Collège de Maisonneuve

PLAN DE COURS

Formation continue
Programme LEA.8F (AEC)

Développement de logiciels : Sécurité des applications mobiles, web et de bureau

Cours 420-950-MA

Cybersécurité

Hiver 2023

60 heures (1-3-1)

Cours préalable : 420-940-MA

Groupe 21624

Chargé de cours : *Jean-Pierre Fiset*

Département d'informatique

Courriel jfiset@cmaisonneuve.qc.ca

1. Présentation du cours

Le cours sur la cybersécurité couvre les mesures qui doivent être appliquées à l'environnement logiciel et au logiciel développé pour assurer la protection contre les menaces de cybersécurité. À l'issue de ce cours, les étudiants devraient être en mesure d'analyser et d'évaluer les risques liés à la sécurité de l'information, d'appliquer des mesures de sécurité dans le cadre du processus de développement afin de protéger le logiciel développé et son environnement, de garantir la confidentialité et l'intégrité des données, et de travailler dans un contexte d'authentification et d'autorisation. Les étudiants devraient également être capables d'intégrer les mesures de sécurité dans leurs pratiques et techniques de développement acquises précédemment.

Les développeurs de logiciels sont censés sécuriser leurs applications afin qu'elles ne puissent pas être facilement compromises. Le cours Cybersécurité aide les étudiants à développer des applications sécurisées en comprenant comment les exploits se produisent et en apprenant les techniques pour s'en défendre. Ce cours ajoute des connaissances en réseautage en plus de ce qui a été appris dans les cours de programmation Web précédents. Il exploite également les concepts appris du cours sur les systèmes d'exploitation, tels que les autorisations et les propriétés des fichiers. Les étudiants doivent avoir suivi avec succès le cours de développement de systèmes, ils sont donc déjà familiarisés avec la conception et le développement d'applications qui les préparent à maîtriser pleinement les concepts de sécurité tels que la validation des entrées de l'utilisateur, le cryptage des données sensibles et la sécurisation des serveurs Web.

2. Compétences à développer dans le cours

Énoncé(s) de compétence	**Élément(s)**
00Q8 **Prendre des mesures préventives en ce qui concerne la sécurité des informations**	1. Analyser les risques de sécurité de l'information. 2. Appliquez les mesures de sécurité reconnues pour protéger le réseau. 3. Appliquer les mesures de sécurité reconnues pour protéger une application.

3. Contenu et déroulement du cours

Semaine	Objectifs d'apprentissage	Laboratoires ou activités d'apprentissage
#1	**Présentation du cours et introduction** • Environnement de support au cours et modalités de fonctionnement; • Révision de Concepts vus à la session précédente; • Introduction des connaissances et les concepts de base en Sécurité; • Interprétation des schémas réseau en Sécurité.	**Exercices – 1%** • Sécurité dans l'architecture des systèmes d'information **Lectures** • Résumé de lectures présentant des sujets et des concepts généraux du cours
#2	**Évolution et Origine du « Bien » et du « Mal »** • La sécurité et la sureté; • Introduction à la Morale; • Introduction l'Éthique; • Introduction à la Déontologie.	**Exercices – 1%** • Bien et le Mal dans le développement de système d'information **Lectures** • Résumé de lectures présentant des sujets et des concepts généraux du cours
#3	**Bases et connaissances générales des réseaux** • Exposition de base au modèle OSI et ses protocoles; • Bases de la cryptographie et des logiciels de sécurité; • Infrastructure à clé publique (PKI); • Autorité de certification (AC); • Certificat signé; • Chiffrer les données sensibles; • Bibliothèques de chiffrement; • Utilitaires de chiffrement; • Protocole de chiffrement (Ex. OpenSSL/TLS).	**Exercices – 1%** • Chiffrement de sécurité **Lectures** • Résumé de lectures présentant des sujets et des concepts généraux du cours
#4	**Principaux Dangers, Attaques, Failles, Incidents** • Identification des techniques de l'Ingénierie Sociale et Piratage Psychologique; • Reconnaissance des origines, des signes et Indices des : Dangers, Attaques, Failles et Incidents pesant sur la Sécurité; • Principaux Logiciels malveillants (Malware); • Terminologie et Classification des Principaux Logiciels malveillants (Malware); • Principaux Symptômes et leurs Méthodes de Prévention. • Terminologie et Classification des Principaux Logiciels malveillants (Malware);	• Failles, Piratage et Malwares **Lectures** Résumé de lectures présentant des sujets et des concepts généraux du cours **Quiz 01 - 05 %**

