DÉVELOPPEMENT DES TALENTS EN CYBERSÉCURITÉ :

PROTÉGER L'ÉCONOMIE NUMÉRIQUE DU CANADA

ICTC CTIC

Recherche effectuée par

Le Conseil des technologies de
l'information et des communications

Financé par le Programme de
stages pratiques pour étudiants
du Gouvernement du Canada.

Canada

EN PARTENARIAT AVEC LE COMITÉ CONSULTATIF NATIONAL DU CTIC SUR
LA FORMATION EN CYBERSÉCURITÉ (CCNFC)

MAY 2022

PRÉFACE

Le Conseil des technologies de l'information et des communications (CTIC) est un centre d'expertise national à but non lucratif dont la mission consiste à renforcer l'avantage numérique du Canada dans l'économie mondiale. Grâce à des recherches fiables, à des conseils stratégiques pratiques et à des programmes créatifs de développement des capacités, le CTIC favorise les industries canadiennes qui, grâce à des talents numériques innovants et diversifiés, sont compétitives sur le plan international. En partenariat avec un vaste réseau de dirigeantes et dirigeants dans le secteur industriel, de partenaires universitaires et de décideuses et décideurs politiques à travers le Canada, le CTIC contribue à façonner une économie numérique solide et intégrée depuis 30 ans.

Comité consultatif national du CTIC sur la formation en cybersécurité (CCNFC)

Pour mieux comprendre les besoins de l'industrie de la cybersécurité et les lacunes en matière de formation qui peuvent exister au Canada, le CTIC a invité un groupe d'expertes et d'experts en la matière issus du milieu universitaire, de l'industrie, du gouvernement et d'associations à examiner les défis et à recommander des solutions. Le Comité consultatif national sur la formation en cybersécurité (CCNFC) du CTIC a été chargé d'examiner les lacunes dans les compétences et les programmes des étudiantes et étudiants de niveau postsecondaire, les obstacles à l'entrée et les problèmes de diversité du secteur, ainsi que les modèles de prestation de la formation les mieux adaptés pour répondre à la demande. Les hypothèses du CCNFC ont été transmises au Groupe de réflexion sur le numérique du CTIC pour validation. Les résultats préliminaires des sondages auprès des employeuses et employeurs et des étudiantes et étudiants du postsecondaire indiquent que bon nombre des hypothèses du Comité étaient correctes.

Pour citer ce rapport :

QUAN, Trevor, Chris HERRON. *Développement des talents en cybersécurité : protéger l'économie numérique du Canada*, Ottawa (Canada), Conseil des technologies de l'information et des communications, 2022.

Recherche et rédaction par Trevor Quan (analyste principal des politiques et de la recherche, CTIC) et Chris Herron (analyste de la recherche, CTIC) avec le soutien généreux de Rob Davidson (directeur, Science des données, CTIC), Xinyi Lin (scientifique de données, CTIC) et Alexandria Chiasson (coordonnatrice des partenariats, CTIC). Traduction de l'anglais : Shafick Osman (CTIC).

TABLE DES MATIÈRES

TABLE DES MATIÈRES

LISTE DES ACRONYMES UTILISÉS DANS CETTE ÉTUDE

États-Unis	Signification
IA	Intelligence artificielle
CTIC	Conseil des technologies de l'information et des communications
CCNFC	CTIC (voir ci-dessus) - Comité consultatif national pour la formation en cybersécurité
IdO	Internet des objets
PI	Propriété intellectuelle
(ISC)²	Consortium international de certification de la sécurité des systèmes d'information (International Information System Security Certification Consortium)
NICE	Initiative nationale pour l'éducation à la cybersécurité (É-UA)
CNP	Code national des professions
NSA	National Security Association (É-UA)
PME	Petites et moyennes entreprises
ROYAUME-UNI	Royaume-Uni
US	États-Unis
AIT	Apprentissage intégré au travail

RÉSUMÉ

La numérisation transforme rapidement l'économie mondiale mais elle a également stimulé la croissance rapide de la prévalence et de l'intensité de la cybercriminalité. La cybersécurité est un domaine aux multiples facettes avec de nombreuses spécialisations, notamment l'administration de réseaux, l'analyse générale de la cybersécurité, la réaction en cas d'incident et la criminalistique numérique. À l'échelle mondiale, il existe un déficit important de talents en cybersécurité. En 2021, l'association internationale des leaders de la sécurité de l'information (ISC)² a fait état d'un déficit mondial de main-d'œuvre en cybersécurité de 2,72 millions de travailleuses et travailleurs, contre 3,12 millions l'année précédente[1]. Le Canada ne fait pas exception à cette tendance. La même étude de (ISC)² a révélé qu'il y avait 123 696 professionnelles/professionnels de la cybersécurité au Canada, une forte augmentation par rapport à deux ans plus tôt, mais qu'il reste une pénurie de talents de 25 000 professionnelles/professionnels dans le domaine[2]. En bref, dans un domaine où le chômage est pratiquement nul, environ un poste sur six n'est pas pourvu.

Le CTIC a créé le CCNFC, le Comité consultatif national du CTIC pour la formation en cybersécurité, afin de proposer une approche fondée sur des preuves pour résoudre la crise des talents en cybersécurité. Ce rapport de recherche qui vise à décrire la situation des talents en cybersécurité au Canada et à proposer des solutions stratégiques potentielles, résume les études existantes sur l'écosystème de la cybersécurité au pays et à l'étranger, et les combine avec des données de recherche originales provenant d'employeuses et d'employeurs et d'étudiantes et d'étudiants. Le rapport examine la viabilité de voies alternatives pour obtenir une formation en cybersécurité, comme les expériences de microapprentissage et l'apprentissage intégré au travail.

Notre recherche confirme que la cybersécurité est un domaine rigoureux et spécialisé confronté à un fort déficit de talents. En raison des salaires élevés motivés par une pénurie de talents, de nombreuses organisations ne parviennent pas à trouver le personnel nécessaire. Et pourtant, malgré des rémunérations très élevées, on observe une autosélection généralisée hors du domaine; près d'un tiers des répondants masculins et environ la moitié des étudiantes finissent par quitter le domaine au cours de leurs études. Parmi ceux qui deviennent des employées/employés à part entière de la cybersécurité, les sentiments d'épuisement professionnel sont courants. D'une certaine manière, la situation des talents en cybersécurité au Canada peut être plus intense qu'aux États-Unis pour plusieurs raisons. Premièrement, l'absence d'un cadre de compétences mis en œuvre à l'échelle nationale (semblable au NICE aux États-Unis) a entravé la communication entre les employeuses et employeurs et les employées/employés potentielles/potentiels en cybersécurité au sujet des compétences nécessaires pour réussir. Deuxièmement, il y a un manque de communication entre l'industrie et le milieu universitaire. Enfin, le Canada est confronté

[1] *A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study*, 2021, (ISC)², 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

[2] *Ibid*.

RÉSUMÉ

au risque de « braconnage de talents » par les États-Unis où l'industrie technologique offre généralement des régimes de rémunération encore plus avantageux.

Néanmoins, l'étude constate également des développements positifs dans l'enseignement de la cybersécurité au Canada. Les programmes de microapprentissage et d'apprentissage intégré au travail sont bien accueillis par les anciennes étudiantes et anciens étudiants du domaine, la majorité d'entre elles et eux indiquant que ces programmes auraient pu les dissuader de quitter le domaine. Puisqu'il n'y a pas d'écart significatif entre ce que les étudiantes et étudiants en cybersécurité désirent étudier et les besoins de l'industrie, le fait de fournir aux étudiantes et étudiants des programmes éducatifs appropriés devrait permettre à la main-d'œuvre de croître tout en satisfaisant les besoins de l'industrie.

INTRODUCTION

Qu'est-ce que la cybersécurité?

La cybersécurité peut être définie au sens large comme la pratique consistant à se protéger et à protéger son organisation contre les attaques numériques[3]. La cybersécurité comprend les responsabilités en matière de sécurité des réseaux, des systèmes et des programmes assumées par des spécialistes, la planification et la réponse aux cyberincidents, ainsi que la formation du personnel de l'ensemble de l'organisation à la cyberconscience. La cybersécurité englobe toutes les mesures prises pour protéger les informations en ligne ainsi que tout actif connecté à un réseau, tout en sécurisant l'infrastructure sur laquelle il réside[4]. La cybersécurité est un processus à multiples facettes et à plusieurs étapes qui permet de prévenir les menaces autant que possible et d'y répondre ensuite. Parmi les exemples de cyberattaques courantes dont la cybersécurité doit se protéger, citons l'hameçonnage, les attaques par embuscade, les rançongiciels, le harponnage ou le déploiement de réseaux de zombies[5]. Pour compléter le nombre croissant de recherches sur le marché du travail en cybersécurité au Canada, le CTIC a entrepris une enquête nationale qui englobe à la fois les employeuses et employeurs en cybersécurité et les étudiantes et étudiants en cybersécurité qui entreront dans la future main-d'œuvre. Ces conclusions, l'analyse et les implications futures sont discutées plus en détail dans ce rapport.

La menace croissante de la cybercriminalité

La numérisation transforme l'économie dans le monde entier et a été accélérée par la pandémie de la COVID-19. Selon une étude réalisée en 2018 par Tech Pro, 70 % des entreprises ont mis en place une stratégie de transformation numérique ou y travaillent[6]. Une enquête menée en juillet 2020 auprès de 800 cadres d'entreprises a révélé que depuis le début de la pandémie COVID-19, 36 % des entreprises ont accéléré la numérisation de leur chaîne d'approvisionnement, 48 % ont accéléré la numérisation des canaux clients, 85 % ont accéléré la numérisation de l'interaction et de la collaboration des employées/employés, et 67 % ont accéléré l'automatisation et l'intelligence artificielle[7]. On estime que 80 % de la valeur des entreprises du classement Fortune 500 provient de la propriété intellectuelle (PI) dont la quasi-totalité est stockée sous forme numérique[8].

---

[3] *What is cybersecurity*, Cisco, https://www.cisco.com/c/en_ca/products/security/what-is-cybersecurity.html#:~:text=Cybersecurity%20is%20the%20practice%20of,or%20interrupting%20normal%20business%20processes.

[4] *Spotlight on Cybersecurity*, Gouvernement du Canada, consulté en 2022, https://www.tradecommissioner.gc.ca/guides/spotlight-pleins_feux/spotlight_cybersecurity_pleins_feux_cybersecurite.aspx?lang=eng.

[5] *Ibid*.

[6] M. Wachsman, « Survey: Despite steady growth in digital transformation initiatives, companies face budget and buy-in challenges », *ZD Net*, 2018, https://www.zdnet.com/article/survey-despite-steady-growth-in-digital-transformation-initiatives-companies-face-budget-and-buy-in/.

[7] S. Lund, et coll., *What 800 executives envision for the postpandemic workforce*, McKinsey & Company, 23 September 2020, https://www.mckinsey.com/featured-insights/future-of-work/what-800-executives-envision-for-the-postpandemic-workforce?utm_campaign=Digital%20Policy%20Salon&utm_medium=email&utm_source=Revue%20newsletter.

[8] Jeff Desjardins, « Cybersecurity: Fighting a Threat That Causes $450B of Damage Each Year », *Visual Capitalist*, 2017, https://www.visualcapitalist.com/cybersecurity-fighting-450b-damage/.

INTRODUCTION

Les entreprises étant de plus en plus dépendantes des solutions numériques, il n'est pas surprenant que la cybercriminalité gagne en sophistication, en fréquence et en impact. Une enquête du Forum économique mondial menée auprès de leaders mondiaux en 2021 a révélé que 39 % des personnes interrogées considéraient les défaillances en matière de cybersécurité comme un danger clair et présent pour l'économie mondiale juste derrière le changement climatique[9]. Le coût mondial de la cybercriminalité devrait atteindre 6 000 milliards de dollars étasuniens d'ici 2021[10].

En réponse à la montée de la cybercriminalité, la cybersécurité a connu une croissance rapide. Des études de marché ont estimé que le marché de la cybersécurité a été multiplié par 35 en 13 ans, avant le plus récent cycle d'investissement de cinq ans[11]. Les analystes du secteur estiment que la croissance varie de 8 à 15 % d'une année sur l'autre et, selon la société de recherche Gartner Inc., le marché mondial de la cybersécurité pourrait atteindre 170,4 milliards de dollars étasuniens en 2022[12].

Le marché du travail précaire de la cybersécurité

Malgré l'augmentation des dépenses dans le domaine de la cybersécurité, le domaine est confronté à de nombreux défis structurels. Même avant les grandes questions de la « Grande Démission » post-2020, qui se caractérise par un niveau historique de démission et de rotation des employées/employés[13], il y avait des préoccupations concernant le personnel de cybersécurité. Une enquête mondiale sur les systèmes de sécurité de l'information a révélé qu'un tiers des répondantes et répondants estimaient qu'une pénurie mondiale de compétences avait un impact important sur leur organisation. Deux tiers des répondantes et répondants ont déclaré que la pénurie de compétences augmentait la charge de travail du personnel existant[14]. Il semble que la pression accrue et la pénurie de personnel entraînent une baisse de la satisfaction au travail et des sollicitations régulières de la part des recruteuses et recruteurs[15].

---

[9] *The Global Risks Report 2021*, Forum économique mondial, 2021, http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

[10] « Cyber Crime Damages $6 Trillion by 2021 », *Cybercrime Magazine, 2017,* https://cybersecurityventures.com/hackerpocalypse-cyber crime-report-2016/.

[11] S. Morgan, « Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021 », Cybercrime Magazine, juin 2019, https://cybersecurityventures.com/cybersecurity-market-report/.

[12] *Ibid*.

[13] J. Liu, « A record 4.4 million people quit in September as Great Resignation shows no signs of stopping », *CNBC*, 12 novembre 2021, https://www.cnbc.com/2021/11/12/a-record-4point4-million-people-quit-jobs-in-september-great-resignation.html.

[14] M. Vizard, *Survey identifies root causes of cybersecurity staff turnover*, Barracuda, mai 2019, https://blog.barracuda.com/2019/05/10/survey-identifies-root-causes-of-cybersecurity-staff-turnover/.

[15] *Ibid*.

INTRODUCTION

Les gouvernements qui possèdent des informations détaillées et personnelles sur leurs citoyennes et citoyens, telles que les adresses, les adresses courriel et les numéros de sécurité sociale, sont des cibles de choix pour les cyberattaques. Pourtant, le recrutement et la rétention de professionnelles/professionnels de la cybersécurité dans le secteur public constituent un défi particulier. Les problèmes identifiés dans le secteur public comprennent des niveaux de rémunération inférieurs à ceux du secteur privé, un financement insuffisant, des obstacles bureaucratiques, des processus d'embauche fastidieux, la vérification des antécédents et l'épuisement professionnel[16].

Dans une étude internationale de 2017, 66 % des travailleuses et travailleurs de la sécurité de l'information ont répondu qu'elles et qu'ils ne se sentaient pas suffisamment dotées/dotés en personnel pour faire face à l'augmentation des cybermenaces[17]. En 2021, (ISC)² a fait état d'un déficit mondial de main-d'œuvre en cybersécurité de 2,72 millions de travailleuses et travailleurs contre 3,12 millions l'année précédente[18]. Près d'un tiers de la demande de talents en cybersécurité se situe dans seulement trois pays : le Brésil, les États-Unis et le Mexique. La figure suivante montre le grand nombre d'employées/d'employés supplémentaires qui sont nécessaires.

NOMBRE DE PROFESSIONNELLES / PROFESSIONNELS DE LA CYBERSÉCURITÉ NÉCESSAIRES DANS LE MONDE EN 2021, PAR PAYS

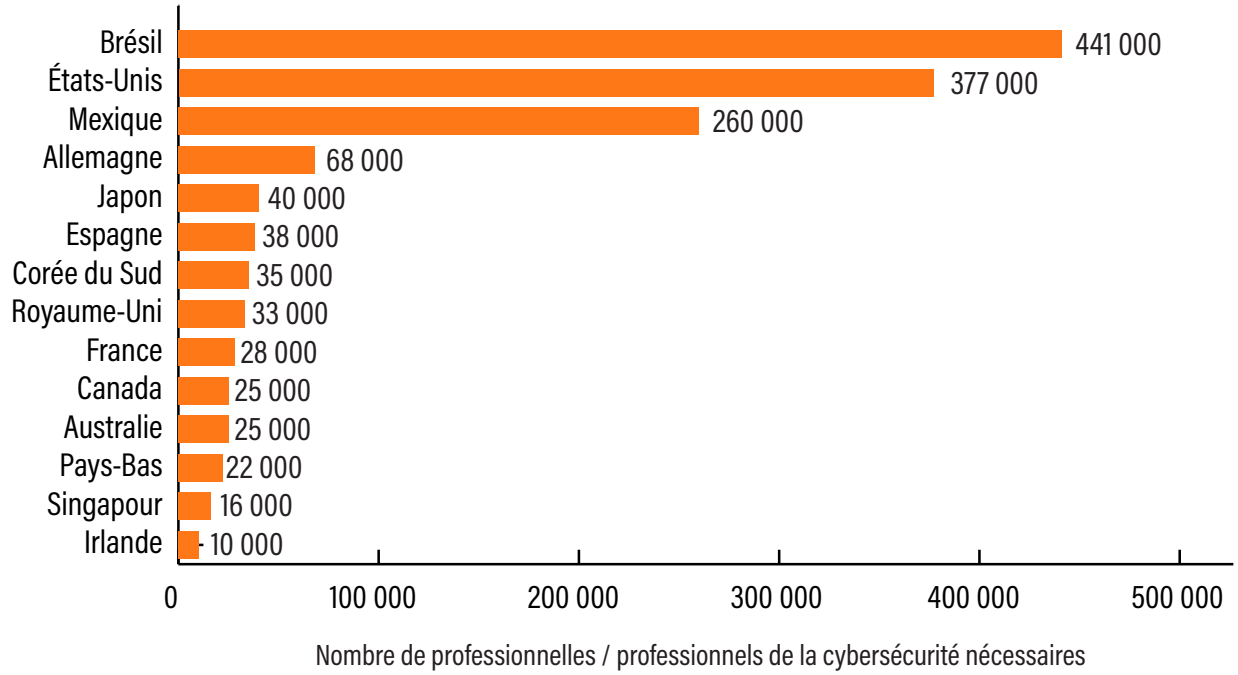


Figure 1 - Nombre de travailleuses et travailleurs en cybersécurité nécessaires dans le monde

[16] H. Rosenkrantz, *The Big Quit : Why Cybersecurity Pros Are Leaving Government*, Endpoint, November 2021, https://endpoint.tanium.com/the-big-quit-why-cybersecurity-pros-are-leaving-government/.

