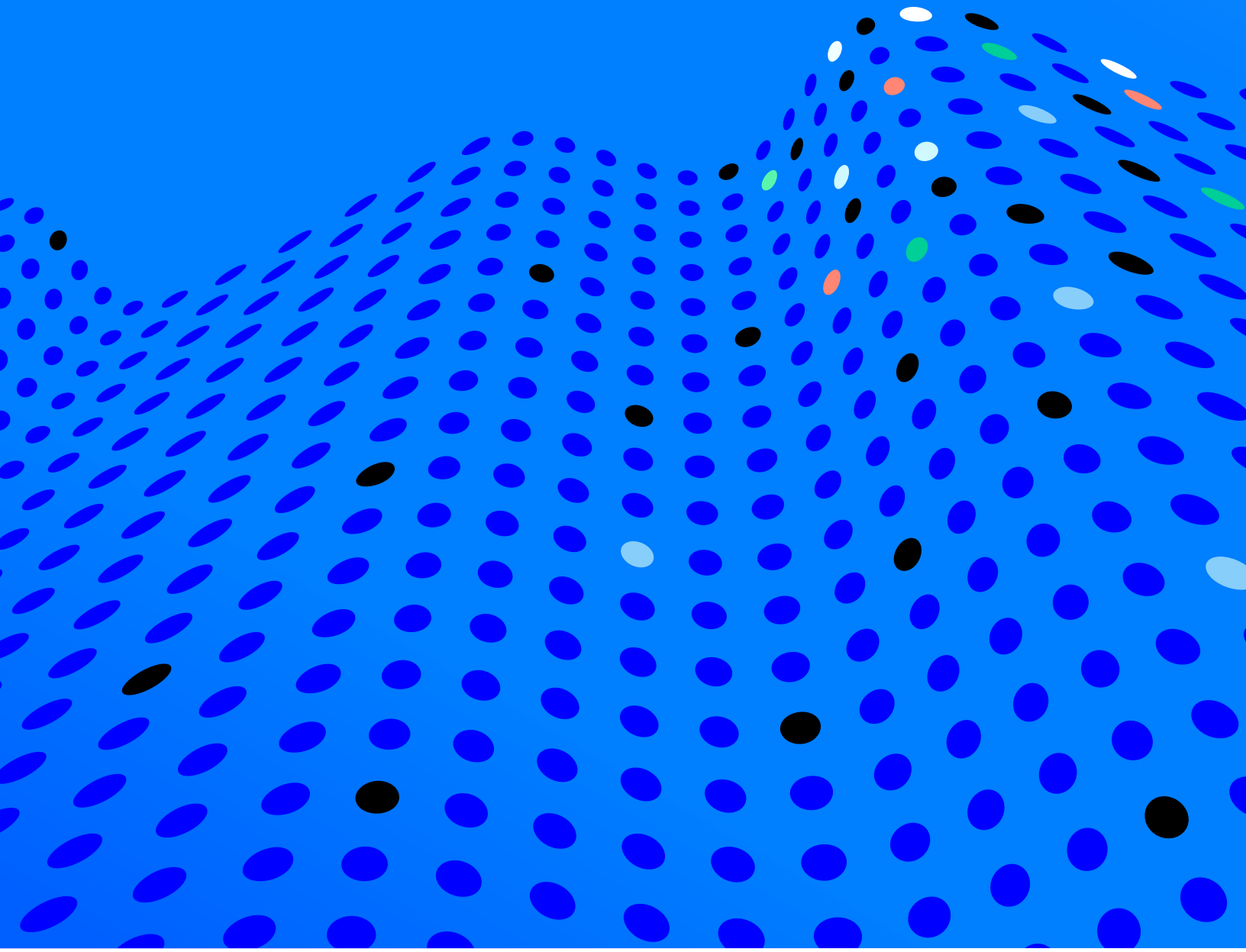
La course aux talents : perspectives des employeurs canadiens en cybersécurité



Centre des Compétences futures

Blueprint

Table des matières

- Sommaire 3
- 1 Introduction 6
- 2 Principales conclusions du sondage 9
- 3 Sondage sur l'industrie en général : premières conclusions 19
- 4 Recommandations 21
- Références 25
- Annexe 26
- Notes de fin 29

Sommaire

Puisque les cybermenaces augmentent en volume et en sophistication, les entreprises canadiennes, grandes et petites, considèrent la cybersécurité comme l'un des principaux risques pour leur croissance. Au Canada, la demande de cybertalents continue d'augmenter, dans un contexte de pénurie aiguë de professionnels qualifiés en cybersécurité.

Bien que cette pénurie de talents ne soit pas propre au Canada, elle représente toutefois pour le pays une occasion unique de puiser dans son bassin croissant de nouveaux arrivants qualifiés, dont beaucoup sont des femmes ou des personnes issues de populations racisées qui sont sous-représentées dans le secteur de la cybersécurité. Les employeurs doivent trouver la meilleure façon de repérer, d'attirer, de recruter et de retenir ces talents pour répondre aux besoins croissants du secteur de la cybersécurité.

Pour rendre le secteur plus accessible aux Canadiens de diverses origines, Rogers Cybersecure Catalyst (Catalyst) a lancé le programme de formation accélérée en cybersécurité (Accelerated Cybersecurity Training Program – ACTP) en 2020. Ce programme a été conçu expressément pour permettre aux femmes, aux nouveaux arrivants et aux travailleurs déplacés d'acquérir les compétences nécessaires pour amorcer une carrière dans le secteur de la cybersécurité. Grâce au financement du Centre des Compétences futures (CCF), Catalyst et Blueprint ont collaboré pour mener une étude auprès des employeurs canadiens en cybersécurité afin de cerner la demande en professionnels de la cybersécurité de niveau débutant, de comprendre les pratiques d'embauche des employeurs et de déterminer leurs besoins en matière de compétences ainsi que les défis qu'ils doivent relever pour répondre à leur demande de cybertalents.

Dans le cadre de cette étude, les équipes de Blueprint et de Catalyst se sont adressées à 49 professionnels intermédiaires et de haut niveau au sein de 23 moyennes et grandes entreprises en étroite relation avec l'ACTP afin de les inviter à remplir le sondage des partenaires en emploi de l'ACTP. De ces 23 employeurs, 17 ont rempli le sondage en tout ou en partie, ce qui nous donne un taux de réponse de 74 %.

L'objectif du rapport principal est de communiquer les conclusions tirées de ce que nous avons appris auprès de ces employeurs. Dans le présent sommaire, nous présentons les principales questions abordées dans le cadre de cette recherche, les conclusions de haut niveau qui répondent à ces questions et les recommandations pour les programmes tels que l'ACTP et pour les employeurs en cybersécurité afin de combler efficacement l'écart croissant entre la demande et l'offre de talents en cybersécurité au Canada.

Principales conclusions

Stratégies des employeurs : Comment les employeurs recrutent-ils et retiennent ils les cybertalents?

- La plupart des partenaires en emploi estiment que les recommandations des employés constituent le canal de recrutement le plus efficace, et certains favorisent également l'embauche de candidats par le biais de programmes de certification qui ne sont pas liés à des programmes d'études universitaires ou collégiaux.
- Les partenaires en emploi estiment que les aspects non monétaires d'un emploi, comme l'horaire flexible et les possibilités de perfectionnement professionnel, peuvent attirer tout autant les candidats que la rémunération.

Défis pour les employeurs : Quels sont les principaux problèmes auxquels sont confrontés les employeurs?

- Les principaux défis de l'industrie sont la pénurie de talents qualifiés en cybersécurité et l'inadéquation entre la rémunération et les avantages offerts et les attentes des candidats.
- Les partenaires en emploi ont déterminé trois obstacles à la création de descriptions de poste précises pour les fonctions de cybersécurité de niveau débutant : une inadéquation entre les attentes de l'entreprise et celles des candidats, un manque de compréhension de la part des responsables des RH et le rythme rapide auquel l'industrie évolue.

Besoins en matière de compétences : Quels sont les rôles et les compétences recherchés?

- Les partenaires en emploi s'attendent à avoir besoin de deux à cent professionnels de la cybersécurité par entreprise au cours de la prochaine année et cette demande pourrait doubler à moyen ou long terme, la demande actuelle et future la plus forte se situant dans la catégorie des rôles de protection et de défense.
- L'intervention en cas d'incident, l'infonuagique et la gestion des cyberrisques continueront de faire l'objet d'une forte demande de la part des partenaires en emploi, la sécurité des données semble constituer un besoin qui refait surface, et l'analyse des données de sécurité pourrait voir la demande diminuer dans l'avenir.
- Les partenaires en emploi valorisent actuellement fortement les compétences techniques telles que les techniques de détection et de réponse aux intrusions, le dépannage et le fonctionnement des systèmes de protection et de défense des réseaux, mais cela devrait changer dans les trois à cinq prochaines années.
- La communication verbale, la résolution de problèmes, la pensée critique et le souci du détail sont actuellement les compétences non techniques les plus valorisées par les partenaires en emploi. La demande pour ces compétences devrait se maintenir au cours des trois à cinq prochaines années.

Diversifier le secteur : Quels sont les défis et les occasions à venir?

- Trente-cinq pour cent des partenaires en emploi ont signalé des difficultés dans le recrutement de personnes autochtones, noires et de couleur ou de femmes dans le secteur de la cybersécurité et ont proposé trois stratégies pour remédier à ce problème : s'associer aux réseaux et événements pertinents, offrir des occasions d'éducation et de formation ciblées et être ouvert à l'embauche de membres de groupes sous-représentés.
- Si la plupart des partenaires en emploi ont mis en œuvre des programmes visant à recruter des candidats diversifiés pour les postes en cybersécurité et offrent une formation générale en matière d'inclusion en milieu de travail, seuls quelques-uns ont investi pour assurer la diversité dans la direction, offrir des occasions de perfectionnement ciblées et proposer une formation approfondie liée à la diversité, à l'équité et l'inclusion.

Recommandations

Programmes tels que l'ACTP

- En plus de doter les participants de compétences techniques et de certifications, les programmes tels que l'ACTP doivent aussi amener les candidats à acquérir des compétences non techniques par l'intermédiaire d'exercices pratiques dans le contexte de la cybersécurité.
- Les programmes tels que l'ACTP peuvent faire la promotion de la cybersécurité en tant que carrière auprès des communautés concernées de personnes autochtones, noires et de couleur et de femmes et aider à lutter contre les perceptions erronées de l'industrie.

Employeurs canadiens en cybersécurité

- Bien que les employeurs perçoivent les recommandations des employés comme un canal de recrutement efficace, ils devraient s'efforcer de remédier à ses limites, notamment en ce qui concerne la manière dont il peut exacerber la sous-représentation actuelle de certains groupes dans la cybersécurité.
- Pour embaucher des candidats issus de groupes traditionnellement sous-représentés, les employeurs doivent s'associer à des réseaux pertinents et participer à des événements ou des panels qui peuvent les mettre en contact avec ce bassin de talents sous-utilisé et être plus ouverts à de nouvelles perspectives.
- Les experts techniques, les RH et les responsables du recrutement des entreprises de cybersécurité devraient travailler ensemble pour rédiger des descriptions de poste précises pour les rôles de cybersécurité de niveau débutant, avec des compétences et des attentes clairement définies.

