UNIVERSITÉ DU QUÉBEC EN OUTAOUAIS

Projet 1 – Audit et Plan d'Action pour la Cybersécurité de E-Commerce Express

Examen Final

Présenté à

Daniel N'dah Yapi

Par

Groupe 2

Ali, Habone Hassan

Barry, Mamadou Bhoye

Biongele, André Mataka

Ebatha-Franck, Brandon

Ibekourene, Lydia

Lyrette, Félix

Mboudi Pwemeu, Franck Arthur

Tadjou, Anzizatou

Département d'informatique et d'ingénierie

INF1753 – Pratique professionnelle et communication en informatique

Gatineau

1 Décembre 2025

TABLE DES MATIÈRES

RÉSUMÉ EXÉCUTIF iii

Constatations principales : iii

Recommandations prioritaires : iii

INTRODUCTION 1

Contexte et enjeux 1

Objectifs de l'audit 1

Méthodologie 1

1. DIAGNOSTIC DE LA SITUATION ACTUELLE 2

1.1 ACTIFS INFORMATIONNELS CRITIQUES 2

a) Infrastructures technologiques 2

b) Données sensibles 2

c) Utilisateurs et accès 3

1.2 ÉVALUATION DES PRINCIPAUX RISQUES 3

a) Risques techniques 3

b) Risques humains 4

c) Risques organisationnels 4

1.3 NORMES ET CADRES DE RÉFÉRENCE PERTINENTS 4

a) Normes internationales 4

b) Cadre légal canadien 5

c) Cadre légal québécois 5

2. ANALYSE ÉTHIQUE, LÉGALE ET DE CONFIDENTIALITÉ 5

2.1 CONFORMITÉ AUX LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS 6

2.2 OBLIGATIONS LÉGALES EN CAS D'INCIDENT DE SÉCURITÉ 7

2.3 DILEMMES ÉTHIQUES LIÉS À LA CYBERSÉCURITÉ ET À LA COLLECTE DE DONNÉES 8

a) Surveillance des employés 8

b) Gestion des accès 8

c) Collecte et usage des données 9

3. PLAN D'ACTION ET RECOMMANDATIONS 9

3.1 MESURES PRÉVENTIVES ET CORRECTIVES 9

3.1.1 Sécurité technique (priorité CRITIQUE) 9

3.1.2 Politiques internes (priorité élevée) 11
3.1.3 Organisation (priorité ÉLEVÉE) 13
3.2 PLAN DE SENSIBILISATION DU PERSONNEL 14
3.2.1 Programme de formation 14
3.2.2 Campagnes de sensibilisation continue 15
3.2.3 Mesure de l'efficacité 16
3.3 ÉCHÉANCIER DU PLAN D'ACTION 16
3.3.1 Diagramme de Gantt – Phase 1 (6 mois) 16
3.3.2 Phase 2 (6-12 mois) : consolidation 17
3.3.3 Phase 3 (12-24 mois) : amélioration continue 17
3.4 BUDGET PRÉVISIONNEL 17
3.5 INDICATEURS DE SUCCÈS (KPI) 17
CONCLUSION 17
4. DOCUMENTATION ET COLLABORATION 18
4.1 MÉTHODE DE COLLABORATION UTILISÉE 18
4.2 CRÉER UN DÉPÔT GITHUB 18
4.3 EXPLIQUER L'INTÉRÊT DU VERSIONNEMENT COLLABORATIF 18
BIBLIOGRAPHIE 19
ANNEXES 20
Annexe A – Budget prévisionnel 20
Annexe B – Indicateurs de succès (KPI) 21
Annexe C – Tableau d'évaluation des risques (probabilité × impact) 22
Annexe E – Capture GitHub 23
Annexe F – Contributions individuelles 24

RÉSUMÉ EXÉCUTIF

L'entreprise E-Commerce Express, entreprise spécialisée dans la vente en ligne d'articles de sport, fait face à des défis critiques en matière de cybersécurité et de protection des données personnelles. À la suite d'une tentative de cyberattaque récente, cet audit identifie les vulnérabilités majeures, évalue la conformité réglementaire et propose un plan d'action structuré pour sécuriser les actifs informationnels de l'entreprise et restaurer la confiance des clients.

Constatations principales :

- Vulnérabilités techniques dans l'infrastructure de sécurité.
- Non-conformité partielle avec la Loi 25 et la LPRPDE.
- Absence de politiques formelles de gestion des incidents.
- Manque de sensibilisation du personnel aux risques cyber

Recommandations prioritaires :

- Mise en œuvre immédiate d'un système de gestion de la sécurité de l'information (SGSI).
- Programme de formation obligatoire en cybersécurité
- Conformité complète aux exigences légales sous 6 mois

INTRODUCTION

Contexte et enjeux

E-Commerce Express est en pleine croissance, et cette expansion s'accompagne d'une hausse importante de la quantité de données personnelles que l'entreprise doit gérer. Elle recueille des informations sensibles comme les données d'identification (noms, adresses, coordonnées), des données financières comme les cartes de crédit ou les historiques de paiement, ainsi que des données comportementales liées aux habitudes d'achat et aux préférences des clients.

La récente tentative de cyberattaque a mis en lumière des failles importantes, ce qui montre qu'il est urgent d'agir pour protéger les actifs informationnels et assurer la continuité de l'entreprise.

Objectifs de l'audit

1. Évaluer l'état actuel de la sécurité informatique et de la gestion des données
2. Identifier les risques techniques, humains et organisationnels
3. Vérifier la conformité aux cadres réglementaires applicables
4. Proposer un plan d'action structuré et réaliste
5. Établir une feuille de route pour l'amélioration continue

Méthodologie

Notre approche s'appuie sur plusieurs références importantes dans le domaine. D'abord, on se base sur la norme internationale ISO/IEC 27001, qui sert de cadre pour gérer efficacement la sécurité de l'information. On tient aussi compte de la Loi 25 au Québec, qui modernise les règles de protection des renseignements personnels, ainsi que de la LPRPDE au niveau canadien. Enfin, on s'inspire des codes d'éthique de l'ACM et de l'IEEE, qui offrent des principes professionnels essentiels en informatique.

