Stratégie de développement des affaires à l'international

Mai 2024

IN·SEC·M
LA GRAPPE CANADIENNE DE LA CYBERSÉCURITÉ

Deloitte.

Explorer comment diversifier les exportations canadiennes de produits et services de cyber-sécurité vers les marchés internationaux

Avis de non-responsabilité

Ce rapport a été produit dans le but d'informer et d'aider In-Sec-M à élaborer sa Stratégie de développement des affaires à l'international.

Deloitte n'assume aucune responsabilité quant aux pertes occasionnées par une tierce partie en raison de la diffusion, de la publication, de la reproduction ou de l'utilisation de ce rapport contrairement à son objectif. Ce rapport a été rédigé uniquement dans le but indiqué et il ne doit pas être utilisé à d'autres fins. Ni ce rapport (y compris les références à celui-ci) ni aucune tierce partie de celui-ci (y compris, sans préjudice, l'identité de Deloitte ou de toute personne signataire ou associée à ce rapport, ou les associations ou organisations professionnelles auxquelles elles sont affiliées) ne doivent être diffusés à des parties quelconques par quelque moyen que ce soit, ou inclus dans un document sans le consentement écrit préalable et l'approbation de Deloitte S.E.N.C.R.L.

Notre rapport de même que le produit de notre travail écrit ne peuvent être inclus ou mentionnés dans aucun document public ou d'investissement sans le consentement préalable de Deloitte S.E.N.C.R.L. Les analyses connexes sont fournies en date du mois de mai 2024, et nous déclinons toute obligation d'informer quiconque de tout changement relatif à n'importe quel fait ou n'importe quelle question affectant cette analyse, qui pourrait venir ou être porté à notre attention après la date des présentes. Sans restreindre les énonciations précédentes, si un changement important dans un fait ou une question affectant les analyses survient après la date des présentes, nous nous réservons le droit de changer, de modifier ou de retirer l'analyse en question.

Les observations sont effectuées en fonction des conditions économiques, industrielles, concurrentielles et commerciales générales en vigueur à la date des présentes. Dans les analyses, nous pouvons avoir formulé des hypothèses au sujet de la performance de l'industrie, des conditions commerciales et économiques générales et d'autres enjeux, dont beaucoup sont hors de notre contrôle, y compris les réglementations gouvernementales et industrielles. Aucune opinion, aucun conseil ou aucune interprétation n'est prévue pour les questions qui nécessitent un avis juridique ou autre avis professionnel approprié. Il est supposé que ces opinions, conseils ou interprétations ont été ou seront obtenus auprès de sources professionnelles adéquates. Dans la mesure où il existe des enjeux juridiques relatifs au respect des lois, réglementations et politiques applicables, nous n'assumons par conséquent aucune responsabilité. Nous estimons que nos analyses doivent être considérées dans leur intégralité et que la sélection de parties des analyses, ou des facteurs pris en compte par celles-ci, sans tenir compte de tous les facteurs et analyses dans leur ensemble, pourrait engendrer une vision trompeuse des questions reliées au rapport. La modification de l'une des hypothèses identifiées dans le présent rapport pourrait avoir un impact important sur notre analyse contenue dans le présent document. Si l'une des hypothèses principales n'était pas exacte ou si l'un des renseignements qui nous ont été fournis n'était pas factuel ou valide, nos analyses, telles qu'exprimées dans le présent rapport, pourraient être manifestement différentes.

Deloitte.

Table des matières

Liste des acronymes

IA	Intelligence artificielle
TCAC	Taux de croissance annuel composé
ACEUM	Accord Canada–États-Unis–Mexique
D&S	Défense et sécurité
BAII	Bénéfices avant intérêts et impôts
GCE	Guide des contrôles à l'exportation
LLEI	Loi sur les licences d'exportation et d'importation
EMBRAPII	Appels de propositions Canada–Brésil
PIB	Produit intérieur brut
RGPD	Règlement général sur la protection des données
GEC	Gouverneur en conseil
GIA	Gestion de l'identité et de l'accès
SCI	Systèmes de contrôle industriel
IEC	Information et communications
IP	Protocole Internet
PARI	Programme d'aide à la recherche industrielle
TIC	Technologies de l'information et des communications
CNRC	Conseil national de recherches du Canada
TO	Technologie opérationnelle
SCADA	Télésurveillance et acquisition de données
PME	Petite et moyenne entreprise
USD	Dollar américain

Objectif de ce rapport

L'objectif principal de cette Stratégie de développement des affaires à l'international (la « Stratégie ») est d'explorer comment diversifier les exportations canadiennes de produits et services de cybersécurité vers les marchés internationaux.

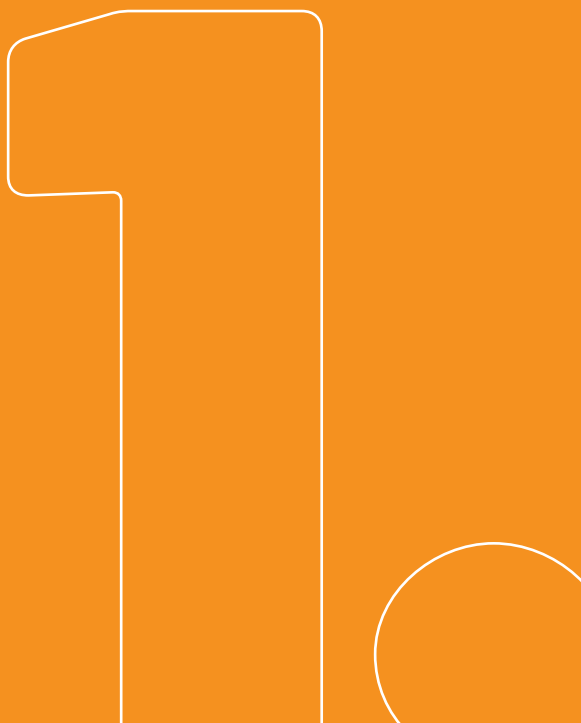
L'étude a été échafaudée en trois phases distinctes. La première phase consistait à réaliser un aperçu intégral du secteur afin de mieux comprendre les empreintes économiques, les caractéristiques de l'industrie, les segments de l'industrie et les compétences du secteur canadien de la cybersécurité. En outre, cette section du rapport a examiné les services offerts par In-Sec-M et ses activités internationales dans le passé. Par ailleurs, une liste des principales conférences internationales qui peuvent faciliter la diversification des exportations pour les entreprises canadiennes a été compilée en vue des considérations futures.

La deuxième phase de l'étude s'est concentrée sur l'analyse des tendances mondiales qui ont un impact sur la demande et la fourniture des services canadiens en matière de cybersécurité. Des informations provenant de diverses sources, notamment l'enquête sectorielle d'In-Sec-M, les rapports antérieurs de mission internationale, les engagements des parties prenantes, les études de marché et les avis d'experts, ont été recueillies pour identifier les marchés présentant un potentiel de diversification des exportations. Une telle analyse a également exploré des domaines en particulier au sein de ces secteurs qui présentent des possibilités d'affaires potentielles.

La troisième phase de cette étude comprenait l'élaboration des objectifs stratégiques et des actions pertinentes à envisager par In-Sec-M et le secteur canadien de la cybersécurité pour une mise en œuvre à avenir.

Il est primordial de noter que cette étude vise à explorer les possibilités de diversification des exportations. Par conséquent, des marchés comme les États-Unis, où existent déjà de fortes activités commerciales, n'ont pas été inclus dans cette étude. Quoi qu'il en soit, il convient également de souligner que cette étude ne limite pas les futures activités d'engagement international d'In-Sec-M et des entreprises canadiennes de cybersécurité. L'exploration de nouveaux marchés et de nouvelles possibilités demeure une priorité pour le développement des marchés et elle devrait continuer à être envisagée.

Analyse sectorielle



1.1 Aperçu général d'In-Sec-M

In-Sec-M est la constellation nationale de la cybersécurité au Canada. Fondé en 2017 grâce au soutien du Conseil national de recherches du Canada (CNRC), In-Sec-M vise à rassembler les entreprises canadiennes spécialisées en cybersécurité afin de les aider à établir une solide présence sur les marchés nationaux et internationaux de la cybersécurité. En tant qu'organisme à but non lucratif (OBNL), In-Sec-M agit comme un pont entre les organisations ayant des besoins en cybersécurité et celles qui fournissent des solutions. Constitué d'un réseau de plus de 200 fournisseurs de solutions et de services de cybersécurité, d'experts indépendants, de centres de recherche, d'établissements d'enseignement et d'agences gouvernementales, In-Sec-M facilite les connexions et effectue la promotion des services canadiens et des solutions de cybersécurité auprès des grands décideurs. De plus, en maximisant l'expertise des entreprises canadiennes chevronnées dans le domaine de la cybersécurité, In-Sec-M collabore avec les ministères provinciaux et fédéraux pour développer et offrir des services sur mesure et des formations personnalisées.

Les objectifs organisationnels

In-Sec-M s'est fixé des objectifs organisationnels ambitieux pour construire une industrie canadienne de la cybersécurité compétitive et reconnue à l'échelle internationale. En raison de la prévalence croissante des cybermenaces et leurs répercussions négatives sur divers aspects de la société, In-Sec-M reconnaît le besoin urgent d'un cadre de cybersécurité robuste. L'organisation reconnaît que les cyberattaques deviennent plus fréquentes, complexes et coûteuses, affectant ainsi l'espace démocratique, les services essentiels et la propriété intellectuelle des innovateurs canadiens. Toutefois, In-Sec-M entrevoit également la cybersécurité comme une possibilité de croissance économique et de création d'emplois. En favorisant un écosystème dynamique et le développement de solutions de haute qualité, In-Sec-M vise à garantir que l'industrie canadienne de la cybersécurité demeure flexible, compétitive et capable de relever efficacement les défis nationaux et internationaux en matière de cybersécurité.

Les compétences professionnelles d'In-Sec-M

Sur le plan stratégique, les compétences professionnelles d'In-Sec-M repose sur trois axes interconnectés :

Innovation : In-Sec-M soutient les initiatives visant à renforcer l'écosystème d'innovation en cybersécurité au Canada, tout en favorisant les partenariats d'innovation avec des organisations étrangères pour répondre aux besoins les plus complexes des entreprises, des secteurs stratégiques et des territoires d'affaires..

Securité : en collaboration avec les gouvernements fédéral et provinciaux, In-Sec-M conçoit et met en œuvre divers programmes et initiatives d'accompagnement et de soutien à la cyber-résilience, mettant l'expertise de l'écosystème à la disposition des organisations souhaitant renforcer leur cybersécurité

Marché : In-Sec-M accompli et met en œuvre des projets qui positionnent stratégiquement l'industrie canadienne de la cybersécurité, agissant ainsi comme une plateforme cohérente afin d'assurer la pénétration des grands marchés nationaux et internationaux pour les différents acteurs de l'écosystème de la cybersécurité.

Les missions commerciales internationales

In-Sec-M organise des missions commerciales stratégiques afin d'augmenter les exportations canadiennes de produits et services de cybersécurité vers les marchés à travers le monde. Chaque année, ces missions commerciales permettent aux entreprises canadiennes — notamment aux petites et moyennes entreprises (PME), aux représentants des centres de recherche, aux organismes de soutien sectoriel et à divers organismes gouvernementaux — d'accroître leurs activités à l'international, de développer des partenariats stratégiques, et de promouvoir l'expertise canadienne à l'échelle internationale, tout en augmentant les possibilités d'investissement au Canada.

Les programmes d'aide

En collaboration avec les gouvernements fédéral et provincial, In-Sec-M offre aux organisations une diversité de programmes d'aide afin de renforcer les aptitudes de l'économie canadienne en matière de cybersécurité. Deux des programmes actuellement disponibles sont décrits ci-dessous.

Programme d'aide MaLoi25 : grâce à la subvention financière du gouvernement du Québec, In-Sec-M a conçu un programme d'aide pour soutenir toute organisation — à but lucratif ou non, ayant son siège social au Québec et comptant moins de 500 employés — à se conformer à la *Loi 25 sur la protection des renseignements personnels* et à renforcer sa cybersécurité. Ce programme comprend l'accès à un outil d'autodiagnostic ainsi que des services de sensibilisation, de formation et d'accompagnement.

Programme d'aide à la cybersécurité des PME : il s'agit d'un programme qui appuie les PME canadiennes innovatrices en leur offrant des services de consultation en cybersécurité par l'intermédiaire du Programme d'aide à la recherche industrielle (PARI) du Conseil national de recherches du Canada (CNRC). Ce programme d'aide offre un accompagnement personnalisé sous forme de services de consultation, notamment dans les domaines de la protection des systèmes informatiques ou de la conformité à des pratiques, lois, règlements, normes ou certifications particulières, ou encore pour le développement de nouvelles solutions en cybersécurité.

1.2 Esquisse sectorielle

Le secteur canadien de la cybersécurité est devenu de plus en plus important, reflétant ainsi l'escalade des cybermenaces à l'échelle mondiale et la transformation numérique rapide au sein de nombreuses industries au Canada. Cette section dépeint une esquisse du secteur canadien de la cybersécurité et elle met en relief son importance.

L'empreinte économique

Le Canada s'est imposé comme un chef de file mondial dans le domaine de la cybersécurité, comme en témoignent son engagement et ses compétences. L'Indice mondial de cybersécurité (IMC)[1] de 2020, publié par l'Union internationale des télécommunications (UIT), sert de mesure complète de l'engagement des pays en matière de cybersécurité à l'échelle mondiale. Sur les 194 pays évalués, le Canada a obtenu une impressionnante 8e position en termes d'engagement relatif à la cybersécurité.

L'empreinte économique de l'industrie canadienne de la cybersécurité et de sa chaîne des valeurs est importante, contribuant ainsi à plus de 3,2 milliards de dollars au PIB national selon l'Enquête[2] de 2020 menée par Statistique Canada. La moitié de la contribution au PIB a été directement attribuée aux activités économiques de l'industrie, tandis que 25 % (0,8 milliard de dollars) ont été procurés par les fournisseurs canadiens de l'industrie, et les 25 % (0,8 milliard de dollars) attribuables aux dépenses de consommation des employés connexes[3].

L'industrie canadienne de la cybersécurité employait directement plus de 14 100 personnes (en 2020) et contribuait au total à plus de 29 400 emplois à l'échelle nationale (y compris les emplois indirects et induits). De 2018 à 2020, l'industrie a connu une croissance énergique démontrée par une augmentation de 860 millions de dollars du PIB et la création de 6 900 nouveaux emplois au total. De plus, l'industrie a également connu une croissance conséquente pendant la pandémie. Par exemple, de 2020 à 2022, les ventes de biens et de services de l'industrie de la cybersécurité ont augmenté de 49 %.

Les caractéristiques de l'industrie canadienne de la cybersécurité

L'Enquête de 2022 sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité a révélé que 463 entreprises exercent leurs activités dans le secteur de la cybersécurité. L'industrie est principalement composée de PME, dont 90 % emploient moins de 250 personnes. Ces PME contribuent à environ 39 % des revenus de l'industrie, 37 % de ses employés, 22 % de ses efforts de recherche et développement (R&D) et 18 % de ses exportations.

En termes de propriété, la majorité des entreprises du secteur canadien de la cybersécurité (81 %, soit 374 entreprises) sont détenues par des Canadiens ou ont leur société mère située au Canada. Ces entreprises canadiennes représentent 71 % des revenus totaux de l'industrie. Parmi les entreprises canadiennes, les trois quarts (339 entreprises) sont des sociétés privées sous contrôle canadien. Cependant, ces sociétés privées ne contribuent qu'à 28 % des ventes de l'industrie. Il y a 56 entreprises (12 % du total des entreprises) opérant au Canada qui appartiennent à des sociétés mères situées aux États-Unis. Malgré leur petit nombre, ces entreprises contribuent à près de 22 % des revenus de l'industrie cybernétique.

L'industrie canadienne de la cybersécurité est réputée pour sa vigoureuse intensité d'activités de R&D. Selon les données de Statistique Canada, les activités de R&D du secteur en 2020 étaient près de 2,5 fois supérieures à la moyenne de l'industrie canadienne des technologies de l'information et des communications (TIC).

1. Publications de l'Union internationale des télécommunications
2. Statistique Canada. Enquête de 2020 sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité. Ottawa, Canada.
3. Les ventes totales de l'industrie canadienne de la cybersécurité, telles qu'elles sont présentées plus loin dans ce document, dépassent sa contribution au PIB. Cet écart est dû au traitement des intrants intermédiaires, c'est-à-dire les ventes totales qui représentent la valeur totale des biens et services vendus, tandis que la contribution au PIB se concentre sur la valeur ajoutée après soustraction du coût des intrants. Des facteurs tels que la dépendance aux importations ou les activités à faibles valeurs ajoutées peuvent contribuer à des ventes totales plus élevées que la contribution au PIB

Les secteurs d'activité de l'industrie canadienne de la cybersécurité

Les secteurs de l'industrie de la cybersécurité au Canada peuvent être fragmentés en des activités commerciales suivantes[4], en fonction des types de biens et services que chaque segment produit :

- **Les vérifications de conformité et le développement de programmes** : ce segment englobe la fourniture des vérifications de conformité, de développement de programmes, de développement de stratégies et de services de gestion des risques et de conseil, y compris les vérifications de cybersécurité, le développement de stratégies, le développement de programmes de conformité et d'autres services de conseil connexes.

- **Les systèmes de contrôle industriel (SCI)** : ce segment se concentre sur les solutions et services de cybersécurité visant à protéger les systèmes de contrôle industriel, la télésurveillance et l'acquisition des données (SCADA) et les technologies d'exploitation (TO), y compris des produits tels que les modules de sécurité matérielle et les modules cryptographiques matériels, tout en excluant la protection des réseaux informatiques des entreprises.

- **Le cryptage/chiffrement** : ce segment englobe les ventes reliées au cryptage/chiffrement matériel ou logiciel, ainsi que les services de développement ou de mise en œuvre du cryptage, y compris les activités relatives aux algorithmes et au chiffrement à l'épreuve des traitements quantiques de l'information, à l'exclusion de l'intégration ou de la revente de cryptage commercial et de cryptage principalement inclus dans une autre catégorie de biens et services.

- **Les solutions d'infrastructure** : ce segment se focalise sur les ventes de services pour l'infrastructure de cybersécurité, y compris la mise en œuvre d'une protection continuelle des réseaux et des données. Cela comprend des services et des solutions tels que des pares-feux, des systèmes de détection et de prévention des intrusions, des fournisseurs de services gérés de cybersécurité, des pares-feux d'applications Web, des passerelles de messagerie sécurisées, la sécurité des terminaux, la détection et l'intervention face aux cyber-incidents, la détection des cybermenaces internes, la gestion ou le contrôle des identités et des accès, les outils de sécurité des applications, la conception et l'intégration de systèmes de sécurité, l'orchestration et l'automatisation de la cybersécurité, les solutions de cybersécurité fondées sur l'infonuagique, et d'autres technologies conçues pour se protéger contre les cyberattaques en utilisant des techniques de cryptanalyse.

- **Les tests d'intrusion et la surveillance des cybermenaces** : ce segment englobe les ventes reliées aux tests d'intrusion, aux évaluations de vulnérabilité et aux activités dans le domaine cybernétique visant à détecter, surveiller, analyser, comprendre et prédire les cybermenaces afin d'améliorer la connaissance de la situation et de renforcer les cyberdéfenses, y compris l'application des mesures de cyberdéfense actives pour protéger les données, les réseaux, les infrastructures et d'autres systèmes contre les propensions et actions cybernétiques agressives et exploitantes.

- **Les enquêtes juridico-informatiques** : ce segment incorpore les ventes reliées à la production de biens et/ou à la fourniture de services pour l'identification, l'évaluation et l'intervention face aux cyberattaques et aux cyber-incidents, y compris les services et outils logiciels pour la criminalistique des réseaux, les services de recherche, l'analyse des fraudes, l'identification des malfaiteurs internes et d'autres services d'intervention face aux cyber-incidents.