1 Introduction

Les entreprises canadiennes, petites et grandes, voient la cybersécurité comme un des trois principaux risques pour leur croissance. Bien que ces entreprises aient redoublé d'efforts sur le plan de la cybersécurité, de la protection des données et de la confidentialité, 36 % des petites et moyennes entreprises et 27 % des PDG estiment ne pas être préparés à une cyberattaque (KPMG, 2021).[1] Il n'est donc pas surprenant que la demande en matière de cybertalents au Canada continue de croître : une étude a estimé le déficit de main-d'œuvre en cybersécurité au Canada[2] en 2021 à 25 000 professionnels ((ISC)[2] ,2022). De plus, il existe une grave pénurie de professionnels qualifiés en cybersécurité (Posadzki, 2019).

Bien que cette pénurie de talents ne soit pas propre au Canada[3], elle représente toutefois pour le pays une occasion unique de puiser dans son bassin croissant de nouveaux arrivants qualifiés, dont beaucoup sont des femmes ou des personnes issues de populations racisées qui sont sous-représentées dans le secteur de la cybersécurité. Les employeurs doivent trouver la meilleure façon de repérer, d'attirer, de recruter et de retenir ces talents pour répondre aux besoins croissants du secteur de la cybersécurité.

Pour rendre le secteur plus accessible aux Canadiens de diverses origines, Rogers Cybersecure Catalyst (Catalyst, ci-après) – centre national de formation, d'innovation et de collaboration en cybersécurité de l'Université métropolitaine de Toronto – a lancé le programme de formation accélérée en cybersécurité (Accelerated Cybersecurity Training Program – ACTP) en 2020. Ce programme d'acquisition de compétences d'une durée de sept mois a été conçu expressément pour permettre aux femmes, aux nouveaux arrivants et aux travailleurs déplacés d'acquérir les compétences nécessaires pour amorcer une carrière dans le secteur de la cybersécurité.

La pénurie de talents en cybersécurité s'explique notamment par le manque de professionnels possédant les qualifications nécessaires pour être embauchés (Lake, 2022). En proposant un programme qui offre des certifications reconnues par l'industrie et qui aide les femmes et les personnes d'origines diverses à intégrer le secteur, Catalyst vise à remédier à la pénurie de compétences tout en favorisant la diversité et l'inclusion dans l'écosystème de la cybersécurité.

En octobre 2021, Catalyst a obtenu un financement du Centre des Compétences futures (CCF) afin de lancer le projet d'initiative de transformation des cybertalents (Cyber Talent Transformation Initiative – CTTI) dans le but d'étendre la portée de l'ACTP aux personnes autochtones, noires et de couleur (PANDC) et pour mener des recherches approfondies qui offrent des perspectives et des recommandations concrètes sur la diversité et l'inclusion dans la cybersécurité.

Blueprint, en tant que partenaire de production de données probantes du CCF, collabore avec Catalyst pour mener la recherche auprès (a) des personnes inscrites à l'ACTP et (b) des employeurs canadiens en cybersécurité. La recherche sur les personnes inscrites au programme vise à comprendre l'expérience du programme et les résultats, en mettant l'accent sur les défis uniques auxquels sont confrontés les PANDC et les femmes dans l'accès à la formation aux compétences en cybersécurité et aux possibilités d'emploi. Les résultats de cette recherche seront communiqués dans un rapport à paraître l'année prochaine. La recherche auprès des employeurs vise à déterminer la demande pour des professionnels de la cybersécurité de niveau débutant, de comprendre les pratiques d'embauche des employeurs et de déterminer leurs besoins en matière de compétences ainsi que les défis qu'ils doivent relever pour répondre à leur demande de cybertalents.

Recherche sur les employeurs : approches et questions clés

Dans la première partie de notre recherche, nous avons approché 23 employeurs entretenant une relation étroite avec l'ACTP[4]. Parmi ces entreprises de moyenne ou grande taille, l'équipe de l'ACTP a identifié 49 dirigeants en cybersécurité ou professionnels des ressources humaines (RH) qui ont été invités à répondre à un sondage approfondi en avril 2022. L'objectif du présent rapport est de communiquer les conclusions tirées de ce que nous avons appris de ces employeurs.[5]

Pour approfondir les résultats du sondage, nous avons interrogé individuellement les répondants qui ont accepté de nous faire part de leurs expériences d'embauche et de leurs réflexions. Nous nous sommes appuyés sur deux de ces entretiens semi-structurés avec des professionnels de la cybersécurité ayant des responsabilités en matière de recrutement et de gestion afin d'étoffer le contexte des résultats du sondage.[6]

La partie en cours de cette recherche (menée de mai à novembre 2022) est axée sur la compréhension des besoins généraux du secteur canadien de la cybersécurité. Pour ce faire, nous explorons les relations émergentes de l'équipe de l'ACTP avec les dirigeants de la cybersécurité ou les professionnels des RH qui connaissent le programme, mais dont l'engagement avec l'ACTP et ses diplômés est encore embryonnaire. Nous présentons quelques résultats préliminaires de cette recherche dans la section 3, et un prochain rapport présentera une analyse approfondie et une comparaison entre les points de vue des employeurs ayant des relations étroites avec l'ACTP et ceux des employeurs ayant des relations émergentes avec le programme.

Les conclusions du rapport sont en lien avec quatre questions clés :

Stratégies des employeurs

Comment les employeurs recrutent-ils et retiennent-ils les cybertalents?

Besoins en matière de compétences

Quels sont les rôles et les compétences recherchés?

Défis pour les employeurs

Quels sont les principaux problèmes auxquels sont confrontés les employeurs?

Diversifier le secteur

Quels sont les défis et les occasions à venir?

Sondage des partenaires en emploi de l'ACTP

Le sondage des partenaires en emploi de l'ACTP a été envoyé à 49 professionnels intermédiaires et de haut niveau au sein de 23 moyennes ou grandes entreprises de services financiers, de TI et télécommunications et de secteurs qui s'intéressent au recrutement de talents en cybersécurité. Près de 40 % des employeurs abordés étaient des grandes entreprises employant plus de 10 000 personnes.

Les équipes de Blueprint et de Catalyst ont réfléchi aux thèmes et aux questions à inclure dans le sondage, lequel a ensuite été finalisé et mené par l'équipe de Blueprint[7]. Sur les 23 employeurs abordés, 17 ont rempli le sondage en tout ou en partie[8], ce qui nous donne un taux de réponse de 74 %. Le taux de réponse individuel était de 51 %[9].

Les lecteurs devraient garder deux choses à l'esprit au moment d'interpréter les résultats présentés dans ce rapport. Il faut tenir compte en premier lieu de la taille de l'échantillon et des taux de réponse au sondage. Les sondages auprès des professionnels de haut niveau ou des cadres supérieurs ont généralement des taux de réponse plus faibles, et bien que nous ayons obtenu des taux de réponse raisonnablement élevés en raison de la relation étroite entre ces professionnels et le personnel de l'ACTP, il est important de garder à l'esprit que les résultats sont basés sur les réponses de 25 professionnels de 17 entreprises.

En second lieu, il faut se souvenir que le sondage n'a été envoyé qu'aux employeurs faisant partie du réseau de l'ACTP au moment du sondage. Ainsi, les conclusions reflètent leurs besoins et préférences spécifiques et pourraient ne pas être représentatives de l'ensemble du secteur canadien de la cybersécurité.

Le reste du rapport est structuré comme suit : dans la section 2 sont présentées les principales conclusions du sondage de l'ACTP auprès des partenaires en emploi et dans la section 3 sont présentées certaines conclusions préliminaires du sondage plus large sur l'emploi en cours de réalisation. À la section 4 sont présentées six recommandations fondées sur nos conclusions à l'intention des organismes qui offrent des programmes similaires à l'ACTP et des employeurs en cybersécurité.

À propos de Blueprint

Blueprint a été fondée sur le principe que les données probantes sont un outil puissant de changement. Nous travaillons avec des décideurs politiques et des praticiens pour créer ainsi qu'utiliser des données probantes afin de résoudre des problèmes complexes touchant des politiques et des programmes. Nous aspirons à un écosystème de politiques sociales au sein duquel les données probantes servent à améliorer les perspectives, à mettre en place de meilleurs systèmes et politiques et à générer un changement social. Notre équipe est composée d'un groupe multidisciplinaire de professionnels aux compétences diverses en matière de recherche en politiques, d'analyse des données, de conception, d'évaluation, de mise en œuvre et de mobilisation des connaissances. En tant que partenaire fondateur du consortium du Centre des Compétences futures, Blueprint travaille avec des partenaires et des parties prenantes pour générer et utiliser des données probantes dans la résolution des défis pressants associés aux compétences futures.

À propos du Centre des Compétences futures

Le **Centre des Compétences futures** (CCF) est un centre de recherche et de collaboration avant-gardiste qui se consacre à la préparation de la population canadienne à la réussite professionnelle. Nous pensons que les Canadiens et les Canadiennes devraient avoir confiance en leurs compétences pour réussir sur un marché du travail en pleine évolution. En tant que communauté pancanadienne, nous collaborons pour trouver, tester, évaluer et partager de manière rigoureuse des approches novatrices pour analyser et développer les compétences dont les Canadiens et les Canadiennes ont besoin pour prospérer dans les jours et les années à venir. Le Centre des Compétences futures a été fondé par un consortium constitué de l'Université métropolitaine de Toronto, de Blueprint et du Conference Board du Canada. Il est financé par le **gouvernement du Canada dans le cadre du programme Compétences futures.**

2 Principales conclusions du sondage

Dans cette section, nous présentons les conclusions qui répondent aux quatre questions énoncées dans l'introduction.

Stratégies des employeurs : Comment les employeurs recrutent-ils et retiennent-ils les cybertalents?

Cibler les bonnes avenues pour trouver des talents est une partie importante d'une stratégie de recrutement réussie. Nous avons demandé aux destinataires du sondage de nous parler des canaux de recrutement qu'ils trouvent les plus efficaces, ainsi que des facteurs qu'ils pensent que les candidats privilégient pendant leur recherche d'emploi.

Découverte nº 1

La plupart des partenaires en emploi estiment que les recommandations des employés constituent le canal de recrutement le plus efficace, et certains favorisent également l'embauche de candidats par le biais de programmes de certification qui ne sont pas liés à des programmes d'études universitaires ou collégiaux.

Les partenaires en emploi ayant répondu au sondage sont majoritairement d'accord sur le canal de recrutement le plus efficace pour embaucher des talents en cybersécurité – recommandations des employés (58 %) (Figure 1). Les entretiens avec deux professionnels de la cybersécurité ont révélé que les recommandations des employés sont intéressantes, car elles font en sorte que les candidats sont examinés par des personnes ayant une connaissance approfondie de la nature du poste et de l'entreprise, qui peuvent donc évaluer plus efficacement si le candidat convient au poste à pourvoir. Outre les recommandations informelles, l'entreprise des deux personnes rencontrées dispose depuis plusieurs années de programmes de recommandation formels, et les primes destinées à inciter les employés à faire appel à leurs réseaux sont étalonnées en fonction du niveau de demande de compétences.

Quelques répondants considèrent l'embauche directe à partir de programmes de formation de certification de la main-d'œuvre qui ne sont pas liés à des programmes universitaires ou collégiaux (p. ex., l'ACTP) comme un canal de recrutement efficace (13 %). Une personne interrogée a indiqué que, bien qu'elle ait tendance à préférer les recommandations des employés, son entreprise aurait besoin de puiser dans différentes ressources en période de forte demande.

