Université de Sherbrooke

Centre de formation en technologie de l'information

INF 803 – Sécurité des systèmes

Plan d'activité pédagogique

Hiver 2026

Enseignants	Mondher Jarraya	David Labelle
Courriel :	mondher.jarraya@usherbrooke.ca	david.labelle@usherbrooke.ca
Local :	L1-2422	F1-3033-1
Téléphone :	+1 450 463-1835 x61785	+1 819 821-8000 x62525

Disponibilités :

- Les échanges se feront par courriel, avec un délai de réponse maximal de 48 heures.
- Si nécessaire et selon la disponibilité de l'étudiant et de l'enseignant, une rencontre sur Teams pourra être planifiée.

Site web du cours : https ://moodle.usherbrooke.ca/course/view.php ?id=42913

Horaire Exposé magistral : Mercredi 18 h 30 à 21 h 50 salle Réunion Microsoft Teams

Description officielle de l'activité pédagogique[1]

Cibles de formation :	Connaître et maîtriser les principaux systèmes d'exploitation disponibles sur le marché. Savoir renforcer la sécurité de ces systèmes. Comprendre les enjeux de sécurité entourant la virtualisation et les systèmes mobiles.
Contenu :	Sécurisation des réseaux. Sécurisation des systèmes d'exploitation. Sécurisation du Web et du nuage. Cryptographie. Sécurité des systèmes mobiles.
Crédits	3
Organisation	3 heures d'exposé magistral par semaine 6 heures de travail personnel par semaine
Particularités	Aucune

[1] https ://www.usherbrooke.ca/admission/fiches-cours/inf803

1 Présentation

Cette section présente les cibles de formation spécifiques et le contenu détaillé de l'activité pédagogique. Cette section, non modifiable sans l'approbation du comité de programme du Centre de formation en technologie de l'information, constitue la version officielle.

1.1 Mise en contexte

Place du cours dans le programme :

L'objectif du cours est d'offrir une vue d'ensemble des principales perspectives théoriques et pratiques liées à la sécurité des systèmes informatiques modernes. Le cours prépare l'étudiante ou l'étudiant à comprendre comment protéger ces systèmes, à analyser leurs vulnérabilités et à mettre en œuvre des stratégies préventives de sécurité adaptées aux organisations.

Dans cette optique, le cours s'appuie sur un survol des principaux systèmes informatiques utilisés en organisation (systèmes d'exploitation, systèmes distribués, environnements virtualisés, infrastructures infonuagiques, systèmes de fichiers et de stockage, services réseau essentiels et plateformes mobiles), ainsi que sur l'analyse de leurs surfaces d'attaque et de leurs mécanismes de sécurité. Ces notions sont approfondies par l'application des bonnes pratiques de sécurisation des postes, des serveurs, des services exposés et des environnements distribués.

1.2 Cibles de formation spécifiques

Le microprogramme en sécurité informatique - volet prévention permet à l'étudiante et 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.