- **La formation** : ce segment inclut les ventes qui correspondent à la production de biens et/ou à la fourniture de services de formation en cybersécurité, de développement de la main-d'œuvre et de services ou solutions pédagogiques qui s'adressent à tous les niveaux, des utilisateurs néophytes aux praticiens avancés, et qui utilisent divers mécanismes de formation tels que des services de conscientisation, des didacticiels, des logiciels, etc.

4. Ibid.

Les compétences canadiennes en cybersécurité

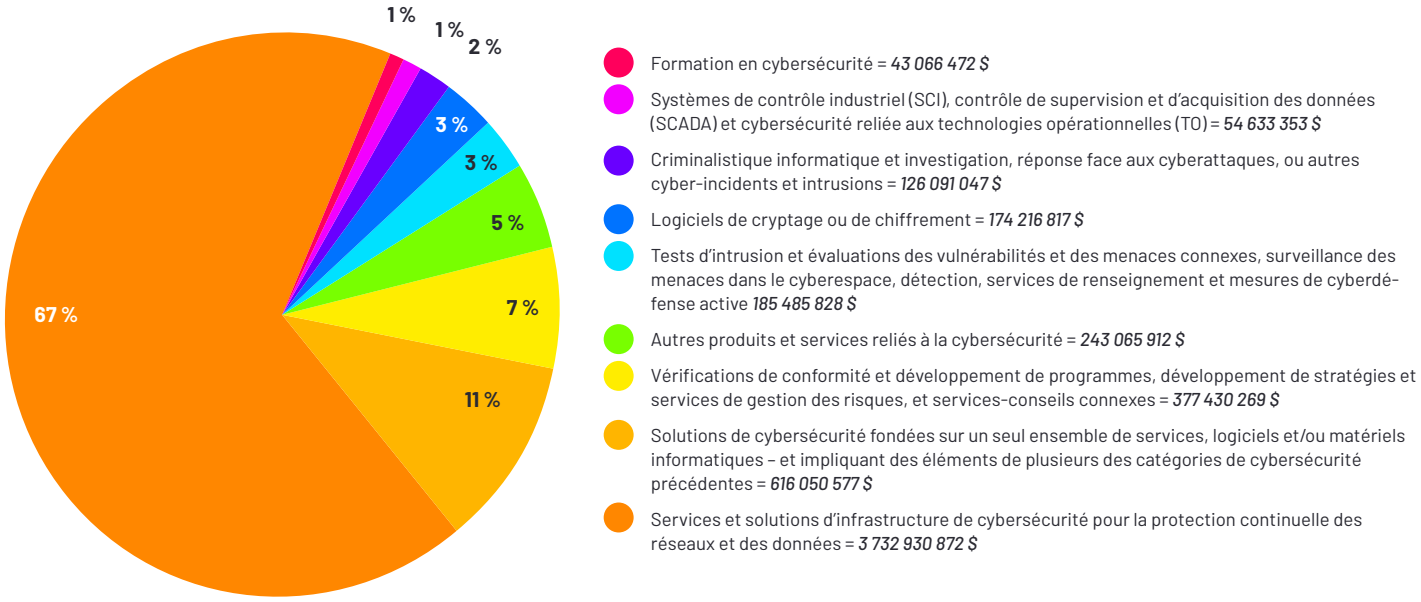
En examinant les ventes des différentes catégories de l'industrie canadienne de la cybersécurité, on constate que la force substantielle de l'industrie canadienne de la cybersécurité réside dans la fourniture de services et de solutions d'infrastructure de cybersécurité pour la protection continuelle des réseaux et des données. En 2022, cette catégorie a enregistré les ventes totales les plus élevées, s'élevant à 3,7 milliards de dollars, et également les ventes les plus élevées en logiciels et/ou en matériel[5], avec 1,5 milliard de dollars. Ces chiffres révélateurs indiquent une solide compétence et une forte demande en matière de fourniture de solutions complètes de cybersécurité pour protéger les réseaux et les données.

L'industrie démontre également une habile compétence en matière des vérifications de conformité, de développement des programmes, d'élaboration des stratégies et des services de gestion des risques et des conseils connexes. Cette catégorie se rapporte au deuxième chiffre d'affaires total le plus élevé (à l'exclusion de la catégorie des solutions de cybersécurité établies sur un seul ensemble de services, de logiciels et/ou de matériel), s'élevant à 377 millions de dollars, et également des ventes importantes en logiciels et/ou en matériel, avec 116 millions de dollars. Ces chiffres suggèrent que les entreprises canadiennes de cybersécurité sont compétentes pour aider les entreprises à se conformer aux réglementations en matière de cybersécurité et à élaborer des stratégies efficaces.

La catégorie « tests d'intrusion, évaluations des vulnérabilités et des menaces connexes, surveillance des menaces dans le cyberespace, détection, services de renseignement et des mesures de cyberdéfense actives » est un autre aspect déterminant de l'industrie canadienne de la cybersécurité. Cumulant un chiffre d'affaires total de 185 millions de dollars, elle représente une part remarquable des revenus de l'industrie. Néanmoins, les ventes de logiciels et/ou de matériel informatique dans cette catégorie sont faibles comparativement aux autres catégories dont les ventes globales sont élevées.

Le cryptage/chiffrement se distingue également comme une compétence robuste, avec un chiffre d'affaires total de 174 millions de dollars et des ventes de logiciels et/ou de matériel informatique s'élevant à 100 260 274 dollars. De tels chiffres indiquent que l'industrie investit considérablement dans les technologies de cryptage/chiffrement qui sont indispensables pour sécuriser les données.

Figure 1 : Ventes de produits et services de cybersécurité, par catégories de produits et services, Canada, 2022



5. La différence entre les ventes totales d'une industrie et ses ventes de matériel et de logiciels peut inclure les revenus générés par les heures facturables de la main-d'œuvre grâce aux services fournis

Tableau 1 : Ventes de produits et services de cybersécurité, par logiciel et/ou matériel informatique, Canada, 2022

Catégorie de produits et services	Ventes totales de la catégorie ($)	Ventes ($) de : logiciel et/ou matériel informatique
Services et solutions d'infrastructure de cybersécurité pour la protection continuelle des réseaux et des données.	3 732 930 872	1 509 967 917
Solutions de cybersécurité fondées sur un seul ensemble de services, logiciels et/ou matériels informatiques – et impliquant des éléments de plusieurs des catégories de cybersécurité précédentes.	616 050 577	325 522 053
Vérifications de conformité et développement de programmes, développement de stratégies et services de gestion des risques, et services-conseils connexes.	377 430 269	116 890 323
Autres produits et services reliés à la cybersécurité.	243 065 912	152 740 766
Tests d'intrusion et évaluations des vulnérabilités et des menaces connexes, surveillance des menaces dans le cyberespace, détection, services de renseignement et mesures de cyberdéfense active.	185 485 828	29 286 658
Logiciels de cryptage ou de chiffrement.	174 216 817	100 260 274
Criminalistique informatique et investigation, réponse face aux cyberattaques, ou autres cyber-incidents et intrusions.	126 091 047	15 437 997
Systèmes de contrôle industriel (SCI), contrôle de supervision et d'acquisition des données (SCADA) et cybersécurité reliée aux technologies opérationnelles (TO).	54 633 353	6 086 022
Formation en cybersécurité.	43 066 472	6 310 658
Ventes totales : industrie de la cybersécurité	**5 552 971 147**	**2 262 502 669**

(Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité, Statistique Canada)

Au cours de la période 2020-2022, les ventes des services d'infrastructure de cybersécurité ont enregistré la plus forte croissance en termes de volume de ventes, générant une augmentation significative de 70 %, ce qui s'est traduit par une augmentation des ventes d'environ 1,54 milliard de dollars. Le segment des vérifications de conformité et du développement des programmes, du développement des stratégies et des services de gestion des risques, et des services-conseils connexes a également connu une augmentation des ventes d'environ 114 millions de dollars. En outre, les ventes des services reliés à la criminalistique informatique, aux cyber-incidents et aux enquêtes sur les intrusions ont connu une augmentation notable de 54 millions de dollars.

Cependant, certaines catégories ont connu une baisse des ventes de 2020 à 2022, en particulier les logiciels de cryptage ou de chiffrement et les catégories reliées aux SCI, SCADA et TO. La catégorie Logiciels de cryptage ou de chiffrement a connu une baisse de 29 % (équivalent à 73 millions de dollars) des ventes en 2022 par rapport à 2020, tandis que la catégorie SCI, SCADA et TO a connu une baisse significative de 68 % (équivalent à 116 millions de dollars) au cours de la même période.

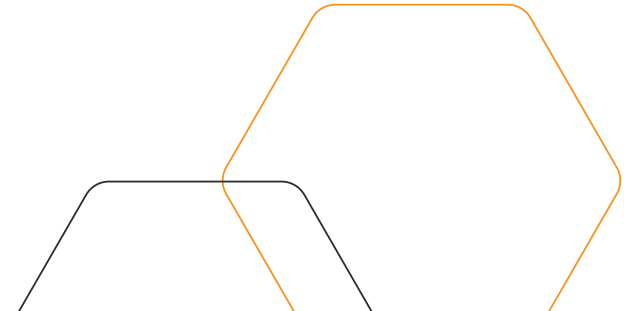


Tableau 2 : ensemble des revenus de l'industrie et évolution entre 2020 et 2022 par catégorie de produits et services

Catégorie de produits et services	Ventes totales de la catégorie ($) (2020)	Ventes totales de la catégorie ($) (2022)	Augmentation des ventes (%) (2020 - 2022)	Total des pourcentages de la catégorie (%) (2022)
Services et solutions d'infrastructure de cybersécurité pour la protection continuelle des réseaux et des données.	$ 2 192 703 687	$ 3 732 930 872	70 %	67,2 %
Solutions de cybersécurité fondées sur un seul ensemble de services, logiciels et/ou matériels informatiques – et impliquant des éléments de plusieurs des catégories de cybersécurité précédentes.	$ 402 764 728	$ 616 050 577	53 %	11,1 %
Vérifications de conformité et développement de programmes, développement de stratégies et services de gestion des risques, et services-conseils connexes.	$ 263 543 386	$ 377 430 269	43 %	6,8 %
Autres produits et services reliés à la cybersécurité.	$ 187 580 158	$ 243 065 912	30 %	4,4 %
Tests d'intrusion et évaluations des vulnérabilités et des menaces connexes, surveillance des menaces dans le cyberespace, détection, services de renseignement et mesures de cyberdéfense active.	$ 174 023 686	$ 185 485 828	7 %	3,3 %
Logiciels de cryptage ou de chiffrement.	$ 246 812 300	$ 174 216 817	-29 %	3,1 %
Informatique judiciaire et investigation, réponse face aux cyberattaques, ou autres cyber-incidents et intrusions.	$ 72 238 812	$ 126 091 047	75 %	2,3 %
Systèmes de contrôle industriel (SCI), contrôle de supervision et d'acquisition des données (SCADA) et cybersécurité reliée aux technologies opérationnelles (TO).	$ 170 577 097	$ 54 633 353	-68 %	1,0 %
Formation en cybersécurité.	$ 26 443 076	$ 43 066 472	63 %	0,8 %
Total des ventes : industrie de la cybersécurité	**$ 3 736 686 930**	**$ 5 552 971 147**	**49 %**	**-**

(Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité, Statistique Canada)

(Remarque : les données rapportées par Statistique Canada indiquent une baisse distinctive des ventes de produits et services de cybersécurité relatifs aux Systèmes de contrôle industriel (SCI), aux systèmes SCADA et aux technologies opérationnelles (TO) de 2020 à 2022. Néanmoins, les données ne fournissent aucune explication à cette baisse. Malgré des recherches supplémentaires pour trouver une explication, aucune information pertinente n'a pu être trouvée.)

Selon les résultats de l'enquête de Statistique Canada, chaque région possède des forces particulières correspondant au secteur de la cybersécurité.

Les avantages géographiques

Selon les résultats de l'enquête de Statistique Canada, chaque région possède des forces particulières correspondant au secteur de la cybersécurité. L'Ontario représentait la plus grande part de l'emploi dans le secteur de la cybersécurité, soit 48 %. Les principales spécialisations régionales en Ontario comprenaient les solutions d'infrastructure de cybersécurité, les solutions regroupées, les vérifications de conformité et le développement des programmes, les tests d'intrusion et la surveillance des cybermenaces, ainsi que le cryptage/chiffrement.

Le Québec était en deuxième position avec une part de 15 % de l'emploi, l'accent étant mis sur les solutions d'infrastructure de cybersécurité, les vérifications de conformité et le développement des programmes, les solutions regroupées, les tests d'intrusion et la surveillance des cybermenaces, ainsi que la formation.

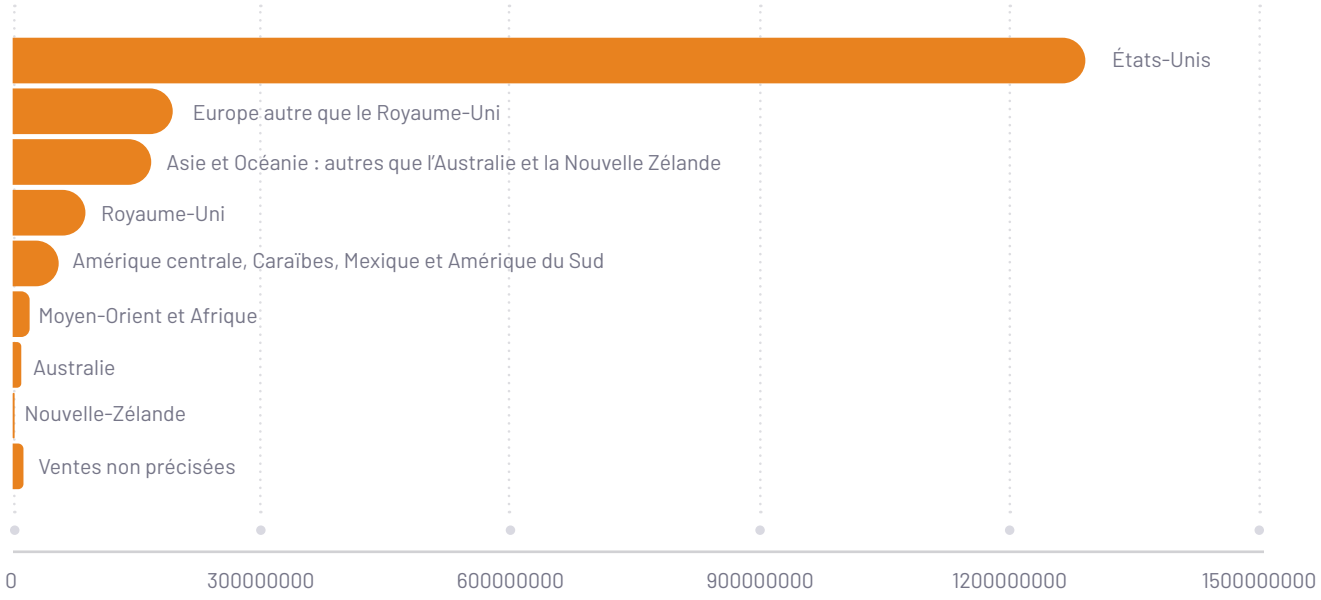
Le Canada atlantique représentait 4 % de l'emploi et se spécialisait dans les systèmes de contrôle industriel (SCI), les solutions regroupées, les solutions d'infrastructure de cybersécurité, les vérifications de conformité et le développement des programmes, de même que la formation.

Enfin, l'Ouest et le Nord du Canada représentaient 33 % de l'emploi et ils se spécialisaient dans les solutions d'infrastructure de cybersécurité, les solutions regroupées, les vérifications de conformité et le développement des programmes, le cryptage et les systèmes de contrôle industriel (SCI). En particulier, la province de la Colombie-Britannique, dans l'Ouest canadien, est devenue une plaque tournante de la cybersécurité, abritant plus de 11 000 entreprises technologiques, des géants de la technologie comme Amazon, Salesforce, Samsung et Microsoft, ainsi que des fournisseurs mondiaux de cybersécurité de premier plan comme Fortinet, Splunk, IBM et Global Intelligence de Mastercard. Des entités locales telles que Trade and Invest B.C. et Cyber Centre of Excellence contribuent activement à l'avancement du secteur de la cybersécurité en Colombie-Britannique.

Les exportations

En 2022, les exportations des produits et services de cybersécurité ont représenté 33 % du chiffre d'affaires total de l'industrie[6]. L'industrie canadienne de la cybersécurité a exporté 1,83 milliard de dollars des produits et services, dont près de 70 % (1,29 milliard de dollars) aux États-Unis. Les autres principaux marchés d'exportation comprennent l'Europe, l'Asie, l'Australie et la Nouvelle-Zélande.

Figure 2 : exportation de produits et services de cybersécurité, par catégorie de client et par pays, Canada, 2022



6. Statistique Canada. Enquête de 2022 sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité. Ottawa, Canada

Tableau 3 : exportation de produits et services de cybersécurité, par catégorie de client et par pays, Canada, 2022

Ventes totales à l'exportation	Ventes à l'exportation ($) (2022)
Ventes au gouvernement fédéral américain	$ 8 835 928
Ventes à des entités non gouvernementales des secteurs de la défense, de la cybersécurité ou de la marine commerciale et civile aux États-Unis (y compris les sous-traitances)	$ 113 772 181
Ventes à d'autres clients américains	$ 1 162 879 378
Ventes non précisées	$ 3 800 758
Total des ventes aux États-Unis	**$ 1 289 288 246**
Ventes en Asie et en Océanie — autres que l'Australie et la Nouvelle-Zélande	$ 192 397 638
Ventes au Royaume-Uni	$ 166 533 552
Ventes : Amérique centrale, Caraïbes, Mexique et Amérique du Sud	$ 87 468 734
Ventes au Moyen-Orient et en Afrique	$ 55 325 559
Ventes en Australie	$ 20 390 194
Ventes en Nouvelle-Zélande	$ 10 345 469
Ventes non précisées	$ 2 160 609
Breakdown not specified	$ 12 973 330
Ventes totales à l'exportation	**$ 1 836 883 330**

(Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité, Statistique Canada)

17 Activités sur les marchés internationaux

L'engagement sur le plan international

Au cours des dernières années, In-Sec-M a considérablement élargi ses efforts d'engagement international pour promouvoir les relations avec les principaux écosystèmes mondiaux de cybersécurité, et faciliter l'entrée des solutions et des fournisseurs de services de cybersécurité canadiens sur les marchés internationaux.

Pour y parvenir, In-Sec-M a organisé 20 missions d'exploration et de développement de marchés en Asie, en Amérique du Nord et du Sud, en Europe, au Moyen-Orient et en Afrique. De plus, l'organisation a participé activement à plus de 20 événements internationaux. Ces initiatives ont permis à In-Sec-M de mettre en valeur les compétences des entreprises canadiennes ayant un potentiel d'exportation, ainsi que motiver des chercheurs universitaires, des experts et des représentants gouvernementaux.

Grâce à ces efforts, In-Sec-M a réussi à établir des alliances stratégiques avec divers écosystèmes mondiaux. Un exemple notable est le récent Accord de partenariat avec le Pôle d'excellence Cyber en France. Cette collaboration vise à renforcer le dynamisme, l'innovation et la promotion de projets communs au sein des écosystèmes de cybersécurité français et canadien.

In-Sec-M est dévoué à amplifier davantage sa portée internationale dans les années à venir. L'organisation prévoit mener des missions exploratoires qui ciblent de nouveaux pays, ainsi que des missions de développement de marché, poursuivant ainsi ses efforts visant à appuyer les entreprises canadiennes de cybersécurité dans leur expansion mondiale.

