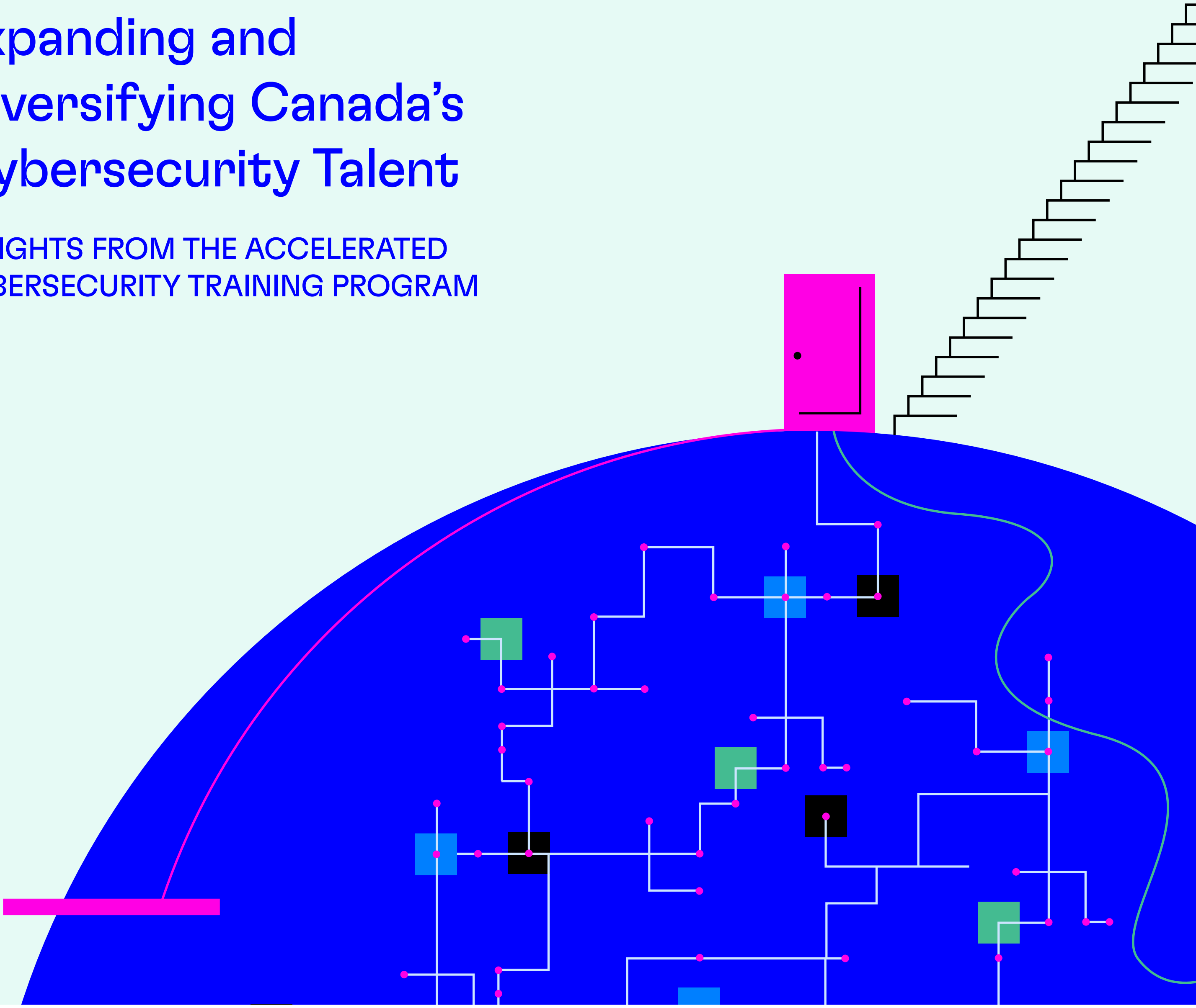
Future Talent

Expanding and Diversifying Canada's Cybersecurity Talent

INSIGHTS FROM THE ACCELERATED CYBERSECURITY TRAINING PROGRAM



Future Skills Centre | Blueprint

Partners

ROGERS cybersecure catalyst

Headquartered in Brampton, Ontario, and offering programs and services across Canada, the Rogers Cybersecure Catalyst empowers individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity. Together with our partners and collaborators, we work to realize a vision of healthy democracies and thriving societies, powered by safe and secure digital technologies. Through our groundbreaking training and certification programs; unique commercial accelerator for cybersecurity start-ups and scale-ups; first-of-its-kind cyber range; wide-ranging public education programs; and influential policy development platform, the Catalyst helps drive Canada's global competitiveness in cybersecurity.

Accelerated Cybersecurity Training Program

The Accelerated Cybersecurity Training Program (ACTP) is a seven-month skills training program designed to give women, new Canadians and displaced workers the skills they need to launch a career in the cybersecurity sector. Delivered in collaboration with the SANS Institute, learners earn three certifications from Global Information Assurance Certification (GIAC): Foundational Cybersecurity Technologies (GFACT), Security Essentials Certification (GSEC), and Certified Incident Handler (GCIH). The program is cohort-based, primarily self-study with regular study groups, mentor calls, alumni contact, labs and bootcamps. Alumni receive ongoing career preparation, employment support, and referrals to employment opportunities from the Catalyst.

Blueprint

Blueprint was founded on the simple idea that evidence is a powerful tool for change. We work with policymakers and practitioners to create and use evidence to solve complex policy and program challenges. Our vision is a social policy ecosystem where evidence is used to improve lives, build better systems and policies and drive social change.

Our team brings together a multidisciplinary group of professionals with diverse capabilities in policy research, data analysis, design, evaluation, implementation and knowledge mobilization.

At the Future Skills Centre, Blueprint works with partners and stakeholders to collaboratively generate and use evidence to help solve pressing future skills challenges.

Future Skills Centre

The Future Skills Centre (FSC) is a forward-thinking centre for research and collaboration dedicated to preparing Canadians for employment success. We believe Canadians should feel confident about the skills they have to succeed in a changing workforce.

As a pan-Canadian community, we are collaborating to rigorously identify, test, measure and share innovative approaches to assessing and developing the skills Canadians need to thrive in the days and years ahead.

The Future Skills Centre was founded by a consortium whose members are Toronto Metropolitan University (TMU), Blueprint and the Conference Board of Canada, and is funded by the Government of Canada's Future Skills Program.

Contents

The Accelerated Cybersecurity Training Program (ACTP), launched by Rogers Cybersecure Catalyst (the Catalyst), aims to connect entry-level cybersecurity candidates with the industry by providing skills training and certifications that create an accessible pathway into the industry.

Key Takeaways

Demand for cybersecurity talent in Canada continues to increase, yet there is an acute shortage of trained cybersecurity professionals. The Accelerated Cybersecurity Training Program (ACTP), launched by Rogers Cybersecure Catalyst (the Catalyst), aims to connect individuals who may not typically seek a career in cybersecurity with the industry by providing skills training and certifications that create an accessible pathway into the industry.

A dual client model, the program works with both Canadian cybersecurity employers to understand their needs and influence hiring practices, and with learners to expand the candidate pool to traditionally excluded groups. The program focuses on recruiting learners that are Black, Indigenous and/or people of colour (BIPOC), women and newcomers, and supports learners' development and job search.

Blueprint partnered with the Catalyst to evaluate the program. Our research, which included surveys and interviews with 413 learners and almost 100 employers, showed ACTP has the potential to benefit both learners and the sector as a whole by expanding the candidate pool and fostering diversity across the sector.

Insights into the Canadian Cybersecurity Industry

- Employers we heard from reported demand for entry-level cybersecurity professionals could double in the next 3–5 years.
- The employers we surveyed said they mostly hire through referrals.
- Sixty-eight percent of employer survey respondents have programs in place to recruit diverse candidates for cybersecurity roles.
- However, learners told us that searching for cybersecurity jobs can be discouraging, and reported facing inflexible job postings, disappointing salary offers and not hearing back when applying for roles.

Demand for entry-level cybersecurity professionals could double in the next 3–5 years...

and recruitment and hiring in cybersecurity often occurs through employee referrals.

89% of ACTP graduates* were satisfied with the program

*graduates who responded to survey

91% of survey respondents believed they had acquired the skills and/or knowledge to be successful in a cybersecurity career

Employers who engaged with ACTP often became more aware of diversity, equity and inclausion (DEI) in their workplace.