#5	**L'analyse de risques et les enjeux de la sécurité** • Enjeux reliés aux données personnelles (PII); • Identifier et catégoriser les éléments d'un actif numérique; • Distinction entre attaque, défense, menace, vulnérabilité; • Acteurs à l'origine des menaces, Analyse des dangers au niveau des périmètres de sécurité, de la Mobilité et de la Connectivité constante à Internet; • Notions et principes de la gestion de risques; • La nomenclature des risques; L'analyse de risques; • La mitigation des risques.	**Exercices – 1%** • Risques de sécurité **Lectures** Résumé de lectures présentant des sujets et des concepts généraux du cours
#6	**La Sécurité des systèmes d'exploitation** • Autorisations des fichiers des systèmes d'exploitation; • Propriété des fichiers des systèmes d'exploitation; • Exécuter des outils de ligne de commande; • Contrôle d'accès et stratégies d'attribution des droits d'accès; • Validation de l'entrée utilisateur.	**Exercices – 1%** • Sécurité des SE/OS **Lectures** • Résumé de lectures présentant des sujets et des concepts généraux du cours
#7	**Livrable 1.** • Stratégies de Sécurité (Défense en Profondeur); • Base du Développement Agile et la sécurité informatique; • La protection des données; • Stratégies de sauvegarde; • Sauvegarder les données sensibles;	**Livrable 01 - 5 %** **Quiz 02 - 05 %**
#8	**Livrable 2.** • La classification des actifs informationnels; • Qu'entend-on par « classification des actifs informationnels »? • Pourquoi? Comment? • La protection des applications. • La protection des hôtes.	**Remise et présentation** **Livrables 01/02 - 5 %**

#9	**Livrable 3.** • Réseau et Périmètre; • Exposition aux protocoles réseau (DHCP, DNS); • Analyseur de Paquets Ethernet (Ex. Wireshark); • Appliquer des filtres de capture et d'affichage; • Plate-forme de tests de sécurité et Équipe de défense; • Tests d'intrusion (injection de commande, injection SQL); • Test d'intrusion des applications; • Pare-feu et Antivirus; • Serveur Web (URL, HTTP (port TCP 80), HTTPs (port TCP 443)).	**Livrable 03 - 5 %** **Quiz 03 - 05 %**
#10	**Livrable 4.** • Physique et inventaires; • Consulter la documentation informatique; • Inventaire précis du parc informatique; • Inventaire précis des applications installées; • Inventaire approprié des menaces et vulnérabilités potentielles; • Identification précise des impacts sur la sécurité; • Choix approprié des mesures de sécurité.	**Remise et présentation** **Livrables 03/04 - 5 %**
#11	**Livrable 5.** • La gouvernance de la sécurité; • Les politiques de sécurité; • Les cadres méthodologiques de gestion de la sécurité; • Audits et conformité. • Quelques exemples : ISO 27000, COBIT;	**Livrable 05 - 5 %** **Quiz 04 - 05 %**
#12	**Livrable 6.** • Agilité et Sécurité Numérique • Système de gestion de la sécurité de l'information et stratégie de cybersécurité • Évaluation de l'emploi de Scrum digne de confiance pour les logiciels agiles • Un cadre de test de sécurité pour les projets de développement, basés sur Scrum	**Remise et présentation** **Livrables 05/06 - 5 %**

#13	**Livrable 07 - Cycle/Itération Agile** • Un cycle agile ou itération courte est une période de travail de 1 semaine qui correspond à une étape de sécurisation.	**Livrable 07 - 5 %** **Quiz 05 - 05 %**
#14	**Livrable 08 - Cycle/Itération Agile** • Un cycle agile ou itération courte est une période de travail de 1 semaine qui correspond à une étape de sécurisation.	**Remise et présentation** **Livrables 07/08 - 5 %** **Révision EF**
#15		**Épreuve Finale – 30 %**

4. Activités d'enseignement et d'apprentissage

Les principales méthodes pédagogiques utilisées dans ce cours sont :

- Exposés théoriques en alternance avec des évaluations formatives (exercices formatifs) et des évaluations sommatives (questionnaires, lectures, exercices et travaux pratiques).
- Exercices ponctuels laboratoires et travaux pratiques principalement réalisés durant les heures de cours prévues à l'horaire et au besoin, complétés en dehors de ces heures.
- Questionnaires réalisés en classe en début de cours (activités individuelles).
- Exercices ponctuels et travaux pratiques (activités en équipe)

Note : Le calendrier précédent pourrait être ajusté en cours de session en fonction du rythme d'apprentissage.