Les conférences internationales

Le tableau à la page suivante fournit une liste complète des principales conférences internationales sur la cybersécurité dans divers marchés. Ces informations précieuses sont indispensables pour les activités de développement commercial futures, car la participation à ces conférences joue un rôle prépondérant pour favoriser les liens avec l'industrie, se tenir au courant des dernières tendances et mettre en valeur l'expertise des fournisseurs canadiens de solutions et de services de cybersécurité. Le tableau est composé des noms, des descriptions, des lieux, de la taille et des dates de ces conférences, offrant ainsi un coup d'œil complet sur les événements clés du paysage mondial de la cybersécurité.

Conférences en Amérique du Nord

Désignation	Description	Lieu	Taille	Date
RSA Conference	Rassemble des experts, des professionnels et des leaders d'opinion mondiaux pour discuter des tendances, des défis et des solutions en matière de cybersécurité. RSA propose une variété d'activités, notamment des discours d'ouverture, des tables rondes, des sessions techniques, des laboratoires pratiques, des ateliers et des événements de réseautage. Cette conférence couvre des sujets tels que la sécurité infonuagique, l'IA, la confidentialité des données, la surveillance des menaces et la cryptographie. RSA comporte également une exposition où les exposants présentent leurs derniers produits et services.	San Francisco, États-Unis	› 40 000 participants › 650 intervenants › Plus de 500 exposants	Du 6 au 9 mai 2024
Cyber Security & Cloud Expo (Congress North America)	Cyber Security & Cloud Expo est l'événement majeur couvrant la vigilance du jour zéro, la détection des cybermenaces, les conflits cybernétiques mondiaux, l'IA générative, l'informatique quantique, la gestion des risques, la transformation de l'infonuagique, les stratégies de l'infonuagique hybride, l'intégration DevSecOps et l'intelligence artificielle (IA), et l'apprentissage automatique (AM) dans les infrastructures.	Santa Clara, États-Unis	› 7 000 participants › 250 intervenants	Du 5 au 6 juin 2024
SecTor	SecTor s'est forgé une solide réputation en réunissant des experts du monde entier pour partager leurs dernières recherches et techniques. De manière non menaçante et productive, SecTor met en lumière les menaces et les méfaits sous-jacents qui menacent les systèmes informatiques des entreprises et des particuliers.	Toronto, Canada	› Non précisée	Du 22 au 24 octobre 2024
Infosecurity Mexico	Infosecurity Mexico est l'un des principaux événements de cybersécurité au Mexique et en Amérique latine. Il s'agit d'une conférence et d'une exposition annuelle qui vise à réunir des professionnels, des experts et des leaders du secteur de la cybersécurité pour discuter et aborder les dernières tendances, défis et solutions dans le domaine.	Mexico, Mexique	› 1 600+ participants › 60+ réunions d'affaires	Du 22 au 23 octobre 2024

Conférences en Amérique du Sud

Désignation	Description	Lieu	Taille	Date
Cybertech Latin America	CyberTech Latin America est le réseau qui relie les principaux écosystèmes de cybernétique, du monde des affaires et d'innovation de la région. La conférence comprendra des sessions sur les technologies innovantes, la collaboration, les données et bien plus encore.	Ville de Panama, Panama	› Non précisée	Du 13 au 14 mars 2024
Cyber Security Summit Brazil	Cet événement annuel réunit des experts du secteur, des leaders d'opinion et des professionnels du domaine de la cybersécurité pour discuter des tendances émergentes, partager des connaissances et explorer des solutions aux défis rencontrés dans le monde numérique. Le Security Leaders Brazil Summit se concentre sur les PME qui adoptent les technologies, les réglementations, les cybermenaces et bien plus encore.	Sao Paulo, Brésil	› Non précisée	Du 28 au 29 octobre 2024

Conférences en Europe

Désignation	Description	Lieu	Taille	Date
CyberSecurity Conference	Cette conférence examine comment l'Europe peut rester à la pointe des avancées en matière de cybersécurité et contribuer aux efforts collectifs mondiaux visant à sécuriser notre avenir numérique. Les principaux sujets abordés comprennent le cadre politique européen de cybersécurité pour la protection de l'économie numérique du continent, l'intégrité de la chaîne d'approvisionnement et l'impact transformateur de l'IA et de la collaboration.	Bruxelles, Belgique	› Plus de 200 participants › 5 séances	19 mars 2024
InfoSecurity Europe	InfoSecurity Europe est l'un des principaux rassemblements du secteur de la sécurité informatique en Europe. Chaque année, nous réunissons la communauté pour partager des innovations, apprendre les uns des autres, tester et comparer des solutions, tisser des relations, générer de nouvelles activités et nouer des liens avec des collègues. Les principaux fournisseurs choisissent InfoSecurity Europe comme une occasion de lancer de nouvelles technologies, des produits innovateurs et de nouveaux services.	Londres, Royaume-Uni	› 13 800+ participants › 380+ exposants	Du 4 au 6 juin 2024
Cybersec Expo & Forum	Cybersec Expo est une conférence de premier plan sur la cybersécurité. Elle met l'accent sur les technologies émergentes, les tendances en matière de cybersécurité et les possibilités d'exportation pour les entreprises du secteur de la cybersécurité, ainsi que les investissements en capital-risque dans la région.	Katowice, Pologne	› Non précisée	Du 19 au 20 juin 2024
Connect at Tech Show London	Exposition et conférence technologique organisée chaque année. Elle rassemble des professionnels du secteur, des innovateurs et des passionnés de technologie du monde entier pour présenter les dernières avancées dans divers domaines tels que la cybersécurité.	Londres, Royaume-Uni	› 14,850+ participants › 71 exposants	Du 12 au 13 mars 2024
National Cyber Security Show	Le National Cyber Security Show de Birmingham propose deux volets principaux : le Solutions Theatre et le Leaders' Summit. Le Solutions Theatre offre aux exposants une excellente plateforme pour présenter les capacités de leurs produits, leurs avancées technologiques et leurs principales solutions de cybersécurité à un public intéressé. Ce public est composé de personnes ayant des projets actifs et un pouvoir d'achat, ce qui en fait une occasion précieuse pour les entreprises de présenter leurs offres et d'attirer des clients potentiels.	Birmingham, Royaume-Uni	› Non précisée	Du 30 avril au 2 mai 2024
CyberWiseCon Europe	CyberWiseCon is a premier IT security conference that brings together cybersecurity experts, industry leaders, and IT professionals from around the Europe. Provides a platform for cybersecurity companies to showcase their latest productions, services and innovations.	Lituanie (également disponible en ligne)	› Plus de 700 participants › Plus de 130 intervenants › Plus de 35 pays	Du 20 au 24 mai 2024
Les Assises de la cybersécurité	Les Assises de la cybersécurité sont l'une des plus importantes conférences sur la cybersécurité en France. Il s'agit d'un événement annuel qui réunit des professionnels de la cybersécurité, des experts et des leaders du secteur pour discuter et aborder les défis et les solutions du domaine.	Monaco	› 1400+ invités › 170+ entreprises partenaires › 120+ experts et journalistes	Du 9 au 12 octobre 2024

InCyber Forum Europe	Le Forum InCyber est l'événement européen de référence en matière de sécurité et de confiance numérique. Sa particularité est de réunir l'ensemble de l'écosystème de la cybersécurité et du « numérique de confiance » : clients finaux, fournisseurs de services, éditeurs de solutions, consultants, forces de l'ordre et agences gouvernementales, écoles et universités.	Lille, France	› Plus de 20 000 visiteurs › Plus de 700 partenaires › 103 pays représentés	Du 1er au 3 avril 2025
Cloud Expo Europe Frankfurt	Cloud & Cyber Security Expo est un événement majeur dans le domaine de la cybersécurité qui se déroule en Allemagne. Il fait partie du Tech Show Frankfurt, présenté par CloserStill Media. L'événement vise à réunir des professionnels du secteur, des experts et des fournisseurs de premier plan pour discuter et présenter les derniers développements, défis et solutions en matière d'infonuagique et de cybersécurité.	Frankfurt, Allemagne	› Plus de 6 200 participants › Plus de 300 sessions › Plus de 1 100 réunions organisées	Du 22 au 23 mai 2024
Global Cyber Conference	La Global Cyber Conference est un événement international sur la cybersécurité qui se déroule en Suisse et qui rassemble un public d'acteurs de premier plan dans le domaine de la cybersécurité, de décideurs, d'autorités publiques et d'universitaires du monde entier. Elle offre aux principaux décideurs une plateforme de réseautage et d'apprentissage pour acquérir une compréhension commune de ce qui doit être fait pour renforcer la cyber-résilience.	Zurich, Suisse	› Plus de 350 participants provenant de plus de 30 pays	Du 26 au 27 novembre 2024
ItaliaSec Cyber Summit	ItaliaSec est une conférence sur la sécurité informatique certifiée CPE, réunissant plus de 150 dirigeants de haut niveau en matière de sécurité des secteurs public et privé italiens.	Rome, Italie	› Plus de 150 leaders en cybersécurité	Du 13 au 14 mai 2025

Conférences en Asie

Désignation	Description	Lieu	Taille	Date
Cyber Security World Asia	Événement annuel qui se déroule à Singapour et qui met l'accent sur les dernières tendances, défis et solutions dans le domaine de la cybersécurité. L'événement propose une gamme d'activités, notamment des discours liminaires, des tables rondes, des ateliers et des expositions, dont les sujets incluent la génération des leaders en cybersécurité.	Singapour	› 23 864 participants ont visité la Tech Week en 2023 (Cyber Security World Asia fait partie de l'événement Tech Week Singapore)	Du 9 au 10 octobre 2024
GovernmentWare (GovWare)	GovWare est la plus grande conférence et exposition sur la cybersécurité de Singapour. GovWare réunit des décideurs politiques, des innovateurs technologiques et des utilisateurs décisionnels à travers l'Asie et au-delà, favorisant des dialogues pertinents sur les dernières tendances et les flux d'informations indispensables.	Singapour	› 12 000+ participants	Du 15 au 17 octobre 2024
CODE BLUE	CODE BLUE propose des conférences de pointe dispensées par des professionnels de la cybersécurité et des possibilités d'échange d'informations et de collaboration au-delà des frontières. En réunissant des experts de divers domaines, la conférence vise à renforcer la coopération-cybersécurité en Asie et à former des chercheurs talentueux au Japon et en Asie. CODE BLUE 2024 en est à sa 12e année.	Tokyo, Japon	› Non précisée	Du 9 au 15 novembre 2024

Objectifs ciblés de développement des affaires à l'international

Cette section du rapport étudie d'abord les tendances socioéconomiques et sectorielles qui affectent l'industrie de la cybersécurité à l'échelle mondiale. Elle présente ensuite des recherches approfondies sur les marchés potentiels pour la diversification des exportations canadiennes. Chaque marché sélectionné est accompagné d'un profil qui décrit les occasions d'affaires et les défis mis en évidences par les études de marché, l'engagement des parties prenantes et les rapports des missions antérieures d'In-Sec-M.

2.1 Tendances sectorielles et perspectives des marchés

Les tendances ayant un impact sur la demande en cybersécurité

Les tendances mondiales suivantes ont une incidence sur la demande de produits et services de cybersécurité. L'industrie canadienne de la cybersécurité qui souhaite diversifier ses exportations de biens et services vers les marchés internationaux doit faire face aux répercussions de ces tendances sectorielles, notamment la numérisation croissante, les conséquences de la pandémie de la COVID-19, l'adoption de l'IA et les réglementations strictes en matière de cybersécurité. Ces tendances produisent des possibilités pour les entreprises canadiennes de cybersécurité de fournir un soutien dans des domaines tels que la sécurisation des transformations numériques, la protection contre les cyber-risques reliés au télétravail, l'exploitation de la technologie de l'IA, et le respect des exigences réglementaires. En répondant à ces tendances et en proposant des solutions qui correspondent aux besoins évolutifs des organisations du monde entier, les entreprises canadiennes peuvent se positionner comme des partenaires fiables sur le marché mondial de la cybersécurité.

La numérisation croissante dans tous les secteurs

Tandis que les technologies informatiques continuent de progresser et que les entreprises reconnaissent les avantages de la numérisation, on observe une tendance notable dans les industries à opter pour les technologies de l'Internet des objets (IDO). Qu'il s'agisse des opérations interentreprises ou des interactions entre les entreprises et les consommateurs, les organisations intègrent de plus en plus l'IDO dans leurs activités d'affaires. L'un des principaux facteurs à prendre en compte en matière de transformation numérique est l'impact financier, en particulier l'analyse coûts-avantages, c'est-à-dire le potentiel de réduction des coûts et, ultimement, la production de revenus augmentés.

De nombreuses organisations perçoivent la numérisation comme un effort couteux. Pourtant, des recherches approfondies indiquent que les dépenses encourues pour être perturbées et éventuellement éliminées du marché sont souvent plus importantes que les investissements nécessaires pour moderniser les opérations. Au sein de l'économie mondiale d'aujourd'hui, les méthodes traditionnelles sont souvent inadéquates pour faire face au rythme rapide et à l'ampleur des défis. Une étude menée par McKinsey & Company en 2020 a précisément abordé cette préoccupation dans le secteur manufacturier[7], démontrant comment les entreprises peuvent améliorer à la fois l'efficacité et la productivité en rationalisant les étapes de la chaîne des valeur grâce aux produits de l'IDO.

Par ailleurs, une étude distincte menée par la Boston Consulting Group a révélé que les organisations qui ont réalisé une transformation numérique connaissent une augmentation significative de leur BAII (bénéfice avant intérêts et impôts). En moyenne, ces organisations ont connu une augmentation de 21 % de leur BAII, contre une augmentation de 10 % pour les organisations qui n'ont pas opté pour la transformation numérique[8]. En outre, en examinant des secteurs tels que le secteur financier, la consommation, l'énergie, les soins de santé, les biens industriels, les assurances et la technologie, on a constaté que 71 % des organisations (ayant choisi la transformation numérique) ont connu une accélération de leurs ventes et de leurs clientèles[9].

Les entreprises canadiennes spécialisées en cybersécurité ont une possibilité considérable de fournir un soutien aux organisations qui se lancent dans des mises à jour de leurs infrastructures grâce à la numérisation. Afin de profiter d'une telle possibilité, il est essentiel que le marché canadien fonctionne proactivement et promeuve efficacement ses solutions comme une option viable pour ces organisations qui font face à une concurrence étrangère grandissante.

7. McKinsey & Company. Étude publiée le 2 juin 2020.
8. Boston Consulting Group. Étude publiée le 7 décembre 2021
9. Ibid.

La pandémie a engendré de nouveaux défis

La pandémie de la COVID-19 a déclenché un impact immense sur le secteur de la cybersécurité à travers le monde entier. Au fur et à mesure que les organisations se sont tournées vers le télétravail, elles ont dû s'appuyer davantage sur les technologies et les plateformes numériques. Toutefois, de nombreuses organisations n'ont pas été en mesure de fournir un environnement de télétravail sécurisé, ce qui a rendu leurs employés vulnérables aux cyber-risques. Cela a provoqué un plus grand besoin des mesures de cybersécurité pour protéger les données confidentielles et prévenir les cyberattaques. L'essor du télétravail a également entraîné une augmentation des cyberattaques parce que les pirates informatiques exploitent les vulnérabilités des employés travaillant à domicile[10]. Les escroqueries par hameçonnage, les sites Web frauduleux et les cyberattaques directes contre les entreprises sont devenus plus fréquents. Les services de vidéoconférence ont été ciblés par les pirates informatiques qui volent des données personnelles et perturbent les activités des entreprises. Le paysage des cybermenaces s'est intensifié et il est devenu plus diversifié parce que les employés malveillants, les cybercriminels, les cyberactivistes[11] et les pirates informatiques adolescents[12] contribuent à l'augmentation des menaces de cybersécurité. Des mécanismes de détection améliorés, tels que l'Analyse du comportement des utilisateurs et des entités (ACUE), sont nécessaires pour identifier les activités anormales et prévenir les cyberattaques. La lutte contre les erreurs humaines et l'adaptation des systèmes informatiques aux environnements de travail à distance sont indispensables pour préserver la cybersécurité. La pandémie a mis en évidence la nécessité pour les organisations de prioriser la cybersécurité et d'investir dans des mesures robustes pour atténuer les cyber-risques.

L'adoption de l'intelligence artificielle (IA)

Le besoin grandissant des solutions de cybersécurité avancées est la principale tendance à l'origine de la croissance de l'IA sur le marché de la cybersécurité. Cette forte hausse de la demande stimule considérablement la demande globale du secteur. Un récent rapport d'Acumen Research and Consulting a estimé que le marché mondial des produits de cybersécurité fondés sur l'IA était de 15 milliards de dollars en 2021 et il devrait atteindre 135 milliards de dollars d'ici 2023, à un taux de croissance annuel composé (TCAC) de 27,8 % [13].

L'utilisation de la technologie de l'IA est de plus en plus répandue dans les organisations spécialisées en cybersécurité. Cette tendance est motivée par la reconnaissance du rôle crucial que l'IA peut jouer dans la détection et la gestion des cybermenaces de sécurité. En simulant différents scénarios de cyberattaque, l'IA peut identifier efficacement les vulnérabilités et signaler les problèmes de cybersécurité potentiels. Cette intégration de l'IA offre des avantages considérables aux entreprises de cybersécurité, car elle leur permet de prévenir de manière proactive les cyberattaques futures. En arrêtant les violations avant qu'elles ne se produisent, non seulement les données des particuliers et des entreprises peuvent être protégées, mais les entreprises peuvent également réduire leurs coûts informatiques.

De plus, le budget 2024 du gouvernement fédéral a introduit plusieurs initiatives visant à faire progresser l'IA au Canada. L'une de ces initiatives est la Stratégie canadienne de calcul souverain en IA, qui vise à promouvoir le développement d'infrastructures d'IA détenues et situées au Canada[14]. Par ailleurs, le budget a alloué 2 milliards de dollars pour construire et fournir un accès à une infrastructure technologique aux chercheurs, aux entreprises en démarrage et aux jeunes entreprises en croissance qui se spécialisent dans l'IA au Canada[15].

En plus du développement de l'infrastructure, le gouvernement fédéral prévoit d'établir l'Institut canadien de la sécurité de l'IA. Doté d'un budget de 50 millions de dollars, cet institut se concentrera sur le développement et le déploiement sécuritaires des systèmes d'IA. Il collaborera avec les intervenants et les partenaires internationaux pour obtenir des connaissances et se

10. Deloitte S.E.N.C.RL. Impact de la COVID-19 sur la cybersécurité
11. Les cyberactivistes sont des individus ou des groupes qui se livrent à des activités de piratage informatique dans le but de promouvoir un programme social ou politique.
12. Les pirates informatiques adolescents sont des individus dotés de compétences techniques limitées qui s'appuient sur des outils de piratage, des scénarios d'attaque informatique ou des logiciels préexistants pour exécuter des cyberattaques.
13. AI and Cybersecurity: A New Era, Morgan Stanley, 2023
14. Bureau du premier ministre du Canada — Justin Trudeau. Pour un avantage canadien en matière d'intelligence artificielle. 7 avril 2024
15. Ibid.

protéger contre les risques relatifs aux systèmes d'IA avancés ou malveillants.

En résumé, le gouvernement canadien favorise un écosystème qui soutient et accélère la croissance de l'industrie de l'IA. En fournissant des ressources et des infrastructures, il vise à cultiver une offre nationale de solutions d'IA qui peuvent répondre à la demande nationale et internationale. Cette approche stratégique aidera à positionner le Canada comme un chef de file dans le domaine de l'IA et à assurer la compétitivité du pays sur le marché mondial.

Les réglementations strictes en matière de cybersécurité

Dans le sillage de l'avancée de l'infrastructure numérique, le risque de cybercriminalité visant les gouvernements, les organisations et les collectivités a considérablement augmenté[16]. Par conséquent, les gouvernements du monde entier mobilisent activement leurs efforts pour combattre, minimiser et ultimement prévenir les cyberattaques.

Au Canada, le gouvernement fédéral a récemment adopté plusieurs nouvelles lois visant à renforcer les mesures de sécurité pour les industries sous réglementation fédérale et le secteur privé. L'une des avancées notables est le Projet de loi C-26, qui vise précisément à consolider la sécurité dans des secteurs clés tels que la finance, les télécommunications, l'énergie et les transports.