1. DIAGNOSTIC DE LA SITUATION ACTUELLE

1.1 ACTIFS INFORMATIONNELS CRITIQUES

Les actifs informationnels critiques englobent toutes les ressources nécessaires à la survie et à la sécurité d'une entreprise. Dans le cas d'E-Commerce Express, on parle des infrastructures informatiques, des données personnelles et transactionnelles recueillies auprès des clients, ainsi que des utilisateurs et autres collaborateurs qui ont accès aux systèmes, comme les administrateurs, les fournisseurs et les partenaires. Il est crucial d'identifier et de protéger ces actifs pour assurer la continuité des opérations, maintenir la confiance des clients et respecter les obligations réglementaires.

a) Infrastructures technologiques

E-Commerce Express repose sur plusieurs infrastructures technologiques essentielles au fonctionnement de sa plateforme d'e-commerce. Les serveurs web et les bases de données hébergent le site transactionnel ainsi que l'ensemble des informations relatives aux clients. Les systèmes de paiement et les partenaires, qui se connectent à des services financiers externes, constituent des composants critiques nécessitant une sécurité renforcée. Le réseau interne, incluant les postes de travail des employés, les routeurs, les commutateurs, les pare-feu et les solutions de sauvegarde, est indispensable pour assurer la continuité des opérations et la disponibilité des services.

b) Données sensibles

Les données personnelles collectées par E-Commerce Express, telles que les noms, adresses et informations de paiement des clients, représentent un actif informationnel hautement sensible. La protection de ces données est essentielle pour prévenir le vol d'identité, la fraude, les fuites et pour respecter les législations sur la protection des données personnelles. Les informations financières, même lorsqu'elles sont chiffrées, demeurent critiques, car leur compromission pourrait entraîner des conséquences graves pour les clients. En plus des données

clients, les historiques d'achats, les données de navigation et les informations transactionnelles doivent aussi être sécurisées car elles ont une valeur stratégique pour l'entreprise et ses clients. L'entreprise détient également des données internes telles que des informations administratives, des documents liés aux ressources humaines et des données financières.

c) Utilisateurs et accès

Les utilisateurs critiques de l'entreprise englobent les clients ainsi que les employés et autres collaborateurs ayant accès aux systèmes et aux données. Cela inclut les gestionnaires du site web, les responsables IT, les équipes de service clientèle, et tout personnel technique disposant de comptes privilégiés. La gestion rigoureuse des accès utilisateurs, avec authentification forte et contrôle des droits, est indispensable pour limiter les risques d'intrusion interne ou d'exploitation des comptes compromis par des cybercriminels. Les clients eux-mêmes représentent un vecteur potentiel d'attaque, puisqu'ils peuvent être ciblés par des campagnes d'hameçonnage ciblant leurs comptes. Une mauvaise gestion des accès ou des privilèges pourrait exposer l'entreprise à des risques de compromission.

1.2 ÉVALUATION DES PRINCIPAUX RISQUES

a) Risques techniques

E-Commerce Express fait face à des risques techniques tels que les vulnérabilités dans ses systèmes informatiques. Ces failles peuvent être exploitées par des pirates pour accéder frauduleusement aux données sensibles des clients (informations personnelles, données bancaires). De plus, les attaques par déni de service (DDoS) pouvant ralentir ou interrompre les opérations de vente en ligne, le malware et les ransomwares représentant des menaces à la disponibilité et à l'intégrité des systèmes sont aussi à prendre en compte. Des mises à jour insuffisantes peuvent laisser des portes ouvertes à l'exploitation de vulnérabilités connues. Une application inadéquate du chiffrement des données, que ce soit en transit ou au repos, peut exposer l'entreprise à des interceptions ou à des fuites de données. De plus, l'entreprise est sujette à des menaces susceptibles de rendre la plateforme inaccessible. Le besoin de sécuriser les connexions réseau, les mises à jour régulières et la gestion des accès est donc essentiel.

b) Risques humains

Les risques humains proviennent principalement du comportement et des connaissances des utilisateurs internes. Les erreurs de manipulation comme la suppression accidentelle de données ou la mauvaise utilisation d'outils peuvent entraîner des pertes ou des interruptions. Le manque de formation en cybersécurité augmente la probabilité que des employés tombent victimes de tentatives de phishing. L'utilisation de mots de passe faibles ou réutilisés expose l'entreprise à des intrusions potentielles. Même les clients peuvent représenter des vecteurs de risque lorsqu'ils sont ciblés par des attaques cherchant à voler leurs identifiants. Ce facteur humain est souvent le maillon faible des systèmes de sécurité, nécessitant des formations régulières et une culture de sécurité forte.

c) Risques organisationnels

Les risques organisationnels incluent l'absence de politiques claires de sécurité des données, de procédures de gestion des incidents et d'audit régulier. Une gouvernance déficiente peut conduire à un manque de coordination entre les équipes IT, juridique et opérationnelle, et à une mauvaise gestion des tiers prestataires qui ont accès aux systèmes. Le non-respect des réglementations sur la protection des données expose également l'entreprise à des sanctions légales et à une perte de confiance des clients. Enfin, le manque de plans de continuité et de reprise après incident exacerbe la vulnérabilité face aux attaques.