Découverte nº 2

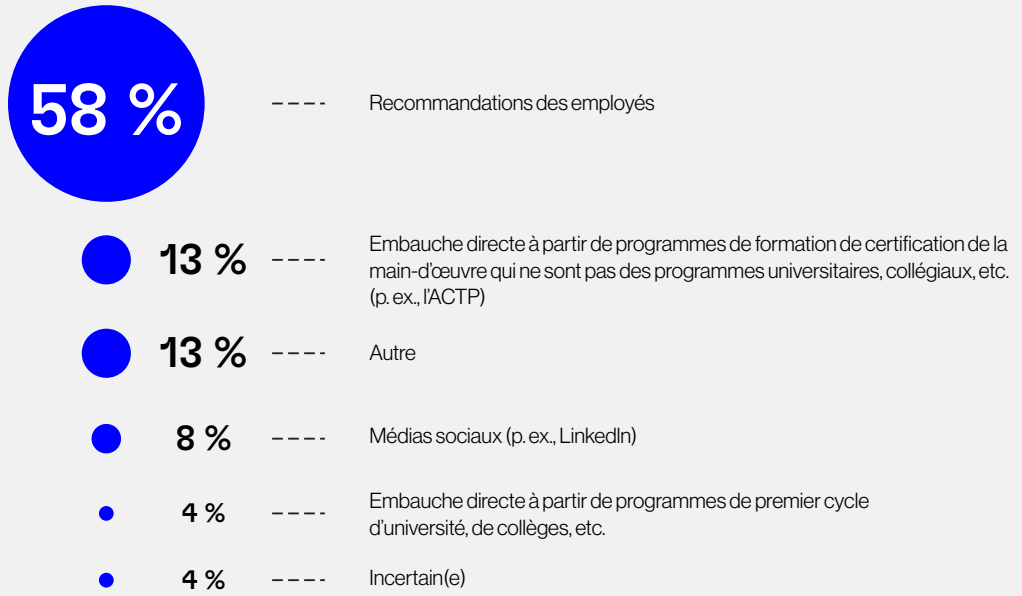
Les partenaires en emploi estiment que les aspects non monétaires d'un emploi, comme l'horaire flexible et les possibilités de perfectionnement professionnel, peuvent attirer tout autant les candidats que la rémunération.

La majorité des partenaires en emploi interrogés estiment que le salaire (88 %), l'horaire de travail flexible et le télétravail (88 %) et les occasions de perfectionnement professionnel (76 %) sont les facteurs les plus importants aux yeux des personnes qui recherchent un emploi en cybersécurité (Figure 2)[10]. Cela veut donc dire que pour attirer les meilleurs candidats, ces partenaires pourraient mettre en valeur des aspects non monétaires d'un emploi,

comme l'horaire flexible et les occasions d'apprentissage (certifications, microcrédits), dans la description de poste et le processus d'embauch.

De nombreux répondants encouragent les possibilités de perfectionnement professionnel[11]. Interrogés sur les moyens spécifiques mis en œuvre par les entreprises pour aider leurs employés à obtenir des certifications en cybersécurité, la plupart des employeurs ont indiqué qu'ils offraient des incitatifs pécuniaires ou payaient les frais de cours (83 %), qu'ils collaboraient avec les employés pour les aider à suivre les cours appropriés (65 %) et qu'ils accordaient des congés pour suivre des formations et assister à des cours (43 %). Comme le mentionne également Kvochko (2021), la formation d'appoint des employés actuels qui montrent un intérêt pour la sécurité peut être une stratégie payante pour les entreprises qui ont du mal à recruter.

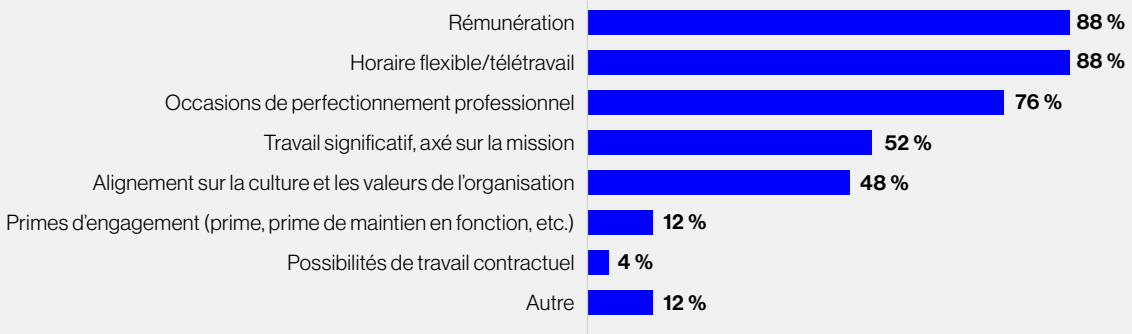
Figure 1 | Canaux de recrutement les plus efficaces



Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Les trois autres options de réponse n'ayant été choisies par aucun des répondants étaient : recruteurs spécialisés externes, affichage sur les babillards d'emploi et compétitions de capture du drapeau (CTF) ou programmes de chasse aux bogues (Bug Bounty).

Figure 2 | Facteurs les plus importants aux yeux des personnes qui recherchent un emploi en cybersécurité, selon les partenaires en emploi



Remarque : Ces pourcentages sont établis en fonction des réponses de 25 personnes.

Besoins en matière de compétences : Quels sont les rôles et les compétences recherchés?

La vitesse fulgurante à laquelle le secteur de la cybersécurité évolue nous oblige à comprendre les besoins en matière de recrutement des partenaires en emploi, de sorte que des programmes tels que l'ACTP puissent s'assurer de concorder avec les besoins de l'industrie. Pour ce faire, nous avons interrogé les répondants sur les besoins de leur entreprise en matière de recrutement et sur la manière dont ces besoins allaient, selon eux, évoluer au cours des trois à cinq prochaines années.

Découverte nº 3

Alors que les partenaires en emploi s'attendent à avoir besoin de deux à cent professionnels de la cybersécurité au cours de la prochaine année, cette demande pourrait doubler à moyen ou long terme, la demande actuelle et future la plus forte se situant dans la catégorie des rôles de protection et de défense.

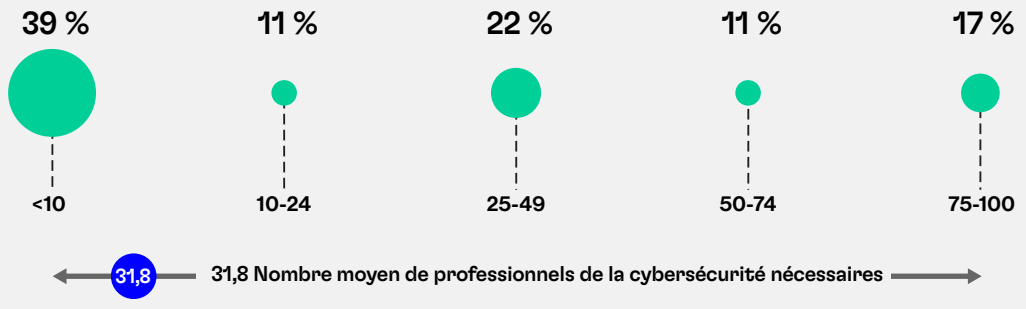
Les besoins en recrutement peuvent varier en fonction de la taille de l'entreprise, de la nature des activités et de la croissance prévue. Les partenaires en emploi interrogés s'attendent à avoir besoin de deux à cent professionnels de la cybersécurité dans leur entreprise au cours des 12 à 18 prochains mois, bien que la plupart d'entre eux estiment que leur entreprise aura besoin de moins de 10 professionnels (40 %) (Figure 3). Les deux répondants interrogés individuellement ont déclaré que leurs besoins en matière de cyberprofessionnels doubleront probablement dans les trois à cinq prochaines années.

En nous appuyant sur le Cadre des compétences en matière de cybersécurité au Canada (TECHNATION, 2022),, nous avons examiné quatre catégories de rôles de cybersécurité axés sur les affaires pour lesquels cette demande est susceptible de se manifester : protection et défense, conception et développement, supervision et gouvernance, et exploitation et maintenance. La catégorie affichant la plus forte demande actuelle et future pour des professionnels de la cybersécurité est la catégorie « protection et défense », ce qui comprend des postes tels qu'analyste en cybersécurité, testeur d'intrusion, intervenant en cas d'incident de cybersécurité et analyste en criminalistique numérique (Figure 4A)[12]. Cette forte demande devrait se maintenir au cours des trois à cinq prochaines années (78 %)[13]. De façon générale, les partenaires en emploi de l'ACTP estiment que toutes les catégories connaîtront un schéma de demande similaire d'ici trois à cinq ans.

Découverte nº 4

L'intervention en cas d'incident, l'infonuagique et la gestion des cyberrisques continueront de faire l'objet d'une forte demande de la part des partenaires en emploi, alors que la sécurité des données semble constituer un besoin émergent tandis que l'analyse des données de sécurité pourrait voir la demande diminuer dans un avenir proche.

Figure 3 | **Estimation du nombre de professionnels de la cybersécurité nécessaires dans 12 à 18 mois**



Remarque : Ces pourcentages sont établis en fonction des réponses de 18 personnes.

Les trois spécialisations les plus recherchées par les partenaires en emploi de l'ACTP sont l'intervention en cas d'incident (54 %), l'infonuagique (46 %) et la gestion des cyberrisques (38 %), et cette demande est susceptible d'augmenter : 65 % des répondants ont indiqué que l'intervention en cas d'incident et l'infonuagique seront les spécialisations les plus recherchées au cours des trois à cinq prochaines années (Figure 4B). Ces résultats sont peut-être dus au fait que l'équipe de l'ACTP a intentionnellement collaboré avec des entreprises qui ont besoin de ces postes, pour lesquels les personnes diplômées de l'ACTP sont formées.

Une spécialisation qui sera probablement recherchée par les partenaires en emploi est la sécurité des données (21 % actuellement, mais 35 % au cours des trois à cinq prochaines années). Puisque le volume de données possédées et gérées par les entreprises est appelé à augmenter, la demande de professionnels spécialisés dans ce domaine suivra le pas, car les entreprises chercheront à protéger leurs données organisationnelles contre la perte, la compromission et l'utilisation non autorisée.

Figure 4A | Catégories de cybersécurité recherchées

	Actuelles	Futures
Protection et défense	75 %	78 %
Conception et développement	38 %	43 %
Supervision et gouvernance	29 %	26 %
Exploitation et entretien	17 %	26 %
Autre	25 %	0 %
Incertain(e)	0 %	13 %

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes (actuelles) et 23 personnes (futures) respectivement.

Figure 4B | Spécialisations en cybersécurité recherchées[14]

	Actuelles	Futures
Intervention en cas d'incident	54 %	65 %
Infonuagique	46 %	65 %
Gestion des risques en cybersécurité	38 %	52%
Gestion des accès par identification	38 %	s. o.
Processus d'automatisation de la sécurité	38 %	39 %
Collecte et analyse des renseignements sur les risques	38 %	39 %
Analyse des données de sécurité	29 %	13 %
Ingénierie de sécurité	25 %	26 %
Processus de sécurité automatisés	25 %	17 %
Sécurité des données	21 %	35 %

Pourcentages établis en fonction des réponses de 24 personnes (actuelles) et 23 personnes (futures) respectivement.