La partie 2 du Projet de loi C-26, connue sous le nom de Loi sur la protection des cyber-systèmes essentiels, est particulièrement importante. Cette loi vise à améliorer le partage d'informations sur les cybermenaces et accorde au gouverneur en conseil (GEC)[17] le pouvoir d'émettre des directives de cybersécurité (DDC)[18]. En vertu de la législation, les opérateurs désignés sont tenus d'agir sur la base des mesures explicitées dans les DDC dans un délai déterminé. Le non-respect d'une DDC peut entraîner des conséquences telles que des sanctions administratives pécuniaires ou des infractions réglementaires, qui peuvent conduire à des amendes ou à une peine d'emprisonnement.

En outre, il est important de noter que les entreprises du secteur privé qui exercent leurs activités en dehors des secteurs réglementés par le gouvernement fédéral sont soumises à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Cette loi établit un ensemble complet de règles et de principes que les organisations doivent suivre pour protéger les renseignements personnels des individus[19]. L'un des principaux objectifs de la LPRPDE est de donner la priorité à la sécurité des renseignements personnels. Pour satisfaire aux exigences de la LPRPDE, les organisations sont obligées de mettre en œuvre diverses mesures de protection pour atténuer les risques potentiels reliés aux données personnelles. Ces risques comprennent la possibilité de perte, de vol, d'accès non autorisé, de divulgation, de copie, d'utilisation ou de modification des renseignements personnels.

En 2022, le gouvernement du Canada a déposé le Projet de loi C-27, la Loi de 2022 sur la mise en œuvre de la Charte numérique, afin de renforcer la loi canadienne sur la protection de la vie privée dans le secteur privé, de créer de nouvelles règles pour le développement et le déploiement responsables de l'intelligence artificielle (IA) et de continuer à faire progresser la mise en œuvre de la Charte numérique du Canada. Ainsi, la Loi de 2022 pour la mise en œuvre de la Charte du numérique introduit trois projets de loi : la Loi sur la protection de la vie privée des consommateurs, la Loi sur l'intelligence artificielle et les données et la Loi sur le Tribunal de la protection des renseignements personnels et des données.

La Loi sur la protection de la vie privée des consommateurs répondra aux besoins des Canadien(ne)s qui dépendent de la technologie numérique et elle tiendra compte des commentaires reçus sur les projets de loi précédents. La Loi sur la protection de la vie privée des consommateurs garantira que la vie privée des Canadien(ne)s sera protégée et que les entreprises innovantes pourront bénéficier des règles claires à mesure que la technologie continue d'évoluer.

Les législations provinciales au Canada imposent également des règles plus strictes en matière de cybersécurité de la collecte, de la communication et du

16. Centre canadien pour la cybersécurité. Centre de la sécurité des télécommunications. Ottawa, Canada
17. Les nominations par le gouverneur en conseil sont faites par le gouverneur général sur l'avis du Conseil privé du Roi pour le Canada (le Cabinet). Les personnes nommées ont des responsabilités allant de la prise de décisions de nature quasi judiciaire à la présentation d'avis et de recommandations reliés aux questions de développement socioéconomique, jusqu'à la gestion des sociétés d'État. Organisations fédérales au Canada.
18. Gouvernement du Canada — Sécurité publique Canada. Protéger les cyber-systèmes essentiels — document d'information. 14 juin 2022
19. Commissariat à la protection de la vie privée du Canada

stockage des renseignements. Au Québec, l'adoption de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (ci-après appelée « Loi 25 »), anciennement connue sous le nom de Projet de loi 64, a entraîné des changements importants pour les organisations qui collectent, communiquent et utilisent des renseignements personnels. S'inspirant en grande partie du « Règlement général sur la protection des données » (RGPD) de l'Europe, cette nouvelle loi provinciale vise à donner plus de droits aux personnes qui partagent leurs renseignements personnels et, en même temps, elle instaure un principe général de transparence.

Sur la scène internationale, les pays accordent de plus en plus d'importance aux règles et réglementations reliées à la cybersécurité, comme le RGPD, la Loi sur la cyber-résilience et les directives NIS au sein de l'Union européenne, ainsi que la Loi générale sur la protection des données au Brésil. Ces réglementations offrent de nouvelles possibilités au secteur canadien de la cybersécurité de fournir des produits et services qui répondent aux exigences de ces marchés. De plus, les certifications et normes industrielles reconnues mondialement, comme la norme ISO 27001, le programme Cyber Essential au Royaume-Uni et la Cybersecurity Maturity Model Certification (CMMC) aux États-Unis, créent de nouvelles possibilités pour les entreprises canadiennes d'aider les organisations à obtenir de telles certifications. En conclusion, le climat actuel des réglementations en matière de cybersécurité présente des possibilités majeures pour les entreprises de cybersécurité. Ces réglementations imposent à certaines catégories d'organisations de mettre en œuvre des mesures pour protéger des catégories précises de données et d'autres renseignements collectés, communiqués et stockés. Cette exigence crée une demande pour les entreprises de cybersécurité, car elles sont bien placées pour fournir les solutions et l'expertise nécessaires en matière de protection des données. En proposant des produits et services conformes aux exigences réglementaires, les entreprises de cybersécurité peuvent capitaliser sur cette possibilité et prospérer sur le marché.

Les tendances ayant une incidence sur l'offre des produits et services de cybersécurité

Les tendances sectorielles suivantes ont une incidence sur l'offre des produits et services de cybersécurité. Ces tendances, notamment les avancées technologiques et l'évolution des cybermenaces, entraînent des répercussions sur les entreprises canadiennes qui exportent des produits de cybersécurité. Les entreprises doivent se tenir au courant des avancées comme l'IA et l'infonuagique pour proposer des solutions de pointe. Le paysage croissant des cybermenaces offre des possibilités d'exportation, mais la concurrence est en train de s'intensifier. Le respect des contrôles à l'exportation est également crucial. Les entreprises canadiennes doivent s'assurer de respecter les réglementations pour être en mesure de réussir sur le marché mondial.

Les progrès technologiques

Le domaine de la cybersécurité a commencé à émerger dans les années 1980 et il a pris de l'importance parallèlement à l'adoption généralisée des ordinateurs personnels. À cette époque, le paysage technologique ne bénéficiait pas de la présence de l'infonuagique et de l'IDO. La cybersécurité s'articulait principalement autour des logiciels antivirus et de pares-feux physiques installés directement à l'intérieur des ordinateurs.

Les programmes antivirus ont été développés à l'origine pour identifier et éliminer les virus informatiques. Cependant, les logiciels antivirus traditionnels n'étaient programmés que pour cibler des virus en particulier, ce qui les rendait inefficaces contre les menaces nouvelles et émergentes jusqu'à ce que les logiciels soient mis à jour. Les pares-feux agissaient comme un bouclier protecteur entre les réseaux internes et externes, surveillant et gérant le trafic réseau entrant et sortant. Néanmoins, les premiers pares-feux avaient des capacités limitées et ils se concentraient principalement sur le filtrage du trafic réseau en fonction des adresses IP (protocole Internet) et des numéros de port.

De nos jours, les progrès technologiques ont révolutionné le domaine de la cybersécurité, entraînant des modifications considérables dans la typologie

des solutions de cybersécurité et leurs complexités. Un exemple notable est l'intégration de l'IA dans les outils de cybersécurité. Les solutions fondées sur l'IA peuvent analyser de vastes quantités de données et identifier des modèles, leur permettant de détecter et de réagir aux menaces en temps réel. De tels outils peuvent apprendre en permanence à partir des nouvelles cybermenaces et ils peuvent adapter leurs mécanismes de défense en conséquence, ce qui les rend très efficaces pour lutter contre les cybermenaces en constante évolution comparativement aux premiers programmes antivirus d'autrefois. Par ailleurs, les avancées en matière de service d'infonuagique ont grandement influencé la catégorie des solutions de cybersécurité disponibles. Les solutions de cybersécurité établies sur l'infonuagique offrent aux entreprises la flexibilité requise pour adapter leurs mesures de sécurité à leurs besoins. Cette flexibilité élimine le besoin d'infrastructure physique sur l'emplacement d'une entreprise et elle permet une gestion plus efficace et plus rentable de la cybersécurité.

L'évolution du paysage des cybermenaces

La tendance croissante à la numérisation a engendré de nombreux avantages, tels qu'une efficacité améliorée et des temps d'intervention plus rapides, comme décrit ci-dessus. Quoiqu'il en soit, la transformation numérique a également élargi les possibilités pour les cybercriminels de lancer des cyberattaques. En raison de l'interconnexion croissante des appareils et des systèmes, les cibles potentielles des cyberattaques se sont multipliées de manière exponentielle. À titre d'exemple, le Forum économique mondial rapporte que la cybercriminalité a coûté aux organisations et aux gouvernements la somme stupéfiante de 11,50 billions de dollars américains à l'échelle mondiale en 2023[20]. Il est choquant de constater que ce chiffre devrait doubler pour atteindre 23 billions de dollars américains d'ici 2027[21].

La prolifération du paysage des cybermenaces a entraîné une augmentation significative du déploiement des produits de cybersécurité sur le marché. Selon Mordor Intelligence, le marché de la cybersécurité devrait atteindre une valeur de 182,84 milliards de dollars américains d'ici 2024[22]. Cette croissance est principalement alimentée par l'abondance des possibilités et des transactions en cours à travers le monde entier. Tandis que les grandes entreprises ont bénéficié de l'avantage d'investir très tôt dans la cybersécurité en raison de leurs ressources, les PME commencent également à reconnaître les avantages connexes aux mesures de sécurité préventives et, par conséquent, le marché de la cybersécurité continuera de croître.

La cybersécurité et le contrôle des exportations

La Loi sur les licences d'exportation et d'importation (LLEI), une législation essentielle au Canada, est une loi qui réglemente la circulation des biens et des technologies à l'intérieur et à l'extérieur du pays[23]. Son objectif principal est de garantir que les entreprises canadiennes se conforment aux accords internationaux, aux mesures de sécurité nationale et aux objectifs de la politique étrangère. En réglementant efficacement les processus d'exportation et d'importation, la LLEI joue un rôle primordial dans la protection des intérêts du Canada et le maintien d'une économie sécuritaire et prospère. La LLEI établit un système de permis qui détaille les marchandises qui doivent recevoir une approbation de permis avant de se lancer dans une activité d'exportation. Ces marchandises sont énumérées dans le Guide de la Liste des marchandises et technologies d'exportation contrôlée du Canada (GLMTECC).

Le GLMTECC ne mentionne pas précisément les produits de cybersécurité. Toutefois, il est important de noter que la Catégorie 5 – Partie 2 du Guide des contrôles à l'exportation Canada est consacrée à la sécurité de l'information[24]. Cette catégorie englobe un large éventail d'articles liés à la sécurité de l'information, notamment les systèmes cryptographiques, les systèmes de communication sécurisés, les systèmes de détection d'intrusion et les outils logiciels pour la sécurité de l'information. En outre, elle couvre les technologies utilisées pour les tests de sécurité de l'information, tels que les outils de test d'intrusion et les outils d'évaluation des vulnérabilités. Il est essentiel pour les entreprises canadiennes de cybersécurité de déterminer si elles sont soumises à cette réglementation et de s'assurer qu'elles ne s'exposent à aucune pénalité en cas de non-conformité.

20. 2023 était une année importante pour la cybercriminalité. Forum économique mondial, 2024
21. Ibid.
22. Analyse de la taille et de la part de marché de la cybersécurité – tendances et prévisions de croissance (2024 à 2029), Mordor Intelligence
23. Gouvernement du Canada. Justice Canada. Lois codifiées du Canada
24. Gouvernement du Canada. Commerce international et investissements

2.2 Secteurs d'activité des membres d'In-Sec-M

En 2024, In-Sec-M a mené une enquête pour recueillir des renseignements au sujet des entreprises canadiennes de cybersécurité, notamment leurs champs de compétence et leurs secteurs d'activité. Cette enquête a été distribuée à tous les membres d'In-Sec-M ainsi qu'aux entreprises non membres à travers le Canada.

Les secteurs d'activité

Sur les 148 entreprises participantes, une majorité significative de 130 (88 %) a indiqué que les PME constituaient un domaine d'intérêt clé pour leurs opérations. Ce résultat met en évidence la demande soutenue de produits et services de cybersécurité au sein du secteur des PME et il souligne les fortes compétences des membres d'In-Sec-M à répondre à de tels besoins.

Le secteur public est apparu comme une autre clientèle importante, avec plus de 70 % des répondants qui ont indiqué qu'ils fournissent des produits et/ou services de cybersécurité aux gouvernements fédéral et provinciaux. De plus, les secteurs de la santé, de la transformation numérique, du commerce électronique et de l'industrie manufacturière ont été identifiés comme des secteurs importants par une majorité de répondants.

Toutefois, les résultats de cette enquête ont également révélé une attention relativement faible accordée aux transports maritimes, aux citoyens canadiens, à la pêche et à l'agriculture. Ces secteurs ont suscité moins d'intérêt parmi les répondants en termes d'orientation commerciale.

Figure 4 :
principaux secteurs d'activité, Enquête d'In-Sec-M sur l'écosystème canadien de la cybersécurité, 2024

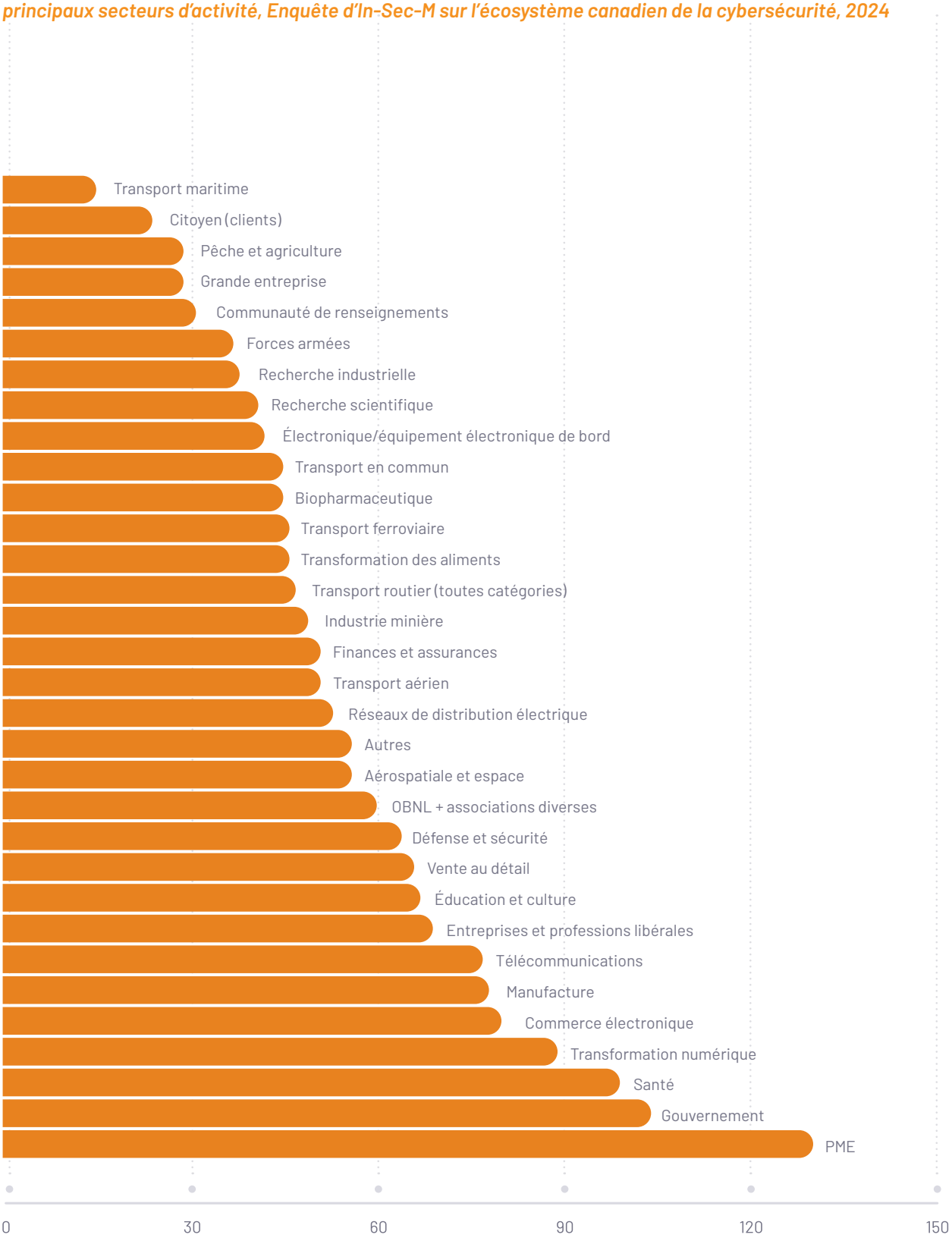


Tableau 4 : principaux secteurs d'activité, Enquête d'In-Sec-M sur l'écosystème canadien de la cybersécurité, 2024

Principaux secteurs d'activité	Nombre de sélections de réponses à l'enquête	% du total des répondants
PME	130	88 %
Gouvernement	104	70 %
Santé	99	67 %
Transformation numérique	89	60 %
Commerce électronique	80	54 %
Industrie manufacturière	78	53 %
Télécommunications	77	52 %
Entreprises et professions libérales	69	47 %
Éducation et culture	67	45 %
Vente au détail	66	45 %
Défense et sécurité	64	43 %
OBNL et associations diverses	60	41 %
Aérospatiale et espace	56	38 %
Autres	56	38 %
Réseaux de distribution électrique	53	36 %
Transport aérien	51	34 %
Finances et assurances	51	34 %
Industrie minière	49	33 %
Transport routier (toutes catégories)	47	32 %
Transformation des aliments	46	31 %
Transport ferroviaire	46	31 %
Biopharmaceutique	45	30 %
Transports en commun	45	30 %
Électronique et équipement électronique de bord	42	28 %
Recherche scientifique	41	28 %
Recherche industrielle	38	26 %
Forces armées	37	25 %
Communauté/service des renseignements	31	21 %
Grande entreprise	29	20 %
Pêche et agriculture	29	20 %
Citoyens (clients)	24	16 %
Transport maritime	15	10 %

La couverture du marché

L'enquête comprenait des questions sur la couverture du marché[25] par les répondants. En examinant les marchés d'Amérique du Nord, d'Amérique centrale et d'Amérique du Sud, il a été observé que plus de la moitié des répondants à l'enquête exportaient leurs produits et/ou services vers les États-Unis. Plus précisément, 31 % (46 répondants) exportaient vers le Mexique et les Caraïbes, tandis que 24 % (36 répondants) exportaient vers l'Amérique centrale et l'Amérique du Sud.

Tableau 5 : couverture des marchés d'Amérique du Nord, d'Amérique centrale et d'Amérique du Sud, Enquête menée par In-Sec-M sur l'écosystème canadien de la cybersécurité, 2024

Marché	Nombre de sélections de réponses à l'enquête	% du total des répondants
États-Unis	88	59 %
Mexique et Caraïbes/Antilles	46	31 %
Amérique centrale et Amérique du Sud	36	24 %

L'Europe apparaît comme un marché important pour les membres d'In-Sec-M. Près de la moitié des répondants (72 répondants = 49 %) ont déclaré exporter leurs produits et/ou services vers la France. Le Royaume-Uni est le deuxième marché européen le plus important parmi les répondants à l'enquête, avec 49 entreprises l'ayant sélectionné comme marché. Les autres marchés européens mentionnés sont l'Italie, l'Espagne, le Benelux et la Scandinavie.