1.3 NORMES ET CADRES DE RÉFÉRENCE PERTINENTS

Afin de renforcer la sécurité et de garantir la conformité d'E-Commerce Express, il est important de s'appuyer sur des normes et des cadres de référence reconnus.

a) Normes internationales

La norme ISO/IEC 27001 constitue la référence mondiale en matière de gestion de la sécurité de l'information. Elle propose un cadre structuré pour évaluer les risques, définir des

politiques de sécurité, mettre en place des contrôles, assurer la gouvernance et instaurer un cycle d'amélioration continue. Son application permet d'uniformiser les pratiques et de renforcer la maturité sécuritaire de l'organisation. (International Organization for Standardization, 2022)

b) Cadre légal canadien

Au niveau fédéral, E-Commerce Express est soumise à la LPRPDE. Cette loi oblige les organisations à obtenir le consentement des individus avant de recueillir leurs renseignements personnels, à assurer des mesures de sécurité proportionnelles à la sensibilité des données, et à déclarer les atteintes présentant un risque réel de préjudice grave. Elle encadre également l'usage, la conservation et la destruction des données personnelles. (Commissariat à la protection de la vie privée du Canada, 2025)

c) Cadre légal québécois

Au Québec, la Loi 25 modernise la législation relative à la protection des renseignements personnels. Elle impose notamment la désignation d'un responsable de la protection des renseignements personnels, la réalisation d'évaluations des facteurs relatifs à la vie privée (EFVP), la mise en place de politiques de confidentialité, la minimisation des données et l'obligation de notifier les incidents aux personnes concernées et à la Commission d'accès à l'information. Cette loi renforce les responsabilités des organisations et exige une transparence accrue dans la gestion des données. (Gouvernement du Québec, 2025).

2. ANALYSE ÉTHIQUE, LÉGALE ET DE CONFIDENTIALITÉ

Aujourd'hui, je vais vous présenter une analyse légale, éthique et de confidentialité concernant le cas d'E-Commerce Express, une entreprise de commerce en ligne qui traite des renseignements personnels comme les noms, adresses et informations de paiement de ses clients. La récente tentative de cyberattaque qu'elle a subie soulève des questions importantes sur sa conformité aux lois, sa gestion des incidents et les dilemmes éthiques liés à l'utilisation des données.

2.1 CONFORMITÉ AUX LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

D'abord, sur le plan légal, E-Commerce Express est soumise aux lois sur la protection des renseignements personnels, puisqu'elle collecte et utilise des données de clients dans un contexte commercial.

Au niveau fédéral, la loi principale est la LPRPDE, aussi appelée PIPEDA. Cette loi s'applique aux organisations privées qui collectent, utilisent ou communiquent des renseignements personnels. Elle impose plusieurs obligations : obtenir un consentement valable de la part des clients, limiter la collecte au strict nécessaire pour des fins précises comme le traitement des commandes ou la facturation, mettre en place des mesures de sécurité appropriées en fonction de la sensibilité des données, ce qui est crucial ici puisqu'il s'agit d'informations de paiement, et permettre aux clients d'accéder à leurs renseignements, de les faire corriger et de savoir comment ils sont utilisés. La LPRPDE prévoit aussi l'obligation de déclarer toute atteinte à la vie privée qui présente un risque réel de préjudice sérieux, à la fois aux autorités compétentes et aux personnes concernées.

Au niveau provincial, par exemple au Québec, la Loi 25 vient renforcer ces exigences. Si E-Commerce Express opère au Québec ou traite avec des clients québécois, elle doit notamment désigner un responsable de la protection des renseignements personnels, réaliser des évaluations des facteurs relatifs à la vie privée pour tout projet impliquant des données sensibles, limiter strictement l'accès aux données aux personnes qui en ont réellement besoin (besoin de savoir), encadrer les transferts de données à l'extérieur du Québec et se conformer à un régime de sanctions financières importantes en cas de non-respect.

Le constat, pour E-Commerce Express, est que la tentative de cyberattaque met en lumière des vulnérabilités. Si les mesures de sécurité en place ne sont pas jugées « raisonnables

» au regard de la sensibilité des données, l'entreprise pourrait être considérée comme non conforme à ses obligations légales.

2.2 OBLIGATIONS LÉGALES EN CAS D'INCIDENT DE SÉCURITÉ

Ensuite, la question est de savoir ce que doit faire E-Commerce Express lorsqu'un incident survient ou même lorsqu'il est seulement suspecté.

D'une part, l'entreprise a une obligation de gestion et de documentation des incidents. Concrètement, elle doit être capable de détecter, consigner et analyser tout incident de sécurité touchant des renseignements personnels. Cela suppose la tenue d'un registre des incidents, où l'on note la nature de l'attaque, les données visées, les mesures prises et les leçons tirées. Cela implique également la mise en place d'un plan de réponse aux incidents, avec des procédures internes claires, des rôles bien définis et une communication rapide en cas de problème.

D'autre part, elle a aussi une obligation de notification. En cas d'atteinte avérée qui présente un risque réel de préjudice sérieux, par exemple une fuite ou un accès non autorisé à des informations de paiement, l'entreprise doit prévenir les autorités compétentes comme le Commissariat à la protection de la vie privée du Canada ou la Commission d'accès à l'information au Québec et informer les clients touchés. Cette notification doit expliquer la nature de l'incident, le type d'informations compromises, les mesures prises pour corriger la situation, ainsi que des recommandations aux clients, comme surveiller leurs comptes ou changer leurs mots de passe.

En cas de manquement, la responsabilité civile et administrative de l'entreprise peut être engagée. Si l'incident est lié à une absence de chiffrement, à un manque de mises à jour ou à un mauvais contrôle des accès, l'entreprise peut être poursuivie pour négligence. Les autorités peuvent imposer des amendes ou des ordonnances correctives, et la réputation de l'organisation peut être sérieusement atteinte, avec des conséquences économiques : perte de confiance et baisse des ventes. En résumé, E-Commerce Express a l'obligation légale non seulement de réagir

à l'incident, mais aussi de pouvoir démontrer qu'elle avait mis en place des mesures de sécurité raisonnables, documentées et proportionnées avant même que l'incident ne survienne.