[17] Frost & Sullivan, *2017 Global Information Security Workforce Study*, Center for Cyber Safety and Education, https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx.

[18] *A Resilient Cybersecurity Profession Charts the Path Forward*: (ISC)2 Cybersecurity Workforce Study, 2021, loc. cit.

INTRODUCTION

Compte tenu de la crise croissante des talents dans le domaine de la cybersécurité, cette enquête du CTIC a été conçue pour étudier les défis du pipeline de développement des talents en cybersécurité au Canada. Il sera crucial de remédier à cette pénurie de main-d'œuvre pour assurer la protection des entreprises et des organismes du secteur public canadiens.

Les recherches antérieures du CTIC sur la cybersécurité ont également révélé des difficultés à retenir les talents en cybersécurité face à la concurrence des autres provinces et des États-Unis, ainsi qu'un décalage entre les compétences de la main-d'œuvre et les exigences des organisations en matière de cybersécurité. Le défi le plus marquant était la pénurie de professionnelles/professionnels de la cybersécurité hautement qualifiées/qualifiés et expérimentées/expérimentés et un surplus relatif de talents de niveau subalterne.

LA MENACE DE CYBERCRIMINALITÉ AU CANADA

LA MENACE DE CYBERCRIMINALITÉ AU CANADA

Bien que la cybercriminalité soit un problème mondial, elle revêt une importance particulière pour le Canada. L'indice national d'exposition 2018 publié par le fournisseur de cybersécurité Rapid7 a déclaré que le Canada était le troisième pays le plus exposé à la cybercriminalité sur 187 pays, après les États-Unis et le Royaume-Uni[19]. La recherche effectuée par IBM a révélé que les incidents d'atteinte à la protection des données (fréquemment causés par des cyberattaques) au Canada sont parmi les plus coûteux au monde à réparer, coûtant en moyenne 5,72 millions de dollars par incident[20]. En 2017 seulement, plus d'un cinquième (21 %) des entreprises canadiennes de toutes tailles ont été touchées par un incident de cybersécurité. L'Autorité canadienne pour les enregistrements Internet a signalé en 2018 que quatre petites et moyennes entreprises (PME) canadiennes sur dix ont subi des attaques par hameçonnage et par virus : environ un tiers ont été victimes de chevaux de Troie et de logiciels espions, et 27 % ont été attaquées par des rançongiciels. Pendant ce temps, un rapport de 2017 a noté que les consommatrices canadiennes et consommateurs canadiens ont perdu 1,5 milliard de dollars (USD) en raison des cyberattaques[21].

De nombreux facteurs rendent le Canada vulnérable aux cybermenaces. L'un d'eux est la détérioration des relations internationales; un rapport du gouvernement canadien de 2020 indiquait que la plus grande menace pour la cybersécurité canadienne était la montée de la cybercriminalité en provenance de la Chine et de la Russie, et prévenait que les attaques commanditées par des États contre le Canada seraient de plus en plus fréquentes[22]. Une autre raison est l'exposition pure et simple à Internet. En 2019, le Canadien moyen a passé 43,5 heures en ligne par mois, soit plus que tout autre pays[23].

Depuis la COVID-19, la menace de cybercriminalité n'a fait qu'augmenter au Canada - près de la moitié des Canadiennes et Canadiens (44 %) passent plus de temps en ligne qu'au début de la pandémie de COVID-19[24]. Dans une enquête menée auprès des leaders canadiennes et canadiens de la sécurité en 2020, 86 % ont déclaré que leur organisation avait subi une violation de données en 2020. Près de neuf personnes sur dix (88 %) touchées par des violations de données ont subi des répercussions « importantes » sur l'organisation. Environ quatre cinquièmes (78 %) ont déclaré que leur organisation faisait face à plus d'attaques que les années précédentes, et une proportion similaire a indiqué que les attaques étaient devenues plus sophistiquées[25].

---

[19] *National Exposure Index 2018*, Rapid 7, 2018, https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf.

[20] S. Randall, *Canada is top 3 for data breach costs warns IBM*, Wealth Professional, 2021, https://www.wealthprofessional.ca/news/industry-news/canada-is-top-3-for-data-breach-costs-warns-ibm/358484.

[21] *2017 Norton Cyber Security Insights Report Global Results*, https://www.nortonlifelock.com/content/dam/nortonlifelock/pdfs/reports/2017-ncsir-global-results-en.pdf.

[22] *National Cybersecurity Threat Assessment 2020*, Centre canadien pour la cybersécurité, 2020, https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf.

[23] *National Cyber Security Strategy*, Gouvernement du Canada, 2018, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.

[24] *Canadians spend more money and time online during pandemic and over two-fifths report a cyber incident*, Statistique Canada, 2020, https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-eng.htm.

[25] *Canada Security Insights Report 2021*, VMWare, 2021, https://www.carbonblack.com/resources/canada-security-insights-report-2021/.

L'écosystème de cybersécurité du Canada

Comparitech a nommé le Canada parmi les pays ayant les meilleurs systèmes de cybersécurité en 2021 sur la base d'une analyse de plus de 70 facteurs[26]. En 2017, les entreprises canadiennes ont dépensé 8 milliards de dollars en salaires pour les seules employées/seuls employés, conseils et entrepreneuses et entrepreneurs en cybersécurité[27]. Les analystes en cybersécurité ont également été identifiées/identifiés comme l'un des dix rôles numériques les plus porteurs dans le rapport sur les perspectives 2023 du CTIC, basé sur la consultation d'expertes et d'experts du secteur des TIC[28]. Selon le rapport 2020 the (ISC)² Cybersecurity Workforce Study, le Canada comptait 101 963 personnes travaillant dans des professions liées à la cybersécurité et avait une pénurie de talents de 16 552 personnes. Cela représente une augmentation de 17 963 personnes dans l'emploi total de la profession par rapport à 2019. D'ici 2021, (ISC)² a indiqué que la main-d'œuvre canadienne en cybersécurité était passée à plus de 123 696 personnes. Cependant, le déficit de talents a augmenté encore plus rapidement, bondissant à 25 000[29]. Le déficit en cybersécurité du Canada représentait 17 % du total de ses postes en cybersécurité. Bien que ce chiffre soit inférieur à celui des États-Unis (25 %), il est supérieur à celui du Royaume-Uni (10 %), de l'Allemagne (13 %) et à peu près égal à celui de l'Australie et de la France (16 %). La croissance rapide du secteur de la cybersécurité semble prête à se poursuivre. En 2018, près des trois quarts (73 %) des cadres canadiennes et canadiens prévoyaient que leur nombre d'employées/d'employés de sécurité à temps plein augmenterait au cours des trois à cinq années suivantes, tandis qu'un quart (25 %) s'attendait à ce que leurs équipes cybernétiques augmentent de plus de 25 %[30].

Bien que la littérature disponible sur l'impact de la « fuite des cerveaux » sur le secteur de la cybersécurité soit limitée, la perte de talents canadiens au profit des États-Unis exige une attention particulière et souligne la fragilité de l'écosystème de cybersécurité du Canada. La pénurie de talents en cybersécurité aux États-Unis est près de 15 fois plus importante que celle du Canada (377 000 emplois contre 25 000 emplois). De plus, les États-Unis offrent des salaires considérablement plus élevés aux employées/employés. Le salaire moyen d'un analyste en cybersécurité au Canada est de 81 881 CAD par année en 2022[31]. En revanche, le salaire d'un « analyste en sécurité de l'information » (une classification qui inclut l'analyste en cybersécurité) aux États-Unis était de 103 590 USD en 2020[32]

---

[26] P. Bischoff, *Which countries have the worst (and best) cybersecurity?*, Comparitech, 2021, https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.

[27] *Impact of Cyber crime on Canadian Businesses*, Statistique Canada, 2017, https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm.

[28] *Ibid*.

[29] *A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021*, loc. cit.

[30] *The Changing Faces of Cybersecurity: Closing the cyber risk gap*, Deloitte, 2020, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF.

[31] https://ca.talent.com/salary?job=cyber+security+analyst#:~:text=The%20average%20cyber%20security%20analyst%20salary%20in%20Canada%20is%20%2481%2C881,up%20to%20%24108%2C474%20per%20year

[32] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

TAILLE DES EFFECTIFS DE CYBERSÉCURITÉ DANS LE MONDE EN 2021, PAR PAYS

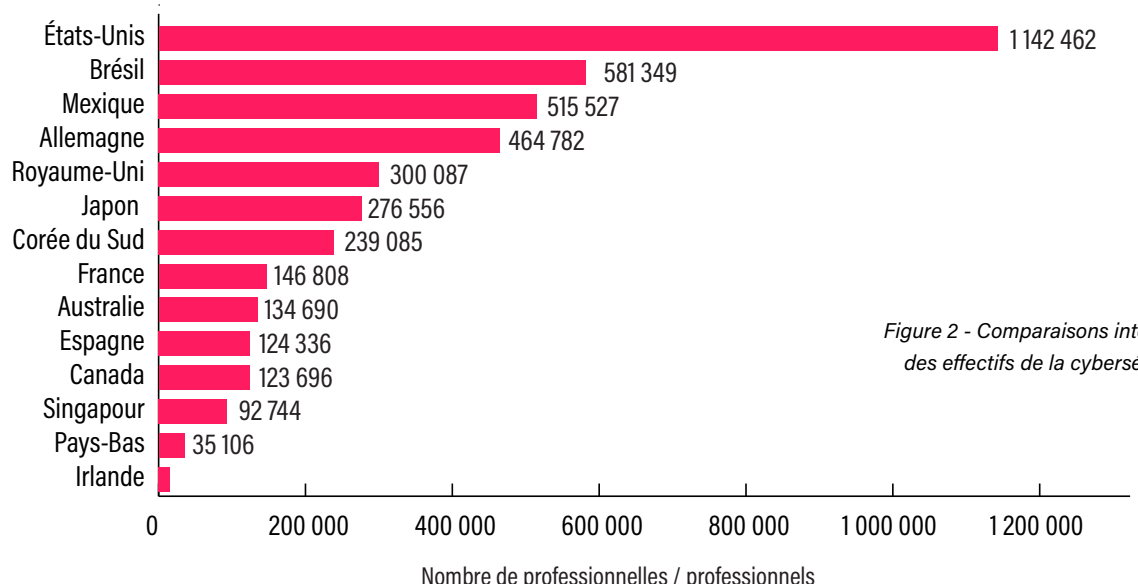


Figure 2 - Comparaisons internationales des effectifs de la cybersécurité, 2021.

(équivalent à 129 677 CAD[33]), un chiffre 58 % plus élevé. Toute stratégie efficace d'éducation à la cybersécurité doit prendre en compte le risque de perte substantielle de talents pour les États-Unis, en particulier sous les administrations qui accueillent avec enthousiasme l'immigration qualifiée.

Bien que le manque de main-d'œuvre en cybersécurité au Canada ne soit pas aussi aigu que dans certains autres pays, l'industrie constate de graves pénuries de personnel en cybersécurité.

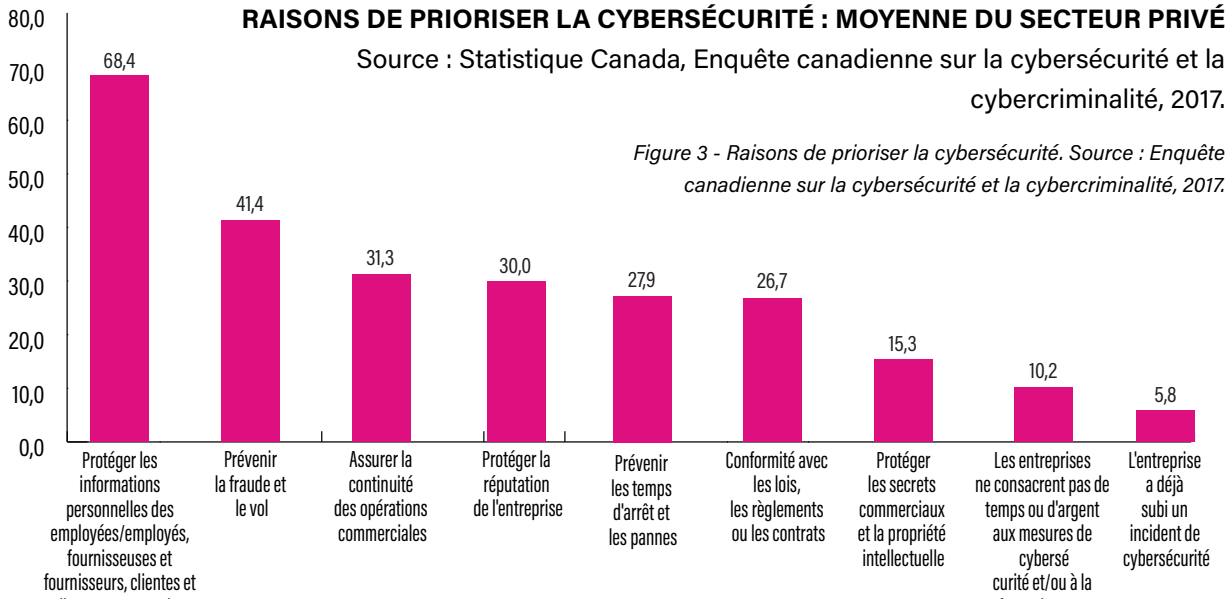
Les organisations au Canada ont de nombreuses motivations pour prioriser la cybersécurité, mais l'Enquête canadienne sur la cybersécurité et la cybercriminalité de 2017 a révélé que la principale motivation était la protection des renseignements personnels. Il s'agissait d'une motivation pour 68,4 % des répondantes et répondants. Les autres motivations clés étaient la prévention de la fraude et du vol (mentionnée par 41,4 % des répondantes et répondants), la garantie de la continuité des opérations commerciales (31,3 %), la protection de la réputation (30,0 %) et la prévention des temps d'arrêt et des pénuries (27,9 %). Seuls 10,2 % des répondantes et répondants ont déclaré que leur entreprise ne consacrait pas de temps ou d'argent à l'acquisition de compétences ou de formations liées à la cybersécurité.

[33] Basé sur le taux de change rapporté le 1er avril 2022.

RAISONS DE PRIORISER LA CYBERSÉCURITÉ : MOYENNE DU SECTEUR PRIVÉ

Source : Statistique Canada, Enquête canadienne sur la cybersécurité et la cybercriminalité, 2017.

Figure 3 - Raisons de prioriser la cybersécurité. Source : Enquête canadienne sur la cybersécurité et la cybercriminalité, 2017.



L'enquête interne du CTIC auprès des employeuses et employeurs pour ce projet a également confirmé que si les rôles de cybersécurité sont très demandés par les employeuses et employeurs, ils restent moins demandés que les rôles dans le domaine des logiciels ou des affaires/de la finance. Les rôles en cybersécurité sont la quatrième catégorie d'emploi en technologie, devant les rôles en données ou les rôles en opérations/logistique.

RÔLES QUE LES ORGANISATIONS CHERCHENT LE PLUS ACTIVEMENT À EMBAUCHER

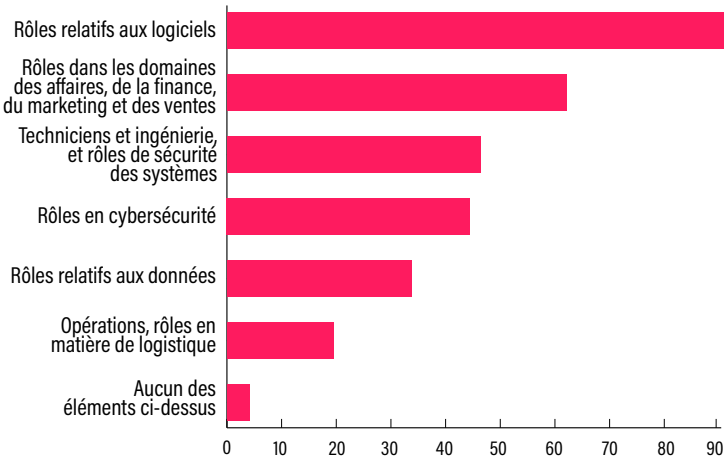


Figure 4 - Types de rôles les plus demandés par les employeuses canadiennes et employeurs canadiens du secteur de la technologie, 2022.

Classification des rôles en matière de cybersécurité

La cybersécurité n'est pas un domaine monolithique; si le domaine contient certainement de nombreuses et de nombreux généralistes travaillant dans des organisations de petite ou moyenne taille, il comporte également de nombreux domaines de spécialisation, particulièrement évidents lorsqu'on examine les équipes des grandes organisations. Comprendre les distinctions nuancées entre les sous-disciplines de la cybersécurité peut éclairer les politiques, en veillant à ce que les ressources soient dirigées vers les rôles ayant le plus fort potentiel de croissance.

Le cadre de l'initiative nationale pour l'éducation à la cybersécurité (NICE) est le cadre mondial dominant pour la classification des rôles de cybersécurité. Ce cadre étasunien fournit une terminologie normalisée pour les emplois en cybersécurité. Le cadre a été adopté par des organisations du monde entier dans le but d'adopter une terminologie normalisée pour les emplois et les compétences en matière de cybersécurité[34]. Il classe le domaine de la cybersécurité selon les critères suivants :

- Sept catégories composées de 32 domaines de spécialité
- Plus de 1 000 tâches, y compris la détermination de la façon dont les résultats de la surveillance continue seront utilisés dans l'autorisation permanente et l'identification et la direction de la remédiation des problèmes techniques rencontrés lors des tests et de la mise en œuvre de nouveaux systèmes
- Plus de 600 domaines de connaissances, y compris les technologies des machines virtuelles et l'établissement de liste blanche et de liste noire
- Plus de 300 compétences dont l'analyse des fusions et l'anticipation des nouvelles menaces de sécurité
- Cent soixante-seize capacités, y compris la maintenance des bases de données et la conception de la réaction en cas d'incident pour les modèles de services dans le nuage.

[34] *Ibid*.

Vous trouverez ci-dessous un résumé des sept principaux types de rôles[35].