Tableau 6 : couverture du marché européen, Enquête In-Sec-M sur l'écosystème canadien de la cybersécurité, 2024

Marché	Nombre de sélections de réponses à l'enquête	% du total des répondants
Europe — France	72	49 %
Europe — Royaume-Uni	49	33 %
Europe — Benelux	38	26 %
Europe — Espagne	37	25 %
Ailleurs en Europe	37	25 %
Europe — Italie	35	24 %
Europe — Scandinavie	30	20 %

Outre ces régions, d'autres marchés internationaux ont également retenu l'attention. Il a été constaté que 19 % (28 répondants) des personnes interrogées exportaient vers Israël, tandis que 18 % (27 répondants) exportaient vers les marchés du Moyen-Orient. L'Afrique et l'Asie étaient également des marchés importants, avec respectivement 24 % et 20 % des répondants exportant vers ces régions.

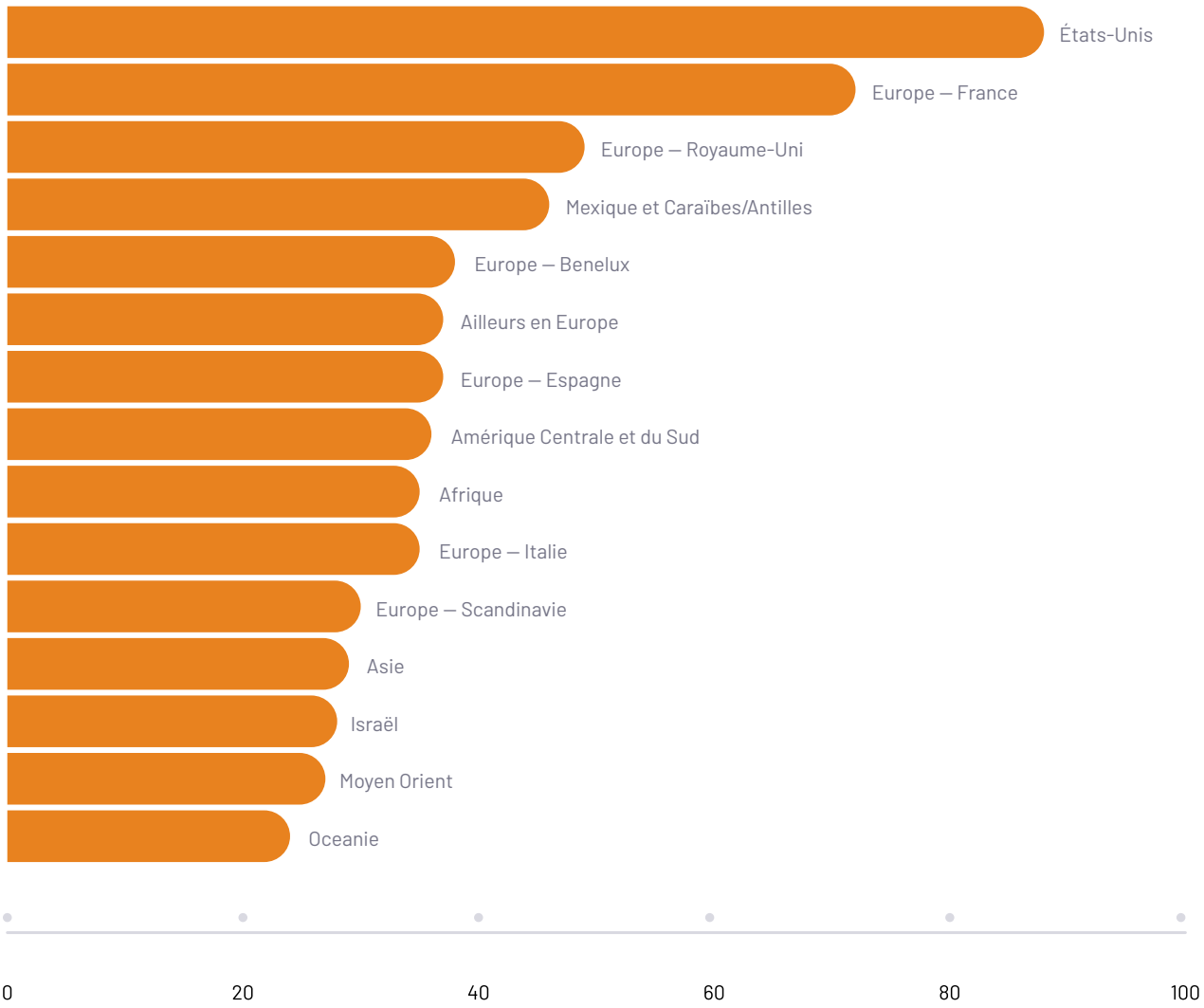
25. Il est important de noter que les répondants à l'enquête ont eu la possibilité de sélectionner plusieurs réponses à cette question. Les répondants ont été invités à indiquer leur couverture du marché. Cependant, la couverture du marché n'implique pas nécessairement la présence physique ou l'emplacement de l'entreprise sur ce marché

Tableau 7 : autres couvertures du marché, Enquête In-Sec-M sur l'écosystème canadien de la cybersécurité, 2024

Marché	Nombre de sélections de réponses à l'enquête	% du total des répondants
Afrique	35	24 %
Asie	29	20 %
Israël	28	19 %
Moyen-Orient	27	18 %
Océanie	24	16 %

Le graphique suivant présente le pourcentage des couvertures du marché parmi les répondants à l'enquête menée par In-Sec-M.

Figure 5 : couvertures du marché, Enquête d'In-Sec-M sur l'écosystème canadien de la cybersécurité, 2024



2.3 Analyse des marchés cibles

L'élaboration d'une stratégie de développement des affaires à l'internationale commence par l'évaluation et la sélection des marchés cibles. La section suivante présente la méthodologie et les perspectives de la recherche résultant du processus de sélection et d'évaluation.

La méthodologie

Sur la base des recherches sectorielles, des entretiens avec les parties prenantes, des rapports de mission antérieurs d'In-Sec-M et des résultats d'enquêtes menées auprès des membres d'In-Sec-M, une liste complète de pays a été établie pour être pris en compte dans l'analyse des marchés cibles. Ces pays ont été mentionnés dans de nombreuses sources d'information et ils sont considérés comme des marchés cibles potentiels. La liste initiale comprend :

- **Les marchés d'Amérique du Nord, d'Amérique centrale et d'Amérique du Sud :** Mexique et Brésil.
- **Le marché européen :** Royaume-Uni, Allemagne, France, Benelux (Belgique, Pays-Bas et Luxembourg), Espagne, Italie et Suisse.
- **Le marché asiatique :** Singapour.

Il est important de noter que même si d'autres pays et régions ont été mentionnés dans les sources, ils n'ont pas été pris en compte en raison d'un manque général d'informations et de données comparatives. Ces pays comprenaient l'Inde, la Malaisie, le Japon et l'Afrique du Sud. Cela ne signifie pas qu'ils ne présentent pas de possibilités d'affaires pour les exportations canadiennes de produits et services de cybersécurité. Le secteur mondial de la cybersécurité en pleine croissance pourrait donner lieu, dans l'avenir, à l'émergence de possibilités d'affaires dans ces pays en question. Par conséquent, il est recommandé à In-Sec-M et à ses membres de continuer à surveiller les possibilités d'exportation vers ces pays et autres régions.

Il convient aussi de remarquer que l'objectif de cette Stratégie de développement des affaires à l'international, conçu par In-Sec-M, est de diversifier les exportations canadiennes de produits et services de cybersécurité. De par ce fait, les États-Unis, qui sont le plus important partenaire commercial du Canada dans ce secteur, ont été exclus de la sélection des marchés cibles potentiels. Néanmoins, les données et de nombreux intervenants ont mis en évidence des possibilités de renforcer les relations commerciales avec les États-Unis, en tirant parti des liens solides existants entre les deux pays. Par conséquent, bien que les États-Unis ne soient pas inclus dans cette analyse, il est recommandé aux entreprises canadiennes et à In-Sec-M de continuer à explorer et à exploiter de nouvelles possibilités commerciales internationales entre le Canada et les États-Unis.

Les pays et régions présélectionnés ont été évalués afin de comprendre les caractéristiques de leurs marchés et les possibilités d'affaires pour les futures exportations canadiennes. L'analyse s'est concentrée sur les domaines suivants :

- **Taille et croissance du marché** : informations sur la taille économique du marché cible potentiel, la taille de son secteur des TIC et/ou de la cybersécurité, et toute initiative majeure relative à la cybersécurité.
- **Entrée sur le marché :** évaluation de la facilité et du coût de faire des affaires, y compris les moyens d'entrée sur le marché et le coût d'entrée sur le marché à l'intérieur des marchés cibles potentiels.
- **Concurrence sur le marché :** évaluation de la concurrence sur les marchés potentiels afin d'identifier les possibilités d'exportation canadiennes. Une concurrence accrue peut entraîner moins de possibilités pour les nouveaux entrants.
- **Possibilités d'affaires :** identification des secteurs cibles précis et de catégories d'entreprises sur les marchés cibles potentiels qui recherchent activement des produits et services de cybersécurité. Ces possibilités peuvent servir de points d'entrée sur les marchés cibles pour les entreprises canadiennes.
- **Risques et défis :** examen des risques potentiels pour les exportations canadiennes, y compris les risques réglementaires et la sensibilité politique autour de la cybersécurité.
- **Renseignements sur les entrevues avec les parties prenantes :** inclusion d'informations supplémentaires recueillies lors des entrevues avec les parties prenantes.
- **Renseignements sur les missions d'In-Sec-M :** inclusion d'informations supplémentaires recueillies lors des missions internationales antérieures d'In-Sec-M.

Les hypothèses et les limites

Pour les exigences de la présente étude, la sélection des marchés cibles repose sur une combinaison de sources de recherche primaires et secondaires.

La recherche primaire comprenait l'engagement des parties prenantes et les avis d'experts de Deloitte. La recherche secondaire consistait en des recherches en ligne, des rapports provenant des missions antérieures conduites par In-Sec-M et des résultats obtenus grâces aux enquêtes. On suppose que ces sources fournissent un aperçu complet des marchés cibles potentiels, de leurs possibilités d'affaires et de leurs défis.

Toutefois, il peut y avoir des limites dans certains cas où les informations sont limitées ou manquantes. Cela peut être dû à une recherche primaire incomplète, par exemple : une demande d'entretien refusée par les parties prenantes, ou à des informations limitées dans la recherche secondaire. La section suivante met en évidence ces limites.

Les marches cibles potentiels

Les renseignements recueillis pour chacun des dix (10) marchés cibles potentiels ont été agrégés. Les principales conclusions et résumés pour chaque marché sont fournis ci-dessous.

Mexique

SURVOL DU MARCHÉ

Le Mexique est la deuxième économie d'Amérique latine et il se classe au 15e rang mondial. Malgré des défis tels que la crise pétrolière de 2019 et la récession mondiale de 2020 causée par la COVID-19, le Mexique a affiché une croissance économique stable avec une tendance à la reprise après la pandémie. En 2022 et 2023, la croissance économique du Mexique a dépassé 3 %. Le pays a connu une croissance significative de la numérisation, ce qui le rend plus vulnérable aux cyberattaques. Le Mexique est le pays le plus attaqué en Amérique latine par les rançongiciels et il a connu une augmentation de 93 % des attaques de logiciels malveillants en 2020. En particulier, le secteur financier mexicain a été ciblé, avec 56 % des attaques de logiciels malveillants et 47 % des attaques d'hameçonnage[26]. Dans la dernière Enquête menée par In-Sec-M auprès des entreprises de cybersécurité, sur 148 répondants, 46 (31 %) d'entre eux exportent des produits et services de cybersécurité vers le Mexique et les Caraïbes/Antilles.

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

La culture d'entreprise mexicaine valorise la communication en face à face pour évaluer le caractère, la fiabilité et la compatibilité des partenaires potentiels. L'Accord Canada–États-Unis–Mexique (ACEUM) renforce les liens économiques du Canada avec les États-Unis et le Mexique. Au cours des cinq dernières années, les entreprises mexicaines sont devenues des acteurs importants du secteur des technologies de l'information, se classant parmi les 20 premiers fournisseurs de services au monde. Le secteur mexicain de la cybersécurité se concentre sur la sécurité des données, la gouvernance et la conformité, la sécurité des services infonuagiques, la détection et la prévention, ainsi que l'intervention face aux cyber-incidents et la criminalistique informatique. Les principales entreprises de cybersécurité au Mexique sont Scitum, Arame et KUI Networks.[27]

POSSIBILITÉS D'AFFAIRES

Le secteur bancaire et financier au Mexique présente des possibilités pour les produits et services de cybersécurité. Les institutions financières investissent davantage dans la technologie et l'innovation pour prévenir et répondre aux activités frauduleuses. En 2021, les banques mexicaines ont augmenté leurs investissements dans la technologie et l'innovation de 20,8 % par rapport à 2020 et de 35 % par rapport à la période prépandémique.[28]

RISQUES ET DÉFIS

L'un des principaux défis du secteur des TIC au Mexique est l'influence des entités monopolistiques qui entravent les réformes requises. La corruption perçue dans les marchés publics du secteur des TIC aux niveaux fédéral, étatique et municipal constitue également un obstacle pour les entreprises étrangères. Le Mexique ne dispose pas d'une loi précisément axée sur la cybersécurité, bien qu'il existe des réglementations sur les crimes financiers, la sécurité de l'information et les délits relatifs aux technologies.[29] [30]

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Les entretiens avec les parties prenantes confirment que le Mexique présente une possibilité importante d'affaires en raison de sa vulnérabilité face aux attaques de cybersécurité durant ces dernières années. Les entreprises mexicaines recherchent activement des services et des solutions de cybersécurité pour faire face aux nouvelles cyberattaques et les prévenir.

26. Aperçu de la cybersécurité au Mexique, Bureau économique d'Israël au Mexique
27. Ibid.
28. Ibid.
29. Ibid.
30. The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment (csis.org)

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale au Mexique, menée par In-Sec-M en mars 2024, a révélé que :

- L'écosystème mexicain de cybersécurité en est encore à ses débuts, avec une faible maturité en termes de structures de cybersécurité. Bien qu'il existe un besoin évident de services de cybersécurité, les organisations mexicaines n'ont pas fait de l'investissement dans ce domaine une priorité.
- La présence d'entreprises de cybersécurité américaines bien établies au Mexique pose un défi aux fournisseurs canadiens. Ces entreprises américaines ont déjà acquis une part de marché importante au Mexique, ce qui rend difficile la pénétration du marché par les entreprises canadiennes.
- Il existe une différence de culture d'entreprise entre le Canada et le Mexique, ce dernier nécessitant un investissement de temps considérable pour les entreprises souhaitant entrer sur le marché mexicain. Cela contraste avec le Canada, les États-Unis et certains grands marchés occidentaux où les processus d'entrée peuvent être plus fluides et plus rapides.
- Les structures mexicaines démontrent un intérêt relativement faible pour l'expertise canadienne en cybersécurité. Quoiqu'il en soit, cette difficulté peut être surmontée grâce aux efforts à long terme des représentants canadiens sur le terrain, en établissant des relations et en valorisant l'expertise canadienne.
- Les PME mexicaines en sont aux premières étapes de leur transformation numérique et elles devront relever des défis substantiels pour améliorer leurs compétences en matière de cybersécurité dans les années à venir. Cela représente une possibilité de marché potentielle pour les entreprises canadiennes qui peuvent offrir des produits et des services adaptés aux besoins et aux prix de ce marché.
- Les partenariats technologiques ont été un moyen efficace de pénétrer les marchés étrangers, mais au Mexique, l'écosystème d'innovation en cybersécurité est déjà dominé par les structures américaines. Cette domination américaine suggère que les entreprises canadiennes pourraient avoir besoin d'explorer des stratégies alternatives pour s'implanter sur le marché mexicain.

Brésil

SURVOL DU MARCHÉ

Le Brésil, huitième économie mondiale et État le plus peuplé d'Amérique du Sud, a réalisé des progrès considérables en matière de numérisation nationale. Le pays compte la cinquième plus grande base d'utilisateurs d'Internet au monde et il est un pays leader en Amérique du Sud en termes d'utilisation des TIC. La Stratégie nationale de cybersécurité du Brésil (E-Ciber) trace les actions stratégiques visant à renforcer la cyber-résilience et la coopération internationale. Le pays reste engagé en faveur de solutions multilatérales et participe activement à des événements et exercices conjoints de cyber-résilience.[31]

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

L'établissement d'un bureau local ou l'établissement d'un partenariat avec un représentant local de confiance est primordial pour réussir sur le marché brésilien. La communication en face à face et le soutien local sont très appréciés par les entreprises brésiliennes. Le marché des télécommunications au Brésil est compétitif et privilégie la collaboration avec des fournisseurs locaux. Les entreprises canadiennes devraient envisager des engagements et des partenariats à long terme pour s'y retrouver dans le système juridique et réglementaire complexe du Brésil.[32]

POSSIBILITÉS D'AFFAIRES

Le secteur de la technologie financière offre des possibilités d'affaires, les banques brésiliennes investissant dans de nouvelles technologies pour soutenir les services de la technologie financières. Il existe une demande en matière de cybersécurité, de services bancaires mobiles et en ligne, d'intelligence artificielle, d'analyse de données, d'IDO, de chaîne de bloc et de services infonuagiques. Au cours de la prochaine décennie, le potentiel de revenus générés par les entreprises de technologie financière au Brésil devrait atteindre 24 milliards de livres sterling (équivalent à environ 41 milliards de dollars canadiens en unité monétaire de 2024). [33]

31. Brazil: EU Cyber Direct
32. Gouvernement du Canada. Services des délégués commerciaux
33. Exporting guide to Brazil—great.gov.uk—great.gov.uk

RISQUES ET DÉFIS

Pour les clients qui sont des organismes fédéraux et étatiques chargés de l'application de la loi au Brésil, leurs exigences en matière d'importation de produits et services de cybersécurité impliquent l'obtention préalable de licences d'importation et du certificat d'importation international (CII) des forces armées brésiliennes. L'actuel gouvernement au Brésil n'a pas donné la priorité à la stratégie cybernétique, ce qui peut avoir un impact sur le développement du secteur de la cybersécurité.[34] [35]

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Aucun renseignement supplémentaire sur les entretiens n'est disponible.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale au Brésil, dirigée par In-Sec-M en Février 2024, a dévoilé que :

- Le marché des services-conseils au Brésil est déjà bien desservi par les entreprises brésiliennes et les grandes sociétés internationales. Cela indique que les entreprises de services-conseils pourraient être confrontées à une forte concurrence sur le marché.
- La mise en œuvre de la LGPD (loi brésilienne sur la protection des données) en 2020 a engendré une demande des services de soutien à la conformité. Les avocats spécialisés dans ce secteur pourraient être intéressés par un partenariat avec des experts étrangers en cybersécurité qui sont capables de fournir des solutions de cybersécurité avancées répondant aux exigences particulières de la LGPD.
- Le Brésil dispose d'un vaste marché pour la protection des renseignements personnels, marché motivé en partie par les mesures prises pour répondre aux besoins de sécurité physique. Par exemple, les données biométriques et les cartes d'identité sont collectées dans les copropriétés et les immeubles de bureaux.
- Le secteur de la santé au Brésil est à la traîne en matière de cybersécurité, malgré un nombre important de Brésiliens disposant d'une assurance privée. Le secteur de la vente au détail représente également une possibilité de marché substantielle en raison de la grande démographie (population nombreuse) du Brésil et de la croissance de son économie.
- Le secteur bancaire brésilien a adopté la transformation numérique et il est à la pointe de la technologie financière. Les grandes institutions bancaires sont intéressées à travailler avec des entreprises canadiennes et à acquérir des solutions canadiennes, notamment dans les solutions de cybersécurité fondées sur l'IA ou l'expertise quantique. Le secteur des télécommunications présente également des possibilités d'affaires potentielles.
- Les secteurs minier et pétrolier de la région de Rio de Janeiro pourraient intéresser les fournisseurs de solutions IDO. Dans le secteur de la défense, il est recommandé d'avoir un partenaire local pour répondre aux appels d'offres gouvernementaux, et les deux cyber-entreprises acquises par Embraer pourraient être essentielles pour entrer sur ce marché.
- Il existe une demande de services de formation et de sensibilisation à la cybersécurité dans tous les secteurs, demande stimulée par des techniques avancées de piratage psychologique au Brésil. En particulier, le secteur bancaire est préoccupé par le nombre de fraudes bancaires qui sont effectuées à travers le pays.
- Les partenariats technologiques, comme par le biais des appels de propositions Canada-Brésil (EMBRAPII), peuvent être une stratégie de pénétration du marché, surtout dans les secteurs où les fournisseurs de services actuels possèdent une expertise de pointe.
- La vente directe de solutions de cybersécurité depuis le Canada est possible si des solutions comparables ne sont pas disponibles au Brésil. Néanmoins, il est généralement préférable de trouver un distributeur, un représentant commercial ou un représentant légal au Brésil en raison de facteurs tels que les responsabilités légales, la facilitation des paiements et la nécessité de communiquer en portugais pour les transactions commerciales.

