation d'un tableau de bord ♦ Cascades d'objectifs COBIT 5 ♦ Objectifs facilitants COBIT 5 ♦ Quelques métriques de gestion d'incidents selon COBIT 5 ♦ Quelques métriques d'incidents selon le NIST-sp-800-61 ♦ Notion de vie privée ♦ Respect de la vie privée ♦ Dimensions du respect de la vie privée ♦ Encadrement vie privée et protection des renseignements personnels (PRP): USA, ONU, Union Européenne, Canada, et Québec ♦ Atteinte à la vie privée et quelques conséquences rattachées au non-respect de la PRP ♦ Quelques contrôles pouvant aider à réduire les risques d'atteinte à la vie privée	Steve Waterhouse
Module 4 : notions d'incident majeur et de gestion de crise 28 *septembre 2021* *5 octobre 2021*	♦ Contexte ♦ Définitions conceptuelles ♦ Anomalie ♦ Incident de sécurité mineur ♦ Incident de sécurité important ♦ Incident de sécurité critique ♦ Notions d'incident majeur ♦ Délimitation d'incident majeur dans le cadre du module ♦ Quelques incidents majeurs : ♦ Verglas (1998) ♦ Y2K (1999) ♦ Wannacry / NotPetya (2017) ♦ ARC / Equifax (2017) ♦ Marriott (2018-2020) ♦ Desjardins (2019) ♦ Capital One (2019)	Steve Waterhouse

	♦ COVID-19 (2020) ♦ Gestion de crise ♦ Généralités ♦ Quelques contrôles de gestion d'incident majeur ♦ Grandes lignes de gestion de crise selon le NIST-sp 800-61 ♦ Quelques constantes dans la gestion de crise ♦ Se préparer avant la crise ♦ Durant la crise ♦ Réponse à la crise ♦ Post-mortem ♦ Stratégies de communication ♦ Exemple de communication de crise	
Module 5 : **Notions de gestion de problèmes et de gestion des changements** *12 octobre 2021*	♦ Contexte ♦ Exploitation de services ♦ Gestion des problèmes ♦ Transition des services ♦ Gestion des changements	Steve Waterhouse
Module 6 – **Savoir évaluer et reconnaître les menaces** *19 octobre 2021* 26 *octobre 2021*	♦ Définitions ♦ Menaces et autres ♦ Anticipation de protection envers la menace ♦ Menaces et exploits ♦ Les acteurs et leurs menaces ♦ Attribution – À qui la faute ? ♦ **Travail pratique #2 – Savoir évaluer et reconnaître les menaces**	Steve Waterhouse
Module 7 - Processus de gestion des vulnérabilités *02 novembre 2021* *09 novembre 2021*	♦ Gestion des risques ♦ Évaluation des menaces et des risques (ÉMR) ♦ Définitions relatives à la gestion des vulnérabilités ♦ Élaboration d'une méthodologie d'évaluation des vulnérabilités ♦ Outils de référence avec lesquels à travailler ♦ **Travail pratique#3 – Gestion des vulnérabilités**	Steve Waterhouse

Module 8 - Processus de gestion des mises à jour *16 novembre 2021* *23 novembre 2021*	♦ Définition de l'importance du processus des mises à jour ♦ Mises à jour PME ♦ Mises à jour GE ♦ Les exceptions (IoT, ICS/SCADA) ♦ Élaboration d'une méthodologie d'évaluation des mises à jour ♦ Problèmes anticipés ♦ Outils ♦ **Travail pratique#4 – Gestion des mises à jour**	Steve Waterhouse
Module 9 - Prévention de l'hameçonnage *30 décembre 2021* *07 décembre 2021*	♦ Définition de ce qu'est l'hameçonnage ♦ Faits vécus ♦ 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 dés escalades post incident (incident/réaction) ♦ **Administration de fin de cours**	Steve Waterhouse

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.

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^{O} 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 20 septembre 2021, 23h59. Le format à recevoir sera sous PDF avec comme nomenclature : INF802-A21-TP1-<nomdefamille.initialprénom>.pdf
ÉVALUATION N^{O} 2 :	**QUIZ (Total de 3)**
▪ ***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) ▪ Établir des métriques d'évaluation de la sécurité (C3)
▪ ***Description :***	▪ Trois quiz individuels à compléter dans Moodle
▪ ***Critères d'évaluation***	Chaque quiz est composé de 2-3 questions à choix de réponses sur les éléments présentés dans le module.
▪ ***Notation :***	Chaque quiz compte pour 5 % pour un total de 15 % de la note finale
▪ ***Date de remise :***	Date à confirmer

ÉVALUATION NO 3:	**Travail pratique #2**
▪ ***Compétence mobilisée :***	Savoir évaluer et reconnaître les menaces
▪ ***Description :***	▪ Selon un scénario présenté, appliquer les meilleures pratiques vues en classe en lien avec les références ▪ 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, 25 % de la note finale
▪ ***Date de remise:***	Le travail est à remettre dans Moodle au plus tard le lundi 19 octobre 2021, 23h59. Le format à recevoir sera sous PDF avec comme nomenclature : INF802-A21-TP2-<nomdefamille.initialprénom>.pdf

ÉVALUATION N^{O} 4 :	**Travail pratique #3**
▪ ***Compétence mobilisée :***	Gestion des vulnérabilités
▪ ***Description :***	Selon un scénario présenté, appliquer les meilleures pratiques vues en classe en lien avec les références. Ceci est un travail individuel.
▪ ***Critères d'évaluation***	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.
▪ ***Notation :***	Note sur 100, 20 % de la note finale
▪ ***Date de remise :***	Le travail est à remettre dans Moodle au plus tard le lundi 15 novembre 2021, 23h59. Le format à recevoir sera sous PDF avec comme nomenclature : INF802-A21-TP3-<nomdefamille.initialprénom>.pdf

ÉVALUATION NO 5 :	**Travail pratique #4**
▪ ***Compétence mobilisée :***	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 29 novembre 2021, 23h59. Le format à recevoir sera sous PDF avec comme nomenclature : INF802-A21-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 votre prénom (exemple: pour le travail 1: Travail1_Nom_Prénom.docx).

DÉLITS RELATIFS AUX ÉTUDES[2]

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

[2] Extrait du Règlement des études 2017-2018

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 autoplagiat, 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[3]

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 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.

[3] Extrait du Règlement des études 2017-2018

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[4]

[4] Extrait du Règlement des études 2017-2018

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;
- NIST Framework Documents - Cybersecurity Framework Version 1.1 (https://www.nist.gov/cyberframework/framework);
- NIST SP 800-61 - Computer Security Incident Handling Guide (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf);
- NIST SP800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS) https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901146
- ISO 27001 -
- TOGAF
- SABSA