La seule spécialisation qui devrait connaître une baisse de demande est des répondants estiment que ce groupe fait partie des groupes les plus recherchés actuellement, seulement 13 % croient que ce sera toujours le cas dans trois à cinq ans (Figure 4B). Cela est probablement dû au fait que l'adoption d'outils d'intelligence artificielle et d'apprentissage automatique est en hausse. Ces attentes changeantes sur le plan de la demande peuvent orienter des programmes tels que l'ACTP qui cherchent à adapter leur programme d'études pour répondre aux besoins des employeurs et du secteur.

Découverte nº 5

Les partenaires en emploi valorisent actuellement fortement les compétences techniques telles que les techniques de détection et de réponse aux intrusions, le dépannage et le fonctionnement des systèmes de protection et de défense des réseaux, mais cela devrait changer dans les trois à cinq prochaines années.

Dans le recrutement pour des postes de niveau débutant en cybersécurité, les trois compétences techniques les plus valorisées par les partenaires en emploi ayant répondu au sondage sont les techniques de détection et de réponse aux intrusions (50 %), le dépannage (42 %) et le fonctionnement des systèmes de défense et de protection des réseaux (38 %). Un tiers des personnes interrogées a également indiqué que l'évaluation des vulnérabilités et la gestion de l'identité et de l'authentification faisaient partie des compétences techniques recherchées (Figure A1 en annexe).

Plus de 60 % des répondants estiment que les compétences techniques les plus valorisées par leur entreprise sont appelées à changer d'ici trois à cinq ans (Figure 5)[15]. En ce qui a trait aux langages de programmation et de script, les partenaires valorisent principalement le langage Python pour les postes de niveau débutant. Les langages relativement peu recherchés sont Shell (42 %), JavaScript (33 %), LINUX (33 %) et Java (29 %) (Figure A4 en annexe).

Découverte nº 6

La communication verbale, la résolution de problèmes et la pensée critique ainsi que le souci du détail sont actuellement les compétences non techniques les plus valorisées par les partenaires en emploi, et ces compétences devraient continuer à être recherchées dans les trois à cinq prochaines années.

Les trois compétences non techniques les plus valorisées par les partenaires en emploi de l'ACTP pour les postes de cybersécurité de niveau débutant sont la communication verbale (88 %), la résolution de problèmes et la pensée critique (88 %) et le souci du détail (83 %) (Figure A2 en annexe)[16]. Les répondants ont également souligné que la capacité d'adaptation et la capacité à travailler sous pression étaient des compétences non techniques précieuses. Cette constatation est conforme à un rapport récent de (ISC)[2] (2021) qui a révélé qu'à l'échelle mondiale, de solides capacités de résolution de problèmes, la curiosité et la soif d'apprendre ainsi que les compétences en communication étaient aussi importantes, sinon plus, que les certifications et l'expérience pertinente en cybersécurité.

Contrairement aux compétences techniques, qui semblent avoir une durée de vie plus courte, ces compétences non techniques devraient continuer à être en demande au cours des trois à cinq prochaines années : 70 % des répondants ont indiqué que ce serait le cas (Figure 5). Une personne rencontrée a déclaré que, même si son entreprise valorise les compétences techniques, elle préférerait probablement des candidats passionnés par le travail et possédant de bonnes aptitudes en résolution de problèmes, même si ces personnes ne possèdent pas exactement les compétences techniques recherchées. Pour des programmes comme l'ACTP, cela signifie de faire comprendre l'importance de ces compétences aux personnes inscrites au programme, afin qu'elles puissent les développer parallèlement à l'acquisition des compétences techniques.

Figure 5 | Évolution de la demande pour les compétences techniques et non techniques

61 % ont indiqué que les compétences techniques recherchées par leur entreprise chez les professionnels de la cybersécurité vont changer d'ici trois à cinq ans.

70 % ont indiqué que les compétences non techniques recherchées par leur entreprise chez les professionnels de la cybersécurité **ne vont pas** changer d'ici

Plus de 35 %
valorisent les compétences suivantes :

- Techniques de détection et de réponse aux intrusions
- Dépannage
- Fonctionnement des systèmes de défense et de protection des réseaux

Plus de 80 %
valorisent ces compétences non techniques

- Communication verbale
- Résolution de problèmes et pensée critique
- Souci du détail

Plus de 46 %
valorisent ces certifications :

- GIAC Security Essentials Certifications
- GIAC Certified Incident Handlers (GCIH)
- CompTIA Security +

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Défis pour les employeurs : Quels sont les principaux problèmes auxquels sont confrontés les employeurs?

Nous voulions connaître les principaux problèmes auxquels sont confrontés les partenaires en emploi dans le recrutement de cybertalents. Nous avons posé aux répondants des questions sur les types de défis auxquels leur entreprise et l'ensemble du secteur de la cybersécurité sont confrontés dans le recrutement de cyberprofessionnels.

Découverte nº 7

Les principaux défis de l'industrie sont la pénurie de talents qualifiés en cybersécurité et l'inadéquation entre la rémunération et les avantages offerts et les attentes des candidats.

Les répondants des partenaires en emploi ont confirmé l'existence d'un défi à l'échelle de l'industrie – une pénurie de talents qualifiés en cybersécurité au Canada – qui empêche les entreprises de répondre à leurs besoins de recrutement (Figure 7). Ce sentiment se reflète également dans les réponses concernant les défis de recrutement propres à chaque entreprise, tels que le manque de qualification du bassin de candidats (58 %), le manque de compétences pertinentes des candidats (50 %) et la forte concurrence pour les bons talents (58 %). Dans le même ordre d'idées, un tiers des répondants estime que le bassin de candidats aux postes à pourvoir est restreint (33 %) (Figure 6). En expliquant davantage certains de ces défis, une personne interrogée individuellement a souligné qu'au niveau débutant, tout le monde veut « faire le travail le plus sexy » (par exemple, être un pirate ou un testeur d'intrusion), mais ces rôles exigent beaucoup de connaissances et ne peuvent pas être assumés par une personne qui débute sa carrière dans le secteur.

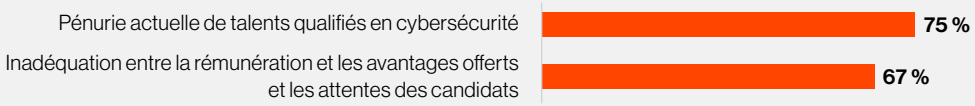
Au niveau sectoriel, les répondants ont perçu une inadéquation entre la rémunération et les avantages offerts et les attentes des candidats (67 %). Une étude effectuée par Deloitte (n.d.) détermine également que « la rémunération et les incitatifs ne suivent pas le rythme des taux du marché, qui sont continuellement gonflés en raison du manque d'offre pour répondre à la demande ». Les personnes interrogées individuellement ont confirmé que même pour les postes de niveau débutant, les candidats s'attendent à gagner 20 à 40 % de plus que ce que les employeurs sont généralement prêts à offrir.

Interrogés à propos des rôles de cybersécurité pour lesquels leur entreprise a eu le plus de difficulté à embaucher au cours des trois derniers mois, 29 % des répondants ont mentionné les postes d'intervenant en cas d'incident de cybersécurité et d'analyste de l'exploitation en cybersécurité comme étant les deux postes les plus difficiles à pourvoir (Figure A5 en annexe).

> Les rôles et les responsabilités en cybersécurité doivent être éclaircis, car actuellement, tout est très flou. Le milieu est très réactif et manque de planification et d'investissements.

Répondant au sondage

Figure 6 | Difficultés de recrutement les plus fréquentes dans l'industrie de la cybersécurité



Moins de 30 % ont choisi ces difficultés de recrutement :

- Trop nombreuses certifications sur le marché et manque de clarté quant aux résultats d'apprentissage de chacune d'entre elles.
- Perception selon laquelle les rôles de cybersécurité sont très stressants, ont une charge de travail importante et des horaires irréguliers
- Manque de flexibilité sur le plan du télétravail
- Descriptions de poste ou offres d'emploi exigeant plus d'expérience que nécessaire
- Compréhension limitée des candidats quant au fait que la cybersécurité constitue un domaine informatique distinct lorsqu'ils postulent à des postes dans ce domaine
- Absence de parcours professionnels clairs et directs menant à la cybersécurité
- Compréhension limitée des employeurs quant au fait que la cybersécurité constitue un domaine informatique distinct lorsqu'ils embauchent pour des postes en cybersécurité
- Manque de clarté pour les candidats concernant les exigences en matière d'éducation, de formation ou d'expérience préalable pour les postes de cybersécurité
- Manque de clarté pour les employeurs concernant les exigences en matière d'éducation, de formation ou d'expérience préalable pour les postes de cybersécurité
- Manque d'options de formation (p. ex., microcrédits, hackathons) pour combler le déficit de compétences
- Autre

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Découverte nº 8

Les partenaires en emploi ont déterminé trois obstacles à la création de descriptions de poste précises pour les fonctions de cybersécurité de niveau débutant : une inadéquation entre les attentes de l'entreprise et celles des candidats, un manque de compréhension de la part des responsables des RH et le rythme rapide auquel l'industrie évolue.

Bien que les descriptions de poste imprécises n'aient pas été mentionnées parmi les principales difficultés de recrutement par les partenaires en emploi ayant répondu au sondage, 70 % d'entre eux ont décrit les obstacles qui pourraient empêcher les organisations de créer des descriptions de poste précises pour les rôles de cybersécurité de niveau débutant[17]. Notre analyse des réponses ouvertes révèle trois grands obstacles.

Divergence entre les attentes du candidat concernant un emploi et ce que l'employeur veut et peut offrir. Cela comprend :

- L'embellissement du poste face aux candidats.
- Un décalage entre le modèle commercial de l'entreprise et les objectifs personnels du candidat.
- Les employeurs qui en demandent trop aux candidats qui postulent à des postes de niveau débutant.
- Certains postes de niveau débutant exigent plus d'expérience que ne le laissent entendre les offres d'emploi.

Manque de compréhension de la part des responsables du recrutement ou des professionnels des RH. Les répondants avaient le sentiment que les gestionnaires d'embauche et les professionnels des RH n'avaient pas une connaissance suffisante du secteur, des exigences professionnelles des rôles dans le domaine de la cybersécurité et de la manière de formuler ces exigences dans une description de poste.

Par exemple, un répondant a souligné que les RH peuvent compliquer à l'excès les compétences requises pour le poste en donnant l'impression qu'il exige une connaissance approfondie de certains sujets en matière de cybersécurité, alors que seules des connaissances générales peuvent être nécessaires.

Secteur en évolution rapide, avec des exigences qui changent rapidement. En raison de l'évolution constante des besoins du secteur de la cybersécurité, il peut être difficile pour les descriptions de poste de suivre le rythm (Rashotte, 2019). Par exemple, la croissance rapide des équipes de cybersécurité peut engendrer des changements dans les tâches et les responsabilités qui ne sont pas reflétés dans les descriptions de poste. De plus, la cybersécurité englobe plusieurs domaines, ce qui rend difficile la tâche de couvrir toutes les tâches en une seule description de poste. Et pour terminer, les partenaires ont également souligné l'absence d'une stratégie générale en cybersécurité.

Diversifier le secteur : Quels sont les défis et les occasions à venir?

