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 2018
Date de début :	1 novembre 2018
Date de fin :	20 décembre 2018
Date limite d'abandon :	4 décembre 2018
Rencontres synchrones :	**Mardis :** 6 novembre 13 novembre 20 novembre 27 novembre 4 décembre 11 décembre **Jeudis :** 1er novembre 8 novembre 15 novembre 22 novembre 29 novembre 6 décembre 13 décembre 20 décembre
Personne(s)-ressource(s) :	Steve Waterhouse Annassou Abokou
Courriel(s) :	Steve.Waterhouse@USherbrooke.ca Annassou.Abokou@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 (C1). Gérer des vulnérabilités et appliquer une approche proactive contre les cyberattaques (C2). Établir des métriques d'évaluation de la sécurité (C3).

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.

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;

[1] Extrait de la fiche signalétique

- 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	37 heures
Laboratoire en classe	6 heures
Conférence externe	12 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 *1er novembre 2018*	♦ Introduction au cours INF 802 et présentation des enseignants/étudiants ♦ Pyramide organisationnelle ♦ Notions de processus ♦ Arrimage de quelques cadres référentiels, normes, etc. ♦ 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. ♦ Fonctions informatiques ♦ Centre opérationnel de sécurité (SOC) ♦ Système de billetterie ♦ Suggestions de lectures	AA
Module 2 : Processus de gestion d'incidents *6 novembre 2018* *8 novembre 2018*	♦ Définitions conceptuelles ♦ Généralités ♦ Processus de gestion d'incidents selon le NIST-sp 800-61: • Objectifs • Phase de planification • Phase de détection et analyse	AA

	• Phase de confinement, éradication et recouvrement • Phase de revue post-incident ♦ Liste de contrôles d'incidents selon le NIST-sp 800-61 ♦ Survol du processus de gestion d'incidents selon COBIT 5 ♦ Métriques ou indicateurs de gestion (ex: gestion d'incidents) ♦ Exemples de processus génériques de gestion d'incidents ♦ Quelques lectures suggérées.	
Module 3 : Processus de gestion d'incidents selon COBIT 5, notions d'incident majeur et de gestion de crise *13 novembre 2018* *15 novembre 2018*	♦ Définitions conceptuelles ♦ Survol du processus de gestion d'incidents selon COBIT 5 ♦ Métriques ou indicateurs de gestion (ex: gestion d'incidents) ♦ Incident majeur ♦ Gestion de crise ♦ Quelques lectures suggérées	AA
Labo classe *20 novembre 2018*	TP est en cours de conception	AA
Module 4 : Processus de gestion des vulnérabilités et des mises à jour *22 novembre 2018*	♦ Définitions ♦ Méthodologie ♦ Priorisation ♦ Défi à prévoir	SW
Module 5 : Processus de gestion des vulnérabilités *27 novembre 2018*	♦ Gestion des vulnérabilités ♦ Définition de l'importance de connaître les vulnérabilités ♦ Priorisation ♦ Élaboration d'une méthodologie d'évaluation de vulnérabilités ♦ Documentation ♦ Outils de référence avec lesquels travailler.	SW

Module 6 : Processus de gestion des mises à jour *29 novembre 2018* *4 décembre 2018*	♦ Gestion des mises à jour ♦ Définition de l'importance du processus des mises à jour ♦ Priorisation ♦ Élaboration d'une méthodologie d'évaluation des mises à jour ♦ Déploiement des mises à jour ♦ Documentation ♦ Outils	SW
Labo classe *6 décembre 2018*	♦ Exercice d'audit des vulnérabilités de PC / serveurs avec détection ♦ Déploiement de mises à jour	SW
Module 7 : Prévention de l'hameçonnage *11 décembre 2018* *13 décembre 2018*	♦ 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 incidents (incident/réaction)	SW

4. 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/.

5. ÉVALUATION DES APPRENTISSAGES

ÉVALUATION N° 1: **DEVOIR #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 :***
  - Suite à 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 en équipe
  - 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:*** 35 % de la note finale
- ***Date de remise :*** 1er décembre 2018

ÉVALUATION N° 2 : **DEVOIR #2 – Analyse de vulnérabilité**

- ***Compétence mobilisée :***
  - Gérer des vulnérabilités et appliquer une approche proactive contre les cyberattaques (C2)
  - Établir des métriques d'évaluation de la sécurité (C3)
- ***Description :*** Suite à une démonstration de l'enseignant, demander à l'étudiant une analyse de vulnérabilité à partir d'une VM déposée dans Moodle

  Travail individuel
- ***Critères d'évaluation*** Pour les consignes précises, de même que les modalités de remise et la grille d'évaluation, consultez Moodle 2.
- ***Notation :*** 30 % de la note finale
- ***Date de remise :*** Date à confirmer

ÉVALUATION N^{O} 3: **QUIZ (Total de 5)**

- ***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 :*** Cinq 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 7 % pour un total de 35 % de la note finale
- ***Date de remise:*** Date à confirmer

6. 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 2 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.

[2] Extrait du Règlement des études 2017-2018

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 auto-plagiat, 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 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 au 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

[3] Extrait du Règlement des études 2017-2018

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.

7. 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.

UNIVERSITÉ DE SHERBROOKE

RÉVISION D'UNE NOTE[4]

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.

8. 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;
- La réingénierie des processus administratifs, Le pouvoir de réinventer son organisation, H. James Harrington, Les Éditions Transcontinentales Inc., ISBN 2-921030-62-4, 2000 ;
- NIST SP 800-61;
- https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=901146

[4] Extrait du Règlement des études 2017-2018