2.3 DILEMMES ÉTHIQUES LIÉS À LA CYBERSÉCURITÉ ET À LA COLLECTE DE DONNÉES

Au-delà des obligations légales, le cas d'E-Commerce Express soulève plusieurs dilemmes éthiques.

a) Surveillance des employés

Le premier concerne la surveillance des employés. Pour prévenir les abus, comme les accès non autorisés ou les fuites internes, l'entreprise peut être tentée de renforcer la surveillance des activités sur ses systèmes : journaux d'accès, suivi des connexions, etc. Mais sur le plan éthique, il y a un équilibre délicat à trouver. Une surveillance excessive peut porter atteinte à la vie privée des employés, créer un climat de méfiance et ouvrir la porte à des dérives comme le profilage interne.

À l'inverse, une surveillance insuffisante augmente les risques de fuites de données et rend plus difficile l'identification des responsables. La position éthique recommandée consiste à être transparent sur les outils de surveillance, à se limiter à ce qui est nécessaire pour la sécurité et à miser sur la formation, la sensibilisation et la responsabilisation plutôt que sur un contrôle systématique.

b) Gestion des accès

Le deuxième enjeu concerne la gestion des accès, souvent formulée comme le principe du « moindre privilège ». Les informations de paiement et les données personnelles ne devraient être accessibles qu'aux employés dont le travail l'exige réellement. Là encore, un dilemme apparaît : si les accès sont trop restreints, cela peut ralentir le service à la clientèle et la gestion des commandes ; s'ils sont trop larges, le risque de fuite, d'erreur ou d'abus augmente. Éthiquement, la bonne approche consiste à définir des rôles et profils d'accès (RBAC), à revoir

régulièrement les droits attribués et à journaliser les accès aux données sensibles pour pouvoir les auditer.

c) Collecte et usage des données

Enfin, un troisième ensemble de dilemmes éthiques concerne la collecte et l'usage des données. E-Commerce Express peut être tentée de collecter beaucoup d'informations sur les préférences, l'historique d'achat ou la navigation des utilisateurs pour améliorer la personnalisation et les ventes. Cependant, collecter plus que nécessaire va à l'encontre du principe de minimisation et peut être perçu comme intrusif. L'utilisation de ces données pour un profilage très poussé, un ciblage agressif ou des segmentations sensibles peut aussi devenir manipulatoire.

On peut alors se demander si le client comprend vraiment ce qu'il accepte lorsqu'il clique sur « J'accepte ». D'un point de vue éthique, il est préférable de se limiter aux données nécessaires à la prestation du service, de rendre les politiques de confidentialité claires et compréhensibles, d'obtenir un consentement vraiment éclairé, par exemple pour l'envoi de promotions, et d'anonymiser ou de pseudonymiser les données lorsqu'il n'est pas indispensable d'identifier les personnes.

3. PLAN D'ACTION ET RECOMMANDATIONS

3.1 MESURES PRÉVENTIVES ET CORRECTIVES

3.1.1 Sécurité technique (priorité CRITIQUE)

3.1.1.1 Renforcement du chiffrement

Le renforcement du chiffrement constitue la première mesure de sécurité technique à mettre en œuvre. L'action consiste à généraliser HTTPS sur l'ensemble du site web et à implémenter le protocole TLS 1.3, qui offre une meilleure protection contre les attaques contemporaines. Cette mesure représente un coût estimé entre 2 000 et 5 000 dollars

américains, avec un délai de mise en œuvre de deux semaines. L'équipe infrastructure demeure responsable de son exécution.

3.1.1.2 Authentification multifacteur

L'authentification multifacteur (MFA) représente une mesure de sécurité essentielle pour les comptes sensibles. L'action proposée consiste à déployer cette technologie pour tous les comptes employés, tout en l'offrant en option aux clients. Le coût estimé pour la licence et l'intégration se situe entre 5 000 et 10 000 dollars, avec un délai d'un mois. L'administrateur système supervise cette implémentation.

3.1.1.3 Gestion des correctifs

La gestion proactive des correctifs de sécurité s'avère cruciale pour maintenir l'intégrité des systèmes. L'action proposée est d'établir un processus de patch management automatisé, réduisant ainsi les risques liés aux vulnérabilités connues. Le coût initial s'élève à 3 000 dollars, augmenté de frais mensuels de 500 dollars pour les outils nécessaires. Le délai de mise en place est estimé à six semaines, sous la responsabilité de l'équipe IT.

3.1.1.4 Système SIEM

L'implémentation d'une solution de surveillance et d'analyse des logs (SIEM) permet une détection précoce des anomalies de sécurité. Cette infrastructure centralise la surveillance de l'ensemble des événements systèmes et réseau. Le coût annuel se situe entre 15 000 et 30 000 dollars, avec un délai de déploiement de deux mois. Cette responsabilité sera confiée au RSSI (Responsable de la Sécurité de l'Information), poste à recruter.

3.1.1.5 Pseudonymisation

Pseudonymisation : technique qui consiste à remplacer les renseignements personnels faciles à identifier par un pseudonyme. Elle permet le traitement des données sans pouvoir identifier la personne.

3.1.1.6 Segmentation réseau

La segmentation des environnements informatiques représente une stratégie de défense en profondeur efficace. L'action consiste à séparer physiquement ou logiquement les environnements de production, développement et administration, limitant ainsi la propagation d'une compromission potentielle.