34. Brazil—Safety and Security (trade.gov)
35. Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible—Carnegie Endowment for International Peace

United Kingdom

SURVOL DU MARCHÉ

Le marché de la cybersécurité au Royaume-Uni a connu une croissance remarquable, avec un chiffre d'affaires annuel total atteignant 10,1 milliards de livres sterling en 2021 (équivalent à environ 17 milliards de dollars canadiens en unité monétaire de 2024), soit une augmentation de 14 % par rapport à l'année précédente. Il existe actuellement 1 838 entreprises actives fournissant des produits et services de cybersécurité au Royaume-Uni. Le gouvernement britannique a activement soutenu la croissance du secteur de la cybersécurité par l'intermédiaire de diverses initiatives, notamment des investissements directs, un soutien aux compétences et aux professions, et des investissements dans les régions et les pôles technologiques.[36] Dans la dernière enquête d'In-Sec-M auprès des entreprises de cybersécurité, sur 148 répondants canadiens, 49 (33 %) d'entre eux exportent des produits et services de cybersécurité vers le Royaume-Uni.

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

Les entreprises qui souhaitent pénétrer le marché britannique de la cybersécurité doivent être bien informées sur les réglementations en matière d'approvisionnement et de stockage des données, qui seront au cœur des négociations sur les ententes commerciales. Le marché britannique est très concurrentiel, avec un grand nombre d'entreprises opérant dans le secteur de la cybersécurité. [37] [38]

POSSIBILITÉS D'AFFAIRES

Grandes entreprises : la majorité du marché de la cybersécurité au Royaume-Uni gravite autour des grandes entreprises commerciales, notamment dans les secteurs des services financiers, des services publics et des transports.

Secteur public : les gouvernements central et locaux du Royaume-Uni investissent massivement dans la sécurisation des données confidentielles dans les domaines de la santé et de l'éducation, ainsi que dans les services en ligne tels que le crédit universel.

Défense et sécurité (D&S) : le marché de la D&S au Royaume-Uni se concentre sur la sécurisation des secrets nationaux et implique les agences de sécurité et de renseignement, ainsi que le ministère de la Défense (les Forces armées britanniques).

PME : de nombreuses PME au Royaume-Uni ne disposent pas de mesures de cybersécurité suffisantes, ce qui les rend vulnérables aux cybermenaces. Le gouvernement encourage les PME à adopter des normes d'hygiène informatique de base, et certains contrats de marchés publics exigent des exigences minimales de cybersécurité pour les chaînes d'approvisionnement. [39]

RISQUES ET DÉFIS

Bien que le marché britannique de la sécurité informatique soit ouvert aux entreprises nord-américaines, il existe des réglementations britanniques précises que les entreprises doivent connaître, notamment la Loi sur la protection des données, la Réglementation sur la confidentialité et les communications électroniques, la Loi sur la liberté d'information et la Réglementation sur les informations environnementales. L'observance conforme à de telles réglementations est essentiel pour opérer sur le marché britannique. [40]

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Les entretiens avec les parties prenantes ont mentionné que le Royaume-Uni a toujours été un marché favorable pour les entreprises canadiennes, offrant ainsi des possibilités de collaboration et d'expansion.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale au Royaume-Uni, conduite par In-Sec-M en Février 2024, a démontré que :

- Le Royaume-Uni est connu pour investir massivement dans l'innovation, notamment dans le secteur de la cybersécurité. Les incubateurs et les accélérateurs du Royaume-Uni soutiennent le développement de solutions de pointe. Le gouvernement a également soutenu la croissance des incubateurs par le biais d'initiatives publiques-privées.
- Le Royaume-Uni attire des travailleurs de haut niveau du monde entier et il abrite de nombreux investisseurs en capital de risque (ICR) et sources d'investissement privé. Le système d'enseignement postsecondaire réputé et

36. Market insights for exporting cyber security to United Kingdom | Market search tool
37. Market insights for exporting cyber security to United Kingdom | Market search tool
38. Cyber security sectoral analysis 2022—GOV.UK (www.gov.uk)
39. export.gov
40. export.gov

le marché concurrentiel font du Royaume-Uni une destination attrayante pour les entreprises de cybersécurité.

- Les pôles de cybersécurité reconnus au Royaume-Uni sont concentrés à Londres, Belfast, Manchester et Cheltenham. Le pôle technologique de Belfast, qui a été construit à l'origine autour de la Queen's University Belfast, s'est positionné comme un pionnier de la cybersécurité. Il abrite des recherches de classe mondiale, attire des entreprises multinationales et propose des programmes de formation accélérée de la main-d'œuvre. L'écosystème de Belfast vise à se positionner comme une passerelle vers les marchés européens et britanniques, à l'instar du Luxembourg pour l'Europe et de Singapour pour l'Asie. Les faibles taux d'imposition sur les sociétés et la présence de grandes sociétés multinationales spécialisées dans la cybersécurité ont incité les entreprises à établir leur siège social à Belfast. Toutefois, le tissu économique local manque de PME.
- Les entreprises canadiennes peuvent avoir des possibilités d'affaires dans le secteur de la cybersécurité au Royaume-Uni en raison du fait que le Canada fait partie de l'alliance de renseignements Five Eyes. Le secteur de la défense, notamment des organisations comme DSTL, est intéressé par des solutions canadiennes ciblées. Parmi les autres sous-secteurs d'intérêt figurent les assurances et la protection des infrastructures essentielles, comme la finance et les centrales nucléaires.
- Au Royaume-Uni, les appels d'offres pour les contrats du gouvernement central nécessitent souvent l'obtention de la certification Cyber Essentials ou Cyber Essentials Plus. Cette certification contribue à la cyber-résilience de l'économie britannique et soutient la santé financière de l'industrie locale de la cybersécurité. Le National Cyber Security Centre joue un rôle sine qua non dans cette initiative.

Germany

SURVOL DU MARCHÉ

Le marché allemand de la cybersécurité est l'un de ceux qui connaît la croissance la plus rapide en Europe, juste derrière la France. En 2021, les dépenses relatives à la sécurité informatique en Allemagne ont atteint 6,2 milliards d'euros (équivalent à environ 9,1 milliards de dollars canadiens en unité monétaire de 2024), soit une augmentation notable de 9,7 % par rapport à l'année précédente. Cette croissance est due à l'emphase mise par le pays sur la cybersécurité en tant que priorité absolue du gouvernement, avec la publication de plusieurs stratégies nationales de cybersécurité depuis 2011. La dernière stratégie de l'Allemagne, publiée en septembre 2021, s'appuie sur les précédentes et elle souligne l'importance de la cybersécurité dans le paysage numérique. [41]

En tant que plus grande économie d'Europe, l'Allemagne est une république fédérale constituée avec autonomie considérable accordée à ses 16 États fédéraux (Länders). Cette autonomie a entraîné une répartition inégale de la demande, du savoir-faire et des possibilités de marché en matière de cybersécurité à travers le pays. Certains États, comme la Bavière, ont été plus proactifs que d'autres dans le domaine de la cybersécurité. Par conséquent, les entreprises qui cherchent à pénétrer le marché allemand doivent tenir compte de ces variations régionales.

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

Les entreprises allemandes ont tendance à être conservatrices et elles hésitent souvent à faire confiance à des entreprises étrangères inconnues. Dans certains cas, une présence locale est légalement requise et généralement souhaitable pour soumettre des offres ou rejoindre des communautés locales spécialisées en cybersécurité. En outre, l'Allemagne a des ambitions d'indépendance technologique et la communauté de la cybersécurité, en particulier dans la recherche et le développement, reconnaît la nécessité de solutions TIC nationales. Cette focalisation sur les entreprises locales en démarrage peut réduire les possibilités d'affaires pour les entreprises et les technologies étrangères.

Afin de surmonter les barrières de confiance et de conservatisme, il est recommandé de s'associer à une partie prenante allemande, tel qu'un sous-traitant principal, un intégrateur de systèmes ou un revendeur à valeur ajoutée. Ces partenaires peuvent fournir un service après-vente en allemand et se conformer aux exigences de disponibilité. De plus, il existe un nombre croissant d'entreprises allemandes en démarrage spécialisées dans le domaine de la cybersécurité, ce qui intensifie la concurrence locale. [42]

POSSIBILITÉS D'AFFAIRES

Le marché allemand de la cybersécurité offre deux principales possibilités d'affaires :

41. Gouvernement du Canada. Services des délégués commerciaux
42. Ibid.

La cybersécurité pour les PME : le tissu économique allemand repose en grande partie sur les PME, également appelées Mittelstand. De telles PME, souvent des leaders mondiaux dans leurs domaines respectifs, peuvent avoir été réticentes à investir dans de nouveaux outils et politiques pour améliorer la sécurité de leurs systèmes TIC. La protection de leurs systèmes est une priorité absolue pour la continuité des activités et pour rester compétitives et innovantes. La sécurité des réseaux, la conformité, la gestion des identités et des accès (GIA) et la sécurité en tant que service (SecaaS) sont identifiées comme des priorités absolues pour les PME afin de se prémunir contre les cybermenaces.

La numérisation des services et du secteur public : la numérisation des services et du secteur public est un point clé de l'ordre du jour de la politique allemande. Bien que les progrès aient été lents, la pandémie de COVID-19 a mis en évidence les déficits numériques du pays, ce qui a donné lieu à de nouvelles initiatives. Cela présente d'importantes possibilités de marché pour le matériel informatique et les logiciels reliés à la cybersécurité. [43]

RISQUES ET DÉFIS

Tandis que l'Allemagne offre des possibilités d'affaires aux fournisseurs de technologies avancées et de haute qualité dans le secteur industriel, il est important de noter que l'environnement réglementaire évolue rapidement. Les changements peuvent survenir soudainement et le respect des réglementations est crucial. Les Lois sur la sécurité informatique 1.0 et 2.0 servent de cadre juridique à l'Allemagne pour la mise en œuvre de la Directive NIS de l'UE. La Loi 2.0, entrée en vigueur au mois de mai 2018, a donné un nouvel élan au secteur allemand de la cybersécurité, en particulier pour les infrastructures essentielles. Elle oblige les entreprises engagées dans les infrastructures essentielles à prendre des mesures de sécurité appropriées et impose des amendes conséquentes en cas de non-respect. La loi accorde également plus de pouvoirs à l'Office fédéral de la sécurité de l'information (BSI). [44]

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Aucune information supplémentaire n'est fournie dans les entretiens avec les parties prenantes pour l'Allemagne.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale en Allemagne, conduite par In-Sec-M en octobre 2023, a révélé que :

- L'écosystème allemand de la cybersécurité est complexe et fragmenté car il manque d'une direction claire et centralisée. Les entreprises privées ont beaucoup d'autonomie et d'influence sur le marché.
- L'écosystème allemand de la cybersécurité est décrit comme très complexe et techniquement avancé. Les entreprises canadiennes qui entrent sur ce marché doivent être prêtes à faire face à une concurrence féroce de la part d'acteurs locaux très compétents.
- L'état d'esprit général des entreprises en Allemagne est souvent comparable à celui des Américains — direct et avec peu de procrastination. Cet état d'esprit peut influencer les interactions commerciales et les processus décisionnels.
- La langue peut être un obstacle important pour les entreprises exportatrices canadiennes, en particulier lorsqu'elles ciblent les PME. Il est essentiel pour les entreprises non germanophones d'avoir des employés qui parlent et écrivent l'allemand pour naviguer efficacement sur le marché.
- IT-SA, un événement important dans le domaine de la cybersécurité en Europe, donne un aperçu de la taille du marché allemand de la cybersécurité, qui est de loin le plus grand d'Europe.

France

SURVOL DU MARCHÉ

Le marché français de la cybersécurité est dynamique et mature, générant 13,4 milliards d'euros de revenus en 2021 (équivalent à environ 19,8 milliards de dollars canadiens en unité monétaire de 2024). Le marché français a connu un taux de croissance de 6,4 % entre 2019 et 2020 et employait 69 200 personnes. Les acteurs étrangers, principalement des israéliens et des américains, représentaient 30 à 40 % du marché de la cybersécurité, y compris les services cybernétiques. Le gouvernement français a mis en place un cadre de soutien solide pour stimuler le développe-

43. Ibid.
44. Ibid.

ment du secteur de la cybersécurité et positionner les acteurs français comme des leaders mondiaux. La France a adopté une stratégie clé en 2011 pour devenir un leader mondial de la cyberdéfense, préserver la souveraineté nationale, renforcer la cybersécurité des infrastructures essentielles et assurer la sécurité dans le cyberespace. Le marché devrait continuer à s'agrandir à un rythme d'environ 6 % entre 2021 et 2026, avec une augmentation des dépenses en cybersécurité motivée par la conformité aux normes du Règlement général sur la protection des données (RGPD). [45]

Dans la dernière enquête d'In-Sec-M auprès des entreprises de cybersécurité, sur 148 répondants canadien, 72 (49 %) d'entre elles exportent des produits et services de cybersécurité vers la France.

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

Pour pénétrer le marché français, il est indispensable de réseauter et de nouer des relations personnelles. Des communautés professionnelles et des associations commerciales actives peuvent contribuer à faire connaître vos produits/services auprès des clients français. La participation à des événements, des concours, des pôles d'innovation, des incubateurs d'entreprises en démarrage et des événements phares comme le Forum InCyber (anciennement connu sous le nom de Forum international de la cybersécurité, ou FIC) et les Assises de la cybersécurité peuvent servir de point d'entrée dans l'écosystème français de la cybersécurité. Il est recommandé de sélectionner un distributeur local ou un revendeur à valeur ajoutée (RVA) disposant de réseaux pertinents, tels qu'Orange Cyberdéfense, Sopra Steria, Atos ou Capgemini. Le marché français demeure fragmenté avec des collaborations et des partenariats stratégiques qui sont tissés pour accroître la présence sur le marché et développer de nouveaux produits et services. [46]

POSSIBILITÉS D'AFFAIRES

Le marché français de la cybersécurité offre des possibilités d'affaires dans différents secteurs :

- **Banque, finance et assurances** : ce secteur représente 17 % du marché.
- **Défense et sécurité** : environ 12 % du marché est consacré à la défense et à la sécurité.
- **Industrie** : le secteur industriel représente 11 % du marché.
- **Secteur public** : environ 10 % du marché est dédié au secteur public.
- **Informatique et numérique** : ce secteur représente 9 % du marché.
- **Aérospatial** : environ 7 % du marché est consacré à l'industrie aérospatiale.
- **Transports** : le secteur des transports représente 6 % du marché.
- **Énergie et environnement** : environ 6 % du marché est consacré aux secteurs de l'énergie et de l'environnement.

Le grand nombre de clients existants et potentiels dans le domaine de la cybersécurité, en particulier les PME, offre une possibilité pour les solutions de cybersécurité de pénétrer sur le marché français. Cette tendance s'est accélérée avec la pandémie de la COVID-19. [47]

RISQUES ET DÉFIS

Bien qu'il offre des possibilités, le marché français de la cybersécurité est très réglementé. Le respect des réglementations est primordia, et il est fondamental de rester informé au sujet de l'évolution de l'environnement réglementaire.

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Les renseignements sur les entretiens avec les parties prenantes suggèrent que la France est considérée comme un marché viable en raison de sa réputation historique de marché digne de confiance et de la présence de la diaspora française vivant au Canada. Ces facteurs peuvent faciliter l'entrée sur le marché et l'établissement de relations commerciales.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale en France, menée par In-Sec-M en 2023 et en 2024, a dévoilé que :

- In-Sec-M possède une connaissance et une expérience approfondies du marché français de la cybersécurité, avec des réseaux établis et des contacts de haut niveau au sein de l'écosystème. Ces réseaux comprennent des

45. Gouvernement du Canada. Services des délégués commerciaux.
46. Ibid.
47. Ibid.

industriels, des associations, des universitaires et des autorités gouvernementales et de cybersécurité.

- L'accès au marché français pour les entreprises canadiennes qui vendent des produits et services de cybersécurité pourrait être difficile, car certaines organisations françaises du secteur public, et les grands groupes industriels français ont tendance à privilégier les solutions nationales en affichant divers niveaux de préférence nationale. L'État français n'envisagera des solutions étrangères que si des options françaises équivalentes ne sont pas disponibles.
- Les exportateurs peuvent être confrontés à une concurrence féroce de la part des entreprises françaises de cybersécurité en termes de compétence technologique. Les entreprises françaises sont connues pour leur expertise et leur innovation dans le domaine, ce qui en fait un marché compétitif pour les acteurs internationaux.
- La France fonctionne à partir d'une culture d'entreprise fondée sur le réseautage. Faire des affaires en France peut être complexe, frustrant et infructueux pour ceux qui n'ont pas de connexions établies au sein des réseaux français. La création et l'exploitation de ces réseaux sont essentielles pour réussir.
- In-Sec-M a signé une Entente de partenariat avec le Pôle d'Excellence Cyber durant sa mission commerciale en Bretagne. Cette Entente de partenariat offre aux entreprises canadiennes un accès privilégié aux acteurs clés de l'écosystème français.

Benelux

(Belgique, Pays-Bas et Luxembourg)

SURVOL DU MARCHÉ

La région du Benelux, composée de la Belgique, des Pays-Bas et du Luxembourg, offre un potentiel sur le marché de la cybersécurité. Le Luxembourg se classe au 11e rang mondial dans l'Indice mondial de la cybersécurité (IMC), ce qui souligne son engagement en matière de cybersécurité et ses meilleures pratiques dans les domaines techniques et de renforcement des capacités. Les Pays-Bas sont présentés comme la porte d'entrée numérique vers l'Europe et disposent d'une robuste économie alimentée par l'Internet. [48] La Belgique reconnaît les cybermenaces comme l'un des foyers de risques les plus importants et elle a mis en œuvre une stratégie de cybersécurité.[49]

Dans la dernière enquête d'In-Sec-M auprès des entreprises de cybersécurité, sur 148 répondants canadiens, 38 (26 %) d'entre eux exportent des produits et services de cybersécurité vers le Benelux.

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

Concernant les Pays-Bas, les entreprises étrangères, notamment américaines, s'implantent souvent au Royaume-Uni avant de pénétrer le marché néerlandais. Le marché néerlandais a l'avantage d'être un pays précoce dans l'adoption des nouvelles technologies. [50] L'étude n'a pas identifié des conditions particulières d'entrée sur le marché ni des recommandations précises pour pénétrer le marché belge et luxembourgeois. Les pratiques d'entrée sur le marché de ces deux pays sont comparables à celles des autres marchés européens.

POSSIBILITÉS D'AFFAIRES

En Belgique, le secteur de la cybersécurité et de la protection des données est ouvert aux acteurs extérieurs. Les entreprises belges ont tendance à externaliser leurs besoins en cybersécurité auprès d'autres homologues de l'UE, ce qui crée des possibilités pour les fournisseurs externes. Il existe également un besoin de PME préparées et un manque de personnel qualifié.[51] Bruxelles abrite également de nombreuses organisations internationales, ce qui crée des possibilités pour une approche paneuropéenne de l'entrée sur le marché.