ACTP Influence

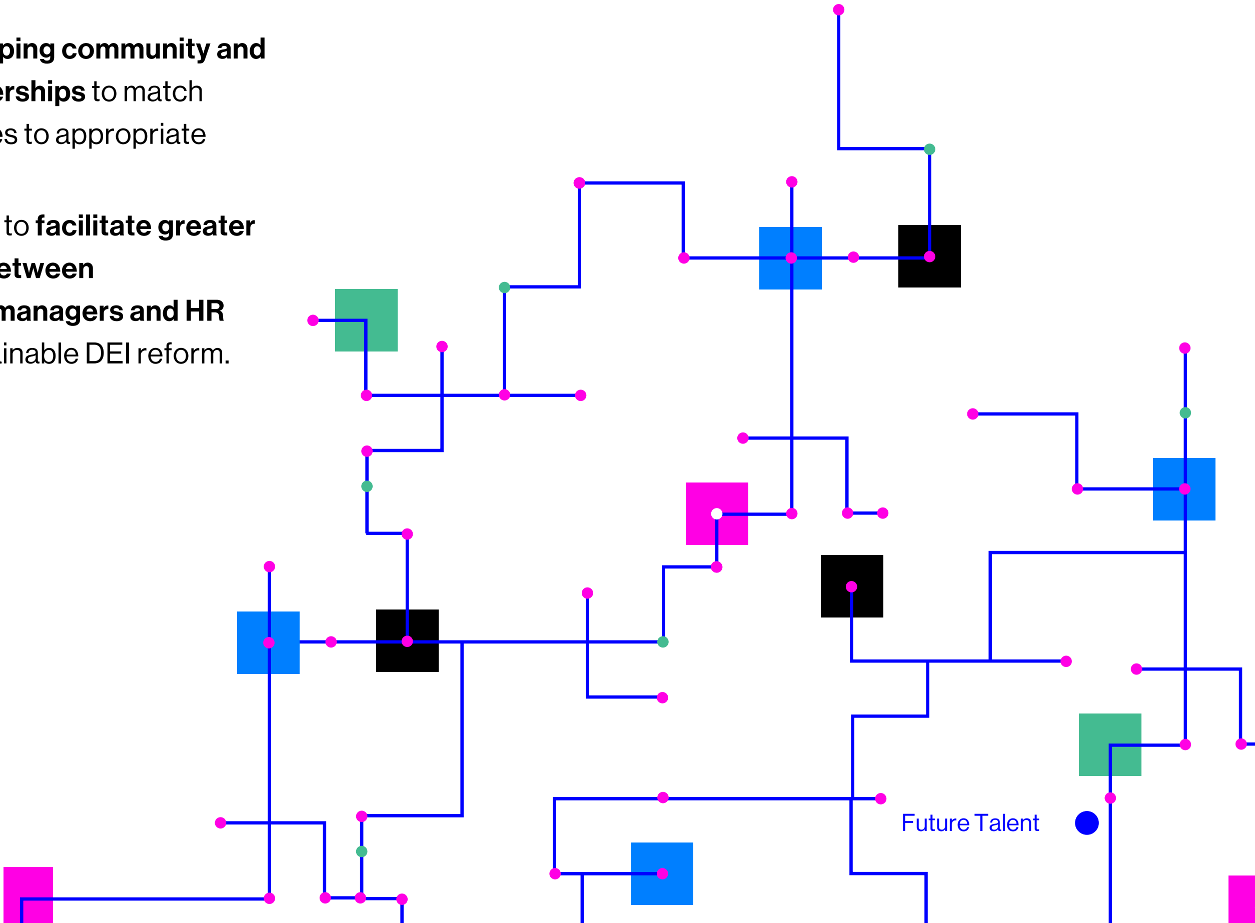
- Eighty-nine percent of ACTP graduates that responded to surveys were **satisfied with the program**, and 97% had recommended or would recommend the program.
- ACTP graduates were **skilled, confident and ready to work** in entry-level cybersecurity roles:
  - Ninety-one percent of survey respondents believed they had acquired the skills and/or knowledge to be successful in a cybersecurity career.
  - Many interviewees felt ACTP provided them with the foundation needed to break into the sector.
- Learners experienced **positive outcomes overall**,[1] including employment and salary increases:
  - Overall employment (in any industry) increased from 61% (program start) to 79% (three months after completing the program).
  - Percentage of learners' work involving technical cybersecurity tasks increased, from 7% (2/30) of employed respondents at program start reporting that more than half their work was in cybersecurity, to 42% (11/26) reporting three months after the program.
  - There were early indications of salary increases: Among two cohorts analyzed, the percentage of respondents earning an annual salary of at least $60,000 grew from 29% (25/85) at program start to 49% (29/59) at program completion and 76% (37/49) three months after completing the program.
- Employers who engaged with ACTP often **became more aware of diversity, equity and inclusion (DEI)** in their workplace. Many took action, from offering training to staff to tracking applicants' sociodemographic characteristics.

[1] Outcomes analysis based on 2 cohorts for which data was available at the time of this report, out of 5 total participant cohorts. More information about sample sizes across different data included in the report can be found on p. 7.

Key Recommendations

Based on our research and the ideas we heard from learners and employers, ACTP shows promising employment results for diverse candidates breaking into the cybersecurity sector. We recommend that to amplify ACTP's influence going forward, the Catalyst could consider:

- **Exploring the value of offering the CompTIA Security+ certification**, in addition to the GIAC Security Essentials Certification (GSEC) and the GIAC Certified Incident Handler (GCIH) that it already offers, to better align with what we heard was most valuable to employers.
- **Fine-tuning the target population of ACTP**, and any other applicable services/programs the Catalyst offers, to differentiate which are best suited for folks early vs. later in their career.
- **Further developing community and industry partnerships** to match more candidates to appropriate roles.
- Exploring ways to **facilitate greater coordination between cybersecurity managers and HR teams** for sustainable DEI reform.



Introduction

Cybersecurity skills are becoming increasingly important and in-demand in Canada. But this demand far outstrips supply: there is already an acute shortage of trained cybersecurity professionals (Posadzki 2019). As of 2021 there was an estimated 25,000-person gap between roles and qualified workers in Canada. ((ISC)2, 2021).

To bridge this gap and make the cybersecurity sector more accessible to Canadians from diverse backgrounds, the Rogers Cybersecure Catalyst (the Catalyst)—Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity—launched the Accelerated Cybersecurity Training Program (ACTP) in 2020.

Cybersecurity skills are becoming more and more important and in demand in Canada. But this demand far outstrips supply: there is already an acute shortage of trained cyber security professionals.

In developing and delivering ACTP, the Catalyst took a dual-client approach, working with both Canadian cybersecurity employers to understand their needs and influence hiring practices, and with learners to expand the candidate pool to traditionally excluded groups.

As of 2021 there was an estimated 25,000 person gap between roles and qualified workers in Canada.

In October 2021, the Catalyst received funding from the Future Skills Centre (FSC) to launch the Cyber Talent Transformation Initiative to expand the reach of ACTP to individuals who identify as Black, Indigenous and/or people of color (BIPOC) by reserving 60 seats for BIPOC learners, of which at least 30 are reserved for women. In this phase, Blueprint conducted in-depth research with program participants and across the cybersecurity sector. We published an interim report in 2022 highlighting hiring practices and needs of the Catalyst's employment partners. Building on that effort, this report presents insights from a broader set of Canadian cybersecurity employers along with in-depth research with program participants. We offer these insights to the Catalyst as they plan their ongoing work to meet Canada's cybersecurity skills demand while creating pathways for BIPOC workers, women and newcomers to break into the cybersecurity industry.

Research Approach

Our research focused on:

- Challenges Canadian cybersecurity employers face in recruiting and hiring diverse candidates.
- ACTP learners' experiences of finding work in cybersecurity.
- Employers' experiences of hiring through ACTP.
- Considerations the Catalyst could use in their work to help meet Canada's cybersecurity skills demand and support diversity in the field.

Employer Research

Our employer research focused on the hiring and recruitment needs and challenges of Canadian cybersecurity employers,[2] and how ACTP can meet employers' demand for talent with the necessary skills.

Employer Surveys

We sent surveys to 201 cybersecurity professionals. Ninety-four replied, all mid- to senior- professionals, from across 65 different organizations. Some of the people we surveyed (25) were from organizations that were familiar with ACTP, while others (69) had less awareness of the program.