Si la sous-représentation des femmes dans les domaines des STIM est un problème de longue date, ces dernières années ont vu des progrès dans la diversification de plusieurs domaines traditionnellement dominés par les hommes. À l'échelle mondiale, les femmes représentent désormais 25 % de la main-d'œuvre en cybersécurité ((ISC2), 2021). Bien que de nombreux employeurs reconnaissent la nécessité de diversifier le secteur, ils adoptent différentes approches formelles et informelles pour garantir la diversité, comme la prescription de quotas[18].

Nous avons cherché à savoir si les employeurs sont confrontés à des difficultés dans le recrutement de PANDC et de femmes spécialisées en cybersécurité, quels programmes ou initiatives existent pour promouvoir une plus grande diversité dans le secteur et quelles stratégies pourraient améliorer le statu quo.

Découverte nº 9

Certains partenaires en emploi ont signalé des difficultés dans le recrutement de personnes autochtones, noires et de couleur et de femmes dans le secteur de la cybersécurité et ont proposé trois stratégies pour remédier à ce problème : s'associer aux réseaux et événements pertinents, offrir des occasions d'éducation et de formation ciblées et être ouvert à l'embauche de membres de groupes sous-représentés.

> « Soyez plus ouverts d'esprit. Si tout le monde a les mêmes chances, il est fort possible que nous puissions toujours trouver les perles rares. »
>
> Répondant au sondage

Près de la moitié des partenaires en emploi interrogés ont déclaré que leur entreprise n'avait pas rencontré de difficultés pour recruter des PANDC ou des femmes spécialisées en cybersécurité à ce jour (48 %). Toutefois, 35 % ont perçu cela comme un défi[19]. Une personne interrogée individuellement a révélé que son entreprise souhaitait étendre ses efforts de recrutement aux populations mal desservies, en particulier les Autochtones, mais que les programmes actuels n'avaient pas été très fructueux. De même, la seconde personne interrogée individuellement a souligné que, bien que son organisation cherche activement à recruter des femmes et des PANDC, il n'est pas facile de trouver des candidats appartenant à ces groupes en raison de la composition actuelle de la population de cybersécurité dans les universités et les collèges où elle embauche.

Pour remédier à ce problème, nous avons demandé aux personnes interrogées de suggérer des mesures à prendre pour promouvoir le recrutement et l'embauche d'un plus grand nombre de PANDC ou de femmes spécialisées en cybersécurité. Près de 70 % des répondants ont fait part de leurs idées, que nous résumons en trois points principaux ci-dessous :

S'associer aux réseaux pertinents :

Les employeurs peuvent s'associer aux réseaux susceptibles de les mettre en relation avec le bassin de talents qu'ils recherchent. Les répondants ont suggéré de s'associer à des réseaux de PANDC et de femmes actives dans le cyberespace, à des organismes sans but lucratif ou à des programmes de formation en cybersécurité réputés (comme l'ACTP) qui possèdent un bassin diversifié de candidats à embaucher. De plus, les employeurs peuvent participer à des panels ou événements s'adressant à des groupes sous-représentés, où ils pourraient rencontrer des employés potentiels. Ces événements peuvent également offrir d'excellentes occasions pour les PANDC et les femmes spécialisées en cybersécurité d'inciter d'autres personnes à rejoindre le secteur.

Créer davantage de possibilités d'éducation et d'amélioration des compétences pour les groupes sous-représentés :

Les employeurs peuvent créer davantage d'occasions axées sur l'éducation et l'amélioration des compétences pour les PANDC et les femmes intéressées au secteur. Parmi les suggestions, notons le fait de leur donner « les bonnes compétences au bon moment », de leur offrir des occasions et un soutien en matière d'éducation en sécurité, de créer des occasions de formation pour les personnes issues de ces groupes si les recruteurs ne parviennent pas à attirer des candidats diversifiés et de promouvoir la cybersécurité en tant que carrière au sein des communautés concernées de PANDC et de femmes afin d'aider à corriger les perceptions erronées à propos du secteur.

Créer un changement de culture pour être plus ouvert à la diversité des origines :

Les employeurs peuvent s'efforcer de faire preuve d'une plus grande ouverture d'esprit lorsqu'il s'agit de recruter des candidats et de les retenir. Les répondants ont suggéré de ne pas se concentrer uniquement sur les diplômes et les aspects techniques de la cybersécurité, mais d'écouter avec un esprit ouvert les perspectives qu'apportent des personnes d'horizons divers.

En plus de ces trois stratégies, une autre suggestion était de proposer une certaine flexibilité dans les lieux de travail, ce qui permettrait aux employeurs de choisir des candidats dans un bassin plus large, et attirerait des membres des groupes sous-représentés basés à divers endroits.

> « La clé est de choisir la bonne personne pour le poste, peu importe son profil démographique. »
>
> Personne interrogée individuellement

Découverte nº 10

Si la plupart des partenaires en emploi ont mis en œuvre des programmes visant à recruter des candidats diversifiés pour les postes en cybersécurité et offrent une formation générale en matière d'inclusion en milieu de travail, seuls quelques-uns ont investi pour assurer la diversité dans la direction, offrir des occasions de perfectionnement ciblées et proposer une formation approfondie liée à la diversité, à l'équité et l'inclusion (DEI).

La plupart des partenaires en emploi ayant répondu au sondage ont indiqué que leur entreprise avait mis en œuvre des programmes visant le recrutement des candidats diversifiés dans les postes de cybersécurité (74 %). Cela reflète probablement les liens que les employeurs entretiennent avec l'équipe

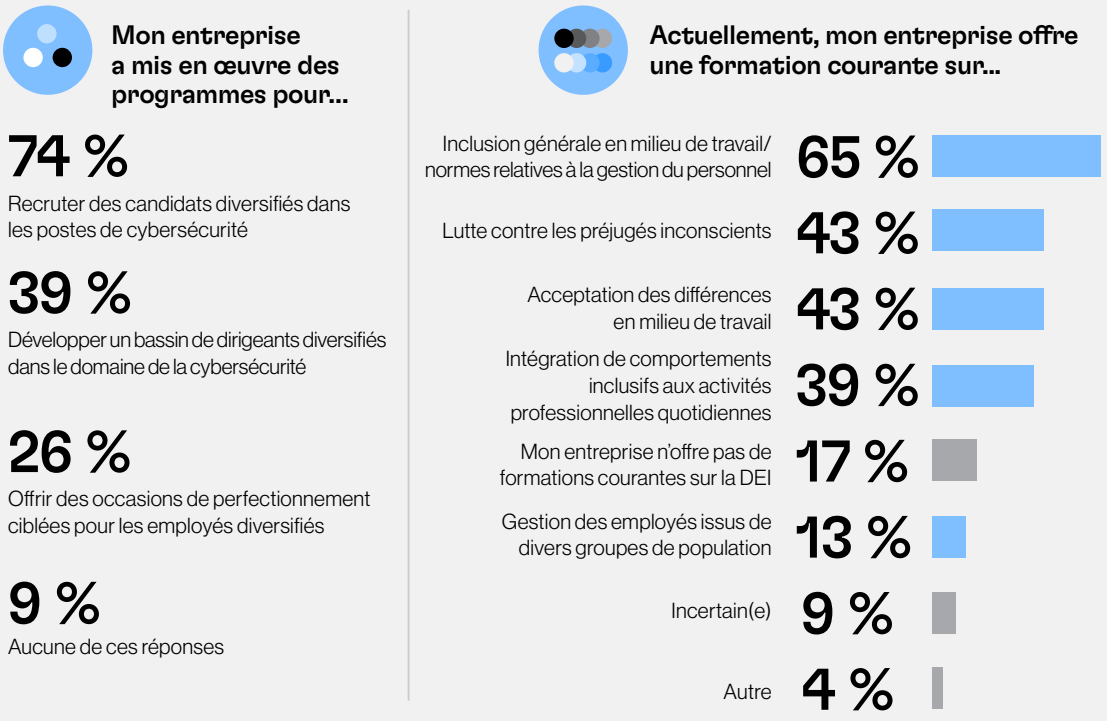
de Catalyst pour recruter des cybertalents de l'ACTP, qui fournit un flux constant de talents diversifiés et qualifiés. Toutefois, un plus petit nombre de répondants ont indiqué que leur entreprise disposait de programmes visant à développer un bassin de dirigeants diversifiés dans le domaine de la cybersécurité (39 %), et seulement 26 % des entreprises interrogées disposent de programmes offrant des occasions de perfectionnement ciblées pour les PANDC et les femmes (Figure 8).

Une personne interrogée individuellement a fait valoir que dans le cadre de ses efforts visant à bâtir une main-d'œuvre plus inclusive, son entreprise offre aux employés une formation portant sur la diversité. Son approche est de « changer la mentalité [sur le plan de la DEI] plutôt que le processus ». Cela signifie que plutôt que de mettre en œuvre des programmes ciblant les PANDC et les femmes parmi leur effectif, certains employeurs offrent des programmes à l'ensemble de leurs employés dans le but d'améliorer la sensibilisation aux questions portant sur la diversité afin de bâtir une main-d'œuvre plus inclusive.

Si la formation n'est qu'une petite partie de l'adoption de la diversité, de l'équité et de l'inclusion sur le lieu de travail, elle indique le niveau d'engagement ou de priorité que les entreprises y accordent. La plupart des répondants ont indiqué que leur entreprise offre une formation générale sur l'inclusion en milieu de travail (65 %)[20]; toutefois, les entreprises sont moins nombreuses à offrir une formation sur la lutte contre les préjugés inconscients (43 %), sur l'acceptation des différences en milieu de travail (43 %) et sur l'intégration de comportements inclusifs aux activités et responsabilités professionnelles quotidiennes (39 %). Très peu d'entre elles offrent une formation sur la gestion des employés issus de divers groupes de population (13 %) et certaines n'offrent aucune formation sur la DEI.

Les conclusions présentées dans cette section ont été établies à partir des réponses données par des employeurs ayant des liens étroits avec l'ACTP. Toutefois, ces informations sont d'une pertinence plus large pour les programmes de formation qui visent à doter les personnes intéressées par le secteur de la cybersécurité des compétences pertinentes pour l'industrie. La prochaine section présente un aperçu de la recherche en cours sur les employeurs, qui va au-delà des partenaires en emploi actuels de l'ACTP, ainsi que quelques conclusions préliminaires de cette recherche.

Figure 7 | Pratiques de recrutement DEI



Remarque : Ces pourcentages sont établis en fonction des réponses de 23 personnes.

3 Sondage sur l'industrie en général : premières conclusions

Pour cette recherche en cours, l'équipe de l'ACTP a dressé une liste de professionnels au sein d'entreprises ayant actuellement des interactions limitées avec l'ACTP et a eu recours aux médias sociaux pour atteindre un large éventail d'employeurs. Les questions posées dans ce sondage sont très semblables à celles posées dans le sondage des partenaires en emploi de l'ACTP. Cela nous permettra de comparer les besoins en matière de recrutement de ces deux groupes d'employeurs. Nous croyons que ces informations peuvent aider l'équipe de l'ACTP à déterminer les besoins et à soutenir les exigences en matière de talents du secteur de la cybersécurité dans son ensemble.