CATÉGORIES	DESCRIPTIONS[36]	LES INTITULÉS DE POSTE LES PLUS COURANTS AU CANADA[37]
Sécuriser l'approvisionnement (SA)	Conceptualise, conçoit, achète et/ou construit des systèmes sécurisés de technologie de l'information (TI), avec la responsabilité de certains aspects du développement de systèmes et/ou de réseaux.	Gestionnaire de sécurité/risque Architecte des systèmes/sécurité Développeuse/Développeur de logiciels Planificatrice/Planificateur de logiciels/systèmes Analyste de la sécurité
Exploitation et maintenance (EM)	Fournit le soutien, l'administration et la maintenance nécessaires pour assurer une performance et une sécurité efficaces et efficientes des systèmes de technologie de l'information (TI).	Administratrice ou Administrateur de données/bases de données ou de sécurité Gestionnaire des risques liés aux connaissances ou à la sécurité Représentante/Représentant du soutien technique ou de l'assistance à la clientèle Administratrice ou Administrateur/Analyste de réseau/systèmes
Encadrer et régir (ER)	Assurer le leadership, la gestion, la direction ou le développement et la défense des intérêts de l'organisation afin qu'elle puisse mener efficacement des travaux de cybersécurité.	Dirigeante principale de l'information/Dirigeant principal de l'information Analyste en stratégie cybernétique Analyste de la politique cybernétique Analyste des communications cybernétiques Gestionnaire de programme cybernétique Gestionnaires de projets et d'acquisitions
Protéger et défendre (PD)	Identifie, analyse et atténue les menaces qui pèsent sur les systèmes et/ou les réseaux TI internes.	Analyste cybernétique Ingénieure/Ingénieur en infrastructure de sécurité/cyberdéfense Répondante/Répondant en cas de cyberincident Analyste des vulnérabilités Gestionnaire du Centre d'opérations de sécurité

[35] *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, National Institute of Standards and Technology, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

[36] *Ibid*.

[37] Basé sur des informations provenant de CyberNB, ainsi que sur une publication de 2018 de Deloitte qui a relié le cadre NICE au contexte canadien : The changing faces of cybersecurity: Closing the cyber risk gap, Deloitte et la Toronto Financial Services Alliance, 2018.

CATÉGORIES	DESCRIPTIONS[36]	LES INTITULÉS DE POSTE LES PLUS COURANTS AU CANADA[37]
Analyser (AN)	Effectuer un examen et une évaluation hautement spécialisés des informations entrantes en matière de cybersécurité afin de déterminer leur utilité pour le renseignement.	Analyste en renseignement sur les menaces Gestionnaire des cyberanalyses Scientifique de données Analyste linguistique/Linguiste informatique
Collecter et exploiter (CE)	Fournit des opérations spécialisées de déni et de tromperie et la collecte d'informations sur la cybersécurité qui peuvent être utilisées pour développer le renseignement.	Informaticienne ou informaticien pirate/Opératrice ou opérateur de collections Planificatrice/Planificateur opérationnel cybernétique Analyste en cybermenaces/Opératrice ou opérateur en cybermenaces
Enquêter (EN)	Enquête sur les événements ou les crimes de cybersécurité liés aux systèmes TI, aux réseaux et aux preuves numériques.	Analyste en criminalistique numérique/cybercriminalité. Cyberenquêtrice/Cyberenquêteur

Figure 5 - Catégories de personnel du cadre NICE

Des recherches effectuées précédemment par le CTIC ont révélé un certain degré de comparabilité entre le cadre NICE, les personas de cybersécurité de Deloitte et le système basé sur la CNP (code de profession nationale) utilisé par le CTIC. Par exemple, le code CNP 0213 (Gestionnaires des systèmes informatiques) correspond à la classification Stratège/Encadrer et régir (ER), tandis que les quatre autres codes CNP correspondent aux classifications Conseillère ou Conseiller/ Sécuriser l'approvisionnement (SA) et Défenseure ou Défenseur/Exploitation et maintenance (EM). En outre, dans la version 2021 du système de la CNP, le code CNP 21220 (Spécialistes de la cybersécurité) comprend des intitulés de postes tels qu'analyste en cybersécurité, analyste en sécurité des systèmes, analyste en sécurité informatique, consultante/ consultant en sécurité informatique, et spécialiste de la sécurité des technologies de l'information (TI). En tant que tel, il est à cheval sur les catégories « sécuriser l'approvisionnement » et « protéger et défendre » du cadre NICE.

Cela dit, le système CNP dans son état actuel n'a pas d'équivalent significatif pour trois autres catégories utilisées par Deloitte et NICE, ce qui pourrait signifier un sous-comptage substantiel des rôles de cybersécurité en utilisant des approches basées sur le CNP[38].

[38] *The Changing Faces of Cybersecurity: Closing the cyber risk gap*, Deloitte, 2020, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF.

CNP	PERSONA DE DELOITTE	CATÉGORIE NICE	LES INTITULÉS DE POSTE COURANTS
0213 - Gestionnaires des systèmes informatiques	Stratège	Encadrer et régir	Dirigeante principale de l'information/ Dirigeant principal de l'information Analyste en stratégie cybernétique Analyste de la politique cybernétique Gestionnaire de programme cybernétique
2171 - Analystes et consultants/ consultantes en informatique **2283 - Évaluateurs/évaluatrices de systèmes informatiques** **21220 - Spécialistes de la cybersécurité**	Conseillère/ Conseiller	Sécuriser l'approvisionnement	Gestionnaire de sécurité/risque Analyste des systèmes/sécurité Développeuse/développeur de logiciels; Planificatrice/Planificateur de logiciels/ systèmes
2172 - Analystes de bases de données et administrateurs/ administratrices de données **2281 - Techniciens/techniciennes de réseau informatique**	Défenseure/ Défenseur	Exploitation et maintenance	Administratrice ou Administrateur de données/bases de données ou de sécurité Représentante/Représentant du support technique Administratrice ou Administrateur réseau/ systèmes Analyste de réseau/systèmes
21220 - Spécialistes de la cybersécurité	Pompier	Protéger et défendre	Analyste de la cybersécurité Ingénieur en infrastructure de sécurité/ cyberdéfense Analyste des vulnérabilités
Aucun équivalent	Informaticienne/ Informaticien pirate	Collecter et exploiter	Informaticienne ou Informaticien pirate/ opératrice ou opérateur de collections Analyste en cybermenaces/opératrice ou opérateur en cybermenaces Planificatrice opérationnelle cybernétique/ Planificateur opérationnel cybernétique
Aucun équivalent	Scientifique	Analyser	Analyste en renseignement sur les menaces Gestionnaire des cyberanalyses Scientifique de données Analyste linguistique/Linguiste informatique
Aucun équivalent	Limière/Limier	Enquêter	Analyste en criminalistique numérique/ cybercriminalité. Cyberenquêtrice/Cyberenquêteur

Figure 6 - Correspondance entre le cadre NICE, les personas de cybersécurité de Deloitte et les CNP liés à la cybersécurité

LA CYBERSÉCURITÉ AU CANADA

Estimation de la taille de la main-d'œuvre en cybersécurité

L'étude 2019 sur la main-d'œuvre en cybersécurité de (ISC)² a estimé qu'il y avait 84 000 professionnelles/professionnels de la cybersécurité dans tout le Canada en 2019[39]. L'édition 2021 de la même étude estimait à 123 696 le nombre de professionnelles/professionnels de la cybersécurité au Canada. Cela représentait une forte augmentation par rapport à deux ans plus tôt, mais il restait une pénurie de talents de 25 000 professionnelles/professionnels en cybersécurité[40].

Une estimation plus faible du nombre de professionnelles/professionnels de la cybersécurité peut être générée à partir du rapport de Deloitte, The Changing Faces of Cybersecurity. Deloitte a estimé que le nombre de professionnelles/professionnels de la cybersécurité au Canada était de 20 000 en 2016 et a prévu qu'il passerait à 28 000 en 2021[41]. L'estimation de Deloitte suppose que les rôles de cybersécurité représentent 1,6 % de toutes les professionnelles et de tous les professionnels des TIC. Deloitte souligne que son estimation est très prudente, ajoutant que « les analystes de l'industrie supposent généralement que les professionnelles/professionnels de la cybersécurité représentent entre 5 % et 6 % du personnel des TI d'une organisation ».

Répartition géographique des rôles en matière de cybersécurité

Le CTIC a constaté, en janvier 2020, que les offres d'emploi axées sur la cybersécurité étaient fortement focalisées sur l'Ontario. L'Ontario a accueilli les trois cinquièmes (60 %) des affichages en cybersécurité du Canada, soit 23,26 % de plus que sa part de la population canadienne. Les quatre provinces atlantiques du Canada, à l'exception de Terre-Neuve-et-Labrador, ont fait mieux que leur part d'affichage en matière de cybersécurité, et la différence était plus marquée en Nouvelle-Écosse. En revanche, plusieurs régions du Canada étaient des « déserts » de cybersécurité qui affichaient une part d'emplois en cybersécurité nettement inférieure à leur part de la population canadienne. Il s'agit notamment de la Saskatchewan, de Terre-Neuve-et-Labrador, du Manitoba et des Territoires. L'Alberta et la Colombie-Britannique affichaient toutes deux une part nettement inférieure des postes de cybersécurité au Canada, bien qu'en tant que grands centres de population, leur nombre absolu d'affichages restait important[42].

---

[39] *Strategies for Building and Growing Strong Cybersecurity Teams*, (ISC)², 2019, https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482.

[40] *A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study, 2021*, loc. cit.

[41] *The Changing Faces of Cybersecurity: Closing the cyber risk gap*, loc. cit.

[42] Chris Herron, Faun Rice et Nathan Snider, *Searching for Hidden Talent: Experience and Expertise in New Brunswick's Cybersecurity Community*, CTIC, 2020, https://www.ictc-ctic.ca/wp-content/uploads/2020/06/new-brunswick-cybersecurityFINAL.EN_.pdf.

LA POPULATION PAR RAPPORT AUX AFFICHAGES D'EMPLOIS EN CYBERSÉCURITÉ
QUELLES SONT LES PROVINCES QUI PERFORMENT AU-DESSUS DE LEUR POIDS?
Source : Statistique Canada, CTIC

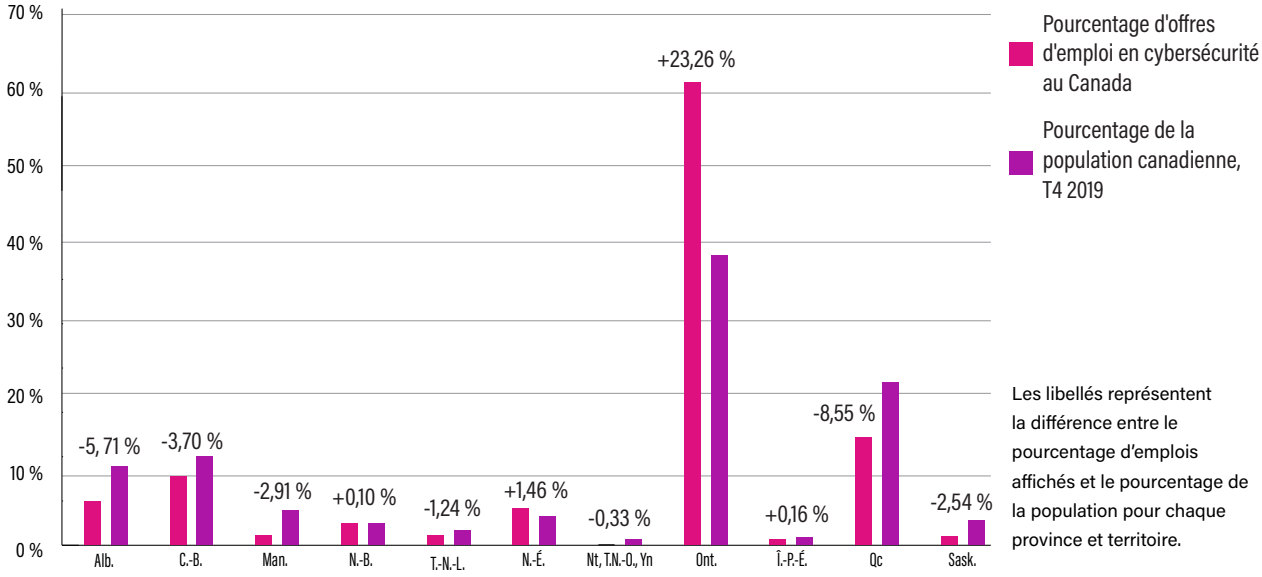


Figure 7 - Proportion de la population canadienne des provinces et des territoires comparée à leur proportion de rôles de cybersécurité affichés. Les données sur l'affichage des emplois datent de janvier 2020. Source : CTIC, Statistique Canada.

Composition sectorielle et niveaux d'emploi en cybersécurité

Les professionnelles/professionnels de la cybersécurité peuvent travailler pour des entreprises et des organisations spécialisées dans la cybersécurité, des établissements universitaires ou des organismes gouvernementaux. Alternativement, les professionnelles/professionnels de la cybersécurité peuvent être des spécialistes intégrées/intégrés dans une grande variété de secteurs. Il peut s'agir de spécialistes d'un domaine de la cybersécurité, de généralistes de la cybersécurité ou même de membres du personnel TI généralistes auxquels on a confié la responsabilité de la cybersécurité. Des recherches antérieures ont révélé que l'investissement dans le personnel de cybersécurité est plus courant dans les grandes organisations au Canada, ce qui pourrait suggérer que les petites organisations sont plus susceptibles de confier au personnel TI généraliste des responsabilités liées à la cybersécurité. Une étude a révélé que si près d'un tiers (29,6 %) des petites organisations (<100 employées/employés) ont déclaré ne pas avoir de personnel de cybersécurité, seulement une sur 14 (7,4 %) des moyennes et grandes organisations (100+ employées/employés) a fait de même[43]. Ces données font écho à la recherche effectuée par (ISC)² qui révèle que les professionnelles/professionnels de la cybersécurité sont le plus souvent employées/employés dans les services TI (22 %), les services financiers (8 %) et le gouvernement (7 %[44]).

[43] Enquête sur l'adoption des TIC, Chambre de commerce du Canada, 2017.

Partout au Canada, de nombreuses industries emploient des professionnelles/professionnels de la cybersécurité. La figure suivante identifie les industries les plus susceptibles d'employer au moins une partie du personnel de cybersécurité, en commençant par les finances et les assurances, où 91,6 % du secteur au Canada a au moins une employées ou un employé désignée/désigné à la cybersécurité.

LES 10 INDUSTRIES QUI EMPLOIENT LE PLUS DE PERSONNEL EN CYBERSÉCURITÉ AU CANADA
Source : Statistique Canada, Enquête canadienne sur la cybersécurité et la cybercriminalité, 2017.

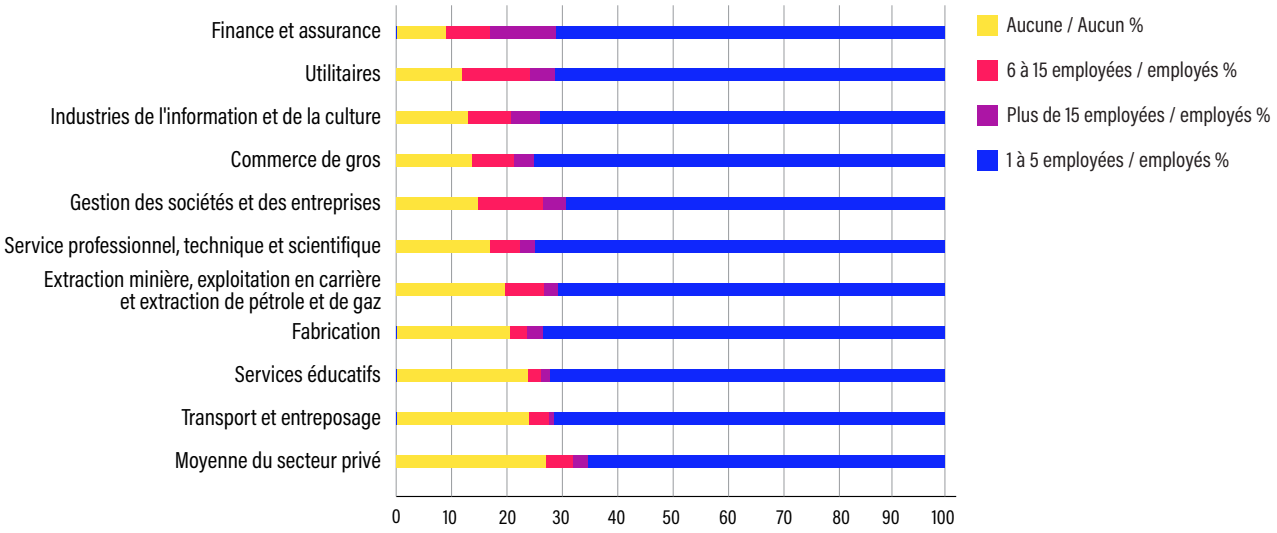


Figure 8: Percentage of businesses indicating the number of employees primarily responsible for overall cybersecurity, including the top 10 industries that are the most likely to have at least one employee responsible for cybersecurity, as well as the private sector average. Source: Statistics Canada 2017 Survey of Cybersecurity and Cyber crime.

Chômage

La cybersécurité est un domaine hautement compétitif avec un fort déficit de talents. À ce titre, il n'est guère surprenant que le taux de chômage dans le domaine de la cybersécurité soit très faible, même selon les normes du secteur des TIC. Certains rapports internationaux sur le déficit de main-d'œuvre en cybersécurité vantent des taux de chômage mondiaux aussi bas que 0 %[45]. Toutefois, ces rapports ne sont pas réalistes car un certain niveau de chômage frictionnel se produira toujours en raison des délais entre les travailleuses et travailleurs qui changent d'emploi.

[44] *Strategies for Building and Growing Strong Cybersecurity Teams*, loc. cit.

[45] Voir, par exemple, des histoires comme suit : Mack Gelber, *This tech field just hit an astonishing 0% unemployment rate*, Monster, n.d., https://www.monster.com/career-advice/article/tech-cybersecurity-zero-percent-unemployment-1016.