3.1.1.7 Tests de pénétration

Les tests de pénétration offrent une évaluation externe et objective de la posture de sécurité. L'action proposée est de réaliser un audit de sécurité externe annuellement, effectué par un consultant spécialisé.

3.1.1.8 Sauvegardes sécurisées

La mise en œuvre d'une stratégie de sauvegarde robuste garantit la continuité des opérations en cas de sinistre. L'action consiste à implémenter la règle 3-2-1 : maintenir trois copies des données, sur deux supports de stockage différents, avec une copie stockée hors site.

3.1.2 Politiques internes (priorité élevée)

3.1.2.1 Politique de sécurité de l'information

La politique de sécurité de l'information constitue le cadre normatif fondamental de l'organisation. Elle doit établir les règles d'utilisation des systèmes, définir les normes de gestion des mots de passe, et classifier les données selon leur sensibilité. Le délai de rédaction et d'approbation est estimé à un mois, avec une révision prévue annuellement pour assurer son adéquation avec l'évolution des menaces.

3.1.2.2 Politique de confidentialité

La mise à jour de la politique de confidentialité s'avère nécessaire pour assurer la conformité réglementaire et la transparence envers les utilisateurs. Le contenu doit présenter un langage clair, énoncer les finalités précises du traitement des données, expliciter les droits des personnes concernées, et fournir les coordonnées du responsable du traitement. Le délai de

révision est estimé à trois semaines, avec une révision semestrielle pour incorporer les changements normatifs.

3.1.2.3 Politique de gestion des incidents

La gestion structurée des incidents de sécurité minimise leur impact opérationnel et réputationnel. Cette politique doit définir les procédures de détection, d'escalade, de notification interne et externe, ainsi que de remédiation. Le délai de rédaction est d'un mois, complété par un exercice de simulation planifié trois mois après l'adoption, permettant aux équipes de tester leur réactivité.

3.1.2.4 Politique de gestion des accès

La politique de gestion des accès formalise le principe du moindre privilège, un fondamental de la sécurité informatique. Elle doit établir le processus d'attribution, de modification et de révocation des accès, ainsi que prévoir une revue trimestrielle des droits actifs. Le délai de mise en place est d'un mois, avec une révision trimestrielle garantissant l'adéquation des accès aux fonctions.

3.1.2.5 Politique de conservation des données

La conservation appropriée des données répond à la fois à des enjeux de sécurité et de conformité légale. Cette politique établit les durées de conservation par type de données et définit la procédure de suppression automatique à l'expiration de ces délais. Le délai de rédaction est de six semaines, avec une révision annuelle.

3.1.2.6 Classification

Classification : la classification est une politique interne en rapport avec la méthode de catégorisation des informations en fonction de leur sensibilité et de leur valeur dans une organisation. Ce processus aide à définir les niveaux d'accès et les mesures de sécurité à appliquer pour protéger les données,

3.1.3 Organisation (priorité ÉLEVÉE)

3.1.3.1 Recrutement d'un RSSI

Le recrutement d'un Responsable de la Sécurité de l'Information s'avère indispensable pour assurer une expertise dédiée et une direction stratégique en matière de sécurité. Ce rôle implique la supervision de l'ensemble des mesures techniques et organisationnelles.

3.1.3.2 Désignation du responsable de la protection des données

La nomination formelle d'un responsable de la protection des données, supportée par une lettre de mandat, s'impose légalement et organisationnellement. Cette fonction peut être confiée à une personne existante ou constituer un nouveau poste.

3.1.3.3 Création d'un comité de sécurité

L'établissement d'un comité de sécurité favorise une gouvernance coordonnée et une prise de décision collective. La composition doit inclure le RSSI, le responsable IT, le responsable des données, et un représentant de la direction. Des réunions mensuelles permettent une supervision continue des initiatives de sécurité. La mise en place est prévue dans un mois.

3.1.3.4 Rétention

Rétention : une politique de rétention interne est une stratégie et un ensemble de pratiques visant à fidéliser les employés et à réduire le taux de roulement du personnel. Elle comprend des mesures telles que l'amélioration des conditions de travail, l'offre d'avantages financiers et la création d'un environnement de travail positif pour maintenir l'attachement des employés à long terme.

3.1.3.5 Assurance cyber

La souscription d'une police d'assurance cyber transfère une partie des risques résiduels à un tiers. Cette couverture doit adresser les risques d'incident, de violation de données, et de rançongiciel. Le coût annuel estimé varie entre 10 000 et 30 000 dollars selon l'étendue de la couverture, avec un délai de mise en place de deux mois.

3.2 PLAN DE SENSIBILISATION DU PERSONNEL

3.2.1 Programme de formation

3.2.1.1 Formation initiale obligatoire

La formation initiale en cybersécurité s'adresse à l'ensemble des employés de l'organisation. D'une durée de trois heures, elle couvre les enjeux de la cybersécurité pour l'entreprise, la reconnaissance du phishing et des techniques d'ingénierie sociale, les bonnes pratiques d'utilisation des systèmes (gestion des mots de passe, téléchargements sécurisés, navigation prudente), et les responsabilités légales et éthiques. Elle inclut également la procédure de signalement des incidents de sécurité. Le format combine un parcours e-learning et une session interactive. Cette formation doit être recyclée annuellement, avec une validation par quiz exigeant 80 % de réussite.

3.2.1.2 Formation approfondie pour le personnel technique

Le personnel IT et les administrateurs systèmes bénéficient d'une formation approfondie de deux jours. Cette formation porte sur les menaces avancées (APT, ransomware), la sécurisation des infrastructures, la gestion des incidents de sécurité, et la conformité réglementaire. Le format privilégie le présentiel avec étude de cas pratiques, permettant une mise en application immédiate. Des modules e-learning interactifs (30–45 minutes chacun), des capsules vidéo courtes (2–3 minutes). Cette formation est proposée annuellement, complétée par une veille continue des menaces.