5. Évaluation formative et sommative

L'évaluation formative se fait en continu, tout au long de la session, par la réalisation d'exercices pratiques en classe et de lectures techniques. Les exercices sont réalisés en présence du professeur qui vous viendra en aide au besoin.
Note : La réalisation de tous les exercices formatifs est fortement recommandée pour développer au maximum les compétences visées par le cours.

L'évaluation sommative s'effectuera au moyen de **cinq Exercices, de cinq quiz, d'une épreuve finale ainsi que d'un projet de comprenant un total de 8 livrables.**

Grille d'évaluation

Quiz :	**25%**
Exercices/Laboratoires :	**05%**
Livrables :	**40%**
Epreuve Finale :	**30%**

Outils d'évaluation	Évaluation	Pondération	Échéancier
Quiz (5)	Théorique	25%	Bloc de 2 heures de la 4-13ième semaine
Exercices (5)	Remise des journaux et laboratoires	5%	De la 1ième à la 6ième semaine
Livrables (8)	Présentation	40%	De la 7ième à la 14ième semaine
Épreuve finale	Remise du rapport de déploiement	30%	Bloc de 3 heures de la 15ième semaine

Livrables

Les étudiants apprendront un processus de sécurisation de l'architecture informatique, en collaborant à la mise en œuvre d'une politique de gouvernance de la sécurité, pour un client du monde réel.

Les contextes réels sont suggérés : (sécurisation de l'architecture informatique, pour un client du monde réel)

- Dans la mesure du possible, les étudiants interagiront régulièrement, avec un client du monde réel.
- La structure et le fonctionnement des équipes sont calqués sur de véritables environnements de mise en place politiques de sécurité de logiciels commerciaux sécurisés.

Activités clés pour les livrables :

Le cours couvre le contrôle d'accès de base, les bases de la cryptographie, l'infrastructure à clé publique et les tests de pénétration des applications. Les étudiants appliquent leur apprentissage au cours de séances de présentations en classe, pour acquérir une expérience pratique des outils et technologies de cybersécurité couramment utilisés.

Le cours couvre également les mesures préventives et les meilleures pratiques, pour atténuer les attaques et améliorer la sécurité de l'application.

Le cours sur la cybersécurité présente aux étudiants une variété de cybermenaces et des techniques d'atténuation essentielles que les informaticiens sont censés appliquer dans le cadre de leur travail. L'étudiant analyse les risques de sécurité impactant les données, un ordinateur, le réseau ou l'application qu'il développe, identifie leur gravité et applique des stratégies pour les atténuer.

Implémentez des mesures de sécurité de l'architecture informatique, telles que la validation des entrées de l'utilisateur contre les exploits potentiels et l'application de l'authentification et de l'autorisation.

L'étudiant serait exposé aux concepts de base de la cybersécurité et de l'évaluation de la vulnérabilité pendant la durée de ce cours.

Sur les plateformes de tests, les étudiants peuvent pratiquer des tests de pénétration de base dans un environnement simulé et être évalués sur les progrès qu'ils font avec chaque tâche associée au laboratoire et démonstration prévus.

Connaissances générales en réseau
- Exposition au modèle OSI lors de l'analyse de paquets Ethernet capturés
- Appliquez des filtres de capture de trames
- Exposition au réseau protocoles de sécurité

Ingéniosité et autonomie :
- Exécuter des outils de ligne de commande, une pratique utile
- Consulter la documentation pour trouver les fonctionnalités et les options de programme et de sécurité souhaitées

Le projet se veut un défi professionnel et est réalisé en équipe de **trois personnes (maximum).**

Quiz (5)

Les quiz sont des épreuves théoriques. Ils porteront sur tous les apprentissages vus depuis le début du cours. Toute documentation est permise.

Épreuve finale

Lors de l'épreuve finale, vous devrez procéder à la sécurisation à la configuration d'une application simple et de petite envergure. Un scénario de sécurisation comprenant des besoins et des contraintes vous sera soumis. Vous devrez alors mettre en œuvre une solution de cybersécurité, qui répond aux besoins spécifiés. Toute documentation est permise pour cette épreuve finale.

6. Modalités d'application des politiques institutionnelles et règles départementales particulières.

Double seuil
Les évaluations sommatives qui sont assujetties à l'atteinte du double seuil de réussite du cours sont l'examen-quiz et l'épreuve finale.

Sous réserve de l'approbation du professeur. Le même sujet ne peut être choisi par deux équipes et ne peut avoir été couvert dans un autre cours de la formation.