Employer Interviews

We interviewed two cybersecurity professionals with hiring and management responsibilities, both of whom have pre-existing relationships with the Catalyst. Data from these two interviews were not used to draw representative conclusions about employers overall, but rather to add richness to findings with larger sample sizes.

Industry Advisory Council Surveys

The Industry Advisory Council (IAC) is composed of eight employer partners who provide strategic guidance, advice and support on ACTP. In March 2023, we sent a survey asking them to reflect on their engagement with ACTP, and five responded. We followed up with a brief facilitated discussion/focus group with all eight IAC members.

[2] "Cybersecurity employers" refer to any organization that employs cybersecurity professionals, including those that offer cybersecurity services.

Learner Research

Our learner research aimed to understand program experience and outcomes of people who participated in ACTP, with a focus on the experiences of BIPOC and women.

Learner Surveys

ACTP is delivered in cohorts, meaning not all participants take the program at the same time. This report includes survey data on ACTP learners in cohorts six through ten, collected between October 2021–March 2023.

Four hundred and thirteen people completed surveys and were asked to complete them at different times: baseline (program start), exit (program end) and three months post-program.

Three month follow-up survey data is only available for cohorts six and seven at the time of this report, meaning the information from follow-up surveys should be interpreted with caution: it may suggest trends but can't ground clear conclusions. We are also conducting six- and nine-month follow-up surveys, which are not included in this report, but will be included in an addendum once that data is available.

TABLE 1

Learner Survey Sample

Survey Touchpoint	Who was invited to participate as of March 28, 2023		Responses	Response Rate
Program start (baseline)	5 cohorts	614 learners	413	68% (413/608)
Program completion (exit)	3 cohorts	161 learners	127	78% (126/161)
3-month follow up	2 cohorts	76 learners	61	80% (61/76)
6-month follow up	1 cohort	43 learners	23	53% (23/43)

Learner Interviews

We interviewed 30 learners across cohorts six through eight of ACTP, chosen to generally represent the sociodemographic makeup of their cohorts. We spoke with them at three points in time:

Start of the program

These interviews focused on motivations for joining ACTP and early program experience. (n=30)

End of the program

Here we focused on program reflections and career goals. (n=22)

Three-month follow-up

These interviews checked-in on employment and/or job searching. (n=14)

Key Learnings

Canadian Cybersecurity Talent Needs

Employers that we surveyed reported an acute need for skilled, entry-level cybersecurity candidates. This aligns with the trends identified in previous research on the sector (Lake, 2022). At the same time, some graduates felt they were in competition for scarce roles.

Employers said they often recruit and hire talent via employee referrals, so the candidate pool is only as large and diverse as their existing network.

Employers and learners agreed that a key challenge in matching talent to roles is the lack of flexibility in the minimum requirements of job posting.

While many of the employers have programs in place to support diversity in hiring, some still struggle to recruit diverse candidates and learners suggested that more formal programs (such as mentorship programs) could support the recruitment, satisfaction and advancement of BIPOC, women and/or newcomers in their workforce.

Employers anticipate continued demand for trained cybersecurity professionals.

The average number of cybersecurity professionals needed in the next 12–18 months among the employers we surveyed was 27, and they shared in interviews that this demand could double in the next 3–5 years.

FIGURE A

Number of cybersecurity professionals needed by organization size

Organization size	Number of cybersecurity professionals needed				
	<10	**10-24**	**25-49**	**50-74**	**+100**
Small (1 - 99 employees, N=19)	74% (14/19)	21% (4/19)	5% (1/19)	0% (0/19)	0% (0/19)
Medium (100 - 499 employees, N = 5)	20% (1/5)	20% (1/5)	40% (2/5)	0% (0/5)	20% (1/5)
Large (+500 employees, N=37)	38% (14/37)	22% (8/37)	11% (4/37)	16% (6/37)	8% (3/37)

Percentage of employer respondents

0% 100%

For entry-level cybersecurity roles, employers valued the technical skills of intrusion detection and response techniques, vulnerability assessment, and application of cloud security technologies and methodologies. They looked for non-technical skills of problem-solving and critical thinking, verbal communication, attention to detail, and written communication. When it comes to certifications, they most valued CompTIA Security+, GSEC, and GCIH (see Tables 2-4).

TABLE 2

Top five technical skills valued by employers for entry-level cybersecurity roles

Technical skills	Employer respondents
Intrusion detection and response techniques	41% (31/76)
Vulnerability assessment	34% (26/76)
Application of cloud security technologies and methodologies	33% (25/76)
Troubleshooting	29% (22/76)
Identity and authentication management	28% (21/76)

TABLE 3

Top five non-technical skills valued by employers for entry-level cybersecurity roles

Non-technical skills	Employer respondents
Problem-solving and critical thinking	79% (59/75)
Verbal communication	75% (56/75)
Attention to detail	63% (47/75)
Written communication	63% (47/75)
Teamwork and leadership	61% (46/75)

TABLE 4

Top five certifications employers reported valuing for entry-level cybersecurity roles

Certifications	Employer respondents
CompTIA Security+	49% (36/74)
GIAC Security Essentials Certification (GSEC)	45% (33/74)
GIAC Certified Incident Handler (GCIH)	32% (24/74)
CompTIA Cybersecurity Analyst+ (CSA+)	31% (23/74)
GIAC Certified Intrusion Analyst (GCIA)	23% (17/74)

Employers and learners see the demand for cybersecurity professionals differently.

Employers who shared via survey, interviews and focus groups agreed that a key hiring challenge was a shortage of qualified candidates. Some learners' perceptions were different: in interviews, some suspected there might not be a shortage of entry-level cybersecurity candidates, and instead a saturation of entry-level-qualified candidates for few roles, citing competition for roles and recent layoffs or hiring freezes at large tech companies.

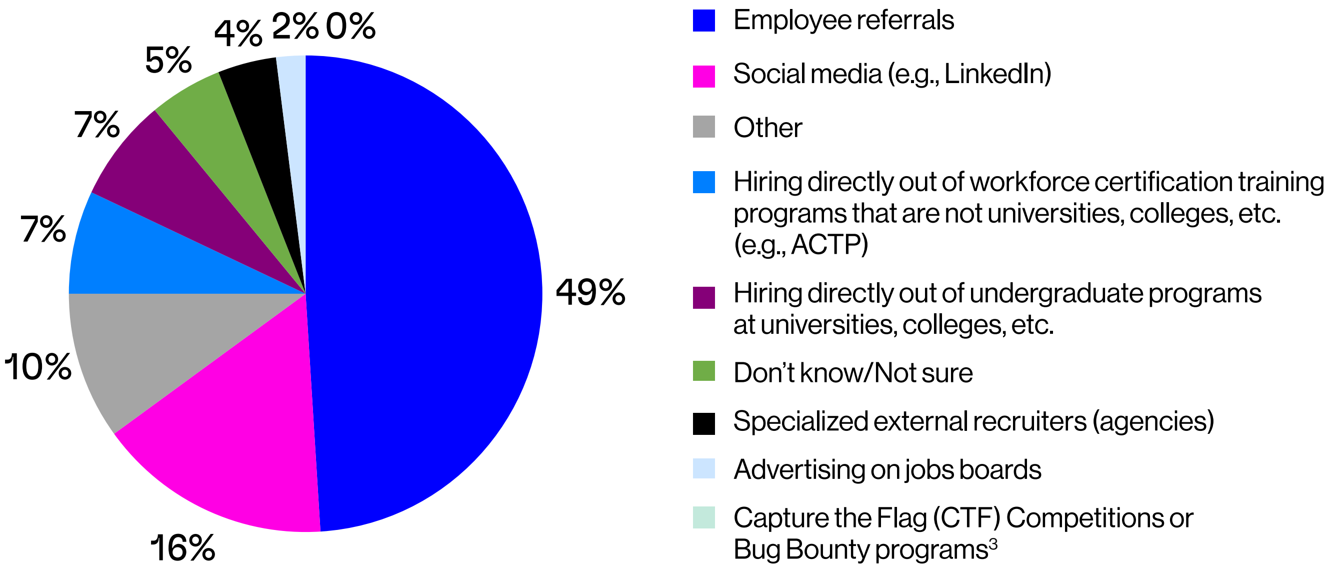
> *"You hear about shortages for those roles in cybersecurity, and if there's shortages they should be looking to hire but I'm not seeing that in the job search."*
>
> *– LEARNER*

Employers most often hire through referrals.