Conditions de travail

Le domaine de la cybersécurité connaissant une importante pénurie de talents dans un contexte de croissance rapide de la cybercriminalité, il n'est guère étonnant que la cybersécurité soit un domaine présentant des niveaux substantiels de stress et d'épuisement professionnel. Selon une étude de 2022, plus de la moitié (57 %) des professionnelles étasuniennes et professionnels étasuniens de la cybersécurité ont déclaré avoir subi un stress accru dû à la rotation du personnel au cours des six derniers mois et un sur cinq envisageait de quitter son emploi[46]. Une étude étasunienne antérieure datant de 2021 a révélé que la moitié (51 %) des professionnelles/professionnels de la cybersécurité ont connu « un stress extrême ou un épuisement professionnel » et que deux tiers (65 %) ont envisagé de quitter leur emploi en raison du stress[47]. Certaines personnes interrogées dans le cadre d'études antérieures du CTIC ont attesté d'une sorte de « cercle vicieux » dans le recrutement en cybersécurité; la pénurie de talents contribue à faire grimper les salaires, mais entraîne également des niveaux élevés de stress et d'épuisement professionnel qui ternissent l'image de la profession et contribuent ainsi à renforcer la pénurie de talents initiale.

[46] *Cybersecurity staff turnover and burnout: How worried should organizations be?*, Helpnet Security, 2022, https://www.helpnetsecurity.com/2022/01/31/cybersecurity-teams-retention-issues/.

[47] J. Pollard, *Predictions 2022* : Cybersecurity, Risk, And Privacy, Forrester, 2021, https://www.forrester.com/report/predictions-2022-cybersecurity-risk-and-privacy/RES176406.

COMPRENDRE LA MAIN-D'ŒUVRE DE LA CYBERSÉCURITÉ

Les professionnelles/professionnels de la cybersécurité varient considérablement en termes de responsabilités, de formation, de compétences, de niveaux d'expérience et de certifications. Il peut être difficile de trouver la bonne combinaison de qualifications. Dans une étude réalisée en 2018 par Deloitte sur l'écosystème de la cybersécurité au Canada, la grande majorité (76 %) des dirigeantes principales de la sécurité de l'information et des dirigeants principaux de la sécurité de l'information ont indiqué que trouver la bonne combinaison de compétences techniques, analytiques et non techniques constituait un défi important lors du recrutement de personnel en cybersécurité[48]. En même temps, les professionnelles/professionnels de la cybersécurité sont hautement qualifiées/qualifiés et certifiées/certifiés. Dans une étude de 2019 portant sur un échantillon de plus de 3 000 professionnelles/professionnels de la cybersécurité dans le monde, la répondante moyenne ou le répondant moyen avait quatre ans d'expérience dans son poste actuel, cinq ans d'expérience dans un rôle de cybersécurité, six ans d'expérience dans son organisation actuelle, neuf ans d'expérience dans des rôles TI, quatre certifications d'organisations de sécurité et trois adhésions à des organisations de sécurité[49].

Compétences techniques et compétences non techniques

Les intitulés et les descriptions de postes dans l'écosystème de la cybersécurité ne sont pas toujours faciles à catégoriser en raison des besoins idiosyncratiques des différentes organisations, ainsi que de la méconnaissance générale que beaucoup ont de la terminologie liée au domaine. Les employeuses et employeurs rédigent souvent des descriptions d'emploi très larges pour attirer un large éventail de candidates et candidats et, par conséquent, les descriptions d'emploi ressemblent souvent à des « listes de souhaits » organisationnels[50].

Les compétences précises requises pour les différents types de professionnelles/professionnels de la cybersécurité varient en fonction de leur niveau d'expérience, de leur domaine de focalisation ou de spécialisation, et de la technologie spécifique de l'employeuse ou de l'employeur. Assurer la sécurité d'une base de données, par exemple, exige un ensemble de compétences légèrement différent de celui nécessaire pour sécuriser une application Web. La figure suivante identifie les principales compétences techniques en cybersécurité.

[48] Ibid.

[49] Strategies for Building and Growing Strong Cybersecurity Teams, loc. cit.

[50] C. Herron, et coll., Searching for Hidden Talent, 11 juin 2020, CTIC, https://medium.com/digitalthinktankictc/searching-for-hidden-talent-2fa7b44becaa?source=.

LES COMPÉTENCES TECHNIQUES LES PLUS IMPORTANTES - ENQUÊTE 2021

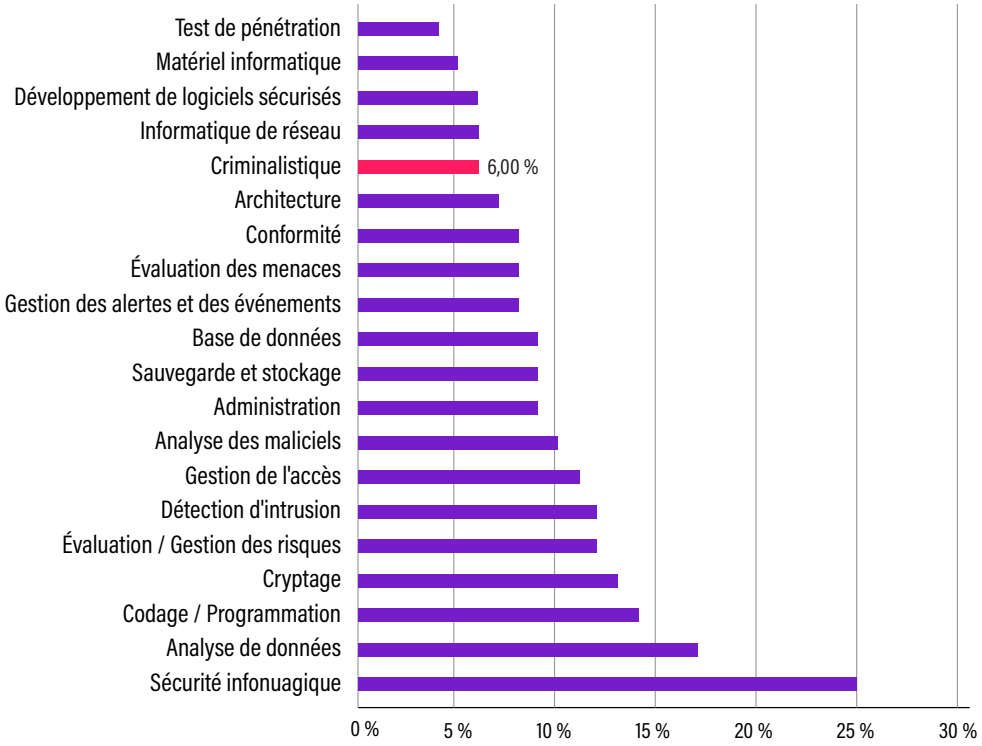


Figure 9 - Comparaison de l'importance des compétences techniques des rôles de cybersécurité - Enquête 2021[51].

Les professionnels de la cybersécurité ont également besoin de compétences non techniques pour bien exercer leur emploi. Certaines de ces compétences, comme la résolution de problèmes et la communication efficace, peuvent être acquises dans un contexte éducatif, tandis que d'autres sont plus adaptées à un apprentissage « sur le tas ». Ces compétences s'appliquent souvent à de nombreux types de rôles différents. Parmi les exemples de compétences non techniques nécessaires en cybersécurité, citons le souci du détail, la visualisation, la conscience des risques, la communication efficace, la résolution de problèmes[52], le raisonnement logique[53], l'adaptabilité, la passion, la curiosité et le travail en équipe[54].

[51] *The Cybersecurity Career Pursuers Study: A Roadmap to Building Resilient Cybersecurity Teams*, (ISC)², 2021, https://www.isc2.org/Research/CareerPursuers?utm_source=isc2&utm_medium=pressrelease&utm_campaign=GBL-careerpursuersreport&utm_content=report.

[52] Michael Kassner, *Don't forget to evaluate soft skills when hiring for cybersecurity positions*, TechRepublic, 2021, https://www.techrepublic.com/article/dont-forget-to-evaluate-soft-skills-when-hiring-for-cybersecurity-positions/.

[53] Bret Fund, *16 Soft Skills You Need to Succeed in Cyber Security*, Flatiron School, 2021, https://flatironschool.com/blog/soft-skills-cyber-security/.

[54] *Soft Skills in Cybersecurity: Communication and Training Are Key*, Maryville University, consulté en 2022, https://online.maryville.edu/online-masters-degrees/cyber-security/careers/skills-in-cybersecurity/.

Formation et éducation pour une carrière en cybersécurité

La cybersécurité est un domaine qui évolue rapidement et attire des professionnelles ambitieuses et professionnels ambitieux et motivées/motivés qui aiment acquérir de nouvelles compétences. C'est également un domaine dans lequel les parcours d'éducation et de carrière ne sont pas clairement définis; une étude réalisée en 2019 par (ISC)² a révélé que près de la moitié des professionnelles/professionnels de la cybersécurité n'ont pas commencé leur carrière en ayant l'intention de poursuivre la cybersécurité[55].

Les voies d'accès au domaine de la cybersécurité peuvent être divisées en trois grandes catégories : certification, diplôme d'études collégiales ou certificat de deuxième cycle, et baccalauréat ou diplôme de deuxième cycle[56]. Ces voies peuvent différer en fonction de l'étape de la carrière et de la spécialisation prévue dans les rôles de cybersécurité.

LES PARCOURS TRADITIONNELS POSTSECONDAIRES

L'Institut canadien pour la cybersécurité, basé à l'Université du Nouveau-Brunswick, propose des cours de cybersécurité et des certifications avancées[57]. De nombreuses universités et institutions postsecondaires canadiennes offrent un enseignement en cybersécurité bien que les programmes de baccalauréat et de maîtrise axés sur la cybersécurité soient rares[58].

NOUVELLES VOIES D'ÉDUCATION

Les camp de redressement de codage, les cours en ligne ouvert aux masses (CLOM) et d'autres formes d'éducation émergentes constituent une approche alternative ou complémentaire à l'éducation traditionnelle dans les universités ou les collèges. Ils peuvent également être plus faciles à mettre à l'échelle que les programmes traditionnels, offrant ainsi une forme plus accessible de formation technique à certaines étudiantes et à certains étudiants. Cependant, alors que les camp de redressement de codage et les CLOM ont été très perturbateurs et ont connu un grand succès dans des domaines tels que le développement de logiciels, mais leur adoption dans le domaine de la cybersécurité a été comparativement faible.

Aucune étude formelle ne s'est penchée sur cette divergence pour plusieurs raisons. Premièrement, la cybersécurité est un petit domaine très spécialisé, ce qui rend difficile la conception d'un curriculum généraliste qui permettrait une transition rapide vers le monde du travail. Deuxièmement, le fait que les emplois dans le domaine de la cybersécurité soient si bien rémunérés et que le taux de chômage soit si faible peut paradoxalement entraver la croissance des possibilités d'éducation : les expertes et experts du domaine peuvent opter pour des emplois bien rémunérés dans le domaine de la cybersécurité plutôt que d'investir leur temps à contribuer à des programmes éducatifs.

---

[55] *Ibid*.

[56] *Cyber Security Career Pathways*, Centre canadien pour la cybersécurité, 2022, https://cyber.gc.ca/en/guidance/career-pathways.

[57] *Canadian Institute for Cybersecurity*, Université du Nouveau-Brunswick, 2021, https://www.unb.ca/cic/.

[58] *Forensic Investigation (Digital Forensics and Cybersecurity Option)*, Institut de technologie de la Colombie-Britannique, 2021, https://www.bcit.ca/programs/forensic-investigation-digital-forensics-and-cybersecurity-option-advanced-certificate-part-time-526jadcert/.

CERTIFICATIONS

Les certifications sont une caractéristique majeure de l'écosystème de la cybersécurité. Une étude de 2019 a révélé que 59 % des professionnelles/professionnels de la cybersécurité prévoyaient d'obtenir au moins une certification cette année-là ou en poursuivaient déjà une[59]. La formation spécifique à la cybersécurité peut inclure une formation obtenue à partir d'une ancienne expérience professionnelle dans le domaine de la cybersécurité ou par le biais d'un titre spécifique à la cybersécurité tel qu'un certificat professionnel. Les certifications Microsoft Solutions Architect (MCSA) permettent aux employées/employés de la cybersécurité de personnaliser leur ensemble de compétences tout en fournissant un cadre fiable pour communiquer les compétences au-delà des frontières nationales et sectorielles. Cependant, bien qu'utiles pour l'industrie de la cybersécurité, les certifications peuvent être coûteuses, et le prix de nombreuses certifications a été critiqué comme dissuadant les entrantes potentielles et entrants potentiels dans le domaine. Une étude réalisée en 2019 par (ISC)² a révélé que seules/seuls 37 % des professionnelles/professionnels de la cybersécurité voyaient leurs certifications entièrement payées par leur organisation tandis que 35 % étaient entièrement responsables du paiement de leur propre certification[60].

Voici quelques exemples de certifications pertinentes dans le domaine de la cybersécurité :

Les principes fondamentaux de la cybersécurité (Cyber Security Fundamentals)

GIAC Security Essentials

CompTIA Security+

Praticienne/Practicien en sécurité avancée de CompTIA (CompTIA Advanced Security Practitioner)

Professionnelle/Professionnel certifiée/certifié en sécurité des systèmes d'information (Certified Information Systems Security Professional)

Gestionnaire de la sécurité de l'information certifié (Certified Information Security Manager)

Certifiée/Certifié en contrôle des risques et des systèmes d'information (Certified in Risk and Information Systems Control)

Praticienne/Practicien certifiée/certifié en sécurité des systèmes (Systems Security Certified Practitioner)

Dirigeante principale de la sécurité de l'information certifiée/Dirigeant principal de la sécurité de l'information certifié (Certified Chief Information Security Officer)

Première répondante/Premier répondant CyberSec (CyberSec First Responder)

Utilisatrice/Utilisateur certifiée/certifié d'ordinateurs sécurisés (Certified Secure Computer User)

[59] *Strategies for Building and Growing Strong Cybersecurity Teams*, loc. cit.

[60] *Ibid*.

Professionnelle/Professionnel certifiée/certifié du cycle de vie des logiciels sécurisés (Certified Secure Software Lifecycle Professional)

Professionnelle/Professionnel certifiée/certifié en sécurité sans fil (Certified Wireless Security Professional)

CertNexus CyberSAFE®

Hackeuse éthique certifiée/Hacker éthique certifié (Certified Ethical Hacker)

Auditrice/Auditeur certifiée/certifié de systèmes d'information (Certified Information Systems Auditor)

Professionnelle/Professionnel certifiée/certifié de la sécurité infonuagique (Certified Cloud Security Professional)

Praticienne/Praticien Nexus de la cybersécurité (Cyber Security Nexus Practitioner)

Professionnelle/Professionnel certifiée/certifié en sécurité offensive (Offensive Security Certified Professional)

Professionnel de la sécurité de l'information GIAC (GIAC Information Security Professional)

Certification de leadership en matière de sécurité GIAC (GIAC Security Leadership Certification)

Les principes fondamentaux de la sécurité de l'information GIAC (GIAC Information Security Fundamentals)

Analyste certifiée/certifié GIAC en protection du périmètre (GIAC Certified Perimeter Protection Analyst)

Analyste d'intrusion certifiée/certifié GIAC (GIAC Certified Intrusion Analyst)

Gestionnaire d'incidents certifiée/certifié GIAC (GIAC Certified Incident Handler)

Administratrice/Administrateur de sécurité UNIX certifiée/certifié GIAC (GIAC Certified UNIX Security Administrator)

Administratrice/Administrateur certifiée/certifié GIAC de sécurité Windows (GIAC Certified Windows Security Administrator)

GIAC Certified Enterprise Defender

Testeuse/Testeur d'intrusion d'applications Web certifiée/certifié GIAC (GIAC Certified Web Application Penetration Tester)

Évaluation des réseaux sans fil GIAC (GIAC Assessing Wireless Networks)

Professionnelle/Professionnel de la cybersécurité industrielle mondiale (Global Industrial Cybersecurity Professional)

Certification GIAC Contrôles critiques (GIAC Critical Controls Certification)

Testeuse/Testeur d'intrusion GIAC (GIAC Penetration Tester)

Experte/Expert en sécurité GIAC (GIAC Security Expert[61])

[61] *Cyber Security Career Pathways,* loc. cit.

La partie de cette étude consacrée au sondage interne auprès des étudiantes et étudiants s'appuie sur les conclusions des études précédentes. Pour chaque certification, il n'y a pas une seule certification que plus de 15 % des étudiantes et étudiants prévoient de poursuivre, probablement en raison de la grande variété de certifications disponibles. En outre, près d'un quart des répondantes et répondants ont déclaré qu'elles/qu'ils ne poursuivaient pas de certifications parce qu'elles étaient « trop chères ». Près d'un tiers ont déclaré qu'elles/qu'ils ne poursuivaient pas de certification parce que les conditions préalables pour les obtenir étaient trop exigeantes.

LES MICROCERTIFICATIONS

En plus des certifications traditionnelles pour les compétences en cybersécurité, il existe également des options de microcertification plus nombreuses. Les microcertifications sont des certifications de compétences évaluées qui sont « additionnelles, alternatives, complémentaires ou une composante d'une qualification formelle[62] ».

Voici quelques exemples de microcertifications en matière de cybersécurité :

- Cybersécurité - Détection d'intrusion (Cybersecurity – Intrusion Detection[63])
- Opérations de cybersécurité Cisco (Cyber Security Operations (Cisco[64])
- Criminalistique numérique (Digital Forensics[65])
- Microaccréditation générale en cybersécurité (General Cyber-Security Micro-credential[66])
- Cybersécurité – Offensive (Cybersecurity – Offensive[67])

SALAIRE

Les salaires élevés sont un thème récurrent tant dans les recherches antérieures du CTIC que dans les études externes. Un tiers des officières principales de la sécurité de l'information canadiennes et des officier principaux de la sécurité de l'information canadiens (OPSI) estiment que les régimes de rémunération en cybersécurité ont été gonflés par la demande[68], et lorsqu'on étend cette impression à l'Amérique du Nord, elle est partagée par 41 % des répondantes

[62] *National Framework for Microcredentials*, Collèges & Instituts Canada, 2022, https://www.collegesinstitutes.ca/policyfocus/micro-credentials/.

[63] *ACS Microcredentials*, Australian Computer Society (ACS), 2022, https://www.acs.org.au/professionalrecognition/microcredentials-home.html.

[64] *Cyber Security Operations (Cisco)*, Futurelearn, 2022, https://www.futurelearn.com/microcredentials/cybersecurity-operations.

