Projet 1 – Audit et Plan d'Action pour la Cybersécurité de

E-Commerce Express

Cours INF1753 – Pratique professionnelle et communication en informatique

Professeur : Dr. N'dah Daniel Yapi

Automne 2025

Contexte du projet

E-Commerce Express est une entreprise fictive en pleine croissance spécialisée dans la vente en ligne d'articles de sport. Son succès a conduit à une augmentation du volume des transactions et de la collecte de données personnelles de ses clients (noms, adresses, informations de paiement).

Récemment, l'entreprise a connu une tentative de cyberattaque qui a mis en lumière des vulnérabilités dans ses systèmes de sécurité et ses pratiques de gestion des données.

Votre équipe est engagée en tant que **consultants en cybersécurité et conformité des données** pour réaliser un audit complet de leurs pratiques actuelles et proposer un plan d'action détaillé pour renforcer leur sécurité et garantir leur conformité. L'objectif est de sécuriser l'entreprise contre de futures menaces et de rassurer ses clients sur la protection de leurs informations.

Objectifs pédagogiques

- Identifier les risques liés à la gestion des données personnelles et à la cybersécurité.
- Appliquer les principes d'éthique, de confidentialité et de conformité légale.
- Intégrer les **normes professionnelles et réglementaires** (Loi 25, LPRPDE, ISO 27001, ACM/IEEE).
- Initier les étudiants à l'usage de **Git et GitHub** comme outils de collaboration et de versionnement.

— Présenter des recommandations concrètes pour un environnement numérique plus sûr et responsable.

Tâche demandée

En équipe de 7 à 8 personnes, vous devez produire un **rapport professionnel complet d'audit de cybersécurité** pour l'entreprise **E-Commerce Express**. Le travail comporte les quatre volets suivants :

1. **Diagnostic de la situation actuelle**
   - Identifier les actifs informationnels critiques (infrastructures, données, utilisateurs).
   - Évaluer les principaux risques (techniques, humains et organisationnels).
   - Mentionner les normes et cadres de référence pertinents (ISO 27001, Loi 25, LPRPDE).
2. **Analyse éthique, légale et de confidentialité**
   - Examiner la conformité aux lois canadiennes et provinciales sur la protection des renseignements personnels.
   - Identifier les obligations et responsabilités légales de l'entreprise en cas d'incident.
   - Discuter des dilemmes éthiques associés à la surveillance, à la gestion des accès et à la collecte de données.
3. **Plan d'action et recommandations**
   - Proposer des mesures préventives et correctives (sécurité technique, politique interne, formation).
   - Élaborer un plan de sensibilisation du personnel à la cybersécurité.
   - Présenter un échéancier sommaire sous forme de tableau ou de diagramme de Gantt.
4. **Documentation et collaboration**
   - Décrire brièvement la méthode de collaboration utilisée (ex. : partage via GitHub, Drive, etc.).
   - Créer, au minimum, un **dépôt GitHub de test** contenant une version du rapport ou du plan d'action.
   - Expliquer en quelques lignes l'intérêt du versionnement collaboratif pour un projet professionnel.

Livrables attendus

— **Rapport écrit (15 – 20 pages)** : format PDF, structuré selon les standards professionnels.

— **Annexes techniques** : tableaux de risques, diagrammes, organigramme de sécurité, extraits de documentation.

— **Présentation orale (12 – 15 minutes)** : support visuel clair et concis (Beamer, PowerPoint ou Canva). *Cette présentation compte pour 20 points dans la grille de notation.*

— **Capture d'écran ou lien du dépôt GitHub de test** (facultatif : pour montrer la compréhension du principe).

Pondération indicative

Éléments d'évaluation	**Points / 100**
Analyse et diagnostic de la cybersécurité	27
Respect des normes éthiques et légales	20
Plan d'action et pertinence des recommandations	23
Qualité de la documentation et utilisation de Git/GitHub	10
Présentation orale (clarté, structure, maîtrise du contenu)	20
Total	**100 pts**

Consignes générales

— Le travail est à réaliser en équipe (7 à 8 membres). Une fiche de répartition des rôles peut être jointe en annexe.

— Toute source d'information ou tout texte repris doit être cité (APA 7 ou IEEE).

— L'usage d'outils d'IA générative doit être déclaré et justifié.

— Le rapport doit être rédigé en français clair, justifié, exempt de fautes, et respecter les politiques linguistiques de l'UQO.

— Les figures et schémas doivent être originaux ou correctement référencés.

Annexes suggérées

— Annexe A : Tableau d'évaluation des risques (probabilité × impact).

— Annexe B : Organigramme des responsabilités et rôles (ex. : Responsable sécurité, Chef de projet, etc.).

— Annexe C : Exemple de page README ou de capture GitHub.

— Annexe D : Plan sommaire de formation du personnel à la cybersécurité.

Remise : Semaine 14 (01 décembre 2025) via Moodle.