From survey responses, we heard that employers perceived employee referrals to be the most effective recruitment method (49% - see Figure B). In interviews, employers shared that they prefer employee referrals because they can help source candidates that are vetted by people with a deep understanding of the nature of the role and the company. However, recruiting via referrals can mean looking for candidates only within existing networks that reflect the current makeup of the industry, which may not promote diversity. Recruitment methods that cast a wider net, like job boards, were not considered as effective.

FIGURE B

Employer rankings of recruitment methods



[3] A bug bounty program is a deal offered by many organizations and software developers where individuals can receive recognition and compensation for reporting "bugs" pertaining to security exploits and vulnerabilities.

Strict criteria in job postings can make matching candidates to roles challenging.

Learners shared in interviews that a key challenge in getting hired was inflexible job requirements with high expectations. Some employers also noted that the skills and knowledge expectations of entry-level roles did not reflect entry-level work. Employers and learners suggested that while HR professionals are responsible for drafting and/or matching candidates to postings, they may not always have the full set of information needed to flexibly assess job requirements that both meet role needs and align with the entry-level skillsets available in the market.

Some employers struggle to recruit diverse candidates into roles.

Cybersecurity employers were fairly split on whether they had challenges recruiting workers that are BIPOC and/or women: in surveys, 43% of employers reported having challenges, and 42% reported not having those challenges (an additional 15% responded "I don't know/not sure). One employer shared that because their organization's HR department does not track candidates' sociodemographic characteristics, it was difficult for them to engage in targeted recruitment of underrepresented groups. Another employer said that while their organization actively looks to recruit BIPOC and/or women professionals, they face challenges finding sufficient candidates who are BIPOC or women in their usual candidate pool, which is largely comprised of people in the traditional university and college system.

● **KEY POINT**

Cybersecurity employers were fairly split on whether they had challenges recruiting workers that are BIPOC and/or women: In surveys, 43% of employers reported having challenges, and 42% reported not having those challenges.

Some employers had DEI programs in place and additional formal programs may further support workers.

Most employer survey respondents reported having programs in place within their organization to recruit diverse candidates for cybersecurity roles (68% - see Figure C).

FIGURE C

Employers' diversity, equity and inclusion programs

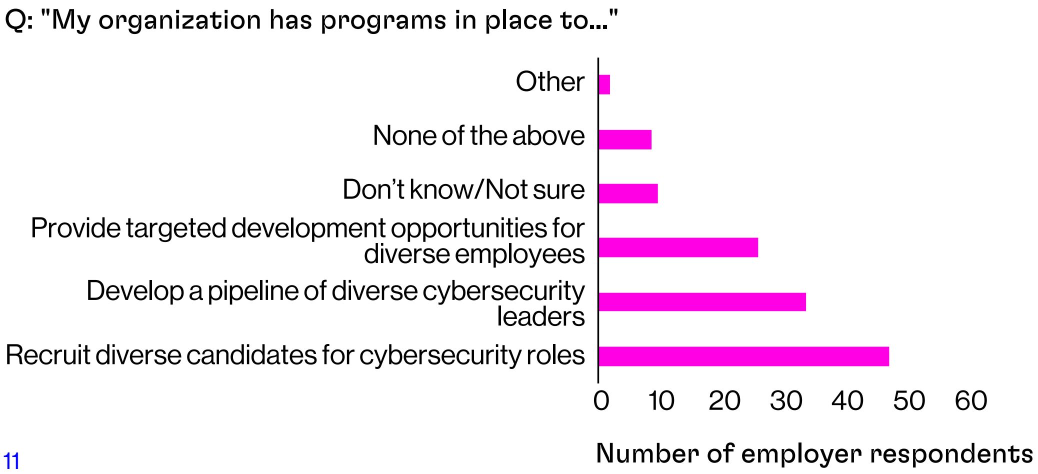
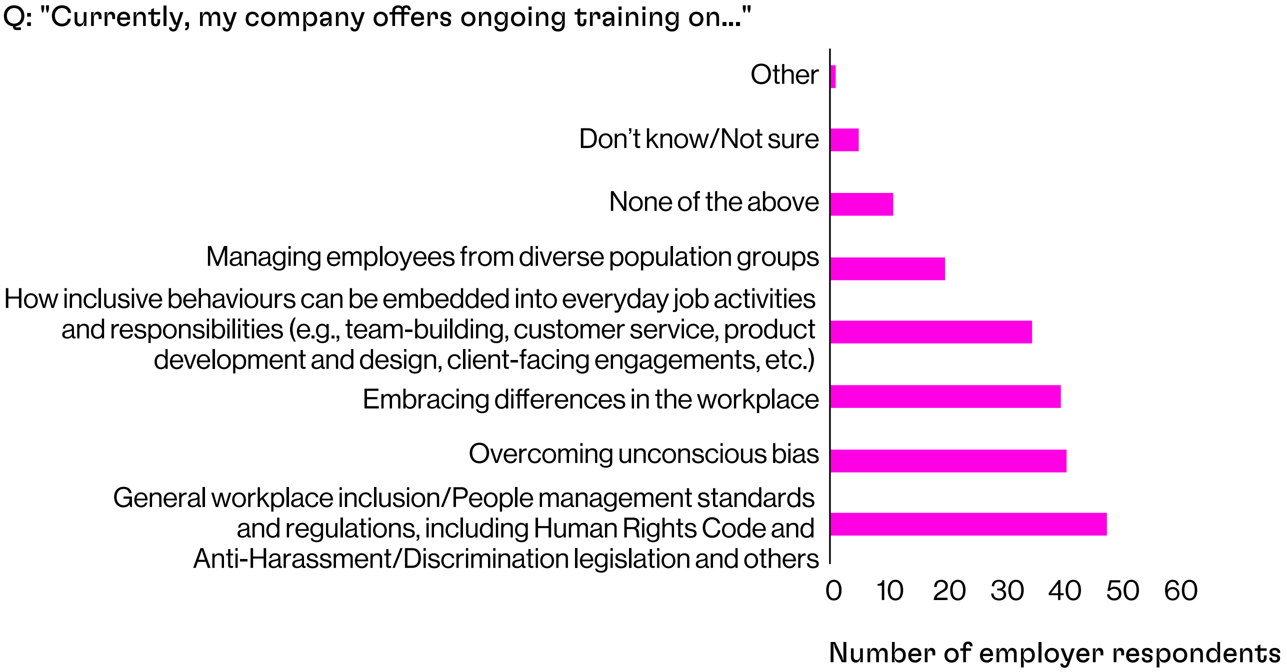


FIGURE D

Employers' diversity, equity and inclusion training offerings



Learners shared examples of workplace DEI initiatives they've experienced that feel supportive, including some that reflect programs employers reported having in place:

- mentor programs for women and/or BIPOC (49% of employers reported having programs in place to develop a pipeline of diverse cybersecurity leaders)
- ongoing learning and development opportunities (38% of employers reported having programs in place to provide targeted development opportunities for diverse employees)

● **KEY POINT**

49% of employers reported **having programs in place** to develop a pipeline of **diverse cybersecurity leaders**

Some examples of workplace DEI initiatives that learners reported finding supportive were not commonly reflected in employer programming, including:

- clubs/committees for employees with a shared background/identity
- acknowledging/celebrating achievements of women and BIPOC employees during Black History Month and International Women's Day

Employers may consider offering additional formal programs, as this could promote employees feeling more supported in the workplace.

Employer and Learner Experience with ACTP

Because the goal of ACTP is to expand and diversify the cybersecurity sector, we looked for indications of whether graduates developed cybersecurity skills, got new jobs, gained cybersecurity work specifically and/or saw changes to their salary. Early indications point to an increase in skills, confidence, employment and salaries. We also saw that after connecting with the Catalyst/ACTP, employers recruited and supported diverse hires. However, some graduates still indicated that the cybersecurity sector was challenging to enter, and graduates later in their career also felt that the opportunities were misaligned with their expectations.