[65] V. Combs, *Micro-credentials are a quicker and cheaper way to improve your resume*, TechRepublic, 2020, https://www.techrepublic.com/article/micro-credentials-are-a-quicker-and-cheaper-way-to-improve-your-resume/.

[66] *Cyber-Security Micro-credential*, BMCC, 2022, https://www.bmcc.cuny.edu/cyber-security-micro-credential/.

[67] *Microcredential Cybersecurity Offensive*, Sheridan College, 2022, https://caps.sheridancollege.ca/products/cybersecurity-offensive.aspx.

[68] *The changing faces of cybersecurity: Closing the cyber risk gap*, op. cit., p. 12-14.

et répondants[69]. Au Canada, 27 % des entreprises interrogées par l'Autorité canadienne pour les enregistrements Internet (CIRA) ont déclaré qu'elles ne disposaient pas des ressources nécessaires pour employer une professionnelle ou un professionnel de la cybersécurité, et les entreprises qui engageaient des consultantes et consultants externes en cybersécurité consacraient en moyenne 19 % de leur budget TI total à la cybersécurité[70].

Les salaires de la cybersécurité sont influencés par les mêmes facteurs que la plupart des autres emplois : ancienneté, expérience, éducation formelle. L'étude (ISC)² Cybersecurity Workforce Study de 2019 a révélé que les employées/employés certifiées/certifiés en cybersécurité en Amérique du Nord avaient un salaire moyen de 93 000 USD, tandis que les employées/employés non certifiées/certifiés ne gagnaient que 76 500 USD[71]. Cependant, il n'a pas été possible de déterminer si cet effet était causal, car la certification aurait pu être corrélée à des facteurs tels que l'expérience.

Les salaires peuvent également varier considérablement en fonction du rôle. Selon les données de Hays Canada, les salaires les plus bas se trouvent dans les rôles d'administration, d'analyse ou de conseil. Les salaires dans ces rôles varient de moins de 50 000 CAD à un peu moins de 100 000 CAD. Les rôles d'ingénierie et d'architecture varient de 80 000 à 160 000 CAD. Les salaires les plus élevés en cybersécurité vont aux cadres, tels que les Officiers principaux de la sécurité de l'information, et les vice-présidents ou directeurs de la sécurité de l'information. Les salaires à ce niveau commencent à six chiffres et peuvent dépasser 200 000 CAD.

RÔLE	FOURCHETTE DE SALAIRE MOYEN
Officière/Officier principale/principal de la sécurité de l'information (OPSI)	180 000 à 230 000
VP, Sécurité de l'information	130 000 à 200 000
Architecte de sécurité d'entreprise	130 000 à 160 000
Directrice/Directeur, Sécurité de l'information	100 000 à 150 000
Architecte de sécurité réseau	105 000 à 135 000
Architecte de la sécurité infonuagique	90 000 à 130 000
Ingénieure/Ingénieur en sécurité des applications	80 000 à 110 000
Analyste en criminalistique numérique	65 000 À 95 000
Testeuse/Testeur d'intrusion principale/principal	60 000 À 90 000
Conseil en sécurité des données	60 000 À 90 000
Analyste de logiciels malveillants	60 000 À 90 000
Administratrice/Administrateur de la sécurité	45 000 À 75 000

Figure 10 - Échelle nationale des salaires pour les rôles de cybersécurité. Source : Hays Canada[72].

[69] Frost & Sullivan, op. cit., p. 4.

[70] *Fall 2018 Cybersecurity Survey Report*, ACEI, 2018, p. 10.

[71] *Strategies for Building and Growing Strong Cybersecurity Teams*, loc. cit.

[72] « Les salaires sont exprimés en dollars canadiens et ne tiennent pas compte des avantages sociaux, des primes ou de tout autre arrangement entre les employeuses et employeurs et les candidates et candidats. » *Ibid*.

L'examen des codes CNP liés à la cybersécurité sacrifie la précision mais permet d'accéder à davantage de données. Bien qu'il y ait quelques divergences selon que l'on utilise les données sur les offres d'emploi de l'entreprise de données sur le marché du travail EMSI (qui compte beaucoup moins d'observations) ou les données de l'Enquête sur la population active de Statistique Canada, toutes les données s'harmonisent globalement et montrent qu'au Canada, les rôles correspondant aux Gestionnaires des systèmes informatiques (CNP 0213) sont les mieux rémunérés, tandis que les Évaluateurs/évaluatrices de systèmes informatiques (CNP 2283) et les Techniciens/techniciennes de réseau informatique (CNP 2281) sont les moins bien payées/payés.

**SALAIRES MÉDIANS DANS LES CODES CNP RELATIFS À LA CYBERSÉCURITÉ
DONNÉES DE L'EMSI ET DE STATISTIQUE CANADA**

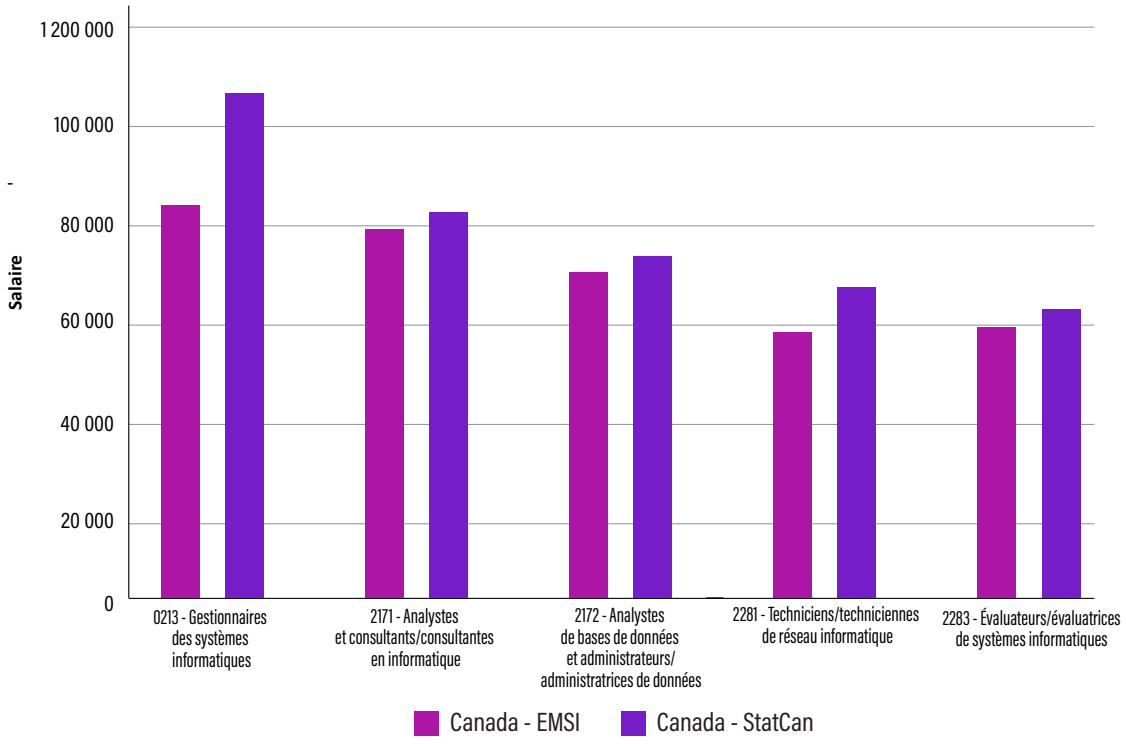


Figure 11 - Salaire médian (salaire de base) par source de données et par région pour la Classification nationale des professions des TIC liés à la cybersécurité. Source : analyse du CTIC, données de l'EMSI et de Statistique Canada, 2020.

ÉQUITÉ, DIVERSITÉ ET INCLUSION DANS LA CYBERSÉCURITÉ

ÉQUITÉ, DIVERSITÉ ET INCLUSION DANS LA CYBERSÉCURITÉ

L'étude 2021 (ISC)² sur la main-d'œuvre en cybersécurité a estimé qu'il y avait une pénurie de 25 000 professionnelles/professionnels de la cybersécurité au Canada[73]. Toutefois, ce chiffre pourrait être beaucoup plus élevé étant donné la présence attestée d'un important marché caché de l'emploi en cybersécurité[74].

Un manque de diversité dans les viviers de talents en cybersécurité peut prolonger la pénurie de talents. Par exemple, les OPSI canadiennes et canadiens ont noté que la sous-représentation des femmes contribue au faible nombre de professionnelles/professionnels expérimentées/expérimentés en cybersécurité[75]. Un rapport publié en 2021 par (ISC)² a également révélé que les personnes de couleur et les femmes étaient sous-représentées dans le domaine de la cybersécurité. Une recherche canadienne a révélé que seulement 20 % des travailleuses et travailleurs en cybersécurité au Canada s'identifient comme des femmes et que seulement 25 % s'identifient comme des personnes autochtones, noires et de couleur (PANDC[76]).

Les disparités entre les sexes se produisent à tous les niveaux d'expérience. L'enquête interne du CTIC auprès des étudiantes et étudiants a révélé que les femmes abandonnent la cybersécurité à un taux 50 % plus élevé que les hommes. Alors que 30 % des hommes ayant répondu à l'enquête ont déclaré avoir quitté le domaine, plus de 50 % des femmes l'ont fait. À l'autre extrémité du spectre d'expérience, une recherche sur l'industrie nord-américaine de la cybersécurité a révélé que les hommes sont quatre fois plus susceptibles d'occuper des postes de cadres et sont neuf fois plus susceptibles d'occuper des postes de gestion[77]. À l'échelle mondiale, en 2016, les femmes dans la cybersécurité ont gagné moins que les hommes à tous les niveaux d'emploi[78], même si les femmes entrent généralement dans la cybersécurité avec des niveaux d'éducation plus élevés que les hommes[79]. Les femmes dans la cybersécurité sont conscientes des difficultés qu'elles rencontrent. L'ISACA a constaté que lorsqu'on les interrogeait sur la disparité entre les sexes en matière de possibilités, seulement 41 % des employées de la cybersécurité estimaient que les femmes se voyaient offrir les mêmes options d'avancement que les hommes (contre 79 % des répondants masculins[80]).

Certains éléments indiquent que la diversité est prise plus au sérieux en tant qu'objectif dans le domaine de la cybersécurité. Le programme de formation accélérée en cybersécurité (Accelerated Cybersecurity Training Program, ACTP) de l'Université Ryerson – dorénavant connue comme la Toronto Metropolitan University - est conçu pour aider les personnes issues de milieux divers,

---

[73] *A Resilient Cybersecurity Profession Charts the Path Forward: (ISC)² Cybersecurity Workforce Study*, 2021, loc. cit.

[74] Rushmi Hasham, *Fostering innovation in cybersecurity through diversity and inclusion*, Future Skills Centre, 2022, https://fsc-ccf.ca/fostering-innovation-in-cybersecurity-edi/.

[75] *The changing faces of cybersecurity: Closing the cyber risk gap*, loc. cit.

[76] Rushmi Hasham, loc. cit.

[77] Frost & Sullivan, *The 2017 Global Information Security Workforce Study: Women in Cybersecurity*, 2017, https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf.

[78] Frost & Sullivan, *2017 Global Information Security Workforce Study*, op. cit., p. 5.

[79] Frost & Sullivan, *2017 Global Information Security Workforce Study*, op. cit., p. 10.

[80] *State of cybersecurity 2019: Current trends in workforce development*, ISACA, 2019, p. 14.

notamment l'éducation, les expériences, les différences culturelles et l'âge (en plus du sexe, de la race et de l'orientation sexuelle). Pour renforcer la diversité, le programme cible les femmes, les personnes en milieu de carrière, les personnes en réorientation de carrière et les nouvelles arrivantes et les nouveaux arrivants au Canada qui peuvent apporter de nouvelles idées et de nouveaux points de vue sur la cybersécurité[81].

L'un des problèmes identifiés liés à la diversité est le manque de mentorat et de possibilités de développer des compétences pertinentes dans les programmes universitaires traditionnels[82]. S'il existe des conditions préalables importantes (réelles ou perçues) pour obtenir d'abord un diplôme d'ingénieur ou d'informaticien, les personnes qui rencontrent des obstacles pour obtenir des diplômes universitaires traditionnels sont fortement découragées de poursuivre leurs études par des cours de cybersécurité[83].

L'enquête du CTIC sur le parcours des étudiants en cybersécurité montre des perceptions mitigées des obstacles à la diversité. Une pluralité de répondantes et de répondants ne sont ni d'accord ni en désaccord avec les obstacles à la diversité dans le domaine. Alors que les étudiantes et étudiants complètement en désaccord sont plus nombreuses et nombreux que celles et ceux qui sont complètement d'accord avec l'existence d'obstacles dans le domaine, les étudiantes et étudiants plutôt d'accord avec la présence d'obstacles liés à la diversité sont plus nombreuses et nombreux que celles et ceux qui sont plutôt en désaccord.

PERCEPTIONS DES CARRIÈRES EN CYBERSÉCURITÉ DES ÉTUDIANTES ET ÉTUDIANTS

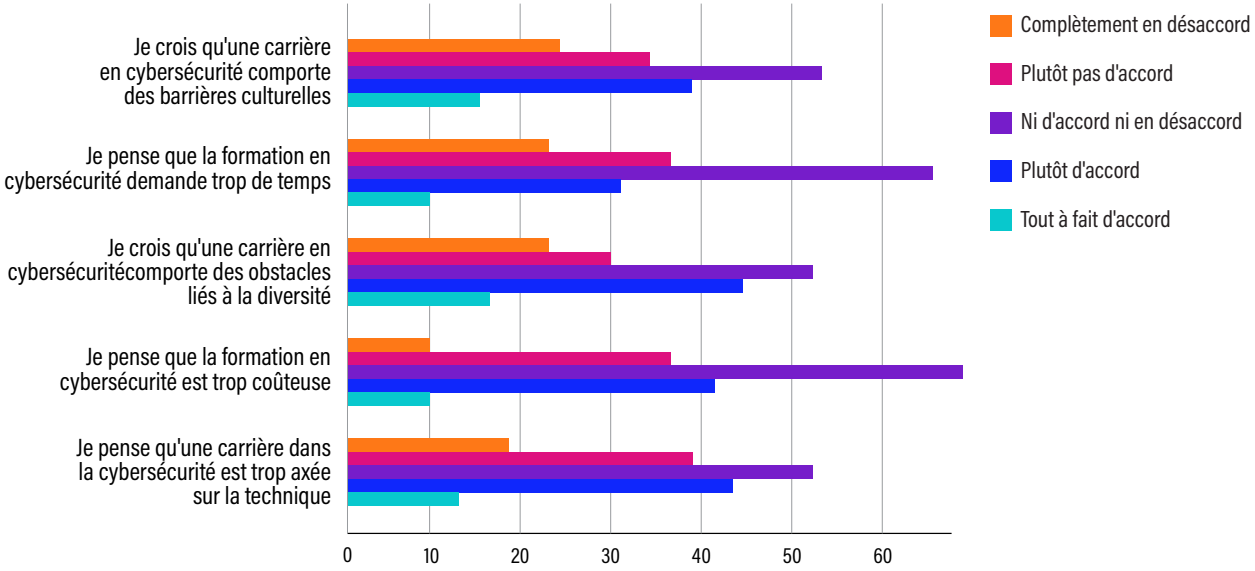


Figure 12 - Perception des étudiantes et étudiants des obstacles à une carrière en cybersécurité. Source : sondage du CTIC auprès des étudiantes et étudiants en cybersécurité, 2022

[81] Rushmi Hasham, loc. cit.

[82] Stefan Palios, To *Become More Diverse, Cybersecurity Experts say Industry Needs More Mentors and Problem Solvers*, BetaKit, 2021, https://betakit.com/to-become-more-diverse-cybersecurity-experts-say-industry-needs-more-mentors-and-problem-solvers/.

[83] *Ibid*.

CONSIDÉRATIONS POUR LA CONCEPTION D'UN PROGRAMME D'APPRENTISSAGE DE LA CYBERSÉCURITÉ

CONSIDÉRATIONS POUR LA CONCEPTION D'UN PROGRAMME D'APPRENTISSAGE DE LA CYBERSÉCURITÉ

Les personnes capables de réussir dans le secteur de la cybersécurité sont des « élites » en termes de compétences et de tempérament et seraient probablement très capables de réussir dans d'autres domaines techniques bien rémunérés tels que l'ingénierie logicielle ou la science des données. Assurer un solide vivier de talents ne consiste donc pas seulement à offrir des programmes de formation en cybersécurité qui répondent aux besoins de l'industrie; il s'agit également d'attirer des talents hautement qualifiés dans le domaine de la cybersécurité, de retenir leur intérêt et de leur permettre de développer un fort sentiment de connexion avec le domaine de la cybersécurité.

Étant donné le rôle important que les décisions et les perceptions des étudiantes et étudiants joueront dans la croissance du domaine de la cybersécurité, il est essentiel pour le CTIC d'analyser les expériences des étudiantes et étudiants en matière de cybersécurité afin de comprendre ce qui les attire dans ce domaine, les compétences qu'elles et qu'ils possèdent et les défis auxquels elles et ils sont confrontées/confrontés. La section suivante détaille les résultats de cette récente enquête menée par le CTIC auprès d'étudiantes et d'étudiants poursuivant des qualifications en cybersécurité au Canada.

L'objectif de cette recherche est de concevoir un programme pour compléter le pipeline de la cybersécurité. La conception d'un tel programme doit tenir compte des besoins des étudiantes et étudiants et des employeuses et employeurs lors de la conception d'un programme d'études.

Il existe une proposition de valeur substantielle dans un programme d'apprentissage intégré au travail (AIT). Une majorité d'anciennes étudiantes et d'anciens étudiants en cybersécurité ont déclaré que leur décision aurait pu être modifiée par l'offre d'AIT ou de microcertifications. Un plus petit nombre (moins de 10 %) était certain que leur décision n'aurait pas été influencée par ces éléments. Les autres étaient incertains.

Rôles principaux

Selon l'enquête menée auprès des étudiantes et étudiants dans le cadre de cette recherche, les emplois les plus fréquemment recherchés par les étudiantes et étudiants sont ceux d'ingénieur en cybersécurité, d'analyste en cybersécurité et d'analyste de réseau. Les rôles suscitant le moins d'intérêt sont la détection d'intrusion, la réaction en cas d'incident et les rôles de spécialistes des équipes rouges et bleues.