Le sondage a été envoyé à environ 150 professionnels intermédiaires et de haut niveau au sein de 85 entreprises[21]. En date de juillet 2022, nous avions reçu 29 réponses, et le sondage demeurera ouvert pendant encore quelques semaines. Dans un rapport de suivi publié l'année prochaine, nous présenterons un portrait approfondi des besoins actuels et futurs en matière de talents en cybersécurité, des écarts sur le plan des compétences, des pratiques existantes pour recruter des candidats plus diversifiés et des défis à relever en fonction des résultats du sondage. Cette courte section présente deux conclusions préliminaires qui servent d'exemples de ce que les partenaires de l'industrie pourront retrouver dans le rapport à venir.

Les employeurs du secteur de la cybersécurité considèrent également que les recommandations des employés constituent le canal de recrutement le plus efficace, mais par rapport aux partenaires en emploi de l'ACTP, certains d'entre eux privilégient également le recrutement de candidats par le biais des médias sociaux et des programmes de premier cycle.

Nous constatons que les recommandations des employés continuent d'être perçues comme le moyen le plus efficace d'embaucher dans le secteur canadien de la cybersécurité (48 %). L'utilisation des médias sociaux, comme LinkedIn, se classe au second rang, mais l'écart est important (21 %). Cela pourrait laisser penser que les employeurs pourraient avoir de moins en moins recours aux offres d'emploi en ligne pour trouver les cybertalents qu'ils recherchent. L'accent placé sur les recommandations des employés a également des répercussions sur la diversification de la main-d'œuvre en cybersécurité : le secteur est largement dominé par des hommes et des personnes ayant une expérience en TI (Deloitte, n.d.) et on y retrouve peu de femmes et de groupes racisés, ce qui signifie qu'un recrutement axé sur les recommandations des employés pourrait avoir comme effet de solidifier cette composition.

Les employeurs en cybersécurité et les partenaires en emploi de l'ACTP s'accordent sur les principaux défis de l'industrie, mais divergent sur d'autres défis auxquels le secteur est confronté.

Le Canada ne semble pas être différent lorsqu'il s'agit du défi le plus important auquel est confronté le secteur de la cybersécurité : il existe à l'heure actuelle une pénurie de talents qualifiés[22]. Tout comme les partenaires en emploi de l'ACTP, les répondants du secteur en général estiment qu'il s'agit là du principal défi en matière de recrutement (62 %), suivi par l'inadéquation entre la rémunération et les avantages offerts et les attentes des candidats (54 %).

Cependant, les répondants divergent de leurs homologues partenaires en emploi de l'ACTP sur deux points. En premier lieu, bon nombre d'entre eux ont souligné le manque de parcours professionnels clairs et direct vers la cybersécurité (42 %).

Cela ne semble pas être un problème propre au Canada : dans un récent sondage, Enterprise Security Group a constaté que 66 % des professionnels de la cybersécurité dans le monde n'ont pas de parcours professionnel clairement établi pour amener leur carrière au niveau supérieur (Deloitte, n.d.).

La seconde divergence porte sur la compréhension limitée des employeurs quant au fait que la cybersécurité constitue un domaine informatique distinct (42 %). Ces défis ne sont pas nécessairement les premiers auxquels les partenaires en emploi de l'ACTP songent, ce qui indique que le secteur en général pourrait avoir des priorités différentes. Les employeurs devront développer leur compréhension des besoins uniques et de la nature distincte de la cybersécurité au sein de l'informatique, et les organismes proposant des formations en cybersécurité devront définir des voies d'accès claires au secteur.

Une proportion similaire d'employeurs du secteur de la cybersécurité ont déclaré être confrontés à des défis dans le recrutement de talents diversifiés, comme les partenaires de l'ACTP : 36 % ont déclaré que leur entreprise a rencontré des difficultés pour recruter et embaucher des PANDC ou des femmes spécialisées en cybersécurité.

Échanger avec les employeurs : Le conseil consultatif sectoriel de Catalyst

Formé de huit cadres supérieurs occupant des postes importants en cybersécurité au sein d'entreprises chefs de file du secteur au Canada, le conseil consultatif de l'ACTP a pour objectif d'orienter la recherche effectuée dans le cadre du projet d'initiative de transformation des cybertalents (CTTI) et d'assurer un dialogue ouvert entre l'équipe de Catalyst et les entreprises qui emploient des personnes diplômées de l'ACTP. Le conseil s'est réuni une première fois en mars 2022 et se rencontre chaque trimestre. Cette approche collaborative permet à l'équipe de Catalyst de partager des mises à jour de recherche pertinentes et d'obtenir des commentaires sur la mise en œuvre de l'ACTP.

Plus particulièrement, le conseil consultatif a pour mandat de :

- Conseiller sur les répercussions potentielles des résultats de la recherche du projet d'initiative de transformation des cybertalents sur l'industrie.
- Conseiller sur les moyens d'améliorer la mobilisation des connaissances, la communication et l'engagement avec l'industrie.
- Déterminer les occasions pour l'ACTP de répondre le plus efficacement aux besoins de talents en matière de cybersécurité.
- Tenir compte des recherches, des pratiques exemplaires et des mesures prises par d'autres institutions pour faire progresser les initiatives de développement des compétences et de diversité dans l'écosystème de la cybersécurité.
- Discuter des idées créatives et des approches nouvelles pour réduire les obstacles existants, y compris les mesures à court et long terme.
- Conseiller sur des questions liées à la certification et aux microcrédits.
- Participer à l'identification des placements étudiants et des occasions d'emploi.
- Faire des recommandations sur les domaines de développement des compétences en matière de cybersécurité.

À la suite de discussions sur la pénurie croissante de talents en cybersécurité au Canada, l'équipe de l'ACTP travaille à la préparation d'un guide de gestion des talents en cybersécurité qui comprendra les pratiques exemplaires en matière de gestion des talents tirées des disciplines des ressources humaines, du développement organisationnel et de la cybersécurité. En s'appuyant sur ces meilleures pratiques, le guide inversera également le scénario de la génération de talents à l'échelle nationale en adoptant une approche fondée sur les besoins pour déterminer les exigences en matière de cybersécurité au Canada et en faisant participer l'ensemble de l'écosystème de la cybersécurité à la création d'un bassin de talents mieux adapté aux besoins nationaux, régionaux et sectoriels.

4 Recommandations

Nos conclusions nous permettent de réitérer l'existence d'un défi auquel est confronté le secteur de la cybersécurité à l'échelle mondiale : une grave pénurie de cybertalents qualifiés qui empêche les entreprises de répondre à leurs besoins de recrutement. De plus, la pandémie de COVID-19 a fait exploser la demande de télétravail, ce qui a engendré l'augmentation de la demande de talents en cybersécurité.

Dans la présente section, nous nous concentrons sur deux groupes de parties prenantes au sein de l'écosystème de la cybersécurité : les responsables des programmes dans les organismes visant à constituer un bassin de talents en mettant l'accent sur les groupes sous-représentés, et les employeurs canadiens de la cybersécurité.

En fonction des conclusions détaillées à la section 2, nous présentons ici trois recommandations clés pour chacun de ces groupes dans le but de combler efficacement l'écart croissant entre l'offre et la demande de talents en cybersécurité au Canada.

Programmes tels que l'ACTP

Recommandation nº 1 : Les programmes tels que l'ACTP devraient se concentrer à doter les participants des compétences requises pour occuper des rôles de protection et de défense.

Les partenaires en emploi ayant répondu au sondage estiment que les rôles de protection et de défense constituent la catégorie la plus recherchée par leur entreprise et s'attendent à ce que cette demande se maintienne au cours des trois à cinq prochaines années (plus de 75 %). Les programmes tels que l'ACTP devraient ainsi concevoir leur programme d'études de manière à répondre efficacement à cette demande.

L'ACTP prépare ses étudiants aux postes de niveau débutant, et bon nombre des rôles de la catégorie « protection et défense » constituent une suite logique à ces rôles de niveau débutant (p. ex., testeur d'intrusion et analyste en criminalistique numérique). Si l'ACTP peut répondre à la forte demande dans la catégorie « protection et défense », cela établira une voie à suivre pour les candidats dans leur carrière en cybersécurité.

De plus, dans les catégories et spécialisations très sollicitées, les compétences techniques recherchées par les employeurs sont susceptibles de changer (60 % l'ont mentionné), et donc, les programmes doivent demeurer flexibles pour s'adapter à l'évolution des besoins.

Recommandation n°2: En plus de doter les participants de compétences techniques et de certifications, les programmes tels que l'ACTP doivent aussi amener les candidats à acquérir des compétences non techniques par l'intermédiaire d'exercices pratiques dans le contexte de la cybersécurité.

Nos conclusions indiquent que bien que les compétences techniques recherchées par les employeurs sont susceptibles de changer d'ici trois à cinq ans, certaines compétences non techniques actuellement recherchées demeureront quant à elles pertinentes dans le futur. Par ailleurs, les employeurs valorisent parfois plus ces compétences que les compétences techniques, qui sont relativement simples à transmettre.

Les programmes tels que l'ACTP qui veulent s'assurer que les participants puissent travailler efficacement comme professionnels de la cybersécurité devraient mettre l'accent sur les compétences non techniques que les employeurs valorisent, comme la communication verbale, la résolution de problèmes et la pensée critique ainsi que le souci du détail. Bien qu'il s'agisse de traits ou d'attributs que les personnes acquièrent généralement en bas âge, les programmes tels que l'ACTP peuvent s'assurer de deux façons que les participants possèdent ces compétences : (a) au stade de la sélection, en établissant des critères pour évaluer ces compétences chez les candidats intéressés; et (b) pendant le programme, en intégrant ces compétences dans des exercices pratiques de cybersécurité pour les participants.

Recommandation n° 3 : Les programmes tels que l'ACTP peuvent promouvoir la cybersécurité en tant que carrière auprès des communautés concernées de PANDC et de femmes et aider à lutter contre les perceptions erronées de l'industrie.

Afin d'attirer davantage de femmes et de personnes racisées dans le secteur de la cybersécurité, les employeurs ont suggéré de promouvoir la cybersécurité en tant que carrière au sein des communautés concernées de PANDC et de femmes. Pour faire progresser cette stratégie, les différentes parties prenantes de l'écosystème ont un rôle à jouer. Par exemple, les écoles et les universités devraient porter attention à la manière dont elles présentent la cybersécurité comme option de carrière et dissiper les stéréotypes liés au genre qui ont contribué à la sous-représentation des femmes dans le secteur.

Les programmes tels que l'ACTP peuvent collaborer avec les universités afin de mieux faire connaître ce que signifie une carrière dans la cybersécurité, de mettre en évidence le rôle des femmes et des PANDC dans ce secteur et d'encourager les jeunes adultes à suivre la formation et à obtenir les qualifications appropriées. Ils peuvent également faire participer les personnes diplômées de leur programme à des forums ou à des événements destinés aux femmes et aux PANDC afin de mettre en avant leurs réussites et d'inspirer la prochaine génération de dirigeants en cybersécurité.

Employeurs canadiens en cybersécurité

Recommandation n° 1 : Bien que les employeurs perçoivent les recommandations des employés comme un canal de recrutement efficace, ils devraient s'efforcer de remédier à ses limites, notamment en ce qui concerne la manière dont il peut exacerber la sous-représentation actuelle de certains groupes dans la cybersécurité.