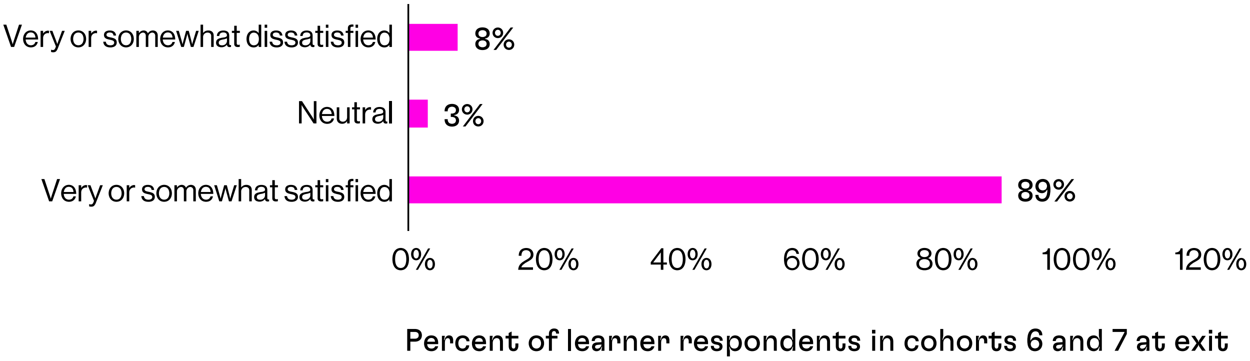
● **KEY POINT**

Early indications point to an **increase in learners' skills, confidence, employment and salaries**

ACTP learners built confidence in their cybersecurity skills and many felt that ACTP provided the foundation needed to break into the sector.

FIGURE E

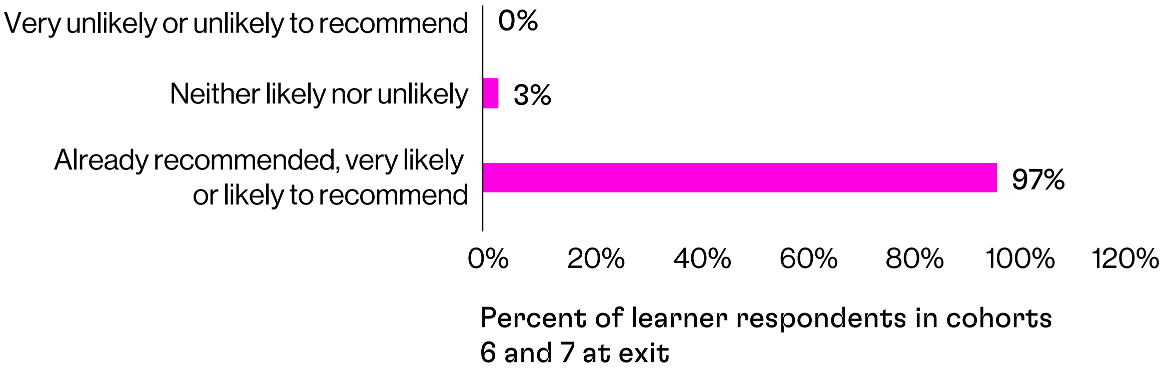
Learners are satisfied with the program overall



Overall, learners were very satisfied with the program: when we surveyed cohorts six and seven at the end of the program, 89% were very or somewhat satisfied with the program, and 97% had recommended or were likely/very likely to recommend the program (see Figure E).

FIGURE F

Learners would recommend the program

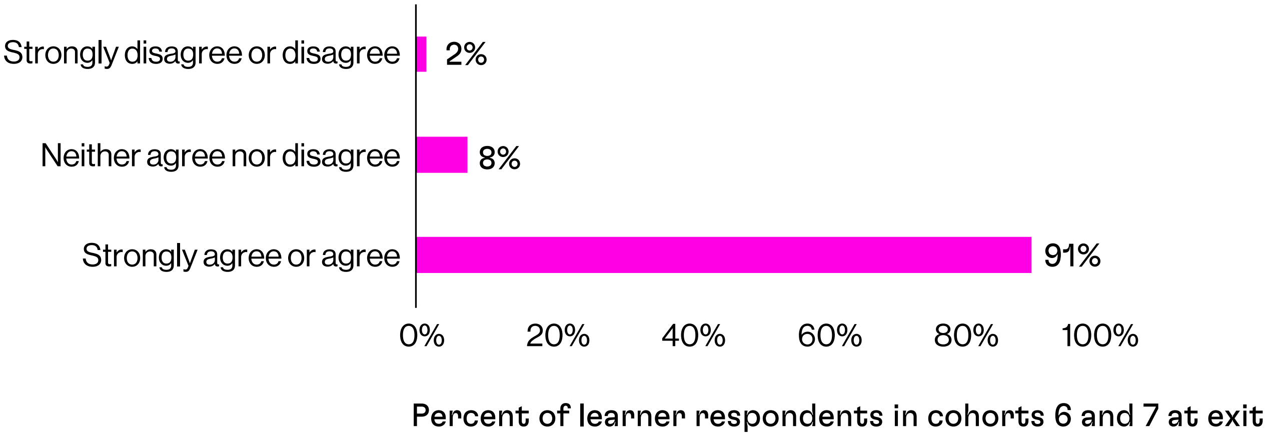


Upon completing ACTP, 91% of survey respondents believed they had acquired the skills and/or knowledge to be successful in a cybersecurity career, and many described in interviews that ACTP provided them with the foundation needed to break into the sector (see Figure G). Those who didn't feel as confident often attributed this to personal traits or habits rather than lack of preparation.

FIGURE G

Learners feel they have the skills and/or knowledge to be successful in a career in cybersecurity

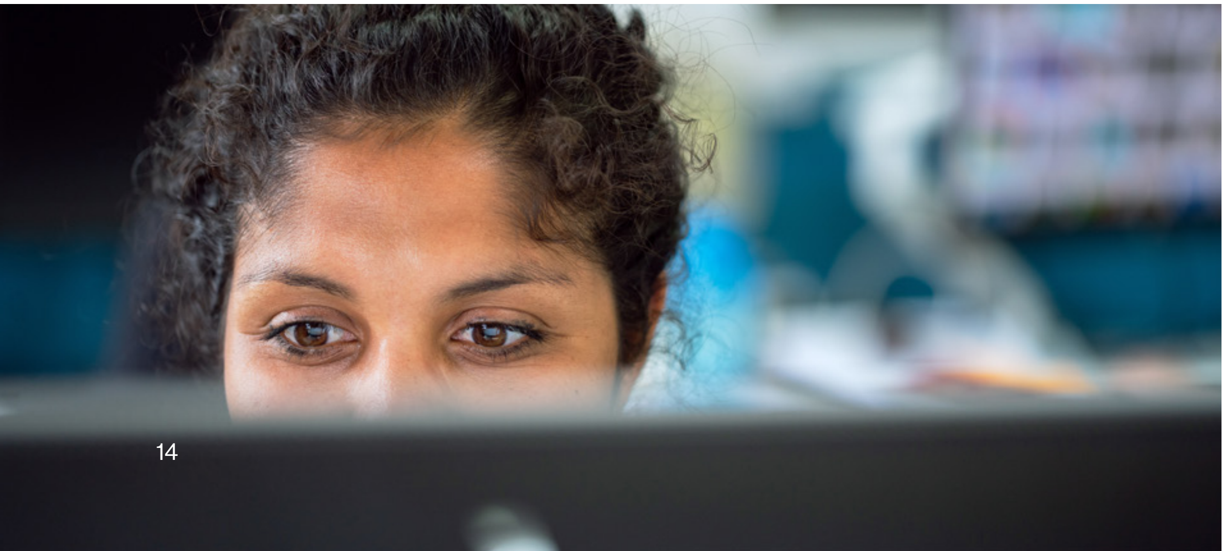
Q: "I have the skills and/or knowledge to be successful in a carrer in cybersecurity"



Learners credited specific components of the program in helping them get their cybersecurity role, particularly:

- the reputation of SANS certifications
- employer sessions (connecting learners and employers directly)
- the Catalyst sharing job postings

Still, some graduates were concerned that the SANS certifications they earned would not be enough to get hired in cybersecurity. They felt that they may need additional training/certifications to secure a cybersecurity job, whether to specialize, practice/solidify skills or develop a portfolio.



Both overall and cybersecurity-specific employment increased among graduates, along with higher salaries.

When considering employment outcomes of participants, ACTP aims to diversify the cybersecurity sector via two routes: previously unemployed learners finding new employment in the sector, and previously employed learners transitioning to better jobs within the sector. To measure these potential outcomes, we considered four indicators:

- The overall proportion of learners employed.
- Whether learners secured a new job (even if they were previously employed), and whether they received a raise or promotion.
- The proportion of learners whose work involves technical cybersecurity tasks, and how much of their work involves these tasks.
- The total income of learners.