Collège de Maisonneuve

Extraits des politiques institutionnelles et départementales

Ces modalités d'application ont été rédigées en complément aux autres politiques et procédures du Collège de Maisonneuve, notamment à la Politique institutionnelle d'évaluation des apprentissages (PIEA), à la Procédure de révision de notes, à la Politique de concertation par programmes, à la Politique de la langue et à la Procédure de conciliation relatives aux plaintes des étudiants..

L'étudiant aurait avantage à consulter ces politiques sur le site Web du collège et dans le guide Étudier à Maisonneuve. En particulier, la PIEA est disponible sur http://www.cmaisonneuve.qc.ca/wp-content/uploads/2014/09/politiqueinstitutionnelleevaluationapprentissagesjuin2014.pdf.

En cas de recours, l'étudiant peut s'adresser au coordonnateur de département ou à la Direction des études.

Au sujet des évaluations

Seuil de réussite

Le seuil de réussite d'un cours est de 60%.
EXIGENCES PARTICULIÈRES À LA RÉUSSITE D'UN COURS
Dans tous les cours sous la juridiction du département d'informatique, il ne suffit pas d'avoir une moyenne générale pondérée de 60% pour réussir le cours.
Un étudiant est réputé avoir réussi le cours que s'il rencontre les deux exigences suivantes :

- Il a obtenu une moyenne générale pondérée d'au moins 60% pour l'ensemble de toutes ses évaluations sommatives.
- Il a maintenu une moyenne pondérée d'au moins 50% pour les évaluations sommatives individuelles exercées dans un environnement contrôlé : examens, épreuve finale, tests, etc. Les évaluations considérées pour ce deuxième seuil de réussite sont identifiées au plan de cours.

Si la deuxième exigence n'est pas rencontrée, la note portée au bulletin pour ce cours ne peut être supérieure à 49%.

Correction d'une évaluation
Le professeur corrige une évaluation en fonction de ce que l'étudiant a effectivement écrit et non en fonction de ce qu'il croit deviner de ce que l'étudiant a voulu écrire.

Authenticité d'une évaluation

Lorsqu'un professeur a des doutes sur l'authenticité d'une évaluation, il peut alors avoir recours à une vérification orale ou écrite du niveau de connaissance de l'étudiant ou des membres de l'équipe. À la suite de cette vérification, il peut modifier au besoin la note préalablement obtenue.

Conservation des documents servant aux évaluations

Le professeur conserve jusqu'au début de la session suivante les documents ayant servis aux dernières évaluations des étudiants.

Il est sous la responsabilité de l'étudiant de conserver tout document remis corrigé pour une éventuelle révision de notes ou la correction d'une erreur de calcul.

Présence et absence lors d'une évaluation

La présence est obligatoire aux évaluations sommatives.

Toute absence à une évaluation doit être justifiée de façon satisfaisante au professeur concerné, sinon la note 0 est attribuée pour cette évaluation. Un billet du médecin n'est pas nécessairement une justification à une absence – voir la rubrique *Reprise d'une évaluation*. Conformément au point 4,4 de la PEIA, toute demande du report d'une évaluation pour fête religieuse doit être traitée et peut faire l'objet d'accommodements raisonnables. L'étudiant doit aviser ses professeurs par écrit avant la fin de la deuxième semaine de la session.

Confidentialité d'une évaluation

L'étudiant a droit de prendre connaissance, après correction, de ses évaluations. Il a droit au respect de la confidentialité de ses évaluations et de toute information relative à son rendement. Il a aussi le droit à une évaluation équitable et impartiale de ses apprentissages. L'étudiant a le droit d'en appeler de chacune de ses évaluations selon les délais prescrits par la procédure de révision de notes – voir l'article ci-dessous Révision de notes.

Ce point fait référence au point 3.8.d de la Politique institutionnelle d'évaluation des apprentissages.

Reprise d'une évaluation

Aucune reprise possible pour une évaluation sommative, sauf dans le cas d'une absence justifiée.

Dans le cas d'une absence justifiée à une évaluation, cette évaluation peut être annulée, ou reprise à une date convenue par le professeur et l'étudiant.

Dans le cas d'une absence justifiée à un des volets de l'épreuve finale, cette évaluation doit être reprise.

Toute évaluation sommative ne peut être reprise oralement.

Les modalités d'application

Admission/sortie du local d'une évaluation sommative

Aucun étudiant ne sera admis après qu'un étudiant ait quitté le local où se déroule l'évaluation sommative.

Aucun étudiant ne doit quitter le local avant que le professeur ne le permette.

