HEC MONTRÉAL

L'équipe interdisciplinaire d'intervention en cas d'incident en cybersécurité : facteurs de succès, rôles et responsabilités

par

Dana Batog

Sciences de la gestion
(Spécialisation Transformation numérique)

Mémoire présenté en vue de l'obtention
du grade de maitrise ès sciences
(M. Sc.)

Avril 2021

Sommaire

L'augmentation et la diversification des menaces en sécurité de l'information dans les dernières années s'annoncent être une tendance pour bien des années à venir. Ceci entraîne une augmentation du nombre d'incidents en sécurité, ce qui force les organisations à revoir leur capacité à faire face à ces incidents, tant au niveau technique qu'humain. En cybersécurité, un manque de ressources humaines est également notable. Ce manque de ressources combiné à l'augmentation et la diversification des menaces pousse les organisations à se concentrer sur la composition de leurs équipes de gestion d'incidents.

En parallèle, les structures des équipes évoluent également. De ce fait, un engouement est développé au sein de plusieurs domaines pour des équipes qui combinent plusieurs disciplines afin d'intégrer plus d'expertise à la prise de décision. Entre autres, les domaines de la santé, de la recherche et de l'éducation utilisent de plus en plus la structure d'équipe interdisciplinaire. La littérature n'offre toutefois pas beaucoup d'information sur le jumelage du concept d'interdisciplinarité à l'équipe de gestion d'incident en cybersécurité. Ainsi, ce mémoire a premièrement comme objectif d'identifier les facteurs de succès d'une telle équipe pour ensuite deuxièmement identifier les rôles qui devraient la composer. Ceci est fait à l'aide d'une étude de cas auprès d'une grande organisation québécoise dans laquelle les perceptions de professionnels en cybersécurité ont été recensées. Le troisième objectif de ce mémoire est d'offrir des propositions aux chercheurs et aux professionnels afin de permettre d'éclaircir le sujet des équipes interdisciplinaires d'intervention en cas d'incident en cybersécurité.

Mots-clés : gestion d'incident, équipe interdisciplinaire, composition d'équipe, facteurs de succès, rôles d'une équipe de cybersécurité

Remerciements

Je veux premièrement remercier ma directrice, Alina Dulipovici que je connais maintenant depuis plusieurs années et qui a toujours su me conseiller, tout en étant à l'écoute de mes craintes. Une femme inspirante empreinte d'une immense générosité que je suis choyée de compter à mes côtés. Merci pour tout, tant ce que tu m'as appris que ce que tu m'as permis de découvrir à mon rythme.

Merci également aux personnes qui ont marqué mon passage à HEC. Mention spéciale à Félix, Karl et Max qui m'ont supportée durant mes innombrables moments de panique et qui ont toujours su me ramener les deux pieds sur terre. Merci à Pauline, ma partenaire de maîtrise sans qui ces deux dernières années n'auraient pas été si mémorables. Audrey et Sorina, merci à vous deux pour vos mots d'encouragement et pour nos soupers qui vont perdurer pour bien des années à venir.

Merci à mes amis qui ont subi mes annulations d'activités et surtout à ceux qui m'ont écouté parler de mon mémoire, même s'ils ne comprenaient pas toujours ce que je leur racontais. Christine et Noémie, vous serez toujours mes partenaires de brunch. Steven et Dana, nos 12 ans d'amitié me sont encore plus précieux aujourd'hui. Andreea et Ana, j'ai bien hâte de monter toutes les montagnes de ce monde avec vous.

Finalement, un grand merci à toute ma famille qui a su me changer les idées lorsque j'en avais besoin et qui a su respecter mon désir de me retrouver seule par moments. Maman, Papa, Sergiu, Katy et Paula, merci.

Table des matières

Sommaire ..... *iv*

Remerciements ..... *v*

Chapitre 1. Introduction *11*

1.1 Problématique **11**

1.1.1 Mise en contexte 11

1.1.2 Problématique générale liée au talent requis en cybersécurité au sein d'une équipe de travail 14

1.1.3 Problématique liée au talent requis dans une équipe d'Intervention en Cas d'Incident en Cybersécurité 15

1.1.4 Problématique liée aux cadres définissant la composition d'une équipe en cybersécurité 18

1.2 Objectifs et question de recherche **20**

1.3 Contributions de l'étude **24**

1.4 Structure du mémoire **25**

Chapitre 2. Revue de la littérature *26*

2.1 Structures de collaboration **28**

2.1.1 Définir le concept de collaboration 29

2.1.2 Équipe interdisciplinaire : définition et exemples 36

2.2 Équipe interdisciplinaire en cas d'un incident en cybersécurité et sa performance **39**

2.2.1 Portrait général d'une équipe ICIC interdisciplinaire 39

2.2.2 Avantages d'une équipe ICIC interdisciplinaire 41

2.2.3 Défis d'une équipe ICIC interdisciplinaire 44

2.2.4 Équipe ICIC interdisciplinaire et performante 48

2.2.4.1 Définir le concept de performance 48

2.2.4.2 Définir le concept d'équipe performante 49

2.2.4.3 Impact d'une équipe ICIC interdisciplinaire sur la performance organisationnelle 50

2.3 Facteurs de succès dans une équipe ICIC interdisciplinaire **52**

2.3.1 Identification des facteurs de succès généraux à une équipe de travail 56

2.3.1.1 Alignement opérationnel en accord avec les objectifs organisationnels 56

2.3.1.2 Communication efficiente au sein de l'équipe 58

2.3.1.3 Coopération continue au sein de l'équipe 61

2.3.1.4 Couverture complète des compétences en cybersécurité 63

2.3.2 Identification des facteurs de succès spécifiques à une équipe ICIC interdisciplinaire 65

2.3.2.1 Adaptabilité efficace face aux cybermenaces 66

2.3.2.2 Détection de menaces en continu dans l'environnement de l'équipe 68

2.3.2.3 Reprise rapide des opérations suite à un incident en cybersécurité 71

2.4 Rôles et responsabilités au sein d'une équipe ICIC interdisciplinaire **74**

2.4.1 Les rôles selon Belbin 75

2.4.2 Les rôles au sein de l'équipe ICIC interdisciplinaire 77

2.4.2.1 Agent de changement 77

2.4.2.2 Agent de liaison 79

2.4.2.3 Conseiller 81

2.4.2.4 Coordonnateur 82

2.4.2.5 Gardien de l'information 83

2.4.2.6 Innovateur 85

2.5 Cadre conceptuel proposé 86

Chapitre 3. Méthodologie 88

3.1 Choix de la méthodologie et justifications 88
3.1.1 Justification de l'étude qualitative 88
3.1.2 Justification du choix de l'étude de cas et du cas 90

3.2 La collecte de données 94
3.2.1 Sélectionner les participants 94
3.2.2 Distribuer le questionnaire de données démographiques 97
3.2.3 Faire l'entrevue semi-dirigée 98
3.2.4 Consulter la documentation pertinente 105

3.3 Analyse des données 106
3.3.1 Transcrire les entrevues 107
3.3.2 Codifier les données collectées 107
3.3.3 Analyser les données (intra-répondants et inter-répondants) 109
3.3.4 Comparer l'analyse à la littérature 109

3.4 Considérations éthiques 110
3.4.1 Consentement des répondants 110
3.4.2 Confidentialité des répondants et des propos rapportés 110
3.4.3 Atténuation des risques 111

3.5 Conclusion 113

Chapitre 4. Analyse des résultats 114

4.1 Caractéristiques des participants 114
4.1.1 Protection de l'anonymat 114
4.1.2 Profils des participants 115

4.2 L'équipe ICIC interdisciplinaire 117

4.3 Les facteurs de succès de l'équipe ICIC interdisciplinaire 119
4.3.1 Les facteurs de succès généraux à une équipe de travail 120
4.3.1.1 Alignement opérationnel en accord avec les objectifs organisationnels 120
4.3.1.2 Communication efficiente au sein de l'équipe 121
4.3.1.3 Coopération continue au sein de l'équipe 123
4.3.1.4 Couverture complète des compétences en cybersécurité 124
4.3.2 Les facteurs de succès spécifiques à une équipe ICIC interdisciplinaire 126
4.3.2.1 Adaptabilité efficace face aux cybermenaces 127
4.3.2.2 Détection de menaces en continu 128
4.3.2.3 Reprise rapide des activités 129

4.4 Les rôles au sein de l'équipe ICIC interdisciplinaire 131
4.4.1 Agent de changement 132
4.4.2 Agent de liaison 133
4.4.3 Conseiller 134
4.4.4 Coordonnateur 135
4.4.5 Gardien de l'information 136
4.4.6 Innovateur 136

4.5 Conclusion 137

Chapitre 5. Discussion *138*

5.1 Facteurs de succès au sein d'une équipe ICIC interdisciplinaire **139**

5.2 Rôles au sein d'une équipe ICIC interdisciplinaire **142**

5.3 L'influence du contexte organisationnel sur les facteurs de succès, les rôles et les responsabilités identifiés **144**

5.3.1 Impact des valeurs favorisées par l'organisation dans le quotidien de l'équipe 144

5.3.2 Une dynamique d'équipe qui s'inscrit dans la prévision 145

5.3.3 Interdépendance des rôles pour une meilleure performance d'équipe 147

5.3.4 Les divers volets de la communication comme fondation à l'organisation de l'équipe 148

5.4 Conclusion **151**

Chapitre 6. Conclusion *152*

6.1 Rappel de la question de recherche et de l'approche méthodologique **152**

6.2 Principaux résultats **154**

6.3 Implications pour les chercheurs et les professionnels **156**

6.4 Limites de l'étude et pistes de recherche **159**

Bibliographie *161*

Annexe 1 : Liste initiale des facteurs clés de succès *170*

Annexe 2 : Courriel de recrutement *173*

Annexe 3 : Questionnaire de données démographiques *174*

Annexe 4 : Protocole de l'entrevue *176*

Annexe 5 : Présentation PowerPoint *180*

Annexe 6 : Grille de codification finale *190*

Liste des figures

Figure 2.1 – Les différentes équipes de collaboration 31

Figure 2.2 – Une illustration d'une équipe ICIC interdisciplinaire 41

Figure 2.3 - Un alignement opérationnel en accord avec les objectifs organisationnels 56

Figure 2.4 - Une communication efficiente au sein de l'équipe 58

Figure 2.5 – Coopération continue au sein de l'équipe 61

Figure 2.6 - Couverture complète des compétences en cybersécurité 63

Figure 2.7 – Adaptabilité efficace face aux cybermenaces 66

Figure 2.8 – Détection de menaces en continu dans l'environnement de l'équipe 69

Figure 2.9 - Reprise rapide des opérations suite à un incident en cybersécurité 71

Figure 2.10 – Agent de changement 77

Figure 2.11 – Agent de liaison 79

Figure 2.12 – Conseiller 81

Figure 2.13 – Coordonnateur 82

Figure 2.14 – Gardien de l'information 83

Figure 2.15 – Innovateur 85

Figure 2.16 - Facteurs de succès et rôles au sein de la composition d'une équipe ICIC interdisciplinaire 86

Figure 3.1 - Survol des différentes étapes de la collecte de données 94

Figure 3.2 – Exemple de structure utilisée lors de la présentation des éléments du cadre conceptuel 104

Figure 3.3 - Survol des différentes étapes de l'analyse de données 107

Liste des tableaux

Tableau 2.1 : Structures de collaboration 32
Tableau 2.2 : Avantages d'une équipe ICIC interdisciplinaire 42
Tableau 2.3 Défis d'une équipe ICIC interdisciplinaire 45
Tableau 2.4 Résumé des facteurs de succès d'une équipe ICIC interdisciplinaire 55
Tableau 2.5 Les rôles de Belbin 76
Tableau 3.1 : Sommaire du protocole d'entrevue 99
Tableau 3.2 : Structure des entrevues semi-dirigées 101
Tableau 4.1 Profil des participants 116
Tableau 4.2 : Pertinence de l'équipe ICIC interdisciplinaire selon les participants 117
Tableau 4.3 : Les facteurs de succès généraux à une équipe de travail 120
Tableau 4.4 : Les facteurs de succès spécifiques à une équipe ICIC interdisciplinaire 126
Tableau 4.5 : Les rôles dans une équipe ICIC interdisciplinaire 131
Tableau 5.1 : Identification des facteurs de succès d'une équipe ICIC interdisciplinaire 139
Tableau 5.2 : Identification des rôles d'une équipe ICIC interdisciplinaire 142

Chapitre 1. Introduction

1.1 Problématique

Cette première section permet d'introduire le sujet à l'étude de ce mémoire. Ainsi, la mise en contexte présente le contexte du domaine de la cybersécurité afin d'y déceler la problématique retenue pour la suite de ce mémoire. Ensuite, la deuxième sous-section détaille la problématique retenue pour en dresser un portrait global avant d'expliquer dans les sous-sections suivantes les différentes composantes de cette problématique. Ces dernières sections préparent la présentation des questions et objectifs de recherche de la section 1.2.

1.1.1 Mise en contexte

Dans les dernières années, les menaces ambitieuses et sophistiquées ont augmenté en nombre et en diversité dans le domaine de la sécurité de l'information, des menaces de natures différentes à celles que les organisations connaissaient auparavant (Chang et Ho, 2006; Caendra Inc, 2017). Différents acteurs comme les cybercriminels ou encore les pirates informatiques bienveillants développent continuellement des stratégies leur permettant de contourner les défenses mises en place par les organisations (Jacob et al., 2018). De ce fait, ces menaces peuvent mener à de lourdes conséquences pour les organisations victimes d'un incident de cybersécurité. En 2020 un incident du type d'une brèche de données coûtait en moyenne 3.86 millions $ US (IBM,2020). De plus, ces incidents peuvent occasionner une perte de confiance de la part des clients (Hall, Sarkani et Mazzuchi, 2011), ce qui mène potentiellement à un problème de réputation pour l'organisation (Kankanhalli et al., 2003; Auyporn, Piromsopa et Chaiyawat, 2020).

Le National Institute of Standards and Technologies (NIST) définit ainsi un incident en cybersécurité :

> « Un événement qui compromet ou peut compromettre la confidentialité, l'intégrité ou la disponibilité d'un système d'information ou qui constitues une violation ou menace imminente de violation de politiques de sécurité, procédures de sécurité ou politiques d'utilisation acceptable. » (NIST, 2019).

Par exemple, le scénario d'un employé malhabile cliquant sur un lien douteux qu'il a reçu par courriel et qui le rend alors victime d'hameçonnage est un incident de cybersécurité. L'action de cliquer sur le lien et d'ainsi possiblement donner accès aux données sensibles de l'organisation met entre autres en péril la confidentialité de l'actif informationnel.

Un incident en cybersécurité est composé de trois éléments : (1) une menace; (2) une vulnérabilité et (3) le risque que l'incident se produise (soit l'impact et la probabilité que l'incident se produise) (ANSSI-CyberEdu, 2015).

Premièrement, une menace est définie comme « un événement potentiel et appréhendé, de probabilité non nulle, susceptible de porter atteinte à la sécurité informatique » (Gouvernement du Québec, 2002). Une grande diversité de menaces peut porter atteinte à l'actif informationnel d'une organisation, soit l'inventaire présentant le portrait de l'ensemble des ressources informationnelles d'une organisation à un moment précis (Gouvernement du Québec, 2002). L'utilisation des technologies émergentes comme l'infonuagique et l'Internet des objets dans les organisations en est un exemple (MacKinnon et Rampado, 2020). Ces technologies permettent, entre autres, aux entreprises de recueillir une plus grande quantité de données sur les habitudes des consommateurs afin d'aiguiser leurs décisions d'affaires. Toutefois, ces données peuvent offrir un retour financier à la personne ou au groupe de criminels qui entrent en leur possession, accroissant la probabilité qu'une action malveillante soit effectuée (McCarthy et Tétrault, 2017). Des menaces peuvent être de nature humaine, soit un employé malicieux ou tout simplement

malhabile, elles peuvent aussi se traduire par une attaque directe sur les systèmes de l'organisation. Par exemple, par l'entremise d'un rançongiciel, il est possible de chiffrer les données de l'organisation afin de dérober de l'argent à celle-ci en retour des données prises en otage (Larousse, 2020). Finalement, un autre exemple de menace en cybersécurité est l'exemple d'une panne d'équipement. Cette menace pourrait mener l'organisation à avoir de la difficulté à effectuer ses activités.

Deuxièmement, une vulnérabilité est « une faiblesse se traduisant par une incapacité partielle à faire face aux menaces de cybersécurité » (Gouvernement du Québec, 2020). Cette vulnérabilité peut provenir de la technologie, d'un réseau ou encore de l'humain. Par exemple, un système qui n'est pas mis à jour régulièrement peut devenir une vulnérabilité technique pouvant être exploitée.

Troisièmement, le risque que l'incident se produise est défini comme « une probabilité plus ou moins grande de voir une menace informatique se transformer en événement réel entraînant une perte » (Gouvernement du Québec, 2020). Ces trois éléments : la menace, la vulnérabilité et le risque sont ainsi tous des éléments qui, une fois combinés, peuvent nuire grandement à l'organisation et mener à un incident de cybersécurité.

Tel que mentionné précédemment, l'environnement de cybersécurité des organisations change constamment. Les acteurs qui agissent à titre de cybercriminels innovent et cherchent de nouveaux vecteurs d'attaques (DeCoster, 2019). Ils obtiennent des données sur les consommateurs ou sur les organisations pour ensuite s'enrichir. En 2020, environ 85% des vols de données étaient motivés par le retour financier possible occasionné (Verizon, 2020).

La cybersécurité, qui vise, entre autres, la mise en place de moyens de protection contre le vol et la manipulation non autorisée des données, combine quatre dimensions : technique, humaine, organisationnelle et régulatrice (Jacob et al., 2018). La dimension technique représente les solutions technologiques pouvant être utilisées pour répondre à un

cybercrime, la dimension organisationnelle représente les processus et procédures des organisations en ce qui attrait à la cybersécurité et la dimension régulatrice est celle de la conformité de l'organisation envers les lois autoritaires et réglementaires (Choras et al., 2015). La dimension humaine, soit la dimension étudiée dans ce mémoire, représente tous les facteurs humains (p. ex. formation et composition d'équipe) ainsi que la sensibilisation qui doit être faite sur l'importance de la cybersécurité (Choras et al., 2015). Cette dimension touche la sensibilisation d'éléments non technologiques, mais également la nécessité d'une expertise spécialisée en cybersécurité et de la disponibilité de celle-ci. Toutes ces dimensions peuvent être affectées lors d'un incident de cybersécurité, tel qu'une brèche de données.

1.1.2 Problématique générale liée au talent requis en cybersécurité au sein d'une équipe de travail

Dû à l'augmentation en nombre et en diversité des différentes menaces en cybersécurité, la demande en spécialistes de cybersécurité augmente. Cette augmentation de la demande de spécialistes, combinée à un nombre stable de main d'œuvre disponible sur le marché, mène à une pénurie des cybertalents (Olyaei, 2019; MacKinnon et Rampado, 2020). Cette pénurie affaiblit les équipes de cybersécurité actuelles qui ont alors moins d'employés spécialisés disponibles pour gérer les modifications dans leurs tâches quotidiennes (Olyaei, 2019). De plus, l'augmentation du nombre de cybermenaces mène également à une évaluation des défis concernés par la cybersécurité (Jacob et al., 2018). Un de ces défis est l'évolution du domaine de la cybersécurité qui est plus rapide que le rythme auquel la main d'œuvre peut être formée (Jon, 2020). Alors, un écart est également visible entre la quantité de professionnels qualifiés en cybersécurité et le nombre grandissant de postes disponibles dans le domaine.

Parallèle à ceci, le domaine de la cybersécurité subit plusieurs changements, dû entre autres à la transformation numérique qui pousse les organisations à revisiter leurs stratégies de

protection en sécurité de l'information et leurs stratégies de main d'œuvre (Raza, 2019). La transformation numérique est le processus par lequel les organisations s'adaptent pour répondre aux éléments changeants de la société moderne, en modifiant la façon dont la technologie est créée, gérée, analysée et consommée (Duncan, 2018).

Donc, une problématique regroupant ces éléments s'installe au sein du domaine de sécurité de l'information. L'écart entre l'augmentation du nombre de menaces en cybersécurité et le manque de ressources humaines pour les contrer mène à porter une réflexion sur la dimension humaine de la cybersécurité. Bien que la cybersécurité soit un défi technique, elle a été désignée être un défi de plus en plus humain (Wood, 1987; Schultz, 2005; Hall, Sarkani et Mazzuchi, 2011). **Les organisations doivent maintenant tenter d'assurer que les équipes désignées de cybersécurité ont les ressources nécessaires afin de protéger l'actif informationnel (Caendra Inc, 2017). Ce mémoire se concentre sur cette problématique en étudiant la composition de l'équipe de travail de cybersécurité (MacKinnon et Rampado, 2020).** Ce choix a été fait, car toute équipe a une influence directe sur la performance de son organisation; il s'agit donc d'une piste de réflexion.

1.1.3 Problématique liée au talent requis dans une équipe d'Intervention en Cas d'Incident en Cybersécurité

Tout d'abord, il est important de définir ce qu'est une équipe. Une équipe est une structure sociale dans laquelle les membres qui la composent sont interdépendants et ont des objectifs de travail communs (Salas, Cook et Rosen, 2008). Le but principal d'une équipe de travail, tous contextes confondus, est d'être efficace et performante afin d'améliorer la performance organisationnelle (Salas, Cook et Rosen, 2008). Une équipe de travail efficace est une équipe qui innove et qui est agile dans son adaptation aux défis auxquels elle fait face (Towler, 2020). Cette efficacité peut être mesurée de plusieurs façons comme les résultats de l'équipe (qualité, vitesse, satisfaction de la clientèle, etc.) ou encore la capacité de l'équipe à bien performer dans le futur en fonction de ce qu'elle développe présentement (Towler, 2020). Le travail en équipe permet aux membres de faire preuve d'un état de

conscience réfléchi et de développer leur pensée critique suite à des discussions et clarifications de la part de leurs pairs (Denton, 1997).

En cybersécurité, plusieurs types d'équipes existent actuellement. Par exemple, certaines équipes se concentrent sur le développement de fonctionnalités ou d'outils pour contrer les cyberattaques (Raza, 2019). D'autres équipes sont axées sur l'analyse de données en priorité afin de prendre des décisions affaires qui sont directement liées aux données de l'organisation et de son environnement (Stevens, 2017). Un troisième exemple d'équipe en cybersécurité est l'équipe qui mise sur la définition de rôles techniques qui influencent directement la prise d'action lors d'un incident en cybersécurité (par exemple : des rôles d'ingénieurs, d'auditeurs ou de défenseurs) (Jon, 2020). Ces équipes ont toutefois toutes un désavantage qui peut potentiellement nuire à l'organisation, soit que leur structure favorise un travail en silos. Elles sont divisées et travaillent chacune de leur côté, engendrant un manque de collaboration entre les fonctions (Simos et Macababbad, 2020).

Présentement, il y a une augmentation de l'intérêt envers une autre équipe, l'équipe d'intervention en cas d'incident en cybersécurité (ICIC). Ceci est dû au fait que la gestion des incidents en cybersécurité devient une discipline qui doit coordonner des éléments à la fois techniques et des éléments de communication qui attraient au reste de l'organisation (Microsoft, 2017). Cette équipe d'intervention a pour objectif de mitiger les menaces potentielles en utilisant des tactiques de préparation, réponse et reprise d'opérations en cas d'incident, le tout en maximisant la préservation de la propriété intellectuelle et de la sécurité de l'information au sein des organisations (NICCS, 2020). Elle a l'avantage d'être également précurseur dans le partage ; l'information qu'elle manipule est partagée avec des parties prenantes provenant du reste de l'organisation. L'utilité de ce type d'équipe est palpable, car 80% des entreprises canadiennes ont été atteintes par une cyberattaque entre 2019 et 2020, et 30% d'entre elles ont vu leur travail au quotidien interrompu (Vumetric, 2020). De plus, depuis le début de la pandémie de la COVID-19, les attaques d'hameçonnage ont augmenté de 670% en un mois chez ces mêmes entreprises (Vumetric , 2020). Une

équipe ainsi dédiée à la protection de l'actif informationnel donne les moyens à l'organisation de se soucier des cyberattaques plausibles. La protection de l'actif informationnel peut être soutenue par plusieurs types d'équipes au sein d'une organisation. Entre autres, le centre d'opérations en sécurité (SOC) est une équipe qui opère dans le sens de cette protection. Un SOC se spécialise en l'implantation d'outils de protection de sécurité et d'un contrôle sur l'infrastructure technologique de l'organisation, le tout en misant sur l'intelligence d'affaires pour prendre des décisions critiques (AT&T, 2021). L'objectif est donc le même que pour l'équipe de gestion d'incidents : la protection de l'actif informationnel. Toutefois, contrairement à l'équipe de gestion d'incidents, le SOC va placer ses ressources sur la compréhension des données et leur manipulation afin de prendre des décisions. L'équipe de gestion d'incidents elle misera plutôt sur le processus et comment les différents intervenants doivent interagir afin d'assurer une bonne prise en charge de l'incident. Tandis que le SOC mise sur l'aspect technique, l'équipe de gestion d'incident elle mise sur l'aspect humain.

En parallèle, l'intérêt est également en croissance pour l'implantation de nouvelles structures d'équipes, des équipes qui intègrent des employés provenant de différentes disciplines. Une comparaison peut alors être effectuée entre des équipes homogènes et des équipes hétérogènes (Denton, 1997). Une équipe hétérogène est une équipe dans laquelle les membres proviennent de différentes disciplines. Les équipes hétérogènes semblent mieux performer que celles homogènes grâce aux différentes perspectives apportées par ces membres et aux discussions actives présentes au sein de l'équipe (Denton, 1997). Ces équipes peuvent prendre la forme de plusieurs structures, dont celle de l'équipe interdisciplinaire. Une équipe interdisciplinaire est une équipe polyvalente dans laquelle les différents membres se complètent en termes de compétences et d'expertise. Au sein de cette équipe, on dénote une intégration de différentes perspectives, techniques, et concepts provenant de différentes disciplines afin d'augmenter les contributions individuelles de chacune d'entre elles (Moirano, Sánchez et Štěpánek, 2020). Ce mémoire adopte l'approche de l'équipe interdisciplinaire pour améliorer la réflexion sur la composition d'une équipe ICIC.

De plus, la littérature mentionne que les équipes actuelles d'intervention en cybersécurité ne sont pas adéquatement préparées pour faire face aux nouveaux risques présents dans le domaine (Olyaei, 2019). Par exemple, pour revenir à l'exemple du SOC, cette équipe concentre ses ressources sur les mesures techniques de protection disponibles. Ceci a comme impact qu'un manque de compréhension se crée sur le rôle que l'humain peut avoir lors d'un incident. Le SOC sera en mesure d'analyser un incident passé ou encore d'identifier des failles technologiques, mais aura plus de difficultés à anticiper les actions d'un employé malhabile par exemple. Pour l'équipe d'intervention, le manque de préparation se traduit plutôt en manque d'organisation des équipes. La définition de nouvelles structures d'équipes est alors encouragée afin de contrer cette problématique et d'améliorer l'adaptation des organisations à la transformation numérique (Raza, 2019). De plus, la recherche existant présentement dans le domaine met l'emphase sur les éléments techniques nécessaires dans une équipe d'intervention et ne se concentre pas suffisamment sur les éléments organisationnels et ceux de gestion qui pourraient définir le succès d'une telle équipe au quotidien (Dawson et Thomson, 2018). **Les rôles traditionnellement présentés dans les équipes d'intervention ne sont plus les seuls rôles nécessaires afin d'optimiser la performance de l'équipe (Simos et Macababbad, 2020). Compte tenu de cet élément et également des avantages précédemment mentionnés sur les équipes hétérogènes, il devient impératif d'apporter des propositions sur la composition d'une équipe d'intervention qui n'utilise pas la structure de travail traditionnelle : l'équipe ICIC interdisciplinaire.**

1.1.4 Problématique liée aux cadres définissant la composition d'une équipe en cybersécurité

Plusieurs cadres détaillant la composition d'une équipe en cybersécurité existent dans la littérature. Ces cadres présentent le type de rôles requis dans une telle équipe ainsi que les éléments critiques qui influencent sa performance. Dans ce mémoire, un rôle est défini

comme « une fonction remplie par quelqu'un [au sein d'une équipe de travail] » (Larousse, 2020). Pour chaque rôle, on associe également des responsabilités qui représentent des éléments à la charge d'un individu occupant le rôle en question. Ces éléments peuvent être présentés comme des mandats, des tâches ou des actions à poser en fonction du rôle porté. Un des cadres détaillant la composition d'une équipe performante en cybersécurité est le cadre *NICE Cybersecurity Workforce Framework* (NCWF). Ce cadre a été conçu par le *National Initiative for Cybersecurity Education* (NICE) et par le département américain de sécurité intérieure. Il définit les requis de la main d'œuvre en cybersécurité en termes de connaissances, compétences et habiletés (Newhouse et al., 2017). Il a été toutefois dénoté que le cadre n'englobe pas suffisamment la dimension humaine de la cybersécurité (Jacob et al., 2018). Entre autres, bien que le cadre présente correctement des catégories d'actions à accomplir en cybersécurité (p.ex. analyser, investiguer et maintenir des systèmes), ceci est suivi par une définition technique de rôles (développeur, contrôleur, architecte TI, etc.) (Petersen et al., 2020). Ainsi, le cadre est une excellente ressource pour définir les requis techniques spécifiques au caractère interdisciplinaire de la cybersécurité et pour tenir le talent de la main d'œuvre à jour (Petersen et al., 2020). Toutefois, ce type de cadre ne répond pas à la problématique du manque de lien entre la composition de l'équipe et l'impact de son succès sur le reste de l'organisation.

En parallèle au cadre NCWF, d'autres cadres se basent sur la charge cognitive afin de définir des rôles au sein d'une équipe. Ainsi, les rôles sont classés par rapport à la charge cognitive associée à chaque tâche à accomplir pour le bon fonctionnement de l'équipe (Campbell, Saner et Bunting, 2016). Ensuite, les individus sont associés aux rôles en fonction de leur aptitude à gérer ces charges cognitives (Campbell, Saner et Bunting, 2016). Bien que ce type de cadre permette d'évaluer les rôles pertinents d'une équipe ICIC interdisciplinaire sous un autre angle, soit celui de la charge cognitive, le lien entre la composition de l'équipe et les éléments favorisant son succès est encore à préciser.

Par ailleurs, le cadre ISO 27110, complété par le cadre ISO 27100, détaille les éléments techniques à prioriser dans la conception d'un système de protection contre les cyberattaques (Naden, 2021). Ceci permet de clarifier la terminologie et les concepts du

domaine de la cybersécurité pour tout utilisateur consultant le cadre. Bien que très pertinent à utiliser, ce cadre place lui aussi une emphase sur l'aspect technique et théorique de la cybersécurité et comporte un manquement envers la dimension humaine.

Finalement, il existe également le cadre MITRE ATT&CK. Ce cadre détaille la façon dont les cyberattaquants sont en mesure de contourner les défenses d'une organisation et infiltrer celle-ci. C'est donc le point de vue de l'attaquant qui y est détaillé, afin de permettre aux organisations de mieux comprendre ses facettes et tactiques utilisées et de mieux s'y préparer (MITRE Corporation, 2021). Par exemple, le cadre détaille ce qui se produit lorsque l'attaquant est en phase de mouvement latéral, soit lorsqu'il cartographie le réseau de l'organisation afin de s'y promener et d'aller retirer les données qu'il souhaite posséder (Ortega, 2017). Ce cadre est lui pertinent afin de se préparer aux incidents de sécurité, mais se concentre encore une fois sur la connaissance technique nécessaire aux organisations.

En conclusion, tous ces cadres et limites que nous avons identifiés nous permettent d'affirmer que **les cadres existants sont insuffisants pour répondre à la problématique humaine soulevée et qu'une autre approche doit être utilisée**.

1.2 Objectifs et question de recherche

L'objectif général de cette étude est de proposer des pistes de réflexion sur la composition d'une équipe interdisciplinaire d'intervention en cas d'incident en cybersécurité (ICIC), équipe qui serait présente en première ligne lors d'un incident en cybersécurité. Par ailleurs, selon la littérature sur les équipes interdisciplinaires, plusieurs facteurs peuvent influencer la performance d'une équipe, dont la composition de l'équipe. Il est donc important de préciser que ce mémoire ne cherche pas à évaluer la performance de l'équipe ICIC. Ce mémoire cherche uniquement à étudier la composition de l'équipe en faisant abstraction de tous ces autres facteurs.

Cette étude tente ainsi de répondre à la question de recherche suivante :

Quelle devrait être la composition d'une équipe interdisciplinaire d'intervention en cas d'incident en cybersécurité ?

Pour définir les rôles au sein de l'équipe ICIC interdisciplinaire, ce mémoire adopte une approche basée sur l'identification des facteurs clés de succès (**FCS**) de l'équipe. Un facteur de succès est un facteur jugé essentiel à l'efficacité de l'équipe pour sa performance (Fortune et White, 2006). En plus de déterminer si l'équipe atteint les objectifs établis, ces facteurs permettent un suivi des opérations effectuées par l'équipe, spécifiquement si ces opérations aident à la bonne performance et si des éléments au sein de ces opérations doivent être améliorés (Iannucci et Garland, 2020). Ainsi, afin d'assurer un contrôle des facteurs de succès au sein d'une équipe, des **indicateurs clés de performance** sont utilisés. Ces indicateurs permettent le suivi des facteurs de succès et, bien que la performance de l'équipe ne soit pas le focus de ce mémoire, ils permettent de comparer les pratiques de l'équipe avec celles de l'industrie et de faciliter la prise de décision opérationnelle dans le quotidien de l'équipe. Par conséquent, leur utilisation ne se résume pas uniquement à la mesure de la performance et ça justifie leur inclusion dans notre approche.

Cette approche a été choisie pour plusieurs raisons. Premièrement, les **facteurs** clés de succès (FCS) et les **indicateurs** de performance sont liés par le **contexte** de performance dans lequel l'équipe ICIC interdisciplinaire est ici placée. L'influence de ces facteurs sur les rôles se rapproche donc du contexte étudié dans la problématique de ce mémoire. Deuxièmement, l'utilisation de FCS permet d'établir un lien direct avec la stratégie de l'organisation et la dimension humaine, surtout l'angle de cette étude soit les équipes de travail. En effet, l'hypothèse est que l'amélioration de la performance d'une équipe grâce au suivi des facteurs de succès permet l'amélioration et l'implantation de la stratégie globale de l'organisation (Dufour, 2020). Troisièmement, la littérature contient des recherches qui ont étudié les différents FCS d'une

équipe en cybersécurité et des recherches qui ont étudié les FCS d'une équipe interdisciplinaire. Toutefois, peu de recherches existent combinant la notion d'équipe interdisciplinaire à celle d'équipe en cybersécurité. De plus, il y a peu d'information dans la littérature sur des facteurs de succès non techniques attribués à une équipe de cybersécurité. Par exemple, plusieurs auteurs parlent du temps nécessaire à l'équipe pour détecter un incident informatique ou encore le temps nécessaire à l'équipe pour réagir à ce type d'incident (Caendra Inc, 2017). Sinon, les recherches qui s'éloignent de l'aspect technique et qui observent l'aspect humain de la performance d'une équipe le font au niveau de l'individu (Van der Kleij, Kleinhuis et Young, 2017). Ces éléments sont de bonnes pistes, par exemple le partage d'information efficace par les employés, afin d'approfondir l'étude des facteurs de succès au niveau d'analyse de l'équipe. **Ainsi, une approche qui place l'emphase sur les facteurs de succès établis au niveau de l'équipe nous parait extrêmement pertinente pour la définition de rôles composant l'équipe ICIC interdisciplinaire.**

Trois objectifs découlent de la question de recherche de ce mémoire :

1. **Identifier les facteurs de succès d'une équipe ICIC interdisciplinaire**

   Ce premier objectif est l'identification de facteurs de succès au sein d'une équipe ICIC interdisciplinaire. Ces facteurs de succès sont essentiels à la performance de cette équipe.

   L'objectif est divisé en trois sous-objectifs :

   - Le premier est l'identification de facteurs de succès essentiels dans une équipe de travail, tous contextes confondus. Ce sous-objectif est pertinent afin d'établir une base sur l'utilisation des facteurs de succès.

- Le deuxième sous-objectif est l'identification de facteurs de succès spécifiques à une équipe interdisciplinaire en cybersécurité. Ce sous-objectif permet de compléter l'identification des facteurs de succès d'une équipe de travail avec ceux pour une équipe ICIC interdisciplinaire.

- Le troisième sous-objectif est l'identification d'indicateurs clés de performance pour chacun des facteurs de succès précédemment indiqué afin de permettre un suivi lors de l'instauration au sein de l'équipe ICIC interdisciplinaire.

2. Identifier les rôles au sein d'une équipe ICIC interdisciplinaire et leurs responsabilités

Ce deuxième objectif est l'identification des rôles composant une équipe ICIC interdisciplinaire. Ces rôles sont inférés suite à l'identification des facteurs de succès.

L'objectif est divisé en deux sous-objectifs :

- Le premier sous-objectif est l'identification des rôles clés dans une équipe ICIC interdisciplinaire, en se basant sur les facteurs de succès précédemment établis d'une telle équipe.

- Le deuxième sous-objectif est l'identification de responsabilités associées à chacun de ces rôles.

L'atteinte des deux premiers objectifs nous permettra d'émettre des propositions pour les chercheurs ainsi que des recommandations aux gestionnaires qui désirent créer des équipes ICIC interdisciplinaires. Le tout sera donc basé sur la synthèse de la littérature et sur l'analyse effectuée suite à la collecte de données.

1.3 Contributions de l'étude

Ce mémoire offre plusieurs contributions pour les chercheurs et les professionnels en cybersécurité. Pour les chercheurs, une première contribution est celle de l'avancement des connaissances sur le sujet de l'équipe interdisciplinaire en cybersécurité. Bien que la littérature existe sur la composition des équipes interdisciplinaires et sur la composition des équipes en cybersécurité, peu d'études combinent les deux (Jacob et al., 2018). Pallier ce manque de littérature permettrait également d'identifier de nouvelles avenues de recherche sur la dimension humaine de la cybersécurité. Une deuxième contribution est l'avancement des connaissances directement reliées à une équipe particulière en cybersécurité, soit celle d'intervention en cas d'incident en cybersécurité. Les propositions suggérées à la suite de cette étude peuvent représenter un point de départ pour la recherche auprès d'autres types d'équipes dans le domaine. Troisièmement, une autre contribution est celle de l'utilisation d'une approche différente, soit la perspective des facteurs de succès, afin de conceptualiser la composition d'une équipe ICIC interdisciplinaire. Plusieurs recherches ont été faites sur la composition des équipes en cybersécurité, mais peu ont été effectuées en établissant des liens entre cette composition et les facteurs qui peuvent influencer le succès de l'équipe (Caendra Inc, 2017; Van der Kleij, Kleinhuis et Young, 2017).

Quant aux professionnels en cybersécurité, ce mémoire vise trois contributions principales. Premièrement, pour le gestionnaire, ce mémoire pourra le guider vers des décisions directement reliées à la composition de son équipe ICIC interdisciplinaire en se basant sur les recommandations tirées d'une synthèse de la littérature et d'une analyse de la collecte de données qui sera effectuée. Deuxièmement, grâce à l'approche basée sur les facteurs de succès, ce mémoire aidera les gestionnaires et les chefs d'équipes ICIC à identifier des indicateurs clés de performance pour permettre le contrôle et le suivi d'une équipe ICIC interdisciplinaire (Fortune et White, 2006). Un gestionnaire pourra ainsi instaurer des mesures au sein de son équipe ICIC interdisciplinaire et pourra déterminer si des modifications doivent être apportées pour faciliter l'atteinte de l'efficacité organisationnelle. Finalement, la présentation de rôles qui abordent la dimension humaine de la cybersécurité permettra également aux gestionnaires qui

ne sont pas familiers avec les termes précis du domaine de comprendre l'importance et l'utilité de chaque rôle de l'équipe (Jacob et al., 2018; MacKinnon et Rampado, 2020). Ces gestionnaires comprendront ainsi plus aisément les objectifs d'une telle équipe et la valeur qu'elle peut apporter pour le reste de l'organisation, favorisant les rapports entre l'équipe et les gestionnaires externes à celle-ci.

1.4 Structure du mémoire

Ce mémoire est divisé en six chapitres, chacun d'entre eux participant à la réalisation de l'objectif principal de l'étude, proposer des pistes de réflexion sur la composition d'une équipe ICIC interdisciplinaire.

Ce premier chapitre a permis de placer l'étude en contexte et d'indiquer la problématique qui sera étudiée et suivie tout au long de ce mémoire. Le chapitre suivant présentera un survol de la littérature sur les équipes interdisciplinaires en cybersécurité, les facteurs de succès ainsi que les rôles et responsabilités au sein d'une telle équipe, afin d'établir une base théorique et de concevoir un cadre conceptuel. Le chapitre 3 détaille la méthodologie utilisée pour effectuer la collecte de données, en expliquant entre autres le protocole développé pour recueillir la perception de professionnels sur le cadre conceptuel conçu à la fin du deuxième chapitre. Ensuite, le chapitre 4 présente l'analyse des données recueillies lors de la collecte. Ceci permet de dresser un portrait global de ce qui a été trouvé sur le terrain. Puis, le chapitre 5 discute l'analyse qui a été effectuée au chapitre 4 afin de répondre à la question de recherche de cette étude. Finalement, le chapitre 6 conclut ce mémoire et présente les implications pour les chercheurs et les professionnels en cybersécurité, les limites et les pistes pour de futures recherches permettant ainsi d'alimenter la réflexion sur la problématique de ce mémoire.

Chapitre 2. Revue de la littérature

L'objectif de ce deuxième chapitre est de recenser la littérature scientifique et la littérature professionnelle afin de s'attaquer aux objectifs de cette étude. Plus spécifiquement, il s'agit de synthétiser l'information au sujet des équipes interdisciplinaires, des équipes en cybersécurité, des facteurs de succès essentiels à une équipe ICIC interdisciplinaire et des rôles et responsabilités la composant. À la fin de ce chapitre sera proposé un cadre conceptuel comportant les facteurs de succès et rôles retenus, cadre qui sera un premier pas vers la réponse à la question de recherche énoncée au premier chapitre :

Quelle devrait être la composition d'une équipe interdisciplinaire d'intervention en cas d'incident en cybersécurité ?

Afin d'effectuer la recension des écrits pertinents à la synthèse de l'information et ultimement à l'élaboration d'un cadre conceptuel, plusieurs sources de données ont été utilisées. Premièrement, des bases de données tant scientifiques que professionnelles ont été consultées. Les bases de données scientifiques *ABI/Inform Complete*, *Web of Science*, *ACM Digital Library* et *IEEE Xplore* ont permis de regrouper des sources pertinentes provenant de différents contextes organisationnels et les bases de données professionnelles *Gartner*, *Forrester* et *Business Source Complete* ont permis de compléter la recherche effectuée auprès de ces premières bases de données mentionnées.

D'autres sources de données ont également été employées, comme le moteur de recherche *Google Scholar* ou encore des rapports publiés par des firmes de consultation tel que *Deloitte,* sources qui ont permis de compléter l'information retrouvée dans les bases de données. Pour le moteur de recherche *Google Scholar*, les recherches ont été limitées à la première page, car la littérature mentionne qu'une recherche effectuée avec un tel moteur de recherche est plus efficace dans les premiers résultats retournés, plus précisément ceux de la première page (Diesch, Pfaff et Krcmar, 2020). De plus, dû à l'évolution rapide du domaine de la cybersécurité

et de l'intérêt récent dans le domaine sur la structure des équipes de travail, des blogues ont également été consultés. Les blogues ont été retenus s'ils répondaient à quatre critères de fiabilités soumis par l'Université de Montréal (2021) :

- Qualité du contenu (c.-à-d. présence de sources citées et qualité d'écriture) ;
- Autorité de la source (c.-à-d. identification de l'auteur ou de l'organisme et qualifications de l'auteur) ;
- Mise à jour (c.-à-d. date de création présente sur la page et fréquence des mises à jour) ;
- Facilité d'utilisation (c.-à-d. structure du site et boutons de navigation).