3.2.1.3 Formation spécialisée pour le service client

Le service client reçoit une formation spécialisée d'une durée de deux heures, semestriellement. Cette formation aborde la protection des données clients, la détection des tentatives de fraude, et les protocoles de communication en cas d'incident de sécurité. Le format atelier pratique favorise l'acquisition de compétences immédiatement applicables**.**

3.2.2 Campagnes de sensibilisation continue

3.2.2.1 Simulations de phishing

Les simulations de phishing mensuelles constituent un outil de mesure et de renforcement de la vigilance. L'objectif est d'atteindre un taux de clics inférieur à 5 % après six mois de campagne. Les personnes cliquant sur les liens phishing reçoivent une formation ciblée pour corriger leur comportement.

3.2.2.2 Communications internes

Les communications internes maintiennent la sensibilisation en permanence. Elles s'appuient sur plusieurs supports : une infolettre mensuelle, des affiches dans les locaux, et des messages d'accueil affichés sur les écrans de connexion. Les thèmes varient de manière rotatoire pour couvrir les mots de passe, les mises à jour logicielles, le phishing, et les pratiques de télétravail sécurisé.

3.2.2.3 Événements thématiques

Des événements trimestriels renforcent l'engagement des employés de manière ludique et participative. Ces événements prennent la forme de « Lunch & Learn », de quiz avec prix, et de challenges thématiques favorisant la compétition amicale.

3.2.2.4 Sécurité du travail à distance

En cas de télétravail ou de travail à distance, il faut :

Sécurisation du Wi-Fi personnel.

Interdiction d’utiliser des appareils personnels non approuvés.

Utilisation du VPN de l’entreprise.

3.2.2.5 Protection des données sensibles

Classification et définition des données sensibles

Responsabilités légales de l’employé (Loi 25, LPRPDE).

Bonnes pratiques : chiffrement, transferts sécurisés, restriction d’accès.

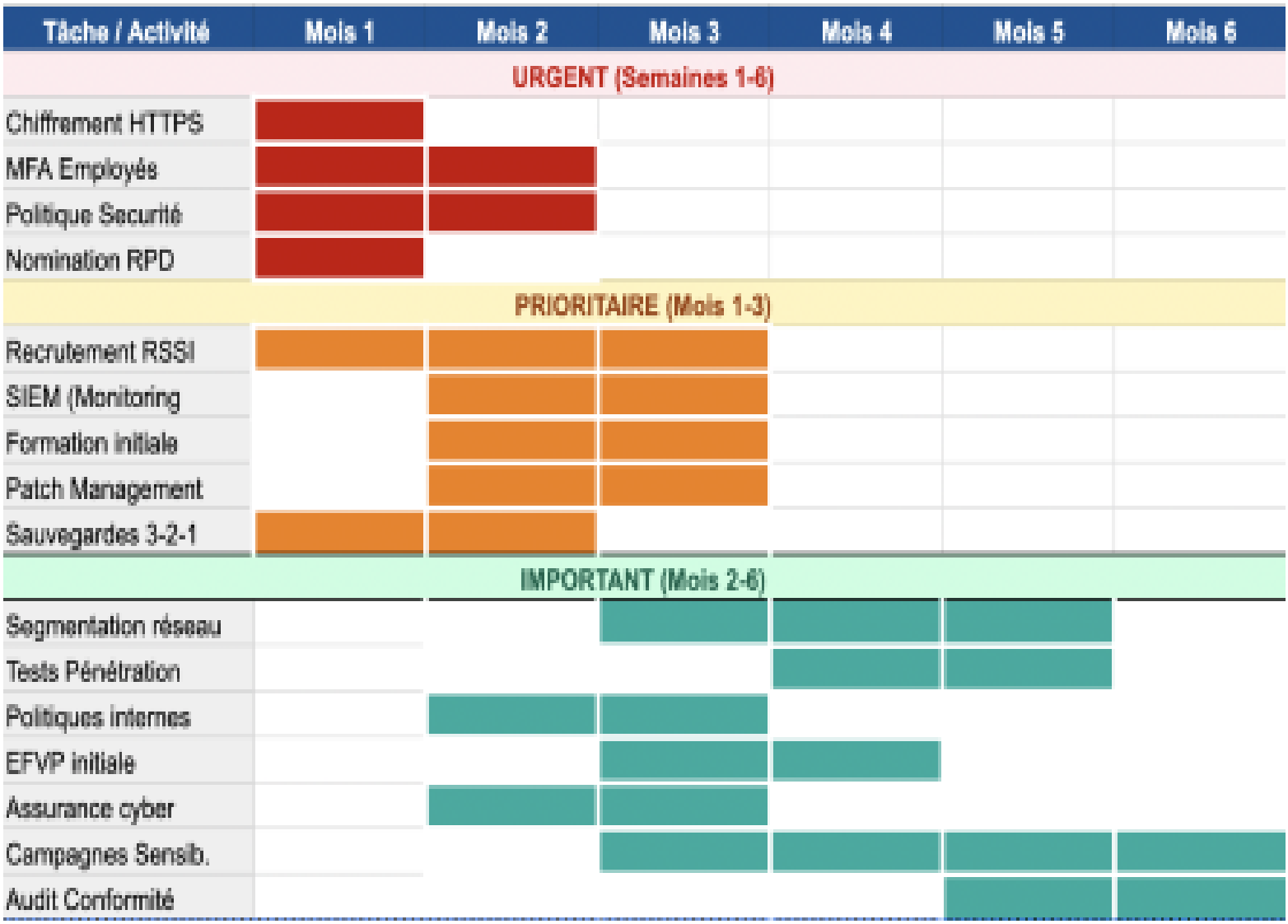
3.2.3 Mesure de l'efficacité

3.2.3.1 Indicateurs clés de performance (KPI)

- Taux de participation aux formations : objectif 100%
- Taux de réussite aux quiz : objectif > 85%
- Taux de clics sur phishing simulé : objectif < 5%
- Nombre d'incidents signalés par les employés : objectif en augmentation
- Délai moyen de détection d'incident : objectif < 24 h