Les autres points de l'article 4.10 de la Politique institutionnelle de l'évaluation des apprentissages s'appliquent.

Administration d'un examen

Le professeur a toute autorité pour permettre ou refuser l'utilisation de n'importe quel appareil de quelque nature que ce soit.

Absence prolongée justifiée

Dans le cas d'une absence prolongée justifiée, l'étudiant doit prévenir dans les plus brefs délais son professeur. Le professeur juge alors des impacts de cette absence prolongée sur la réussite du cours. S'il le juge à propos, il élabore une stratégie d'intervention avec le coordonnateur de département et le transmet à l'étudiant.

Révision de notes

Un étudiant insatisfait d'une correction doit d'abord en discuter avec son professeur le plus tôt possible. S'il maintient son insatisfaction, l'étudiant peut se prévaloir de la procédure de révision de notes.

Les autres points de l'annexe 1 de la Politique institutionnelle de l'évaluation des apprentissages s'appliquent.

Présentation et remise d'un travail

Un professeur peut refuser un travail dont il juge la présentation inacceptable. Lorsqu'un professeur donne un travail, il en précise alors les exigences, la date et l'heure de la remise. Si l'heure de remise n'est pas précisée, le travail doit être remis avant l'heure du début des cours de la journée suivante. Par exemple, si un professeur donne comme date de remise d'un travail pratique un vendredi et qu'il ne mentionne pas l'heure de remise, l'étudiant aura jusqu'au lundi à 8h15 pour remettre son travail et ce, sans pénalité de retard.

Le professeur n'accepte jamais un travail lorsqu'il a déjà remis les copies corrigées ou lorsque cela s'applique, un autre professeur a remis ses copies corrigées du même travail pratique à un autre groupe du même cours. La note 0 est alors consignée au dossier de l'étudiant.

Les autres points de l'article 4.6 de la Politique institutionnelle d'évaluation des apprentissages s'appliquent.

Délai de correction

Conformément à l'article 3.8 de la de la PIEA, normalement, l'étudiant reçoit ses résultats dans un délai de deux semaines après la date de remise du travail au professeur.

À défaut de la remise de la correction du travail dans les délais prévus, l'étudiant peut en appeler auprès du coordonnateur du département.

Retard et pénalité de retard

Le professeur peut refuser un travail en retard.

Par contre, lorsqu'un professeur accepte les retards, il doit pénaliser le travail de 10% de la **note maximale** pour chaque jour ouvrable de retard, et ce jusqu'à concurrence de 50%. Aucun travail ne sera accepté au-delà de 5 jours ouvrables de retard.

Règlements concernant le plagiat et la fraude

Échange de document ou d'appareils

L'étudiant doit s'assurer d'avoir en main tout le matériel permis et ce avant le début d'une évaluation sommative.

L'utilisation de téléphone mobile, de tablette ou tout autre appareil de communication est formellement interdite. Les points de l'article 4.9 de la Politique institutionnelle de l'évaluation des apprentissages s'appliquent.

Sanction pour plagiat ou fraude
Les points de l'article 4.9 de la Politique institutionnelle de l'évaluation des apprentissages s'appliquent.

Qualité du français et présentation des travaux écrits
Un professeur n'est pas tenu d'accepter un travail dont la langue, la présentation, la lisibilité, ou le non-respect des spécifications exigées sont jugés insuffisants. L'étudiant devra reprendre le travail et subir les pénalités inhérentes à sa remise ultérieure.
Les autres points de l'article 4.1 et l'annexe 1 de la Politique institutionnelle de l'évaluation des apprentissages s'appliquent.

7. Recours prévus pour les étudiants

Voir la section intitulée Extraits des politiques institutionnelles et départementales, en annexe.

8. Médiagraphie

Site Internet
https://www.ssi.gouv.fr
https://www.microsoft.com
https://opensource.com/

Références

Disponible sur Léa :
o Plusieurs notes de cours, articles, sites Web, références documentant la sécurité, la cybersécurité, les défaillances et la vulnérabilité des systèmes informatiques.

9. Frais

Aucun

10. Disponibilité

Sur demande par MIO ou jfiset@cmaisonneuve.qc.ca**.**

POLITIQUE POUR PRÉVENIR ET CONTRER LES VIOLENCES À CARACTÈRE SEXUEL

Pour consulter la politique, porter plainte, recevoir de l'aide ou de l'accompagnement :

- www.cmaisonneuve.qc.ca/soutien-violence-sexuelle
- violencesexuelle@cmaisonneuve.qc.ca
- Local D-3608D

Collège de Maisonneuve