Des écrits provenant également d'autres domaines que celui de la cybersécurité ont été utilisés. Ces domaines sont ceux de la santé, de l'éducation, du travail social et de la recherche. Dans ceux-ci, des recherches ont été effectuées auprès d'experts qui ont reconnu la pertinence d'équipes interdisciplinaires dans de tels contextes. L'utilisation de ces recherches est pertinente pour évaluer les ressemblances et différences entre ces domaines et celui de la cybersécurité.

Ensuite, plusieurs mots-clés ont été utilisés pour trouver des textes en relation avec les sujets étudiés comme *interdisciplinary teams, team roles, cybersecurity teams, success factor cybersecurity* et *group success factors.* Une attention particulière a été accordée aux textes des quatre dernières années étant donné le contexte en évolution constante de la cybersécurité et ainsi favoriser la lecture des éléments plus récents ainsi que des avancées du domaine. Toutefois, si un article était jugé pertinent dû à son utilisation dans des articles ultérieurs reconnus par d'autres auteurs, il a été inclus dans la synthèse présentée de ce chapitre. Les articles ont été sélectionnés premièrement en fonction de leur titre, à l'aide de recherches effectuées avec ces mots-clés. Ceci a permis une première sélection rapide de sources qui pouvaient être pertinentes. Ensuite, une lecture du résumé de chaque article a été effectuée pour vérifier que l'article traitait du sujet à l'étude de ce mémoire. Suite à la lecture de l'article concerné, la méthode de *backwards reference searching* a été effectuée sur les sources bibliographiques de l'article pour identifier d'autres articles pertinents sur le sujet. Finalement, du *forward reference*

searching a également été effectué pour voir si de nouveaux articles sur le sujet ont cité l'article précédemment lu, et ainsi valider s'il y a eu des avancées sur le sujet. Cette diversification des sources d'information utilisées et l'utilisation de critères différents ont ainsi dressé un portrait global, à l'aide de plus d'une centaine de sources, du sujet de l'interdisciplinarité en cybersécurité qui est assez récent dans la littérature.

Ce chapitre est divisé en plusieurs sections et chaque section a un objectif précis qui permet de répondre à l'objectif du chapitre en entier qui est de recenser la littérature sur le sujet des équipes interdisciplinaires dans un contexte de cybersécurité. La première section du chapitre définit les concepts de collaboration et d'équipe interdisciplinaire qui seront utilisés tout au long de ce mémoire afin d'établir une base théorique sur les concepts principaux de cette étude. La deuxième section présente l'équipe ICIC et son impact sur la performance organisationnelle pour déterminer son influence et son importance au sein d'une organisation. Ensuite, la troisième section désigne les facteurs de succès pertinents pour une équipe ICIC interdisciplinaire ainsi que les indicateurs clés de performance rattachés à chacun des facteurs, ce qui contribuera à notre compréhension de la littérature en lien avec le premier objectif de recherche. Puis, la quatrième section contribuera à notre compréhension de la littérature en lien avec le deuxième objectif de recherche en indiquant les rôles clés à avoir au sein d'une équipe ICIC interdisciplinaire et les responsabilités associées à ces rôles. Finalement, la cinquième section illustre le cadre conceptuel proposé regroupant les facteurs de succès et rôles sélectionnés pour une équipe ICIC interdisciplinaire suite à la recension des écrits de recherche et les écrits professionnels.

2.1 Structures de collaboration

Cette première section commence par présenter les définitions des concepts en lien avec l'interdisciplinarité qui seront utilisés tout au long du mémoire. Ensuite, l'équipe interdisciplinaire est présentée, tout contexte confondu. Cette section permet d'établir la base des concepts principaux du mémoire et agit en guise d'introduction aux sections ultérieures qui se concentrent plus précisément sur l'équipe ICIC et sa composition.

2.1.1 Définir le concept de collaboration

Cette sous-section définit le concept de collaboration ainsi que d'autres concepts qui y sont liés.

Tout d'abord, le dictionnaire Larousse définit le mot équipe ainsi :

« Un ensemble de personnes travaillant à une même tache, une équipe de collaborateurs »

- (Larousse, 2020)

Cette définition est également présente dans la littérature, les auteurs définissant le concept d'une équipe comme un regroupement de deux personnes ou plus travaillant ensemble (Bronstein, 2003 ; Petri 2010 ; D'amour et al., 2005). Le travail en équipe est ainsi une collaboration entre plusieurs membres (Fewster-Thuente et Velsor-Friedrich, 2008), collaboration dans laquelle les membres sont interdépendants et ont des objectifs de travail communs (Salas, Cook et Rosen, 2008).

La définition du concept de collaboration est également très répandue à travers la littérature. Les définitions observées reprennent généralement les quatre mêmes éléments :

- Le partage ;
- La création d'un partenariat entre les membres de l'équipe ;
- Une interdépendance entre les membres et ;
- Le traitement de ce concept comme un processus dynamique.

Le partage, premier élément de la collaboration, englobe le partage de plusieurs composantes nécessaires à l'équipe comme les responsabilités, la prise de décision, les valeurs et la planification des activités (D'amour et al., 2005). Cet élément est pertinent afin de résoudre des conflits qui peuvent survenir au sein de l'équipe quant aux décisions à prendre au niveau opérationnel (Petri, 2010). Le deuxième élément, la création d'un partenariat, réfère au travail conjoint effectué par minimalement deux personnes (D'amour et al., 2005; Petri, 2010). De ce fait, chacun des partis doit comprendre les contributions possibles qu'amènent les autres partis

pour le bien commun de l'équipe. Le troisième élément, l'interdépendance entre les membres, représente la dépendance mutuelle entre ceux-ci. L'interdépendance au sein de l'équipe permet de maximiser la contribution individuelle et ainsi éventuellement mener à l'action collective qui sera bénéfique pour l'équipe et l'organisation dont elle fait partie (D'amour et al., 2005). Finalement, le quatrième élément définissant la collaboration est que celle-ci est un processus dynamique dans lequel les membres contribuent à l'amélioration du service offert par l'équipe, que ce soit par la structuration d'une action collective ou encore par un processus interpersonnel motivant (D'amour et al., 2005).

Les quatre éléments mentionnés dans le paragraphe précédent sont des éléments essentiels à la collaboration optimale au sein d'une équipe. Tel que mentionné au premier chapitre, l'environnement d'affaires est présentement en changement constant (Jacob et al., 2018), et les organisations doivent s'assurer que les équipes désignées de cybersécurité ont les ressources nécessaires afin de protéger l'actif informationnel (Caendra Inc, 2017). De plus, la complexité des besoins en termes de protection de cet actif pousse l'émergence de nouvelles structures d'équipe (Voyer, 2000). Cette complexité provient de l'augmentation du nombre d'incidents en cybersécurité et de leur sophistication (McCarthy Tétrault, 2017). L'utilisation de structures d'équipes qui diffèrent du modèle d'équipe habituel est également encouragée afin de contrer la problématique du manque de main d'œuvre pour faire face à la transformation numérique (Raza, 2019). Par modèle d'équipe habituel, on entend ici une équipe composée d'individus provenant de la même discipline, donc une équipe qui n'effectue que des activités qui sont en lien avec cette discipline. Par exemple, dans une équipe de conformité en cybersécurité, on retrouverait alors uniquement des individus qui effectueraient des actions en relation avec la conformité TI (entre autres : processus d'évaluation, vérification de la règlementation et vérification des responsabilités attitrées aux contrôles) (Lendick, 2019).

La figure ci-dessous, *Figure 2.1 Les différentes équipes de collaboration*, illustre les principales structures de collaboration potentielles au sein des équipes de travail.

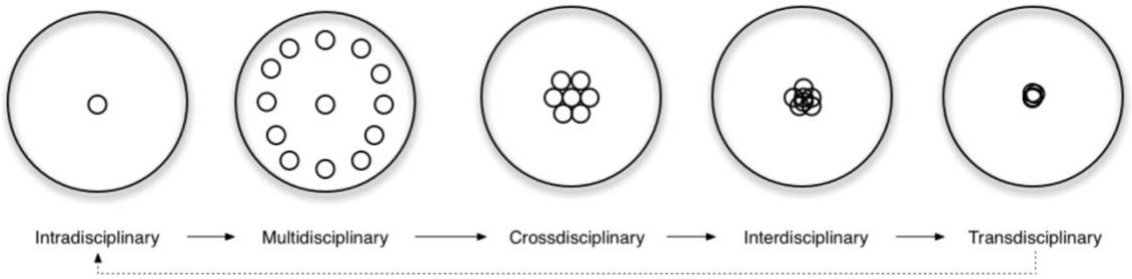


Figure 2.1 – Les différentes équipes de collaboration
Source : Jensenius, 2012

Chacune de ces structures est composée de ses propres caractéristiques, mais doit également posséder les quatre éléments essentiels à une collaboration optimale mentionnés plus haut. Plusieurs structures de collaboration combinent ainsi, entre autres, les compétences de différentes disciplines.

De la figure 2.1, les équipes intradisciplinaires et crossdisciplinaires ne sont pas des équipes retenues pour la suite de ce mémoire. L'équipe intradisciplinaire est composée d'une seule discipline (Jensenius, 2012) tandis que l'équipe crossdisciplinaire est comprise d'individus qui font des activités en relation avec un sujet externe à leur discipline respective (Seel, 2012). Ceci ne rejoint pas les objectifs de recherche de ce mémoire, car il n'y a pas d'intégration entre plusieurs disciplines au sein de ces structures et cette intégration est la piste de réflexion utilisée sur la problématique de la dimension humaine de la cybersécurité.

Afin de valider le choix de l'équipe interdisciplinaire pour ce mémoire, une synthèse des caractéristiques des trois équipes restantes de la figure 2.1 a été effectuée, soit l'équipe transdisciplinaire, l'équipe multidisciplinaire et l'équipe interdisciplinaire. Bien qu'un intérêt grandissant soit notable pour l'équipe interdisciplinaire (Raza, 2019), cette synthèse permet de valider le choix effectué également en comparant les composantes définissant ces équipes aux objectifs actuels des équipes en cybersécurité.

Le tableau ci-dessous, *Tableau 2.1 Structures de collaboration,* présente ces composantes. Suite au tableau, un résumé de cette synthèse est présenté.

Tableau 2.1 : Structures de collaboration

Composantes / Équipes	***Multidisciplinaire***	***Interdisciplinaire***	***Transdisciplinaire***
Intégration de différentes disciplines	***X***	***!***	***Approche holistique au-delà des disciplines***
Frontières établies entre disciplines	***!***	***X***	***X***
Échange de connaissances entre individus	***!***	***!***	***!***
Emphase sur le processus et non sur la solution finale	***X***	***Résolution de problèmes à l'aide des disciplines***	***Résolution de problèmes à l'aide de praticiens et bénéficiaires au-delà des disciplines***
Innovation	***X***	***Innovation perturbatrice***	***Innovation avec des perspectives non traditionnelles***
Création de nouvelles théories / nouveaux concepts	***X***	***X***	***!***
Légende : X - Composante non présente dans la structure et ! - Composante présente dans la structure			
Sources utilisées : (Aboelela et al., 2007); (Choi et Pak, 2006); (D'amour et al., 2005); (Jensenius, 2012); (Kestler, 2017); (Leahhey et al., 2017); (Mumumi, O'Reilly et Kaliannan, 2015); (Ness et Soreide, 2014); (Perignat et Katz-Buonincontro, 2019); (Priest, 2020); (Seel, 2012); (Tang et Werner, 2017); (Timmis et Williams, 2017); (Wognum et al., 2019).			

Bien que chacune des structures présentées a des avantages et des inconvénients, l'emphase du tableau a été placée sur les composantes qui définissent ces structures. L'objectif du tableau est de déterminer quelle structure est potentiellement la meilleure piste à suivre pour continuer l'étude de la problématique énoncée au chapitre 1. Cette problématique est celle de l'écart entre l'augmentation du nombre de menaces en cybersécurité et le manque de ressources humaines pour les contrer.

Trois éléments inférés du tableau permettent d'alimenter cette réflexion :

- **L'équipe multidisciplinaire n'offre pas d'intégration entre plusieurs disciplines.**

En effet, l'équipe multidisciplinaire est une équipe qui utilise les connaissances de plusieurs disciplines, mais chacune de ces disciplines demeure dans ses frontières (Choi et Pak, 2006). Ainsi, le partage s'arrête aux connaissances qui sont nécessaires pour résoudre le problème. L'équipe multidisciplinaire est une équipe de collaboration et non une d'intégration. Toutefois, dans la mise en contexte étudiée, la suggestion est faite que la création d'un ensemble (concepts, méthodes, théories, etc.) permet d'améliorer la prise de décision de l'équipe. De plus, les équipes multidisciplinaires sont considérées des équipes à effet additif, donc des équipes qui travaillent de façon séparée et collaborent pour permettre l'atteinte d'une solution (Choi et Pak, 2006). Chaque discipline présente son point de vue sur le problème d'affaires en fonction de la perspective qu'elle a l'habitude de prendre dans cette situation (Caldwell, 2015). Les équipes multidisciplinaires offrent moins d'interaction entre les membres (Kestler, 2017 ; Perignat et Katz-Buonincontro, 2019).

En parallèle, l'équipe interdisciplinaire est considérée comme une équipe interactive et l'équipe transdisciplinaire elle comme une équipe holistique (Choi et Pak, 2006). Une équipe holistique va au-delà des disciplines et le résultat de sa formation est une nouvelle approche de travail, approche qui n'est pas celle d'aucune des disciplines la formant (Caldwell, 2015). La réflexion a ainsi continué entre l'équipe transdisciplinaire et celle interdisciplinaire.

- **L'équipe transdisciplinaire mène à la création de nouvelles approches.**

La littérature démontre qu'il existe des similitudes entre l'équipe interdisciplinaire et l'équipe transdisciplinaire, le résultat de l'interaction au sein de chaque équipe est toutefois différent. L'équipe interdisciplinaire analyse puis développe les liens entre les disciplines qui la composent

pour créer une entité unie (Choi et Pak, 2006). L'équipe transdisciplinaire, elle, intègre premièrement les disciplines puis devient une entité qui transcende leurs approches respectives (Choi et Pak, 2006). Les deux équipes sont composées de disciplines qui vont affecter la perception des autres disciplines présentes dans l'équipe (Caldwell, 2015).

Le travail effectué conjointement par les différentes disciplines d'une équipe transdisciplinaire, afin de créer et d'innover sur des concepts, des théories ou des méthodes de recherche qui vont plus loin que ce à quoi les disciplines sont habituées (Aboelela, 2007). L'innovation n'est habituellement pas présente au sein d'une équipe multidisciplinaire et est présentée dans une équipe interdisciplinaire sous le rôle d'une perturbation de l'environnement d'affaires. Par contre, dans une équipe transdisciplinaire l'innovation provient de l'emphase de l'utilisation de perspectives non traditionnelles par les disciplines (Seel, 2012). Pendant que l'équipe interdisciplinaire résout des problèmes à l'aide des disciplines et intègre les outils de celles-ci, l'équipe transdisciplinaire offre une intégration avec des éléments externes à ces disciplines comme par exemple des bénéficiaires (Tang et Werner, 2017). Toutefois, l'équipe interdisciplinaire est l'équipe qui permet d'intégrer des éléments divers en prenant en compte les différentes perspectives pour améliorer la capacité de prise de décision (Aboelela, 2007). Ainsi, bien que l'équipe transdisciplinaire apporte des points innovateurs intéressants, elle ne répond pas précisément à la problématique ici étudiée.

- **L'équipe interdisciplinaire s'inspire des perspectives de chaque discipline pour améliorer la capacité de prise de décision collective.**

Finalement, l'équipe interdisciplinaire prend en compte chacune des disciplines et tente de trouver des liens entre les perspectives de chacun pour ensuite les harmoniser lors de la prise de décision commune. Les théories et pratiques de chaque discipline sont mélangées et intégrées tout au long du processus de prise de décision (Seel, 2012). Ainsi, bien que les équipes multidisciplinaires travaillent en silos pour permettre un avancement des disciplines de façon

individuelle et que les équipes transdisciplinaires créent de nouvelles connaissances à partir des perspectives existantes, les équipes interdisciplinaires **coopèrent** pour utiliser les connaissances diverses existantes (Tang et Werner, 2017). Tout ceci dans le but d'améliorer la performance de l'organisation.

De plus, les théories et cadres des différentes disciplines sont utilisés et intégrés afin de lier les éléments semblables (Aboelela, 2007). En faisant ceci, la méthodologie utilisée n'est pas limitée à une seule discipline et nécessite continuellement les connaissances, perspectives et compétences de toutes les disciplines pour l'avancement de l'équipe et de son objectif principal (Aboelela, 2007). L'équipe interdisciplinaire aboutit donc à des solutions qui vont au-delà des frontières d'une seule discipline (Kestler, 2017).

Cette réflexion a permis de confirmer le potentiel que représente l'équipe interdisciplinaire dans la mise en contexte étudiée de cette étude. L'équipe interdisciplinaire a ainsi été retenue pour trois raisons :

1. L'équipe est orientée vers la prise de décision à l'aide de l'intégration des différentes disciplines et de leurs perspectives. En cybersécurité, ceci est un avantage afin de réduire l'impact potentiel d'un cybercrime qui peut provenir d'une multitude d'angles différents, comme une attaque d'hameçonnage, de rançongiciel ou un vol d'équipement.

2. Au sein de l'équipe interdisciplinaire, la coopération est favorisée par la nature même de l'équipe. Une plus grande quantité d'interactions permet également d'avoir accès à un plus grand nombre de connaissances et d'outils afin de déterminer le meilleur moyen afin de répondre aux menaces grandissantes envers les organisations (thinkCSC, 2018).

3. Une équipe interdisciplinaire a un impact qui dépasse les frontières des disciplines. Donc, un plus grand impact sur le domaine en entier. Étant donné que la cybersécurité est en changement constant face aux menaces de cybercriminels qui sont de plus en plus en

contrôle de l'infrastructure technologique (Gouvernement du Canada, 2020), l'équipe serait ainsi en mesure d'influencer l'avancement de la cybersécurité de façon globale.

L'équipe interdisciplinaire présente de nombreux avantages pour une organisation, dont une amélioration de la capacité d'adaptation face à un environnement en changement constant, une augmentation du partage d'expertise diverse au sein d'une même équipe et l'augmentation de l'efficacité de l'équipe face à des situations ou incidents précis (St-Cyr Bouchard, 2013).

La sous-section qui suit définit l'équipe interdisciplinaire.

2.1.2 Équipe interdisciplinaire : définition et exemples

Cette sous-section présente une définition de l'équipe interdisciplinaire et conclue en détaillant comment elle s'illustre dans un contexte de cybersécurité.

L'équipe interdisciplinaire est définie comme une équipe permettant la flexibilité, la réactivité et la créativité de ses membres et ainsi une adaptation à un environnement d'affaires qui est de plus en plus complexe pour l'organisation (Langevin, 2004).

Les équipes interdisciplinaires sont des équipes dans lesquelles les professionnels possèdent et travaillent vers un but commun. Dans cette équipe, un plus grand degré de collaboration est requis, car les interactions ne sont plus limitées à certains projets, mais se produisent en continu (D'amour et al., 2005)**.** Le résultat de ces interactions est de façon générale favorable, car des solutions à des problèmes plus complexes peuvent être trouvées grâce au jumelage des différentes compétences des membres de l'équipe.

Pour la suite de ce mémoire, l'équipe interdisciplinaire est une équipe définie ainsi suite au survol effectué dans la littérature sur le sujet :

Une intégration de différentes disciplines composée d'un partage des responsabilités entre les membres et d'un travail interactif orienté vers une prise de décision efficace visant l'aboutissement à des solutions innovatrices et créatives.

Les paragraphes suivants détaillent les caractéristiques de cette définition. Étant donné que ce mémoire place l'emphase sur la performance de l'équipe, les explications de chacune des caractéristiques de la définition sont des explications dans un contexte de travail d'équipe et non dans un contexte de travail individuel.

1. Intégration de différentes disciplines

Une équipe interdisciplinaire est une équipe d'individus provenant de plusieurs disciplines (Bronstein, 2003; San Martin-Rodriguez et al., 2005; Fewster-Thuente et Velsor-Friedrich, 2008; Petri, 2010). Chacune des disciplines incluses dans l'équipe est nécessaire à la réalisation d'objectifs de travail et donc l'opinion de tous les membres est nécessaire (Petri, 2010). Le jumelage des disciplines différentes en une seule équipe contribue à la réalisation de l'objectif commun (Bronstein, 2003). De plus, cette intégration de plusieurs disciplines permet entre autres l'apport de diverses compétences techniques et managériales du domaine ce qui permet de meilleures synthèses et analyses de situations.

2. Partage des responsabilités

La deuxième caractéristique est celle du partage des responsabilités au sein de l'équipe, peu importe les disciplines présentes. Tous les membres doivent être tenus responsables de l'atteinte de résultats optimaux (Poulin, 2006). C'est une caractéristique différenciant l'équipe interdisciplinaire à l'équipe multidisciplinaire par exemple, qui elle travaille en silos. Dans une équipe interdisciplinaire, toutes les disciplines travaillent en collaboration vers un but commun (Poulin, 2006).

3. Travail interactif

La fusion des différentes disciplines et le partage des responsabilités mènent à la troisième caractéristique, le travail interactif. Cette caractéristique est empreinte d'une définition de coopération entre toutes les disciplines. Cette coopération doit être saine afin de mener à une synergie positive les disciplines. Grâce à ces deux éléments, soit la coopération et la synergie d'équipe, la réalisation des objectifs communs au sein de l'équipe est ainsi renforcée.

4. Prise de décision efficace

L'élément central d'une équipe représente son objectif principal qui doit être commun pour tous les membres de l'équipe. Par exemple, pour une équipe en santé, l'élément central est le client et son bien-être (Poulin, 2006). C'est le bien-être du client qui pousse l'équipe à bien performer et à trouver de bonnes solutions. Ces solutions sont soulevées suite à une prise de décision efficace. L'équipe interdisciplinaire constitue un mélange des connaissances, outils et théories des différentes disciplines au sein de l'équipe (Kestler, 2017 ; Perignat et Katz-Buonincontro, 2019). Ce mélange permet à l'équipe de sélectionner et d'intégrer les éléments essentiels à la prise de décisions qui mènera vers une solution qui prendra en compte toutes les disciplines.

5. Solutions innovatrices et créatives

Finalement, la dernière caractéristique de l'équipe interdisciplinaire est possible suite à la mise en place de toutes les caractéristiques précédentes. Cette dernière caractéristique est celle des solutions innovatrices et créatives (CAPP, 2017). Au sein d'une équipe interdisciplinaire, l'innovation est de nature perturbatrice, soit en tenant en compte tous les éléments qui changent dans l'environnement d'affaires de l'organisation. Plus précisément, dans le cas de l'équipe ICIC ici à l'étude, l'objectif est de réagir plus efficacement à des menaces grandissantes de la part de cybercriminels (Chang et Ho, 2006). Étant donné que ces cybercriminels diversifient leurs méthodes et contournent les moyens de protection mis en place par les organisations, ces

équipes interdisciplinaires peuvent jumeler les compétences de différents experts pour préparer une défense plus efficace. Cette défense a pour objectif d'aider l'organisation à contrer un plus grand nombre d'attaques.

La section qui suit place l'équipe interdisciplinaire dans le contexte d'un incident de cybersécurité et lie sa performance à celle de l'organisation.

2.2 Équipe interdisciplinaire en cas d'un incident en cybersécurité et sa performance

Cette deuxième section présente en détail l'équipe ICIC interdisciplinaire ainsi que ses avantages et défis afin de justifier le choix de l'équipe interdisciplinaire dans ce contexte spécifique. Finalement, la notion de performance au sein d'une équipe ICIC interdisciplinaire est définie ainsi que son importance pour la performance du reste de l'organisation.

2.2.1 Portrait général d'une équipe ICIC interdisciplinaire

Pour revenir au contexte de cybersécurité, **l'équipe ICIC interdisciplinaire proposée dans ce mémoire tente de prévenir, détecter, investiguer et répondre à des incidents en cybersécurité** qui pourraient avoir un impact sur l'organisation, ses activités ou clients (Cyware , 2018). L'équipe a besoin de professionnels de différentes disciplines pour coordonner plusieurs fonctions de sécurité et flux d'informations concernant ces différentes disciplines comme la compréhension des menaces, les opérations TI et les opérations de sécurité (STM, 2020). L'objectif est d'accélérer la réponse de l'organisation face aux incidents de cybersécurité tout en réduisant les risques et coûts organisationnels (Cyware, 2018). L'organisation est ainsi mieux préparée aux différentes formes de cyberattaques qui peuvent survenir, car elle a une équipe en place qui a les compétences nécessaires pour répondre à celles-ci, le tout dans un délai identifié comme raisonnable par l'organisation (STM, 2020). Bien qu'il ne soit pas possible d'enlever tout risque qu'un incident en cybersécurité se produise, le but est de minimiser le risque dans un premier

temps pour ensuite être prêt au cas où un incident se produit (Cichonski et al., 2012 ; Van der Kleij, Kleinhuis et Young, 2017).

Cette équipe d'intervention vient compléter le travail effectué par d'autres équipes de sécurité de son organisation et doit être différenciée à celles-ci. Entre autres, plusieurs organisations ont maintenant des centres d'opérations en sécurité (SOC). Ces centres se concentrent sur la protection technique des données et systèmes de l'organisation (Stern, 2017). Toutefois, le SOC ne développe pas la stratégie de sécurité, mais s'occupe plutôt de l'opérationnalisation de ce processus (De Groot, 2020). Cette opérationnalisation est faite à l'aide d'outils de surveillance (Stern, 2017), d'analyses criminelles avancées, de cryptanalyse et de la compréhension de logiciels malveillants (De Groot, 2020). Le SOC doit travailler et être arrimé avec l'équipe d'intervention afin de la supporter dans ses décisions (De Groot, 2020). Toutefois, l'équipe a un mandat plutôt technique, axé sur les données. L'équipe ICIC interdisciplinaire est donc séparée au SOC, elle s'occupe de la gestion du processus d'intervention tandis que le SOC est axé sur l'opérationnalisation de la protection technique. Les deux équipes doivent collaborer afin de protéger l'actif informationnel de l'organisation.

La figure ci-dessous (*2.2 Une illustration d'une équipe ICIC interdisciplinaire)*, présente une illustration possible de l'équipe ICIC interdisciplinaire en plaçant l'objectif principal de cette équipe au centre, la protection de l'organisation et de ses clients à travers l'actif informationnel. Les professions dans cette figure interagissent entre elles et également avec l'objectif principal de l'équipe. À noter que cette figure agit à titre d'exemple et qu'une équipe ICIC interdisciplinaire pourrait être composée d'individus provenant d'autres professions.

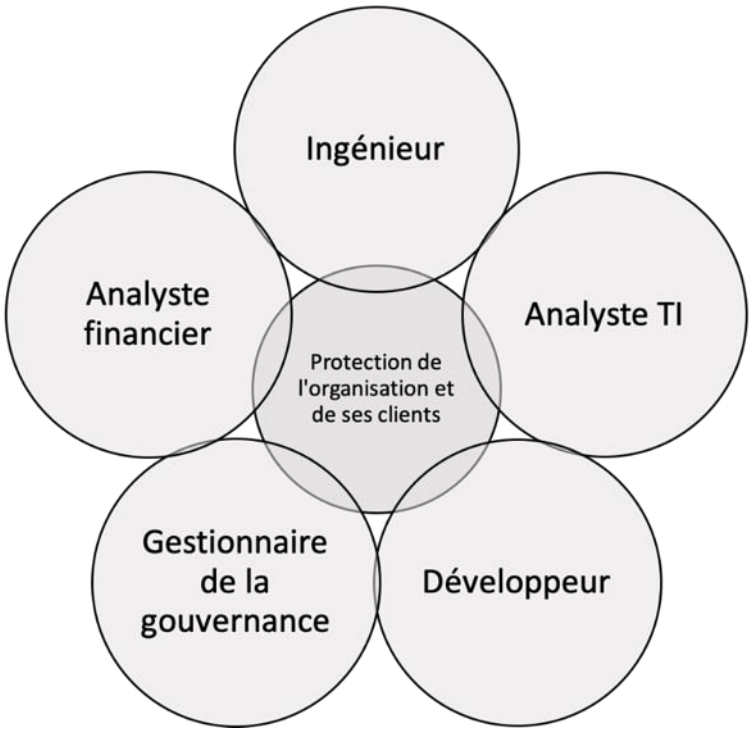


Figure 2.2 – Une illustration d'une équipe ICIC interdisciplinaire

Dans cette étude, le nombre d'équipes ICIC interdisciplinaires nécessaires par organisation n'est pas évalué. La discussion se porte plutôt sur la composition possible de cette équipe pour qu'elle soit efficace. La sous-section suivante, 2.2.2, présente les avantages principaux de l'implantation d'une équipe ICIC interdisciplinaire au sein de son organisation.

2.2.2 Avantages d'une équipe ICIC interdisciplinaire

Cette sous-section présente les avantages organisationnels découlant de l'intégration de l'équipe ICIC interdisciplinaire au reste de l'organisation. Premièrement, le tableau ci-dessous (*Tableau 2.2 Avantages d'une équipe d'intervention en cas d'incident en cybersécurité)* énonce une synthèse des cinq avantages principaux qu'une organisation peut décerner lors de la création d'une telle équipe. Les cinq avantages ne représentent pas une liste exhaustive, mais sont ceux qui revenaient le plus souvent lors du survol de la littérature. De plus, chaque avantage a été lié

à une des composantes de la définition de l'équipe ICIC interdisciplinaire. Les paragraphes qui suivent ce tableau offrent une synthèse de ces avantages.

Tableau 2.2 : Avantages d'une équipe ICIC interdisciplinaire

Avantage	Description	Lien avec la définition ICIC	Sources principales consultées
Complémentarité de l'expertise en cybersécurité	- Le travail à plusieurs permet de rassembler plusieurs compétences et connaissances nécessaires à la préparation face aux cybercrimes	Intégration de différentes disciplines	(Turcotte, 2005); (Nancarrow at al., 2013); (Steinke et al., 2015); (Blair, Hall et Sobiesk, 2019).
Un meilleur traitement de l'information	- Grâce au travail d'équipe lors d'un incident - Influence la productivité, l'adaptabilité et la créativité de l'équipe	Partage des responsabilités	(Gladstein, 1984); (Hackman, 1987); (Salas et al., 2005); (Turcotte, 2005); (Laplante, 2007).
Priorisation des risques améliorée	- Risques évalués en fonction de faits soulevés à travers plusieurs disciplines - Vue d'ensemble - Coopération	Travail interactif	(Turcotte, 2005); (Caendra Inc., 2017); (Blair, Hall et Sobiesk, 2019).
Gestion améliorée des frontières d'attaque	- Méthodologie constante utilisée pour gérer un incident - À l'aide de plusieurs activités : analyse de l'événement, triage des informations recueillies, gestion de l'incident informatique par les acteurs appropriés - Comparable à un audit interne qui permet de découvrir des pièges en cybersécurité	Prise de décision efficace	(Caendra Inc., 2017); (Cichonski et al., 2012); (Cyware, 2018).
Innovation face à la gestion d'incidents en cybersécurité	- Jumelage de services de sécurité informatique - Utilisation de technologies d'automatisation - Intégration des services jugés essentiels à l'organisation pour une meilleure protection	Solutions créatives et innovatrices	(Accenture 2018); (Glastein, 1984); (Hackman; 1987); (Beaumier et Lescarbeau, 2001); (Salas et al., 2005); (Laplante, 2007).

Les cinq avantages présentés dans le tableau ci-haut permettent individuellement et collectivement l'atteinte d'un bénéfice global ; une analyse plus rapide et plus précise d'incidents en cybersécurité.

L'intégration des différentes disciplines au sein de l'équipe interdisciplinaire permet une **complémentarité de l'expertise en cybersécurité** (Steinke et al., 2015). Ceci permet une approche proactive dans le mode de fonctionnement de l'équipe (Nancarrow et al., 2013). Une approche proactive est une approche dans laquelle les professionnels qui composent l'équipe ICIC sont unifiés face aux cyberattaques que l'organisation pourrait subir. Cela est habituellement effectué en tentant de prévenir le plus possible les situations d'incident informatique possibles (Gouvernement du Québec, 2017). Outre l'approche proactive qui caractérise une équipe ICIC interdisciplinaire, les activités de cette équipe facilitent également l'action face aux cybercrimes.

Ainsi, l'équipe ICIC interdisciplinaire peut effectuer plusieurs opérations qui faciliteront les activités de l'organisation en relation aux cybercrimes (Booz Allen Hamilton Inc., 2018). Une de ces opérations est un **meilleur traitement de l'information**, soit comment celle-ci est assimilée ou modifiée. Le partage de responsabilités favorise ce traitement de l'information amélioré grâce à l'emphase qui est alors placée sur le travail d'équipe. Cette importance associée au travail d'équipe crée un travail interactif qui mène à une meilleure **priorisation des risques**. Ces risques sont alors évalués en fonction de faits recueillis et non de perceptions de la part des individus. Ceci est également possible grâce à la complémentarité des disciplines présentes.

Ensuite, la prise de décision efficace mène à une **gestion améliorée des frontières d'attaques**. Cette gestion améliorée est également possible grâce à tous les avantages précédemment mentionnés. Elle permet, entre autres, de découvrir des pièges posés en cybersécurité sur les organisations (Caendra Inc., 2017).

De plus, l'équipe peut également concevoir un plan d'action amélioré lors d'incident en cybersécurité, car la cohésion sociale et l'expertise des membres lui permettent d'innover et de renouveler ses idées. Le support opérationnel est augmenté grâce à la participation de différentes disciplines au sein d'une même équipe. Il s'agit donc une fusion de stratégies, de tactiques et de plans opérationnels pour une prédiction, analyse et réaction plus rapide aux cyberattaques (Cyware, 2018). Tous ces éléments augmentent la visibilité de la cybersécurité au

sein des organisations, tout en réduisant les délais pour anticiper et réagir aux cyberattaques et ainsi protéger plus adéquatement les actifs de l'organisation (Booz Allen Hamilton Inc., 2018). L'organisation peut alors agir de façon plus cohésive et prendre les meilleures décisions possibles au bon moment (Cyware, 2018; Booz Allen Hamilton Inc., 2018).

Par ailleurs, l'équipe ICIC interdisciplinaire permet de solidifier la chaîne de valeur et l'écosystème de l'organisation en permettant à cette dernière de devenir plus résiliente à travers toutes ses fonctions. Une organisation qui innove et qui solidifie sa chaîne de valeur peut ensuite encore plus croître et innover, car elle a plus de contrôle sur ses activités (Accenture, 2018). La priorisation d'utilisation de solutions créatives et innovatrices au sein d'une équipe ICIC interdisciplinaire pousse son **innovation sur le processus de gestion des incidents en cybersécurité**. Cette innovation permet d'éviter le choix d'une solution qui serait alors prématurée. Finalement, les situations d'innovation et de résolution de problèmes sont favorisées par la diversité présente dans ce type d'équipe (Langevin, 2004). La sous-section qui suit présente les défis encourus lors de la création d'une équipe ICIC interdisciplinaire. Cette sous-section est nécessaire afin de dresser le portrait de l'influence que ce type d'équipe peut avoir sur son organisation.

2.2.3 Défis d'une équipe ICIC interdisciplinaire

Similaire à la sous-section précédente, cette sous-section présente premièrement un tableau, le *Tableau 2.3 Défis d'une équipe d'intervention en cas d'incident en cybersécurité*, qui résume les différents défis auxquels fait face une équipe ICIC interdisciplinaire. Ces défis sont ensuite décrits en deuxième partie dans les paragraphes qui suivent. Ces défis ne représentent pas une liste exhaustive de tous les défis possibles, mais ont été sélectionnés, car ils étaient souvent présents dans la littérature des équipes interdisciplinaires, des équipes en cybersécurité ou encore celles d'intervention. De plus, chacun des défis retenus dans le tableau présenté ci-dessous est un défi qui peut affecter négativement la mise en place et le fonctionnement de l'équipe, en plus de

mettre en danger la bonne exécution de chacune des caractéristiques présentées dans la définition de l'équipe interdisciplinaire.

Tableau 2.3 Défis d'une équipe ICIC interdisciplinaire

Défi ICIC	Description du défi	Lien avec la définition ICIC	Source(s)
Influence des disciplines une sur l'autre	Affecte les actions posées et leur ordre lors d'un incident en cybersécurité.	Intégration de différentes disciplines	(Beaumier et Lescarbeau, 2001) ; (Nancarrow et al., 2013) ; (St-Cyr Bouchard, 2013) ; (St-Cyr Bouchard et Saint-Charles, 2018).
Manque de compétences en cybersécurité	Manque de main d'œuvre spécialisée en cybersécurité ce qui augmente la demande d'individus pouvant faire partie de ce type d'équipe.	Partage des responsabilités	(Nancarrow et al., 2013) ; (Weil, 2017) ; (Jacob et al., 2018) ; (Olyaei, 2019) ; (MacKinnon et Rampado, 2020).
Problèmes de communication et de cohésion	Les différentes disciplines doivent apprendre à travailler afin de ne pas perdre de vue leur tâche principale qui est celle d'intervenir en équipe.	Travail interactif	(Beaumier et Lescarbeau, 2001) ; (Tang et Hsiao, 2013) ; (Moore, 2019).
Manque de confiance	Les visions perceptions, points de vue, outils, modèles différents peut mener à une difficulté de prise de décision.	Prise de décision efficace	(Abramson , 1990) ; (Voyer, 2000) ; (D'amour et al., 2005) ; (Poulin, 2006) ; (St-Cyr Bouchard, 2013).
Clarté des rôles	L'emphase est placée sur les éléments techniques et non sur les rôles organisationnels qui peuvent pousser le processus innovateur d'intervention.	Solutions innovatrices	(Laplante, 2007) ; (Campbell, Saner et Bunting, 2016) ; (MacKinnon et Rampado, 2020) ; (Peterson et al., 2020).

Premièrement, **l'influence des disciplines une sur l'autre** dû à leur intégration au sein d'une même équipe peut affecter la priorisation qui est faite sur l'ordre des actions à poser lors d'un incident. Ceci peut avoir une influence sur les structures de pouvoir au sein de l'équipe et mener à une augmentation des conflits (St-Cyr Bouchard et Saint-Charles, 2018). Bien que cette caractéristique soit valable pour toute équipe interdisciplinaire, elle est pertinente à relever dans un contexte de cybersécurité. Lors d'un incident de cybersécurité, les bonnes actions doivent être rapidement posées afin de diminuer l'impact négatif potentiel de cet incident. Ainsi, si l'équipe n'est pas unie dans son intégration, l'emphase sera plutôt portée sur la négociation que sur l'action. Ceci engendrait des conséquences directes pour l'organisation. Cette influence peut

provenir lorsque certaines disciplines ont plus de poids, car elles représentent un plus grand bassin de connaissances pour une situation particulière (St-Cyr Bouchard, 2013).

Ensuite, le manque de main d'œuvre en cybersécurité représente un défi pour les équipes ICIC interdisciplinaires qui pourraient alors avoir un **manque de compétences dans leurs équipes**. Bien que certaines organisations accordent un grand budget à l'acquisition de talents en cybersécurité, la forte demande de ceux-ci dans le domaine rend le marché compétitif et certaines équipes se retrouvent ainsi en manque de compétences critiques de cybersécurité (Weil, 2017). Ce manque de compétences alourdit le processus de partage des responsabilités, car certaines disciplines doivent alors prendre plus de responsabilités auxquelles elles ne sont pas habituées ce qui ralentit l'équipe lorsqu'un incident se produit.

Troisièmement, **les problèmes de communication et de cohésion** dans n'importe quelle équipe rendent le travail interactif beaucoup plus compliqué. Dans une équipe ICIC interdisciplinaire, ce défi a un impact énorme. La cybersécurité est de plus en plus intégrée aux fonctions d'affaires d'une organisation qui ne peut plus opérer sans cette intégration. Ainsi dès que ce type de problème survient dans une équipe qui agit directement sur la santé de la cybersécurité de l'organisation, c'est l'entièreté de l'actif informationnel de l'organisation qui devient chamboulé. Ceci mène donc à une perte de temps, d'énergie et de ressources dans une équipe interdisciplinaire (St-Cyr Bouchard, 2013) qui devrait plutôt se concentrer sur sa tâche principale d'intervention.

Puis, **le manque de confiance entre les disciplines** peut engendrer une prise de décision moins efficace. La collaboration dans une telle équipe vient chambouler les construits et règles spécifiques établis dans chaque discipline (D'amour et al., 2005). Un individu provenant d'une discipline quelconque aura une vision qui pourrait être différente d'un individu provenant d'une autre discipline (San Martin-Rodriguez et al., 2005). Le défi est alors ici d'adopter une vision de groupe qui permettra de répondre aux objectifs de celui-ci, et ce sans s'attarder sur les visions

individuelles de chacun. En cybersécurité, ceci peut se traduire par une mauvaise compréhension de l'apport de chaque discipline lors de l'intervention.

Finalement, **la clarté des rôles** au sein d'une équipe ICIC interdisciplinaire reste un élément à développer. Ces rôles doivent être décrits et compris (Laplante, 2007). Pour ce faire, des cadres plutôt techniques, tel que NICE, existent. Ces cadres sont construits en fonction des habiletés des individus (Peterson et al., 2020) et des requis fonctionnels des postes (Campbell, Saner et Bunting, 2016). D'autres cadres, comme celui de Campbell (2016), évaluent le choix de tels rôles en fonction de la charge cognitive des tâches à effectuer. Ces tâches cognitives sont par exemple le développement de solutions, l'exploitation des données ou encore la défense face à des cyberattaques (Campbell, Saner et Bunting, 2016). Finalement, MacKinnon et Rampado (2020) eux ont désigné des rôles sous l'angle de la dimension humaine et organisationnelle. C'est-à-dire, ils se basent sur les capacités individuelles des employés afin de leur assigner des rôles (MacKinnon et Rampado, 2020). Toutefois, l'angle adopté dans ce mémoire est celui de l'analyse des pratiques de l'équipe afin de déterminer ce qui lui attribue un succès. Pour ce faire, des facteurs de succès sont premièrement identifiés au niveau de l'équipe, contrairement à un niveau individuel.

Enfin, la nature complexe du domaine de cybersécurité demande nécessairement l'intégration de différentes disciplines afin d'obtenir la profondeur nécessaire pour répondre aux demandes du domaine. Ainsi, malgré ces défis, il est impératif de trouver des pistes potentielles afin d'avoir une équipe performante. La prochaine sous-section se concentre sur ceci et détaille les raisons derrière le choix de l'utilisation des facteurs de succès et comment ceux-ci influencent l'atteinte de cette performance.

2.2.4 Équipe ICIC interdisciplinaire et performante

Dans ce mémoire, la performance de l'équipe ICIC n'est pas évaluée ; l'accent est mis plutôt sur la composition de cette équipe. Toutefois, la littérature relève le lien serré entre le caractère interdisciplinaire et la performance d'une équipe. Ainsi, cette sous-section a pour but de dresser le portrait de l'influence de la performance sur la composition de l'équipe ICIC interdisciplinaire. Pour ce faire, cette sous-section présente d'abord la définition du concept de performance tel qu'il sera utilisé dans la suite de ce mémoire. Ensuite, le concept est rattaché à l'équipe pour décrire le concept d'équipe performante dans le domaine de la cybersécurité. Finalement, la sous-section se termine par une description de l'impact d'une équipe ICIC interdisciplinaire sur la performance organisationnelle.