These indicators helped us understand whether:

- the net employment of ACTP learners increased
- learners transitioned into roles that utilize cybersecurity skills
- learners are better compensated.

● **KEY POINT**

Early indications point to increases in:

- overall employment (in any industry)
- the amount of learners' work that involves technical cybersecurity tasks
- salaries

Considering the results for the first of these indicators, overall employment (in any industry) increased, from 61% (60/99) at program start to 79% (48/61) three months after the program (see Figure H).

Among cohort seven graduates, 41% (14/34) had new jobs three months after the program.

FIGURE H

Employment (in any industry) increased among learners (cohort six and seven)

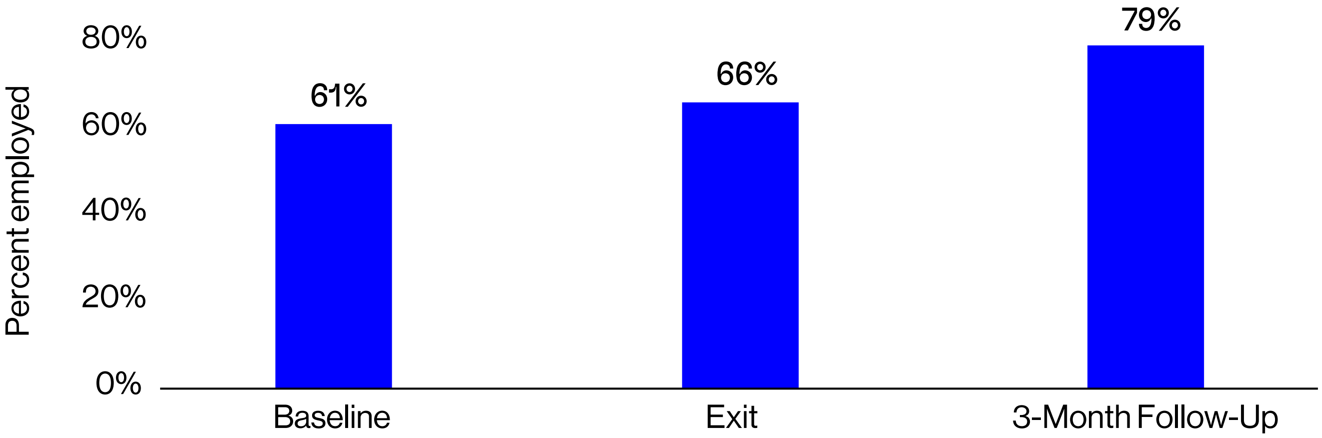
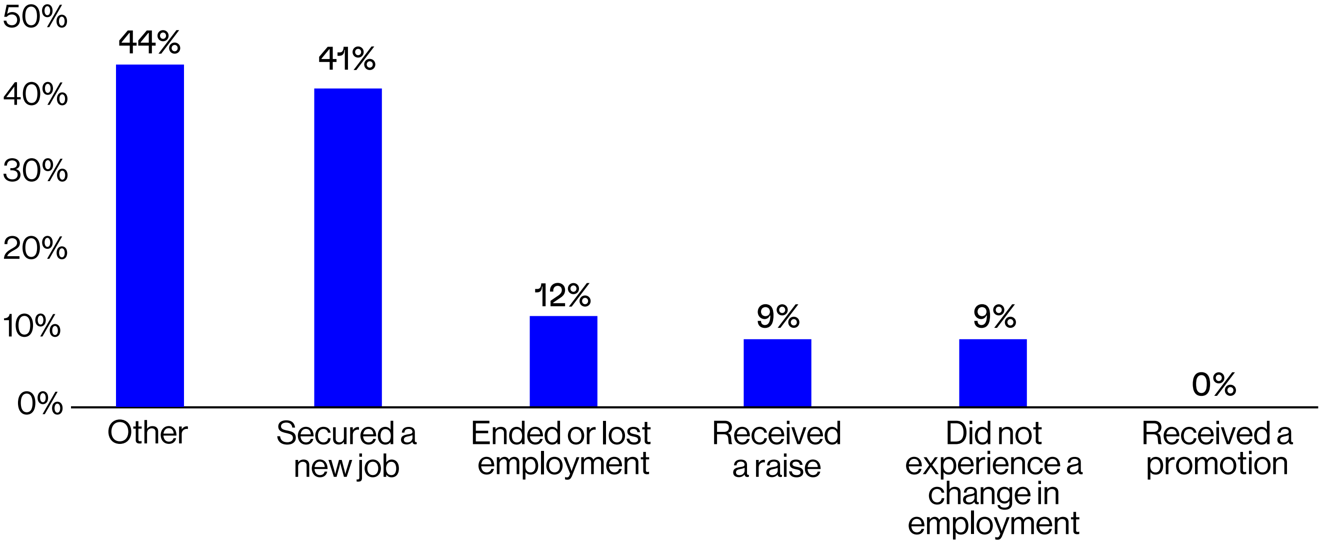


FIGURE I

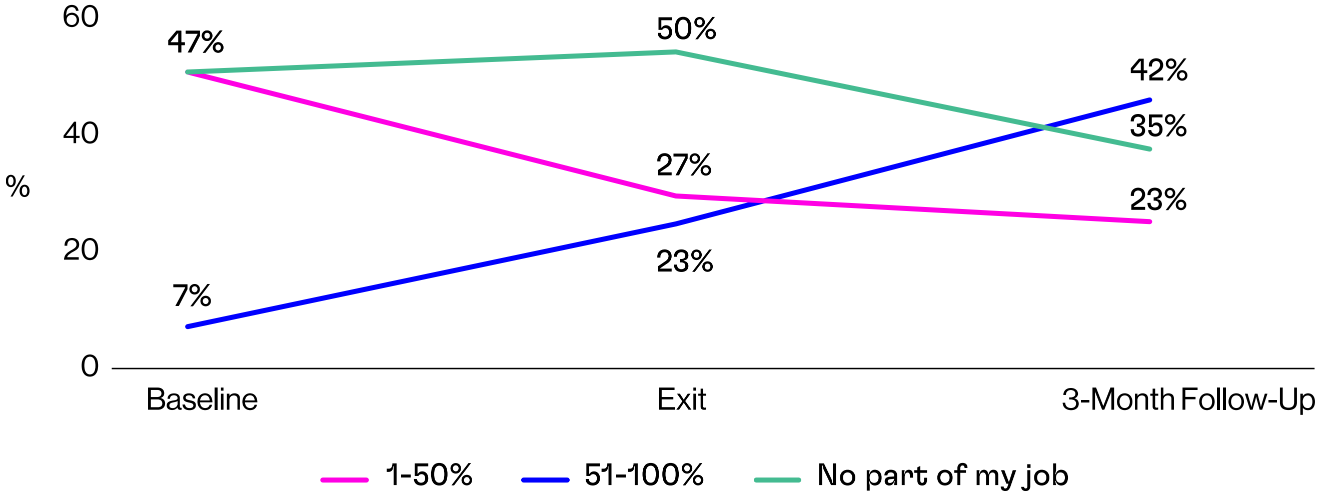
Employment status among ACTP leaners (cohort seven)



We also see early indications that the amount of learners' work that involves technical cybersecurity tasks increased (Figure J).. At the beginning of the program, 7% (2/30) of employed respondents in cohort seven reported that more than half their work was in cybersecurity, and three months after the program, 42% (11/26) of employed respondents reported more than half their work was in cybersecurity. Cohort six respondents were not asked this question, and it will be important to see if this trend continues with cohorts eight through ten.