LES EMPLOIS DE CYBERSÉCURITÉ QUI INTÉRESSENT

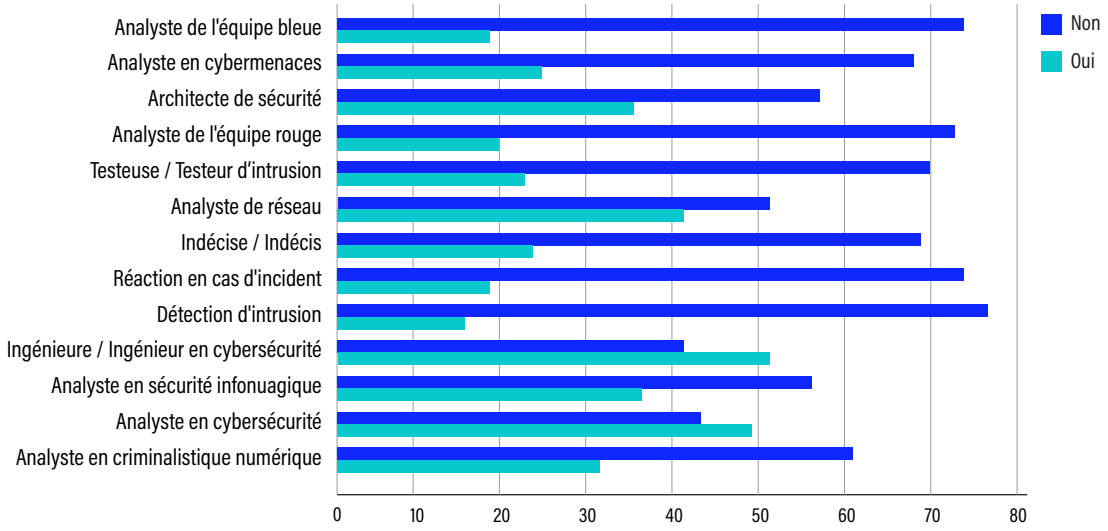


Figure 13 - Types d'emplois en cybersécurité qui intéressent les étudiantes et étudiants. Source : sondage du CTIC auprès des étudiantes et étudiants en cybersécurité, 2022

Les principaux rôles recherchés par les employeuses et employeurs sont les analystes en cybersécurité, les ingénieures/ingénieurs en cybersécurité et les analystes en sécurité. Les rôles les moins intéressants sont les analystes en cybermenaces, les analystes en criminalistique numérique et les analystes des équipes rouges et bleues

Dans l'ensemble, les principaux rôles recherchés par les étudiantes et étudiants correspondent bien aux principaux rôles recherchés par les employeuses et employeurs. Il s'agit d'une constatation heureuse pour la conception d'un programme qui attire les étudiantes et étudiants et répond aux besoins de l'industrie.

LES RÔLES DE CYBERSÉCURITÉ TRÈS RECHERCHÉS

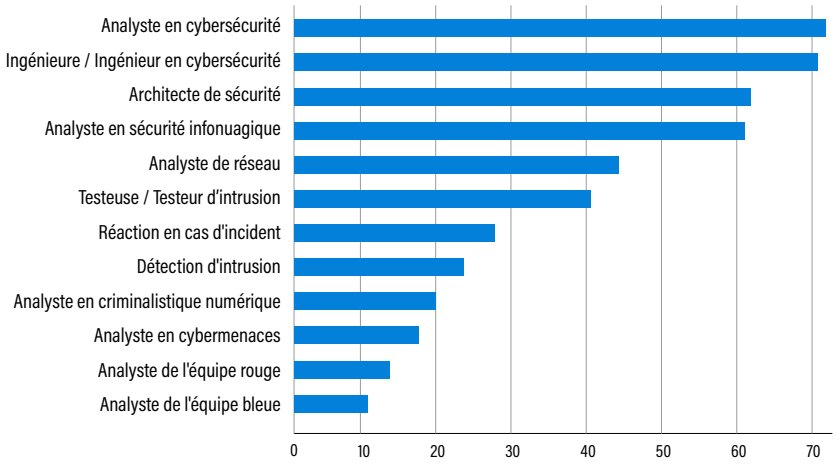


Figure 14 - Emplois en cybersécurité en forte demande. Source : Enquête du CTIC auprès des employeuses et employeurs en matière de cybersécurité, 2022.

Compétences techniques

L'enquête auprès des étudiantes et étudiants a révélé que les étudiantes et étudiants ont attribué les meilleures notes à leurs compétences en matière de systèmes d'exploitation, de protocoles Internet et de réseaux. Dans ces catégories, une pluralité d'entre elles et eux ont déclaré être « plutôt à l'aise ». Pour la sécurité infonuagique, la criminalistique numérique et la réaction en cas d'incident, une pluralité de répondantes et de répondants ont évalué leur confort comme étant « neutre ». Mais les étudiantes et étudiants en général semblaient quelque peu hésitantes et hésitants quant à leurs compétences - beaucoup moins se sont déclarées/déclarés « très à l'aise ».

Dans l'enquête auprès des employeuses et employeurs, la cryptographie est classée comme relativement moins cruciale que d'autres compétences techniques. Les opérations de sécurité, la sécurité des réseaux et la sécurité infonuagique sont identifiées comme les plus essentielles pour les rôles de cybersécurité. Notamment, la sécurité des réseaux obtient le plus grand nombre de votes pour « essentiel au rôle » et « une exigence pour l'embauche ».

CONFORT DES ÉTUDIANTES ET ÉTUDIANTS EN MATIÈRE DE COMPÉTENCES TECHNOLOGIQUES

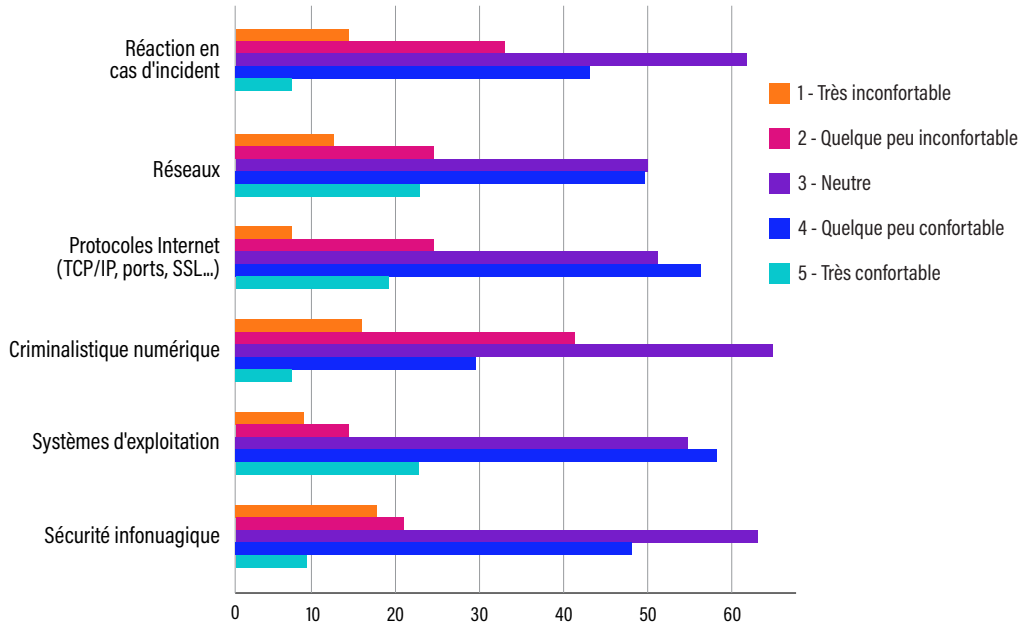


Figure 15 - Niveaux de confort des étudiantes et étudiants en cybersécurité avec diverses compétences techniques. Source : sondage du CTIC auprès des étudiantes et étudiants en cybersécurité, 2022.

IMPORTANCE DES COMPÉTENCES TECHNIQUES

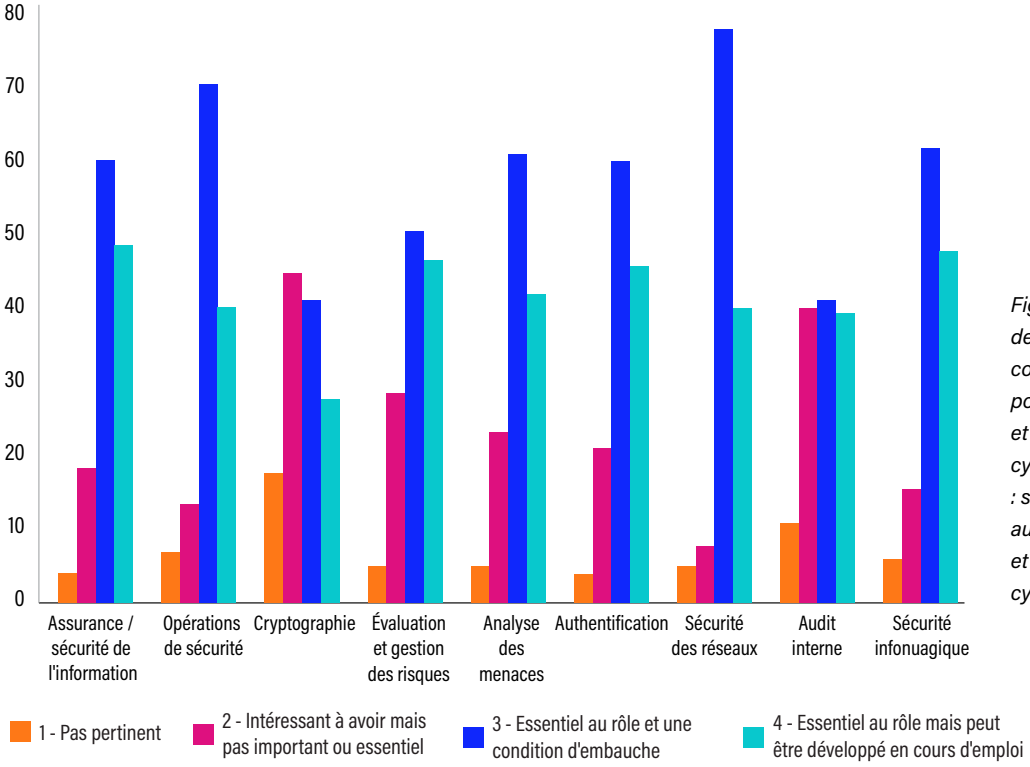


Figure 16 - Importance des diverses compétences techniques pour les employeuses et employeurs en cybersécurité. Source : sondage du CTIC auprès des employeuses et employeurs en cybersécurité, 2022.

L'enquête auprès des employeuses et employeurs a également invité les participantes et participants à identifier les compétences qui, selon elles et eux, font le plus défaut aux diplômées/diplômés des programmes de cybersécurité. La réponse la plus courante était la sécurité infonuagique qui est l'une des compétences techniques hautement essentielles, comme le montre le tableau précédent. En ce qui concerne la sécurité infonuagique, un plus grand nombre d'employeuses et d'employeurs ont indiqué qu'il s'agissait d'une exigence nécessaire à l'embauche plutôt que d'une capacité qui peut être développée en cours d'emploi. Il est donc important que les établissements d'enseignement et les étudiantes et étudiants s'assurent qu'elles et qu'ils peuvent acquérir ces compétences en matière de sécurité infonuagique avant d'entrer sur le marché du travail. Les autres lacunes importantes en matière de compétences sont la réaction en cas d'incident et la criminalistique numérique, bien que les employeuses et employeurs signalent une demande considérablement moins importante pour ces compétences que pour la sécurité infonuagique.

COMPÉTENCES EN CYBERSÉCURITÉ DONT LES DIPLÔMÉES/ DIPLÔMÉS MANQUENT LE PLUS

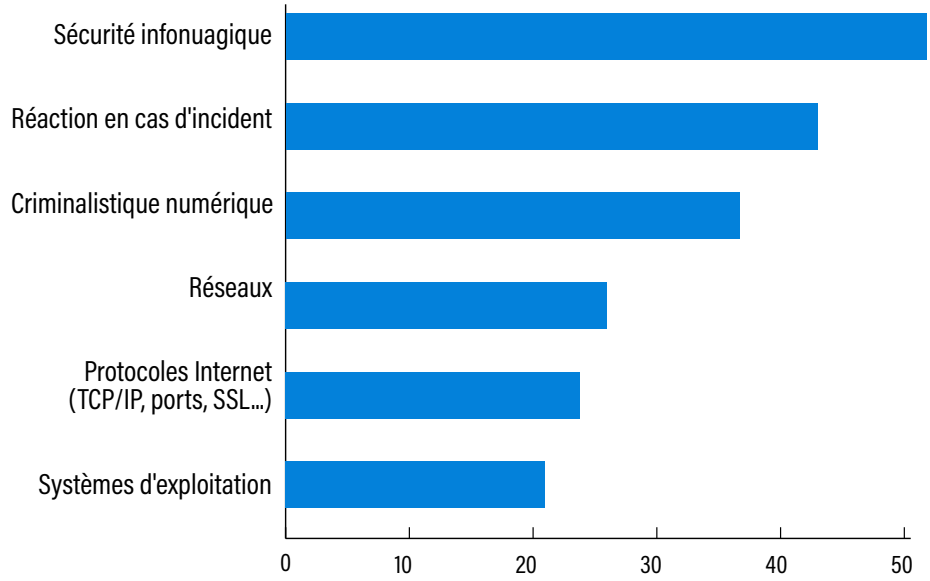


Figure 17 - Domaines de compétences qui font le plus défaut aux diplômées/diplômés des programmes de cybersécurité, selon les employeuses et employeurs du secteur de la cybersécurité. Source : sondage du CTIC auprès des employeuses et employeurs en cybersécurité, 2022.

Les compétences non techniques

L'enquête auprès des étudiantes et étudiants a révélé que les étudiantes et étudiants en cybersécurité sont assez confiantes et confiants dans leurs compétences « générales » ou « non techniques ». Pour huit des neuf domaines de compétences profilés, une pluralité de répondantes et de répondants ont indiqué qu'elles et qu'ils étaient très à l'aise dans leurs capacités. Les réponses étaient orientées vers le côté positif. Pour les neuf domaines de compétences, seul un très faible pourcentage (moins de 10 %) a indiqué être très mal à l'aise ou quelque peu mal à l'aise. Les domaines de compétences ayant les plus hauts niveaux de confiance sont « Lecture et écriture », « Communication » et « Adaptabilité ». « Travailler sous pression » présente les plus faibles niveaux de confiance autodéclarés, et c'est le seul domaine de compétences dans lequel une pluralité a déclaré n'être que « plutôt à l'aise ». À ce titre, les futurs programmes pourraient souhaiter ajouter d'autres possibilités pour les étudiantes et étudiants de travailler dans des environnements à forte pression (missions à durée limitée, par exemple). Cependant, des recherches supplémentaires pourraient également être nécessaires pour déterminer si ces niveaux de confiance autoévalués correspondent aux évaluations des employeuses et employeurs en cybersécurité.

LE CONFORT DES ÉTUDIANTES ET ÉTUDIANTS EN MATIÈRE DE COMPÉTENCES NON TECHNIQUES

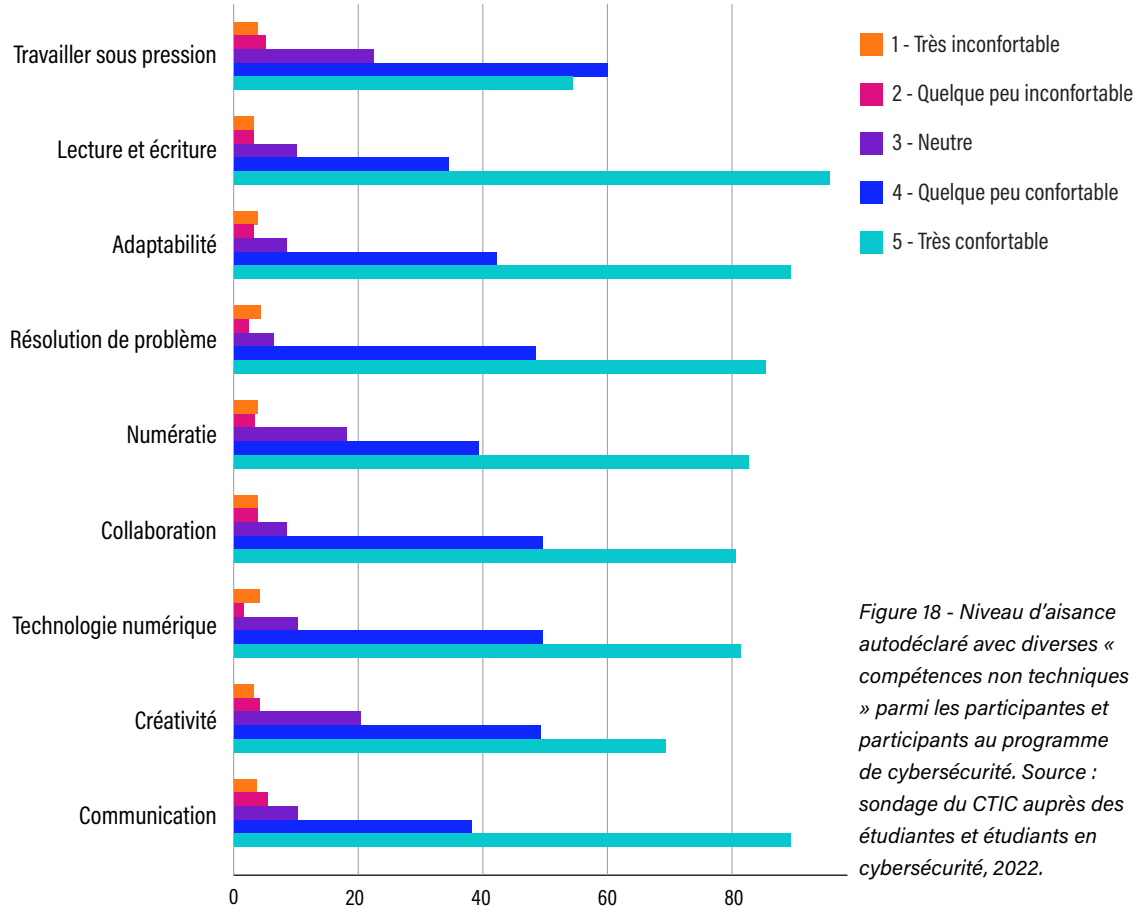


Figure 18 - Niveau d'aisance autodéclaré avec diverses « compétences non techniques » parmi les participantes et participants au programme de cybersécurité. Source : sondage du CTIC auprès des étudiantes et étudiants en cybersécurité, 2022.