2.2.4.1 Définir le concept de performance

Initialement, le terme performance a vu le jour vers la fin du 15^{e} siècle et était défini comme un accomplissement ou la complétion de quelque chose (Douglas Harper, 2020). De nos jours, le terme a évolué pour premièrement intégrer un nouvel élément qui est celui du résultat. Performance est maintenant synonyme de résultat et de plus, le terme n'est plus nécessairement synonyme de quelque chose de positif étant donné qu'une performance peut être tant positive que négative. Ainsi, la définition retenue du concept de performance pour le reste de ce mémoire, celle du Larousse, est celle-ci :

« Résultat obtenu dans un domaine précis par quelqu'un, une machine, un véhicule »
(Larousse, 2020).

La sous-section dans son entièreté est bâtie autour du fait qu'une performance est un résultat qui peut être positif ou négatif. L'équipe performante est expliquée ci-dessous pour placer le concept de performance dans un contexte organisationnel. À noter que pour les fins de ce mémoire, chaque mention du concept d'équipe est celui d'une équipe de travail, bien qu'une équipe puisse être retrouvée dans d'autres contextes de la société également.

2.2.4.2 Définir le concept d'équipe performante

Pour débuter, en guise de rappel du premier chapitre, le concept d'équipe est défini comme suit dans cette étude :

« Une structure sociale dans laquelle les membres qui la composent sont interdépendants et ont des objectifs de travail communs. » (Salas, Cook et Rosen, 2008)

En tenant en compte la définition de la notion de performance présentée plus haut ainsi que la notion d'équipe, une description de l'équipe performante peut maintenant être donnée.

Bien que le concept de performance n'ait ni une connotation positive ni une connotation négative, l'adjectif du concept, soit performant(e), a lui une connotation positive (Larousse, 2020). Donc, il est possible d'inférer qu'une équipe performante est une équipe qui obtient de très bons résultats. Une attention particulière portée sur la performance d'une équipe de travail présente plusieurs avantages pour celle-ci comme une meilleure contribution de tous les membres, un meilleur effort ou encore une participation plus engagée. En cybersécurité, ceci se traduit par l'intégration des différentes disciplines, leur partage, leur interaction, la prise de décision commune et un processus de développement de solutions innovatrices dans un contexte actuellement tendu. Cette équipe doit être en mesure de bien répondre à un incident en cybersécurité pour protéger l'actif informationnel de son organisation.

Les conditions du succès de cette performance sont définies dans le contexte de cette étude en facteurs clés de succès. Leur suivi est possible à l'aide d'indicateurs clés de performance. Ces indicateurs sont des éléments devant bien fonctionner pour que l'équipe soit performante, une attention doit donc leur être donnée de façon constante (Fortune et White, 2006). En plus de déterminer si l'équipe atteint les objectifs établis, ces indicateurs permettent un suivi des opérations effectuées par l'équipe, si elles aident à une bonne performance et quels éléments au sein de ces opérations doivent être améliorés (Iannucci et Garland, 2020). Dans le cadre de

cette étude, les différents éléments de la méthode SMART pour les objectifs (Spécifique, Mesurable, Atteignable, Réaliste et Temporel) (INSPQ, 2016) ont été appliqués aux indicateurs clés de performance. Ceci a permis de délimiter quels indicateurs devaient être retenus.

L'équipe performante a un impact marquant sur le reste de l'organisation. Ce lien avec le reste de l'organisation est expliqué ici-bas.

2.2.4.3 Impact d'une équipe ICIC interdisciplinaire sur la performance organisationnelle

Toute équipe d'intervention a un rôle à jouer dans la performance organisationnelle. Une équipe performante est en apprentissage constant et essaye continuellement d'innover, de s'améliorer et de créer de la valeur pour le reste de l'organisation (Reina, 2020). Dans ce mémoire, l'équipe performante est une constante dans l'étude. L'équipe ICIC interdisciplinaire est une équipe jugée performante et sa performance n'est pas mesurée. Plutôt, l'identification des éléments lui permettant d'atteindre une performance optimale est développée. Avant de se pencher sur le rôle de l'équipe ICIC interdisciplinaire sur la performance organisationnelle, il est pertinent d'analyser celui de toute équipe d'intervention sur celle-ci.

Une équipe d'intervention favorise la performance organisationnelle de plusieurs façons. Premièrement, une équipe d'intervention permet de centraliser les ressources pertinentes au même endroit. Cela réduit la possibilité d'un bloquant potentiel à la gestion du processus d'incidents. De plus, cette centralisation permet une meilleure gestion de l'information. Une stabilité s'installe alors au sein du processus ce qui améliore la performance organisationnelle (Kong et al., 2015). Deuxièmement et plus précisément au niveau de l'intervention en cas d'incident, une équipe d'intervention permet de protéger l'actif informationnel de l'organisation. Cette protection agit contre différentes menaces internes et externes pouvant nuire à l'organisation et à ses clients. L'équipe d'intervention vient protéger la confidentialité, l'intégrité et la disponibilité des données lors de telles menaces (Ursillo et Arnold, 2019). Troisièmement, l'apport de l'équipe d'intervention sur la performance organisationnelle peut également être mesuré en fonction de termes économiques et opérationnels. Une réduction des délais de

traitement dû à la centralisation des ressources permet à l'organisation d'améliorer sa posture financière en ce qui concerne la gestion d'incidents. De façon opérationnelle, cela s'illustre par la pertinence d'une telle équipe pour les différentes parties prenantes de l'organisation (Tahir, 2020). Pour le cas d'une équipe d'intervention, tant les fournisseurs que les employés et les clients d'une organisation veulent s'assurer que celle-ci aille le contrôle sur ses processus. Ils veulent également s'assurer que l'organisation met en place les contrôles nécessaires pour intervenir lorsqu'une menace survient. L'équipe d'intervention démontre ainsi de plusieurs façons son implication au niveau de la performance organisationnelle.

En ajoutant le concept d'interdisciplinarité à l'équipe ICIC, la performance organisationnelle est augmentée. Les différents avantages d'avoir une équipe ICIC interdisciplinaire mènent à cette augmentation. La complémentarité de l'expertise, l'amélioration du traitement de l'information, l'amélioration de la priorisation des risques, l'amélioration de la gestion des frontières d'attaques et l'innovation possible sur le processus de gestion d'incidents sont tous des points développant cette influence sur la performance organisationnelle. Entre autres, l'intégration de plusieurs disciplines permet un meilleur partage de responsabilités et un travail interactif qui mène vers une prise de décision plus efficace que lorsque l'équipe n'est composée que d'une discipline.

Cette section a débuté avec une présentation de l'équipe ICIC interdisciplinaire. Ensuite, les avantages principaux de celle-ci ont été présentés, comme entre autres une gestion améliorée des frontières d'attaque. Puis, ses défis principaux ont également été présentés afin d'offrir un portrait global. Par exemple, un des défi est comment les différentes habitudes de travail (en termes en autres d'outils de travail, méthodes et théories) peuvent poser problème lors de la prise de décision au sein d'une équipe interdisciplinaire**. Ensuite, le concept de performance au sein de l'équipe a été introduit, en plus de comment celle-ci est mesurée soit à l'aide de facteurs clés de succès. Finalement, un lien a été fait entre ces concepts et la performance organisationnelle.** La section suivante présente les facteurs clés de succès d'une équipe ICIC interdisciplinaire afin de favoriser sa performance.

2.3 Facteurs de succès dans une équipe ICIC interdisciplinaire

Pour cette section, la littérature a été recensée afin de permettre de répondre au premier objectif du mémoire : l'identification des facteurs de succès de l'équipe ICIC interdisciplinaire. Pour ce faire, la littérature des équipes interdisciplinaires et celle des équipes en cybersécurité ont été étudiées. Ces facteurs de succès sont placés en contexte d'équipe performante afin d'évaluer le succès d'une telle équipe.

Chacun des facteurs de succès est évalué à l'aide d'indicateurs clés de performance, indicateurs qui permettent le suivi et l'évaluation de la performance de l'équipe.

La définition suivante des facteurs de succès a été retenue pour justifier leur sélection :

Les facteurs de succès permettent de gérer les aspects humains de ces équipes et d'assurer que l'organisation offre une performance compétitive et atteint ses objectifs visés (Fortune et White, 2006).

Lorsque les facteurs de succès définis sont bien compris par l'équipe, ils permettent à celle-ci de connaître du succès face à ses objectifs, et ce peu importe le domaine (Iannuci et Garland, 2020). Une attention constante doit donc être portée à ceux-ci de la part de l'équipe (Fortune et White, 2006).

De ce qui a été traité dans la littérature, une cinquantaine de facteurs ont été initialement ressortis (Annexe 1). Lors du processus de sélection des facteurs de succès, des frontières ont été établies. Du nombre de facteurs étudiés, plusieurs ont été exclus de la sélection finale pour les raisons suivantes :

- Les ***facteurs externes*** n'ont pas été retenus, car le sujet de ce mémoire se concentre sur les éléments qui peuvent être influencés par l'organisation, et les facteurs externes sont indépendants aux décisions de l'organisation (Belassi et Tukel, 1996).

  Exemples de facteurs externes : lois, règlements, conformité aux régulations gouvernementales

- Les ***facteurs individuels*** **et** ***facteurs organisationnels*** n'ont pas été retenus, car l'unité d'analyse de ce mémoire est celle de l'équipe. Ainsi, bien que ces facteurs puissent influencer la performance d'une équipe, l'emphase a été placée sur la présentation de facteurs de succès de groupe. Un facteur organisationnel représente des propriétés de l'organisation et non d'une équipe (Diesch, Pfaff et Krcmar, 2020), s'éloignant ainsi de l'unité d'analyse sélectionnée.

  Exemples de facteurs individuels : expérience individuelle, actions éthiques de l'individu

  Exemples de facteurs organisationnels : taille de l'organisation, support de la haute direction, culture organisationnelle, relations avec les fournisseurs

- Les ***facteurs techniques*** n'ont pas été retenus, car l'emphase a été placée sur les éléments managériaux d'une équipe en cybersécurité. Comme mentionné au chapitre 1, la cybersécurité est devenue un domaine dans lequel la dimension humaine prend de plus en plus d'importance (Hall, Sarkani et Mazzuchi, 2011). De ce fait, le reste de ce mémoire se concentre sur des facteurs de succès de cette dimension humaine uniquement.

  Exemples de facteurs techniques : Intégration des différents logiciels, niveau d'utilité d'applications, simplicité d'utilisation des logiciels

Suite à ce processus de sélection, le nombre de facteurs de succès retenus a diminué à une vingtaine**.** Bien que cette diminution soit notable, la qualité et pertinence des facteurs de succès retenus et des conclusions tirées pour la création du cadre conceptuel ne sont pas affectées. Les facteurs ont été sélectionnés s'ils étaient nommés explicitement dans la littérature (p.ex. une communication efficiente au sein de l'équipe favorise son succès) ou encore inférés suite à la lecture d'un écrit (p.ex. L'équipe doit avoir des compétences en cybersécurité tant explicites que tacites pour bien performer (Bassellier, Reich et Benbasat, 2001). Ainsi, le facteur de succès de couverture complète des compétences en cybersécurité a par exemple été inféré suite à l'énoncé précédent.

Finalement, les facteurs de succès qui revenaient le plus souvent ont été sélectionnés, ce qui a amené la liste à un total de 7 facteurs**.** Ces facteurs sont définis et expliqués ci-dessous. Par ailleurs, suite au survol de la littérature, deux catégories principales de facteurs de succès ont été soulevées. De ce fait, la structure sélectionnée pour la présentation des facteurs de succès d'une équipe ICIC interdisciplinaire est celle de deux catégories de facteurs distincts. En effet, la littérature dénote une catégorie de facteurs de succès généraux, peu importe le type d'équipe étudié. Ensuite, des facteurs de succès ont également été observés spécifiquement en lien à l'équipe interdisciplinaire, et ce dans un contexte de cybersécurité.

Ainsi, les facteurs de succès sont divisés, pour cette étude, en deux catégories principales :

1. L'identification de facteurs de succès généraux à retrouver dans une équipe de travail, tout contexte confondu et;

2. L'identification de facteurs de succès spécifiques à une équipe ICIC interdisciplinaire.

À noter que bien que les facteurs de succès sélectionnés soient présentés de façon individuelle dans cette section, ils sont interdépendants. C'est-à-dire, la présence d'un facteur peut influencer le suivi et la performance d'un autre (Belassi et Tukel, 1996 ; Diesch, Pfaff et Krcmar, 2020).

Le tableau ci-dessous présente un récapitulatif des facteurs de succès retenus dans la littérature. La première colonne regroupe les facteurs sous les deux catégories mentionnées précédemment (général ou spécifique). La catégorie « *général »* regroupe les facteurs de succès essentiels à toute forme d'équipe de travail, facteurs qui seront présentés dans la sous-section 2.3.1. Puis, la catégorie *« spécifique »* présente les facteurs reliés au contexte de l'équipe ICIC interdisciplinaire. Cette catégorie est présentée dans la sous-section 2.3.2.

Tableau 2.4 Résumé des facteurs de succès d'une équipe ICIC interdisciplinaire

Catégorie	Nom du facteur
Général	Un alignement opérationnel en accord avec les objectifs organisationnels
	Une communication efficiente au sein de l'équipe
	Une coopération continue au sein de l'équipe
	Une couverture complète des compétences en cybersécurité
Spécifique	Une adaptabilité efficace à l'environnement
	Une détection de menaces en continu
	Une reprise rapide des opérations lors d'un incident

Chacun des facteurs de succès est présenté à l'aide d'une carte contenant la définition de celui-ci et trois indicateurs clés de performance associés au facteur. Les indicateurs ont été retenus au nombre de 3 afin de dresser une liste concise des éléments les plus souvent observés dans la littérature. Suite à chaque carte, une explication textuelle a été ajoutée afin d'offrir plus de détails sur le contexte du facteur de succès.

2.3.1 Identification des facteurs de succès généraux à une équipe de travail

Cette sous-section détaille les 4 facteurs de succès jugés pertinents pour la performance optimale d'une équipe, peu importe sa structure. Les prochains paragraphes détaillent chacun de ces facteurs de succès, tous regroupés sous la catégorie « *général »* du tableau 2.4. Ces facteurs sont présentés en ordre alphabétique, il n'y a pas d'ordre de priorité entre eux.

2.3.1.1 Alignement opérationnel en accord avec les objectifs organisationnels

L'alignement opérationnel est le premier facteur de succès général pertinent pour toute équipe de travail.

Alignement opérationnel

Cet alignement est un accord entre les objectifs de l'équipe et ceux de l'organisation.

Indicateurs de performance :
- Avoir accès aux politiques organisationnelles qui permettent de définir les objectifs de l'équipe
- Établir une procédure de contrôle pour chacun des objectifs
- Documenter et quantifier les écarts entre les résultats et ce qui était initialement espéré pour chaque objectif

Figure 2.3 - Un alignement opérationnel en accord avec les objectifs organisationnels

L'alignement opérationnel permet d'établir le positionnement de l'équipe vis-à-vis le reste de l'organisation (Iannucci et Garland, 2020). Ce facteur se manifeste par une bonne gestion des opérations et des solutions retenues au sein de l'équipe TI qui doivent être alignées avec les objectifs d'affaires de la compagnie (Lee, Trauth et Farwell, 1995 ; Alshawaf, Ali et Hasan, 2005). Ceci est utile afin d'indiquer les bases sur lesquelles les objectifs de l'équipe sont établis pour mesurer l'efficacité de l'équipe. Le facteur d'alignement est ainsi lié aux autres facteurs de succès. Par exemple, le facteur qui suit, la communication efficiente, a un impact positif sur

l'alignement opérationnel de l'équipe. Une équipe qui sait communiquer de manière à optimiser son temps et ses ressources sera une équipe mieux alignée sur les objectifs organisationnels.

Les indicateurs clés de performance utilisés pour effectuer le suivi de ce facteur sont décrits ainsi :

1) *L'accès aux politiques organisationnelles*

   Ce premier indicateur qualitatif permet de vérifier que l'équipe a un accès direct aux politiques de l'organisation, politiques définissant les objectifs en sécurité de l'information de l'organisation. Les buts, objectifs, responsabilités et procédures pour plans d'action doivent s'y retrouver. Un niveau faible d'atteinte de cet indicateur est lorsque l'accès aux politiques est difficile pour les membres de l'équipe tandis qu'un niveau optimal d'atteinte de l'indicateur est lorsque l'équipe a accès à ces politiques en continu. Il est possible de vérifier l'atteinte de cet indicateur en observant si l'équipe a accès à un répertoire qui contient ces politiques.

2) *Procédure de contrôle pour chacun des objectifs*

   Un meilleur suivi de chaque objectif peut être fait à l'aide de l'adoption de procédures de contrôles internes (McCarthy et Tétrault, 2017). En utilisant ces procédures, l'équipe aura ainsi la possibilité d'avoir une meilleure visibilité et transparence des défis encourus par l'organisation. Un niveau faible de cet indicateur est lorsqu'il n'y a pas de procédure existante tandis qu'un niveau optimal est lorsqu'une procédure existe et est documentée pour chacun des objectifs. Cet indicateur qualitatif peut être mesuré en vérifiant la disponibilité de ces procédures ou encore en demandant aux membres de l'équipe s'ils ont des connaissances de telles procédures et d'où les trouver.

3) *Documentation des écarts entre les résultats et les objectifs initiaux*

   Afin de mesurer la qualité des résultats, les objectifs et la vision de l'équipe doivent être documentés. Ensuite, l'équipe devrait pourra exprimer quels sont ces objectifs dans ses propres mots. L'explication doit alors se rapprocher de la définition donnée par

l'entreprise. Un faible niveau d'atteinte de cet objectif a lieu lorsqu'il existe un grand écart entre l'objectif initial et l'objectif réel, tandis qu'un niveau optimal représente l'atteinte de l'objectif. Cela peut être mesuré par l'équipe en quantifiant les écarts et en leur donnant un degré de sévérité.

2.3.1.2 Communication efficiente au sein de l'équipe

La communication efficiente au sein de l'équipe est le deuxième facteur de succès général pertinent pour toute équipe de travail.

Communication efficiente
Structure fluide dans laquelle l'information circule grâce à des interactions fréquentes entre les membres de l'équipe.
Indicateurs de performance : - Comprendre les objectifs de l'équipe - Utiliser des canaux de communication de façon régulière - Avoir des rencontres d'équipe fréquentes et en fonction du besoin

Figure 2.4 - Une communication efficiente au sein de l'équipe

La définition de la structure fluide que représente la communication au sein d'une équipe de travail provient de Alaoui, Laferrière et Meloche (1996). De cette définition est inférée que dans le contexte de l'équipe ICIC les interactions entre les membres représentent les interactions entre les disciplines présentes dans l'équipe.

Comme mentionné dans le nom du facteur, la communication doit être efficiente. Une communication efficiente est pertinente pour le succès d'une équipe de travail, car elle permet de clarifier les objectifs de l'équipe et les résultats espérés (Steinke et al., 2015), et de faciliter l'échange d'information au sein de l'équipe. Ceci permet de clarifier les connaissances communes aux membres (Espinosa, Nan et Carmel, 2015). De plus, une communication efficiente est une communication qui aide à l'atteinte des objectifs de l'équipe, tout en optimisant l'utilisation des

ressources nécessaires. Cette optimisation se crée lorsque l'équipe utilise uniquement les ressources de communication dont elle a besoin pour atteindre ses objectifs et est en mesure de prioriser les éléments qui feront la différence dans le succès de l'équipe.

Les indicateurs clés de performance utilisés pour effectuer le suivi de ce facteur sont décrits ainsi :

1) *Compréhension des objectifs de l'équipe*

   L'équipe doit comprendre ses objectifs de travail, car cette compréhension permet ensuite d'assurer une cohérence entre les actions posées. Cette cohérence facilite la bonne prise de décisions rapide pour l'équipe par la suite (Eliet, 2020). Un faible niveau de compréhension serait représenté par une perception différente de chaque discipline de l'équipe ICIC sur les objectifs de celle-ci tandis qu'un niveau optimal prendrait place lorsque toutes les disciplines auraient la même opinion sur les objectifs de l'équipe. Afin de mesurer cet indicateur qualitatif, la perception des membres de l'équipe peut être demandée et les réponses entre disciplines peuvent être comparées pour voir s'il y a un consensus. Bien que cette mesure soit exécutée au niveau individuel, les individus représentent des disciplines, et l'intégration des disciplines représente un des éléments principaux de toute équipe interdisciplinaire. Ainsi, le but de la mesure est l'évaluation du résultat obtenu et non l'évaluation de chaque individu.

2) *Utilisation de canaux de communication*

   L'utilisation de canaux de communication permet de circuler l'information de manière à obtenir une meilleure interaction entre les disciplines (Aubé et Rousseau, 2016) et de faciliter l'échange d'information au bon moment. Il est important de circuler l'information et non de la contrôler (Schultz, 2020), ce que les canaux de communication peuvent faire. Un niveau optimal d'utilisation de canaux de communication est lorsque l'équipe est informée de ces canaux et de chacun de leur utilité tandis qu'un faible niveau se produit si l'existence des canaux n'est pas communiquée. Afin de mesurer cet indicateur qualitatif, il est pertinent d'exécuter une rétroaction sur l'efficacité de l'échange

d'information (Van der Kleij, Kleinhuis et Young, 2017). Cette rétroaction peut être complétée au niveau de l'équipe à l'aide d'une discussion qui permettra de déterminer si l'équipe connait les outils à sa disposition pour communiquer.

3) *Organisation de rencontres d'équipe fréquentes*

Les rencontres d'équipe sont déterminantes dans la mise en place d'une bonne structure de communication au sein d'une équipe de travail. Bien que la fréquence exacte de ces rencontres devrait être déterminée en fonction des contraintes de l'équipe, la littérature suggère une rencontre hebdomadaire (Laplante, 2007; Brode, 2020). Une rencontre hebdomadaire permet d'effectuer un retour sur la semaine de travail et de préparer la semaine suivante. Ceci représente un niveau optimal et permet de concentrer la discussion sur des éléments ou défis pertinents à la réussite de l'équipe pour la semaine. Toutefois, en fonction des besoins de l'équipe et si celle-ci se retrouve en contexte de crise, ces rencontres peuvent être effectuées de façon plus fréquente. Par contre, une équipe qui ne se rencontre qu'une fois par mois, par exemple, représente un niveau faible d'accomplissement de cet indicateur. L'indicateur est ainsi mesuré de façon quantitative par la fréquence de ces rencontres d'équipe.

2.3.1.3 Coopération continue au sein de l'équipe

Le troisième facteur de succès retenu pour cette catégorie est celui de la coopération continue au sein de l'équipe.

Coopération continue
Contribution et engagement de l'équipe vers l'atteinte d'un objectif commun.
Indicateurs de performance :
- Effectuer un suivi sur les activités de l'équipe pour déterminer l'engagement de celle-ci - Utiliser un outil facilitant la collaboration au sein de l'équipe - Avoir un taux de résolution des conflits optimal au sein de l'équipe

Figure 2.5 – Coopération continue au sein de l'équipe

Le facteur est défini ainsi :

« La coopération est l'action de prendre part, contribuer et participer à une œuvre commune. » (Larousse, 2020)

Le terme de cohésion est souvent rattaché au principe de coopération (Dawson et Thomson, 2018). Une coopération efficace permet d'améliorer la coordination des tâches pour l'équipe (Jariwala et al., 2012).

Les indicateurs clés de performance utilisés pour effectuer le suivi de ce facteur sont décrits ainsi :

1) *Suivi des activités de l'équipe*

   Le suivi des activités de l'équipe doit miser sur la contribution et l'engagement des disciplines. Ici, il faut faire une distinction entre engagement et participation. L'engagement a lieu lorsque les disciplines sont impliquées dans la prise de décision et dans la recherche d'information afin d'arriver à un consensus apprécié par tous (Standish Group International, 2015). Tandis que la participation elle est simplement lorsque les

disciplines donnent leur point de vue, sans être impliquées par la suite dans toute prise de décision (Hastie et Wojewoda, 2015). Afin d'assurer un niveau optimal de cet indicateur, l'engagement doit être mis à l'avant, la participation représentant un niveau plus faible. Afin de mesurer l'indicateur, il peut être demandé aux disciplines d'expliquer le mandat de l'équipe dans leurs propres mots. Une compréhension claire et précise du mandat est preuve d'un engagement de la part des disciplines (Laplante, 2007).

2) *Utilisation d'un outil favorisant la collaboration*

La collaboration est un processus dynamique représenté par un partenariat entre les membres d'une équipe dans lequel ces membres sont interdépendants et font preuve de partage. Ce processus permet d'avoir des modes de fonctionnement et des processus qui faciliteront la bonne performance de l'équipe. Toutefois, il faut adopter un minimum de standards pour maximiser efficacité de l'équipe (Laplante, 2007). Un outil permet de visualiser cette collaboration et d'effectuer un diagnostic pour identifier les besoins de l'équipe. En plus des rencontres d'équipe fréquentes permettent une **communication efficiente** et permettent d'atteindre un niveau optimal de collaboration (Aubé et Rousseau, 2016). Cet indicateur qualitatif peut être mesuré en demandant aux membres de l'équipe leur perception vis-à-vis l'utilité de l'outil. L'utilité est une bonne mesure, car c'est alors qu'il est possible d'inférer que les membres de l'équipe sentiront le besoin d'utiliser l'outil et que cette utilisation deviendra volontaire (Hsieh et Zmud, 2006).

3) *Taux de résolution des conflits optimal au sein de l'équipe*

Une résolution de conflits est ici identifiée comme une résolution de différents points de vue sur un même sujet, différents points de vue des différentes disciplines de l'équipe ICIC. Toutefois, ceci ne veut pas dire que l'équipe doit simplement résoudre un conflit pour atteindre le taux souhaité. L'équipe doit résoudre le conflit de façon constructive en évaluant toutes les options. L'équipe peut déterminer le taux de résolution qu'elle pense souhaitable, la littérature n'exigeant pas un taux précis, car celui-ci dépend des objectifs de l'organisation et de l'équipe. Toutefois, afin d'améliorer l'exécution des tâches lors

d'urgences ou d'interventions (Aubé et Rousseau, 2016), au minimum le taux de résolution devrait être supérieur à 60%. L'équipe peut mesurer cet indicateur en plaçant initialement un objectif et en observant à la suite d'un mois par exemple si cet objectif est atteint ou si des améliorations doivent être planifiées.

2.3.1.4 Couverture complète des compétences en cybersécurité

Finalement, le dernier facteur de succès permettant une bonne performance d'une équipe de travail est celui de la possession d'une couverture complète des compétences en cybersécurité au sein de l'équipe.

Couverture complète des compétences en cybersécurité

Une couverture complète des compétences en cybersécurité établit que l'équipe a les compétences nécessaires afin d'intervenir adéquatement lors d'un incident en cybersécurité.

Indicateurs de performance :

- Offrir de la formation technique chaque trimestre de l'année
- Utiliser un outil de partage de connaissances à travers l'équipe
- Tenir un registre comparant les compétences acquises versus les compétences nécessaires

Figure 2.6 - Couverture complète des compétences en cybersécurité

Dans une équipe de travail, les compétences sont définies ainsi :

La compétence est un pouvoir d'agir, de réussir et de progresser qui permet de réaliser adéquatement des tâches ou des activités de travail et qui se fonde sur un ensemble organisé de savoirs (connaissances, habiletés de divers domaines, perceptions, attitudes, etc.). (Ministère de l'Éducation, 1999)

Ces compétences permettent à l'équipe de mieux planifier et d'exécuter les activités qu'elle doit effectuer de manière efficace (Chang et Ho, 2006; Alshawaf, Ali et Hasan, 2005; Tu et Yuan, 2014).

Ces compétences doivent être évaluées afin de permettre la compréhension et la mesure du niveau de qualité des compétences au sein de l'équipe (Dufour, 2020). Suite à cette évaluation, les points forts de l'équipe peuvent être identifiés, mais également les défis et les compétences sur lesquelles l'équipe doit travailler en fonction des conclusions tirées.

Les indicateurs clés de performance utilisés pour effectuer le suivi et l'évaluation de ce facteur sont décrits ainsi :

1) *Une formation technique à chaque trimestre de l'année*

   Pour être en mesure d'effectuer des tâches et répondre aux objectifs de travail, la formation technique est un élément important à adopter dans l'équipe. Une formation régulière et documentée permet d'atteindre un niveau optimal de mise à jour de compétences (McCarthy et Tétrault, 2017). Pour mesurer cet indicateur, deux méthodes sont possibles. Premièrement, il est possible de mesurer la moyenne de jours de formation donnés de l'équipe et ensuite comparer le résultat à la moyenne de l'industrie que l'organisation peut trouver (Gartner, 2019). Une autre méthode existe et est recommandée dans la littérature, soit d'offrir de la formation chaque trimestre, soit environ aux 4 mois (Bambulas, 2020). Une sensibilisation des employés aux défis de la sécurité de l'information peut réduire les chances d'un incident en cybersécurité, comme une brèche de données, jusqu'à 70% (Lancaster, 2020).

2) *Un outil de partage de connaissances à travers l'équipe*

   Il y a un développement continu qui est exécuté en cybersécurité, effectué sous forme de recherche et d'apprentissage. Un outil de partage de connaissances permettrait d'aider ce développement lors de l'intégration des différentes disciplines. Un niveau optimal permettrait ainsi de savoir qui dans l'équipe a des compétences en quel domaine afin que l'équipe soit plus efficace. Il est possible de mesurer cet indicateur à l'aide de la perception des membres de l'équipe quant au partage qui est fait au sein de l'équipe.

3) Registre comparant les compétences acquises versus les compétences nécessaires

   Puis, pour mieux planifier et évaluer les besoins de l'équipe, un registre peut être tenu. Ce registre serait constamment mis à jour et serait documenté afin d'aider l'équipe à combler ses lacunes. Pour atteindre un niveau optimal, le nombre de compétences acquises serait documenté et comparé au nombre de compétences nécessaires pour pouvoir évaluer ce qui reste à compléter par l'entremise de formation ou de nouveaux talents (Gartner, 2018). La progression peut ensuite être mesurée en observant le nombre de compétences acquises.

Ainsi, les facteurs de communication efficiente, de couverture complète des compétences en cybersécurité, d'alignement opérationnel en accord avec les objectifs organisationnels et de coopération continue au sein de l'équipe sont les facteurs de succès composant la première catégorie de facteurs de succès retenue suite à la recension des écrits, la catégorie de facteurs de succès généraux à une équipe de travail. La sous-section qui suit présente la deuxième catégorie de facteurs de succès, soit les facteurs de succès spécifiques à une équipe ICIC.

2.3.2 Identification des facteurs de succès spécifiques à une équipe ICIC interdisciplinaire

Cette sous-section présente les facteurs de succès directement reliés à une équipe ICIC interdisciplinaire. Ces facteurs sont directement reliés à ce type d'équipe, car ils influencent directement les caractéristiques d'une équipe ICIC interdisciplinaire. Ces facteurs peuvent aussi être pertinents pour une autre équipe de travail que l'équipe ICIC interdisciplinaire, mais ils sont définis comme indispensables à l'équipe ICIC interdisciplinaire. Cette conclusion est tirée pour tous les facteurs, car chacun d'entre eux a un lien établi avec au moins une des caractéristiques de l'équipe ICIC interdisciplinaire.

En guise de rappel, voici les caractéristiques principales d'une équipe interdisciplinaire :

(1) Une intégration de différentes disciplines
(2) Un partage des responsabilités
(3) Un travail interactif
(4) Une prise de décisions efficace
(5) Une recherche de solutions innovatrices et créatives

Les prochains paragraphes détaillent chacun de ces facteurs de succès et les indicateurs de performance associés. Dans la description des facteurs, des liens sont effectués avec les caractéristiques d'une équipe interdisciplinaire, en plaçant les facteurs dans le contexte de la cybersécurité. Les facteurs de succès sont présentés en ordre alphabétique afin de faciliter leur ordre de présentation.

2.3.2.1 Adaptabilité efficace face aux cybermenaces

Le premier facteur de succès dans cette catégorie est celui de l'adaptabilité efficace de l'équipe ICIC interdisciplinaire face aux cybermenaces présentes dans son environnement.

Adaptabilité efficace

Flexibilité et résilience de l'équipe face à des événements changeants dans son environnement.

Indicateurs de performance :

- Avoir accès à des ressources financières
- Avoir des mécanismes de contrôle pouvant être divisés en plusieurs étapes d'exécution
- Innover en fonction des opportunités du marché

Figure 2.7 – Adaptabilité efficace face aux cybermenaces

Ce premier facteur fait la preuve de résilience de l'équipe qui doit faire face à des événements qui changent son quotidien. Cette résilience lui permet de mieux réagir par la suite (Schultz, 2020) lorsqu'il sera nécessaire de le faire dans le cas d'un incident de cybersécurité qui peut nuire à l'actif informationnel.

Les trois indicateurs clés de performance liés à ce facteur de succès sont les suivants :

1) Accès à des ressources financières

   Le budget est un élément important pour toute équipe de travail. Certains éléments favorisent l'atteinte à un budget qui est bénéfique pour l'équipe de travail. Entre autres, du budget doit être alloué aux ressources humaines pour leur embauche, ou encore à des ressources techniques qui facilitent l'atteinte des objectifs de l'équipe. Par exemple, en cybersécurité, des programmes de protection et de sécurité TI existent qui peuvent favoriser la protection de l'actif informationnel pour les organisations (McCarthy et Tétrault, 2017). Un exemple de ces programmes est l'implantation d'une solution de détection et de prévention d'incident sur les postes informatiques qui permet de détecter les menaces dans l'environnement de l'équipe afin que celle-ci puisse y réagir plus rapidement (Schultz, 2020). Le budget qui devrait être alloué à l'équipe dépend de plusieurs facteurs comme le niveau de sensibilité de l'information que l'équipe opère, la taille de l'organisation et son domaine ou encore les éléments de conformité (lois, standards) auxquels l'organisation doit se soumettre (Rinaldi, 2020). Toutefois, l'industrie révèle qu'un minimum de 5% du budget TI des organisations est alloué à la cybersécurité et qu'un niveau maximal relevé est de 20% (Rinaldi, 2020). Pour mesurer cet indicateur, l'organisation devrait initialement émettre ses objectifs et l'équipe devrait ensuite évaluer ses besoins. C'est avec cette liste de besoins qu'elle sera en mesure d'expliquer quel budget elle a besoin. Ensuite, une comparaison peut être faite avec l'industrie en termes de budget.

2) Mécanismes de contrôle pour faciliter les étapes d'exécution

Les mécanismes de contrôle sont essentiels à toute équipe qui veut assurer la protection de l'actif informationnel (Diao, 2018). Un mécanisme de contrôle permet l'adoption de bonnes pratiques de sécurité et de continuité des activités (Gouvernement du Canada, 2021). Un exemple de niveau optimal d'utilisation de mécanismes de contrôle est la mise en place de mises à jour automatiques aux systèmes d'exploitation et applications utilisées par l'équipe (Gouvernement du Canada, 2021). Comparativement, un niveau faible serait lorsqu'une liste de contrôles est énoncée dans la stratégie de l'équipe, mais qu'aucun suivi n'est effectué afin d'en assurer la complétion. Afin de mesurer l'atteinte de l'indicateur, une liste devrait être créée en suivant les indications et standards de l'industrie et il devrait y avoir un suivi effectué sur cette liste pour confirmer ce qui a été fait.

3) Innovation en fonction des opportunités du marché

L'innovation est importante afin que l'équipe fasse preuve d'ouverture à de nouveaux défis. Cette ouverture lui permettra de créer de la valeur d'affaires pour l'organisation, mais également une valeur ajoutée pour ses clients. Les opportunités du marché sont souvent un bon indice sur par exemple les technologies émergentes présentes dans le domaine. Afin d'atteindre un niveau optimal, l'équipe doit développer ses capacités de changement en fonction de ce qui est observé dans son environnement (Herath, Herath et Bremser, 2010). Ces capacités lui permettront d'avoir les outils et moyens pour innover en continu (Herath, Herath et Bremser, 2010). Pour mesurer cet indicateur, la perception des membres de l'équipe sur la capacité de l'équipe à innover peut être demandée.

2.3.2.2 Détection de menaces en continu dans l'environnement de l'équipe

Le deuxième facteur de succès de cette catégorie est celui de la détection de menaces provenant de l'environnement interne ou externe à l'équipe.

Détection de menaces en continu

Investiguer afin de comprendre quelles sont les menaces auxquelles l'équipe fait face et quels éléments les composent.

Indicateurs de performance :
- Vérifier la conformité des mesures à l'aide de tests de pénétration
- Utiliser des données historiques pour effectuer un suivi des vulnérabilités de l'organisation
- Utiliser une plateforme qui permet de suivre les menaces dans l'environnement organisationnel

Figure 2.8 – Détection de menaces en continu dans l'environnement de l'équipe

La détection de menaces en continu permet de constamment être au courant de ce qui se passe dans l'environnement de l'équipe et comment celle-ci doit se préparer ou à quoi elle doit s'attendre.

Les trois indicateurs clés de performance liés à ce dernier facteur de succès sont les suivants :

1) Tests de pénétration pour la vérification de la conformité des mesures

   Les tests de pénétration sont des tests dans lesquels l'équipe tente de déjouer la protection qu'elle a mise en place afin d'évaluer les lacunes dans ses contrôles ou dans sa stratégie de protection. Ces tests peuvent être effectués par des membres de l'organisation ou encore par des membres externes à celle-ci. En plus, ceci permet un suivi des pratiques à l'interne (McCarthy et Tétrault, 2017). Une certaine fréquence des tests est nécessaire. Cette fréquence dépend des objectifs et entre autres des menaces de l'environnement, mais devrait être minimalement effectuée deux fois par an (Gouvernement du Canada, 2021). Une comparaison pourrait être effectuée avec l'industrie afin de donner un aperçu de ce qui est attendu.

2) Utilisation de données historiques pour une gestion des vulnérabilités

   L'utilisation de données historiques est pertinente pour comprendre l'impact potentiel des menaces (Schultz, 2020). En utilisant des données historiques, il est possible de

remarquer une tendance ou une saisonnalité sur certains types de menaces. Ceci permettrait à l'équipe de prévenir les menaces possibles. Toutefois, ces données ne peuvent que représenter des hypothèses. L'indicateur devrait être mesuré en effectuant un suivi sur la fréquence de l'utilisation de ces données (Herath, Herath et Bremser, 2010). Par exemple, une fois par trimestre, l'équipe pourrait déterminer si une tendance dans les dernières années pourrait laisser entrevoir des risques pour cette période. Entre autres, le mois de décembre est une période plus achalandée où plus d'information circule dû à la période des Fêtes.

3) Utilisation d'une plateforme pour faire un suivi des menaces

   Pour pouvoir répondre aux questions critiques, il est possible d'utiliser une plateforme qui permet de faire un suivi en temps réel des menaces qui pèsent contre l'organisation. Alors, une communication efficiente est primordiale afin de transmettre par la suite l'information aux parties impliquées. En plus des menaces, les vulnérabilités peuvent également être suivies à l'aide d'une solution de détection et de prévention des menaces (Simplilearn, 2020). Un contrôle est alors effectué sur les réseaux ou applications principalement utilisées. Afin de mesurer cet indicateur, il est pertinent de déterminer si l'accessibilité à l'information et la disponibilité de celle-ci est immédiate pour l'équipe lorsqu'elle en a besoin.

2.3.2.3 Reprise rapide des opérations suite à un incident en cybersécurité

Le dernier facteur de succès est celui de la reprise rapide des opérations suite à un incident en cybersécurité.

Reprise rapide des opérations

La continuation des opérations et la rapidité de recouvrement suite à un incident informatique grâce aux capacités techniques et d'affaires de l'équipe.

Indicateurs clés de performance :

- Avoir des ressources disponibles (main d'œuvre, plan de contingence, mesures techniques)
- Réagir dès qu'un incident est soulevé
- Avoir un taux de résolution élevé d'incidents rapportés à l'équipe dans les 12 derniers mois

Figure 2.9 - Reprise rapide des opérations suite à un incident en cybersécurité

La définition retenue de ce facteur de succès est celle-ci :

La continuation des opérations suite à un incident informatique grâce aux capacités techniques et d'affaires de l'équipe (Alshawaf, Ali et Hasan, 2005 ; Hall, Sarkani et Mazzuchi, 2011). L'équipe doit pouvoir s'adapter aux changements imposés sur celle-ci suite à un événement externe ou interne qui modifie son contexte d'affaires (Rockart, Earl et Ross, 2003 ; Diesch, Pfaff et Krcmar, 2020).

Ce facteur définit spécifiquement la cybersécurité dû à l'augmentation des cybercrimes. Une équipe de cybersécurité qui est en mesure de reprendre rapidement ses opérations à la suite d'une cyberattaque est une équipe plus performante. En relation aux caractéristiques de l'équipe interdisciplinaire, ce facteur est lié aux caractéristiques du partage des responsabilités entre les individus ainsi que du travail interactif au sein de l'équipe. Cette interaction entre les membres de l'équipe ainsi que le partage des responsabilités permettent à l'équipe de bien se préparer à un incident informatique ainsi que d'effectuer un bon suivi après cet incident.

Dans le cas d'un incident, cela veut également dire que l'équipe ICIC interdisciplinaire est en mesure de continuer à livrer le résultat espéré (AlHogail, 2015). La continuité peut aussi être mesurée sous un angle d'affaires dans lequel elle représente des instructions qui décrivent comment les fonctions essentielles de l'organisation pourront être soutenues avant que celle-ci ne retourne aux opérations normales (Diesch, Pfaff et Krcmar, 2020). La continuation doit être utilisée de façon proactive par l'équipe, soit avant qu'un incident se produise.

Les trois indicateurs clés de performance liés à ce facteur de succès sont :

1) Disponibilité des ressources lors d'un incident

   Afin de pouvoir bien répondre lors de tout incident, les ressources doivent être disponibles pour l'équipe lorsque celle-ci en a besoin (Herath, Herath et Bremser, 2010). Plus particulièrement, il est ici question des ressources détaillées dans le plan d'intervention de l'équipe (McCarthy et Tétrault, 2017). Ce plan doit définir les frontières de l'incident et quelles données ont été touchées (OCRCVM, 2020). Ensuite, une piste sur les actions à poser en fonction de ces éléments doit être déjà établie dans ce plan (Aubé et Rousseau, 2016). Ceci permettra de contenir les effets de l'incident, de déterminer qui doit être contacté dans l'organisation et d'évaluer les conséquences de l'incident (OCRCVM, 2020). Afin d'atteindre un niveau optimal, tous ces éléments doivent être présents dans le plan. Il est possible de mesurer le niveau en comparant le plan créé par l'équipe à un plan contenant les meilleures pratiques de l'industrie.

2) Réaction immédiate lors de la détection d'un incident

   Un bon taux de rapidité de réponse après une interruption, représente l'habileté de l'équipe à continuellement livrer le résultat initialement intentionné malgré un cyberincident (Björck et al., 2015). Ainsi, pour une bonne continuation des opérations, la réaction de l'équipe doit être immédiate lors de la détection d'un incident. Ceci est possible lorsqu'il existe, entre autres, un mécanisme de signalement des incidents (McCarthy et Tétrault, 2017) qui permet de diminuer le temps moyen de découverte de

l'incident (Caendra Inc., 2017). Ceci peut être mesuré en évaluant si l'équipe a une politique en matière de conservation des données qui lui indique quoi faire, et si l'équipe a un processus de sauvegarde en place en cas d'un incident (Diao, 2018).

3) Taux de résolution élevé d'incidents rapportés à l'équipe dans les 12 derniers mois
   L'efficacité de l'équipe peut aussi être évaluée en fonction de ce qui a été amené à l'attention de l'équipe et si l'équipe a su bien y répondre. Ceci est fait en utilisant convenablement les ressources à leur disposition, en utilisant le plan d'intervention de manière adéquate (rapidement, mais sans sauter d'étapes) et en fonction des attentes de l'organisation. Par exemple, l'équipe peut déterminer que lorsqu'une mise à jour d'application est disponible, celle-ci doit être installée dans un délai de 30 jours (Gartner, 2018). Ceci dépend de l'organisation et de la gravité de la mise-en-jour en question, en plus de l'impact possible sur les opérations si celle-ci n'est pas installée (Gartner, 2018). Un taux de résolution positif est un bon indicateur de l'efficacité de l'équipe à mesurer.