1.3 Contenu détaillé

Thème	Contenu	Nbr. d'heures	Objectifs
1	Sécurité des stations de travail : • Introduction & présentations • Présentation de la sécurité des systèmes • Introduction aux systèmes d'exploitation • Sécurité des postes Windows	3	
2	Introduction aux serveurs et virtualisation : • Versions de Windows Server • Architecture, installation et configuration • Rôles et fonctionnalités • Virtualisation, « Bac à sable » • Hyper V • Unix -Linux	3	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
3	Sécurisation d'Active Directory dans un système distribué : • Gestionnaire de serveur • Service de domaine Active Directory • LDAP, infrastructure logique, physique, site, forêt, domaine • Outils d'administration • Sécurité de l'administration à distance (RDP, WinRM et JEA pour PowerShell)	3	
4	Profils et permissions : • Gestion des objets (utilisateurs, groupes) • Unité d'organisation • Profils d'utilisateurs, script d'ouverture de session • Permissions de partage	3	
5	Sécurisation des politiques et des accès dans un système distribué : • DFS (Distributed File System) • Stratégies de groupe (Group Policy) • Gestion des accès, héritage et restrictions	3	
6	Gestion des accès et mise à jour : • Mise à jour de Windows Server WSUS • L'utilisation de l'authentification forte • Gestion des identités et des accès (GIA)	3	
7	Examen pratique	3	
8	Sécurisation des serveurs Web et introduction aux systèmes infonuagiques : • Surfaces d'attaques des services exposés • Bonnes pratiques de configuration (TLS, permissions, confidentialité…) • Introduction au cloud	3	
9	Détection des compromissions et analyse des traces système : • Types d'attaques courantes (phishing, ransomware, exploitation de vulnérabilités) • Indicateurs de compromission (IoC) et analyse d'alertes • Techniques et outils de détection, journaux, SIEM, EDR/XDR • Bonnes pratiques de surveillance et de réponse initiale	3	
10	Audit des systèmes et gestion des certificats de sécurité : • Auditer les événements d'ouverture de session sur un compte • Auditer la gestion des comptes utilisateur • Auditer les ouvertures et fermetures de sessions • Auditer les changements de stratégie • Auditer l'utilisation des privilèges • Certificats de sécurité	3	
11	Résilience des systèmes et continuité des opérations : • Élaboration d'un plan de reprise informatique • Identification des actifs critiques, élaboration d'un PCO, indicateurs RPO/RTO • Stratégies de sauvegarde, chiffrement et intégrité, immuabilité des sauvegardes • CMDB • Sécurisation du stockage • Stratégies de récupération, réplication, basculement (*failover*), haute disponibilité	3	
12	Haute disponibilité, PowerShell et fédération d'identité (ADFS) : • Répartiteur de charge et présentation de l'architecture haute disponibilité • Notion de cluster • Introduction à PowerShell et la sécurité des scripts • Authentification, SSO et fédération d'identité avec MS ADFS	3	

Table 1 :

Thème	Contenu	Nbr. d'heures	Objectifs
13	Conteneurisation et systèmes mobiles : • Conteneurisation avec Docker, risques associés et bonnes pratiques de sécurité • Introduction aux systèmes mobiles et sécurité associée • *Mobile Device Management* • *Mobile Application Management*	3	

2 Organisation

Cette section propre à l'approche pédagogique de chaque enseignante ou enseignant présente la méthode pédagogique, le calendrier, le barème et la procédure d'évaluation ainsi que l'échéancier des travaux. Cette section doit être cohérente avec le contenu de la section précédente.

2.1 Méthode pédagogique

Le cours INF803 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 Teams et les forums de discussion.

Puisqu'il s'agit d'un cours en ligne, toutes les ressources et les consignes sont disponibles sur Moodle : https ://moodle.usherbrooke.ca

2.2 Calendrier

Semaine	Commençant le	Thème
1	2026-01-05	1
2	2026-01-12	2
3	2026-01-19	Activités étudiantes
4	2026-01-26	3
5	2026-02-02	4
6	2026-02-09	5
7	2026-02-16	6
8	2026-02-23	7
9	2026-03-02	Relâche
10	2026-03-09	8
11	2026-03-16	9
12	2026-03-23	10
13	2026-03-30	11
14	2026-04-06	12
15	2026-04-13	13
16	2026-04-20	Semaine des examens finals
17	2026-04-27	Semaine des examens finals

2.3 Évaluation

Type de l'évaluation	Pondération	Utilisation des IAG[1]
Quiz	10 %	Interdite
Discussions	5 %	Interdite
Examen intra	40 %	Interdite
Examen final	45 %	Interdite

[1] Référez-vous à la page "Balises d'utilisation des outils d'intelligence artificielle générative" à la fin du document.

Type d'évaluation	**Pondération**	**Utilisation des IAG**
Quiz (séances : 3, 7, 10, 12 et 13)	**10 %**	**Interdite**
Participation aux forums	**5 %**	**Interdite**
Projet 1	**40 %**	**Interdite**
Examen final	**45 %**	**Interdite**

2.3.1 Qualité de la langue et de la présentation

Conformément à l'article 17 du Règlement facultaire d'évaluations des apprentissages[2] l'enseignante ou l'enseignant peut retourner à l'étudiante ou à l'étudiant tout travail non conforme aux exigences quant à la qualité de la langue et aux normes de présentation.