Les employeuses et employeurs considèrent la plupart des compétences non techniques comme « essentielles au rôle et une condition d'embauche » (en particulier la fiabilité) ou « essentielles au rôle mais pouvant être développées en cours d'emploi ». Par rapport aux autres compétences non techniques, le leadership et la créativité sont différents. Le leadership est généralement considéré comme « agréable à avoir » mais pas important ou essentiel; il a reçu le plus grand nombre de votes « non pertinent » de toutes les compétences non techniques. La créativité obtient très peu de réponses « non pertinentes », mais elle a une part similaire de réponses pour « bon à savoir », « essentiel et une condition d'embauche » et « essentiel mais peut être développé en cours d'emploi ». Les compétences hautement essentielles sont la pensée critique/analytique, la résolution de problèmes et le raisonnement.

IMPORTANCE DES COMPÉTENCES NON TECHNIQUES

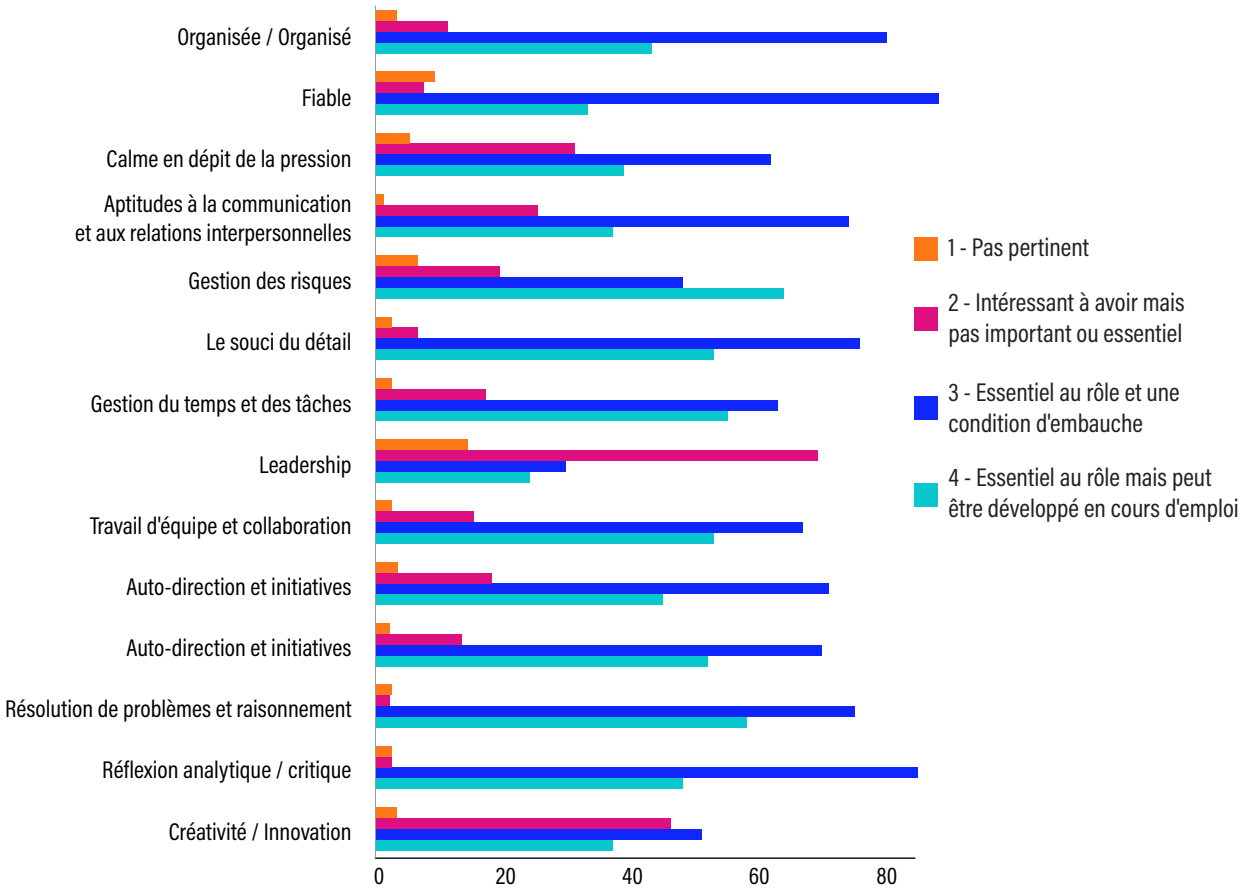


Figure 19 - Importance de diverses compétences non techniques pour les employeuses et employeurs en cybersécurité. Source : sondage du CTIC auprès des employeuses et employeurs en cybersécurité, 2022.

Cadres de travail

Les cadres suivants ont également été classés dans l'enquête auprès des employeuses et employeurs qui a révélé que certains sont plus pertinents que d'autres. Parmi ces cadres de cybersécurité, le cadre de cybersécurité du NIST reçoit le plus grand nombre de votes comme « très important » et « obligatoire ». Plus de réponses le considèrent comme « très important » que « assez important ». Les autres cadres reçoivent plus de votes pour « quelque peu important » que pour « très important ».

L'IMPORTANCE DES CADRES

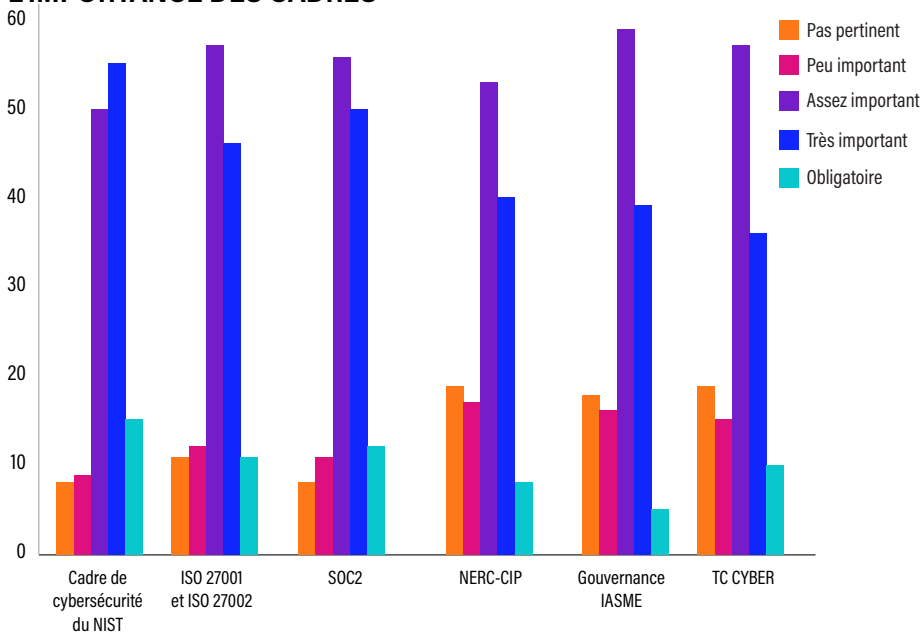


Figure 20 - Importance des différents cadres de cybersécurité pour les employeuses et employeurs de la cybersécurité. Source : sondage du CTIC auprès des employeuses et employeurs en cybersécurité, 2022.

Certifications

La certification du secteur est généralement considérée comme moins importante que la connaissance des cadres de cybersécurité par les diplômées/diplômés. Le CISSP (Certified Information Systems Security Professional) obtient le plus grand nombre de votes agrégés pour les mentions plutôt « important », « très important » et « obligatoire ».

IMPORTANCE DES CERTIFICATIONS DE L'INDUSTRIE

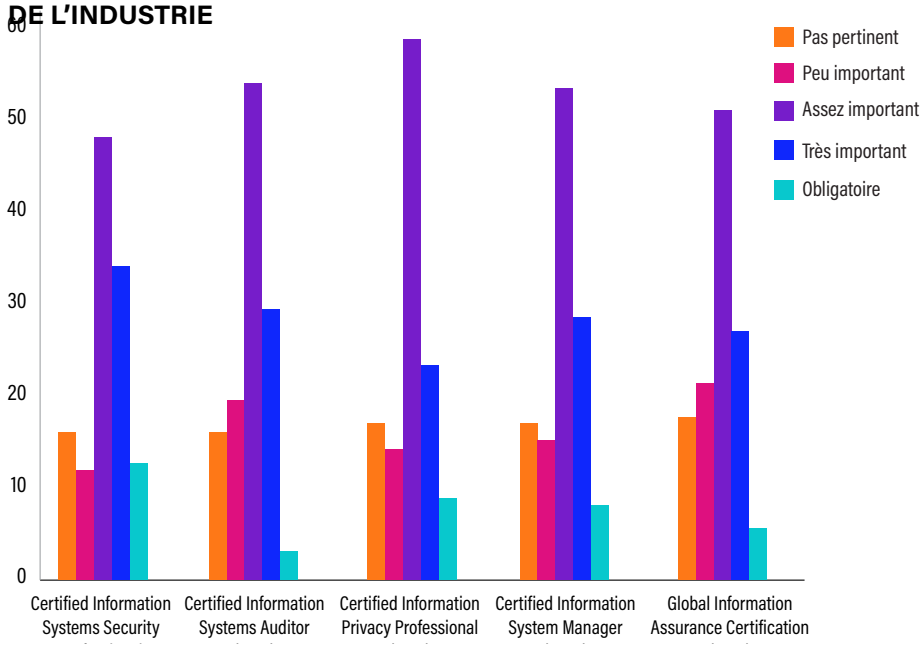


Figure 21 - Importance des diverses certifications en cybersécurité pour les employeuses et employeurs en cybersécurité. Source : sondage du CTIC auprès des employeuses et employeurs en cybersécurité, 2022.

Compétences en matière d'applications

Un programme efficace de préparation de la main-d'œuvre tiendra également compte du processus de candidature en particulier. L'enquête interne du CTIC auprès des employeuses et employeurs a révélé que les entreprises recherchent des talents par diverses méthodes allant des tableaux d'affichage des offres d'emploi au bouche-à-oreille. Les organisations ont identifié l'entrevue d'emploi comme l'aspect le plus important de la candidature. Le CV ou curriculum vitae du candidat a été considéré comme le deuxième élément le plus important lors de l'embauche. Notez que les missions/tests peuvent être considérés comme faisant partie de l'entrevue technique. Il n'est pas surprenant que les recommandations, le bouche-à-oreille ou les relations dans l'industrie soient également considérés comme des facteurs d'embauche. Dans le domaine de la cybersécurité, les lettres de motivation ont été identifiées comme étant moins cruciales lors de l'examen des candidates potentielles et des candidats potentiels à l'emploi.

IMPORTANCE DES ASPECTS DANS LES CANDIDATURES

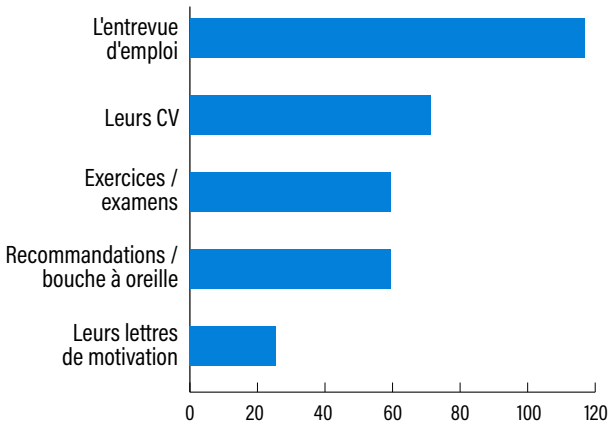


Figure 22 - Importance des différents aspects des candidatures pour les employeuses et employeurs en cybersécurité. Source : sondage du CTIC auprès des employeuses et employeurs en cybersécurité, 2022.

À ce titre, les éducatrices canadiennes et éducateurs canadiens en cybersécurité doivent s'assurer que les candidates et candidats sont bien préparées/préparés à faire une bonne impression grâce à leur CV et à leurs compétences en matière d'entrevue.

S'attaquer aux obstacles et à l'attrition

Le taux d'attrition élevé dans les programmes de cybersécurité constitue un défi majeur pour l'industrie de la cybersécurité car il retarde la résorption du déficit de talents. L'attrition est également déséquilibrée en fonction du sexe, ce qui signifie que même si davantage de femmes s'intéressent au domaine, les gains finaux dans la main-d'œuvre peuvent être limités; l'enquête du CTIC auprès des étudiantes et étudiants a révélé que plus de 50 % des femmes qui ont commencé une carrière en cybersécurité ont abandonné le domaine, contre 30 % des hommes.

Lorsqu'on a demandé aux anciennes étudiantes et aux anciens étudiants pourquoi elles et ils avaient abandonné leurs études en cybersécurité, les trois principales raisons étaient de meilleures possibilités ailleurs, le fait de trouver la cybersécurité trop technique ou la perte d'intérêt pour le domaine. Certains effets de cohorte intéressants ont été observés parmi les étudiantes et étudiants ayant des antécédents différents. Les ingénieures/ingénieurs, par exemple, ont eu tendance à quitter le domaine pour ce qu'elles et qu'ils considéraient comme de meilleures possibilités ailleurs. Les ingénieures/ingénieurs

et les étudiantes et étudiants en commerce étaient plus susceptibles de trouver le domaine trop technique. Les étudiantes et étudiants en informatique étaient les plus susceptibles de déclarer que le domaine était trop stressant ou qu'elles/qu'ils avaient perdu tout intérêt.

Pour les étudiantes et étudiants qui ont abandonné la cybersécurité comme cheminement de carrière, la majorité des répondantes et répondants à l'enquête ont indiqué que la disponibilité de programmes d'apprentissage intégré au travail et/ou d'offres de microcertification aurait influencé leur décision d'autosélection hors de la cybersécurité.

L'enquête auprès des étudiantes et étudiants a révélé que les niveaux élevés de stress, le temps consacré et les exigences techniques étaient les trois principaux facteurs ayant un impact négatif sur l'intérêt des étudiantes et étudiants pour les programmes d'apprentissage de la cybersécurité. En revanche, l'intérêt des étudiantes et étudiants n'a été que très peu affecté par les considérations liées à la diversité et à la culture ou par l'accessibilité financière.

Cependant, la capacité d'un programme d'apprentissage de la cybersécurité à apaiser ces inquiétudes à long terme peut être limitée. La cybersécurité est un domaine qui exige un engagement de temps important et une certification technique élevée, et qui soumet fréquemment ses travailleuses et travailleurs à un stress considérable. Bien que la conception d'un programme de cybersécurité très flexible puisse encourager davantage de personnes à étudier la cybersécurité, ainsi que fournir une alternative pour celles et ceux qui ne sont pas inspirées/inspirés par une approche universitaire ou collégiale rigoureuse, les impacts à long terme d'un tel programme pourraient être moins bénéfiques que prévu. Un tel programme pourrait simplement retarder la sortie des travailleuses et travailleurs inadaptées/inadaptés, plutôt que de l'éliminer.

Évaluation de l'écart des attentes entre les établissements postsecondaires et les employeuses et employeurs

Bien que les établissements d'enseignement postsecondaire (EEPS) n'aient pas été inclus dans les enquêtes en raison du temps et des ressources limités du projet, on a constaté des différences nettes entre les autoévaluations des étudiantes et étudiants liées aux compétences techniques et aux compétences générales, et les évaluations et attentes des employeuses et employeurs. Ceci est particulièrement important pour les compétences que les employeuses et employeurs ont identifiées comme des compétences « indispensables avant l'embauche » par rapport à celles qui peuvent être développées en cours d'emploi.

Un manque de communication entre les EEPS et les employeuses et employeurs d'emplois en cybersécurité a été identifié par le Comité consultatif national sur la formation en cybersécurité du CTIC (CCNFC) et se reflète dans les différences entre les réponses des étudiantes et étudiants et des employeuses et employeurs des sondages. Les recherches futures pourraient inclure une compréhension plus approfondie de la façon dont les compétences essentielles avant l'embauche, tant techniques que non techniques, peuvent être développées. Ceci est extrêmement important pour les étudiantes et étudiants qui peuvent ne pas être en mesure de développer et d'évaluer avec précision ces compétences préalables à l'embauche avant de tenter d'entrer dans la main-d'œuvre en cybersécurité.

CONCLUSION

Les recherches existantes ont relevé l'importance du domaine de la cybersécurité au Canada et à l'étranger. Compte tenu de la numérisation croissante du travail, qui a été accélérée par la croissance du travail à distance en raison de la COVID-19, la cybersécurité est une priorité pour les secteurs public et privé. Il existe de multiples voies d'accès aux rôles de cybersécurité comme directement à partir d'un programme collégial ou universitaire pertinent ou dans le cadre d'une transition en milieu de carrière par l'amélioration des compétences. Il convient également de considérer le rôle des programmes d'apprentissage intégré au travail (AIT) et des microcertifications comme des voies alternatives pour améliorer les capacités dans ce domaine. Cependant, le recrutement et la rétention pour ces rôles de cybersécurité très demandés posent des défis. L'ampleur des défis s'est accrue et il s'agit toujours d'une industrie exigeante. Des recherches indiquent qu'il existe des niveaux élevés d'épuisement professionnel et que de nombreuses employées et de nombreux employés envisagent de partir au cours de l'année suivante. Comme on l'a vu dans d'autres domaines, la « grande démission » et l'équilibre changeant entre l'offre et la demande de main-d'œuvre donnent plus de poids aux demandeuses et demandeurs d'emploi et posent des défis au recrutement des entreprises.

Les recherches en cours et la récente enquête du CTIC fournissent de nouvelles données sur une variété de dimensions différentes pour les employeuses et employeurs en cybersécurité, comme le classement relatif de l'importance des certifications de l'industrie, les cadres, les considérations clés d'embauche et les exigences de compétences des employées/employés. Ces données sont complétées par des données d'enquête qui se concentrent sur les perspectives des étudiantes et étudiants en cybersécurité (telles que leurs impressions sur les aspects négatifs du domaine ou leur autoévaluation du niveau de compétences) afin de mieux comprendre le futur pipeline d'approvisionnement en cybersécurité. En fin de compte, ces données peuvent être utilisées pour comparer les besoins et les attentes des employées/employés et des employeuses et employeurs, et répondre aux besoins en talents du domaine de la cybersécurité au Canada.