Les recommandations d'employés sont attrayantes pour les employeurs pour diverses raisons, et si cette option est souvent la moins risquée lorsqu'il s'agit de trouver des talents, elle n'est pourtant pas sans coût. S'appuyer sur les recommandations des employés, c'est faire largement appel à des réseaux de même type et à des personnes ayant des antécédents sociodémographiques et professionnels similaires. Il est donc probable que cette stratégie fasse obstacle aux mesures visant à lutter contre la sous-représentation des femmes et des personnes racisées dans le secteur.

Pour relever certains des défis potentiels liés au fait de dépendre fortement des recommandations d'employés, les employeurs devraient s'adresser activement aux communautés en ligne, comme les réseaux de femmes ou les nouveaux arrivants au Canada, afin d'établir des liens solides qui peuvent les aider à accéder aux talents dont ils ont besoin au sein de ces communautés. La publication de descriptions de poste précises et claires peut également faire des médias sociaux (p. ex., LinkedIn) un canal plus efficace qu'il ne l'est actuellement.

Recommandation n° 2 : Pour embaucher des candidats issus de groupes traditionnellement sous-représentés, les employeurs doivent s'associer à des réseaux pertinents et participer à des événements ou des panels qui peuvent les mettre en contact avec ce bassin de talents sous-utilisé et être plus ouverts à de nouvelles perspectives.

Pour recruter plus de talents issus de groupes sous-représentés, les répondants ont suggéré de s'associer à des réseaux de PANDC et de femmes actives dans le cyberespace, à des organismes sans but lucratif ou à des programmes de formation en cybersécurité réputés (comme l'ACTP) qui possèdent un bassin diversifié de candidats à embaucher.

Les employeurs peuvent encourager leurs employés, surtout les PANDC et les femmes dans des postes de direction, à participer à des événements et à des panels pour partager leurs histoires et leurs expériences. Les discours de ces cadres peuvent être une forte source de motivation et d'inspiration pour les jeunes professionnels qui envisagent de rejoindre le secteur et d'y rester.

Les répondants ont également indiqué que les employeurs doivent faire preuve d'une « plus grande ouverture d'esprit » en ce qui concerne le recrutement de personnes issues de milieux divers et adopter une vision plus complète de ce qu'un candidat peut offrir, plutôt que de se concentrer uniquement sur ses diplômes et ses compétences techniques. Les employeurs peuvent élargir considérablement leur bassin de candidats s'ils commencent à mettre l'accent sur les compétences et les attributs non techniques et créent des possibilités de formation et de perfectionnement adéquates pour ces personnes[23]. À court terme, alors que l'industrie continue d'utiliser des titres de compétences reconnus, les employeurs devraient travailler avec les organismes pour s'assurer que les personnes issues de groupes diversifiés aient des possibilités appropriées d'obtenir ces titres de compétences.

Recommandation nº 3 Les experts techniques, les RH et les responsables du recrutement des entreprises de cybersécurité devraient travailler ensemble pour rédiger des descriptions de poste précises pour les rôles de cybersécurité de niveau débutant, avec des compétences et des attentes clairement définies.

Les employeurs ont signalé qu'une divergence entre les attentes des candidats concernant un emploi et ce que l'employeur veut et peut offrir, ainsi qu'un manque perçu de compréhension de la part des responsables des RH, compliquent la tâche de rédiger des descriptions de poste précises pour les rôles de cybersécurité de niveau débutant. Pour remédier à ce problème, les experts techniques, les RH et les responsables du recrutement devraient travailler ensemble pour rédiger des descriptions de poste précises et axées sur ce qui est nécessaire, sans compliquer à outrance les exigences requises.

Bien que les employeurs puissent avoir des exigences différentes en fonction de la taille de leur entreprise et de leur équipe ainsi que de la nature de leur activité (les services professionnels comparativement aux services financiers, par exemple), un bon point de départ pour les employeurs serait de discuter des rôles et des responsabilités pour les rôles et les postes courants en matière en cybersécurité et qu'ils se mettent d'accord sur les titres et les qualifications requis ou souhaitables. En ayant des normes de base sur lesquelles s'appuyer, les employeurs pourraient ensuite se rencontrer régulièrement pour réévaluer ces exigences et s'assurer qu'elles suivent l'évolution des besoins de l'industrie.

Conclusion

Le présent rapport livre les vues et les perspectives d'un groupe d'employeurs : les moyennes et grandes entreprises entretenant un lien étroit avec l'ACTP et qui ont besoin de cybertalents. Nous avons examiné leurs stratégies de recrutement pour embaucher et retenir les talents, leur demande en matière de compétences et les défis auxquels elles sont confrontées pour embaucher plus de femmes et de personnes racisées.

Dans un rapport à paraître l'an prochain, nous partagerons les résultats d'un sondage en cours auprès des employeurs qui font partie de l'écosystème canadien de la cybersécurité, ainsi que ceux de la recherche menée auprès des participants à l'ACTP. Nous réunirons les points de vue des participants et des employeurs afin de partager des idées concrètes sur la façon dont les programmes tels que l'ACTP et les employeurs en cybersécurité peuvent mieux combler l'écart entre l'offre et la demande de cybertalents au Canada.

Références

Deloitte. (n.d.). *The changing faces of cybersecurity: Closing the cyber risk gap*. https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

(ISC)². (2021). *A resilient cybersecurity profession charts the path forward*. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

(ISC)². (2022). *(ISC)² Cybersecurity hiring managers guide: Best practices for hiring and developing entry- and junior-level cybersecurity practitioners*. https://www.isc2.org//-/media/ISC2/Research/2022/ISC2-Cybersecurity-Hiring-Managers-Guide.ash

KPMG. (2021). *Perspectives des chefs de la direction — Résultats canadiens*. https://home.kpmg/ca/fr/home/insights/2022/09/kpmg-2022-ceo-outlook-canadian-insights.html

Kvochko, E. (19 octobre 2021). How to attract cybersecurity talent. *Forbes*. https://www.forbes.com/sites/sap/2021/10/19/how-to-attract-cybersecurity-talent-and-build-a-culture-of-security/?sh=7f1a116a6b5f

Lake, S. (30 juin 2022). Companies are desperate for cybersecurity workers — more than 700K positions need to be filled. *Fortune*. https://fortune.com/education/business/articles/2022/06/30/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/

Posadzki, A. (2019). Hackers wanted: Canada faces a troubling shortage of cybersecurity talent. *Globe and Mail*. *https://www.theglobeandmail.com/business/article-canada-faces-a-troubling-shortage-of-cybersecurity-workers/*

PwC. (15 mars 2022). *Using upskilling to solve the cybersecurity talent shortage*. https://proedge.pwc.com/blog/using-upskilling-to-solve-the-cybersecurity-talent-shortage

Rashotte, R. (4 juillet 2019). *The critical shortage of cybersecurity expertise*. Policy Options. https://policyoptions.irpp.org/fr/magazines/july-2019/the-critical-shortage-of-cybersecurity-expertise/

TECHNATION (2022). Canadian Cybersecurity Skills Framework. Retrieved September 21, 2022, from https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurityskills-framework/

Annexe

Figure A1 :

Compétences techniques les plus valorisées	% des répondants
Techniques de détection et de réponse aux intrusions	50 %
Dépannage	42 %
Fonctionnement des systèmes de défense et de protection des réseaux	38 %
Évaluation des vulnérabilités	33 %
Gestion de l'identité et de l'authentification	33 %
Tests d'intrusion	29 %
Application des technologies et méthodologies de sécurité en infonuagique	29 %
Analyse de sécurité	29 %
Tests et évaluation de la sécurité	25 %
Criminalistique numérique	25 %
Langages de programmation et de script relatifs à la sécurité (codage de sécurité)	21 %
Ingénierie de sécurité	21 %
Protection de la gestion des données	21 %
Analyse des logiciels malveillants et ingénierie inverse	21 %
Dépannage des dispositifs de sécurité	17 %
Installation, intégration et essais des dispositifs de sécurité	17 %
Développement de la sécurité des applications	17 %
Vérification et conformité	13 %
Cryptographie, chiffrement et gestion des clés	8 %
Autre	25 %

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Figure A2 :

Compétences non techniques les plus valorisées	% des répondants
Communication verbale	88 %
Résolution de problèmes et pensée critique	88 %
Souci du détail	83 %
Communication écrite (y compris la rédaction de rapports techniques et non techniques)	67 %
Capacité d'adaptation	63 %
Capacité à travailler sous pression	63 %
Travail d'équipe et compétences en leadership	58 %
Service à la clientèle	54 %
Analyse du risque	25 %
Analyse des données ou science des données	25 %
Gestion de projet	25 %
Modélisation des risques	13 %
Autre	13 %

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Figure A3 :

Certifications en cybersécurité les plus valorisées pour les postes de niveau débutant	% des répondants
GIAC Security Essentials Certification (GSEC)	54 %
GIAC Certified Incident Handler (GCIH)	46 %
CompTIA Security +	46 %
GIAC Certified Intrusion Analyst (GCIA)	25 %
CompTIA CyberSecurity Analyst+ (CSA+)	25 %
Certified Information Systems Security Professional (CISSP)	8 %
EC-Council Certified Network Defender	0 %
EC-Council Certified Security Operations Center Analyst	8 %
EC-Council Certified Ethical Hacker (CEH)	17 %
GIAC Security Expert (GSE)	8 %
GIAC Security Leadership Certification (GSLC)	0 %
CompTIA Advanced Security Practitioner (CASP)	8 %
Certified Information Systems Auditor (CISA)	4 %
Certified Information Security Manager (CISM)	0 %
Cybersecurity Practitioner (CSX-P)	0 %
SSCP Security Administrator	8 %
Offensive Security Certified Professional (OSCP)	17 %
Autre	4 %

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Figure A4 :

Langages de programmation et de script les plus valorisés actuellement	% des répondants
Python	63 %
Shell	42 %
JavaScript	33 %
LINUX	33 %
Java	29 %
C++	13 %
Ruby	13 %
C	8 %
PHP	8 %
Perl	8 %
Pascal	0 %
Autre	13 %
Ne sais pas / Incertain	33 %

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Figure A5 :

Postes les plus difficiles à pourvoir	% des répondants
Intervenant en cas d'incident de cybersécurité	29 %
Analyste de l'exploitation en cybersécurité	29 %
Gestionnaire de la cybersécurité ou de la sécurité des systèmes informatiques	21 %
Testeur ou analyste d'intrusion	21 %
Spécialiste de la gestion de l'identité et de l'authentification	17 %
Architecte de la cybersécurité	17 %
Ingénieur de la cybersécurité	17 %
Spécialiste du renseignement sur les cybermenaces	17 %
Ingénieur ou développeur de logiciels sécuritaires	17 %
Ingénieur ou analyste de l'automatisation de la sécurité	13 %
Analyste de l'évaluation des vulnérabilités	13 %
Technicien d'exploitation en cybersécurité	13 %
Spécialiste de la confidentialité des données	8 %
Analyste en criminalistique numérique	8 %
Analyste de la sécurité technologique en exploitation (p. ex., systèmes de contrôle des procédés industriels, SCADA, etc.)	8 %
Spécialiste des ventes en cybersécurité	8 %
Rôles de niveau supérieur, y compris chef de la sécurité de l'information, chef de la sécurité informatique et autres	8 %
Mon entreprise n'a pas eu de difficulté à pourvoir ses postes en cybersécurité	8 %
Cryptographe/Cryptanalyste	4 %
Spécialiste des essais et de l'évaluation de la sécurité	4 %
Administrateur de la sécurité	4 %
Représentant du service à la clientèle en cybersécurité	0 %
Exploitant en sécurité des réseaux	0 %
Vérificateur de la sécurité de l'information	0 %
Autre	29 %

Remarque : Ces pourcentages sont établis en fonction des réponses de 24 personnes.