2.3.2 Plagiat

Le plagiat consiste à utiliser des résultats obtenus par d'autres personnes afin de les faire passer pour sien et dans le dessein de tromper l'enseignante ou l'enseignant. Vous trouverez en annexe un document d'information relatif à l'intégrité intellectuelle qui fait état de l'article 9.4.1 du Règlement des études[3]. Lors de la correction de tout travail individuel ou de groupe une attention spéciale sera portée au plagiat. Si une preuve de plagiat est attestée, elle sera traitée en conformité, entre autres, avec l'article 9.4.1 du Règlement des études de l'Université de Sherbrooke. L'étudiante ou l'étudiant peut s'exposer à de graves sanctions qui peuvent être soit l'attribution de la note E ou de la note zéro (0) pour un travail, un examen ou une activité évaluée, soit de reprendre un travail, un examen ou une activité pédagogique. Tout travail suspecté de plagiat sera transmis au Secrétaire de la Faculté des sciences. Ceci n'indique pas que vous n'ayez pas le droit de coopérer entre deux équipes, tant que la rédaction finale des documents et la création du programme restent le fait de votre équipe. En cas de doute de plagiat, l'enseignante ou l'enseignant peut demander à l'équipe d'expliquer les notions ou le fonctionnement du code qu'elle ou qu'il considère comme étant plagié. En cas d'incertitude, ne pas hésiter à demander conseil et assistance à l'enseignante ou l'enseignant afin d'éviter toute situation délicate par la suite.

2.4 Échéancier des travaux

Les dates de remise des travaux seront indiquées sur les énoncés.

[2] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/2017-10-27_Reglement_facultaire_-_evaluation_des_apprentissages.pdf

[3] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

2.5 Utilisation d'appareils électroniques et du courriel

Selon le règlement complémentaire des études, section 4.2.3 [4], l'utilisation d'ordinateurs, de cellulaires ou de tablettes pendant une prestation est interdite à condition que leur usage soit explicitement permise dans le plan de cours.

Dans ce cours, l'usage de téléphones cellulaires, de tablettes ou d'ordinateurs est autorisé. Cette permission peut être retirée en tout temps si leur usage entraîne des abus.

Tel qu'indiqué dans le règlement universitaire des études, section 4.2.3[5], toute utilisation d'appareils de captation de la voix ou de l'image exige la permission de la personne enseignante.

Note : Je réponds aux questions posées par courriel à l'extérieur des périodes de cours.

3 Matériel nécessaire pour l'activité pédagogique

- Moodle est utilisé pour le partage des notes de cours.
- Microsoft Teams sert à organiser les rencontres en ligne.
- Le forum Moodle est dédié aux échanges sur divers sujets liés au cours.

[4] https://www.usherbrooke.ca/sciences/fileadmin/sites/sciences/documents/Etudiants_actuels/Informations_academiques_et_reglements/Sciences_Reglement_complementaire.pdf

[5] https://www.usherbrooke.ca/registraire/droits-et-responsabilites/reglement-des-etudes/

Faculté des sciences UdS

Délits relatifs aux études

Extrait du règlement des études (Règlement 2575-009)

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, des passages ou idées tirés de l'œuvre d'autrui ou du contenu, de toute forme, généré par un système d'intelligence artificielle (ce qui inclut notamment le fait de ne pas indiquer la source et la référence adéquate);
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 procéder à une substitution de personne lors d'une production évaluée ou de toute autre prestation obligatoire;
d) fournir ou obtenir toute forme d'aide non autorisée, qu'elle soit collective ou individuelle (incluant l'assistance provenant d'un système d'intelligence artificielle), pour une production faisant l'objet d'une évaluation;
e) obtenir par vol ou toute autre manœuvre frauduleuse, posséder ou utiliser du matériel non autorisé de toute forme (incluant le matériel numérique et celui généré par un système d'intelligence artificielle) avant ou pendant une production faisant l'objet d'une évaluation;
f) copier, contrefaire ou falsifier un document pour l'évaluation d'une activité pédagogique;
k) posséder ou avoir à sa portée un appareil électronique ou numérique interdit durant une activité d'évaluation;

[...]