Afin de valider et de mettre en œuvre les conclusions de ce rapport, il est recommandé que le CCNFC et le CTIC explorent les possibilités de concevoir et de mettre en œuvre un projet pilote, en partenariat avec un ou plusieurs collèges canadiens offrant une formation en cybersécurité, afin de combler les principales lacunes en matière de compétences (compétences techniques et non techniques) des diplômées/diplômés en cybersécurité et d'inclure au moins une microcertification et un programme d'AIT.

MÉTHODOLOGIE DU PROJET SUR LES TALENTS EN CYBERSÉCURITÉ

La méthodologie de ce projet sur les talents en cybersécurité comprenait une analyse documentaire et une recherche primaire consistant en une enquête auprès des employeuses et employeurs et une enquête auprès des étudiantes et étudiants.

L'analyse documentaire était une méta-étude, consolidant les recherches actuelles et pertinentes sur la cybersécurité et l'AIT, les articles, les cadres de compétences en cybersécurité existants et les tendances de l'emploi dans le secteur. L'analyse documentaire a permis de guider la conception des sondages.

L'objectif du projet est d'avoir un coup d'œil sur la recherche qui servira de base à la conception d'un projet pilote de cybersécurité axé sur l'AIT afin de s'attaquer aux problèmes les plus pressants en matière d'embauche de diplômées/diplômés d'établissements postsecondaires dans le domaine de la cybersécurité et de valider/affiner les hypothèses du Comité consultatif national sur la formation en cybersécurité (CCNFC) du CTIC.

Recherche originale

La recherche originale comportait deux volets, en commençant par une enquête auprès des employeuses et employeurs pour mieux comprendre :

- Comment les employeuses et employeurs évaluent les compétences nécessaires lorsqu'elles et lorsqu'ils recrutent pour des postes de cybersécurité.
- Quelles sont les lacunes en matière de compétences que les employeuses et employeurs constatent chez les diplômées/diplômés de niveau postsecondaire à la recherche de postes en cybersécurité?
- Quelle compréhension des contrôles de sécurité/autorisations est nécessaire pour l'embauche de rôles de cybersécurité.

La dernière composante de la recherche originale était un sondage auprès des étudiantes et étudiants des établissements postsecondaires. L'enquête cible les étudiantes et étudiants de :

- Sources de talents en cybersécurité dans les programmes traditionnels (science informatique, réseaux, TI).
- Sources non traditionnelles de talents en cybersécurité (entreprises, arts libéraux).

L'enquête a cherché à comprendre :

- Si les étudiantes et étudiants ont fait l'autosélection de ne pas poursuivre une carrière dans la cybersécurité.
    - Pourquoi elles et ils ont quitté la filière de la cybersécurité.
    - Quels étaient les obstacles perçus.
    - Quelles offres de cours (c.-à-d., microcertification, certification…) et/ou quelles mesures d'atténuation du cheminement de carrière auraient pu les faire changer d'avis?
- Comment la disponibilité des programmes d'AIT influence leurs choix de carrière.
- Comment les étudiantes et étudiants évaluent elles-mêmes et eux-mêmes leur état de préparation aux carrières de la cybersécurité

ANNEXE

Compétences en cybersécurité en demande[84]

Comme l'ont noté plusieurs informatrices et informateurs clés, les titres et les descriptions d'emploi dans l'écosystème de la cybersécurité ne sont pas toujours faciles à catégoriser, car les employeuses et employeurs rédigent régulièrement des descriptions de poste très larges afin d'attirer un large éventail de candidates et de candidats. Il a également été noté que les représentantes et représentants de l'industrie sursaturent intentionnellement les exigences en matière de compétences (humaines et techniques) pour les affichages, car les exigences en matière de qualifications limitées ou étroites découragent souvent les candidates et candidats appropriées/appropriés. Les ensembles de compétences sont donc à la fois spécifiques à des rôles particuliers et, fréquemment, transversaux et applicables à un large éventail d'intitulés d'emploi. L'analyse ci-dessous inverse les ensembles de compétences du moins spécifique au plus spécifique, en examinant d'abord les compétences humaines et transférables mises en avant par les employeuses et employeurs de deux manières : par le biais d'interviews d'informatrices et d'informateurs clés et de descriptions d'offres d'emploi. Les ensembles de compétences sont classés grossièrement selon l'ordre d'importance attribué par les répondantes et répondants au sondage du CTIC auprès des employeuses et employeurs du Nouveau-Brunswick. Bien que les ensembles de compétences varient nécessairement de façon importante selon le rôle, le classement et la comparaison qui suivent reflètent un certain degré d'importance transversale (particulièrement pour les compétences moins spécialisées) parce que les personnes interrogées et les répondantes et répondants au sondage ont nommé des compétences qui n'étaient pas rattachées à un intitulé de poste particulier. Par conséquent, l'analyse de la **figure 16** est une vue d'ensemble des priorités des employeuses et employeurs du Nouveau-Brunswick et des compétences transférables qui peuvent aider les nouvelles venues et nouveaux venus sur le marché du travail à réussir.

En ce qui concerne les **compétences humaines et transférables**, les répondantes et répondants au sondage ont classé la responsabilité et le professionnalisme, le travail d'équipe et les compétences en communication comme les plus importants. Il est intéressant de noter que ces options de réponses multiples se révèlent beaucoup plus granulaires dans l'analyse de l'extraction du Web et des interviews, où les employeuses et employeurs se sont concentrées/concentrés sur le personnel indépendant, expérimenté, dévoué et organisé. Cet accent mis sur les professionnelles/professionnels expérimentées/expérimentés et responsables renforce la conclusion générale selon laquelle les employeuses et employeurs recherchent fréquemment du personnel de cybersécurité ayant plusieurs années d'expérience professionnelle pertinente. De même, le travail en équipe, les compétences interpersonnelles et l'adaptabilité/flexibilité sont considérés comme assez importants sur le lieu de travail.

[84] Tiré du rapport *À la recherche des talents cachés: L'expérience et l'expertise de la communauté de cybersécurité du Nouveau-Brunswick*, https://thinktanknumeriquectic.com/rapports/a-la-recherche-des-talents-caches.

ANNEXE

Bien que l'option à choix multiple de l'enquête, la « **créativité** » soit légèrement moins bien classée, les résultats des interviews et des offres d'emploi mettent en lumière les différences sémantiques qui peuvent en être la cause : plutôt que la « créativité », les employeuses et employeurs en cybersécurité peuvent rechercher la **pensée critique**, l'**analyse**, la résolution **de problèmes** et la **réflexion stratégique**. De même, bien qu'un QE (quotient émotionnel, c.-à-d. « **empathie** ») élevé ne soit pas une des réponses préférées de l'enquête, les employeuses et employeurs ont indiqué spontanément des priorités autour de l'**intelligence émotionnelle** et de la **conscience situationnelle**, et le rang inférieur du leadership est démenti par l'importance du mentorat, d'un bon travail d'équipe, des compétences commerciales, de l'expérience antérieure et de la somme cumulative de plusieurs de ces compétences humaines qui, ensemble, créent une bonne ou un bon leader.

Outre les compétences humaines, la **figure 16** énumère les compétences techniques en matière de cybersécurité qui ont été mentionnées dans chacune de ces sources de données. Les compétences sont regroupées et ordonnées à nouveau selon le classement d'importance des répondants à l'enquête. Nous avons demandé à deux professionnelles/professionnels ayant une expertise technique en cybersécurité de coder et de regrouper indépendamment les ensembles de compétences dans ces catégories, et leurs analyses ont été combinées (bien qu'elles aient été largement en accord) aux fins de la visualisation ci-dessous. Bien que ce graphique conserve un haut degré de granularité, plusieurs points à retenir sont clairs. En particulier, plusieurs ensembles de compétences sont renforcés de manière générale et utiles dans un certain nombre d'applications, notamment la **sécurité des communications et des réseaux**; **l'ingénierie de la sécurité**; **l'architecture**, **la sécurité**, **les outils et les protocoles des réseaux**; et les **concepts de protection**, parmi beaucoup d'autres. Les deux codeuses ont noté qu'en raison de la combinaison de nombreuses sources de données (c'est-à-dire, plusieurs affichages d'emploi et plusieurs personnes interrogées), il y avait un chevauchement important entre plusieurs des compétences énumérées ci-dessous. La figure 16 conserve toutefois, dans la mesure du possible, le libellé original de ces sources afin de présenter les demandes réelles des employeuses et des employeurs.

ANNEXE

COMPÉTENCES CLASSÉES PAR ORDRE D'IMPORTANCE SELON LE SONDAGE DU CTIC AUPRÈS DES EMPLOYEUSES ET EMPLOYEURS DU NOUVEAU-BRUNSWICK[85]	COMPÉTENCES DIRECTEMENT MENTIONNÉES DANS LES INTERVIEWS OU SPÉCIFIQUES AUX QUALIFICATIONS MENTIONNÉES DANS LES INTERVIEWS	COMPÉTENCES EXTRAITES D'OFFRES D'EMPLOI AU NOUVEAU-BRUNSWICK (REGROUPÉES LORSQU'ELLES SONT SIMILAIRES)
COMPÉTENCES HUMAINES ET TRANSFÉRABLES		
1. Responsabilité/Professionnalisme	• Motivation personnelle • Forte éthique du travail • Familiarité avec les systèmes au niveau de l'entreprise • Passion/intérêt pour la cybersécurité • Curiosité professionnelle	• Indépendance • Expérience en environnement d'entreprise • Gestion de projet
Le travail d'équipe	• Collaboration et compétences interpersonnelles	• Compétences interpersonnelles • Mentorat, formation et développement des capacités des collègues
Communication	• Compétences en matière de présentation • Aptitudes à communiquer (écrites et verbales).	• Communication écrite et verbale
2. Flexibilité	• Adaptabilité	• Gestion du temps, flexibilité
Créativité	• Pensée critique	• Résolution de problème, analyse, réflexion stratégique • Analyse du comportement humain
3. Courtoisie/Empathie	• Intelligence émotionnelle (empathie) • Les compétences en matière de service à la clientèle	• Intelligence émotionnelle • Conscience situationnelle • Le service à la clientèle
Leadership	• Aptitudes au leadership • Expérience de bénévolat/stage	• Leadership, compétences en matière de gestion et de supervision
COMPÉTENCES TECHNIQUES SPÉCIFIQUES À LA CYBERSÉCURITÉ		
Groupe 1 (le mieux classé dans l'enquête)		
• Sécurité des réseaux	• Ingénierie de la sécurité • Communications et sécurité des réseaux	• Architecture, sécurité, outils et protocoles de réseau • Concepts de protection • Gestion des pare-feux

[85] On a demandé aux répondantes et répondants : « Lors de l'embauche de personnel en cybersécurité au Nouveau-Brunswick, lesquels des ensembles de compétences [humaines ou techniques] suivants sont les plus importants? ». Les classements sont basés sur les évaluations des répondantes etrépondants, de la plus importante à la moins importante, les compétences ayant des évaluations très similaires étant regroupées. Ces questions d'enquête ont donné lieu à 40 réponses individuelles complètes.

ANNEXE

COMPÉTENCES CLASSÉES PAR ORDRE D'IMPORTANCE SELON LE SONDAGE DU CTIC AUPRÈS DES EMPLOYEUSES ET EMPLOYEURS DU NOUVEAU-BRUNSWICK[85]	COMPÉTENCES DIRECTEMENT MENTIONNÉES DANS LES INTERVIEWS OU SPÉCIFIQUES AUX QUALIFICATIONS MENTIONNÉES DANS LES INTERVIEWS	COMPÉTENCES EXTRAITES D'OFFRES D'EMPLOI AU NOUVEAU-BRUNSWICK (REGROUPÉES LORSQU'ELLES SONT SIMILAIRES)
• Connaissance de la sécurité de l'infonuagique	• Communications et sécurité des réseaux • Sécurité de l'infonuagique	• Concepts de protection
Groupe 2 (deuxième plus haut)		
• Ingénierie des systèmes et des réseaux	• Ingénierie de la sécurité • Communications et sécurité des réseaux • La gestion des identités et de l'accès • Opérations des systèmes d'information	• Architecture, sécurité, outils et protocoles de réseau • Concepts de protection
• Intégration des technologies, des systèmes et des services	• Ingénierie de la sécurité • Communications et sécurité des réseaux • La gestion des identités et de l'accès • Sécurité du développement de logiciels	• Architecture, sécurité, outils et protocoles de réseau • Protection et cryptage des données
• Sécurité de l'information et connaissance des meilleures pratiques en matière d'architecture des systèmes	• Ingénierie de la sécurité • Communications et sécurité des réseaux • La gestion des identités et de l'accès	• Architecture, sécurité, outils et protocoles de réseau • Protection et cryptage des données • Concepts de protection • Automatisation (configuration, gestion, systèmes de sécurité) • Processus et concepts du Centre des opérations de sécurité (COS) • Gestion des systèmes de sécurité à l'échelle de l'entreprise
• Gouvernance et conformité	• Analyse de la sécurité • Gestion des risques • Sécurité des actifs • Opérations de sécurité • Audit des systèmes d'information • Acquisitions de systèmes d'information • Responsabilité de la gestion • Gouvernance de la sécurité de l'information • Gestion des risques	• Gouvernance et conformité • Concepts de protection • Atténuation et gestion des risques • Mesures et production de rapports en matière de sécurité

ANNEXE

COMPÉTENCES CLASSÉES PAR ORDRE D'IMPORTANCE SELON LE SONDAGE DU CTIC AUPRÈS DES EMPLOYEUSES ET EMPLOYEURS DU NOUVEAU-BRUNSWICK[85]	COMPÉTENCES DIRECTEMENT MENTIONNÉES DANS LES INTERVIEWS OU SPÉCIFIQUES AUX QUALIFICATIONS MENTIONNÉES DANS LES INTERVIEWS	COMPÉTENCES EXTRAITES D'OFFRES D'EMPLOI AU NOUVEAU-BRUNSWICK (REGROUPÉES LORSQU'ELLES SONT SIMILAIRES)
• Test de pénétration et de vulnérabilité	• Analyse de la sécurité • Communications et sécurité des réseaux • La gestion des identités et de l'accès • Évaluation et tests de sécurité • Sécurité du développement de logiciels • Audit des systèmes d'information	• Évaluation et gestion des vulnérabilités • Analyse de l'évaluation de la menace; Architecture de réseau, sécurité, outils et protocoles • Connaissance des méthodes d'attaque • Concepts de protection • Test de pénétration
• Enquête et réaction en cas d'incident	• Analyse de la sécurité • Gestion des risques • Communications et sécurité des réseaux • La gestion des identités et de l'accès • Opérations de sécurité • Audit des systèmes d'information • Opérations des systèmes d'information • Gestion des incidents • Sécurité infonuagique • La chasse aux cybermenaces	• Protection et cryptage des données • Évaluation et gestion des vulnérabilités • Criminalistique numérique • Analyse de l'évaluation de la menace • Gestion des pare-feux • Architecture, sécurité, outils et protocoles de réseau • Processus et concepts du Centre des opérations de sécurité • Réaction en cas d'incident • Traitement des systèmes compromis • Concepts de protection • Gestion des systèmes de sécurité de l'entreprise • Détection des brèches complexes et avancées • Développement de routines de chasse et de détection • Atténuation et gestion des risques • Exécution de systèmes SIEM (renseignements sur la sécurité et gestion des événements) et de prévention des pertes de données (DLP) • Automatisation (configuration, gestion, systèmes de sécurité)

ANNEXE

COMPÉTENCES CLASSÉES PAR ORDRE D'IMPORTANCE SELON LE SONDAGE DU CTIC AUPRÈS DES EMPLOYEUSES ET EMPLOYEURS DU NOUVEAU-BRUNSWICK[85]	COMPÉTENCES DIRECTEMENT MENTIONNÉES DANS LES INTERVIEWS OU SPÉCIFIQUES AUX QUALIFICATIONS MENTIONNÉES DANS LES INTERVIEWS	COMPÉTENCES EXTRAITES D'OFFRES D'EMPLOI AU NOUVEAU-BRUNSWICK (REGROUPÉES LORSQU'ELLES SONT SIMILAIRES)
Groupe 3		
· Évaluation et gestion des risques	· Analyse de la sécurité · Gestion des risques · Évaluation et tests de sécurité · Audit des systèmes d'information · Gestion des risques · Gestion de la sécurité	· Évaluation et gestion des vulnérabilités ; · Analyse de l'évaluation des menaces · Concepts de protection · Atténuation et gestion des risques · Mesures et production de rapports en matière de sécurité
· Connaissance de la sécurité de l'IdO	· Analyse de la sécurité · Gestion des risques · Ingénierie de la sécurité · Communications et sécurité des réseaux · La gestion des identités et de l'accès · Sécurité infonuagique	· Évaluation et gestion des vulnérabilités · Analyse de l'évaluation des menaces · Architecture, sécurité, outils et protocoles de réseau · Concepts de protection
· Cryptage et cryptographie, cryptographie à résistance quantique	· Ingénierie de la sécurité · Communications et sécurité des réseaux	· Protection des données et cryptage · Connaissance des méthodes d'attaque
AUTRES COMPÉTENCES TECHNIQUES [RÉPONSES DONNÉES À L'ALTERNATIVE OUVERTE, « UN AUTRE ENSEMBLE DE COMPÉTENCES IMPORTANTES (VEUILLEZ PRÉCISER) »]		
Compréhension des communications et des protocoles de réseau		· Administration et infrastructure des serveurs · Connaissance de la technologie mobile et de la radiotéléphonie
Développement fondamental de logiciels	· Programmation de base · Expérience de l'intelligence artificielle/ de l'apprentissage automatique	· Méthodologies agiles · Programmation de base et avancée · Connaissance de la mémoire et des structures de données
Valeurs aberrantes (non classées par les codeuses et codeurs)	· Gestion informatique · Documentation · Audit, amélioration continue · Familiarité avec les systèmes d'entreprise (planification des ressources de l'entreprise)	· Administratrice/Administrateur de base de données · Gestion des archives et des documents · Intégration et entreposage de données

Figure 16