FIGURE J

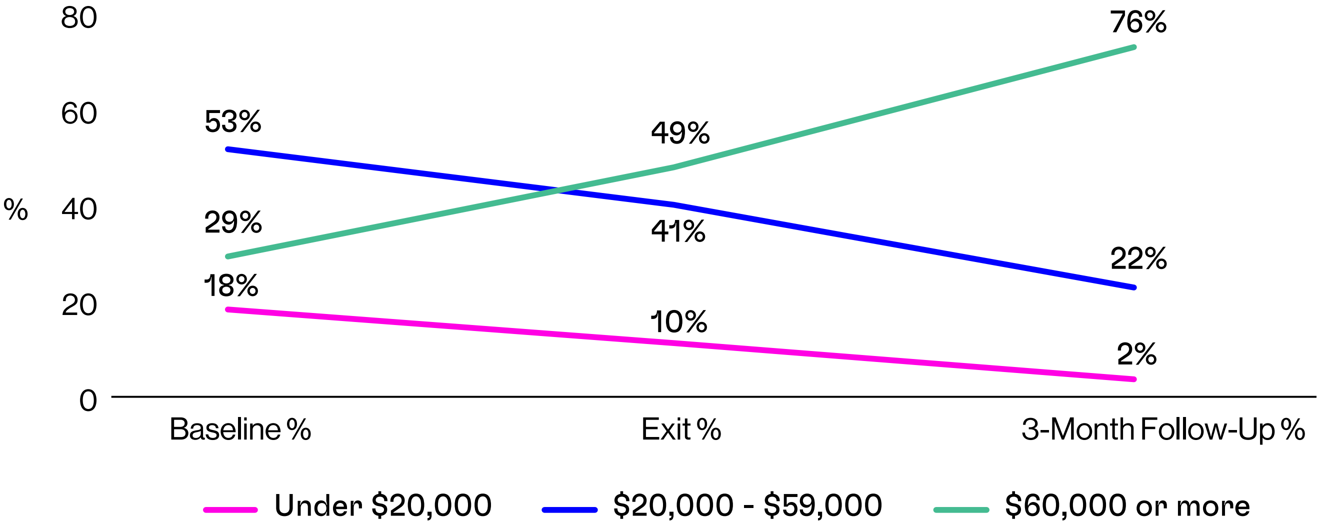
The amount of learners' work that involves technical cybersecurity tasks increased over time (cohort seven)



We also see early indications of salary increases among graduates in cohorts six and seven: the percentage of respondents earning an annual salary of at least $60,000 grew from 29% (25/85) at program start to 49% (29/59) at program completion and 76% (37/49) three months after completing the program (see Figure K).

FIGURE K

Annual salary of learners increased over time (cohort six and seven)



Some employers changed their hiring practices because of ACTP.

We asked employers in the IAC in both a survey and focus group whether their hiring or recruitment practices had changed after engaging with ACTP/the Catalyst. They said that the Catalyst:

- Helped them to “think outside the box” in terms of the skills and experience they look for in cyber professionals by providing candidates from different backgrounds, ages and industries who may possess different skill sets and experience than traditional candidates.
- Inspired them to raise awareness of diversity in the workplace and deliver more DEI training to employees after increasing diversity in the workplace by hiring ACTP graduates.
- Highlighted for them the value of their HR departments tracking applicants’ sociodemographic metrics to improve awareness about how their hiring processes reflect diversity in their organizations.

● **KEY POINT:**

Employers in the IAC said **the Catalyst helped them to “think outside the box” in terms of the skills and experience they look for in cyber professionals** by providing candidates from different backgrounds, ages and industries who may possess different skill sets and experience than traditional candidates.

Some IAC members explained that hiring non-traditional candidates has brought additional diversity to their teams and a “good dynamic to the [work] environment.”

The Canadian cybersecurity job market can be discouraging to candidates.

Many graduates we interviewed were feeling excited when they first entered the cybersecurity job market, but some grew increasingly disappointed when they didn't hear back after applying to jobs or weren't contacted after interviewing. Shortly after completing ACTP, while graduates felt prepared for cybersecurity careers, fewer reported feeling prepared for the hiring process. Similarly, upon completing ACTP, 91% of survey respondents believed they had the skills and/or knowledge to be successful in a career in cybersecurity, but only 70% felt confident in applying for a job in cybersecurity. Some said that they know they are ready to work in the sector, but that convincing a recruiter or interviewer could be an obstacle to securing a job.

"Unfortunately the starting salary and just everything was not currently what I'm being paid."

– LEARNER

Because of starting salaries, ACTP may be best suited for those early in their career.

The expectation of high salaries in the cybersecurity field was a key motivation for learners to start ACTP: interviewees told us they see cybersecurity as exciting and constantly evolving, with lots of career opportunities and high paying jobs. While salaries generally increased for learners after ACTP, many graduates shared in interviews that they were disappointed with the salaries of the cybersecurity jobs for which they were qualified or interviewed. Graduates who were earlier in their career or unemployed following ACTP were more willing to accept a salary that did not meet their original expectations to get their start in the sector. Those with more extensive career history and/or higher family expenses were more often hesitant to accept cybersecurity roles.

"I'm happy with the salary I'm earning… it was more about getting the opportunity to get into the industry than the salary."

– LEARNER

Opportunities to Further Meet the Sector's Diverse Talent Needs

We asked learners about how the Catalyst can improve their experience going through ACTP and the cybersecurity job market, and asked employers about how to best address the industry's hiring challenges, particularly around diversity. They shared suggestions for how the Catalyst can do more to help more BIPOC learners, women and newcomers break into the sector, modify the program to focus on industry need and scale up their influence on the sector, and what employers themselves can do to move the needle on DEI in their workplaces.

The Catalyst can continue to emphasize–and deepen–job search supports.

Learners were mostly satisfied with the employment supports provided in ACTP: 85% of survey respondents reported that the Catalyst provided support to help find employment in cybersecurity, of which 75% were satisfied or very satisfied with that support.

In interviews, learners shared examples of job search supports provided by ACTP that were particularly helpful in securing jobs. In addition to sharing job postings from employers, learners found insights into the employers very helpful, such as information about the workplace culture, willingness to train and intel on the flexibility of job posting requirements.

We heard from learners that it was helpful when the Catalyst gave direct encouragement to apply to specific jobs, whether based on industry insights or simply to inspire confidence among learners. We particularly heard this among women and newcomers, who asked for more of this support from the Catalyst to help overcome cultural barriers and/or obstacles with their confidence.

Many women and newcomers found the career preparation section of the program helpful for building skills and confidence for the hiring process. Particularly for those newer to applying to jobs in Canada, these sessions helped them understand how to translate their knowledge into job offers. Some mentioned that in this section of the program they were encouraged to conduct mock interviews with their peers but would have preferred mock interviews with program staff. Some interviewees also shared that support or guidance in choosing a specialty or career path within cybersecurity could help to build their confidence in their job search and understand which core skills to highlight in job applications.

"[The Catalyst] said 'ignore the 2-5 years experience in this posting'. They probably spoke to the employer and learned it's a nice-to-have, not a requirement... they help us sift through the nice-to-have, when they have a direct relationship with the employer."

– LEARNER

Graduates appreciated the guest speakers during the career preparation section. They wanted more direct opportunities to network with cybersecurity employers, including HR staff, who represent the first step in the recruitment process. Graduates wanted direct introductions and to practice explaining their competencies to HR staff.

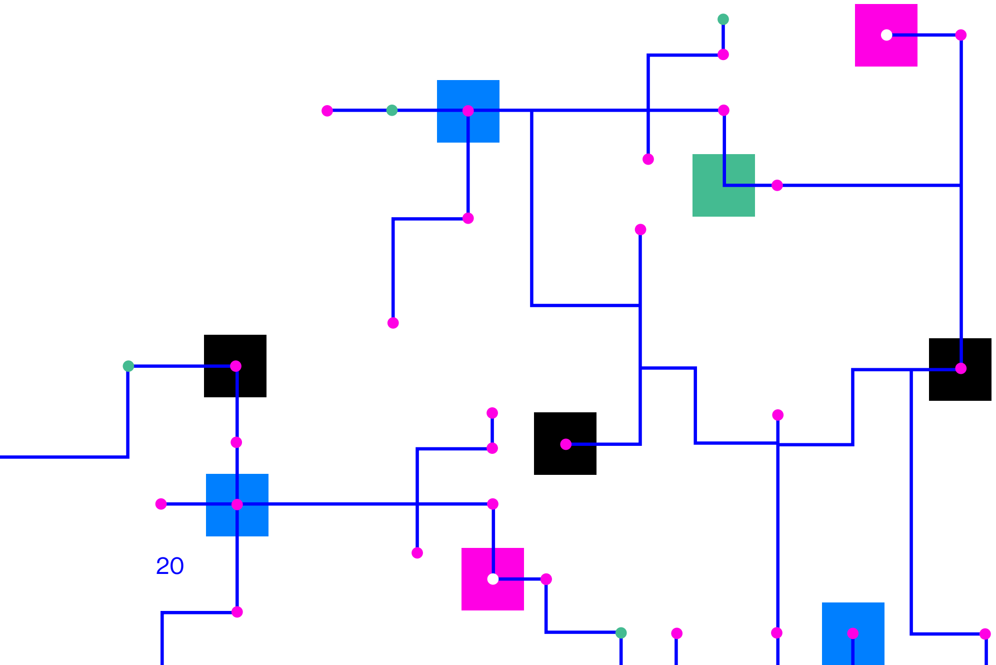
> *“Maybe someone on the HR side who can say what they’re looking for when they look at resumes... they’ll get the managers, who talk about what makes a good employee.”*
>
> *– LEARNER*

The Catalyst can further align programming with industry talent needs.