L'offre de cybersécurité du Luxembourg se caractérise par l'implication d'entreprises informatiques traditionnelles et d'entreprises du secteur bancaire, des services financiers et des assurances (BSFA). Les petites entreprises jouent un rôle important et les possibilités de marché pour les solutions européennes émergentes restent ouvertes.[52]

Les Pays-Bas disposent des possibilités similaires à celles d'autres pays avancés et hautement numérisés. Le marché néerlandais est réceptif aux nouvelles technologies, ce qui en fait une cible attrayante pour les entreprises étrangères.[53]

48. Netherlands—Cyber Security (trade.gov)
49. The European Cybersecurity Market, Enterprise Ireland
50. Netherlands—Cyber Security (trade.gov)
51. Belgium—Market Challenges (trade.gov)
52. Luxembourg Cybersecurity Ecosystem, Cybersecurity Luxembourg
53. Netherlands—Cyber Security (trade.gov)

RISQUES ET DÉFIS

Les pays du Benelux ont chacun leur propre identité économique et leur propre culture d'entreprise. Ils bénéficient néanmoins d'un État de droit fort, d'une protection des droits de la propriété intellectuelle et d'une application transparente des contrats, ce qui crée un environnement commercial favorable.

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Les renseignements à propos des entretiens avec les parties prenantes suggèrent que les Pays-Bas ont toujours été un marché favorable pour les entreprises canadiennes. Cette réputation historique peut faciliter l'entrée sur le marché et l'établissement des relations commerciales.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale au Benelux, organisée par In-Sec-M en octobre 2023, a révélé que :

- Dans les années à venir aux Pays-Bas, il pourrait être intéressant de travailler à inviter des représentants de l'industrie canadienne à prendre la parole lors de la One Conference (sur invitation uniquement), qui est une bonne tribune pour démontrer l'excellence de l'industrie canadienne à un groupe restreint de représentants.
- Au Luxembourg, le gouvernement a choisi de se concentrer sur une économie numérique robuste et les quelques secteurs stratégiques et de pointe qui vont de pair, dans un environnement où tous les acteurs agissent de manière concertée et diligente. Le territoire est petit, il est relativement facile de se connecter avec tous les acteurs pertinents de son secteur d'activité, et la société luxembourgeoise a les moyens de ses ambitions. Le Luxembourg « gère » la cybersécurité de manière diligente car le ministère de l'Économie est en contact direct avec le House of Cybersecurity, qui est le premier point de contact avec l'industrie, et le Cybersecurity Board coordonne les acteurs des différents ministères.
- En plus du secteur financier, qui intéresse fortement les fournisseurs de solutions et services canadiens ciblant particulièrement les services financiers — notamment avec la réglementation DORA — le Luxembourg est une porte d'entrée attrayante vers le marché européen, et il se positionne ouvertement comme tel. L'accompagnement proposé aux entreprises étrangères est particulièrement important et de qualité.
- Les entreprises luxembourgeoises de cybersécurité ont développé leur offre pour les grands clients, comme les banques, alors que les besoins des PME luxembourgeoises et européennes augmentent, et les entreprises canadiennes de cybersécurité ont développé une expertise dans les solutions et services adaptés à cette clientèle.
- Le Centre interdisciplinaire pour la sécurité, la fiabilité et la confiance de l'Université du Luxembourg a lancé en novembre 2023 son CyberHub qui bénéficiera de 3,5 millions d'euros par année. Ils disposent d'un programme d'accélération, offrent des services de modérateur aux entreprises souhaitant accéder au marché européen, et un appui technique aux entreprises établissant leur siège social au Luxembourg.
- Concernant la Belgique, des organisations en particulier offrent d'excellentes possibilités pour rencontrer des acheteurs majeurs et développer des partenariats technologiques potentiels en vue de pénétrer le marché européen.
- Outre les relations bilatérales avec la Belgique, et le marché belge plus précisément, la création de partenariats stratégiques avec des organisations paneuropéennes ayant leur siège à Bruxelles pour contribuer à faire entendre la voix des PME canadiennes au sein des comités de normalisation, par exemple, pourrait profiter à l'industrie canadienne en termes d'interopérabilité, d'influence sur la demande future et d'informations privilégiées pour adapter l'offre en conséquence.
- Un accès privilégié aux acheteurs, investisseurs et partenaires européens potentiels, par le biais d'alliances avec des organisations paneuropéennes ciblées, peut également être une stratégie pour accroître les exportations canadiennes et maintenir l'excellence de son écosystème d'innovation.
- Il est nécessaire de renforcer les relations entre la délégation conjointe du Canada auprès de l'OTAN et l'industrie canadienne pour contribuer plus efficacement aux cyberdéfenses des alliés.

Espagne

SURVOL DU MARCHÉ

Le marché espagnol offre d'importantes possibilités pour les produits et services de cybersécurité en raison du dynamisme du paysage commercial du pays et de sa transformation numérique en cours. Le programme Next Generation EU a injecté des investissements substantiels dans l'économie espagnole, en mettant l'accent sur la numérisation par le biais du Plan national de relance et de résilience. Le plan alloue une part substantielle de son budget à la transformation numérique, y compris aux initiatives de cybersécurité. Le secteur espagnol des TIC est très avancé, avec des investissements importants dans les infrastructures et la connectivité.[54]

Dans la dernière enquête d'In-Sec-M auprès des entreprises de cybersécurité, sur 148 répondants canadiens, 37 (25 %) d'entre eux exportent des produits et services de cybersécurité vers l'Espagne.

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

Le gouvernement espagnol a mis en place des mesures pour attirer les entreprises et les investissements étrangers, en assouplissant la réglementation et en offrant des incitations. Les rencontres en face à face et les relations personnelles sont très appréciées dans la culture d'entreprise espagnole, d'où l'importance d'établir un contact direct avec les représentants locaux. La maîtrise de la langue espagnole est recommandée, car les cadres locaux maîtrisent relativement peu l'anglais. De grandes entreprises internationales, dont IBM, Microsoft, HP, Google Cloud et Amazon, ont choisi l'Espagne pour leurs centres de recherche et développement, et leurs centres de données. [55] [56] [57]

POSSIBILITÉS D'AFFAIRES

Aucun secteur en particulier n'est identifié dans la recherche.

RISQUES ET DÉFIS

L'Espagne dispose d'un cadre juridique complet en matière de cybersécurité, notamment des lois sur la protection des données et des législations visant à protéger les infrastructures essentielles et les communications électroniques. Le respect de ces réglementations est obligatoire pour les entreprises opérant sur le marché espagnol.

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Aucun renseignement supplémentaire issu des entretiens n'est fourni.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission d'In-Sec-M en Espagne, durant le mois de février 2024, dans le but d'assister à une conférence (MWC Barcelona) a permis de constater que :

› Le MWC Barcelona est un événement important qui rassemble les principaux acteurs du secteur des télécommunications du monde entier. Il offre l'occasion à des organisations comme In-Sec-M d'identifier les acteurs clés et d'établir des liens. De nombreux pays du monde entier ont des pavillons lors d'un tel événement.

Italie

SURVOL DU MARCHÉ

Le marché de la cybersécurité en Italie a connu une croissance notable, avec une valeur marchande de 2,1 milliards USD en 2022 (équivalent à environ 2,9 milliards USD en unité monétaire de 2024), ce qui représente une augmentation de 18 % par rapport à l'année précédente. Le gouvernement italien a reconnu l'importance de la cybersécurité et a mis en œuvre des stratégies pour faciliter les investissements en R&D et augmenter les niveaux de culture numérique. Les grandes entreprises sont les moteurs du marché de la cybersécurité, les secteurs financier/bancaire et des services publics étant les principaux utilisateurs finaux. Pourtant, de nombreuses PME ne sont toujours pas préparées à faire face à des cybermenaces croissantes.[58]

54. Gouvernement du Canada. Services des délégués commerciaux
55. Information and Communications Technologies (ICT) market in Spain (wedc.org)
56. Spain: Cybersecurity | Insights | DataGuidance
57. Spain—Market Entry Strategy (trade.gov)
58. The Italian Cyber Security Market 2019, Ibs Italia

Dans la dernière enquête d'In-Sec-M auprès des entreprises de cybersécurité, sur 148 répondants canadiens, 35 (24 %) d'entre eux exportent des produits et services de cybersécurité vers l'Italie.

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

Les entreprises qui s'implantent sur le marché italien doivent s'assurer que leurs accords de distribution, de franchise et d'agence sont conformes aux lois européennes et italiennes. De nombreuses entreprises étrangères ont établi leurs propres organisations de vente en Italie, tandis que d'autres travaillent avec des importateurs ou des agents commerciaux spécialisés. Il est courant que les entreprises italiennes bien établies préfèrent des accords exclusifs.[59]

POSSIBILITÉS D'AFFAIRES

L'Italie est un marché intéressant pour le Canada dans le domaine de la cybersécurité, avec un potentiel de collaboration et de synergie entre les deux pays. Les innovations disruptives et les infrastructures numériques — tels que les services infonuagiques, la gestion des incidents de sécurité et de confidentialité, l'IDO et les mégadonnées — offrent des possibilités de collaboration. Les secteurs clés pour les solutions de cybersécurité comprennent le gouvernement, la défense, l'énergie, les médias et la technologie, les transports, la finance et l'automobile.[60]

RISQUES ET DÉFIS

Pas de risque ni de défi identifié.

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Aucun renseignement supplémentaire provenant des entretiens n'est fourni.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale en Italie, menée par In-Sec-M en novembre 2023, a dévoilé que :

- La présence d'In-Sec-M à Cybertech Europe a facilité les échanges directs avec les responsables de la cybersécurité des grands groupes industriels italiens, favorisant les connexions entre les clients européens et les fournisseurs de solutions canadiens. Cet événement a attiré des délégations et des entreprises internationales intéressées par l'expansion de leurs marchés en Italie et en Europe.
- L'Italie recherche activement des solutions technologiques de pointe en matière de cybersécurité, mais les considérations budgétaires restent une priorité. Les exportateurs canadiens qui entrent sur ce marché devraient en tenir compte lors du positionnement de leurs offres.
- L'Italie suscite un vif intérêt pour l'expertise canadienne en matière de distribution de clés quantiques (DCQ). Cela représente une possibilité pour les exportateurs canadiens de répondre à cette demande.

Suisse

SURVOL DU MARCHÉ

La Suisse est connue pour son innovation, ses entreprises compétitives et ses excellentes universités, ce qui en fait un pays de premier plan en matière d'innovation. Le pays dispose d'une infrastructure bien établie, d'une sécurité juridique et d'un système politique équilibré. Une stratégie nationale de protection de la Suisse contre les cyber-risques a été élaborée en 2012, fournissant un cadre pour lutter plus efficacement contre les cybermenaces. Les entreprises suisses se tournent de plus en plus vers les services de cybersécurité gérés en raison de la pénurie de main-d'œuvre qualifiée dans le secteur de la cybersécurité et du rythme rapide des cycles d'innovation dans la cyberdéfense.[61]

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

La Suisse et le Canada partagent des intérêts et des valeurs communs dans la lutte contre les cybermenaces. Les deux pays disposent de structures fédérales, de sociétés multilingues et d'économies de marché ouvertes qui encouragent le commerce et les investissements. Les échanges commerciaux bilatéraux entre la Suisse et le Canada sont régis par un accord de libre-échange. La Suisse fait partie des principaux investisseurs étrangers au Canada

59. Italy—Cybersecurity (trade.gov)
60. The Italian Cyber Security Market 2019, Ibs Italia
61. Cyber Security Market Study— Switzerland & Liechtenstein, Canada Trade Commissioner Services

et la coopération économique entre les deux pays est importante. Les atouts de la Suisse, notamment sa neutralité, sa sécurité juridique et sa stabilité politique, sont également évidents dans le secteur de la cybersécurité. De nombreuses organisations internationales choisissent la Suisse comme lieu idéal pour leurs centres de données régionaux. [62]

POSSIBILITÉS D'AFFAIRES

La sécurité des réseaux est un domaine important sur le marché suisse de la cybersécurité. Le pays est reconnu comme un centre d'expertise en matière de gouvernance de l'Internet et un pourcentage important des activités Internet mondiales sont domiciliées en Suisse. Le secteur financier en Suisse et au Liechtenstein considère les données et la propriété intellectuelle comme des actifs d'entreprise importants, ce qui crée des possibilités dans le domaine de la sécurité et du traitement des données. Parmi les autres possibilités d'affaires potentielles dans le secteur des TIC figurent l'externalisation suisse des services informatiques, l'informatique sociale, l'optimisation des processus et la cybersécurité des données.[63]

RISQUES ET DÉFIS

Le système juridique suisse est conservateur dans la mise en œuvre de la législation pertinente à la cybercriminalité. De nouvelles lois sont introduites lorsque les lois et mécanismes conventionnels ne parviennent pas à lutter efficacement contre la cybercriminalité.

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Aucun renseignement supplémentaire n'est disponible au sujet des entretiens.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale en Suisse, conduite par In-Sec-M en octobre 2023, a permis de découvrir que :

- La Suisse dispose d'un marché immense avec une forte demande de solutions de pointe pour la cyber-protection des réseaux, des communications et des infrastructures financières. Cela présente des possibilités d'affaires pour les entreprises canadiennes du secteur de la cybersécurité.
- Les organismes de développement économique régionaux montrent un grand intérêt à développer des liens opérationnels avec le Canada, notamment avec le Québec en raison de la langue commune — le français. La Suisse a mis en place des programmes pour accueillir et soutenir les entreprises étrangères qui cherchent à s'implanter dans le pays.
- La Suisse a une forte demande en technologies de confiance numérique et d'identité numérique, offrant des possibilités aux entreprises canadiennes ayant une expertise de pointe dans ces domaines.
- La Suisse accorde la priorité à l'accueil d'entreprises technologiques innovatrices, et de nombreux programmes de soutien sont disponibles pour ces entreprises. Cela démontre l'engagement du pays à favoriser l'innovation et à attirer les entreprises étrangères dans le secteur technologique.
- De nombreux médiateurs d'affaires suisses estiment que la Suisse est un point d'entrée presque parfait pour les entreprises canadiennes qui cherchent à pénétrer le marché européen dans son ensemble. La position géographique centrale de la Suisse, sa capacité à faire des affaires dans plusieurs langues (anglais, français, allemand et italien), sa stabilité économique, son régime fiscal avantageux et son accès à une expertise de pointe en font une destination attrayante pour les entreprises canadiennes.

Singapour

SURVOL DU MARCHÉ

Le marché de la cybersécurité à Singapour connaît une augmentation spectaculaire des cybermenaces, avec une hausse de 145 % des cyberattaques en 2021 par rapport à l'année précédente. Les rançongiciels et le vol des données sont les catégories d'attaques les plus courantes. Le coût moyen d'une violation de cybersécurité à Singapour est le plus élevé de la région Asie-Pacifique. En 2022, le pays a connu une augmentation des incidents

62. Ibid.
63. Ibid.

d'hameçonnage, de rançongiciels, d'infrastructures infectées et de dégradations de sites Web. Singapour offre un environnement favorable au secteur de la cybersécurité, avec le soutien du gouvernement et un cadre réglementaire solide.[64]

ENTRÉE SUR LE MARCHÉ ET CONCURRENCE

Le Cyber Security Agency (CSA) encourage la croissance du secteur de la cybersécurité à Singapour en soutenant les capacités avancées de recherche et d'ingénierie. La CSA collabore avec le Economic Development Board (EDB) pour tirer parti du climat favorable aux entreprises et de la main-d'œuvre qualifiée de Singapour. Singapour abrite de nombreuses organisations de cybersécurité de premier plan, et la CSA, en collaboration avec Infocomm Media Development Authority, soutient la création d'un pôle d'incubation d'entreprises de démarrage en cybersécurité.[65]

POSSIBILITÉS D'AFFAIRES

Singapour offre un marché de la cybersécurité vaste et compétitif, au service des entreprises locales et multinationales. Les principales possibilités du marché comprennent la gestion des identités et des accès, la sécurité avancée des terminaux, des réseaux et de l'infonuagique, la gestion des cybermenaces et des vulnérabilités, la sécurité SCI et SCADA, les informations sur les infrastructures essentielles, l'intelligence artificielle, l'analyse et la protection des données, l'IDO, la chaîne de bloc, la technologie des registres distribués et la cryptographie/informatique quantique.[66]

RISQUES ET DÉFIS

Le gouvernement de Singapour offre un environnement favorable au secteur de la cybersécurité, avec un soutien et des cadres réglementaires et juridiques pertinents. Cependant, le marché est très concurrentiel et il peut être difficile d'y pénétrer. Le marché est réceptif aux solutions innovantes, mais les produits redondants peuvent rencontrer des difficultés.

RENSEIGNEMENTS SUR LES ENTRETIENS AVEC LES PARTIES PRENANTES

Les renseignements glanés à partir des entretiens avec les parties prenantes soulignent la force de Singapour, l'un des plus grands marchés de la cybersécurité en Asie. Néanmoins, le marché est très concurrentiel et il peut être difficile d'y pénétrer. Le marché singapourien privilégie les solutions innovantes aux produits redondants.

RETOMBÉES DE LA MISSION INTERNATIONALE CONDUITE PAR IN-SEC-M

La mission internationale à Singapour, dirigée par In-Sec-M en novembre 2023, a révélé que :

- La mission exploratoire a permis de mieux comprendre l'écosystème complexe et mature de la cybersécurité à Singapour. Elle a permis d'identifier les principaux acteurs locaux nécessaires à la réussite sur le marché.
- Le niveau d'expertise technique des acteurs existants à Singapour est très élevé. Cela indique que le marché est réservé aux fournisseurs de solutions dotés d'une expertise de pointe et d'une capacité avérée à rivaliser dans un environnement hautement concurrentiel, où opèrent les meilleurs fournisseurs de cybersécurité au monde.
- Singapour démontre un fort intérêt pour l'innovation étrangère et a une approche accueillante pour l'intégration des jeunes entreprises en démarrage et des entreprises innovantrices dans les programmes existants. Cela représente une voie prometteuse pour les entreprises canadiennes qui cherchent à pénétrer le marché singapourien. Singapour est considéré comme une porte d'entrée vers les marchés de l'Asie-Pacifique.

64. Singapore Cybersecurity Market (trade.gov)
65. Ibid.
66. Ibid.

Les priorités de développement

Les marchés présélectionnés, comme indiqué ci-dessus, ont été classés en groupes particuliers en fonction de leurs priorités en matière de développement futur des exportations. Le processus de priorisation a principalement pris en compte l'expérience passée d'In-Sec-M dans les visites de ces marchés cibles, ainsi que les résultats de recherche supplémentaires évoqués dans la section précédente. Il a également pris en compte les compétences du Canada et les possibilités d'affaires présentes sur les marchés cibles, ainsi que les informations recueillies lors des entretiens.

Les marchés hautement prioritaires

Les pays et régions énumérés ci-dessous ont été classés comme marchés hautement prioritaires qui devraient être la priorité à court terme (1 an) pour explorer de nouvelles possibilités d'exportation et/ou renforcer les partenariats d'exportation existants. Ces pays et régions présentent un potentiel important pour l'exportation de produits de cybersécurité du Canada.

Marchés hautement prioritaires	Secteurs des possibilités d'affaires
Royaume-Uni	› Finance › Santé › Défense et Sécurité › Vente au détail et PME › Énergies et services publics › Éducation
France	› Banque, finance et assurances › Santé › Défense et Sécurité › Vente au détail et PME › Industrie › Secteur public › Aérospatial et transports › Énergie et environnement
Suisse	› Réseaux et télécommunications › Santé › Industrie › Energie et secteur public › Transports et logistique › Banque, finance et assurances

Les marchés moyennement prioritaires

Les pays et régions suivants sont considérés comme des marchés moyennement prioritaires qui devraient faire l'objet d'une attention particulière à moyen terme (1 à 3 ans) alors que le Canada continue de diversifier ses exportations de produits et services de cybersécurité. Ces pays et marchés présentent des possibilités, mais ils peuvent également imposer des incertitudes ou des risques/défis. Pour certains marchés, l'entrée sur le marché pourrait prendre du temps et nécessiter la construction des relations.