Ainsi, **cette section du deuxième chapitre a présenté les 7 facteurs de succès sélectionnés suite à une recension de la littérature sur les sujets d'équipe en cybersécurité et d'équipes interdisciplinaires. Ces facteurs de succès sont divisés en deux catégories, soit la catégorie générale à toute équipe de travail (4 facteurs de succès) ainsi que la catégorie plaçant l'emphase spécifiquement sur l'équipe ICIC interdisciplinaire (3 facteurs de succès).** La section suivante présente les rôles sélectionnés dans la littérature ainsi que leurs responsabilités au sein d'une équipe ICIC interdisciplinaire.

2.4 Rôles et responsabilités au sein d'une équipe ICIC interdisciplinaire

La littérature nous indique qu'il est important de définir des rôles dans une équipe afin qu'ils soient compris par les membres de celle-ci (Petri, 2010). Ainsi, chaque membre de l'équipe doit premièrement comprendre son rôle individuel par rapport au succès de l'équipe et ce qu'il peut faire pour aider l'équipe, mais doit également comprendre les rôles qu'ont les autres membres de son équipe (Petri, 2010). Ceci permettra de délimiter les frontières des responsabilités de chaque membre de l'équipe. La définition de rôles ne doit toutefois pas entrer en conflit avec la définition des buts collectifs de l'équipe (Bronstein, 2003). De ce fait, l'emphase doit toujours rester sur l'atteinte d'un ou des objectifs communs de l'équipe, car l'équipe interdisciplinaire est premièrement basée sur la collaboration entre les membres composant l'équipe.

Cette section présente les **6** catégories de rôles sélectionnées lors de la recension des écrits dans la littérature. De façon générale, la littérature dénote que l'emphase est majoritairement mise sur les compétences techniques nécessaires à une équipe en cybersécurité et non assez sur le côté humain des rôles (MacKinnon et Rampado, 2020). Chaque rôle clé retenu est lié à un ou plusieurs facteurs de succès identifié dans la section précédente, *2.3 Les facteurs de succès au sein de l'équipe ICIC*. Les responsabilités associées à chacun des rôles ont également été identifiées à l'aide de la littérature.

Avant la présentation de ces rôles, la sous-section qui suit présente l'origine de l'identification des rôles dans une équipe de travail, soit la théorie de Belbin. Cette explication permet d'offrir un contexte des rôles d'une équipe de travail avant d'émettre des liens avec les rôles de l'équipe ICIC interdisciplinaire qui sont à la fois influencés de cette théorie et du survol de la littérature spécifique aux équipes en cybersécurité et équipes interdisciplinaires.

2.4.1 Les rôles selon Belbin

Belbin (1991, 1993) est un des premiers à avoir identifier les rôles clés à avoir dans une équipe. Ultimement, il présente neuf rôles qu'il croit pertinents à retrouver dans une équipe. Comme mentionné plus haut, ces rôles de Belbin sont présentés avant ceux retenus dans la littérature pour l'équipe ICIC interdisciplinaire. Ces rôles n'ont pas été directement transposés pour l'équipe ICIC interdisciplinaire, car ils ont été basés sur les personnalités des membres de l'équipe, leur esprit critique ainsi que leurs comportements (Aritzeta et al., 2007) tandis que ce mémoire base ses propositions de rôles clés sur les facteurs de succès d'une équipe ICIC interdisciplinaire. Toutefois, la théorie de Belbin permet d'établir une base théorique qui peut ensuite être développée. Par exemple, dans le tableau 2.5 ci-dessous, le rôle du travailleur d'équipe a été développé et a évolué pour être jumelé au rôle du coordonnateur au sein de l'équipe ICIC interdisciplinaire. L'essence de ce rôle selon Belbin, soit la création de liens au sein de l'équipe, a été conservée car elle revenait souvent dans la littérature interdisciplinaire et celle en en cybersécurité. Les deux rôles ont toutefois été jumelés car la littérature récente ramenait le concept de créations de liens à l'individu au sein de l'équipe répartissant les tâches. De plus, Belbin est également de l'avis qu'un rôle clé dans une équipe doit être différencié du rôle fonctionnel qui représente plus les compétences techniques et les postes affichés (Artizeta et al., 2007). Ainsi, plusieurs membres au sein d'une équipe pourraient avoir les mêmes rôles fonctionnels, soit les mêmes postes, mais avoir des rôles qui diffèrent. Finalement, ce modèle de rôles de Belbin a également été lié au contexte d'équipe performante (Artizeta et al., 2007). Ainsi, le modèle représente une bonne inspiration pour le contexte de cette étude qui est également celui d'une équipe performante. Une courte description de chacun de ces rôles est offerte dans le tableau ci-bas (Belbin 1991, 1993) (traduction libre).

Tableau 2.5 Les rôles de Belbin

Rôle	Description
L'enquêteur de ressources	Doit développer des opportunités pour l'équipe et s'inspirent des ressources qu'il connait et observe pour ramener des idées de solutions.
Le travailleur d'équipe	Permet de créer des liens au sein de l'équipe et définit quelles tâches doivent être effectuées en équipe et par l'équipe.
Le coordonnateur	Place l'emphase sur les objectifs de l'équipe et délègue les tâches de façon appropriée
L'innovateur	Personne créative qui doit aider à résoudre des défis en usant d'innovation dans la présentation de solutions. Émet des suggestions d'amélioration.
L'évaluateur du contrôle	Présente une mentalité logique et n'émet pas de jugement personnel sur les options qui se présentent à l'équipe lors d'une prise de décision.
Le spécialiste	Amène des connaissances et compétences spécifiques pour le bien commun de l'équipe.
Le façonneur	Garde le focus de l'équipe sur la tâche à effectuer et a le courage de surmonter les obstacles qui pourraient survenir. Pousse l'équipe à suivre des activités qui sont dirigées par un objectif.
Le réalisateur	Permet la planification d'une stratégie d'équipe et sa réalisation d'une manière efficiente.
Le finisseur	Évalue le travail effectué pour identifier des erreurs, s'assure du contrôle de la qualité.

Pour chaque rôle énoncé dans cette section, la définition et le détail des rôles sont énoncés ainsi que les responsabilités liées à chacun de ces rôles. Cette structure reprend la structure de la sous-section précédente qui a été utilisée pour présenter les facteurs de succès sélectionnés. Certains rôles ont été exclus de l'étude bien qu'ils soient pertinents dans une équipe. Par exemple, le rôle de l'utilisateur n'est pas présenté. Un rôle d'utilisateur est un rôle dans lequel l'employé a accès uniquement à l'information dont il a besoin pour effectuer ses tâches et se soumet à des contrôles d'accès qui ne sont pas spécifiés par lui (Wood, 1987). Ce rôle n'a pas été retenu, car ce mémoire se positionne sur les rôles clés qu'une équipe interdisciplinaire en cybersécurité devrait avoir dans l'optique de rôles naturels tel que présenté par Belbin. Dans le but de ne pas créer de liste exhaustive tout simplement sur tous les rôles possibles, les rôles présentés ci-bas

ont été sélectionnés s'ils combinaient minimalement deux facteurs de succès précédemment établis dans la section antérieure et s'ils étaient jugés comme rôle clé par la littérature du domaine de la cybersécurité. Un rôle clé a été identifié ainsi s'il revenait souvent dans la littérature.

2.4.2 Les rôles au sein de l'équipe ICIC interdisciplinaire

Cette sous-section présente les 6 catégories de rôles retenus qui complètent la composition de l'équipe ICIC interdisciplinaire de ce mémoire. Chaque rôle est défini, un lien est ensuite fait entre ce rôle et certains des facteurs de succès (en **gras**) et finalement quelques responsabilités sont détaillées pour chacun des rôles afin d'illustrer les frontières du rôle. Dans chaque carte, trois responsabilités ont été ciblées, mais celles-ci ne représentent pas une liste exhaustive, plutôt les responsabilités qui revenaient souvent dans le survol de la littérature et qui permettaient de bien définir le rôle. À noter que les rôles sont présentés de façon alphabétique, car aucun rôle n'est prioritaire envers un autre.

2.4.2.1 Agent de changement

Le premier rôle est celui de l'agent de changement.

Agent de changement

L'agent de changement accompagne l'équipe en temps réel à l'aide de différents outils.

Responsabilités :

- Sensibiliser l'équipe avant l'arrivée du changement
- Communiquer avec les membres de l'équipe les nouvelles pertinentes
- Faire des ateliers pour répondre aux questions de l'équipe suite au changement

Figure 2.10 – Agent de changement

L'agent de changement accompagne l'équipe dans le changement et s'assure que l'équipe a les outils nécessaires pour comprendre la nécessité des modifications apportées dans leur quotidien. De plus, il s'assure que l'équipe se sente écoutée lorsqu'elle doit s'adapter à des événements hors de son contrôle**.** L'agent de changement a donc un rôle direct dans le processus facilitant le changement qui peut survenir pour l'équipe (Bourgon, Gutierrez et Ashton, 2012). Ce changement peut être de nature différente, dont entre autres : dans les méthodes de travail (Thémélis, 2019), dans les produits offerts (Thémélis, 2019), sous forme d'évolution technologique ou encore sous forme de restructuration des équipes de travail (Vachon, 2016). Ainsi, l'agent de changement doit être présent tout au long du processus, soit avant pendant et après le changement. De plus, l'information doit être constamment communiquée aux membres de l'équipe. Le facteur de succès de **communication efficiente au sein de l'équipe** a donc un grand rôle à jouer pour ce rôle.

Avant le changement, l'équipe doit être sensibilisée et éduquée sur la nécessité du changement (Simplilearn, 2020). Les nouvelles doivent ensuite être communiquées. Ces nouvelles sont principalement par rapport à n'importe quel changement dans l'organisation, que ce soit au niveau de la structure ou d'une intervention particulière. Il est important pour l'agent de changement de déterminer le moment et la méthode de divulgation de la nouvelle en question (McCarthy et Tétrault, 2017). Puis, des ateliers sont pertinents suite au changement afin de favoriser la **coopération continue au sein de l'équipe** et son **adaptabilité efficace** face à son environnement.

2.4.2.2 Agent de liaison

Le deuxième rôle est celui de l'agent de liaison.

Agent de liaison

L'agent de liaison fait le lien entre l'équipe les autres parties prenantes internes à l'organisation en partageant les perceptions de l'équipe avec celles-ci.

Responsabilités :

- Suivre régulièrement les mises à jour sur les politiques organisationnelles afin d'adopter les pratiques de l'équipe
- Gérer l'obtention des ressources de travail
- Rapporter les incidents à la direction

Figure 2.11 – Agent de liaison

L'agent de liaison fait le lien entre l'équipe et les gens externes à celle-ci, mais interne à l'organisation. Par exemple, ce pourrait être avec la direction ou encore avec d'autres équipes de travail au sein de l'organisation (Bartock et al., 2016). Ce lien est créé à l'aide d'une **communication efficiente** qui est favorisée lorsque : les points de l'équipe sont transmis à d'autres parties prenantes de l'organisation, le vocabulaire utilisé par l'équipe est expliqué aux autres parties prenantes (Gray, 2008) et l'agent de liaison communique adéquatement les besoins de l'équipe en termes de ressources (Bartock et al., 2016). D'un autre côté, la direction doit communiquer également les besoins de l'organisation face à l'équipe à l'agent de liaison et les opportunités de cette équipe (Gray, 2008).

Pour faciliter cet échange entre la direction et l'équipe, un suivi des politiques organisationnelles doit être fait, et ce pour faciliter **l'alignement opérationnel** de l'équipe. Ce suivi peut être fait par exemple en ayant accès à un répertoire contenant les politiques organisationnelles mises à jour par d'autres équipes de l'organisation, mais auxquelles minimalement l'agent de liaison aurait accès.

Cet agent permet donc de faciliter l'échange et le flux d'information entre des groupes ou individus qui ont, par exemple, une barrière cognitive comme le fait de provenir de différentes disciplines (Long, Cunningham et Braithwaite, 2013). Cette intégration des différentes disciplines est une des caractéristiques clés définissant l'équipe interdisciplinaire, et ses défis peuvent donc être mitigés à l'aide du rôle de l'agent de liaison. La performance de l'équipe est améliorée lorsque l'information est transmise adéquatement entre les parties prenantes (Long, Cunningham et Braithwaite, 2013).

Pour ce qui est de la gestion de l'obtention des ressources, cela attrait à créer une liste de besoins, à travailler sur un budget, à déterminer la disponibilité nécessaire des ressources, le tout pouvant être fait conjointement avec l'agent de changement. L'agent de changement et l'agent de liaison travaillent conjointement, car le premier s'implique sur toute forme de changement dans l'équipe tandis que le deuxième doit communiquer les perceptions de l'équipe durant ce changement aux autres parties prenantes internes de l'organisation. Finalement, les incidents de cybersécurité doivent être rapportés à la direction pour ce même souci de transparence et pour obtenir un meilleur support de sa part dans la prise de décisions (Brode, 2020). Pour ce faire, l'utilisation de rapports ou de présentations visuelles dans des rencontres permet d'améliorer cet échange d'information.

2.4.2.3 Conseiller

Le troisième rôle présenté est celui du conseiller.

Conseiller

Le conseiller analyse les menaces de l'environnement à l'aide des données qu'obtient l'équipe.

Responsabilités :

- Suivre les vulnérabilités technologiques et humaines auxquelles l'organisation fait face
- Concevoir une liste de besoins pour l'équipe
- Avoir une connaissance sur les technologies émergentes dans le domaine de l'organisation

Figure 2.12 – Conseiller

Le conseiller analyse et **détecte les menaces** présentes dans l'environnement de l'organisation à l'aide de plusieurs méthodes comme l'utilisation de plateformes de détection, l'utilisation de données historiques ou encore l'étude des incidents ou des vulnérabilités en croissance dans le domaine de l'organisation. Ceci est fait afin de travailler pour mitiger les risques et ainsi pouvoir effectuer une **reprise rapide des opérations** lorsqu'un incident se produit. Pour ce faire, une évaluation des vulnérabilités doit être faite par le conseiller (Unni, 2019) ce qui permet de surveiller les risques (McCarthy et Tétrault, 2017) et d'ainsi établir une liste des besoins pour l'équipe. Cette liste de besoins est faite en **coopération** avec l'agent de liaison qui est celui qui gère l'obtention des ressources.

Ainsi, cette emphase sur la mitigation des risques de cybersécurité permettra de déterminer quels contrôles sont sur le coup trop faible au sein de l'organisation et l'impact que cela peut avoir sur la performance de l'équipe celle de l'organisation (Diesch, Pfaff et Krcmar, 2020). Pour ce faire, le conseiller doit également comprendre l'infrastructure TI de l'organisation afin de pouvoir prioriser l'ordre de restauration en cas d'incident (Bartock et al., 2016) en plus d'évaluer les contrôles en place. Finalement, le conseiller évalue les technologies émergentes du domaine et les opportunités qu'elles présentent pour son organisation afin de déterminer quelles

fonctionnalités techniques additionnelles sont nécessaires (Bartock et al., 2016). Tout ceci est fait dans un but de défense de l'actif informationnel en surveillant, analysant et facilitant la prise de décision lors d'un incident de cybersécurité (Caendra Inc., 2017).

2.4.2.4 Coordonnateur

Le quatrième rôle est celui du coordonnateur.

Coordonnateur

Le coordonnateur oriente les efforts des membres de l'équipe afin de résoudre les problèmes qui surviennent lors d'un incident ou de développer des projets pour la promotion de la cybersécurité dans l'organisation.

Responsabilités :

- Assigner des tâches en fonction des compétences des membres de l'équipe
- Effectuer un suivi des tâches et projets avec l'équipe
- Gérer les ressources suite à leur obtention

Figure 2.13 – Coordonnateur

Le coordonnateur agit comme le responsable de l'incident, car il amasse l'information sur l'incident et est le responsable de la planification de sa résolution (Bartock et al., 2016). Ainsi, il identifie et priorise les problèmes à résoudre suite à cet incident, et détermine un plan initial pour y remédier (Long et al., 2013). Son objectif principal est de minimiser les dommages et l'impact de l'incident de cybersécurité sur la performance et survie de l'organisation (Brode, 2020).

Pour ce faire, il assigne des tâches en fonction des compétences de chaque membre de l'équipe et également en fonction de leur charge actuelle de travail et de l'échéancier prescrit par la tâche. Il doit donc être activement au courant des **compétences en cybersécurité** présentes au sein de l'équipe ICIC interdisciplinaire. Suite à cette assignation, le coordonnateur est celui qui s'occupe

du suivi de ces tâches ou projets en faisant la promotion de la **coopération** au sein de l'équipe pour assurer le partage de tous sur leurs réussites ou leurs défis.

Puis, il optimise les ressources de l'équipe (Bartock et al., 2016 ; Eliet, 2020). Il travaille ainsi avec le conseiller qui connait les besoins de l'équipe afin d'optimiser l'utilisation des ressources au bon moment suite à leur obtention. Il tient par exemple un registre qui est mis à jour dans lequel la priorité des différents actifs ainsi que leur degré de criticité est établie (OCRCVM, 2020). Ceci est utile pour avoir une **reprise rapide des activités** lors d'un incident. Ainsi, le coordonnateur s'occupe également du plan d'intervention qui est utilisé par l'équipe et l'organisation à ce moment.

2.4.2.5 Gardien de l'information

Le cinquième rôle est celui du gardien de l'information.

Gardien de l'information

Le gardien de l'information a sous sa responsabilité l'accès à l'actif informationnel de l'organisation.

Responsabilités :

- Orchestrer des tests de pénétration
- Développer un processus de gestion des accès
- Contrôler la qualité des mesures de contrôle des pratiques de sécurité

Figure 2.14 – Gardien de l'information

Le gardien de l'information a comme tâche principale la protection de l'actif informationnel (OCRCVM, 2020). Bien que tous les membres de l'équipe ICIC interdisciplinaire ont également cette tâche, le gardien agit comme ligne de défense pour le contrôle des accès à cet actif informationnel. Son objectif est d'aider à l'atténuation des menaces internes et externes à l'organisation en orchestrant des tests de pénétration, en effectuant un suivi constant sur les accès et en contrôlant la qualité des pratiques de sécurité.

Premièrement, les tests de pénétration permettent de détecter de manière proactive les vulnérabilités auxquelles fait face l'organisation pour ensuite également **déterminer les menaces** possibles (Caendra Inc., 2017). Ceci permet d'être préparé un minimum en cas d'incident afin d'assurer une **reprise rapide des opérations**.

Ensuite, le gardien de l'information gère l'accès à l'information (Simplilearn, 2020). Ceci est fait par l'entremise d'un processus de contrôle de ceux-ci en utilisant par exemple l'authentification à doubles facteurs, en déterminant une date d'échéance pour les différents comptes ayant des accès hautement privilégiés (OCRCVM, 2020) et en s'assurant que ceux ayant accès à tout type d'information ont besoin de celle-ci dans le cadre de leurs fonctions (Diao, 2018). Un compte à hauts privilèges est un compte qui par exemple détient un accès à de l'information secrète sur la compagnie, comme les plans stratégiques ou encore des mots de passe importants.

De plus, le gardien contrôle la qualité des pratiques de sécurité de l'organisation et celle des fournisseurs. Ce contrôle de qualité est fait, entre autres, en fonction des normes de l'industrie. Il est nécessaire d'évaluer également les fournisseurs de façon constante, car leurs vulnérabilités sont également les vulnérabilités de l'organisation (McCarthy et Tétrault, 2017). Par exemple, un fournisseur qui a un historique de nombreuses vulnérabilités, qui s'occupe des données sensibles de l'organisation et qui a une grande portée d'impartition est un fournisseur à surveiller. Bien que le gardien de l'information ne puisse à lui seul surveiller tous les fournisseurs, il peut émettre des recommandations sur les contrôles à effectuer sur ces fournisseurs au reste de l'organisation. Ces contrôles peuvent être de par exemple effectuer des examens de temps en temps sur les pratiques du fournisseur, de revoir ses responsabilités ou encore de documenter les changements que le fournisseur effectue sur ses pratiques de sécurité (OCRCVM, 2020).

2.4.2.6 Innovateur

Le dernier rôle présenté dans la composition de l'équipe ICIC interdisciplinaire est le rôle de l'innovateur.

Innovateur

L'innovateur est toujours à la recherche de nouvelles idées afin de permettre à l'organisation de créer de la valeur ajoutée et de la valeur d'affaires.

Responsabilités :

- Innover les processus d'affaires de l'organisation en fonction de son environnement
- Intégrer la protection de l'actif informationnel dans l'innovation
- User de créativité pour améliorer les moyens de protection de l'actif informationnel

Figure 2.15 – Innovateur

L'innovateur développe de nouvelles méthodes et outils de travail en repensant les méthodes de travail utilisées par l'organisation. Pour ce faire, il doit donc innover dans les processus d'affaires, offrir une balance entre protection et innovation et user de créativité à travers ses mandats. Ainsi, le processus de détection d'un incident, celui de reprise d'opérations lors d'un incident ou encore le processus d'action suite à un incident sont des exemples de processus sur lesquels l'équipe ICIC peut innover (Aubé et Rousseau, 2016 ; Bartock et al., 2016). Toutefois, l'innovateur ne doit jamais perdre de vue que la protection de l'actif informationnel reste une tâche centrale de l'équipe ICIC et doit donc s'assurer qu'il y a une balance entre l'innovation et la protection de cet actif (Scholtz, 2020). Pour ce faire, l'innovation doit être intégrée à cette protection en développant des pratiques de travail qui encouragent la créativité dans la prise de décision. Par exemple, le *BYOD* (Bring Your Own Device) est de plus en plus utilisé par les organisations, permettant aux employés d'utiliser leurs propres appareils pour travailler. Toutefois, les organisations doivent être en mesure d'éduquer leurs employés et d'employer des méthodes de protection adéquates afin de protéger l'actif informationnel. Tout ceci permet de faciliter **l'adaptabilité** de l'équipe (Aubé et Rousseau, 2016).

Cette quatrième section du chapitre 2 a présenté les 6 rôles retenus dans la composition de l'équipe ICIC interdisciplinaire : l'agent de changement, l'agent de liaison, le conseiller, le coordonnateur, le gardien de l'information et l'innovateur. Ces rôles doivent tous travailler conjointement afin d'assurer que l'équipe est en mesure de prévenir, détecter, investiguer et répondre à des incidents en cybersécurité qui pourraient avoir un impact sur l'organisation, ses activités ou clients (Cyware, 2018). La section qui suit, la section 2.5, est la dernière section de ce chapitre et illustre à l'aide d'un cadre conceptuel les 7 facteurs de succès et les 6 rôles ainsi que les liens qui les unissent.

2.5 Cadre conceptuel proposé

Cette section présente le cadre conceptuel sur les facteurs de succès et rôles composant une équipe ICIC interdisciplinaire. Ce cadre a été créé suite à la recherche effectuée auprès de plus d'une centaine de sources d'écrits professionnels et d'articles de recherche.

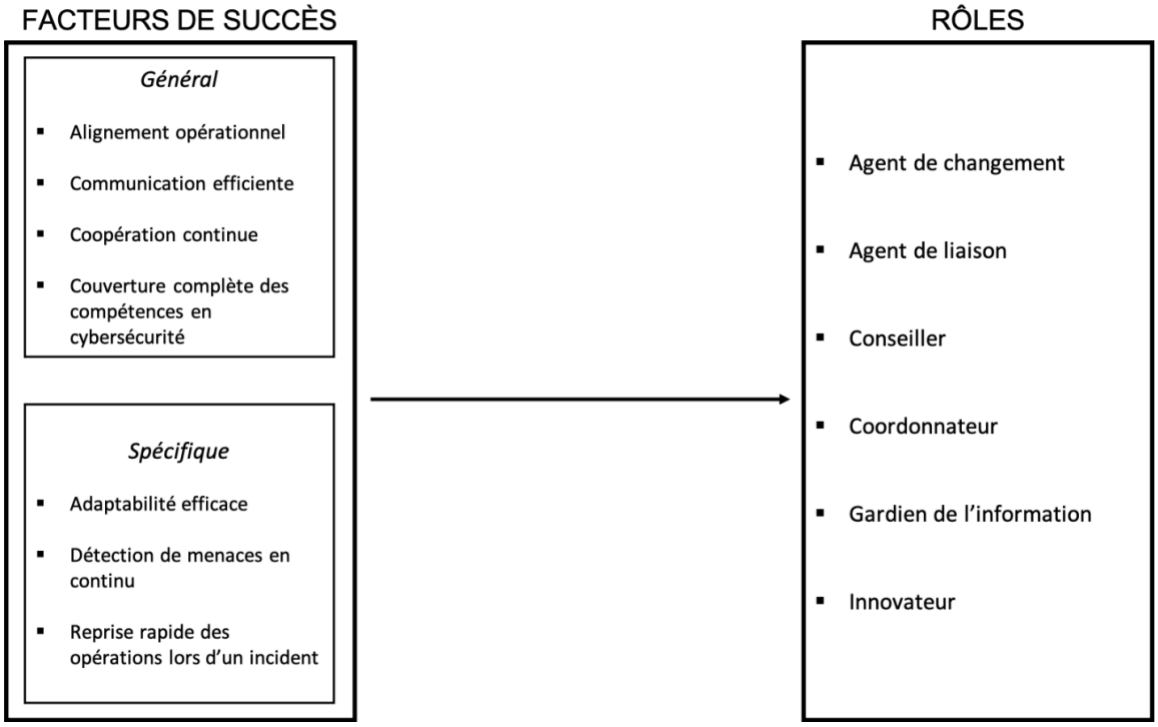


Figure 2.16 - Facteurs de succès et rôles au sein de la composition d'une équipe ICIC interdisciplinaire

La figure ci-haut présente premièrement les facteurs de succès à gauche et les rôles clés de l'équipe ICIC interdisciplinaire à droite. À gauche se retrouvent les facteurs de succès, divisés dans les deux catégories mentionnées initialement soit la catégorie « général » (pour toute équipe de travail et la catégorie « spécifique » (directement liée à une équipe d'intervention en cybersécurité). Puis, à droite sont les six rôles clés identifiés. Les rôles sont présentés à la suite des facteurs de succès, car ils reposent sur ceux-ci afin que leurs objectifs respectifs soient déterminés. Par exemple, les facteurs de communication efficiente, coopération continue et adaptabilité de l'équipe ont mené à l'identification de l'agent de changement comme clé pour l'équipe ICIC interdisciplinaire. Ce rôle existe pour d'autres équipes de travail, mais étant donné qu'un rôle était nécessaire pour incarner ces facteurs de succès, ce rôle-ci a été retenu, car les responsabilités lui étant attribuées dans la littérature reposaient sur les facteurs identifiés. Ainsi, les six rôles ont tous été identifiés de cette façon, suite au choix des facteurs de succès pour l'équipe ICIC interdisciplinaire. Étant donné le contexte de cette étude, soit celui de la composition d'une équipe performante, seuls les facteurs et rôles qui favorisaient une bonne performance (selon ce qui étaient mentionné dans la littérature) ont été retenus. De plus, cette équipe performante a ainsi un impact positif sur la performance organisationnelle (Iannucci et Garland, 2020) en permettant le suivi et contrôle des opérations.

Ce chapitre a présenté le survol de la littérature qui a été effectué afin de premièrement cibler la structure d'équipe interdisciplinaire comme structure d'équipe pour cette étude. Ensuite, l'emphase a été placée sur l'équipe d'intervention en cas d'incident en cybersécurité afin de détailler sa composition. Ceci a été fait par l'entremise de facteurs de succès et de rôles indiqués dans la littérature. Finalement, le cadre conceptuel initial a été présenté afin de permettre une visualisation de cette composition. Le chapitre 3 qui suit présente la méthodologie employée dans cette étude pour ultérieurement être en mesure de valider ce qui a été trouvé dans la littérature par l'entremise d'une collecte de données.

Chapitre 3. Méthodologie

En guise de rappel, ce mémoire a pour objectif principal de proposer des pistes de réflexion sur la composition d'une équipe interdisciplinaire d'intervention en cas d'incident en cybersécurité. De plus, des sous-objectifs sur l'identification de facteurs de succès et rôles favorisant la performance de l'équipe ICIC interdisciplinaire sont également poursuivis. À la fin de la revue de la littérature, un cadre conceptuel a été présenté suite à une recension d'écrits professionnels et de recherche. Ce troisième chapitre présente la méthodologie utilisée pour valider les éléments qui y sont présentés.

Ce chapitre est divisé en 4 parties. Premièrement, l'approche méthodologique choisie pour cette étude, l'approche qualitative de l'étude de cas, est expliquée et justifiée par rapport aux objectifs de recherche. Ensuite, les diverses étapes de la collecte de données sont détaillées en présentant entre autres les outils de collecte et le déroulement des entrevues semi-dirigées. Troisièmement, les grandes lignes de l'analyse des données recueillies sont présentées. Finalement, la dernière partie du chapitre est celle plaçant l'emphase sur le respect de l'éthique au sein de cette étude.

3.1 Choix de la méthodologie et justifications

Cette section détaille et explique le choix de la méthodologie de l'étude de cas pour répondre aux objectifs de recherche. La section est divisée en deux parties : (1) Une justification du choix de l'étude qualitative dans ce contexte et (2) Une justification du choix de l'étude de cas pour cette étude.

3.1.1 Justification de l'étude qualitative

L'étude qualitative a été choisie pour ce mémoire. Plusieurs facteurs ont déterminé ce choix dont le type de questions de recherche, la position de l'étude et la logique en fonction des objectifs

de recherche et finalement les avantages que l'étude qualitative présente pour le contexte étudié contrairement à l'étude quantitative.

Premièrement, la question de recherche de cette étude est une question exploratoire. Étant donné que le sujet des équipes interdisciplinaires en cybersécurité est un sujet peu étudié dans la littérature, la question de recherche présentée au premier chapitre est une question plus ouverte qui permet d'explorer le sujet et d'entamer sa compréhension. Ainsi, les concepts étudiés sont des concepts jugés embryonnaires par la littérature en cybersécurité et la chercheure s'est concentrée sur la cueillette d'impressions et perceptions de la part des répondants (Micheneau, 2012). Deuxièmement, la position de l'étude est une position positiviste. Dans cette étude, l'objectif est d'expliquer comment la composition d'une équipe ICIC interdisciplinaire pourrait être établie. Les faits sont alors interrogés pour découvrir une structure dans laquelle les relations peuvent être analysées afin de confirmer ou réfuter des éléments. Troisièmement, la logique de l'étude est une logique inductive. Étant donné qu'il n'y a pas beaucoup de théorie dans la littérature sur le sujet étudié, la logique inductive est préférée à celle déductive, car dans la logique inductive nous pouvons baser nos propositions finales sur ce qui est relevé lors de la collecte de données (Kumar, 2011). C'est-à-dire, le cadre conceptuel proposé peut être modifié, des éléments enlevés ou ajoutés, en fonction de ce qui ressort lors de la collecte de données. Ceci est également possible grâce à une caractéristique propre à l'étude de cas qui est celle de la flexibilité (Kumar, 2011). Finalement, l'étude qualitative a été préférée à celle quantitative, car elle nous permet de comprendre, d'explorer et de clarifier un phénomène en plus d'offrir plus de fluidité que l'étude quantitative (Kumar, 2011). L'étude de cas permet ainsi d'investiguer un phénomène dans son contexte et d'avoir une compréhension plus en profondeur de ce phénomène plutôt que de rechercher à généraliser les résultats (Orlikowski et Baroudi, 1991). En suivant cette logique, les données recueillies à l'aide d'une méthodologie qualitative reflètent également plus le contexte organisationnel qui est placé au premier plan de l'étude et la perception des répondants interrogés lors d'une collecte en plus proche proximité que lorsqu'un questionnaire quantitatif est transmis, par exemple (Miles et Huberman, 1994). Étant donné que les objectifs de recherche de ce mémoire poussent vers la

compréhension et l'exploration du phénomène des équipes interdisciplinaires en cybersécurité, l'approche qualitative a été utilisée.

3.1.2 Justification du choix de l'étude de cas et du cas

Comme mentionné, l'étude de cas est l'approche méthodologique qui a été choisie pour ce mémoire, et ce pour plusieurs raisons. Premièrement, cette étude mène à des propositions sur la composition d'une structure d'équipe basée sur une idée embryonnaire au sein du contexte de cybersécurité. Deuxièmement, l'étude de cas permet de supporter la nature exploratoire de l'étude (Micheneau, 2012). Troisièmement, l'étude de cas permet l'évolution du cadre conceptuel de par sa flexibilité dans la méthode de collecte de données et dans la méthode d'analyse de données (Kumar, 2011). Finalement, tel que mentionné au premier chapitre, un intérêt grandissant est démontré dans le domaine des TI sur les éléments humains influençant celui-ci, et ainsi non seulement sur les éléments techniques (Paré, 2004). Dû à ceci, l'étude de cas s'applique bien à ce type d'étude, car elle place le contexte organisationnel en avant-plan de l'étude.

Plusieurs domaines, autre que celui de la cybersécurité, ont déjà entrepris l'étude de la création d'une équipe interdisciplinaire. Dans ce mémoire, un minimum de deux disciplines est retenu dans toute mention de ce type d'équipe. Ceci suit la logique de la définition du concept d'équipe, logique dans laquelle deux individus sont nécessaires pour créer une équipe (Fewster-Thuente et Velsor-Friedrich, 2008). Par exemple dans le domaine de la santé, les équipes interdisciplinaires permettent aux praticiens de prendre des décisions plus informées supportées par d'autres experts dans leur domaine respectif (Drotar , 2002). Cette intégration entre plusieurs perspectives peut également être bénéfique en cybersécurité aux équipes qui doivent contrer la montée des cybercrimes et les attaques variées des cybercriminels. L'organisation peut ainsi avoir accès à un plus grand niveau et une plus grande diversité d'expertise pour prévenir et réagir à ce type d'attaque.

Ensuite, en éducation, déjà en 1956 on disait que plusieurs têtes sont mieux qu'une. Le domaine de l'éducation spécialisée voyait le potentiel de résoudre des problèmes à l'aide d'individus qui proviennent de formations différentes (Bradley, 1956). Avec le temps, la place de l'équipe interdisciplinaire en éducation a également augmenté. Avant les années 2000, on voyait l'amélioration que cette équipe représente comparativement aux structures traditionnelles et les différentes perspectives d'enseignement qui pouvaient ainsi émerger d'une structure interdisciplinaire (Davis, 1995 ; Dinitz et al., 1997). Puis, les années récentes ont vu une évolution de premièrement une compréhension sur les changements au sein de la société auxquels il est nécessaire de s'adapter (Fauvel et al., 2010) ; deuxièmement que de nouvelles perspectives peuvent être utiles pour l'avancement du domaine académique (Krometis et al., 2011) et ; troisièmement les étudiants eux-mêmes ont mentionné qu'ils voient la valeur ajoutée et l'importance de jumeler des compétences qui proviennent de différentes disciplines pour régler un problème (Collins, 2017).

Puis, il y a également un intérêt dans le domaine de la recherche sur les équipes interdisciplinaires. L'argument principal avancé est que les individus ont rarement toute l'expertise nécessaire pour livrer des solutions, que ce soit dans le domaine de la santé, de l'éducation ou encore des affaires (Lakhani et al., 2012). Ceci permet non seulement la résolution de problèmes, mais permet également l'avancement de toutes les disciplines au sein de l'équipe (Palmer, 2017), rendant tout ce processus dynamique. De plus, en recherche il a été noté que les équipes interdisciplinaires sont souvent des équipes avec une grande ouverture d'esprit dans lesquelles l'apprentissage de la contribution potentielle des différentes disciplines est autant important que l'arrivée à une solution (Lyall et Meagher, 2007).

Tous ces domaines et d'autres ont vu des avantages clairs et précis suite à l'implantation d'une équipe interdisciplinaire au sein d'organisations. Ceci combiné avec les éléments favorisant le choix de l'équipe interdisciplinaire en cybersécurité complète la réflexion qui a mené au choix de l'utilisation de cette structure de collaboration pour cette étude de cas.

Étant donné la nature exploratoire de cette étude et le peu de littérature disponible sur la composition d'une équipe interdisciplinaire en cybersécurité, un seul cas est étudié dans cette étude bien que plusieurs recherches existent dans d'autres domaines. Une étude multicas aurait été préférée dans un contexte dans lequel le sujet à l'étude est développé dans la littérature et les différents cas auraient pu alors être comparés afin d'analyser les différences et ressemblances entre eux (Yin, 2003 ; Baxter et Jack, 2008). Toutefois, étant donné que le but de ce mémoire est d'étudier en profondeur les facteurs de succès et rôles composant une équipe ICIC interdisciplinaire, l'étude d'un seul cas a été sélectionnée.

La stratégie utilisée pour le choix du cas est par critères (*criterion sampling*), car elle permet au chercheur de sélectionner un cas en fonction de critères préétablis (Paré, 2004).

Les critères suivants ont mené au choix de l'étude de cas de cette étude :

- Une culture organisationnelle favorisant la protection de l'actif informationnel ;
- Une culture organisationnelle favorisant le travail en équipe dont les membres proviennent de différentes fonctions et domaines liés à la cybersécurité ;
- Une culture organisationnelle misant sur l'innovation des procédures de travail et ;
- Une expérience organisationnelle sur la gestion de risques pouvant mener à des incidents de sécurité.

Ces critères sont tous pertinents à considérer pour le choix de l'organisation, car celle-ci doit posséder une culture et expérience organisationnelle afin de comprendre le potentiel d'une équipe interdisciplinaire présente de façon permanente. La littérature n'a pas de référence sur le nombre de disciplines requis pour rendre une équipe interdisciplinaire.

Suite à l'établissement de ces critères, l'organisation ABC[1] a été sélectionnée pour l'étude de cas de ce mémoire puisqu'elle satisfait à tous ces critères. Cette grande organisation québécoise est

[1] Conformément à l'entente de confidentialité signée avec l'organisation, le nom et la description de l'organisation sont présentés de façon anonyme.

un cas très riche pour valider les éléments du cadre conceptuel proposé. La culture de cette organisation met l'emphase sur la sécurité de l'information, l'incluant dans ses principaux piliers et objectifs stratégiques. L'autorisation de l'organisation ABC a été demandée et un accord a été convenu entre celle-ci et la chercheure.

Après avoir obtenu un accord tacite pour cette collaboration de recherche, la chercheure a également obtenu un emploi au sein de cette organisation, ce qui lui a permis de confirmer le respect des critères de sélection pour le cas. De plus, elle a pu observer que des cellules de crise gérant des incidents de façon permanente existent au sein d'ABC. Ces cellules collaborent en fonction de l'incident et se partagent l'information nécessaire pour la gestion de celui-ci. L'organisation ABC est également en processus d'ajouter une équipe SOC à ses équipes, équipe axée sur la gestion technique de cyberattaques. En plus des critères précédemment mentionnés, l'organisation ABC est intéressante à étudier, car elle comporte des équipes d'incidents qui devront éventuellement s'arrimer avec une équipe SOC. Bien que ces équipes ne soient pas interdisciplinaires, la grande place qui leur est accordée au sein de l'organisation ABC permet d'approfondir les discussions sur la gestion d'incidents.

Étant donné que la chercheure travaille au sein d'ABC, un conflit d'intérêt potentiel existe. Toutefois, aucune information identificatoire recueillie dans le cadre des entrevues n'a été partagée avec quiconque faisant partie de l'organisation. Ce type d'information a été réservé à l'analyse pour les fins du mémoire uniquement. De plus, la chercheure n'a pas passé en entrevue des supérieurs immédiats afin d'éviter tout conflit éthique qui pourrait survenir. Aucun propos énoncé par les différents employés ou aucune retranscription effectuée n'ont été rapportés directement à l'organisation pour limiter les risques de bris de confidentialité des participants.

3.2 La collecte de données

La collecte de données est divisée en quatre étapes (la sélection des participants, la collecte des données via un questionnaire, la collecte des données via les entrevues et la collecte des données provenant des documents organisationnels) qui sont illustrées dans la figure 3.1 ci-dessous puis décrites brièvement dans les sous-sections suivantes. À noter qu'étant donné le contexte de pandémie de la COVID-19, les observations en mode présentiel n'ont pas été effectuées.

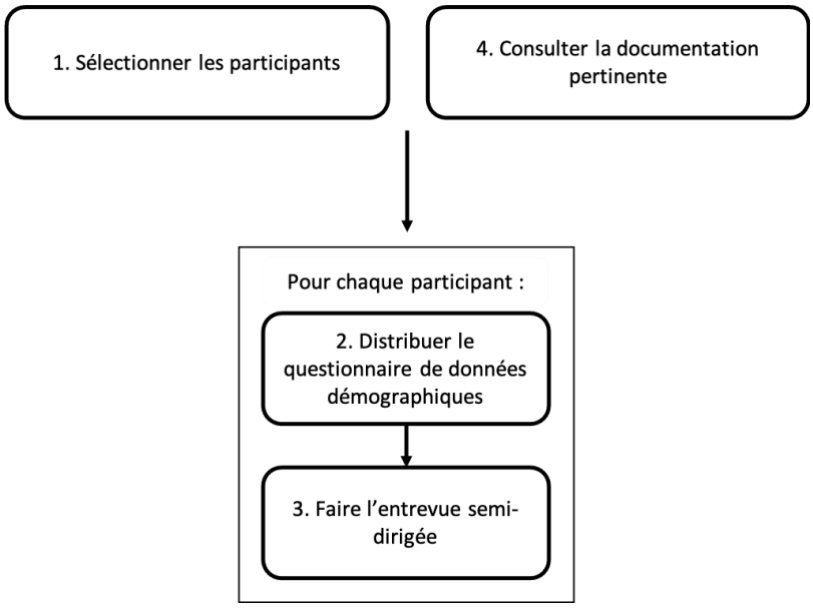


Figure 3.1 - Survol des différentes étapes de la collecte de données

3.2.1 Sélectionner les participants

La population visée par cette étude est celle des employés de l'organisation ABC qui travaillent dans un domaine en TI de l'organisation comme par exemple la gouvernance de la sécurité de l'information, l'exploitation des systèmes ou encore des réseaux. Cette population s'élève à approximativement 4000 employés au sein de l'organisation ABC. Des critères d'inclusion et d'exclusion ont été établis pour cibler le type de participant visé par l'étude :

(1) Avoir un poste au sein de l'organisation ABC ;

Étant donné la nature de l'étude, une recherche qui a pour une étude de cas de l'organisation ABC, chaque participant doit être présentement employé au sein de l'organisation ABC (et non pas un consultant externe travaillant sur un mandat ponctuel au sein de l'organisation).

(2) Avoir une expérience en sécurité de l'information d'au minimum 3 ans ;

Une expérience minimale en sécurité de l'information est requise pour que le participant comprenne les défis de la cybersécurité et soit en mesure d'apporter des propos constructifs lors de l'entrevue en ayant en tête son expérience professionnelle dans le milieu et les situations auxquelles il a dû faire face.

(3) Avoir une expérience au sein d'une équipe de travail interdisciplinaire de minimalement le temps d'un projet ;

Pour ce critère, une expérience de longue durée n'est pas nécessaire, car l'objectif du critère est uniquement que le candidat comprenne la structure à l'étude. Il doit être en mesure de se placer mentalement dans une telle situation lorsqu'il répond aux questions.

(4) Une diversité dans les postes et départements des participants (échantillonnage non aléatoire pour cette raison) ;

- Environ 2 spécialistes des politiques organisationnelles
- Environ 2 spécialistes en gestion des vulnérabilités
- Environ 2 spécialistes en gestion d'identité et des accès
- Environ 2 chefs d'équipe (depuis minimalement 1 an dont 6 mois consécutifs au minimum au sein d'ABC)
- Environ 2 directeurs (depuis minimalement 1 an dont 6 mois consécutifs au minimum au sein d'ABC)

Le but de ce critère est d'obtenir une diversité dans les postes afin d'obtenir l'opinion de plusieurs départements en sécurité de l'information au sein de l'organisation ABC.