Un guide sur l'intégrité intellectuelle vous est rendu disponible par le service des bibliothèques et des archives de l'Université de Sherbrooke, afin de bien comprendre les différents délits et ainsi éviter d'être aux prises avec un dossier disciplinaire et une ou des sanctions.

Les mesures pouvant être imposées à titre de sanctions disciplinaires sont les suivantes :

a) la réprimande simple ou sévère consignée au dossier étudiant pour la période fixée par l'autorité disciplinaire ou à défaut, définitivement. En cas de réprimande fixée pour une période déterminée, la décision rendue demeure au dossier de la personne aux seules fins d'attester de l'existence du délit en cas de récidive;
b) l'obligation de reprendre une production ou une activité pédagogique, dont la note pourra être établie en tenant compte du délit survenu antérieurement;
c) la diminution de la note ou l'attribution de la note E ou 0;

[...]

UDS Faculté des sciences

Balises d'utilisation des outils d'intelligence artificielle générative

Autorisés ou pas dans les situations d'apprentissage et d'évaluation ?

NIVEAU 0	NIVEAU 1	NIVEAU 2	NIVEAU 3	NIVEAU 4
L'utilisation des outils d'intelligence artificielle générative (IAg) est limitée, voire complètement interdite parce que la personne enseignante considère que l'usage de ces outils nuit au développement de compétences essentielles. Ces compétences peuvent être disciplinaires, comme elles peuvent être d'ordre méthodologique, rédactionnel ou informationnel. Considérant que l'utilisation des IAg requiert un esprit critique, il peut s'agir d'une situation d'apprentissage ou d'évaluation sans IAg qui vise à développer celui-ci. Dans ces situations, **la personne étudiante produit le travail**.			L'utilisation prononcée des IAg est permise parce que la personne enseignante considère que les personnes étudiantes sont en mesure d'exercer un esprit critique et sont capables de juger de la qualité des contenus produits par les IAg. Ou encore, l'utilisation est encouragée parce que la situation d'apprentissage ou d'évaluation proposée contribue à développer leur esprit critique. Dans ces situations, l'IAg produit le travail préliminaire, alors que **la personne étudiante s'assure de sa qualité en l'améliorant**.	
				
Utilisation interdite	**Utilisation limitée**	**Utilisation guidée**	**Utilisation balisée**	**Utilisation libre**
Le **NIVEAU 0** signifie que l'**utilisation est interdite**. Ceci signifie que si la personne enseignante a un motif de croire qu'il y a eu l'utilisation d'une IAg dans une situation d'évaluation, elle doit dénoncer les faits auprès de la personne responsable des dossiers disciplinaires universitaires. Il s'agit d'un délit relatif aux études tel que stipulé dans le Règlement des études.	Le **NIVEAU 1 D'UTILISATION** signifie que l'**utilisation est autorisée uniquement pour assister l'apprentissage dans le domaine disciplinaire ou des langues**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation peut être considérée comme un délit. Par exemple : Domaine disciplinaire : - S'inspirer - Générer des idées - Explorer un sujet pour mieux le comprendre - Générer du matériel pour apprendre Domaine des langues : - Identifier ses erreurs et se les faire expliquer - Reformuler un texte - Générer un plan pour aider à structurer un texte - Traduire un texte	Le **NIVEAU 2 D'UTILISATION** signifie que l'**utilisation est autorisée pour améliorer un travail produit par la personne étudiante**. Dans ce contexte, la personne étudiante **est tenue de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Analyser des contenus - Obtenir une rétroaction - Évaluer la qualité de son travail à partir de critères - Demander à être confronté relativement à ses idées, à sa démarche - Diriger les processus de résolution de problèmes	Le **NIVEAU 3 D'UTILISATION** signifie que l'**utilisation est autorisée pour produire un travail qui sera amélioré.** Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Par exemple : - Résumer ou rédiger des parties d'un texte - Générer un texte ou un modèle d'une production et l'adapter - Réaliser des calculs mathématiques - Produire du code informatique - Résoudre des problèmes complexes - Répondre à une question - Générer des images, ou autres contenus multimédias	Le **NIVEAU 4 D'UTILISATION** signifie qu'**aucune restriction spécifique n'est imposée**. Dans ce contexte, la personne étudiante **est tenue de citer selon les normes[1] le contenu généré par l'IAg** ou **de déclarer l'utilisation qu'elle en a faite** selon les consignes fournies par la personne enseignante sans quoi l'utilisation est considérée comme un délit. Ce niveau inclut tout ce qui précède, de l'exploration à la production, ainsi que toute autre tâche particulière jugée complexe.