3.3 ÉCHÉANCIER DU PLAN D'ACTION

3.3.1 Diagramme de Gantt – Phase 1 (6 mois)



3.3.2 Phase 2 (6-12 mois) : consolidation

- Mois 7-8 : certification ISO 27001 (préparation)
- Mois 9-10 : Déploiement complet du SGSI (Système de Gestion de la Sécurité de l'Information)
- Mois 11-12 : audit de conformité final, certification ISO 27001

3.3.3 Phase 3 (12-24 mois) : amélioration continue

- Maintien et amélioration du SGSI
- Audits annuels externes
- Veille technologique et adaptation des mesures

3.4 BUDGET PRÉVISIONNEL

Voir annexe A.

Nous avons utilisé l'IA pour nous donner des valeurs fictives.

3.5 INDICATEURS DE SUCCÈS (KPI)

Voir annexe B.

Nous avons utilisé l'IA pour nous donner des valeurs fictives.

CONCLUSION

À la suite de l'audit réalisé pour E-Commerce Express, il a été diagnostiqué que l'entreprise fait face à des enjeux majeurs liés à la sécurité technique, à la gouvernance des données et aux conformités légales. La tentative récente de cyberattaque met en évidence un problème de vulnérabilité sur le plan technique, humain, organisationnel et légal qui constitue un obstacle pour la sécurité des données sensibles et la confiance des clients.

Les failles identifiées soulignent la nécessité d'une intervention globale et rigoureuse de la cybersécurité. Les mesures proposées permettront de renforcer la capacité de l'entreprise à faire face aux incidents, tout en préservant la confidentialité des données personnelles.

Loin d’être une intervention après attaque, ce projet constitue aussi une feuille de route pour améliorer la croissance de l’entreprise et établir une culture de sécurité durable dans un monde numérique où les risques deviennent de plus en plus importants.

4. DOCUMENTATION ET COLLABORATION

4.1 MÉTHODE DE COLLABORATION UTILISÉE

Concernant la collaboration, nous nous sommes principalement coordonnés via Teams et avons partagé nos documents à travers Google Drive (Docs et Sheets).

Le travail s'est déroulé en trois phases. D'abord, nous avons établi la structure du groupe et réparti les tâches. Ensuite, nous avons procédé à la correction et à la consolidation du travail collectif. Enfin, nous avons finalisé la mise en page, créé un dépôt test et produit une présentation PowerPoint.

4.2 CRÉER UN DÉPÔT GITHUB

Lien du dépôt : https://github.com/easynoneybuckets/TRAVAIL2.git

Voir annexe D.

4.3 EXPLIQUER L’INTÉRÊT DU VERSIONNEMENT COLLABORATIF

Le versionnement collaboratif permet à plusieurs membres d’une équipe de travailler en même temps sur le même projet, en nous permettant de garder un historique des modifications effectuées.

Ça nous permet de faciliter la coordination, d'éviter de créer des conflits avec plusieurs fichiers, on peut aussi revenir à des versions précédentes du travail et améliorer la contribution de chacun. Cela rend le travail plus efficace, structuré et organisé dans le contexte professionnel.

BIBLIOGRAPHIE

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security management systems — Requirements* (ISO Standard No. 27001:2022). https://www.iso.org/standard/82875.html

Commissariat à la protection de la vie privée du Canada. (2025). *Commissariat à la protection de la vie privée du Canada*. https://www.priv.gc.ca/fr/

Gouvernement du Québec. (2025). *Entrée en vigueur des nouvelles dispositions de la Loi 25*. https://www.quebec.ca/nouvelles/actualites/details/entree-en-vigueur-des-nouvelles-dispositions-de-la-loi-25-50723

ANNEXES

Annexe A – Budget prévisionnel

CATÉGORIE	ANNÉE 1	ANNÉE 2	ANNÉE 3
Personnel			
RSSI	100 000 $	105 000 $	110 000 $
Responsable données (nouveau poste)	60 000 $	63 000 $	66 000 $
Infrastructure			
Chiffrement et certificats	5 000 $	2 000 $	2 000 $
MFA	10 000 $	3 000 $	3 000 $
SIEM	25 000 $	25 000 $	25 000 $
Segmentation réseau	20 000 $	2 000 $	2 000 $
Sauvegardes	12 000 $	12 000 $	12 000 $
Sécurité et conformité			
Tests de pénétration	20 000 $	20 000 $	20 000 $
Audit externe conformité	15 000 $	10 000 $	10 000 $
Certification ISO 27001	30 000 $	10 000 $	10 000 $
Assurance cyber	20 000 $	22 000 $	24 000 $
Formation			
Programme de formation	15 000 $	8 000 $	8 000 $

Campagnes sensibilisation	5 000 $	5 000 $	5 000 $
Divers et imprévus	20 000 $	15 000 $	15 000 $
TOTAL	357 000 $	302 000 $	312 000 $