(5) Avoir fait partie d'une équipe ayant fait face à un événement d'incident de cybersécurité dans les 2 dernières années.

Ce dernier critère est important, car il rejoint l'objectif principal de l'équipe proposée dans cette étude, soit une intervention de première ligne lors d'un incident en cybersécurité. Les participants doivent avoir eu une implication récente dans un incident de sécurité pour être en mesure de se placer mentalement en contexte d'incident en répondant aux questions. Dans le cadre de cette étude, les détails de l'incident ne sont pas demandés par la chercheure pour assurer la confidentialité des participants.

À la suite de l'établissement de ces 5 critères, une liste de participants potentiels a été obtenue par réseau de contacts de la chercheure à travers l'organisation ABC. Ensuite, la méthode boule de neige a été utilisée. À l'aide de celle-ci, les participants ont pu à leur tour proposer des participants potentiels à la chercheure. La chercheure a ensuite contacté ces participants potentiels par courriel en leur envoyant le même courriel de recrutement. Pour assurer la confidentialité de tous les participants, les noms de ceux ayant proposé d'autres individus comme participants potentiels n'ont jamais été divulgués. L'objectif ultime était de sélectionner entre 12 et 15 individus. Nous estimons qu'un tel échantillon nous permet d'obtenir des données riches tout en respectant des contraintes logistiques liées à la réalisation de ce mémoire.

Le premier contact avec les participants potentiels a été effectué par courriel lors de l'envoi d'une lettre de recrutement par la chercheure. Ce courriel présentait l'objectif principal de l'étude aux destinataires, la définition globale de l'équipe ICIC interdisciplinaire et un aperçu des thèmes abordés lors de l'entrevue individuelle (Annexe 2).

3.2.2 Distribuer le questionnaire de données démographiques

Le premier outil de collecte utilisé est celui du questionnaire de données démographiques (Annexe 3). L'objectif de cette étape est de réduire la durée des entrevues et de laisser les participants répondre à ces questions au moment qui leur convient. Pour ce faire, le questionnaire a été conçu sur la plateforme de sondage en ligne, Qualtrics. Tous les participants de l'étude ont dû répondre au questionnaire en y accédant par un lien qui leur a été envoyé par la chercheure par courriel. Le lien n'a été envoyé qu'aux participants de l'étude, après qu'ils aient consenti à participer.

Une seule version du questionnaire a été conçue pour l'ensemble des participants, peu importe leur poste hiérarchique au sein de l'organisation ABC. Cette décision a été prise, car le but de ce questionnaire est de récolter des données démographiques afin de dresser un portrait global des participants. Ainsi, il n'était pas nécessaire de séparer les participants.

Le questionnaire est composé de 7 questions et ces questions portent sur la formation académique du participant, son expérience professionnelle générale ainsi que son expérience au sein de projets nécessitant une réponse à un incident en cybersécurité. Les questions du questionnaire ont été sélectionnées par la chercheure en utilisant sa compréhension de la dynamique de l'organisation ABC, mais également en s'inspirant de questions contenues dans des questionnaires démographiques présentés dans d'autres mémoires de HEC Montréal. Plus précisément, les questions ont été reprises du questionnaire démographique du mémoire de Dhennin (2011), de la présentation du profil des répondants de Chartrand (2010) et de Loyer (2016). De plus, les choix de réponse aux questions posées (par exemple : le poste occupé présentement au sein d'ABC) ont été sélectionnés en fonction des connaissances de la chercheure sur les postes les plus répandus en sécurité de l'information chez l'organisation ABC. La chercheure a connaissance de ces postes, car elle travaille présentement au sein de cette organisation.

Un prétest a été effectué afin de valider les questions posées et la durée approximative pour y répondre ainsi que pour déterminer si des clarifications devaient être apportées aux questions posées. Le prétest a été effectué auprès de 2 étudiants à la maîtrise en Transformation Numérique de HEC ainsi qu'auprès d'un gestionnaire et une analyste au sein de l'organisation ABC. Suite à ces prétests, des modifications mineures ont été apportées au questionnaire Qualtrics. Ces modifications visaient la formulation de certaines questions et choix de réponses.

3.2.3 Faire l'entrevue semi-dirigée

Le deuxième outil de collecte de données pour cette étude est l'entrevue individuelle semi-dirigée. L'objectif de ces entrevues est de permettre une analyse comparative entre le cadre conceptuel proposé et les propos des participants. Plusieurs choix, autre que dû à l'étude de cas, ont poussé la sélection de l'entrevue semi-dirigée pour la collecte de données. Premièrement, l'entrevue semi-dirigée se déroule majoritairement comme une conversation entre le chercheur et les répondants, conversation durant laquelle le chercheur peut plus facilement s'adapter et adapter ses questions au rythme de la conversation. Deuxièmement, la flexibilité que l'entrevue semi-dirigée apporte permet d'obtenir une compréhension plus riche du phénomène étudié (Kumar, 2011). Troisièmement, tous ces éléments permettent de stimuler la discussion encore plus comparativement à une entrevue structurée, mais permettent quand même de délimiter les frontières de l'entrevue contrairement à une entrevue non dirigée. Ces frontières sont délimitées à l'aide des questions ouvertes contenues dans le guide d'entrevue préparé à l'avance.

Bien que l'utilisation de la structure semi-dirigée pour les entrevues a ses forces, soit entre autres la possibilité d'expliquer les questions aux participants si un élément n'est pas bien compris ou pas bien énoncé initialement, cette structure a également des faiblesses dont il faut tenir en compte. Premièrement, des détails de l'entrevue peuvent être oubliés si la prise de note ou la retranscription des entrevues ne sont pas bien effectuées (Paré, 2004). D'autre part, la qualité des données dépend de la qualité des réponses obtenues. Pour contrer ces éléments, une synthèse a été effectuée par la chercheure suite à chaque entrevue à l'aide de grilles d'analyses

individuelles des entrevues. De plus, lors des entrevues, la chercheure a posé des questions supplémentaires aux participants afin de pousser la profondeur de leurs réponses si nécessaire.

3.2.3.1 Quelques détails sur le protocole d'entrevue

Un protocole d'entrevue détaillé (Annexe 4) a été élaboré pour tous les participants, peu importe leur poste au sein de l'organisation ABC. Cette décision a été prise, car il a été jugé que tout participant répondant aux critères de sélection pour l'étude serait en mesure de répondre adéquatement aux questions posées. Plus spécifiquement, le protocole d'entrevue a été conçu de manière à pousser la conversation et la réflexion des participants sur le sujet de l'équipe ICIC interdisciplinaire. Ainsi, les questions ont été orientées sur la perception des participants au niveau des facteurs de succès et rôles proposés par la littérature au sein d'une équipe ICIC interdisciplinaire. Tout comme pour le questionnaire de données démographiques, plusieurs mémoires de HEC Montréal ont inspiré la structure du protocole d'entrevue. Entre autres, les mémoires de Chartrand (2010), Dhennin (2011), Nguyen (2017) et de Frigault (2018) ont été consultés. Finalement, le contexte et le climat de l'organisation ABC ont aussi été une source d'inspiration afin de déterminer comment commencer les conversations lors des différentes entrevues. Le tableau ci-dessous présente un résumé du protocole d'entrevue :

Tableau 3.1 : Sommaire du protocole d'entrevue

Partie du guide d'entrevue	Questions posées
Présentation de l'équipe ICIC interdisciplinaire	• Commentaire(s) sur la définition de l'équipe ICIC interdisciplinaire • Pertinence de la présence de l'équipe au sein de l'organisation
Cadre conceptuel – Facteurs clé de succès	• Pertinence du facteur pour favoriser la performance de l'équipe ICIC interdisciplinaire • Perception des indicateurs de performance présentés
Cadre conceptuel – Rôles	• Pertinence du rôle pour favoriser la performance de l'équipe ICIC interdisciplinaire

3.2.3.2 Quelques détails sur l'entrevue et sa structure

Les entrevues ont été effectuées par vidéoconférence, à l'aide de l'outil Microsoft Teams. La vidéoconférence a été utilisée pour faciliter la planification des entrevues en fonction des disponibilités des participants, mais également dû à la situation de pandémie mondiale de la COVID-19. En effet, dû à cette pandémie, la distanciation physique est essentielle et obligatoire, ce qui rendait les entrevues en mode présentiel impossible à compléter.

Par ailleurs, tout comme pour le questionnaire de données démographiques, un prétest a été effectué auprès de 2 étudiants à la maîtrise en Transformation Numérique de HEC Montréal ainsi qu'auprès d'un gestionnaire et d'une analyste au sein de l'organisation ABC afin que ceux-ci valident la clarté des questions et la durée estimée d'une heure par entrevue. Suite à ces prétests, des modifications mineures ont été effectuées. Entre autres, la formulation de certains éléments du cadre conceptuel a été revue afin d'améliorer leur compréhension. De plus, une suggestion généralisée a été d'utiliser un support visuel (PowerPoint) pour améliorer le dynamisme de la rencontre. Pour ce faire, le support devait être utilisé dans un angle de présentation utilisé en contexte professionnel à l'aide de l'ajout de figures et d'images. Par exemple, il fut suggéré d'utiliser des figures d'individus pour les rôles afin d'illustrer ceux-ci, au lieu d'utiliser simplement du texte pour les décrire.

Les questions d'entrevue n'ont pas été transmises aux participants avant l'entrevue afin de pouvoir stimuler la discussion et garder les participants engagés en plus d'obtenir des réponses spontanées lors de l'entrevue. Le tableau ci-dessous résume le déroulement d'une entrevue et est inspiré de la méthode de Rubin et Rubin (1995) :

Tableau 3.2 : Structure des entrevues semi-dirigées

Parties de l'entrevue	Objectifs	Application pratique lors de l'entrevue
Présenter l'étude	• Rassurer le participant • Présenter les objectifs de l'étude et de l'entrevue	• Présentation de la chercheure • Remerciement de la participation du participant • Explication du but de l'étude et de l'entrevue • Explication du déroulement de l'entrevue • Rappel du formulaire de consentement • Vérification avec le participant s'il a des questions
Poser les questions plus faciles	• Encourager la discussion • Introduire le participant au sujet de l'entrevue	• Questionnement sur la perception du répondant sur la définition de l'équipe ICIC interdisciplinaire présentée (partage d'écran) • Vérification avec le participant s'il a des questions ou commentaires sur les objectifs de l'équipe ICIC interdisciplinaire
Poser les questions plus difficiles	• Poser des questions sur les éléments du cadre conceptuel • Pousser la profondeur des réponses du participant • Garder le participant engagé	• Validation du cadre conceptuel à l'aide de cartes (partage d'écran) • Utilisation de mises en contexte • Validation des facteurs clés de succès • Validation des rôles
Atténuer le niveau d'intensité	• Permettre au participant d'émettre des commentaires ou de poser des questions sur des éléments soulevés lors de l'entrevue	• Faire un retour sur ce qui a été mentionné lors de l'entrevue • Recueillir les commentaires du participant
Conclusion	• Clore le sujet • Ouvrir la possibilité d'un suivi avec le participant	• Remercier le participant de son temps • Proposer de transmettre les résultats • Demander la permission de recontacter le participant en cas de questions supplémentaires • Mentionner au participant de communiquer tout nom qui représenterait un participant potentiel pour la suite de l'étude

La première partie permet de remercier le participant de son engagement dans l'étude et de lui rappeler le rôle de son organisation dans celle-ci. En plus, elle permet de répondre à tous les questionnements du participant au sujet de l'étude avant de commencer l'entrevue.

Dans la deuxième partie, l'équipe ICIC interdisciplinaire est présentée au participant afin d'introduire le sujet de l'entrevue. À partir de cette phase, la chercheure a partagé son écran. Le partage d'écran a été privilégié durant l'entrevue pour faciliter l'échange et la communication avec le participant. Bien que les participants aient reçu la définition de l'équipe à l'avance, cette phase de l'entrevue a été nécessaire afin de recueillir leur opinion sur la pertinence de la présence d'une équipe de ce genre au sein de l'organisation ABC.

Ensuite, la troisième partie de l'entrevue a également été faite à l'aide du partage d'écran. Dans cette phase, l'objectif principal était de recueillir la perception des participants sur chaque élément du cadre conceptuel conçu. Pour ce faire, des mises en situation d'incidents en cybersécurité ont été utilisées afin de stimuler la discussion et placer les participants en contexte d'incident relativement comparable. Ces mises en situation s'inspirent fortement des incidents réels survenus chez ABC ou à d'autres organisations similaires. De plus, ces mises en situation ont un niveau de risque relativement comparable, où le risque est défini comme un effet de l'incertitude sur les objectifs de l'organisation, qui provient de pressions de l'environnement de l'organisation (la norme ISO 31000). Autrement dit, le niveau de risque est exprimé en termes de vulnérabilités potentielles, de menaces exploitant ces vulnérabilités et de probabilité que ce risque et ses conséquences surviennent. Bien que, théoriquement, on puisse distinguer un risque direct (soit l'influence d'un événement précis sur les activités de l'organisation) et un risque indirect (soit l'influence de tous les autres éléments externes à l'événement, mais qui sont liés à celui-ci, sur les activités de l'organisation), la collecte de données vise uniquement le risque direct vu la complexité d'évaluer le risque indirect. Ainsi, en se basant sur les leçons tirées dans la littérature professionnelle à la suite des incidents de la même nature que ceux décrits dans les mises en situation, il a été estimé que le niveau de risque de ces mises en situation se situe entre modéré et élevé pour l'organisation ABC.

Pour chaque participant, une mise en situation a été sélectionnée aléatoirement parmi les 5 mises en situation suivantes :

- Le mot de passe d'un fichier contenant des informations confidentielles est laissé à découvert sur le poste de travail d'un employé (par exemple, un post-it collé sur l'écran), à la vue d'autres employés ;
- Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe ;
- Une feuille de route de suivi d'une vulnérabilité technique connue d'un fournisseur en approvisionnement technologique n'est pas mise en place par l'organisation ;
- Un employé négligent utilise son appareil mobile pour envoyer des informations confidentielles de clients de son adresse courriel professionnelle vers son adresse courriel personnelle ;
- Un dossier partagé confidentiel n'est pas détruit à la fin de son utilisation et des employés ont encore accès aux informations confidentielles de clients à l'intérieur de celui-ci.

À l'écran, la chercheure a affiché une présentation PowerPoint (Annexe 5) dans laquelle s'affichait premièrement dans le haut de la page la mise en contexte choisie aléatoirement. Par la suite, chacune des diapositives suivantes présentait tour à tour les 13 éléments du cadre conceptuel. Dans les diapositives sur les rôles, des figures étaient également illustrées afin de représenter visuellement chacun de ces rôles et d'ajouter au dynamisme de la rencontre.

Voici un exemple de structure de diapositive, soit celle du facteur clé de succès *Communication efficiente au sein de l'équipe* :

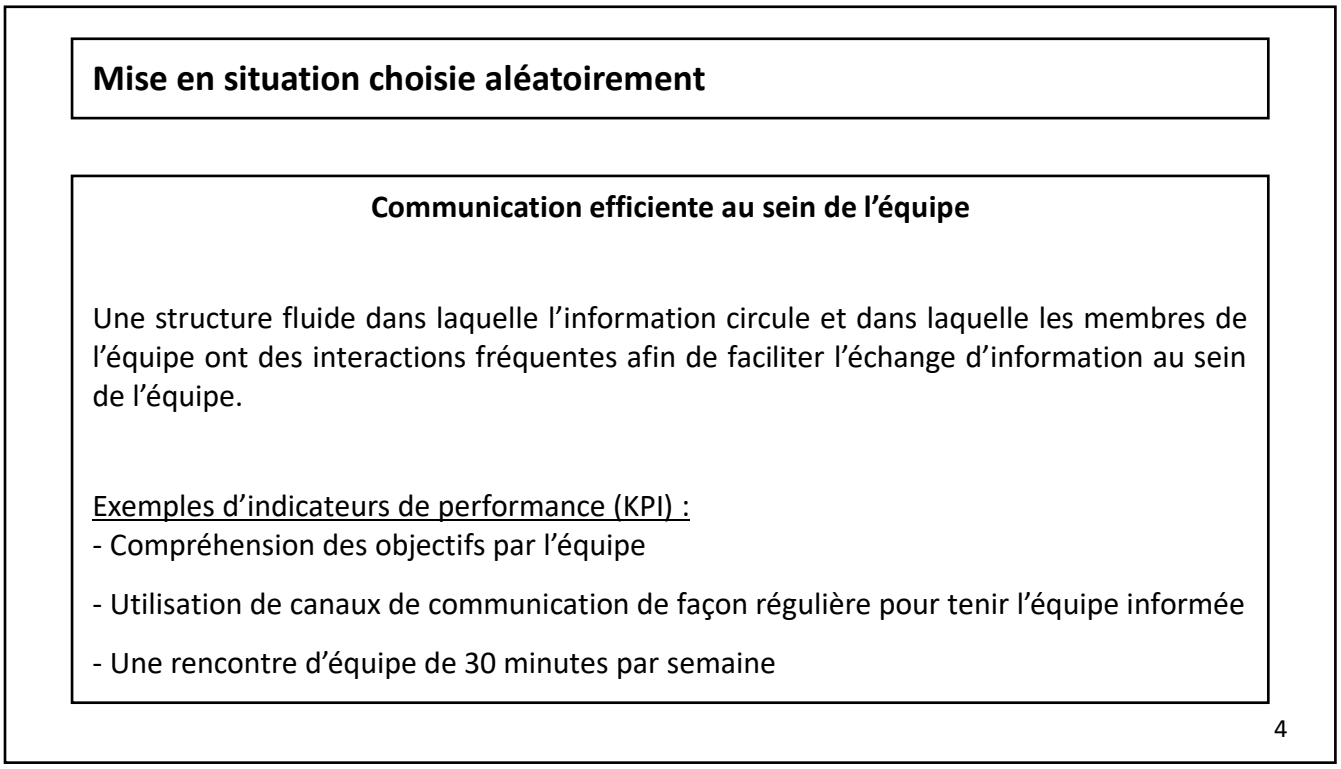


Figure 3.2 – Exemple de structure utilisée lors de la présentation des éléments du cadre conceptuel

Ces diapositives présentant les éléments du cadre conceptuel ont été affichées de façon aléatoire au participant lors de l'entrevue. Les éléments sont présentés de façon aléatoire afin de minimiser le biais dans les réponses des répondants et de minimiser le biais de préférence de la chercheure.

Afin de garder le participant engagé tout au long de l'entrevue et pour obtenir une réponse spontanée de sa part, en plus des mises en situation un énoncé a été indiqué au participant lors des questions. Cet énoncé a été présenté comme suit, avant chaque question sur un élément du cadre conceptuel :

Dans la situation X (mise en situation sélectionnée aléatoirement), 'Y' (élément questionné du cadre conceptuel) n'aurait **pas** été utile à l'équipe pour répondre à l'incident en cybersécurité.

Toutefois, suite aux prétests effectués, il a été décidé de varier la formulation de l'énoncé. En effet, cela a été favorable afin de ne pas perdre l'attention du participant. Ainsi, l'énoncé était formulé sous forme de négation pour certains éléments tandis qu'il était formulé comme une affirmation pour d'autres éléments du cadre conceptuel. En plus de l'évaluation des éléments, dans la section d'évaluation des facteurs clés de succès, l'opinion sommaire des participants sur les indicateurs de performance a également été demandée.

Pour atténuer le niveau d'intensité de l'entrevue, dans la quatrième partie la chercheure a fait un résumé au participant de l'entrevue en rappelant les objectifs de l'équipe ICIC interdisciplinaire et en illustrant les 13 éléments à l'aide du cadre conceptuel. Le cadre a uniquement été présenté à la fin de l'entrevue afin de ne pas perdre l'attention du participant au tout début en lui indiquant à l'avance quels éléments en faisaient partie. En plus, l'illustration du cadre avait pour but de stimuler une dernière réaction de la part du participant. Il a alors été demandé au participant s'il avait des commentaires supplémentaires à apporter.

Pour clore l'entrevue, le participant a d'abord été remercié une dernière fois. Ensuite, la chercheure a demandé si elle pouvait le recontacter si des clarifications étaient nécessaires. L'entrevue s'est terminée en mentionnant au participant que s'il avait des recommandations pour des participants potentiels, il pouvait communiquer avec la chercheure à tout moment.

3.2.4 Consulter la documentation pertinente

Le troisième et dernier outil lors de cette collecte de données est la documentation au sein de l'organisation ABC. Cet outil de collecte a permis à la chercheure de valider des éléments de la culture organisationnelle et de corroborer l'information obtenue lors des entrevues par l'entremise d'autres sources d'information. Pour ce faire, l'autorisation de l'organisation ABC a été obtenue pour consulter toute donnée secondaire jugée pertinente pour répondre aux objectifs de recherche. L'utilisation de données secondaire est appropriée dans le cadre de cette étude pour les raisons suivantes : (1) elles permettent d'obtenir plus d'informations sur le

contexte organisationnel ; (2) elles sont stables dans le temps et peuvent être consultées lorsque jugé nécessaire (Paré, 2004) et (3) elles permettent d'appuyer les éléments apportés par les participants. Dans le cadre de l'étude, les données secondaires consultées sont les politiques organisationnelles et des exemples de postes de travail au sein de l'organisation ABC en sécurité de l'information.

3.3 Analyse des données

Cette sous-section détaille les différentes étapes suivies lors de l'analyse des données collectées à l'aide des questionnaires, des entrevues semi-dirigées et de la documentation consultée. Cette analyse a permis à la chercheure de consolider l'information recueillie lors de la collecte. Ainsi, l'analyse avait comme objectif de consolider toute cette information pour ultérieurement établir des propositions.

L'unité d'analyse de cette étude est les pratiques de l'équipe ICIC interdisciplinaire, terme qui englobe tant les facteurs de succès que les rôles au sein de cette équipe. En effet, bien que l'unité de collecte soit celle de l'individu, car les participants sont rencontrés individuellement lors des entrevues, ce que l'étude tente d'approfondir sont les pratiques de l'équipe ICIC interdisciplinaire afin d'ensuite établir des liens entre ces pratiques et les différents facteurs de succès et rôles composant l'équipe. Il est ici question de la manière dont le groupe agit et comment ceci influence sa structure, le groupe étant donc un ensemble naissant de cet agissement (St-Cyr Bouchard, 2013). Ainsi, les objectifs de recherche énoncés pour cette étude placent les pratiques de l'équipe au centre de cette étude, ce pour quoi elles ont été ciblées comme unité d'analyse. La codification a donc été déterminée afin de permettre une compréhension du contexte de ces pratiques d'équipe et des différents éléments les composant. La figure ci-dessous illustrant une synthèse des étapes de l'analyse de données est décrite dans les sous-sections suivantes.

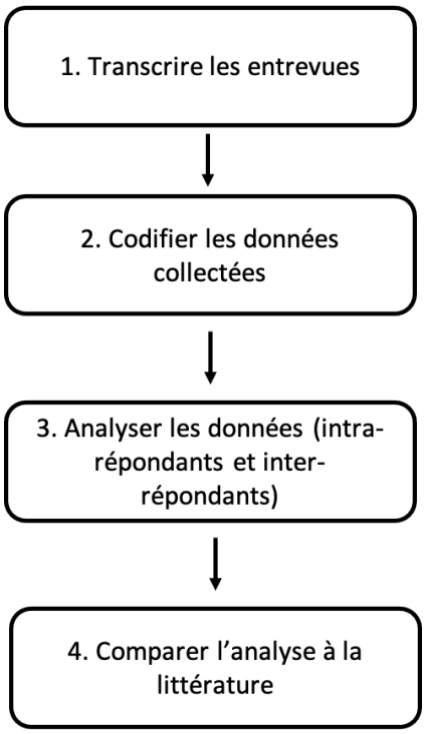


Figure 3.3 - Survol des différentes étapes de l'analyse de données

3.3.1 Transcrire les entrevues

La première étape fut celle de la transcription. Les entrevues, dans leur intégralité, ont été transcrites afin d'avoir une trace écrite de ce qui a été discuté. De plus, cela a permis à la chercheure de faciliter la suite de l'analyse afin de ne pas uniquement se fier à sa mémoire des propos rapportés lors de l'entrevue. La transcription des entrevues a permis ensuite d'analyser toute l'information recueillie sous un même format. Ainsi, les entrevues et la documentation ont pu être regroupées pour discuter de propositions sous des thèmes communs et non sous les différents outils de collecte.

3.3.2 Codifier les données collectées

Suite à la transcription des entrevues, une codification des données provenant des transcriptions, des questionnaires, des notes de la chercheure et des documents organisationnels a été effectuée. Cette codification a été effectuée sur toutes ces sources de collecte d'information pour

que l'analyse puisse ensuite être complétée en même temps pour celles-ci. La codification des questionnaires a permis de (1) dresser le profil des participants et (2) d'observer des liens entre ce profil et les propos ensuite rapportés lors des entrevues effectuées, elles aussi codifiées.

Initialement, une grille de codification a été produite afin de faciliter le processus d'analyse et pour avoir une structure à suivre lors de la codification initiale. Cette grille de codification initiale comportait 4 catégories de codes :

1. Une catégorie sur le Contexte professionnel du Participant (CP) contenant notamment des éléments comme son domaine de formation académique (CP-FA) ou encore le poste qu'il occupe présentement au sein de l'organisation ABC (CP-P);
2. Une section sur les propos rapportés sur l'Équipe Interdisciplinaire (EII) comme sa définition (EII-DEF) ou encore la pertinence de sa présence (EII-PERT) au sein d'ABC;
3. Une première section sur le cadre conceptuel, par rapport aux Facteurs Clés de Succès (FCS), qui inclue un code pour chaque élément (par exemple : FCS-COMM pour le facteur clé de succès de la communication efficiente) et;
4. Une deuxième section sur le cadre conceptuel, par rapport cette fois-ci aux Rôles (ROL), qui inclue un code pour chaque élément (par exemple : ROL-AC pour le rôle d'agent du changement).

Toutefois, la codification est un processus qui se veut être une évolution itérative (Urquhart, 2001). Ainsi, lors de l'analyse des transcriptions, certains codes ont été ajoutés à la grille de codification initiale pour former une meilleure représentation des propos rapportés lors des entrevues (Annexe 6). En résumé, des codes ont été ajoutés lorsqu'ils étaient souvent nommés par les participants. Par exemple, le code TYPE-I a été ajouté, car les participants rappelaient souvent l'influence qu'aura le type de l'incident sur les actions posées par l'équipe. Des codes ont également été ajoutés lorsque des facteurs de succès ou rôles non initialement présentés ont été soulevés par plusieurs participants. De plus, le nom des participants a été codifié afin de ne pas afficher leurs noms lors de la présentation des résultats, à l'aide d'une numérotation. Par

exemple, le premier participant a été nommé P1 sur sa grille d'analyse individuelle. Le logiciel Nvivo a été utilisé pour faciliter le processus de codification étant donné la réputation du logiciel et sa facilité d'utilisation.

3.3.3 Analyser les données (intra-répondants et inter-répondants)

Suite à la codification des propos, une première analyse des propos de chacun des répondants été effectuée. Cette première analyse a permis de déterminer quels thèmes revenaient le plus souvent à l'aide de la codification complétée et quels propos et échanges répondaient le plus aux objectifs de recherche précédemment établis. De plus, la documentation consultée fut ajoutée aux endroits où elle pouvait renforcer l'analyse. L'objectif n'était pas d'effectué un classement ou de compter le nombre de fois un thème était soulevé. Plutôt, de comprendre le contexte dans les propos des participants afin de comprendre les raisons qui poussent leur raisonnement et l'influence de la mise en situation sur leur perception. Ensuite, une analyse comparative entre les participants a été effectuée pour consolider les résultats obtenus. Ceci a permis de valider si les propos retenus lors de l'analyse pouvaient être généralisés à tous les participants de cette étude et de bonifier ces propos.

3.3.4 Comparer l'analyse à la littérature

Finalement, suite à la consolidation des propos lors de ces deux analyses, une comparaison de celle-ci a été effectuée avec la littérature. Cette comparaison permet premièrement d'observer de nouvelles interprétations possibles de l'analyse effectuée sur les propos des participants (Dhennin, 2011). Ceci a également permis de réviser les extrants de l'analyse effectuée et de justifier les propositions en s'appuyant à la fois sur la littérature et sur la pratique. L'objectif final était ainsi de pouvoir émettre des propositions suite aux entrevues.

3.4 Considérations éthiques

Tout au long de la collecte des données et de leur analyse, des précautions ont été prises par la chercheure afin d'assurer le consentement des répondants, la confidentialité de leurs propos et renseignements personnels ainsi que pour minimiser les risques de leur participation à l'étude. Le Comité d'Éthique en Recherche de HEC Montréal a également approuvé l'étude avant que la collecte de données ne débute.

3.4.1 Consentement des répondants

Pour ce qui est premièrement du consentement des répondants, leur consentement a d'abord été demandé pour participer à l'étude. Ce consentement a été demandé par l'entremise d'un formulaire électronique dans lequel le consentement d'enregistrement audio de l'entrevue a également été demandé. Le répondant a été informé lors de l'envoi de ce formulaire par courriel que sa participation était volontaire et que l'organisation ABC avait donné l'autorisation à la chercheure d'effectuer cette étude. Le répondant a également été informé qu'il pouvait arrêter de contribuer à l'étude à n'importe quel moment, et ce rappel a été fait aussi au tout début de l'entrevue. Les répondants ont été avertis qu'ils consentaient à participer à l'étude lorsqu'ils acceptaient la réunion Microsoft Teams envoyée par la chercheure. En début de rencontre, ils ont encore une fois énoncé qu'ils acceptaient de participer à l'étude.

3.4.2 Confidentialité des répondants et des propos rapportés

La confidentialité des propos rapportés a également été une dimension éthique surveillée tout au long de la collecte et l'analyse des données.

Premièrement, bien que la confidentialité complète des participants ne puisse être assurée, des mesures ont été mises en place pour minimiser cette possibilité. La confidentialité complète ne peut être assurée, car la liste des participants potentiels a été obtenue à l'aide du réseau de contacts de la chercheure au sein de l'organisation ABC. Ainsi, un répondant pourrait suggérer le nom d'un individu comme participant potentiel et si un des deux partage cette information,

d’autres membres de l’organisation auraient pu être mis au courant. Toutefois, lorsqu'un participant proposait une nouvelle personne, la chercheure n'a pas informé ce participant si la personne a accepté ou refusé de participer à l'étude.

Deuxièmement, en ce qui a trait aux renseignements personnels, certaines données recueillies auraient pu permettre d’identifier les participants que ce soit lors des réponses données pour le questionnaire de données démographiques ou encore lors des entrevues semi-dirigées. Ces données ont été recueillies pour faciliter l’analyse démographique et sont connues dû à ces méthodes de collecte de données, mais n’étaient pas utilisées dans le cadre de l’étude.

Troisièmement, les données secondaires contiennent elles aussi des renseignements identificatoires. Toutefois, ces renseignements ne sont pas pertinents à l’avancement de l’étude et n’étaient donc pas utilisés et ne seront pas diffusés dans ce mémoire. La chercheure a fait abstraction totale des renseignements identificatoires et s’est uniquement concentrée sur, par exemple, la description des postes et responsabilités associées au sein de la documentation consultée de l’organisation ABC. Un exemple de renseignement identificatoire dans cette documentation est le nom d’un employé associé à un poste précis.

3.4.3 Atténuation des risques

Finalement, tout au long de la collecte et l’analyse de données, la chercheure a tenté de diminuer tout risque que des activités non éthiques se produisent.

Premièrement, l’utilisation de mises en contexte réalistes, mais fictives diminue le risque que les participants ne dévoilent de l’information confidentielle appartenant à l’organisation ABC. Advenant le cas que ceci se produise, le participant n’avait qu’à le mentionner à la chercheure qui ferait abstraction totale de cette information lors de l’analyse.

Deuxièmement, bien que des données démographiques ont été recueillies sur le profil général des répondants, aucune d’entre elles n’a permis ensuite d’identifier les réponses d’un participant

lors des entrevues semi-dirigées. Les données ont également été agrégées, ce qui permet d'obtenir l'anonymat partiel pour les répondants, anonymat dans lequel le nom n'est pas cité, mais l'identité du participant pourrait être dévoilée si quelqu'un connaissait le terrain de recherche. Tous les participants ont été avertis de cette possibilité lors de la réception du formulaire de consentement de participation à l'étude et au début de l'entrevue.

Troisièmement, les données identificatoires contenues dans la documentation de l'organisation ABC n'ont pas été transposées dans ce mémoire et sont restées sur les sites sécurisés de l'organisation. Bien qu'il existe un conflit d'intérêts, car la chercheure est elle-même employée par l'organisation ABC, la chercheure a fait également abstraction de toute information qu'elle apprend dans le cadre de ses fonctions, mais qu'elle n'a pas le droit de divulguer.

Quatrièmement, aucune information n'a été relayée aux supérieurs hiérarchiques des participants afin que ceci n'affecte pas, entre autres, l'opinion d'autres employés de la compagnie sur les participants. Ceci inclut toute information obtenue dans le cadre de l'étude ou encore le refus d'un participant potentiel de participer à l'étude. De plus, les propos des participants sont présentés de façon anonyme dans le mémoire et ainsi les autres participants ne peuvent pas identifier les individus en fonction des réponses données lors de l'entrevue.

Finalement, la chercheure a conservé les données recueillies dans des fichiers chiffrés et sur des serveurs sécurisés de HEC Montréal et les détruira lorsqu'elles ne seront plus nécessaires à l'aide d'un logiciel de destruction des fichiers.

3.5 Conclusion

L'objectif de ce chapitre était de présenter et de justifier le choix de l'approche méthodologique qualitative de l'étude de cas pour valider le cadre conceptuel proposé au chapitre précédent. Premièrement, un questionnaire Qualtrics a été envoyé aux participants ayant accepté de participer à l'étude afin de récolter des données démographiques. Ensuite, des entrevues semi-dirigées ont été complétées avec ces mêmes participants pour obtenir leur perception sur le cadre conceptuel initialement conçu. En parallèle, de la documentation de l'organisation ABC a été consultée afin d'appuyer les propos recueillis lors des entrevues. Troisièmement, une retranscription des entrevues a été effectuée ainsi qu'une codification des propos afin de garder une trace des propos rapportés et de faciliter l'analyse. Suite à ceci, une analyse intra-répondant et une autre inter-répondants ont permis de consolider les données recueillies sur le terrain. Finalement, une comparaison a été effectuée avec ce qui a été trouvé initialement dans la littérature. Le prochain chapitre présentera les résultats obtenus lors de la collecte de données.

Chapitre 4. Analyse des résultats

Ce quatrième chapitre détaille les résultats de l'analyse de la collecte de données composée d'entrevues virtuelles avec 10 employés de l'organisation ABC et d'un survol de la documentation pertinente de l'organisation. L'analyse des résultats se concentre sur les éléments principaux permettant de répondre aux deux premiers objectifs de recherche de cette étude :

1. **Identifier les facteurs de succès d'une équipe ICIC interdisciplinaire et;**
2. **Identifier les rôles au sein d'une équipe ICIC interdisciplinaire et leurs responsabilités.**

Le chapitre est divisé en 4 sections. La première section présente le portrait global des participants, afin de placer en contexte l'expérience de chacun. Ensuite, la deuxième section détaille l'analyse de la perception des participants envers la pertinence de l'équipe ICIC interdisciplinaire, et si celle-ci favoriserait le succès d'une grande organisation. Puis, la troisième section énonce l'analyse de la perception des participants sur les facteurs de succès initialement ciblés, tandis que la quatrième section évoque plutôt leur perception sur les rôles initialement soulevés lors de la revue de la littérature.

4.1 Caractéristiques des participants

Cette section présente l'échantillon final rencontré, soit 10 participants. Tous les participants proviennent de l'organisation ABC, et des rencontres individuelles ont été effectuées auprès de chacun d'entre eux, à l'exception de deux participants qui ont été rencontrés ensemble. Les sous-sections qui suivent expliquent comment la protection de l'anonymat des participants a été effectuée tout au long de l'étude et présente le portrait global de leur expérience professionnelle.

4.1.1 Protection de l'anonymat

Afin de protéger l'anonymat des participants, des codes leur ont été attribués. Les codes P1 à P10 ont été utilisés pour lier les réponses inscrites dans le questionnaire Qualtrics aux bons

participants et pour ensuite codifier leurs propos lors de l'analyse. De plus, la communication par courriel a été effectuée de façon individuelle afin de ne pas exposer les noms des participants à d'autres employés de l'organisation ABC. Finalement, l'organisation ABC n'est pas nommée dans et les noms des départements dans lesquels travaillent les participants ont été modifiés afin d'illustrer les secteurs d'affaires qu'ils représentent. Ceci a été fait afin de préserver la confidentialité de l'organisation ABC et des propos rapportés par les participants.

La sous-section qui suit présente un portrait global des profils des participants. Les données présentées ont été agrégées et proviennent du questionnaire Qualtrics rempli par les participants. Dans le cadre de cette étude, 10 participants ont été rencontrés et chacun d'entre eux a envoyé son questionnaire.

4.1.2 Profils des participants

Le niveau d'expérience des participants de cette étude est d'une moyenne de 15.3 années d'expérience professionnelle. Le participant P7 est celui ayant le plus d'expérience soit 21 années, toutes chez ABC. Le nombre d'années d'expérience des participants en combinaison avec leur expérience en termes d'implication lors d'incidents de sécurité a permis d'enrichir les résultats de cette collecte. Cet élément représente un bon indice que les participants rencontrés ont, en moyenne, une bonne connaissance du sujet, car la moitié de ceux-ci ont participé à la résolution de plus de 50 incidents de sécurité chacun. Pour ce qui est des postes des participants, des postes de conseiller ont principalement été rencontrés. Parmi ceux-ci on dénote les postes de conseiller junior, conseiller senior et conseiller au chef d'équipe. Rencontrer ces trois différents postes a permis de récolter plusieurs opinions et d'ainsi diversifier les résultats. La dernière entrevue a été exécutée en groupe avec deux participants. Elle a été utilisée comme une triangulation des résultats obtenus des entrevues précédentes. L'analyse préliminaire des données collectées ayant déjà été débutée et le point de saturation théorique presque atteint, cette entrevue avec les deux participants a pu être utilisée comme une validation de ce qui avait été précédemment soulevé.

Le tableau 4.1 qui suit présente le profil des participants résumé ci-haut :

Tableau 4.1 Profil des participants

Éléments du profil	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Formation académique	Administration	Génie informatique	Administration	Administration	Criminologie	Cybersécurité des réseaux	Cybersécurité des réseaux	Administration	Génie informatique	Administration
Domaine de travail avant arrivée chez ABC	Consultation	Commerce au détail; Consultation	Consultation	Investissement	N/A*	N/A*	N/A*	Commerce au détail	N/A*	Consultation
Poste chez ABC	Conseiller au chef d'équipe	Conseiller junior	Responsable de produit**	Analyste d'affaires	Conseiller senior	Directeur	Champion en continuité des affaires	Conseiller junior	Analyste d'affaires	Chef d'équipe
Nom de la l'équipe	Menace interne	Surveillance en continu	Projets en sécurité	Analyse d'incidents	Gestion d'incidents	Gestion d'incidents	Gestion d'incidents	Transformation numérique	Gestion de risques	Surveillance en continu
Expérience en sécurité (années)	9	15	20	6	15	17	21	20	12	18
Nombre de **projets** interdisciplinaires	Entre 11 et 50	Entre 6 et 10 projets	Entre 6 et 10 projets	Entre 1 et 5 projets	Entre 11 et 50 projets	Entre 11 et 50 projets	Entre 11 et 50 projets	Entre 11 et 50 projets	Entre 1 et 5 projets	Entre 6 et 10 projets
Durée **moyenne** de ces projets	Plusieurs mois	Plusieurs mois	Entre une semaine et un mois	Entre une semaine et un mois	Entre une semaine et un mois	Plusieurs mois	Plusieurs mois	Plusieurs mois	Entre une semaine et un mois	Plusieurs mois
Nombre **d'incidents**	Entre 1 et 5	Plus de 50	Entre 6 et 10	Entre 1 et 5	Plus de 50	Plus de 50	Plus de 50	Entre 1 et 5	Entre 6 et 10	Plus de 50

* Ne s'applique pas
** Product Owner en anglais

La section suivante détaille la perception des participants sur la pertinence de l'équipe ICIC interdisciplinaire au sein d'une grande organisation comme ABC en regardant ses objectifs et l'impact qu'une telle équipe pourrait avoir.

4.2 L'équipe ICIC interdisciplinaire

Toutes les entrevues ont commencé avec la présentation de l'équipe ICIC interdisciplinaire aux participants. Ceux-ci ont commenté sa pertinence au sein d'une grande organisation, sans pour autant connaître plus de détails sur la structure de l'équipe (c.-à-d. les facteurs de succès et rôles qui ont été présentés ultérieurement). Les participants ont tous été convaincus de la pertinence de l'équipe ICIC interdisciplinaire dans un contexte d'une grande organisation comme celui de ABC, selon leur expérience professionnelle dans le domaine de la sécurité de l'information.

Le tableau 4.2 rapporte les aspects principaux soulevés par les participants sur la pertinence de l'équipe ICIC interdisciplinaire. Des explications détaillées des différents aspects sont placées à la suite du tableau.

Tableau 4.2 : Pertinence de l'équipe ICIC interdisciplinaire selon les participants

Aspect	Justification
Permanence de l'équipe	• Alignement des objectifs; • Constance dans le choix des indicateurs clés de performance; • Standardisation des processus de gestion d'incidents.
Jumelage des disciplines pertinentes à la gestion d'incidents	• Diminution des délais de gestion d'incidents; • Collaboration à travers les secteurs d'affaires.
Responsabilité du processus de gestion d'incidents	• Une équipe composée de généralistes de différentes disciplines; • Une attention placée sur la gestion et non sur la mise à jour continue de compétences techniques.

Présentement au sein d'ABC, plusieurs équipes de gestion d'incidents existent. Toutefois, ces équipes de gestion d'incidents ne sont pas des équipes interdisciplinaires. Selon les participants, cette structure actuelle amène une perte de temps notable dans la gestion d'incidents, un problème d'alignement des objectifs de travail et un désalignement dans l'utilisation de différents indicateurs afin de mesurer le succès et la performance de l'équipe. Les équipes collaborent lors d'un incident, mais ont leurs propres objectifs. De plus, selon P5, la volumétrie de travail en matière de gestion d'incidents est à considérer. En fait, son poste en tant que conseiller senior l'a fait participer à la résolution d'environ 3 à 5 incidents par mois dans les dernières années. Selon lui, le volume grandissant d'incidents en sécurité justifie une évolution dans la gestion de ceux-ci au sein des grandes organisations.

Lors de cette discussion initiale, les participants ont noté plusieurs avantages à la mise en place d'une équipe ICIC interdisciplinaire qui viendrait contrer les désavantages de la structure actuellement implantée. Premièrement, l'équipe serait une équipe dédiée qui développerait une expérience en gestion d'incidents, expérience favorisant le succès de l'organisation à ce niveau. L'aspect de permanence de cette équipe permet de standardiser les processus et des lignes directrices, comparativement à une équipe temporaire. La majorité des participants indique toutefois que l'équipe ICIC interdisciplinaire devrait être une équipe d'affaires, qui a un rôle de coordination, de standardisation d'outils et processus, et une capacité de relais entre les membres de l'équipe. Tel que rapporté par P5, un incident peut durer 4 jours, 18 heures par jour, ce qui nécessite une approche d'affaires dans laquelle une standardisation est implantée. L'équipe serait alors composée de généralistes en cybersécurité qui auraient l'autorité de demander la contribution de spécialistes de certains domaines (p.ex. rançongiciel ou encore menace interne) lorsqu'un incident particulier survient. Ceci, selon P6 et P7, permettrait de créer un lien fonctionnel entre les différents secteurs d'affaires de l'organisation.