Marchés moyennement prioritaires	Secteurs des possibilités d'affaires
Mexique	› Banque, finance et assurances › PME › Transports et logistique › Énergie › Secteur publique
Brésil	› Banque, finance et assurances › Santé › Mines et énergie › Agriculture › Vente au détail et PME › Transports et logistique › Industrie
Allemagne	› Banque, finance et assurances › Santé › Gouvernement, défense et sécurité › Énergie › Secteur manufacturier et industrie › Transports et logistique › Secteur publique › PME
Benelux	› Banque, finance et assurances › Transports et logistique › Défense et sécurité › Secteur publique › Vente au détail et PME › Industrie automobile
Italie	› Banque, finance et assurances › Industrie automobile › Transports et logistique › Défense et sécurité › Télécommunications › Énergies et services publics › Santé
Singapour	› Finance, technologie financière et banque › Santé › Gouvernement et secteur public › Transports et logistique › Énergie › Télécommunications › Industrie et secteur manufacturier › Défense et sécurité

Les considérations pour l'avenir

L'Espagne n'est actuellement pas répertoriée comme un marché prioritaire ou de priorité moyenne en raison du manque d'informations tout au long de l'exercice de recherche. Cependant, il est recommandé de continuer à recueillir et à surveiller les informations et, chaque fois que les possibilités le permettent, d'examiner plus en détail les possibilités d'affaire en Espagne. Bien que les pays suivants — Inde, Malaisie, Japon et Afrique du Sud — aient été mentionnés dans l'une des multiples sources d'information utilisées au cours du processus de recherche et d'entretien avec les parties prenantes, ils n'ont pas été inclus dans l'analyse présélectionnée ci-dessus. Toutefois, il est recommandé de surveiller de près ces pays en vue d'une éventuelle prise en compte dans l'avenir.

Les recommandations

Les analyses de marché et les priorités présentées ci-dessus peuvent être utilisées par In-Sec-M et les entreprises canadiennes du secteur de la cybersécurité pour envisager leur future diversification des exportations. Étant donné que différentes entreprises peuvent démontrer des forces et des compétences différentes, la priorité du marché au niveau de chaque entreprise doit être soigneusement évaluée. Néanmoins, les analyses de marché décrites ci-dessus fournit des informations complètes à prendre en considération.

Alors que ce rapport est en cours de préparation, des activités d'engagement international sont activement poursuivies et menées par In-Sec-M. Par conséquent, à mesure que de nouvelles informations et de nouveaux renseignements sont reçus, les recommandations ci-dessus doivent être revues en permanence et actualisées régulièrement.

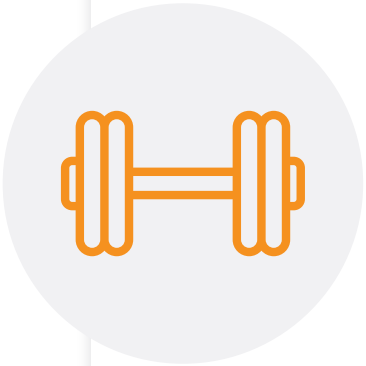
Il convient également de noter que l'objectif de cette étude est de diversifier les exportations canadiennes de produits et de services de cybersécurité, et que les marchés présélectionnés présentés ci-dessus ont été choisis en fonction d'un agrégat de plusieurs sources d'information. Certains marchés qui ont déjà établi de solides relations commerciales avec l'industrie canadienne de la cybersécurité ne sont pas inclus dans cette analyse, mais cela ne signifie pas que les exportations futures ne doivent pas se concentrer sur ces marchés. Les entreprises canadiennes devraient continuer à tirer parti de leurs partenariats existants sur ces marchés. De plus, l'exploration de nouveaux marchés reste une activité importante pour le développement des marchés. In-Sec-M et les entreprises canadiennes du secteur devraient rechercher activement de nouvelles possibilités de développement de marché.

Stratégie de développement des affaires à l'international

Dans cette section, les résultats de l'analyse sectorielle et de l'analyse du marché cible ont été regroupés pour fournir une analyse complète des FFPM. Cette analyse sert de base à l'établissement d'objectifs stratégiques et à l'élaboration d'un plan d'action détaillé pour In-Sec-M et les entreprises canadiennes dans leurs efforts pour diversifier leurs exportations dans le secteur de la cybersécurité. En identifiant les forces, les faiblesses, les possibilités et les menaces, cette analyse FFPM guidera la formulation de stratégies et d'actions efficaces pour capitaliser sur le potentiel du marché et surmonter les défis. Grâce à une approche ciblée, In-Sec-M et les entreprises canadiennes peuvent tirer parti de leurs forces, remédier à leurs faiblesses, saisir les possibilités et atténuer les menaces pour étendre avec succès leur présence sur les marchés internationaux.

3.1 Analyse des FFPM

L'analyse suivante des FFPM résume les forces, les faiblesses, les possibilités et les menaces identifiées dans l'analyse sectorielle et la sélection des marchés cibles.



Les forces

- In-Sec-M a fait preuve de leadership dans le secteur canadien de la cybersécurité grâce à ses objectifs organisationnels ambitieux, à ses missions commerciales internationales, et à la vaste gamme de services offerts à l'industrie.
- Le secteur canadien de la cybersécurité a affiché une croissance robuste en termes de revenus, de création d'emplois et de PIB au cours des dernières années, ce qui indique des tendances positives.
- L'industrie canadienne de la cybersécurité possède de solides capacités en matière de fourniture de services et de solutions d'infrastructure de cybersécurité, ce qui pourrait être avantageux sur les marchés étrangers et auprès des clients dont l'infrastructure est déficiente.
- Les entreprises canadiennes font preuve d'un engagement robuste pour servir les PME et le secteur public. Les secteurs de la santé, du commerce électronique et de l'industrie manufacturière sont également des clients importants des entreprises canadiennes de cybersécurité.

Les faiblesses

- Certains sous-secteurs de l'industrie de la cybersécurité canadienne n'ont pas connu de croissance. Entre 2020 et 2022, des secteurs comme le chiffrement/cryptage, les systèmes de contrôle industriel (ICS), les systèmes SCADA et les technologies opérationnelles (TO) ont connu une baisse de leurs ventes.
- Plus de 70 % des exportations canadiennes de produits et services de cybersécurité sont destinées aux États-Unis, ce qui indique un partenariat commercial solide, mais révèle également un manque de diversification des exportations.

Les possibilités

- La présente étude a permis d'identifier plusieurs conférences internationales majeures sur la cybersécurité qui pourraient offrir aux entreprises canadiennes des occasions d'accroître la notoriété de leur marque et d'explorer d'éventuelles possibilités d'exportation.
- Les tendances socioéconomiques mondiales entraînent une demande amplifiée de produits et de services de cybersécurité. Ces tendances comprennent la numérisation croissante dans tous les secteurs, les nouveaux défis découlant de la pandémie et l'adoption croissante de l'IA.
- Les tendances au sein du secteur de la cybersécurité offrent aux entreprises canadiennes des occasions d'innover et d'améliorer leurs capacités. Ces tendances comprennent l'évolution rapide de la technologie et la complexité croissante des cybermenaces.
- Des possibilités de diversification des exportations potentielles existent sur les marchés suivants : Amérique du Nord, Amérique centrale et Amérique du Sud (Mexique et Brésil), Europe (Royaume-Uni, Allemagne, France, Benelux (Belgique, Pays-Bas, Luxembourg), Espagne, Italie et Suisse et Asie (Singapour).

Les menaces

- À l'échelle internationale, plusieurs pays imposent des réglementations plus strictes en matière de souveraineté des données, ce qui pourrait avoir des répercussions sur les fournisseurs de solutions internationales, augmenter les coûts d'entrée sur le marché et entraîner des risques géopolitiques.
- Les contrôles à l'exportation dans certains pays pourraient également constituer une menace pour l'exportation canadienne de produits et services de cybersécurité.
- Sur certains marchés cibles, bien que la demande en matière de cybersécurité augmente, elle peut ne pas être une priorité absolue pour les entreprises et/ou le gouvernement.
- Certains marchés cibles sont caractérisés par une forte concurrence et l'entrée sur le marché peut être difficile, car il faut du temps pour construire des relations, des partenariats et des solutions de haute qualité et à prix compétitifs pour réussir.
- En raison des différences culturelles et environnementales, les entreprises canadiennes qui cherchent à diversifier leurs marchés doivent développer une compréhension de leurs marchés cibles, et elles peuvent bénéficier d'informations et de conseils d'experts et d'organisations sectorielles.

3.2 Objectifs stratégiques

Bien que l'expansion internationale comporte des risques et des défis, tels que les problèmes réglementaires et les fluctuations monétaires, l'expansion sur les marchés internationaux peut offrir aux entreprises des possibilités de croissance importantes et des avantages stratégiques. Ces potentiels de croissance et ces bénéfices stratégiques incluent généralement :

1. **La croissance du chiffre d'affaires :**
les marchés internationaux offrent de nouvelles perspectives de clientèle, ce qui peut conduire à une augmentation des ventes et du chiffre d'affaires.

2. **La diversification :**
entreprendre des affaires dans plusieurs pays peut aider les entreprises à réduire les risques en diversifiant leurs sources de revenus et en minimisant l'impact des ralentissements économiques sur un marché unique.

3. **L'accès aux ressources :**
les entreprises peuvent s'étendre à l'international pour accéder à des ressources telles que des matières premières, une main-d'œuvre qualifiée ou une expertise technologique qui peuvent être rares ou coûteuses dans leur pays d'origine.

4. **L'avantage concurrentiel :**
l'expansion mondiale peut offrir aux entreprises un avantage concurrentiel en leur permettant de proposer des produits ou des services uniques, de profiter de coûts de production plus faibles ou d'accéder à de nouveaux canaux de distribution.

5. **La saturation du marché :**
les entreprises peuvent s'étendre à l'international lorsque leur marché intérieur est saturé, offrant ainsi des possibilités de croissance.

6. **Les économies d'échelle :**
opérer sur plusieurs marchés peut conduire à des économies d'échelle, permettant aux entreprises de réduire les coûts de production et d'augmenter l'efficacité.

7. **Le développement de l'image de marque :**
l'expansion internationale peut aider les entreprises à renforcer leur présence et leur réputation à l'échelle mondiale.

8. **Les partenariats stratégiques :**
les entreprises peuvent étendre leurs activités à l'international pour former des partenariats stratégiques avec des entreprises étrangères, leur permettant ainsi d'accéder à de nouveaux marchés ou à de nouvelles technologies.

Pour les entreprises canadiennes du secteur de la cybersécurité, la diversification des exportations commence par l'identification des objectifs stratégiques globaux. Les quatre objectifs stratégiques suivants ont émergé de la recherche et de l'engagement des parties prenantes.

Objectifs stratégiques

#1

Améliorer la notoriété et la réputation du secteur canadien de la cybersécurité à l'échelle mondiale

Améliorer la notoriété et la réputation du secteur canadien de la cybersécurité à l'échelle mondiale est primordial pour sa réussite à l'échelle internationale. Afin d'y parvenir, il faut combiner des initiatives de marketing, un leadership éclairé et la démonstration d'une expertise dans la gestion des menaces de cybersécurité. La participation à des forums internationaux sur la cybersécurité, la publication d'articles de recherche et la présentation d'études de cas réussies peuvent positionner le Canada comme un chef de file dans le domaine. En outre, s'assurer que les produits et services canadiens de cybersécurité répondent aux normes mondiales les plus élevées peut améliorer la réputation du secteur en matière de qualité et de fiabilité. L'objectif est de faire du secteur canadien de la cybersécurité une priorité pour les organisations du monde entier qui recherchent des solutions robustes de cybersécurité.

#2

Établir des alliances et des partenariats stratégiques mondiaux pour le secteur canadien de la cybersécurité

L'établissement d'alliances et de partenariats stratégiques peut aider les entreprises canadiennes de cybersécurité à étendre leur portée mondiale et à accéder plus efficacement à de nouveaux marchés. Ces partenariats peuvent être conclus avec des entreprises technologiques locales, des entités gouvernementales ou même des universités sur les marchés cibles. De telles alliances peuvent offrir de précieuses informations sur les marchés locaux, faciliter la conformité réglementaire et fournir une clientèle plus établie. De plus, les partenariats peuvent mener à l'innovation collaborative, aidant ainsi les entreprises canadiennes à rester à l'avant-garde de la technologie de la cybersécurité. L'objectif est de construire un réseau d'alliances pouvant fournir une plate-forme solide pour la croissance internationale du secteur canadien de la cybersécurité.

#3

Renforcer la présence des entreprises canadiennes de cybersécurité sur les marchés cibles

Pour renforcer la présence des entreprises canadiennes de cybersécurité sur les marchés cibles, il ne suffit pas de vendre des produits et des services. Il faut également établir des relations solides avec les clients locaux, comprendre leurs besoins particuliers et leur fournir des solutions sur mesure. Cela peut se faire par le biais de plusieurs canaux, tels que des bureaux ou des représentants locaux, des activités d'engagement client et des campagnes de marketing localisées. Il est important de noter que différents pays peuvent exiger des méthodes différentes en raison des disparités culturelles et commerciales, ainsi que du niveau de pénétration du marché. Par ailleurs, offrir un excellent service à la clientèle, et une aide logistique dans la langue locale et conformément aux normes culturelles locales peut améliorer la satisfaction et la fidélité des clients. L'objectif est de faire des entreprises canadiennes de cybersécurité le choix préféré des clients sur les marchés cibles.

#4

Maximiser la pénétration du marché et explorer de nouvelles possibilités de marché

En plus des objectifs stratégiques susmentionnés, il est important de continuer à accroître la présence et la pénétration des entreprises canadiennes de cybersécurité sur les marchés déjà bien desservis ou sur les marchés qui ont établi de solides partenariats commerciaux avec l'industrie canadienne de la cybersécurité, tout en explorant simultanément de nouvelles opportunités de marché. Cet objectif vise à tirer parti des relations et des partenariats existants pour renforcer davantage la part de marché et la génération de revenus, tout en se diversifiant dans des marchés inexploités pour attirer de nouveaux clients et accroître la portée globale du marché.

3.3 Plan d'action tactique

Le tableau d'actions tactiques suivant présente les actions potentielles qu'In-Sec-M pourrait envisager afin de mettre en œuvre la présente Stratégie de développement des affaires à l'international, de progresser vers les objectifs stratégiques, et de diversifier les exportations canadiennes de produits et services de cybersécurité.

Strategic Objectives

#1

Améliorer la notoriété et la réputation du secteur canadien de la cybersécurité à l'échelle mondiale

Action	Description	Chronologie
1.1	Mettre en valeur et présenter les produits et services canadiens de cybersécurité aux acheteurs potentiels lors d'événements et de conférences internationaux de l'industrie sur des marchés cibles potentiels.	En cours
1.2	Amplifier la visibilité des exportateurs canadiens auprès des principaux acheteurs sur les marchés cibles potentiels grâce à la collaboration avec les entités locales, les représentants diplomatiques et les délégués commerciaux du Canada.	En cours
1.3	Actualiser les tactiques de marketing et de marque existantes et développer des stratégies supplémentaires complètes qui valorisent les forces et les compétences du secteur canadien de la cybersécurité.	À court terme
1.4	Exploiter les plateformes numériques (comme la publicité en ligne et les vidéos promotionnelles) pour accroître la visibilité et la portée mondiales des produits et services de cybersécurité canadiens.	À moyen terme

#2

Établir des alliances et des partenariats stratégiques mondiaux pour le secteur canadien de la cybersécurité

Action	Description	Chronologie
2.1	Organiser un événement de réseautage entre le Canada et les marchés cibles potentiels lors de conférences internationales de l'industrie de la cybersécurité.	Sur demande
2.2	Planifier des réunions avec des associations de cybersécurité et des partenaires privés sur des marchés cibles potentiels afin d'intégrer des solutions technologiques canadiennes dans les portefeuilles de cybersécurité existants.	Sur demande
2.3	Continuer à solliciter les commentaires des membres d'In-Sec-M par le biais des canaux de communication existants, comme l'enquête auprès des entreprises, sur les possibilités de partenariats à l'étranger.	Récurrent annuellement

#3

Renforcer la présence des entreprises canadiennes de cybersécurité sur les marchés cibles

Action	Description	Chronologie
3.1	Sur la base des informations fournies dans la présente Stratégie et en collaboration avec les agences gouvernementales concernées, élaborer un Guide complet d'entrée sur le marché, et une Formation pour chaque marché cible potentiel qui tient compte des réglementations locales, des pratiques commerciales et des nuances culturelles.	À court terme
3.2	Offrir un soutien constant et des ressources continuelles aux entreprises canadiennes de cybersécurité pour les aider à s'orienter et à réussir sur les marchés cibles potentiels. Explorer les collaborations avec d'autres partenaires et organisations, notamment les délégués commerciaux du Canada.	En cours

#4

Maximiser la pénétration du marché et explorer de nouvelles possibilités de marché

Action	Description	Chronologie
4.1	Pour les marchés déjà bien desservis ou bénéficiant de solides partenariats commerciaux, renforcer les relations avec les partenaires existants en collaborant activement à des initiatives communes, en partageant des ressources, et en explorant ensemble de nouvelles possibilités commerciales. Cela peut inclure une communication régulière, des campagnes conjointes de marketing et l'organisation combinée d'événements ou de webinaires.	En cours
4.2	Pour les nouveaux marchés, effectuer des visites de marché et participer à des événements sectoriels sur de nouveaux marchés potentiels pour évaluer le potentiel du marché, rencontrer les acteurs locaux et comprendre l'environnement réglementaire.	En cours
4.3	Actualiser activement et régulièrement la stratégie commerciale internationale pour refléter les nouvelles réalisations et identifier les opportunités émergentes, afin de garantir qu'In-Sec-M et l'industrie canadienne de la cybersécurité restent bien positionnés pour une réussite continuelle.	Annuellement

Deloitte.

www.deloitte.ca

À propos de Deloitte

Deloitte fournit des services vérification et de certification, de consultation, de conseil financier, de conseil en gestion des risques, de fiscalité et autres services connexes à des clients publics et privés de nombreux secteurs d'activité. Deloitte est au service de quatre des cinq entreprises du classement Fortune Global 500® par l'intermédiaire d'un réseau mondial de cabinets membres dans plus de 150 pays et territoires, qui offrent des compétences, des connaissances et des services de classe mondiale pour répondre aux défis commerciaux les plus complexes des clients. Deloitte S.E.N.C.R.L., société à responsabilité limitée de l'Ontario, est le cabinet membre canadien de Deloitte Touche Tohmatsu Limited. Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited, société privée à responsabilité limitée par garanties du Royaume-Uni, et son réseau de cabinets membres, lesquels constituent chacun une entité juridiquement distincte et indépendante. Veuillez consulter le site www.deloitte.com/about pour une description détaillée de la structure juridique de Deloitte Touche Tohmatsu Limited et de ses sociétés membres.

Notre raison d'être mondiale est d'avoir un impact qui compte. Chez Deloitte Canada, cela se traduit par la construction d'un avenir meilleur en accélérant et en élargissant l'accès au savoir. Nous croyons que nous pouvons atteindre cette raison d'être en incarnant nos valeurs communes : montrer la voie, servir avec intégrité, prendre soin les uns des autres, favoriser l'inclusion et collaborer pour avoir un impact mesurable.

Pour en savoir davantage sur les quelque 330 000 professionnels de Deloitte, dont plus de 11 000 font partie de la société canadienne, veuillez nous contacter via LinkedIn, Twitter, Instagram, ou Facebook.


IN·SEC·M
LA GRAPPE CANADIENNE DE LA CYBERSÉCURITÉ