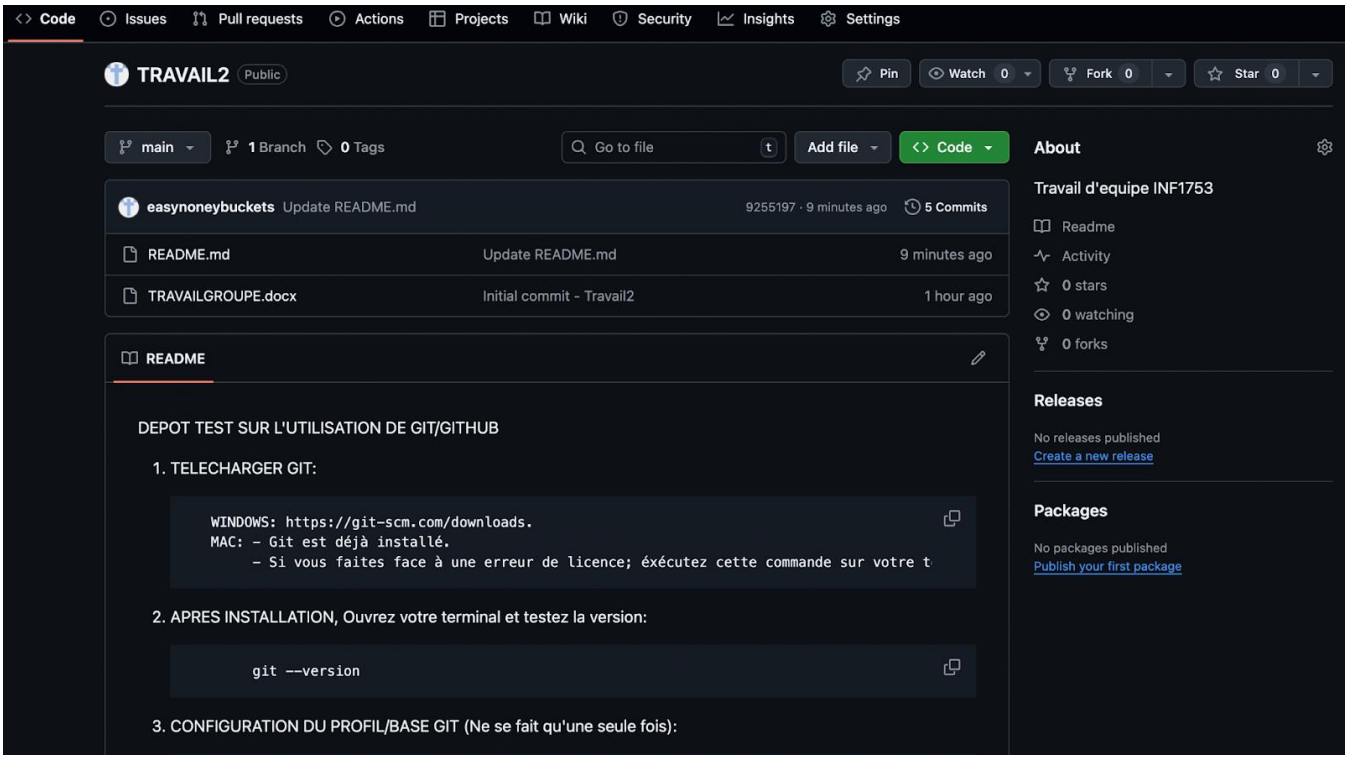
Annexe B – Indicateurs de succès (KPI)

INDICATEUR	VALEUR ACTUELLE	OBJECTIF EN 6 MOIS	OBJECTIF EN 12 MOIS
Temps moyen de détection d'incident	Non mesuré	< 48 h	< 24 h
Temps moyen de résolution	Non mesuré	< 7 jours	< 3 jours
Taux de conformité réglementaire	60 %	85 %	100 %
Couverture MFA	0 %	100 % (employés)	100 % + 50 % clients
Fréquence des sauvegardes	Hebdomadaire	Quotidienne	Continue
Tests de sauvegarde	Jamais	Mensuel	Mensuel
Employés formés	0%	100 %	100 % + recyclage
Vulnérabilités critiques non corrigées	12	0	0

Annexe C – Tableau d'évaluation des risques (probabilité × impact)

ID	RISQUE	PROBABILITÉ	IMPACT	RISQUE	MESURES RECOMMANDÉES
R01	Fuite de données clients	Élevée	Critique	Critique	Chiffrement complet, MFA
R02	Ransomware	Moyenne	Critique	Élevé	Sauvegardes 3-2-1, EDR
R03	Compromission des paiements	Moyenne	Critique	Élevé	Audit PCI, surveillance
R04	Attaque DDoS	Moyenne	Élevé	Moyen	Protection anti-DDoS
R05	Injection SQL	Élevée	Élevé	Élevé	WAF, tests sécurité
R06	Phishing employés	Très élevée	Moyen	Élevé	Formation, MFA
R07	Accès non autorisés	Moyenne	Élevé	Moyen	Moindre privilège
R08	Non-conformité Loi 25	Élevée	Élevé	Élevé	Audit, mise à jour politiques
R09	Perte de données	Moyenne	Critique	Élevé	Sauvegardes quotidiennes
R10	Ingénierie sociale	Élevée	Moyen	Moyen	Formation

Annexe E – Capture GitHub



Annexe F – Contributions individuelles

NOM	TÂCHES PRINCIPALES (1–2 LIGNES)	SIGNATURE
Ali, Habone Hassan	Écriture de la partie 1 Révision et mise en page du rapport Annexe	HA
Barry, Mamadou Bhoye	Écriture de la partie 2, de l'introduction et du résumé	MB
Biongele, André Mataka	Écriture de la partie 3, de l'introduction et du résumé Présentation Powerpoint Création du dépôt GitHub	AB
Ebatha-Franck, Brandon	Écriture de la partie 2	BE
Ibekourene, Lydia	Écriture de la partie 1 Révision et mise en page du rapport Annexe	LI
Lyrette, Félix	ABSENT	
Mboudi Pwemeu, Franck Arthur	Écriture de la partie 2 et du résumé	FM
Tadjou, Anzizatou	Écriture de la partie 3 et de la conclusion	AT