Un défi est toutefois perçu par les participants par rapport à l'équipe ICIC interdisciplinaire, soit qu'avant la création de l'équipe ses différents membres ne viendraient pas de la même équipe. Le « chapeau organisationnel » (selon P1) serait alors différent pour tous, surtout dans un contexte d'une grande organisation comme ABC. Pour mitiger ce défi, le tiers des participants a

proposé de miser sur une gestion du changement en amont afin d'assurer que tous comprennent l'objectif principal de la nouvelle équipe dans laquelle ils font partie.

Finalement, les participants ont apporté une attention particulière sur les spécificités du domaine de la cybersécurité. En fait, 90% d'entre eux indiquaient que chaque incident a ses propres spécificités, qu'elles soient technologiques ou non, et qu'il serait très difficile de trouver une équipe permanente qui sera en mesure de répondre à toutes ces spécificités. Ainsi, la proposition soutenue par plusieurs fut de garder l'équipe ICIC interdisciplinaire comme point de contact pour les différents secteurs d'affaires de l'organisation lors d'un incident en cybersécurité. Cette équipe « contact » serait impliquée dans l'évolution des processus et mécanismes de protection de l'organisation. De plus, l'évolution du domaine de la cybersécurité augmente de façon exponentielle. Ceci compliquerait la tâche d'une équipe qui devrait être au courant de tous ces avancements, en plus de gérer les incidents de son organisation. L'équipe discutée devrait avoir comme seul objectif d'être porteuse du processus de gestion d'incidents, selon les participants. Plusieurs disciplines seraient ainsi présentes au sein de l'équipe ICIC interdisciplinaire, mais ces disciplines devraient avoir un angle d'affaires dans le domaine, comme par exemple celui de la gouvernance en sécurité.

Ces éléments, jumelés à l'ouverture initialement notable au sein d'ABC à l'équipe ICIC interdisciplinaire, justifieraient l'implantation d'une telle équipe. La section suivante présente l'analyse des résultats obtenus sur la pertinence des facteurs de succès préalablement identifiés.

4.3 Les facteurs de succès de l'équipe ICIC interdisciplinaire

Cette section analyse les résultats de la deuxième section de l'entrevue et de la documentation sur les objectifs et suivis au sein d'ABC. Elle permet de répondre au premier objectif de recherche de l'étude, soit l'identification des facteurs de succès d'une équipe ICIC interdisciplinaire. La section est divisée en deux sous-sections : (1) les facteurs de succès généraux à une équipe de travail et (2) les facteurs de succès spécifiques à une équipe ICIC interdisciplinaire.

4.3.1 Les facteurs de succès généraux à une équipe de travail

Cette première sous-section présente l'analyse des résultats concernant les facteurs d'alignement opérationnel, de communication efficiente, de coopération continue et de couverture complète des compétences de cybersécurité. Le tableau 4.3 illustre les éléments retenus au sein de cette catégorie qui seront ensuite détaillés sous chaque facteur de succès.

Tableau 4.3 : Les facteurs de succès généraux à une équipe de travail

Facteur de succès	Éléments retenus
Alignement opérationnel en accord avec les objectifs organisationnels	• Les objectifs organisationnels représentent le pourquoi et les objectifs d'équipes le comment; • Le succès du facteur passe par sa communication et son suivi.
Communication efficiente au sein de l'équipe	• Diminution des délais de traitement et l'impact d'un incident; • L'importance de savoir à qui communiquer, quand et comment.
Coopération continue au sein de l'équipe	• L'engagement au centre de la coopération; • Le recul favorise la coopération.
Couverture complète des compétences en cybersécurité	• Prioriser les éléments d'affaires lors de la gestion d'incidents; • Comprendre le processus avant de comprendre les moyens de l'exécuter.

4.3.1.1 Alignement opérationnel en accord avec les objectifs organisationnels

Ce premier facteur est jugé nécessaire dans le contexte étudié par tous les participants. Selon eux, les objectifs de l'équipe doivent découler des piliers stratégiques de l'organisation. Ces piliers sont des objectifs stratégiques pour toute l'organisation, peu importe le secteur d'affaires auquel appartient une équipe.

« Tes objectifs d'équipe doivent permettre d'expliquer le comment du pourquoi des objectifs stratégiques. » (P2)

Il doit y avoir un lien entre le niveau stratégique et le niveau opérationnel afin que tous comprennent les tâches qu'ils doivent accomplir dans leur quotidien pour participer favorablement à la gestion d'incidents. Par exemple, l'organisation ABC place la sécurité comme pilier stratégique ce qui devient une priorité pour toutes les équipes, entre autres celles d'affaires qui lui accordaient moins de ressources préalablement. Plusieurs projets peuvent alors être développés en fonction de cet objectif organisationnel. Les participants sont également d'avis que la communication des objectifs stratégiques initie l'alignement opérationnel. Cette communication doit provenir de l'exécutif qui la transmet aux équipes. La communication permet également l'évaluation de l'alignement, à travers des discussions à la mi-échéance ou à l'échéance des objectifs. Ceci permet de partager au sein de l'équipe ce qui a été bien fait et ce qui peut être amélioré en fonction des résultats attendus.

L'importance de cet alignement s'illustre dans la priorisation des actions à poser lors de la gestion d'un incident selon P10 :

« Si l'objectif principal de ton équipe ICIC interdisciplinaire c'est de protéger à tout prix l'actif informationnel de l'organisation ABC alors que l'objectif principal de ABC c'est de protéger l'actif informationnel de ses clients, il y a aura un enjeu dans la manière dont les incidents seront gérés et comment les équipes travaillent ensemble. »

Il y a donc un besoin d'alignement opérationnel qui doit se traduire par une compréhension des actions à poser au quotidien qui est communiquée par les bonnes personnes.

4.3.1.2 Communication efficiente au sein de l'équipe

Le deuxième facteur, la communication efficiente, est le facteur le plus apprécié par tous les participants. Plusieurs participants avancent que la communication permet de réduire les délais

et l'impact d'un incident, d'autres qu'elle permet à tous de comprendre l'objectif principal de l'équipe et d'établir la stratégie à suivre lors d'un incident. Ce facteur complète plusieurs éléments et influence directement le succès d'une équipe :

« Même si tu as la meilleure stratégie au monde, elle ne sera pas opérationnelle si les membres de l'équipe ne la connaissent pas. » (P9)

Quatre volets forment ce facteur suite à l'analyse des rencontres : qui, quand, quoi et comment. Premièrement, la communication de l'information doit uniquement être effectuée auprès des personnes autorisées : « Il faut protéger l'information, donc la communiquer selon le besoin et seulement si nécessaire. » (P1)

Ainsi, les éléments pertinents d'un incident doivent être rapportés aux personnes concernées uniquement. Un survol de la documentation d'ABC sur ce sujet a d'ailleurs permis de noter que ce principe est le fondement de toutes les exigences de sécurité de l'organisation. En effet, l'organisation met à l'avant ce principe en indiquant que l'information ne doit être communiquée qu'aux personnes autorisées, soit celles qui en ont besoin pour effectuer leurs tâches dans le cadre de leurs fonctions ou concernant un besoin d'affaires.

Deuxièmement, la communication est pertinente à tous moments lors d'un incident : lors de la préparation, pendant un incident, et en post-mortem. La documentation d'ABC indique que l'information doit être communiquée par les personnes désignées et en fonction des besoins de l'incident : « Ce n'est pas pendant l'incident que tu établis tes canaux de communications et la manière dont tu communiques, c'est quelque chose qui doit être fait en amont. » (P7)

Troisièmement, l'information communiquée doit être la bonne et doit être celle pertinente afin de permettre de répondre à un incident. Finalement, la façon dont la communication est effectuée est également un point revenant souvent auprès des participants. Chez ABC, cette communication est effectuée de plusieurs façons dont : le signalement à l'aide d'outils d'alerte,

la communication des objectifs de la part du coordonnateur au reste de l'équipe, les suivis pendant un incident lorsque nécessaire ou encore les pistes d'amélioration en post-mortem à un incident. L'organisation favorise les rencontres d'équipe, surtout en moment d'incident, pour que tout le monde soit au courant de l'incident et de son impact probable. Une importance particulière doit être accordée à la nature de l'information communiquée et au volume communiqué afin d'établir un équilibre. Dans certains cas, il est de la responsabilité d'un membre de l'équipe de s'assurer que l'information reste confidentielle (p.ex. en menace interne) ce qui fait en sorte que le choix de partage d'information devient beaucoup plus difficile. Ces quatre volets regroupés forment le facteur de la communication qui a ensuite une influence sur tous les autres facteurs de succès. En effet, selon tous les participants, aucun facteur de succès ne peut être mis en place si la communication efficiente n'est pas ancrée au sein de l'équipe ICIC interdisciplinaire, et ce entre autres dû à la sévérité des situations dont l'équipe traite.

4.3.1.3 Coopération continue au sein de l'équipe

Pour le troisième facteur, les participants s'entendent en unanimité qu'une équipe qui coopère est une équipe plus performante. L'engagement est, selon eux et selon la documentation soulevée, un élément primordial de la coopération. À noter qu'étant donné que les équipes actuelles chez ABC ne sont pas des équipes interdisciplinaires permanentes, l'importance du facteur de coopération et donc de la capacité de se relayer au sein de l'équipe est possiblement jugée supérieure par les participants qui parlent à partir de leur propre expérience. Étant donné l'importance donnée au facteur dans la littérature au sein d'équipes permanentes, l'influence de ce facteur sur le succès de l'équipe ICIC interdisciplinaire reste notable et a donc été prise en compte lors de l'analyse des résultats.

La gestion d'incidents apporte beaucoup d'anxiété et de travail, selon les participants, dû aux journées de travail pouvant durer jusqu'à 18 heures lors d'un incident majeur. L'engagement et la capacité de l'équipe de se relayer deviennent alors primordiaux dans une telle situation. Une décision prise lors de la première journée de gestion de l'incident pourrait être modifiée au jour 3 ce qui complique la tâche de coordination au sein de l'équipe.

« Des fois, quelqu'un va commencer à traiter l'incident pour les premières 12 heures et après quelqu'un d'autre embarque pour la suite, ils doivent être en mesure de bien communiquer et le transfert de responsabilité de l'incident doit être efficace. » (P9)

De plus, P2 soulève l'importance de la coopération dans une équipe interdisciplinaire qui regroupe plusieurs expertises. Les membres de l'équipe doivent être dissuadés de travailler en silos, ce qui peut avoir un grand impact sur la résolution de l'incident. Dans un incident de longue haleine, tous ont besoin de prendre du recul pour pas la suite mieux aider l'équipe. Ce recul favorise la coopération dans des moments clés, selon P8 :

« En avion, on te dit de mettre ton masque avant de le mettre à la personne à côté de toi. C'est le même principe en gestion d'incident. Tu as beau vouloir aider les autres membres de l'équipe, si tu es trop proche de l'incident tu ne seras pas en mesure d'évaluer toutes les avenues de sortie possibles. »

Plusieurs moyens peuvent être employés pour favoriser une coopération continue comme par exemple des événements virtuels, des activités, des attentions en temps de télétravail, etc. Au sein d'ABC, l'engagement des employés est entre autres mesuré à l'aide d'un sondage regroupant plusieurs catégories – relation avec le chef d'équipe, sentiment d'appartenance, croissance personnelle, relation avec les pairs et bien-être général de l'employé. Ces catégories tentent de mesurer un aspect important d'une équipe de travail, et ce sans se concentrer sur des mesures quantitatives.

4.3.1.4 Couverture complète des compétences en cybersécurité

Le dernier facteur de succès de cette première catégorie est celui des compétences de cybersécurité. Bien qu'elles soient pertinentes, elles ne représentent pas la voie que l'équipe étudiée devrait prendre selon les participants.

Les participants ont dénoté plusieurs avantages à avoir des compétences en cybersécurité au sein de l'équipe ICIC interdisciplinaire. Entre autres, les délais de réponse à l'incident seraient réduits si l'équipe de gestion d'incidents avait ces compétences. Ces délais seraient réduits, car l'équipe n'aurait alors pas besoin d'aller demander l'avis d'experts à l'extérieur de l'équipe. De plus, ces compétences permettent à l'équipe d'avoir une meilleure compréhension de l'incident qui se produit, ce qui leur permettrait de prendre des décisions plus efficaces. Par contre, une grande place accordée à des compétences plutôt techniques viendrait allonger certains délais. Ces délais seraient présents lors de communications avec des gestionnaires hors de l'équipe :

« Si on s'assoit à table et que je te demande de me résumer l'incident qui vient de se produire, que tu me parles de je ne sais pas trop quelle infrastructure ça ne va rien me dire. Plus tu emploies un langage technique, plus ça va être long avant de prendre une décision parce que tout le monde va vouloir comprendre ce qui vient de se dire. » (P6)

Étant donné le manque de pouvoir décisionnel perçu par les participants pour cette équipe ICIC interdisciplinaire, ceux-ci proposent en majorité que l'équipe ne devrait pas avoir un profil principalement de cybersécurité, mais un profil de compétences d'affaires. Un professionnel qui a des compétences techniques de cybersécurité en profondeur aura moins de compétences qui lui permettront de gérer un incident, soit principalement une prise en charge et une capacité à faire des liens entre certains concepts. De plus, pour continuellement apporter de la valeur à son équipe, le professionnel technique devra toujours être à l'affût des dernières nouvelles :

« Les compétences techniques tu ne pourras jamais toutes les avoir pour couvrir tous les types d'incidents possibles : tu devras te spécialiser en continu et en cybersécurité il y a une vitesse d'évolution exponentielle qui est dure à suivre. » (P8)

Selon les participants, l'équipe devrait être porteuse de la gestion d'incidents et doit déterminer de quels experts du reste de l'organisation elle a besoin en fonction du type d'incident à gérer. L'équipe devient une équipe généraliste qui se fait appuyer dans sa réflexion par des experts qui

eux seront spécialistes. Par exemple, P5 a mentionné que les compétences spécifiques nécessaires pour répondre à un rançongiciel ne seront pas les mêmes que lorsqu'un employé gagne accès aux systèmes de l'organisation.

Ainsi, l'analyse de cette première catégorie a soulevé principalement la place qui devrait être accordée à la standardisation des méthodes de travail afin de placer l'emphase sur les éléments humains qui favoriseront la résolution d'incidents de sécurité de façon efficace. La sous-section qui suit complète l'analyse des facteurs de succès avec la deuxième catégorie.

4.3.2 Les facteurs de succès spécifiques à une équipe ICIC interdisciplinaire

Cette deuxième sous-section présente maintenant l'analyse des résultats des facteurs d'adaptabilité efficace, de détection de menaces en continu et de reprise rapide des activités. Le tableau 4.4 présente les éléments retenus au sein de cette catégorie.

Tableau 4.4 : Les facteurs de succès spécifiques à une équipe ICIC interdisciplinaire

Facteur de succès	Éléments retenus
Adaptabilité efficace face aux cybermenaces	• L'accès aux projets, les méthodes de travail et les mécanismes de contrôle pour atteindre l'adaptabilité; • La place de l'adaptabilité dans le comportement humain.
Détection de menaces en continu	• L'importance d'intégrer la surveillance à la détection; • Vérifier constamment ce qui a été implanté auparavant.
Reprise rapide des activités	• Tester la reprise rapide des activités à l'aide d'un plan; • Évaluer suite à un incident ce qui a moins bien été.

4.3.2.1 Adaptabilité efficace face aux cybermenaces

Pour débuter cette deuxième catégorie, tous les participants ont placé l'emphase sur l'adaptabilité pour le succès de l'équipe ICIC interdisciplinaire.

D'un côté, certains participants voient ce facteur plutôt comme un synonyme d'anticipation soit prévoir un événement d'affaires ou de sécurité. La majorité d'entre eux adoptait plutôt la définition que l'adaptabilité est « l'étude et la compréhension des vulnérabilités qui nous entourent, que ce soit à l'interne ou à l'externe de l'organisation » (P4). Les participants misaient également sur l'importance d'étudier l'environnement externe et l'environnement interne. L'importance de la compréhension de l'environnement externe pousse la compréhension des événements de sécurité ou d'affaires soulevés dans d'autres organisations afin de ne pas reproduire les erreurs alors commises. La compréhension de l'environnement interne elle permet, entre autres, de comprendre l'état de l'environnement applicatif (qu'il soit de sécurité ou d'affaires) de l'organisation.

Pour que l'adaptabilité soit efficace au sein d'une équipe ICIC interdisciplinaire, plusieurs moyens peuvent être utilisés dont : l'accès aux projets, les méthodes de travail et les mécanismes de contrôle. Premièrement, l'accès aux projets permet d'explorer la compréhension de l'environnement, tant interne qu'externe. Cette accessibilité aux projets est faite conjointement avec l'accès aux ressources financières. Ensuite, les méthodes et outils de travail, comme par exemple un plan d'action lors d'un incident, doivent pouvoir être adaptés lorsque nécessaire en fonction du type d'incident. Comme le soulèvent les participants, un plan doit pouvoir être modifié en fonction de ce qui se produit au moment de l'incident. Dans une équipe ICIC interdisciplinaire, cette adaptation du plan prend tout son sens lorsque les membres provenant de différentes disciplines n'ont pas tous le même manuel de stratégie initiale (*playbook* en anglais). Puis, les mécanismes de contrôle doivent également pouvoir être adaptés pour permettre « d'évaluer en temps réel la capacité et l'efficacité de ce qui a été mis en place et d'assurer une certaine flexibilité qui est une condition absolue au succès » (P6). Ceci peut se traduire lors de vigies effectuées par l'équipe, dans laquelle une surveillance accrue est placée sur l'environnement de l'organisation.

La dissonance des réponses réside toutefois majoritairement dans la place accordée à l'impact du comportement des membres de l'équipe. Plus précisément, plusieurs avancent que l'adaptabilité se traduit par la flexibilité des membres de l'équipe afin de faire face à des situations ambiguës, inconnues ou encore imprévues. Dans l'organisation ABC, la façon dont les équipes fonctionnent présentement en cas d'incident justifie ce point. Une équipe de gestion d'incidents comprend plusieurs coordonnateurs qui, chacun leur tour, doivent gérer un incident en fonction de leurs compétences et de leur expérience :

« Si un de mes coordonnateurs ne démontre pas qu'il est en mesure de s'adapter, je vais avoir peur que les incidents qui sont gérés par cette personne soient gérés de manière plus rigide et que des angles d'attaque ne soient pas évalués. » (P5)

Cette dissonance ne réduit pas l'impact que peut avoir l'adaptabilité sur la gestion d'un incident, mais vient plutôt questionner si ce facteur en est un d'équipe.

4.3.2.2 Détection de menaces en continu

Pour le facteur de détection de menaces en continu, il y a eu un consensus clair de sa pertinence. Cette détection en continu permet d'être constamment à l'affût des changements qui peuvent survenir, d'anticiper ce qui peut se produire et d'évaluer des cas de figure (P1). Cette détection permet ainsi d'identifier les signes avant-coureurs ou encore tout élément déclencheur avant qu'un incident se produise.

Un élément central de ce facteur est l'analyse qu'il est possible d'effectuer suite à cette détection. Par analyse, les participants avançaient le point suivant : une identification de l'incident principal qui est ensuite décortiqué en plusieurs parties (qui, quoi, quand, comment). Cette décortication permet possiblement d'anticiper certains éléments à l'avenir. Ainsi, l'équipe pourra rester informée de ce qui se produit dans son environnement et développer une expérience plus précise sur certains types de menaces.

Selon les participants par contre, une attention particulière doit être accordée à la surveillance des menaces :

« Tu ne détectes pas si tu ne surveilles pas, puis tu ne détectes pas si tu ne sais pas quoi surveiller. » (P5)

Cette surveillance doit être précisément par rapport à ce qui a été implanté d'un côté par l'équipe et d'un autre côté par d'autres équipes au sein de l'organisation.

« Si je mets un outil de sécurité pour assurer de détecter un rançongiciel possible, mais je ne surveille pas cet outil, je ne m'assure pas qu'il travaille comme il faut. Si je crois que seulement en le mettant en place il va fonctionner comme il faut, il ne fonctionnera pas. » (P2)

Ce principe de confiance à ce qui a été implanté, mais de continuer tout de même de vérifier les outils et méthodes de travail est reconnu par la majorité des participants. C'est la combinaison de la détection et de la surveillance qui rend possible la compréhension de la situation. Les participants soutiennent qu'une étape ne peut pas être plus importante qu'une autre en gestion d'incident. Le plus important selon eux est de gérer de manière la plus efficace possible l'incident afin de recommencer à effectuer les activités de l'organisation.

4.3.2.3 Reprise rapide des activités

Pour le dernier facteur de succès présenté, les participants lui voient une pertinence extrêmement grande. Cette pertinence s'illustre selon eux à chaque étape de la gestion d'incident, et une reprise rapide des activités n'est pas possible si un travail n'est pas effectué en amont. Une planification de cette reprise doit être effectuée et préalablement testée. De plus, des améliorations doivent être mises en place sur cette planification suite à la reprise des activités :

« Tu ne veux jamais te faire frapper deux fois par la même situation dont tu aurais pu te protéger, c'est inacceptable. » (P2)

Ainsi, avant d'arriver à la reprise des activités, les participants énoncent qu'un arrimage opérationnel doit être effectué entre tous les acteurs pour qu'ils comprennent leur rôle respectif dans la gestion de tout incident. Toutefois, ce plan est un plan comprenant certaines lignes directrices. L'expérience est un élément très important à considérer : avoir une équipe habituée à gérer des incidents et être capable d'effectuer une prise en charge rapidement. Il y a une priorisation qui doit être faite lors de l'incident qui ne peut être planifiée, à savoir si l'objectif est de régler l'incident le plus rapidement possible ou encore par exemple de la manière la moins coûteuse possible.

Chez ABC, l'objectif d'une telle équipe serait clair pour tous les participants :

« Je verrais mal nos clients attendre après nous pendant une semaine parce qu'on n'a pas été en mesure de se relever lorsqu'on a comme objectif que dans les 12 heures suivant un incident on veut continuer nos activités. » (P3)

Finalement, en post-mortem, des informations doivent être disponibles sur entre autres, combien de temps l'équipe a eu besoin pour régler l'incident, quels ont été les défis et quelles pistes d'amélioration sont maintenant possibles.

En conclusion, cette troisième section du chapitre a détaillé l'analyse des différents facteurs de succès présentés aux participants. De cette section on peut identifier l'importance de prioriser quelle information est transmise, de comprendre le processus de gestion d'incidents et de placer à un pied d'égalité les activités principales de ce processus. La section suivante détaille l'analyse de la dernière partie de l'entrevue, soit celle des rôles au sein d'une équipe ICIC interdisciplinaire.

4.4 Les rôles au sein de l'équipe ICIC interdisciplinaire

Lors des entrevues, les discussions ont également porté sur les 6 rôles les plus souvent soulevés dans la littérature au sein d'une équipe de gestion d'incidents et d'une équipe interdisciplinaire. La perception des participants a alors été demandée afin d'évaluer si, premièrement, ces rôles étaient pertinents et, deuxièmement, s'ils l'étaient dans une équipe interdisciplinaire. La section précédente, sur les facteurs de succès, a également permis d'alimenter l'analyse de cette section-ci. Le tableau 4.5 soulève les principaux éléments retenus pour chacun des rôles. Les sous-sections qui suivent le tableau détaillent ces éléments.

Tableau 4.5 : Les rôles dans une équipe ICIC interdisciplinaire

Rôle	Éléments retenus
Agent de changement	• Le rôle a une plus grande utilité en amont d'un incident que pendant; • Délimiter les frontières du rôle afin de supporter les autres rôles.
Agent de liaison	• Remonter les besoins organisationnels au bon moment; • Déterminer combien d'information doit être partagée.
Conseiller	• Une nécessité de proactivité qui n'est pas assez présente; • Adopter des compétences d'affaires avant les compétences techniques.
Coordonnateur	• L'importance de se relayer pour mieux gérer des incidents; • Apporter un sentiment de sécurité en se concentrant sur les compétences qui apporteront le plus de valeur.
Gardien de l'information	• Un rôle qui devrait être moins technique;

	• Minimiser les croisements d'information en ciblant préalablement les exigences.
Innovateur	• Pousser la créativité de toute l'équipe à l'aide d'un seul rôle; • Naviguer les différents angles d'une seule situation pour optimiser le processus de création.

4.4.1 Agent de changement

Pour ce premier rôle, la majorité des participants voyaient sa pertinence dans une équipe composée de plusieurs disciplines. Toutefois, plusieurs se questionnent sur l'utilité de ce rôle lors d'un incident, et le verraient plutôt en amont ou en aval lorsqu'il n'y a pas de crise à gérer. Cet élément a été soulevé, car lors d'un incident il n'y aura pas de grands changements (organisationnels, dans les méthodes de travail) et ce rôle n'aurait alors pas nécessairement de valeur ajoutée lors de temps de crise.

Toutefois, les participants P1, P3, P7, P8 et P10 ont tous vu l'utilité de ce rôle dans une équipe ICIC interdisciplinaire en amont :

« Plus tu prends ta gestion de changement en amont et plus tu lui fais de la place au sein d'une équipe, plus tu auras du succès dans tes projets et en temps de crise. » (P3)

De plus, étant donné l'interdisciplinarité au sein de l'équipe, les participants ont indiqué qu'un rôle plaçant l'humain en priorité est ce qui permettra à une équipe de concentrer ses ressources et d'avoir du succès. L'agent de changement au sein de l'équipe pourrait avoir un rôle plus précis, par exemple faire un résumé des grandes nouvelles communiquées sur le portail des employés chaque mois. Cette personne s'assurerait ainsi d'aller chercher les réponses aux questions des membres de l'équipe par la suite, laissant l'équipe se concentrer sur les incidents. Il existerait alors une séparation entre le rôle du gestionnaire qui se concentrerait plutôt sur les grands changements organisationnels et l'agent de changement qui lui se concentrerait sur les grandes

nouvelles concernant les modifications dans les méthodes de travail ou encore les nouveaux outils technologiques mis de l'avant par l'organisation. C'est entre autres la communication efficiente de ces éléments qui permet de supporter le rôle de l'agent de changement.

4.4.2 Agent de liaison

Les participants ont indiqué en consensus que le rôle de l'agent de liaison est primordial pour une équipe interdisciplinaire gérant des incidents.

Une équipe qui gère des incidents doit être en mesure de remonter des besoins organisationnels en fonction de ce qui est évalué lors d'un incident. Un agent de liaison ancré au sein de l'équipe ICIC interdisciplinaire doit être celui qui remonte ce qui manque au sein de l'organisation suite à des lacunes lors de la gestion d'incident, lacunes soulevées par l'équipe. L'esprit de coopération doit alors être ancré au sein de l'équipe, sans quoi certaines lacunes pourraient ne pas être identifiées. L'agent de liaison sera ensuite celui effectuant la reddition aux gestionnaires à l'externe de l'équipe.

Les participants, en majorité, ont indiqué ces éléments comme ceux qui devant être rapportés par ce rôle afin d'alimenter le succès de l'équipe et ainsi le succès de l'organisation :

- Nombre total d'incidents dans le dernier mois;
- Catégorisation des incidents en fonction du sujet;
- Résumé des gestes posés par l'équipe durant ces incidents;
- Éléments (techniques ou non) mal compris par l'équipe durant ces incidents

« Chaque incident va générer des plans d'action et quand tu regardes le portrait global de tes menaces et de comment tu as été attaqué, tu seras capable de déterminer ce qui t'a fait le plus mal. Ensuite tu peux te poser la question suivante : Qu'est-ce que je peux faire en tant qu'organisation pour me protéger davantage contre ce type d'incident ? » (P5)

Finalement, le rôle de l'agent de liaison devrait aussi inclure combien et à quel moment remonter l'information. En temps de gestion de crise, une partie de l'information doit peut-être être directement remontée, car l'équipe a besoin de ressources immédiates pour gérer l'incident dont elle n'a pas le pouvoir d'obtenir. À d'autres moments, l'équipe a peut-être plutôt besoin de remonter des besoins suite à un incident. L'agent de liaison est celui qui va faire ce choix.

4.4.3 Conseiller

Le rôle du conseiller est, selon les participants et la documentation d'ABC consultée, un rôle moins pertinent que les autres rôles. Bien qu'un conseiller en théorie soit quelqu'un qui peut avoir une vision 360 sur les projets qui se déroulent au sein de l'équipe, les participants ont déterminé que ce rôle serait trop difficile à combler de façon continue. Premièrement, le rôle n'est pas assez proactif pour certains participants. Deuxièmement, lorsque l'équipe a une question spécifique, elle pourrait alors chercher l'information à l'extérieur de l'équipe, auprès de ressources présélectionnées. Ceci est dû au fait qu'une seule personne ne pourra pas tout savoir sur la cybersécurité, car le domaine est très grand et diversifié :

« Si on a besoin d'aide pour un sujet en particulier, on va s'assoir avec toute une équipe qui a l'expertise sur le sujet. Ce n'est pas une personne qui va nous dire quoi faire ou comment se défendre face à l'incident. » (P4)

Les participants n'étaient pas fermés à la possibilité qu'une personne ayant toutes les connaissances en cybersécurité existe, par contre l'opinion généralisée est que ce type de profil est rare. De plus, quelqu'un ayant beaucoup de connaissances sur un domaine (dans ce cas, la cybersécurité) aura probablement moins de connaissances spécifiques sur un sujet en particulier du domaine, comparativement à un expert du sujet en question. Un lien a alors été créé par les participants qui rappelaient l'importance d'un profil plutôt d'affaires, comme ce qui a été mentionné pour le facteur de succès des compétences en cybersécurité.

4.4.4 Coordonnateur

Le rôle le plus pertinent soulevé lors des différentes entrevues est celui du coordonnateur. Tous les participants ont indiqué que ce rôle fera la différence dans le succès de l'équipe, et ce peu importe la structure de l'équipe. C'est un rôle d'action et de proactivité, ce qui attire beaucoup les participants dans le cadre d'une gestion d'incident où il faut planifier et déléguer.

Les participants indiquent d'ailleurs qu'un système de rotation pourrait être mis en place. Coordonner des incidents peut être très drainant pour la majorité des gens, comme l'ont fait remarquer les participants. Drainant, car premièrement la personne doit gérer toutes les actions posées, mais doit également tout documenter (communications, post-mortem, actions posées, etc.) ce qui peut représenter beaucoup de tâches administratives. Les coordonnateurs ont tous différentes expertises, surtout dans le cadre d'une équipe interdisciplinaire :

« Des fois tu vas avoir certains types d'incidents puis tu vas décider de les donner au Coordonnateur X ou au Coordonnateur Y. Ils peuvent aussi s'entraider si certains sont moins familiers avec un type d'incident : tu peux aller chercher non seulement les connaissances, mais aussi l'expérience de tes collègues pour maximiser ton rôle de coordonnateur. » (P9)

Finalement, la personne qui joue le rôle du coordonnateur n'a pas besoin d'avoir toutes les connaissances spécifiques sur n'importe quel sujet en cybersécurité, mais doit plutôt avoir des compétences de gestion qui lui permettront de gérer le processus de prise en contrôle d'incident. Ceci est représenté par l'expérience de P8 :

« Je suis sur un incident en ce moment et il me parle de plein d'éléments techniques que je ne connais pas, mais le but c'est d'être capable de les aider à structurer leurs actions, de monter des échéanciers et de faire des suivis après que cette structure est organisée. »

En bref, ce rôle amène un aspect de sécurité à l'équipe qui doit gérer l'incident dû aux compétences qu'a l'employé, et ce en fonction des objectifs de l'équipe.

4.4.5 Gardien de l'information

De façon générale, le rôle de gardien a été reconnu comme pertinent par la majorité des participants, bien que la définition initiale semble adopter un angle trop technique pour certains. Le rôle devrait plutôt être un rôle de définition d'exigences lors d'un incident : soit quelle personne devrait avoir accès à quel genre d'information. Selon eux, le rôle ne devrait pas être technique, car cette expertise devrait être cherchée à l'extérieur de l'équipe lors d'un incident. De plus, ce ne sont pas tous les incidents qui sont des incidents de gestion d'accès, bien que ce sujet revienne souvent. Ainsi, le rôle devrait en être un plus généraliste dans lequel les exigences d'accès à l'information devraient être révisées. Le choix des outils ne devrait pas être l'élément retenant alors le plus l'attention des membres de l'équipe.

« On doit s'assurer que c'est les bonnes personnes qui ont accès à la bonne information, que ce sont les bonnes personnes qui collaborent avec l'équipe. Quand on arrive à un niveau de sensibilité plus élevé, on doit alors rapetisser le groupe en fonction de l'information qui est partagée. » (P5)

Ce rôle, selon les participants, permettrait d'avoir moins de croisement d'informations entre des individus qui ne devraient pas avoir accès à un certain type d'information, car ils n'en ont pas besoin dans le cadre de leurs fonctions

4.4.6 Innovateur

Les participants ont vu un grand intérêt au rôle d'innovateur. Premièrement, cela mettrait à l'avant un processus beaucoup plus créatif selon eux. Le rôle permettrait de s'arrêter et de se questionner sur ce qui est fait par l'équipe dans le cadre d'un incident. Ce questionnement permettrait donc de proposer des nouvelles façons de faire qui seraient plus efficientes pour l'équipe. L'équipe pourra alors travailler sur des pistes d'amélioration en fonction des commentaires en question. Deuxièmement, ce rôle est un rôle qui analyse tous les angles d'une situation. Dans une situation de crise, les acteurs font souvent ce qu'ils sont habitués à faire afin

d'agir le plus rapidement possible et de régler l'incident. Toutefois, d'après les participants c'est un rôle pertinent pour limiter les dégâts par la pensée critique et l'analyse. Troisièmement, la personne ayant ce rôle pourrait venir directement travailler avec le gestionnaire afin de revisiter les méthodes de travail de l'équipe. Selon P10, l'innovateur pourrait prendre un processus manuel et proposer de le rendre plus dynamique. Par exemple, si la stratégie de l'équipe est documentée de manière manuelle dans des documents, elle pourrait être transposée dans une application qui permet de rendre l'évolution de cette stratégie interactive.

Ainsi, ce rôle permet en bref de se poser des questions sur la manière dont l'équipe travaille, sur si d'autres solutions pourraient être envisageables, que ce soit au niveau des méthodes de travail ou des outils de travail. De plus, ce rôle aurait une grande place lors des post-mortem d'incidents, selon les participants. Ceci placerait l'amélioration continue des pratiques de travail au centre de l'intérêt des membres de l'équipe ICIC interdisciplinaire.

4.5 Conclusion

Ce quatrième chapitre a analysé les résultats obtenus lors de la collecte de données à l'aide d'entrevues semi-dirigées et de la consultation de documentation de politiques organisationnelles au sein de l'organisation ABC. Cette analyse a été divisée en trois sections : (1) la pertinence de la présence de l'équipe ICIC interdisciplinaire, (2) les facteurs clés de succès et (3) les rôles au sein de l'équipe ICIC interdisciplinaire. Premièrement, l'analyse de la pertinence de l'équipe a soulevé plusieurs points tels qu'une standardisation des processus de gestion d'incidents et une meilleure collaboration à travers les secteurs d'affaires. Deuxièmement, l'analyse des facteurs clés de succès a été divisée en deux parties, les facteurs de la catégorie générale et ceux de la catégorie spécifique. L'analyse des facteurs a entre autres soulevé le point d'une nécessité de compréhension du processus avant de comprendre les moyens d'exécuter ce dernier. Finalement, l'analyse des données collectées sur les rôles a elle détaillé parmi d'autres éléments que les aspects et compétences d'affaires doivent être adoptés avant ceux techniques. Le prochain chapitre discute de cette analyse en profondeur, à l'aide de différents axes de discussion.

Chapitre 5. Discussion

Ce cinquième chapitre se base sur l'analyse de la collecte des données du chapitre précédent afin de discuter des nuances que cette analyse apporte à la littérature sur la composition des équipes interdisciplinaires en cybersécurité. L'objectif de ce chapitre est de proposer des réponses aux objectifs de cette étude :

1- **Identifier les facteurs de succès d'une équipe ICIC interdisciplinaire et ;**
2- **Identifier les rôles au sein d'une équipe ICIC interdisciplinaire et leurs responsabilités.**

Ces deux objectifs sont répondus à l'aide des nuances et du consensus entre la littérature et la pratique. Le chapitre est divisé en trois sections. La première section répond au premier objectif de recherche, tandis que la deuxième section au deuxième objectif de recherche. Puis, la troisième section complète ces réponses aux objectifs de recherche en développant la discussion sur quatre axes distincts :

1- L'impact de la culture organisationnelle sur le quotidien de l'équipe ;
2- Une dynamique d'équipe qui s'inscrit dans la proactivité ;
3- L'interdépendance des rôles pour une meilleure performance d'équipe et ;
4- Les différents volets de la communication comme fondation à l'organisation de l'équipe.

Les réponses de ces deux objectifs en plus des axes de discussion permettent la présentation de propositions pour les chercheurs ainsi que pour les gestionnaires sur le sujet des équipes ICIC interdisciplinaires, propositions présentées tout au long de ce chapitre.

5.1 Facteurs de succès au sein d'une équipe ICIC interdisciplinaire

Le premier objectif de recherche de cette étude est celui de l'identification des facteurs de succès d'une équipe ICIC interdisciplinaire. Le tableau 5.1 résume cet objectif de recherche, l'explication de celui-ci est détaillée dans les paragraphes suivants.

Tableau 5.1 : Identification des facteurs de succès d'une équipe ICIC interdisciplinaire

Identification des facteurs clés de succès	Conservé sans modification	Conservé avec modification	Délaissé
Adaptabilité efficace	X		
Alignement opérationnel	X		
Communication efficiente	X		
Coopération continue	X		
Couverture complète des compétences en cybersécurité		Couverture complète des compétences humaines	
Détection de menaces en continu		Contrôle efficace des menaces inconnues	
Reprise rapide des activités		Réalisation efficiente des phases d'incident (avant, pendant et après l'incident)	

Suite à l'analyse de la cueillette des données, un consensus existe entre la littérature et la pratique sur certains facteurs de succès présentés dans cette étude. **En effet, les facteurs de (1) alignement opérationnel en accord avec les objectifs organisationnels, (2) communication efficiente au sein de l'équipe, (3) coopération continue au sein de l'équipe et (4) adaptabilité efficace face aux cybermenaces ont tous été confirmés.** Les trois autres facteurs de succès initialement présentés, soit (5) couverture complète des compétences en cybersécurité, (6) détection de menaces en continu et (7) reprise rapide des activités, comportent eux des précisions face à ce qui avait été initialement décelé dans la littérature.

Premièrement, l'analyse sur le terrain a permis de recentrer le facteur de couverture complète des compétences en cybersécurité sur le mandat attribué à l'équipe ICIC interdisciplinaire. De ce fait, étant donné la description de cette équipe donnée au deuxième chapitre qui évoque que l'équipe en est une de gestion d'incidents et la confirmation reçue des participants sur leur perception du mandat que l'équipe devrait avoir soit celui de la gestion d'incidents, les compétences de cybersécurité ici évoquées adoptent un angle trop technique. La collecte a permis de recentrer la portée de l'équipe, à celle d'une équipe de gestion de processus. **Ainsi, le critère de compétences de cybersécurité est remplacé par celui de compétences humaines** (p.ex. des habiletés à déléguer ou à s'entraider). Ces compétences permettront d'améliorer le succès de l'équipe en gestion de processus. Les compétences techniques de cybersécurité seront soutenues par les équipes spécialistes au sein de l'organisation (p.ex. équipe SOC) qui seront arrimées avec l'équipe ICIC interdisciplinaire qui elle pourra viser le processus de gestion d'incident.

Deuxièmement, bien que la détection de menaces en continu ne soit pas un facteur exclu dans la liste finale, à la détection vient s'ajouter le principe de surveillance. Afin de jumeler ces deux concepts, un nouveau facteur a été nommé, le facteur du contrôle efficace des menaces inconnues. Ce nouveau facteur inclut ainsi celui de la détection et celui de la surveillance des menaces qui ont été jumelés, car ce sont deux activités de contrôle. Aucune priorité n'est donnée à ces deux concepts, car les deux doivent être complétés en continu comme cela a été soulevé lors de la collecte. Les regrouper sous un seul facteur permet de faire confiance aux contrôles mis en place tout en vérifiant continuellement la posture de sécurité de l'organisation.

Troisièmement, une modification similaire au facteur de détection de menaces en continu est faite à celui de la reprise rapide des activités. **La reprise rapide des activités est jumelée à la planification de la gestion d'incident et l'évaluation de la prise en charge de l'incident en post-mortem. Le facteur découlant de ce jumelage est le facteur de réalisation efficiente des phases d'incident.** En effet, le processus de gestion d'incidents inclue plusieurs phases (avant, pendant,

après) et ce facteur permet maintenant d'intégrer toutes ces phases au cadre conceptuel. Initialement, la littérature plaçait beaucoup d'emphase sur le « pendant » ce pour quoi ce facteur fut celui retenu. Lors de la collecte, il a été toutefois dénoté qu'une phase ne doit pas avoir un impact plus grand qu'une autre dans le processus de gestion des incidents. Ainsi, une des propositions de ce mémoire est qu'une importance égale soit accordée à l'ensemble des phases du processus de gestion d'incidents lors du choix de la composition de l'équipe ICIC interdisciplinaire. Ce facteur de succès permet de placer cet élément à l'avant-plan et d'ensuite le découper dans ces différentes phases.

Donc, pour répondre au premier objectif de recherche de cette étude, les facteurs clés de succès retenus sont : (1) alignement opérationnel en accord avec les objectifs organisationnels, (2) communication efficiente au sein de l'équipe, (3) coopération continue au sein de l'équipe, (4) adaptabilité efficace face aux cybermenaces, (5) couverture complète des compétences humaines, (6) contrôle efficace des menaces inconnues et (7) réalisation efficiente des phases d'incident.

La sous-section suivante répond au deuxième objectif de recherche, l'identification des rôles au sein d'une équipe ICIC interdisciplinaire.

5.2 Rôles au sein d'une équipe ICIC interdisciplinaire

Pour répondre à ce deuxième objectif, le tableau 5.2 présente sommairement les rôles retenus puis leur explication est détaillée dans les paragraphes qui suivent.

Tableau 5.2 : Identification des rôles d'une équipe ICIC interdisciplinaire

Identification des rôles	Conservé sans modification	Conservé avec modification	Délaissé
Agent de changement	X		
Agent de liaison	X		
Conseiller			X
Coordonnateur	X		
Gardien de l'information		Définir les exigences de sécurité et non les implanter	
Innovateur	X		

Des six rôles soulevés initialement, ceux de : (1) l'agent de changement, (2) l'agent de liaison, (3) le coordonnateur et (4) l'innovateur ont tous été adoptés. À noter qu'une précision a été apportée quant au moment de l'implication de ces rôles soit en amont pour l'agent de changement, pendant un incident pour le coordonnateur et en aval pour l'agent de liaison et l'innovateur. Bien que leur implication devrait être plus élevée lors de ces moments, ces rôles peuvent toujours aider le succès de l'équipe. Ceci surtout en considérant l'importance donnée à la communication et à la coopération qui sont primordiales pour l'équipe ICIC interdisciplinaire. De plus, le rôle du conseiller a été délaissé et celui du gardien de l'information a quant à lui été modifié.

Pour ce qui est du conseiller, le choix était entre délaisser totalement le rôle ou plutôt proposer de réévaluer sa portée au sein de l'équipe ICIC interdisciplinaire. Finalement, le rôle est délaissé, car il est plutôt le rôle d'un spécialiste. Étant donné qu'il a été déterminé que cette

équipe ICIC interdisciplinaire devrait plutôt être porteuse du processus de gestion d'incident et non spécialiste des angles de cybersécurité, le rôle perd alors son sens au sein de l'équipe. La proposition est donc de concentrer les ressources de l'équipe sur des rôles qui lui permettent de gérer le processus et de s'arrimer ensuite avec des équipes qui sont composées de conseillers plus spécialisés. De plus, le rôle du coordonnateur agit dans la même lignée que celui d'un conseiller en gestion d'incident. Le rôle du coordonnateur est donc suffisant et ne doit pas être dédoublé dans celui du conseiller également.