UDS Faculté des sciences

À considérer avant l'utilisation d'outils d'intelligence artificielles génératives

Si, en tant que personne étudiante envisagez d'utiliser un outil d'intelligence artificielle générative (IAG) lorsque l'évaluation autorise les niveaux 1 à 4 d'utilisation mentionnés précédemment.

Dans ce cas, gardez à l'esprit les éléments clés suivants.

- Vous assumez la responsabilité de tout le contenu produit, avec ou sans IAG, et intégré à votre production.
- Les produits des outils d'IAG peuvent très souvent comporter **des erreurs ou des faussetés** (hallucinations) : on doit donc impérativement valider tout contenu généré par ces outils.
- Dans l'état actuel de la Loi sur le droit d'auteur du Canada, les **productions faites par l'IAG sont du domaine public,** puisque les outils d'IAG ne sont pas reconnus comme des auteurs au sens de la Loi et que les contenus générés ne répondent pas aux critères d'une œuvre protégée, notamment aux critères d'originalité.
- L'entreprise qui fournit le service pourrait émettre certaines exigences dans ses conditions d'utilisation. Comme l'algorithme et le code informatique appartiennent à l'entreprise qui les a développés, nous devons tenir compte de ces conditions. Celles-ci pourraient également fournir des précisions relatives à la **réutilisation des données soumises (confidentialité)**.

Comment déclarer l'utilisation d'outils d'intelligence artificielle générative

Dans l'esprit d'une conduite intègre et responsable, vous devez TOUJOURS mentionner de façon explicite toute utilisation de l'intelligence artificielle, conformément au Règlement des études (9.4.1 Délits relatifs aux études). De plus, à des fins pédagogiques, il est recommandé de toujours intégrer à la production les requêtes, de même que les réponses intégrales générées par les outils d'IAG. Celles-ci pourront être intégrées directement dans le corps du texte ou en note de bas de page. Les réponses longues pourraient être insérées en annexe de votre document ou dans des documents supplémentaires, selon les directives de la personne enseignante.

L'utilisation de ces deux documents s'avèrera utile, ils se trouvent sous licence libre, donc vous pouvez utiliser les tableaux et les adapter selon votre besoin:

1. Modèle de citation : Ce formulaire, à remplir par l'enseignant, donne un exemple aux étudiants de citation de l'IAg dans la réalisation d'un travail évalué ou non.
2. Déclaration d'usage : Ce formulaire, à remplir par les étudiants, doit être remis avec une réalisation afin de déclarer l'usage de l'IAg dans la réalisation, qu'elle soit évaluée ou non.

Référence

La Faculté des sciences tient à remercier le SSF pour la production des documents.

- Cabana, M. et Côté, J.-A. (2024). Balises d'utilisation des outils d'intelligence artificielle générative. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. et Beaudet, M. (2024). Directives de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.
- Cabana, M. (2024). Formulaire de déclaration de l'utilisation de l'intelligence artificielle générative dans une production étudiante. Service de soutien à la formation, Université de Sherbrooke. Sous licence CC BY 4.0.