Notes de fin

1 Le rapport 2021 de KPMG indique également que « si 73 % se disent bien préparés à une cyberattaque potentielle, 59 % des entreprises interrogées s'estiment "assez confiantes" en leur capacité à détecter et à réagir à une cyberattaque ».

2 Dans l'étude de (ISC)2 (2021), ceci est défini comme le nombre de professionnels supplémentaires dont les entreprises ont besoin pour défendre adéquatement leurs actifs critiques.

3 Selon un rapport publié par Cybersecurity Ventures, le nombre de postes vacants en cybersécurité dans le monde a augmenté de 350 % de 2013 à 2021, passant de un million à 3,5 millions, et les chercheurs prévoient le même nombre de postes disponibles en 2025 (Lake, 2022).

4 Ces dirigeants en cybersécurité ou professionnels des RH étaient en contact régulier avec l'équipe de l'ACTP depuis plus de six mois au moment du sondage, et leur entreprise avait procédé à au moins une embauche dans le cadre de l'ACTP.

5 Tous les chiffres de ce rapport sont basés sur cette recherche, sauf indication contraire.

6 Quatre des vingt-trois employeurs ont accepté d'être contactés pour un entretien et nous avons parlé à deux personnes faisant partie de la même entreprise.

7 L'invitation à répondre au sondage a été envoyée par l'équipe de l'ACTP, et le sondage est resté ouvert pendant environ quatre semaines, période durant laquelle l'équipe a envoyé trois rappels.

8 La plupart des questions étaient à choix multiples et les répondants pouvaient choisir plusieurs réponses parmi les options. Par conséquent, les pourcentages présentés dans les figures contenues dans le présent rapport ne donnent pas un total de 100 %, mais représentent plutôt la proportion des répondants ayant choisi une réponse donnée.

9 Sur les 49 personnes ayant reçu le sondage, 47 % (23/49) y ont répondu entièrement et 4 % (2/49) y ont répondu partiellement.

10 Afin d'évaluer le degré de concordance entre les perceptions des employeurs et celles des candidats quant aux facteurs les plus importants pour les candidats lors de la recherche d'un emploi, Blueprint posera une question similaire aux personnes inscrites à l'ACTP. Nous en présenterons les résultats dans le rapport final qui sera publié l'an prochain.

11 Un sondage mené en 2021 auprès de gestionnaires d'embauche au Canada a révélé que 93 % d'entre eux disent accorder aux membres de l'équipe de cybersécurité de niveau débutant et subalterne du temps de développement de carrière pendant les heures de travail ((ISC)^2,2022)).

12 Les principaux partenaires en emploi de Catalyst sont des fournisseurs de services de sécurité. Il était donc probable que la majorité des répondants à ce sondage aient besoin de postes de protection et de défense. Ainsi, ces résultats pourraient ne pas refléter les besoins du secteur de la cybersécurité dans son ensemble.

13 Bien qu'elle soit loin de la forte demande observée pour la catégorie « protection et défense », la catégorie « conception et développement » est actuellement recherchée (38 %) et continuera de l'être au cours des trois à cinq prochaines années (43 %). Cette catégorie comprend des postes tels que programmeur de logiciels sécuritaires, architecte de sécurité, ingénieur de sécurité et analyste de systèmes. (TECHNATION, 2022)

14 En raison d'une erreur de programmation, l'option « Gestion des accès par identification » a été accidentellement exclue des choix de réponse à cette question.

15 Les répondants qui ont répondu « oui » à la question de savoir si les compétences techniques recherchées par leur entreprise changeront dans les trois à cinq prochaines années pouvaient indiquer dans leur réponse les compétences en question : les réponses les plus courantes étaient infonuagique (36%) et le développement, la sécurité et l'exploitation (DevSecOps) et la sécurité et l'exploitation (SecOps) (29%).

16 Bien qu'elles aient relativement moins de valeur, les compétences en communication écrite (y compris la rédaction de rapports techniques et non techniques) peuvent également aider les employeurs à distinguer les bons candidats (67 %).

17 L'équipe de Catalyst, dans ses échanges avec les employeurs du conseil consultatif sectoriel, (voir Encadré 3), avait précédemment établi que le manque de descriptions de poste précises était l'un des défis à relever dans le secteur de la cybersécurité. L'équipe de Blueprint a ajouté une question ouverte pour les employeurs : « D'après votre expérience, quels obstacles pourraient empêcher les entreprises de créer des descriptions de poste précises pour les rôles de cybersécurité de niveau débutant? »

18 Les deux personnes interrogées individuellement ont indiqué que, bien qu'il n'y ait pas de quotas spécifiques en ce qui concerne l'embauche de femmes et de PANDC spécialisées en cybersécurité, leur entreprise surveille le pourcentage de personnes appartenant à chacun de ces groupes dans leur effectif de cybersécurité. En fonction de ces pourcentages, l'entreprise établit des cibles de diversité visant à atteindre la parité au sein des équipes – comme le fait d'avoir un ratio de 50/50 entre les hommes et les femmes.

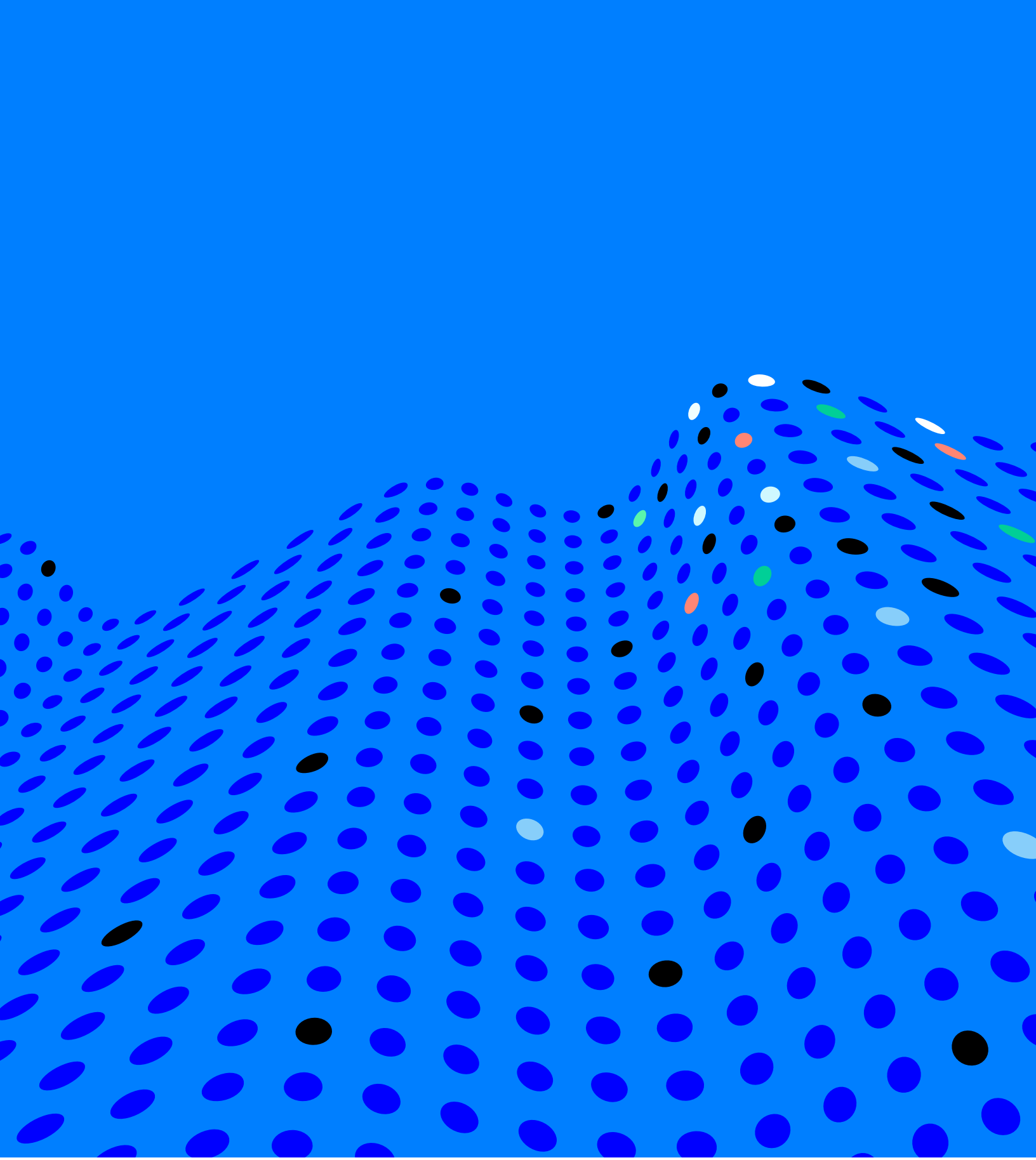
19 Environ 17 % ont répondu « Ne sais pas/Incertain » à la question « À ce jour, votre entreprise a-t-elle rencontré des difficultés dans le recrutement et l'embauche de PANDC et de femmes? »

20 Cette option comprenait les normes et réglementations relatives à la gestion du personnel, notamment le Code des droits de la personne et la législation relative à la lutte contre le harcèlement et la discrimination.

21 Nous avons utilisé une approche double simultanée pour cibler le plus large éventail possible d'employeurs. Premièrement, nous avons obtenu l'accès à une base de données créée par CyberDB (une plateforme de recherche), dans laquelle nous avons ciblé 95 entreprises qui offrent des services et consultations en cybersécurité. Plus de 50 % des employeurs que nous avons contactés étaient des petites entreprises employant de une à cinquante personnes, et 95 des personnes avec lesquelles nous avons échangé étaient des cadres de niveau supérieur, par exemple des chefs de la direction ou des présidents. Alors que l'objectif était d'obtenir une représentation plus large des employeurs au Canada, cette approche de prospection téléphonique ne nous a pas permis d'obtenir des réponses. De plus, l'équipe de l'ACTP a dressé une liste de personnes à contacter au sein de 85 entreprises avec lesquelles elle entretient divers liens professionnels (à la fois des contacts personnels et professionnels). L'équipe de l'ACTP a envoyé à ces entreprises une invitation par courriel, a publié le lien vers le sondage sur les médias sociaux (LinkedIn et Facebook) et a invité ses contacts à partager ce lien à d'autres personnes respectant les critères d'admissibilité. Dans ce rapport, nous vous présentons les conclusions préliminaires établies en fonction des réponses obtenues en date du 19 juillet 2022.

22 À l'échelle mondiale, on estime que 3,5 millions d'emplois en cybersécurité étaient à pourvoir en 2021. Aux États-Unis, il y a 50 % de candidats en moins par rapport aux besoins dans le secteur de la cybersécurité (PwC, 2022).

23 Par exemple, pour aider à pourvoir certains rôles très demandés, Deloitte Cyber a mis au point un programme de formation à l'embauche qui forme les candidats dans des disciplines liées à la cybersécurité pour occuper des postes pour lesquels ils ne seraient pas traditionnellement qualifiés (Lake, 2022).



Centre des
Compétences futures

Blueprint