Finalement, une modification est apportée au rôle du gardien de l'information. Initialement, ce rôle adoptait un angle plus technique en évaluant les outils utilisés par les membres de l'équipe ICIC interdisciplinaire en plus de gérer de façon opérationnelle les accès aux systèmes de l'organisation. Suite à l'analyse, ce rôle doit, dans le même ordre d'idée que le facteur de compétences en cybersécurité, plutôt se concentrer sur l'angle humain. **Pour ce faire, le gardien de l'information conserve son titre, mais a plutôt comme mandat de définir les exigences de sécurité sur l'accès à un type d'information (p.ex. en quoi consiste un compte à hauts privilèges).** Ce rôle, de par son mandat, rend possible l'harmonisation des termes utilisés au sein de l'organisation sur la gestion de l'information.

Les sections 5.1 et 5.2 ont répondu sommairement aux deux objectifs de recherche initialement établis. Toutefois, des nuances et précisions doivent être apportées sur ce que le contexte de l'étude a permis de soulever. Ces précisions sont développées dans la prochaine section.

5.3 L'influence du contexte organisationnel sur les facteurs de succès, les rôles et les responsabilités identifiés

Dans cette troisième section, quatre axes de discussion sont soulevés et développés. Cette section permet de bonifier les réponses données pour les deux premiers objectifs de recherche. L'approche méthodologique choisie, l'étude de cas, peut influencer ces réponses en raison de la place qui est accordée à certains éléments, propres à l'organisation ABC. Cette section présente donc quatre axes de discussion et les nuances qu'ils apportent pour compléter les propositions de l'étude. Ces quatre axes ont émergé lors de la collecte des données, spécifiquement lors des entrevues avec les participants.

5.3.1 Impact des valeurs organisationnelles dans le quotidien de l'équipe

Le premier axe de discussion de cette section est l'impact des valeurs favorisées par l'organisation dans le quotidien de l'équipe.

La communication efficiente, qui prenait beaucoup de place au sein des discussions avec les participants, permet d'établir un lien entre ces différentes valeurs. Ce lien est celui qu'afin de bien intégrer les valeurs favorisées par l'organisation, une stratégie de communication doit être conçue et appliquée (Wardhani et Kartikawangi, 2020). De plus, la modification de la portée du rôle du gardien de l'information suite aux commentaires des participants démontre également l'importance donnée à certaines valeurs par l'organisation. Il semble avoir un lien établi entre le mandat du rôle dans la définition d'exigences de sécurité et l'importance de certaines valeurs au sein d'ABC. Par la suite, la communication permet de créer un engagement chez les employés de l'organisation afin qu'ils puissent s'identifier aux différentes valeurs organisationnelles (Wardhani et Kartikawangi, 2020) et qu'ils respectent ces valeurs.

Concrètement, les participants de cette étude semblaient souvent faire référence aux valeurs favorisées par l'organisation ABC, parfois explicitement et parfois implicitement. Entre autres, ceux-ci faisaient souvent référence à la valeur d'entraide et à celle d'agilité. Pour l'organisation ABC, ces valeurs se traduisent par la mise en place de comportements qui, entre autres,

favorisent le travail en équipe et qui poussent l'innovation dans les méthodes de travail. Ces valeurs et d'autres ont motivé la priorisation effectuée par les participants sur certains facteurs de succès et rôles. Par exemple, bien que la majorité des participants n'avaient préalablement pas entendu parler du rôle de l'innovateur, tous étaient emballés à l'idée d'avoir une personne dédiée à ce rôle au sein de l'équipe. La valeur d'innovation mise à l'avant par ABC a sensiblement affecté la perception des participants. Les employés doivent comprendre les valeurs de l'organisation et les voir sous un œil positif afin de les intégrer dans leur quotidien : les organisations ne doivent pas s'arrêter à définir ces valeurs, mais doivent également les partager à chaque occasion avec tous leurs employés (Dermol et Sirca, 2018). ABC semble avoir réussi à effectuer ceci, étant donné le discours des participants influencé à plusieurs endroits par les valeurs de l'organisation. Ceux-ci se sentent alors engagés et performent mieux dans leur quotidien (Gochhayat, Giri et Suar, 2017).

La présence positive des valeurs favorisées par l'organisation ABC sur les participants de cette étude a sans doute influencé certaines de leurs réponses. **Le dénouement de cet angle de discussion propose de porter une attention particulière au partage des valeurs organisationnelles aux équipes tactiques.**

5.3.2 Une dynamique d'équipe qui s'inscrit dans la prévision

Le deuxième axe de discussion est celui de la place de la prévision dans la dynamique de l'équipe. La prévision a pu être inférée des propos des participants et de la documentation disponible tout au long de la collecte de données. En effet, les facteurs de succès priorisés par les participants (c.-à-d. la communication et la coopération) et les rôles priorisés (c.-à-d. agent de changement, coordonnateur et innovateur) sont tous motivés par un besoin de prévision. De plus, cette prévision semble être présente tout au long du processus de gestion d'incidents.

Le concept de prévision fut un concept souvent soulevé lors de la collecte de données, soit tenter de prévoir et anticiper ce qui peut arriver au lieu de simplement recevoir l'événement de sécurité.

Cette anticipation est possible lorsqu'une expérience se crée au sein de l'équipe grâce à un apprentissage constant de l'environnement et de ce qui a été préalablement accompli pour contrer les cybermenaces. Cet apprentissage peut alors se traduire en compréhension qui permet d'agir parfois avant qu'un événement se produise. L'objectif est ici d'échapper le moins possible des incidents qui pourraient survenir. D'ailleurs, la littérature indique qu'une équipe en mesure de prendre des risques est une équipe plus efficace, car cette prise de risque lui permet de développer une certaine expérience par la suite dans ses différents mandats (Shin et Eom, 2014). Évidemment, dans un contexte de cyberattaques, la prise de risque doit être nuancée afin de continuer à protéger l'actif informationnel. Toutefois, par l'entremise de la prévision, cette prise de risque peut être implantée et favorisée par l'équipe. De plus, l'implantation de tâches variées au sein d'une équipe augmente cette capacité de prévision, car elle doit s'adapter lors de son quotidien (Wu et Wang, 2015). Dans un contexte d'incident de cybersécurité, ceci se produit au quotidien dû aux types d'incidents variés également. Tout ceci explique la grande importance accordée aux facteurs de communication et de coopération par les participants de cette étude.

Dans la littérature, la compréhension de l'environnement et des événements mentionnée ci-haut est dénommée par le fait d'avoir une conscience de la situation. Cette conscience recueille de l'information utile afin d'établir des perceptions de celle-ci (Ahmad et al., 2021). En sécurité de l'information, cela se traduit par une compréhension du contexte afin de détecter des anomalies et d'interpréter des événements de sécurité, et ce même si les signes ne sont pas évidents. Ces signes sont ceux des signaux faibles. La théorie des signaux faibles a majoritairement été utilisée dans le domaine de la stratégie, mais peut être traduite par des alertes en sécurité. Ces alertes permettent de prendre des décisions sur la possibilité qu'un incident se produise ou encore l'impact d'un incident possible, entre autres. Pour être capable de détecter toute forme de signal, une surveillance doit être effectuée. La mentalité de l'individu face à ces signaux, soit son habitude d'interpréter les événements d'une certaine manière va également venir influencer la complémentarité entre les signaux et la conscience de la situation (Ahmad et al., 2021).

La deuxième proposition exprimée est de mettre en place des rôles qui ont un impact plus fort à une phase précise de la gestion d'incidents. Ceci permet de gérer en son ensemble le processus

et d'avoir au minimum quelqu'un de très impliqué à chaque phase. Ceci permet également d'assurer une prévision qui permettra de comprendre l'environnement de l'organisation et ainsi d'avoir une conscience de la situation pour détecter des signaux faibles. Les rôles peuvent influencer cette capacité à prévoir tandis que les facteurs clés de succès permettent de la mesurer.

5.3.3 Interdépendance des rôles pour une meilleure performance d'équipe

Le troisième axe de discussion présente la place accordée à l'interdépendance des rôles. En fait, cette interdépendance semble être un élément favorisant la performance d'une équipe ICIC interdisciplinaire suite à l'analyse des données. Cette section analyse la portée du terme afin de le rattacher à des concepts soulevés lors de l'étude.

En guise de rappel, une équipe est composée de minimalement 2 individus travaillant sous un objectif commun. Cet objectif en étant un d'équipe, il doit être atteint collectivement à l'aide de l'apport de tous les membres de l'équipe (Aubé, Rousseau et Tremblay, 2015). Suite à l'analyse des données de cette étude, il semble que cet apport se matérialise sous forme de coopération principalement. L'interdépendance des tâches est définie comme le niveau auquel les membres de l'équipe doivent travailler ensemble afin de performer une tâche quelconque ; lorsque cette interdépendance est basse, les membres de l'équipe travaillent majoritairement de façon indépendante (Aubé, Rousseau et Tremblay, 2015).

Dans le contexte de l'équipe ICIC interdisciplinaire, cette interdépendance s'illustre premièrement dans la place accordée par les participants au coordonnateur et deuxièmement au lien invisible, mais bien présent qui unit tous les rôles. Pour ce qui est du coordonnateur, ce rôle est sans équivoque un des rôles ayant retenu le plus l'engouement des participants. Il semble être la pièce centrale des rôles qui favorise entre autres la coopération et la communication des membres de l'équipe. Puis, un lien invisible se crée entre chacun des rôles de l'équipe. Ce lien invisible incite tous les membres de l'équipe à travailler conjointement afin d'assurer l'atteinte

de l'objectif commun. Entre autres, l'agent de liaison ne peut travailler sans le gardien de l'information qui lui ne peut travailler sans l'apport de l'agent de changement. Tous ceux-ci ne peuvent à leur tour pas donner leur maximum sans l'apport de l'innovateur et celui du coordonnateur. Ainsi, les tâches et la performance de tous les membres vont avoir un effet sur la performance de l'équipe et la performance organisationnelle (Aumais, Laflamme et Venne, 2012). Plus précisément, dans le cas de l'équipe ICIC interdisciplinaire, ceci est illustré par une interdépendance réciproque dans laquelle un membre dépend du travail d'un autre pour bien effectuer sa tâche, le tout d'une façon cyclique. Donc, personne ne peut se passer de bien travailler, car ceci aura un impact sur quelqu'un d'autre pour ultimement avoir un impact sur la performance organisationnelle. Sundstrom et al. (2000) affirment que la collaboration ne peut exister sans cette interdépendance des rôles qui elle amène un partage des responsabilités (d'ailleurs, ce partage de responsabilités caractérise la structure d'équipe interdisciplinaire). Il peut donc être proposé que l'interdépendance des rôles a ainsi un effet sur l'exécution des tâches, sur la collaboration de l'équipe, sur la performance de celle-ci et finalement sur la performance organisationnelle.

La troisième proposition de cette section est de prendre en compte cette interdépendance des rôles lors de leur définition et implantation au sein d'une équipe ICIC interdisciplinaire.

5.3.4 Les divers volets de la communication comme fondation à l'organisation de l'équipe

Le dernier axe de discussion de ce chapitre est celui des différents volets de la communication : qui, quand, quoi et comment. Ces volets composent le facteur de succès de la communication qui représente la fondation de l'équipe ICIC interdisciplinaire.

Sans l'ombre d'un doute, avoir une communication efficiente est un des premiers facteurs clés de succès composant chaque équipe de travail, tout domaine confondu. Selon la littérature et selon les participants, ce facteur permet la compréhension, la réalisation et l'évaluation des

autres facteurs de succès au sein d'une équipe. La communication doit être proactive tout comme l'équipe (Deloitte, 2020) et peut être analysée sous plusieurs angles. **Dans cette étude, les angles dénotés sont du nombre de quatre (qui, quand, quoi et comment).** Le choix s'est arrêté sur ceux-ci suite à l'analyse de la collecte de données en plus des recherches existantes dans la littérature. Ces angles sont ici discutés dans le contexte d'une situation de gestion d'incidents pour l'équipe interdisciplinaire afin de justifier leur présence.

Premièrement, le « qui » représente le besoin de savoir. C'est-à-dire qu'un individu ne devrait pouvoir manipuler que l'information dont il a besoin pour effectuer ses tâches dans le cadre de ses fonctions. Ce concept du besoin de savoir permet de réduire tout défi qu'amène une situation d'information partagée aux mauvaises personnes, et de diminuer un croisement d'informations non nécessaire entre plusieurs personnes. Dans un contexte d'incident, ceci se traduit lorsque l'équipe ICIC interdisciplinaire doit décider quels membres externes à son équipe aller chercher afin de pouvoir prendre des décisions concernant l'incident. L'équipe ne doit donc pas penser que de par son interdisciplinarité elle pense pouvoir répondre à tous les besoins de la situation, mais plutôt qu'elle doit sélectionner ceux qui peuvent l'appuyer. De plus, un point de contact doit être désigné à l'extérieur de l'équipe afin d'assurer que l'information est transmise aux individus qui pourront aider l'équipe et pour choisir ce point de contact des critères doivent être définis (Chapple, 2020) en fonction des objectifs d'affaires de l'équipe premièrement et de l'organisation deuxièmement.

Deuxièmement, le « quand » provient du moment opportun pour communiquer l'information aux personnes préalablement sélectionnées. De plus, ce volet peut également se traduire par le moment où l'équipe ICIC interdisciplinaire elle-même reçoit l'information qui lui permettra de mieux se préparer aux incidents auxquels elle peut faire face. Par exemple, le rôle de l'agent de changement a sa place en amont du processus de gestion d'incidents ici présenté. Ceci permet d'assurer que l'équipe est incluse dans tout processus qui modifiera ses méthodes ou outils et qu'elle se sente ainsi engagée dès le départ. Troisièmement, le « quoi » reprend en partie le principe du besoin de savoir afin de déterminer quelle information doit être partagée. Ainsi, être

en mesure de précisément identifié ce qui est en train de se produire permet d'identifier la taille de l'incident et quelle est sa gravité (Cert NZ, 2020). L'information partagée ne devrait être que celle nécessaire pour effectuer les tâches qui permettront aux intervenants du processus de gérer l'incident. Finalement, le « comment » vient compléter les trois éléments précédents. Ce volet exprime la manière dont la communication est effectuée, soit par des modèles de communication préétablis à suivre lors d'un incident (Chapple, 2020). Pour une équipe de gestion d'incidents qui est toujours en action, celle-ci doit s'assurer de communiquer l'information dont elle a besoin de manière à être efficiente afin de réduire entre autres les délais de traitement.

L'importance qui est donnée à la communication dans cette étude a une influence sur tous les autres facteurs clés de succès premièrement, puis également sur les rôles. En effet, l'analyse des données a soulevé que la communication est précurseur de tous les facteurs de succès qui pourraient être implantés au sein de l'équipe ICIC interdisciplinaire. Ainsi, des facteurs supplémentaires à ceux présentés dans le cadre de ce mémoire pourraient très bien être ajoutés, temps et aussi longtemps que le facteur de communication est ancré. Les participants et l'organisation semblent accorder une plus grande importance à la mise en place des facteurs de succès qu'à l'évaluation des rôles composant l'équipe ICIC interdisciplinaire. Ceci peut être dû à la place accordée aux facteurs dans les objectifs identifiés par l'organisation pour tous ses employés.

La proposition soulevée par cet axe est de prioriser la mise en place d'une communication efficiente au sein de l'équipe ICIC interdisciplinaire. Ainsi, selon le contexte ici étudié, cette fondation est nécessaire à une équipe ayant à gérer des situations imprévisibles tel que des incidents est la communication. Ensuite, les facteurs de succès doivent être sélectionnés et doivent être appuyés par une communication efficiente. C'est après ceci que les rôles peuvent être inférés uniquement. Pour finir, la communication affecte à elle seule grandement la performance de l'équipe, en plus de la performance de l'organisation et ses objectifs. Cet élément est présent dans toutes les activités de l'équipe et les influence toutes également, et

doit donc être analysé dans le contexte même de l'équipe et de ses tâches afin d'illustrer de la meilleure façon comment l'équipe peut agir (Brindusa, 2016).

5.4 Conclusion

En conclusion, cette étude a permis de répondre aux objectifs de recherche et même d'apporter des précisions à quatre axes de discussion importants. De ce fait, en plus de l'identification des facteurs clés de succès et rôles pertinents au sein de l'équipe ICIC interdisciplinaire, le chapitre a permis d'identifier que **(1) les valeurs organisationnelles a un impact sur le quotidien de l'équipe, (2) la dynamique de l'équipe s'inscrit dans la proactivité, (3) l'interdépendance des rôles améliore la performance de l'équipe et (4) la communication est la fondation de l'organisation de l'équipe**. Le prochain chapitre conclut cette étude à l'aide d'un rappel de ce qui a été fait et d'une ouverture sur ce que la recherche peut entreprendre sur le sujet des équipes ICIC interdisciplinaires.

Chapitre 6. Conclusion

Ce sixième et dernier chapitre conclut cette étude qui avait comme objectif général d'offrir des pistes de réflexion sur la composition d'une équipe interdisciplinaire d'intervention en cas d'incident de cybersécurité (ICIC), soit sur ses facteurs clés de succès et ses rôles. Cet objectif a été atteint à l'aide d'une comparaison entre la littérature et la pratique qui a permis d'établir sur quels éléments on retrouve un consensus et sur quels éléments des nuances doivent être apportées. Des axes de discussion ont permis d'améliorer la tenure des propositions en développant sur les nuances rencontrées.

Afin de conclure ce mémoire, ce chapitre est divisé en quatre sections. La première section offre un rappel sur la question de recherche et l'approche méthodologique afin de recentrer le contexte de cette étude. Ensuite, la deuxième section présente les résultats principaux de façon concise afin de préparer la troisième section qui elle fait un retour sur les implications pratiques et théoriques de l'étude. Finalement, la dernière section du chapitre détaille les principales limites rencontrées et renchérit sur les pistes de recherche futures sur la composition des équipes ICIC interdisciplinaires.

6.1 Rappel de la question de recherche et de l'approche méthodologique

La problématique étudiée dans ce mémoire est celle du manque de préparation et d'efficacité des équipes actuelles d'intervention en cybersécurité face aux risques qui se diversifient et se multiplient (Olyaei, 2019). La recherche existante (c.-à-d. les cadres) se penche davantage sur l'angle technique de cette équipe (p.ex. ses outils ou contrôles techniques) que sur sa composition représentant l'angle humain (Dawson et Thomson, 2018). De plus, il a été dénoté qu'il y aurait un besoin d'explorer le phénomène d'interdisciplinarité, car celui-ci améliore l'innovation d'une équipe. L'interdisciplinarité a

donc été ajoutée au contexte de cette problématique. Ainsi, le mémoire s'est concentré sur la composition de l'équipe interdisciplinaire d'intervention en cas d'incident en cybersécurité.

Pour offrir des pistes de réflexion sur la problématique soulevée, la question de recherche suivante a été posée :

Quelle devrait être la composition d'une équipe interdisciplinaire d'intervention en cas d'incident en cybersécurité ?

Suite à la définition de la problématique et au survol de la littérature existante sur les équipes d'intervention en cybersécurité et celles interdisciplinaires, une collecte de données a été effectuée en utilisant une approche qualitative à l'aide de l'étude de cas. L'organisation ABC a été l'objet de cette étude de cas, car, entre autres, sa culture organisationnelle favorisait l'innovation des méthodes de travail. De plus, il y existe une expérience organisationnelle sur la gestion de risques pouvant mener à des incidents de sécurité.

La collecte s'est divisée en trois phases. Premièrement, un questionnaire Qualtrics a été partagé aux participants afin de recueillir des données démographiques, entre autres sur leur expérience professionnelle, et placer en contexte l'étude de cas présentée. Deuxièmement, des entrevues individuelles semi-dirigées ont été conduites avec ces mêmes participants. Ces entrevues d'une durée approximative de 60 minutes ont été effectuées sur Microsoft Teams. Durant celles-ci, des mises en contexte ont été utilisées par la chercheure afin de favoriser la discussion entre elle et chacun des participants. Les questions posées variaient entre des connotations positives et négatives afin d'obtenir une réaction spontanée de la part des participants. Finalement, en parallèle à ces entrevues, la documentation de l'organisation ABC a été consultée, en particulier les politiques organisationnelles et des exemples de postes. Cette consultation a permis de confirmer certains propos des participants et d'aller pousser la compréhension du contexte de l'étude de cas.

Pour ce qui est de l'analyse, les entrevues et la documentation ont été codifiées à l'aide du logiciel Nvivo et d'une grille de codification conçue par la chercheure. Ceci a permis de regrouper les propos des participants sous des catégories préidentifiées (p.ex. le facteur clé de succès de la communication efficiente). Une analyse intra-répondant a été premièrement effectuée puis une analyse inter-répondants qui a permis d'ajuster la grille de codification avec de nouveaux éléments soulevés lors de l'analyse.

6.2 Principaux résultats

Suite à l'analyse de la collecte des données, plusieurs résultats notables ont pu être soulevés afin de répondre aux objectifs de recherche de l'étude. Cette section présente les principaux résultats de cette analyse en commençant par la pertinence de la présence d'une équipe ICIC interdisciplinaire dans une organisation, en poursuivant avec les facteurs clés de succès de l'équipe puis finalement les rôles qui s'y retrouvent.

Premièrement, les participants ont indiqué en unanimité que l'équipe ICIC interdisciplinaire est une équipe pertinente pour toute grande organisation devant gérer des incidents de sécurité. Entre autres, l'aspect de permanence de l'équipe qu'apporte le concept d'interdisciplinarité a plu aux participants. Ceux-ci dénotaient un meilleur alignement des objectifs, une constance dans la mesure de la performance et une standardisation des processus de gestion d'incidents. De plus, le jumelage de plusieurs disciplines diminue selon eux les délais de gestion d'incidents et augmente la collaboration à travers les secteurs d'affaires. Les participants avançaient également que l'équipe devrait avoir la responsabilité du processus de gestion d'incidents et être alors arrimée avec des spécialistes en fonction de l'incident.

Lorsque la discussion s'est tournée vers les facteurs clés de succès pertinents pour un équipe ICIC interdisciplinaire, l'engouement des participants a été notable. Les facteurs de l'alignement opérationnel en accord avec les objectifs organisationnels, la communication efficiente au sein de l'équipe, la coopération continue au sein de l'équipe et l'adaptabilité efficace face aux

cybermenaces ont tous été adoptés. Ensuite, le facteur de couverture complète des compétences en cybersécurité a été modifié pour le facteur de couverture complète des compétences *humaines.* Ces compétences regroupent par exemple, une habileté de déléguer des tâches ou encore d'aider ses collègues dans leurs mandats. Puis, le facteur de détection de menaces en continu a été remplacé par celui du contrôle efficace des menaces inconnues afin d'englober la détection et la surveillance des menaces qui fut un élément soulevé par la majorité des participants. Finalement, le facteur de reprise rapide des activités a lui aussi été modifié afin d'inclure toutes les phases (avant, pendant et après) du processus de gestion d'incidents : le facteur de réalisation efficiente des phases d'un incident.

Pour ce qui est des rôles, ceux de l'agent de changement, l'agent de liaison, le coordonnateur et l'innovateur ont tous été désignés comme pertinents par la littérature et la pratique. Puis, le rôle du conseiller a été délaissé étant donné que le mandat de l'équipe ICIC interdisciplinaire a été recentré sur le mandat de porter le processus de gestion d'incidents. L'angle technique a donc été mis de côté, en précisant que l'équipe allait devoir être arrimée avec des équipes de spécialistes au sein de l'organisation. Ensuite, le rôle du gardien de l'information a été conservé, mais toutefois modifié pour que celui-ci ne se concentre plus sur les outils techniques, mais sur les exigences de sécurité associées à la gestion des accès à l'information. Cela a permis entre autres d'énoncer que le rôle devait se pencher sur la définition de quel type d'employé pouvait avoir accès à quel type d'information. Tout ceci dans le même objectif de recentrer les rôles conservés au sein de l'équipe ICIC interdisciplinaire sur des rôles se concentrant sur l'aspect humain de la cybersécurité.

Dans le chapitre précédent, quatre axes de discussions ont permis de développer des nuances apportées lors de l'analyse et d'énoncer quatre propositions supplémentaires à celles dénotées dans le choix des facteurs de succès et des rôles pour l'équipe ICIC interdisciplinaire. Le premier axe a indiqué l'importance d'accorder une attention particulière au partage des valeurs organisationnelles aux équipes tactiques. Ensuite, le deuxième axe a indiqué que les rôles mis en place doivent tous avoir un impact fort à une phase (avant, pendant ou après) précise de la

gestion d'incidents. Puis, le troisième axe met de l'avant la compréhension de l'interdépendance des rôles lors de leur définition et implantation au sein de l'équipe ICIC interdisciplinaire. Finalement, le quatrième axe priorise la communication efficiente comme fondation à tous les autres éléments composant l'équipe. La section suivante présente les implications de cette étude pour les chercheurs et les professionnels.

6.3 Implications pour les chercheurs et les professionnels

Les implications de cette étude peuvent être divisées en un premier temps les implications théoriques pour les chercheurs et en un deuxième temps les implications pratiques pour les professionnels de la cybersécurité.

Trois implications théoriques principales sont apportées par cette étude. Premièrement, cette étude pousse la compréhension d'un phénomène embryonnaire du domaine de la cybersécurité en combinant l'étude de la composition d'une équipe interdisciplinaire à l'étude de la composition des équipes en cybersécurité. Cette contribution est exposée dans la présentation du cadre conceptuel au cinquième chapitre qui conclut sur les développements de l'étude. Deuxièmement, l'approche de l'utilisation des facteurs clés de succès pour conceptualiser la composition de l'équipe ICIC interdisciplinaire ouvre la porte à la recherche dans laquelle des propositions sont effectuées en partant du succès d'une équipe ou d'une organisation.

Troisièmement, les propositions regroupées dans le cinquième chapitre offrent un point de départ à de la recherche supplémentaire. Ces propositions sont les suivantes :

- **Proposition 1 :**

Les facteurs de succès de (1) l'alignement opérationnel en accord avec les objectifs organisationnels, (2) la communication efficiente au sein de l'équipe, (3) la coopération continue au sein de l'équipe et (4) l'adaptabilité efficace face aux cybermenaces sont implantés et suivis afin d'évaluer la performance de l'équipe ICIC interdisciplinaire.

- **Proposition 2 :**

Le facteur de succès de la couverture complète des compétences humaines (p.ex. des habiletés à déléguer ou à s'entraider) est implanté afin de centrer la portée de l'équipe à celle d'une équipe de gestion de processus.

- **Proposition 3 :**

La détection et la surveillance des menaces de cybersécurité sont jumelées sous le facteur du contrôle efficace des menaces inconnues et une vérification continuelle est ainsi effectuée sur la posture de sécurité au sein de l'organisation.

- **Proposition 4 :**

Toutes les phases (avant, pendant et après) du processus de gestion d'incidents sont intégrées à l'aide de l'attention accordée à la planification, la reprise rapide des activités et au post-mortem lors du processus.

- **Proposition 5 :**

Les rôles de (1) l'agent de changement, (2) l'agent de liaison, (3) le coordonnateur et (4) l'innovateur composent l'équipe ICIC interdisciplinaire.

- **Proposition 6 :**

L'équipe ICIC interdisciplinaire concentre ses ressources sur des rôles qui permettent de gérer le processus de gestion d'incident et s'arrime avec des spécialistes au sein de son organisation pour des questions plus techniques.

- **Proposition 7 :**

Le gardien de l'information définit les exigences de sécurité concernant l'accès à l'information et harmonise les termes de gestion de l'information utilisés au sein de l'organisation.

- **Proposition 8 :**

Les valeurs organisationnelles sont partagées aux équipes tactiques afin d'accorder une place aux éléments humains qui font la différence lors de situations imprévisibles comme celle d'un incident.

- **Proposition 9 :**

Chaque rôle inclus dans la composition de l'équipe ICIC interdisciplinaire est impliqué et a un impact lors d'au moins une des trois phases du processus de gestion d'incidents.

- **Proposition 10 :**

L'interdépendance des rôles au sein de l'équipe ICIC interdisciplinaire permet d'améliorer la performance de l'équipe et la performance organisationnelle.

- **Proposition 11 :**

La communication efficiente au sein de l'équipe agit comme fondation pour tous les autres éléments qui prennent place dans la gestion d'incidents.

Cette dernière contribution théorique en est également une pratique, car elle offre des pistes de réflexion aux gestionnaires et professionnels qui voudraient instaurer une équipe ICIC interdisciplinaire dans leur organisation.

Deux autres contributions pratiques peuvent être soulevées suite à cette étude. Premièrement, la présentation des indicateurs clés de performance sous chaque facteur de succès permet d'alimenter la réflexion des gestionnaires sur la façon dont doit être mesurée la performance d'une telle équipe. Entre autres, un point récurrent est d'effectuer cette mesure tant avec des éléments qualitatifs que quantitatifs afin d'avoir un meilleur portrait de la situation. Finalement, l'utilisation de rôles davantage humains que techniques permet à tout gestionnaire de comprendre leur importance et leur utilité. L'accent est ainsi placé sur ce que l'humain peut apporter à l'équipe pour son succès, plutôt que quels outils techniques doivent être implantés.

6.4 Limites de l'étude et pistes de recherche

Cette étude comporte plusieurs limites. Premièrement, le fait d'avoir effectué une seule entrevue par participant sans trianguler avec l'observation de leurs comportements en action limite la profondeur des résultats. De plus, un échantillon de 10 participants a permis de répondre aux objectifs de recherche et d'émettre des propositions, mais n'a pas permis d'approfondir davantage la réflexion. Étant donné le faible niveau d'échantillonnage, le portrait global de l'organisation de l'étude de cas ne peut alors être perçu. De plus, le concept de l'équipe ICIC interdisciplinaire n'a pas été étudié dans plusieurs contextes organisationnels. Ceci aurait permis de comparer plusieurs études une à l'autre et de déterminer si des propositions additionnelles auraient pu être soulevées des ressemblances et différences de ces cas. Finalement, une étude qualitative apporte son lot de biais. Bien que la chercheure ait payé attention à ne pas intégrer de biais personnel dans l'analyse des données, certains biais auraient pu se glisser, et ce tant du côté des participants que de la chercheure.

En fonction de ces limites, plusieurs pistes de recherche peuvent être soulevées. Premièrement, le sujet des équipes ICIC interdisciplinaires pourrait être étudié à plus grande échelle. Entre autres, l'échantillon de répondants pourrait être plus grand et donc aléatoire contrairement à cette étude qui a eu un échantillon non aléatoire dû au petit nombre de participants rencontrés. Puis, une équipe longitudinale permettrait d'approfondir les échanges effectués avec les participants. Ceci permettrait de voir si une évolution existe dans la perception des participants après plusieurs mois par exemple.

Ensuite, chacune des propositions de recherche (voir liste de la section 6.3) devrait être étudiée. Par exemple, concernant les valeurs organisationnelles qui semblent avoir une influence dans le travail quotidien de l'équipe ICIC interdisciplinaire, une étude pourrait détailler cette interaction et identifier comment cette interaction s'opère concrètement au sein d'une telle équipe. Ensuite, une autre étude pourrait comparer les propositions obtenues ici à des propositions obtenues dans d'autres domaines sur le sujet des équipes interdisciplinaires. En effet, étant donné que

plusieurs domaines (santé, éducation, recherche, etc.) comportent plusieurs études sur le sujet des équipes interdisciplinaires, il serait intéressant d'évaluer si une généralité peut être identifiée.

Ce mémoire a atteint son l'objectif de décrire la composition d'une équipe ICIC interdisciplinaire. Toutefois, comme mentionné lors de la discussion, les participants semblaient accorder plus d'importance aux facteurs clés de succès qu'aux rôles à identifier au sein d'une telle équipe. Ça serait donc pertinent d'étudier davantage la place à accorder aux facteurs clés de succès au sein d'une équipe ICIC interdisciplinaire pour favoriser sa performance.

Bibliographie

Aboelela, Sally W., Suzanne Bakken, Olveen Carrasquillo et Elaine Larson (2007). « Defining interdisciplinary research: Conclusions from a critical review of the literature », *Health Services Research*, vol. 42, no 1, p. 329-346.

Abramson, Julie S. (1990). « Making teams work », *Social Work with Groups*, vol. 12, no 4, p. 45-63.

Accenture (2018). *Gaining ground on the cyber attacker*. Récupéré le 20 mai 2020 de https://www.accenture.com/us-en/insights/security/2018-state-of-cyber-resilience-index

Ahmad, Atif, Sean B. Maynard, Kevin C. Desouza, James Kotsias, Monica T. Whitty et Richard L. Baskerville (2021). « How can organizations develop situation awareness for incident response: A case study of management practice », *Computers & Security*, vol. 101, no 1, p. 1-15.

Alaoui, Aïcha, Thérèse Laferrière et Danièle Meloche (1996). « Le travail en équipe », *Université de Laval*.

AlHogail, Areej (2015). « Design and validation of information security culture framework », *Computers in Human Behavior*, vol. 49, no 1, p. 567-575.

Alshawaf, Abdulridha, Jafar M.H. Ali et Merza H. Hasan (2005). « A benchmarking framework for information systems management issues in kuwait », *Benchmarking: An International Journal*, vol. 12, no 1, p. 30-44.

Aritzeta, Aitor, Stephen Swailes et Barbara Senior (2007). « Belbin's team role model: Development, validity and applications for team building », *Journal of Management Studies*, vol. 44, no 1, p. 96-118.

AT&T (2021). *The security operations center (soc) team: Operations & responsibilities*. Récupéré le 5 avril 2021 de https://cybersecurity.att.com/solutions/security-operations-center/building-a-soc/soc-team

Aubé, Caroline, Vincent Rousseau, Sébastien Tremblay (2005). « Perceived shared understanding in teams: The motivational effect of being 'on the same page' », *British Journal of Psychology*, vol. 106, no 1, p. 468-486.

Aumais, Nancy, Stéphanie Laflamme et Catherine Venne (2012). *Les leviers qui favorisent la collaboration inter-équipes* [synthèse de recherche], Sherbrooke, Université de Sherbrooke.

Auyporn, Wipawadee, Krerk Piromsopa, Thitivadee Chaiyawat (2020). « Critical factors in cybersecurity for smes in technological innovation era », communication présentée au *ISPIM Connects Bangkok – Partnering for an Innovative Community*, Bangkok, 1-4 mars, The Montien Riverside Hotel.

Bambulas, Nick (2020). *How often should you do cybersecurity awareness training?* Récupéré le 4 avril 2020 de https://www.gflesch.com/elevity-it-blog/how-often-should-you-do-cybersecurity-awareness-training

Bartock, Michael, Jeffrey Cichonski, Murugiah Souppaya, Matthew Smith, Greg Witte, Karen Scarfone (2016). « Guide for cybersecurity event recovery », *NIST Special Publication 800-184*.

Bassellier, Geneviève, Blaize Horner Reich et Izak Benbasat (2001). « Information technology competence of business managers: A definition and research model », *Journal of Management Information Systems*, vol. 17, no 4, p. 159-182.

Baxter, P., et Jack, S. (2008). « Qualitative case study methodology: Study design and implementation for novice researchers », *The Qualitative Report*, vol. 13, no 4, p. 544-556.

Beaumier, Martin et Robert Lescarbeau (2001). « La gestion de la diversité dans les équipes de travail multidisciplinaires », *Interactions*, vol. 5, no 1, p. 154-184.

Belassi, Walid et Oya Icmeli Tukel (1996). « A new framework for determining critical success/failure factors in projects », *International Journal of Project Management*, vol. 14, no 3, p. 141-151.

Belbin (2020). *The nine belbin team roles*. Récupéré le 4 octobre 2020 de https://www.belbin.com/about/belbin-team-roles

Björck, F., M. Henkel, J. Stirna et J. Zdravkovic (2015). « Cyber resilience – fundamentals for a definition », *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol. 353.

Blair, Jean R.S., Andrew O. Hall et Edward Sobiesk (2019). « Educating future multidisciplinary cybersecurity teams », *Curricular Foundations For Cybersecurity*, vol. 1, no 1, p. 58-66.

Bourgon, Guy, Leticia Gutierrez et Jennifer Ashton (2012). « From case management to change agent: The evolution of 'what works' community
supervision », *Corrections Research: User Report*.

Bradley, Charles (1956). « Interdisciplinary teamwork in special education », *Pediatrics and psychiatry*, vol. 23, no 1, p. 5-38.

Brindusa, Maria Popa (2016). « Communicating for success », *Journal of Defense Resources Management*, vol. 7, no 2, p. 79-84.

Bronstein, Laura R (2003). « A model for interdisciplinary collaboration », *Social Work*, vol. 48, no 3, p. 297-306.

Caendra (2017). *How to build a skilled it security team in 5 steps*. https://dsxte2q2nyjxs.cloudfront.net/whitepaper/How_to_build_your_IT_Security_team_in_5_steps.pdf

Caldwell, Willie (2015). *Multi/inter/trans – disciplinary, what's the difference?* Récupéré le 3 octobre 2020 de https://blogs.lt.vt.edu/grad5104/multiintertrans-disciplinary-whats-the-difference/

Campbell, Susan G., Lelyn D. Saner et Michael F. Bunting (2016). « Characterizing cybersecurity jobs: Applying the cyber aptitude and talent assessment framework », communication présentée au *HotSoS* Pittsburgh, 19-21 avril,

Canada, Gouvernement du (2021). *Pleins feux sur la cybersécurité*. Récupéré le 13 mars 2021 de https://www.deleguescommerciaux.gc.ca/guides/spotlight-pleins_feux/spotlight_cybersecurity_pleins_feux_cybersecurite.aspx?lang=fra

CAPP (2017). *Le travail interdisciplinaire : Concepts, conditions de réussite et organisation*. Récupéré le 16 octobre 2020 de http://www.capp-asbl.be/travail_interdisciplinaire.pdf

CertNZ (2020). *Top 11 cyber security tips for your business*. Récupéré le 28 mars 2021 de https://www.cert.govt.nz/business/guides/top-11-cyber-security-tips-for-your-business/

Chang, Shuchih Ernest et Chienta Bruce Ho (2006). « Organizational factors to the effectiveness of implementing information security management », *Industrial Management & Data Systems*, vol. 106, no 3, p. 345-361.

Chapple, Mike (2020). *Cybersécurité : Gérer la communication en cas d'incident*. Récupéré le 13 mars 2021 de https://www.lemagit.fr/conseil/Cybersecurite-gerer-la-communication-en-cas-dincident

Choi, Bernard C K et Anita W P Pak (2006). « Multidisciplinarity, interdisciplinarity and transdisciplinarity in health research, services, education and policy: 1. Definitions, objectives, and evidence of effectiveness », *Clinical and investigative medecine. Medecine clinique et experimentale.*, vol. 29, no 6, p. 351-364.

Choras, Michal, Rafal Kozik, Maria Pilar Torres Bruna, Artsiom Yautsiukhin, Andrew Churchill, Iwona Maciejewska, Irene Eguinoa et Adel Jomni (2015). « Comprehensive approach to increase cyber security and resilience », communication présentée au *10th International Conference on Availability, Reliability and Security*, Toulouse, 24-27 août,

Cichonski, Paul, Tom Millar, Tim Grance et Karen Scarfone (2012). « Computer security incident handling guide », *NIST Special Publication 800-61*.

Collins, Sarah Migas (2017). *Examining interdisciplinary education and collaboration in higher education* [mémoire de maîtrise], Saint Paul, St. Catherine University.

CyberEdu (2015). *Sensibilisation et initiation à la cybersécurité*[document inédit], France, 68 p.

Cyware (2018). *What is a cyber fusion center and how is it different from security operations center (soc)?* Récupéré le 20 avril 2020 de https://cyware.com/educational-guides/cyber-fusion-and-threat-response/what-is-cyber-fusion-center-and-how-is-it-different-from-security-operations-center-soc-b13a

D'Amour, Danielle, Marcela Ferrada-Videla, Leticia San Martin Rodriguez et Marie-Dominique Beaulieu (2005). « The conceptual basis for interprofessional collaboration: Core concepts and theoretical frameworks », *Journal of Interprofessional Care*, vol. 1, no 1, p. 116-131.

Davis, J.R. (1995). *Interdisciplinary courses and team-teaching: New arrangements for learning*. Récupéré le 3 octobre 2020 de http://blogs.ubc.ca/ubcmix/resource-guides/interdisciplinary-team-teaching/

Dawson, Jessica et Robert Thomson (2018). « The future cybersecurity workforce: Going beyond technical skills for successful cyber performance », *Frontiers in Psychology*, vol. 9, no 744, p. 1-12.

De Groot, Juliana (2020). *What is a security operations center (soc)?* Récupéré le 3 mars 2021 de https://digitalguardian.com/blog/what-security-operations-center-soc

DeCoster, Paul (2019). *The changing structure of cybersecurity teams*. Récupéré le 20 novembre 2020 de https://www.infosecurity-magazine.com/opinions/structure-cybersecurity-teams-1-1/

Deloitte (2020). *Réponse aux incidents : Préparez-vous à l'inévitable, réagissez aux menaces changeantes, reprenez rapidement vos activités.* https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-fr-cyber-incident-response.pdf

Denton, H G (1997). « Multidisciplinary team-based project work: Planning factors », *Design Studies*, vol. 18, no 1, p. 155-170.

Dermol, Valerij et Nada Trunk Širca (2018). « Communication, company mission, organizational values, and company performance », *Procedia - Social and Behavioral Sciences*, vol. 238, no 1, p. 542-551.
Diesch, Rainer, Matthias Pfaff et Helmut Krcmar (2020). « A comprehensive model of information security factors for decision-makers », *Computers & Security*, vol. 92, no 1, p. 1-21.
Dinitz, S., Drake, J., Gedeon, S., Kiedaisch, J., et Mehrtens, C. (1997). *The odd couples: Interdisciplinary team teaching*. Récupéré le 3 octobre 2020 de http://blogs.ubc.ca/ubcmix/resource-guides/interdisciplinary-team-teaching/
Drotar, Dennis (2002). « Reflections on interdisciplinary collaboration in the new millennium: Perspectives and challenges », *Journal of Developmental & Behavioral Pediatrics*, vol. 23, no 3, p. 175-180.
Duncan, Sandra (2018). *What is digital transformation?* Récupéré le 16 février 2021 de https://www.bmc.com/blogs/what-is-digital-transformation/
Espinosa, J. A., N. Nan et E. Carmel (2015). « Temporal distance, communication patterns, and task performance in teams », *Journal of Management Information Systems*, vol. 32, no 1, p. 151-191.
Fauvel, A. M., Miller, L. K., Lane, P., et Farris, J. (2010). *Reflections on an interdisciplinary, community-based, team-taught adventure*. Récupéré le 3 octobre 2020 de http://blogs.ubc.ca/ubcmix/resource-guides/interdisciplinary-team-teaching/
Fewster-Thuente, Lori et Barbara Velsor-Friedrich (2008). « Interdisciplinary collaboration for healthcare professionals », *Nursing Administration Quarterly*, vol. 32, no 1, p. 40-48.
Fortune, Joyce et Diana White (2006). « Framing of project critical success factors by a systems model », *International Journal of Project Management*, vol. 24, no 1, p. 53-65.
Gochhayat, Jyotiranjan, Vijai N. Giri et Damodar Suar (2017). « Influence of organizational culture on organizational effectiveness: The mediating role of organizational communication », *Global Business Review*, vol. 18, no 3, p. 691-702.
Gray, Barbara (2008). « Enhancing transdisciplinary research through collaborative leadership », *American Journal of Preventive Medicine*, vol. 35, no 2S, p. S124-S132.
Hall, Jacqueline H., Shahram Sarkani et Thomas A. Mazzuchi (2011). « Impacts of organizational capabilities in information security », *Information Management & Computer Security*, vol. 19, no 3, p. 155-176.
Harper, Douglas (2020). *Performance (n.)*. Récupéré le 2 octobre 2020 de https://www.etymonline.com/word/performance
Herath, Tejaswini, Hemantha Herath et Wayne G. Bremser (2010). « Balanced scorecard implementation of security strategies: A framework for it security performance management », *Information Systems Management*, vol. 27, no 1, p. 72-81.
Hsieh, Po-An J.J., Robert W. Zmud (2006). « Understanding post-adoptive usage behaviors: A two- dimensional view », *Management Information Systems Commons*.
Iannucci, Brian A., Jennifer Garland (2020). « Six strategies for team success », *IABS Journal*, p. 1-20.
Inc, Booz Allen Hamilton (2021). *Cyber fusion center: Your essential cybersecurity functions, unified*. Récupéré le 10 janvier 2021 de https://www.boozallen.com/markets/commercial-solutions/cyber-fusion-center.html

INSPQ (2016). *Planifier la réalisation du projet*. Récupéré le 20 février 2021 de https://inspq.qc.ca/exercer-la-responsabilite-populationnelle/realiser-un-projet-en-lien-avec-la-responsabilite-populationnelle/planifier-la-realisation-du-projet-et-convenir-des-modalites-de-soutien/planifier-la-realisation-du-projet

International, Standish Group (2015). « Chaos report ».

Jacob, Johanna, Wei Wei, Kewei Sha, Sadegh Davari et T. Andrew Yang (2018). « Is the nice cybersecurity workforce framework (ncwf) effective for a workforce comprised of interdisciplinary majors? », communication présentée au *Conference of Scientic Computing*, Bergen, 6-8 juin, Studentsenteret.

Jariwala, Shree, Michael Champion, Prashanth Rajivan et Nancy J. Cooke (2012). « Influence of team communication and coordination on the performance of teams at the ictf competition », *HUMAN FACTORS and ERGONOMICS SOCIETY 56th ANNUAL MEETING*.

Jensenius, Alexander Refsum (2012). *Disciplinarities: Intra, cross, multi, inter, trans*. Récupéré le 20 novembre 2020 de https://www.arj.no/2012/03/12/disciplinarities-2/

Jon (2020). *The 5 cybersecurity roles you need to know about*. Récupéré le 4 octobre 2020 de https://infosecjon.com/the-5-cybersecurity-roles-you-need-to-know-about/

Kankanhalli, Atreyi, Hock-Hai Teo, Bernard C.Y. Tan et Kwok-Kee Wei (2003). « An integrative study of information systems security effectiveness », *International Journal of Information Management*, vol. 23, no 1, p. 139-154.

Kestler, Grady (2017). *An application of multidisciplinary, interdisciplinary, and transdisciplinary approaches in collaboration* [mémoire de maîtrise], San Diego, UC San Diego.

Kong, Heekyung, Suhyun Jung, Insung Lee et Seung-Jun Yeon (2015). « Information security and organizational performance: Empirical study of korean securities industry », *ETRI Journal*, vol. 37, no 2, p. 428-437.

Kraemer, Sara, Pascale Carayon et John Clem (2009). « Human and organizational factors in computer and information security: Pathways to vulnerabilities », *Computers & Security*, vol. 28, no 1, p. 509-520.

Krometis, L. H., Clark, E. P., Gonzalez, V., et Leslie, M. E. (2011). *The "death" of disciplines: Development of a team-taught course to provide an interdisciplinary perspective for first-year students*. Récupéré le 3 octobre 2020 de http://blogs.ubc.ca/ubcmix/resource-guides/interdisciplinary-team-teaching/

Kumar, Ranjit (2011). *Research methodology: A step-by-step guide for beginners*, SAGE Publications.

Lakhani, J., K. Benzies et K. Hayden (2012). « Attributes of interdisciplinary research teams: A comprehensive review of the literature. », *Clinical and investigative medecine. Medecine clinique et experimentale.*, vol. 35, no 5.

Lancaster, Kevin (2020). *Security awareness training including phishing resistance dramatically reduces risk if you keep it up*. Récupéré le 4 avril 2020 de https://www.idagent.com/security-awareness-training-works-if-you-maintain-it

Langevin, Pascal (2004). « Quels facteurs de performance pour quels types d'équipe? L'avis des managers », *Normes et Mondialisation*.

Laplante, Suzanne (2007). « La multidisciplinarité ou comment travailler en équipe multidisciplinaire », *Colloque sur l'établissement et le retrait en agriculture : Ensemble, établissons l'agriculture de demain!*

Larousse (2020a). *Coopération*. Récupéré le 4 avril 2020 de https://www.larousse.fr/dictionnaires/francais/coopération/19056
Larousse (2020b). *Définitions : Équipe*. Récupéré le 6 avril 2020 de https://www.larousse.fr/dictionnaires/francais/équipe/30690
Larousse (2020c). *Performance*. Récupéré le 16 octobre 2020 de https://www.larousse.fr/dictionnaires/francais/performance/59512
Larousse (2020d). *Rançongiciel*. Récupéré le 4 avril 2020 de https://www.larousse.fr/dictionnaires/francais/rançongiciel/188382
Larousse (2020e). *Rôle*. Récupéré le 4 octobre 2020 de https://www.larousse.fr/dictionnaires/francais/rôle/69736
Lee, Denis M. S., Eileen M. Trauth et Douglas Farwell (1995). « Critical skills and knowledge requirements of is professionals: A joint academic/industry investigation », *MIS Quarterly*, vol. 19, no 3, p. 313-340.
Lendick, Mathieu (2019). *La conformité ti et la sécurité: Le cas des institutions financières*. Récupéré le 10 octobre 2020 de https://www.rcgt.com/fr/nos-conseils/conformite-ti-securite-institutions-financieres/
Long, Janet C, Frances C Cunningham et Jeffrey Braithwaite (2013). « Bridges, brokers and boundary spanners in collaborative networks: A systematic review », *BMC Health Services Research*, vol. 13, no 158, p. 1-13.
Lyall, Catherine et Laura Meagher (2007). *A short guide to building and managing interdisciplinary research teams*, Edinburgh, ISSTI University of Edinburgh.
MacKinnon, Mark et Steve Rampado (2020). « The changing faces of cybersecurity: Closing the cyber risk gap », *Deloitte*.
Micheneau, Thomas (2012). *La distance relationnelle dans un contexte de télésurveillance à domicile* [mémoire de maîtrise], Montréal, HEC Montréal.
Microsoft (2017). *Working with kpis in reporting services*. Récupéré le 4 avril 2020 de https://docs.microsoft.com/en-us/sql/reporting-services/working-with-kpis-in-reporting-services?view=sql-server-ver15
Miles, Matthew B. et A. Michael Huberman (1994). *Qualitative data analysis second edition*, Thousand Oaks, SAGE Publications.
MITRE (2021). *Getting started*. Récupéré le 13 mars 2021 de https://attack.mitre.org/resources/getting-started/
Moirano, Regina, Marisa Analía Sánchez et Libor Štěpánek (2020). « Creative interdisciplinary collaboration: A systematic literature review », *Thinking Skills and Creativity*, vol. 35, no 1, p. 1-14.
Moore, Sandra (2019). *The role of diverse skill sets in incident response* [thèse de doctorat], Washington D.C., CAPITOL TECHNOLOGY UNIVERSITY.
Naden, Clare (2021). *Assurer la cybersécurité*. Récupéré le 13 mars 2021 de https://www.iso.org/fr/news/ref2629.html
Nancarrow, Susan A, Andrew Booth, Steven Ariss, Tony Smith, Pam Enderby et Alison Roots (2013). « Ten principles of good interdisciplinary team work », *Human Resources for Health*, vol. 11, no 19, p. 1-11.

Newhouse, William, Stephanie Keith, Benjamin Scribner et Greg Witte (2017). « National initiative for cybersecurity education (nice) cybersecurity workforce framework », *NIST Special Publication 800-181*.
NIST (2019). *Glossary*. Récupéré le 13 mars 2021 de https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary
OCRCVM (2020). « Gestion des cyberincidents guide de planification », *Guide de planification à l'intention des courtiers membres de l'OCRCVM*.
Olyaei, Sam (2019). « New security roles emerge as digital ecosystems take over », *Gartner*.
Orlikowski, Wanda J. et J. J. Baroudi (1991). « Studying information technology in organizations: Research approaches and assumptions », *Information Systems Research*, vol. 2, no 1, p. 1-28.
Palmer, Joshua C. (2017). *Interdisciplinary research collaborations: A guide to creating new research teams*. Récupéré le 17 octobre 2020 de https://www.apa.org/science/about/psa/2017/11/tell-friends
Paré, Guy (2004). « Investigating information systems with positivist case research », *Communications of the Association for Information Systems*, vol. 13, no 1, p. 233-264.
Perignat, E., et J. Katz-Buonincontro (2019). « Steam in practice and research: An integrative literature review », *Thinking Skills and Creativity*, vol. 31, no 1, p. 31-43.
Petersen, Rodney, Danielle Santos, Matthew C. Smith, Karen A. Wetzel et Greg Witte (2020). « Workforce framework for cybersecurity (nice framework) », *NIST Special Publication 800-181*, p. 1-18.
Petri, Laura (2010). « Concept analysis of interdisciplinary collaboration », *Nursing Forum*, vol. 45, no 2, p. 73-82.
Poulin, Julie (2006). *Le fonctionnement des équipes de travail interdisciplinaires en santé : Une étude exploratoire* [mémoire de maîtrise], Montréal, HEC Montréal.
Québec, Gouvernement du (2002a). *Actif informationnel n. M.* Récupéré le 4 avril 2020 de https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/actif_informationnel.html
Québec, Gouvernement du (2002b). *Menace informatique n. F.* Récupéré le 4 avril 2020 de https://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/terminologie_sec_informatique/menace_informatique.html
Québec, Gouvernement du (2017). *Exemples pour une démarche proactive*. Récupéré le 23 septembre 2020 de https://www.ophq.gouv.qc.ca/loi-et-politiques/politique-de-lacces-aux-documents-et-aux-services/exemples-pour-une-demarche-proactive.html
Raza, Muhammad (2019). *Types of it teams*. Récupéré le 16 février 2021 de https://www.bmc.com/blogs/it-teams/
Reina, Daniel Sanchez (2020). « The art of building high-performing teams », *Gartner*.
Rinaldi, Andrew (2020). *The cost of cybersecurity and how to budget for it*. Récupéré le 4 avril 2020 de https://www.mdsny.com/the-cost-of-cybersecurity-and-how-to-budget-for-it/
Rockart, J., M. Earl et J. Ross (2003). « The new it organization : Eight imperatives », *In Proceedings.*
Rubin, H. J. et Rubin, I. S. (1995). *Qualitative interviewing: The art of hearing data*, Thousand Oaks, Californie, SAGE Publications.

San Martin-Rodriguez, Leticia, Marie-Dominique Beaulieu, Danielle D'Amour et Marcela Ferrada-Videla (2005). « The determinants of successful collaboration: A review of theoretical and empirical studies », *Journal of Interprofessional Care*, vol. 1, no 1, p. 132-147.

Seel, Norbert M. (2012). *Cross-disciplinary learning*. Récupéré le 3 octobre 2020 de https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-1428-6_1476#howtocite

Shin, Yuhyung et Chanyoung Eom (2014). « Team proactivity as a linking mechanism between team creative efficacy, transformational leadership, and risk-taking norms and team creative performance », *The Journal of Creative Behavior*, vol. 48, no 2, p. 89-114.

Simos, Mark et Ryen Macababbad (2020). *How to organize your security team: The evolution of cybersecurity roles and responsibilities*. Récupéré le 16 février 2021 de https://www.microsoft.com/security/blog/2020/08/06/organize-security-team-evolution-cybersecurity-roles-responsibilities/

Simplilearn (2020). *Key roles and responsibilities of cyber security professionals*. Récupéré le 20 novembre 2020 de https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article

St-Cyr Bouchard, Maude (2013). *Les équipes de travail interdisciplinaires : Regard sur les facteurs d'une réussite* mémoire de maîtrise, Montréal, Université du Québec à Montréal.

St-Cyr Bouchard, Maude et Johanne Saint-Charles (2018). « La communication et le succès des équipes interdisciplinaires », *Communiquer*, vol. 23, no 1, p. 21-38.

Steinke, Julie, Balca Bolunmez, Laura Fletcher, Vicki Wang, Alan J. Tomassetti, Kristin M. Repchick, Stephen J. Zaccaro, Reeshad S. Dalal et Lois E. Tetrick (2015). « Improving cybersecurity incident response team effectiveness using teams-based research », *IEEE Security & Privacy*, vol. 15, no 1, p. 20-29.

Stern, Amos (2017). *Understanding the soc team roles and responsibilities*. Récupéré le 16 octobre 2020 de https://www.siemplify.co/blog/understanding-the-soc-team-roles-and-responsibilities/

Stevens, Melissa (2017). *Cybersecurity team structure: 7 important roles & responsibilities*. Récupéré le 28 mai 2020 de https://www.bitsight.com/blog/cybersecurity-teams

STM (2020). *Cyber fusion center*. Récupéré le 28 septembre 2020 de https://www.stm.com.tr/en/our-solutions/cyber-security-and-informatics/cyber-fusion-centre

Sundstrom, E., M. McIntyre, T. Halfhill et H. Richards (2000). « Work groups: From the hawthorne studies to work teamsof the 1990s and beyond », *University of Tennessee Knoxville Group Dynamics: Theory, Research and Practice*, vol. 4, no 1, p. 44-67.

Tahir, Sumbul (2020). *Organizational performance: What it is and how to measure and improve it*. Récupéré le 16 novembre 2020 de https://www.ckju.net/en/organizational-performance-what-it-is-how-to-measure-and-improve-it

Tétrault, McCarthy et (2017). *Cybersecurity risk management*. https://www.mccarthy.ca/sites/default/files/2017-11/DOCS-%2314515529-v1-Cybersecurity_Guide.PDF

Thémélis, Thérèse (2019). *Comment devenir un bon agent du changement pour votre entreprise?* Récupéré le 2 octobre 2020 de https://www.journalactionpme.com/2019/01/comment-devenir-un-bon-agent-du-changement-pour-votre-entreprise/

thinkCSC (2018). *Collaboration is the future of cybersecurity*. Récupéré le 3 mai 2020 de https://www.thinkcsc.com/collaboration-is-the-future-of-cybersecurity/

Tu, Zhiling et Yufei Yuan (2014). « Critical success factors analysis on effective information security management: A literature review », communication présentée au *Twentieth Americas Conference on Information Systems*, Savannah, 7-9 août,

Unni, Ajay (2019). *Building the right cyber security team structure*. Récupéré le 20 novembre 2020 de https://www.stickman.com.au/building-the-right-cyber-security-team-structure/

Ursillo, Steve Jr. et Christopher Arnold (2019). *Cybersecurity is critical for all organizations – large and small*. Récupéré le 4 avril 2020 de https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

Vachon, Nathalie (2016). *Comment être un bon agent de changement*. Récupéré le 2 octobre 2020 de http://leducrh.ca/fr/non-classe/etre-agent-de-changement/

Van der Kleij, Rick, Geert Kleinhuis et Heather Young (2017). « Computer security incident response team effectiveness: A needs assessment », *Frontiers in Psychology*, vol. 8, no 1, p. 1-8.

Verizon (2020). *Data breach investigations report*.

Voyer, Philippe (2020). « L'interdisciplinarité, un défi à relever », *The Canadian Nurse*, vol. 96, no 5.

Wardhani, Shabriena et Dorien Kartikawangi (2020). « Internal communication in building organizational culture and organizational branding of government institution », communication présentée au *2nd International Conference on Inclusive Business in the Changing World*, South Jakarta, 6-7 mars, Universitas Katolik Indonesia Atma Jaya.

Weil, Steven (2017). *Dedicated security teams: The pros and cons of splitting focus areas*. Récupéré le 22 octobre 2020 de https://searchsecurity.techtarget.com/tip/Dedicated-security-teams-The-pros-and-cons-of-splitting-focus-areas

Wognum, Nel, Cees Bil, Fredrik Elgh, Margherita Peruzzini, Josip Stjepandic et Wim J.C. Verhagen (2019). « Transdisciplinary systems engineering: Implications, challenges and research agenda », *Int. J. Agile Systems and Management*, vol. 12, no 1, p. 58-89.

Wood, Charles Cresson (1987). « Information systems security: Management success factors », *Computers & Security*, vol. 6, no 1, p. 314-320.

Yin, R. K. (2003). « Case study research: Design and methods. », *Thousand Oaks, CA: Sage*.

Annexe 1 : Liste initiale des facteurs clés de succès

Nom du facteur	Source(s)	Retenu	Justification
Support haute direction	(Mijnhardt, Baars et Spruit, 2016) ; (Diesch, Pfaff et Krcmar, 2020); (Kankanhalli et al., 2003).	Non retenu	Facteur organisationnel
Formalisation de processus, de polices	(Mijnhardt, Baars et Spruit, 2016) ; (Sanderson et Forcht, 1996); (von Solms et von Solms, 2004); (Chang et Lin, 2007); (AlHogail, 2015); (Kraemer et al., 2009); (Tu et Yuan, 2014).	Retenu	Nombre de sources adéquat et facteur géré par équipe
Amélioration continue de la stratégie de gestion de risques	(Mijnhardt, Baars et Spruit, 2016) ; (Tu et Yuan, 2014).	Retenu	Jumelé au facteur d'alignement
Connaissances de l'employé sur la tâche et le sur le processus d'affaires	(Mijnhardt, Baars et Spruit, 2016)	Non retenu	Facteur individuel
Importance accordée au flux d'information à travers l'organisation	(Mijnhardt, Baars et Spruit, 2016) ;	Non retenu	Facteur organisationnel
Compétences TI de l'équipe	(Chang et Ho, 2006); (Alshawaf et al., 2005) (Bassellier, Reich et Benbasat, 2001) ; (Lee, Trauth et Farwell, 1995) ; (Croteau et Raymond, 2004) ; (von Solms et von Solms, 2004); (Tu et Yuan, 2014).	Retenu	Nombre de sources et facteur étudié sous l'angle d'une équipe
Type de l'industrie	(Chang et Ho, 2006)	Non retenu	Étant donné le contexte du sujet à l'étude déjà défini, ce facteur ne fut pas jugé comme important à conserver, car tous les facteurs allaient être sélectionnés au sein de l'industrie de sécurité de l'information

Taille de l'organisation	(Chang et Ho, 2006)	Non retenu	Facteur organisationnel
Gestion des ressources TI	(Alshawaf et al., 2005); (Diesch, Pfaff et Krcmar, 2020); (Kraemer et al., 2009)	Retenu	Nombre de sources
Communication au sein de l'équipe	(Alshawaf et al., 2005); (Diesch, Pfaff et Krcmar, 2020); (AlHogail, 2015); (Ashenden, 2008) ; (Kraemer et al., 2009); (Iannucci et Garland, 2020).	Retenu	Nombre de sources
Produits et solutions TI adaptés à l'industrie	(Alshawaf et al., 2005);	Non retenu	Technique
Justification des besoins en ressources TI	(Ashenden, 2008)	Retenu	Jumelé au facteur de gestion des ressources TI
Conformité aux lois et régulations gouvernementales	(Alshawaf et al., 2005); (von Solms et von Solms, 2004); (AlHogail, 2015);	Non retenu	Facteur externe
Alignement de la stratégie de l'équipe TI aux objectifs de l'organisation	(Alshawaf et al., 2005); (Croteau et Raymond, 2004).	Retenu	Facteur d'alignement
Capacités de recouvrement après incident informatique	(Alshawaf et al., 2005); (Diesch, Pfaff et Krcmar, 2020); (Hall, Sarkani et Mazzuchi, 2011)	Retenu	Nombre de sources
Alignement des solutions TI aux objectifs de l'organisation	(Lee, Trauth et Farwell, 1995)	Retenu	Jumelé au facteur d'alignement de la stratégie TI
Bonne gestion des relations interpersonnelles	(Lee, Trauth et Farwell, 1995) ; (Dhillon et Backhouse, 2000) ; (von Solms et von Solms, 2004); (Chang et Lin, 2007).	Retenu	Nombre de sources; jumelé au facteur de coopération suite aux définitions retenues
Lien de confiance entre les membres de l'équipe	(Dhillon et Backhouse, 2000); (Diesch, Pfaff et Krcmar, 2020);	Retenu	Nombre de sources; jumelé au facteur de coopération
Adaptation des opérations au sein de l'équipe	(Diesch, Pfaff et Krcmar, 2020);	Retenu	Jumelé au facteur de continuation des opérations
Relations avec les fournisseurs	Alshawaf et al., 2005)	Non retenu	Facteur externe
Conscientisation de l'équipe face aux menaces internes et	(Sanderson et Forcht, 1996); (von Solms et von Solms, 2004); (Chang et Lin, 2007);	Retenu	Nombre de sources; jumelé au facteur de communication

externes en cybersécurité	(Hall, Sarkani et Mazzuchi, 2011).		
Responsabilité de gouvernance corporative	(von Solms et von Solms, 2004).	Non retenu	Facteur organisationnel
Utilisation des 'meilleures pratiques'	(von Solms et von Solms, 2004).	Retenu	Jumelé au facteur de formalisation de processus et polices de sécurité
Actions éthiques	(Dhillon et Backhouse, 2000); (von Solms et von Solms, 2004);	Non retenu	*Out of scope*
Utilisation de mesures pour bien surveiller les opérations effectuées	(von Solms et von Solms, 2004); (Ashenden, 2008)	Retenu	Jumelé au facteur d'alignement des objectifs
Culture organisationnelle	(Chang et Lin, 2007); (AlHogail, 2015); (Tu et Yuan, 2014).	Non retenu	Out of scope, facteur organisationnel
Mesures évaluant l'atteinte d'objectifs	(Chang et Lin, 2007); (Diesch, Pfaff et Krcmar, 2020);	Retenu	Jumelé au facteur d'alignement des objectifs
Innovation dans la quête de solutions	(Chang et Lin, 2007); (Iannucci et Garland, 2020).	Retenu	Jumelé au facteur de continuation (adaptation aux événements)
Remédiation aux vulnérabilités techniques	(Diesch, Pfaff et Krcmar, 2020);	Non retenu	Facteur technique
Maintien d'une sécurité physique	(Diesch, Pfaff et Krcmar, 2020);	Non retenu	*Out of scope*
Niveau de préparation de l'équipe face à des événements imprévus	(Iannucci et Garland, 2020).	Retenu	Jumelé au facteur de continuation

Annexe 2 : Courriel de recrutement

Bonjour **Nom de la personne**,

Dans le cadre de mon mémoire pour l'obtention de mon diplôme en Transformation Numérique à HEC Montréal, j'aimerais vous inviter à participer à une étude qui a pour but de discuter la structure d'une équipe interdisciplinaire en cybersécurité dont l'objectif principal serait d'intervenir lors d'un incident en cybersécurité.

Cette équipe d'Intervention en Cas d'Incident en Cybersécurité (ICIC) est définie comme suit :

L'équipe ICIC est une équipe interdisciplinaire qui regroupe des individus provenant de différentes disciplines liées à la sécurité de l'information. Tous ces employés travaillent au sein de l'équipe de façon permanente sous un thème commun, qui est la protection de l'actif informationnel de l'organisation en cas d'incident en cybersécurité. L'équipe ICIC a plusieurs objectifs dont de limiter l'impact d'un incident en cybersécurité, d'améliorer la coordination lors d'un tel incident et la compréhension des vulnérabilités et menaces qui peuvent mener à un incident en cybersécurité.

Dans le cadre de cette étude, vous êtes invité à participer à une entrevue virtuelle via Microsoft Teams, d'une durée approximative d'une heure, au cours de laquelle je recueillerai votre opinion sur cette équipe d'intervention et différents éléments la composant :

- Pertinence de la présence d'une telle équipe au sein de votre organisation ;
- **Facteurs de succès et KPI** pertinents à avoir au sein d'une telle équipe (par exemple : une communication efficiente au sein de l'équipe) ;
- **Rôles et responsabilités** composants cette équipe (par exemple : le rôle de l'agent de changement).

L'anonymat complet ne peut être assuré étant donné le processus de collecte de données qui est de contacter des participants potentiels à travers le réseau de contact de la chercheure au sein de l'organisation, mais votre nom ne sera pas associé aux réponses lors de la publication de l'étude et la chercheure ne partagera pas votre nom à d'autres individus. **Vous n'êtes pas obligé de participer à cette étude ; votre participation est optionnelle.**

L'étude est effectuée sous la supervision d'Alina Dulipovici, professeure agrégée à HEC Montréal, qui peut être contactée par téléphone au 514-340-7301 ou par courriel à alina.dulipovici@hec.ca.

N'hésitez pas à m'écrire si vous avez plus de questions sur l'étude ou si vous avez besoin de clarifications. Merci pour votre temps et en espérant un retour positif de votre part.

Cordialement,
Dana Batog

Annexe 3 : Questionnaire de données démographiques

1- Dans quel(s) domaine(s) avez-vous complété votre formation académique?

- Administration.
- Communication.
- Informatique.
- Ingénierie.
- Autre : _____.

2- Dans quelle(s) industrie(s) avez-vous travaillé avant votre arrivée dans l'organisation ABC?

- Commerce au détail.
- Divertissement.
- Domaine bancaire.
- Éducation.
- Gouvernement.
- Santé.
- Ne s'applique pas.
- Autre : _____.

3- Quel poste occupez-vous présentement au sein de l'organisation ABC?

- Analyste TI.
- Architecte de solutions TI.
- Conseiller TI.
- Développeur.
- Gestionnaire de projet TI.
- Chef d'équipe.
- Directeur.
- Autre : _____.
- Dans quelle direction? : _____.

4- Combien d'années d'expérience professionnelle en TI avez-vous?
    - Années d'expérience en TI : _____

5- Dans combien de projets avez-vous collaboré au sein d'une équipe jugée multidisciplinaire ou interdisciplinaire? Une équipe de travail de cette nature est une équipe dans laquelle des individus provenant de différentes disciplines travaillent conjointement vers l'atteinte d'un objectif commun.

    - Entre 1 et 5 projets.
    - Entre 6 et 10 projets.
    - Plus de 10 projets.
    - Je préfère ne pas répondre à cette question.

6- Quelle était la durée moyenne de ces projets?
    - Plusieurs semaines.
    - Plusieurs mois.
    - Plus d'un an.
    - Je préfère ne pas répondre à cette question.

7- Le NIST définit un incident en cybersécurité comme suit : Des actions posées par l'entremise d'un système d'information ou d'un réseau qui peuvent mener à des conséquences sur ce système d'information, un réseau ou encore l'information qui y réside. *Cet événement a le potentiel de mettre en danger la confidentialité, l'intégrité ou la disponibilité de l'actif informationnel d'une organisation.* Dans combien de projets qui ont nécessité une réponse à un incident en cybersécurité avez-vous été impliqué?

    - Entre 1 et 5 projets.
    - Entre 6 et 10 projets.
    - Plus de 10 projets.
    - Je préfère ne pas répondre à cette question.

Annexe 4 : Protocole de l'entrevue

Note : Le texte en italique indique des explications de la chercheure, mais qui ne seront pas précisées aux répondants.

Introduction

Bonjour M/Mme Nom du répondant, je voudrais tout d'abord vous remercier d'avoir accepté de m'aider pour la collecte de données de mon mémoire dans le cadre de mon diplôme de maîtrise en Transformation Numérique à HEC Montréal. En guise de rappel, mon mémoire a pour objectif de proposer une équipe interdisciplinaire d'Intervention en Cas d'Incident en Cybersécurité (ICIC). Ainsi, pour la collecte de données, je souhaite effectuer des entrevues auprès de plusieurs individus de l'entreprise dans laquelle vous travaillez présentement afin de recueillir leur avis sur cette équipe proposée, notamment sur ses facteurs de succès ainsi que les rôles des membres qui la composent.

L'entrevue sera d'une durée d'environ une heure. Premièrement, nous reviendrons sur la définition de l'équipe ICIC que vous avez reçue dans mon courriel d'invitation. Puis, nous passerons en revue les facteurs de succès de cette équipe (par exemple : la communication efficiente) ainsi que les principaux rôles (par exemple : le rôle de l'agent de changement) des membres qui la composent et je vous poserai des questions pour que vous puissiez me donner votre opinion. Prenez le temps dont vous avez besoin pour répondre aux questions et n'hésitez pas à me poser des questions si vous avez besoin de clarifications avant de répondre.

Avant de débuter l'entrevue, je veux vous donner la possibilité de me poser des questions, si vous en avez, concernant le formulaire de consentement que vous avez préalablement signé ainsi que toute autre question sur l'étude que vous avez avant que nous débutions.

Première partie : Présentation de l'équipe ICIC proposée

La définition de l'équipe ICIC est envoyée à l'avance aux participants. Néanmoins, on utilise un fichier PowerPoint pour l'afficher encore une fois à l'écran.

Je vais maintenant partager mon écran. Sur mon écran, vous voyez la description de l'équipe ICIC que vous avez déjà reçue par courriel. Je vais vous laisser quelques minutes pour la relire, dites-moi lorsque vous aurez terminé.

Diapositive no. 1 : Description de l'équipe ICIC qui s'affiche sur l'écran

L'équipe ICIC est une équipe interdisciplinaire qui regroupe des individus provenant de différentes disciplines liées à la sécurité de l'information. Tous ces employés travaillent au sein de l'équipe de façon permanente sous un thème commun, qui est la protection de l'actif informationnel de l'organisation en cas d'incident en cybersécurité. L'équipe ICIC a plusieurs objectifs dont de limiter l'impact d'un incident en cybersécurité, d'améliorer la coordination lors d'un tel incident et la compréhension des vulnérabilités et menaces qui peuvent mener à un incident en cybersécurité.

1- Avez-vous des questions sur les objectifs ou la description de cette équipe qui vous a été présentée?

2- À première vue, cette équipe ICIC vous semble-t-elle pertinente dans son objectif d'intervention au sein du département de sécurité de l'information d'une organisation? Expliquez votre réponse en quelques mots.

Deuxième partie : Discussion sur les facteurs de succès d'une équipe ICIC et les rôles des membres d'une équipe ICIC

La deuxième partie de cette entrevue est une discussion sur ce qui a été trouvé dans la littérature afin d'établir les facteurs de succès et les rôles essentiels au sein de l'équipe ICIC. Le but de cette partie est de recueillir votre opinion sur ces éléments. Pour ce faire, nous nous concentrerons sur une mise en contexte.

Je vais maintenant partager mon fichier PowerPoint. Lisez bien la mise en contexte qui s'affiche à l'écran.

Mise en contexte aléatoirement sélectionnée qui s'affiche à l'écran (X).

À l'aide des diapositives qui suivent, je vais vous présenter, un par un, 7 facteurs clés de succès d'une équipe ICIC et vous poser quelques questions. Par la suite, je vais faire la même chose avec les 6 rôles que je propose pour les membres d'une équipe ICIC. Gardez en tête la mise en contexte précédemment lue *(la mise en contexte reste présente sur chaque diapositive)*. Prenez le temps dont vous avez besoin pour me répondre.

Les diapositives qui suivent présentent, une par une, les 7 facteurs clés de succès du cadre conceptuel ainsi que des KPI possibles et les 6 rôles et leurs responsabilités. Les facteurs clés de succès sont présentés de façon aléatoire et non selon leur niveau d'importance perçu dans la littérature afin de minimiser le biais dans les réponses des répondants et de minimiser le biais de préférence de la chercheure. Les 6 rôles sont également présentés de façon aléatoire pour les mêmes raisons.

À titre d'exemple du protocole pour cette section de l'entrevue, j'ai inclus une diapositive pour un facteur clé de succès et une diapositive pour un rôle. La présentation PowerPoint utilisée est présentée en Annexe 5.

Diapositive no. 2 : Facteur clé de succès

Communication efficiente au sein de l'équipe

Une structure fluide dans laquelle l'information circule et dans laquelle les membres de l'équipe ont des interactions fréquentes afin de faciliter l'échange d'information au sein de l'équipe.

Exemples d'indicateurs de performance (KPI) :
- Compréhension des objectifs par l'équipe
- Utilisation de canaux de communication de façon régulière pour tenir l'équipe informée
- Fréquence des rencontres d'équipe

1- *Dans la situation (mise en contexte sélectionnée aléatoirement),* ***une communication efficiente n'aurait pas été utile à l'équipe pour répondre à l'incident informatique****.*

   Quel est votre avis sur l'énoncé que je viens de vous mentionner?

2- Avant de poursuivre, pouvez-vous me donner très sommairement votre avis sur les exemples de KPI présentés? Il y en a-t-il d'autres qui selon vous devraient absolument être présentés sur cette carte?

Diapositive no. 9 : Rôle et responsabilités

Agent de changement

Facilite le changement pour l'équipe en mode pratique à l'aide d'une boîte à outils et en misant sur l'implication des membres plus que de seulement miser sur leur participation

Responsabilités :
- Communiquer avec les employés les alertes/nouvelles pertinentes pour l'équipe
- Sensibilisation et formation pour annoncer et préparer le changement avant qu'il ne survienne à l'aide d'un plan de communication
- Créer *workshops* pour parler de la transition et répondre aux questions en fournissant une direction à l'équipe

1- *Dans la situation (mise en contexte sélectionnée aléatoirement),* ***un agent de changement n'aurait pas été utile à l'équipe pour répondre à l'incident informatique****.*

   Quel est votre avis sur l'énoncé que je viens de vous mentionner?

Troisième section : Conclusion

Avant de terminer notre rencontre, je voudrais encore une fois vous remercier pour votre temps et votre aide grandement appréciée pour cette étude.

1- En terminant, avez-vous d'autres points ou suggestions à amener qui n'ont pas été mentionnés durant l'entrevue?

2- Si j'ai besoin d'autres clarifications, me donnez-vous la permission de vous recontacter?

3- Si jamais vous êtes intéressés, je peux vous transmettre les propositions finales de mon étude concernant les éléments essentiels à retrouver au sein d'une équipe performante ICIC.

4- Pour finir, si jamais vous pensez après notre rencontre à quelqu'un qui répondrait aux critères de l'étude et qui serait intéressé à répondre à ces questions également, s'il vous plait me le mentionner par courriel. La personne ne saura pas que vous êtes celui/celle qui me l'a recommandée.

Annexe 5 : Présentation PowerPoint

L'ÉQUIPE INTERDISCIPLINAIRE D'INTERVENTION EN CAS D'INCIDENT EN CYBERSÉCURITÉ

Dana Batog
Février 2021

Déroulement

1. **Contexte de l'étude**
2. **L'équipe ICIC interdisciplinaire**
3. **Facteurs clés de succès**
4. **Rôles**
5. **Conclusion**

2

① Contexte de l'étude

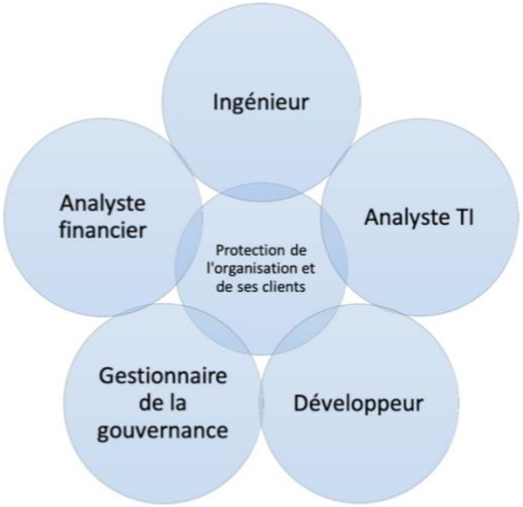
- D'ici 2021, le coût annuel de la cybercriminalité s'élèvera à 6 billions de $
- Manque de compréhension de la dimension humaine
- Intérêt grandissant envers l'interdisciplinarité

② L'équipe ICIC interdisciplinaire

Une équipe qui regroupe des individus provenant de **différentes disciplines** liées à la sécurité de l'information.

L'objectif principal de l'équipe est la **protection de l'actif informationnel** de l'organisation **en cas d'incident en cybersécurité.**

- Limiter l'impact de l'incident
- Améliorer la coordination des parties impliquées
- Obtenir une bonne compréhension des vulnérabilités et menaces pouvant mener à un incident



Exemple de disciplines au sein d'une équipe ICIC interdisciplinaire

③ Facteurs clés de succès

LISEZ ATTENTIVEMENT LA MISE EN CONTEXTE SUIVANTE :

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe

5

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Communication efficiente

Structure fluide dans laquelle l'information circule grâce à des interactions fréquentes entre les membres de l'équipe.

6

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Adaptabilité efficace

Flexibilité et résilience de l'équipe face à des événements changeants dans son environnement.

KPIs

- Avoir accès à des ressources financières
- Avoir des mécanismes de contrôle adaptés aux tendances de l'environnement
- Innover en fonction des opportunités du marché

7

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Détection de menaces en continu

Investiguer afin de comprendre quelles sont les menaces auxquelles l'équipe fait face et quels éléments composent celles-ci.

KPIs

- Vérifier l'efficacité des mesures implantées à l'aide de tests de pénétration
- Utiliser des données historiques pour effectuer un suivi des vulnérabilités de l'organisation
- Utiliser une plateforme qui permet de suivre les menaces de l'environnement

8

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Reprise rapide des activités

La continuation des activités et la rapidité de recouvrement suite à un incident informatique grâce aux capacités techniques et d'affaires de l'équipe.

9

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Couverture complète des compétences de cybersécurité

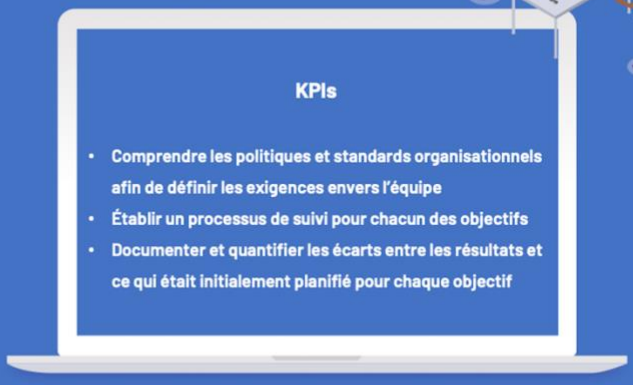
Il est jugé que l'équipe a les compétences nécessaires afin d'intervenir adéquatement lors d'un incident en cybersécurité.

10

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Alignement opérationnel

Cet alignement est un accord entre les objectifs de l'équipe et ceux de l'organisation.



11

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Coopération continue

Contribution et engagement de l'équipe vers l'atteinte d'un objectif commun.

12

④ Rôles

TOUJOURS À L'AIDE DE LA MÊME MISE EN CONTEXTE :

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe

13

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Mes responsabilités

- Sensibiliser l'équipe avant l'arrivée du changement
- Communiquer avec les membres de l'équipe les nouvelles pertinentes
- Faire des ateliers pour répondre aux questions de l'équipe suite au changement

14

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Mes responsabilités

- Orchestrer des tests de pénétration
- Développer les exigences principales de gestion des accès
- Contrôler la qualité des mesures de contrôle envers les pratiques de sécurité

Je suis la gardienne de l'information.

Je gère l'accès à l'actif informationnel de l'organisation lors d'un incident.

15

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Mes responsabilités

- Suivre les vulnérabilités technologiques et humaines auxquelles l'organisation fait face
- Concevoir une liste de besoins de l'équipe
- Avoir une connaissance sur les technologies émergentes dans notre domaine

Je suis la conseillère.

Je supporte mes collègues dans leur prise de décision à l'aide de données récoltées sur les menaces de notre environnement.

16

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Mes responsabilités

- Suivre régulièrement les mises-à-jour des politiques organisationnelles afin d'adapter les pratiques de l'équipe
- Gérer les demandes et l'accès aux ressources de travail
- Rapporter les incidents à la direction lors de rencontres mensuelles

Je suis l'agent de liaison.

Je fais le lien entre l'équipe et les gestionnaires de l'organisation en partageant les perceptions de l'équipe.

17

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Mes responsabilités

- Innover les processus métiers de l'organisation en fonction de notre environnement
- Créer une balance entre la protection de l'actif informationnel et l'innovation
- Promouvoir la créativité au sein de l'équipe

Je suis l'innovateur.

Je suis toujours à la recherche de nouvelles idées afin de permettre à l'organisation de développer sa valeur ajoutée.

18

Un document confidentiel n'est pas chiffré et est ensuite partagé par erreur à des employés non autorisés qui à leur tour pourraient le partager à des individus à l'externe.

Mes responsabilités

- Assigner des tâches en fonction des compétences des membres de l'équipe
- Effectuer un suivi des tâches et projets avec l'équipe
- Gérer les ressources suite à leur obtention

Je suis la coordonnatrice.

J'oriente les efforts de l'équipe afin de résoudre les problèmes qui surviennent lors d'un incident. Je pousse le développement de la promotion de la cybersécurité dans l'organisation.

19

EN CONCLUSION

FACTEURS DE SUCCÈS

Général

- Alignement opérationnel
- Communication efficiente
- Coopération continue
- Couverture complète des compétences en cybersécurité

Spécifique

- Adaptabilité efficace
- Détection de menaces en continu
- Reprise rapide des opérations lors d'un incident

RÔLES

- Agent de changement
- Agent de liaison
- Conseiller
- Coordonnateur
- Gardien de l'information
- Innovateur

20

Annexe 6 : Grille de codification finale

NOTE : Les éléments présentés ***en gras et italique*** dans le tableau ci-dessous ont été ajoutés lors de l'analyse des propos rapportés par les participants.

Code	Nom du code	Description
Contexte professionnel du participant (CP)		
CP-FA	Formation académique	Domaine de formation académique du participant
CP-DOM	Domaine d'expérience	Domaine dans lequel le participant a une expérience professionnelle
CP-EXP	Expérience	Expérience du participant en sécurité de l'information (en années)
CP-E	Équipe	Équipe dans laquelle le participant travaille actuellement au sein de son organisation
CP-P	Poste	Poste qu'occupe le participant actuellement dans son organisation
Équipe interdisciplinaire d'intervention (EII)		
EII-DEF	Équipe interdisciplinaire-Définition	Définition de l'équipe interdisciplinaire et de ses objectifs
EII-PERT	Équipe interdisciplinaire-Pertinence	Pertinence de la présence d'une équipe interdisciplinaire en sécurité de l'information
EII-DEFI	Équipe interdisciplinaire-Défi	Défis de la présence et mise en place d'une équipe interdisciplinaire en sécurité de l'information
Facteurs de succès (FCS)		
FCS-COMM	Facteur de succès-Communication efficiente	Communication efficiente au sein de l'équipe
FCS-COMP	Facteur de succès-Compétences complètes	Couverture complètes des compétences nécessaires en cybersécurité
FCS-AOP	Facteur de succès-Alignement opérationnel	Alignement opérationnel de l'équipe envers les objectifs organisationnels
FCS-COOP	Facteur de succès-Coopération continue	Coopération continue au sein de l'équipe
FCS-REP	Facteur de succès-Reprise rapide des opérations	Reprise rapide des opérations suite à un incident informatique

FCS-ADAPT	Facteurs de succès-Adaptabilité efficace	Adaptabilité efficace de l'équipe face à son environnement
FCS-DET	Facteur de succès-Détection de menaces en continu	Détection de menaces internes et externes à l'organisation en continu
FCS-KPI	***Facteur de succès-KPI***	***Ajout sur les indicateurs clés de performance de la part du participant***
FCS-HUM	***Facteur de succès-Humain***	***Mention du facteur humain par le participant***
FCS-SURV	***Facteur de succès-Surveillance***	***Surveillance des menaces par l'équipe***
FCS-PLAN	***Facteur de succès-Planification***	***Planification de la gestion de l'incident***
Rôles (ROL)		
ROL-AC	Rôle-Agent de changement	Le rôle de l'agent de changement
ROL-AL	Rôle-Agent de liaison	Le rôle de l'agent de liaison
ROL-GARD	Rôle-Gardien	Le rôle du gardien de l'information
ROL-COORD	Rôle-Coordonnateur	Le rôle du coordonnateur
ROL-CONS	Rôle-Conseiller	Le rôle du conseiller
ROL-INNOV	Rôle-Innovateur	Le rôle de l'innovateur
Type d'incident		
TYPE-I	***Type-Incident***	***Type d'incident de cybersécurité***
Organisation ABC		
CAS-ABC	***Cas-ABC***	***Exemple spécifique à l'organisation ABC***