Employer and learner feedback both suggested that ACTP can further fine tune its certifications. Employers we surveyed were specifically interested in the CompTIA Security+ certification (n=36), which is not included in ACTP, as well as two certifications ACTP already includes (GSEC (n=33), and GCIH (n=24)). The Catalyst could explore whether adding certification in CompTIA Security+ (or similar) to ACTP could help graduates’ qualifications better align with industry need.

> *“If you’re getting hired by a security person they know what you’re talking about. If you’re hiring with HR then they don’t really know that kind of stuff.”*
>
> *– LEARNER*

We heard from both employers and learners that while certifications are helpful when applying to roles in cybersecurity, additional hands-on or practical experience could help learners build a portfolio of work to highlight in interviews and applications. Many learners took it upon themselves to practice or solidify what they learned in ACTP after completing the program, using sandbox environments like TryHackMe and Splunk. Employers were interested in candidates with more direct experience working with security data specifically, and some felt ACTP graduates did not know how to write about data points or tailor their reports to audiences, so training in technical writing skills could be added.



The Catalyst can grow its influence.

Learner interviewees and IAC members shared that the Catalyst should continue to help BIPOC, women and newcomer candidates reach the industry and help promote awareness of DEI in the workplace. To push DEI efforts forward, learners thought the Catalyst could offer DEI training to cybersecurity employers and staff. IAC members suggested that the Catalyst can increase the number of learners they train and work to expand their employer partner network beyond Ontario to the rest of Canada.

To increase their visibility, learners suggested in interviews that the Catalyst could attract learners through outreach with community organizations, including libraries, women's groups or newcomer settlement organizations that can share information with immigrants when they first arrive to Canada. IAC members agreed that working in partnership with other cyber skills-training organizations that target marginalized communities could be an "amazing investment" as it could create a recruitment pipeline for those who may traditionally be excluded. Specifically, IAC members noted an organization in their network that works with Indigenous communities that they'd be interested in seeing the Catalyst connect more closely with.

> *"More publicity to reach people. There are a lot of new immigrants that don't know about this program. I have met people that did not know what programs were available to them. It should be promoted at those neighborhood organizations."*
>
> *– LEARNER*

Employers can strengthen their DEI initiatives.

In our engagement with both learners and employers, we heard that while some progress has been made toward DEI, deliberate, ongoing action from employers will be required for sustainable success of BIPOC, women and newcomers in the sector. In fact, when asked what role the Catalyst could play in advancing DEI, many learner interviewees noted that employers should lead these efforts.

In surveys and focus groups, employers shared some ideas about ways the industry can further promote and support DEI in the sector. They suggested that employers can:

- **Increase awareness and visibility** (n=16): Outreach, speaking on panels, showcasing successful cybersecurity professionals from diverse backgrounds and reaching people at a young age can all help demystify cybersecurity and show that "anybody can be anything."
- **Strengthen partnerships with network**s (n=11): Connecting with BIPOC, women and/or newcomer networks, non-profit or government organizations, universities, local/community groups and training programs like ACTP could expand the pool of candidates.
- **Increase the number of education and upskilling opportunities for potential candidates in underrepresented groups** (n=8): Work-based training, internships and training programs like ACTP can help create a larger pool for recruiters to select from.
- **Develop or support formal processes that encourage an equitable and inclusive culture** (n=7): Organizations could invest more in offering internal education and training on workforce bias, fostering diversity among leadership teams, building pathways to leadership roles, fostering safe and inclusive environments and implementing and enforcing zero-tolerance policies around discrimination.

> *"It's the employer's responsibility to make sure DEI isn't just [lip] service but how they're implementing it and how bias plays out."*
>
> *– LEARNER*

Both employers and learners agreed that to promote DEI, HR departments can work to make job postings more inclusive by:

- having more flexible requirements
- reducing the minimum education requirements
- eliminating gendered language
- generally including those with non-traditional backgrounds, skillsets and experiences.

Conclusion

Our research points to a range of recruitment challenges that may be holding the cybersecurity sector back from building a diverse workforce. From learner outcomes and employer feedback, ACTP shows promising employment results for diverse candidates breaking into the cybersecurity sector. The Catalyst can consider modifying program certifications to further align with industry need and targeting entry-level workers. Situated at the nexus of candidates and employers, they may also be well positioned to market candidates for roles and facilitate sustainable relationships to support diverse hiring, recruitment and advancement in the sector.

These findings suggest several areas for the Catalyst to further consider in both refining programming, and expanding its impact beyond just the bounds of ACTP.

Programming

In addition to GSEC and GCIH, the Catalyst can explore the value of offering the CompTIA Security+ certification.

There are three certifications that employers reported were most valuable: CompTIA Security+, GSEC and GCIH. Of these, ACTP offers GSEC and GCIH. ACTP also offers GFACT which, as a foundations certification, is less in-demand from employers but may benefit learners with less prior experience. The Catalyst may explore the benefit of offering the CompTIA Security+ certification to equip learners with the most in-demand industry certifications.

The Catalyst could consider fine-tuning its target population for ACTP.

ACTP is geared toward those interested in breaking into the cybersecurity sector, which can include people with a wide range of previous work experience. Our research with learners showed that those with established careers, especially in relatively well-paying industries such as IT, were more often disappointed with the salary offers of cybersecurity roles. On the other hand, those earlier in their career more often valued the experience of breaking into the sector over a higher paying wage. For this reason, it seems ACTP is best suited for those earlier in their career and could be differentiated from a cybersecurity upskilling program for those already established in cybersecurity or a peripheral sector.

Beyond Programming

By further developing their community and industry partnerships, the Catalyst might be able to match more candidates to roles.

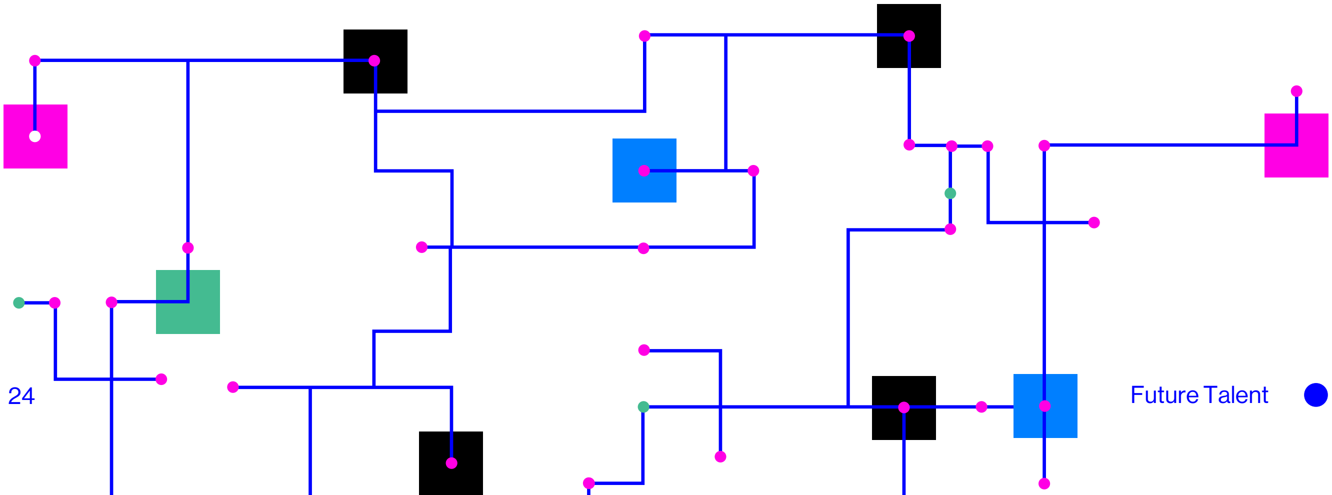
Training diverse cybersecurity candidates and connecting them to employers has contributed to diversifying the sector. A special value of ACTP is its dual-client model and its ability to combine and account for both employer and learner needs. Deepening its role as liaison between diverse and talented candidates and cybersecurity employers could increase the Catalyst's impact as a change agent for diversity in the sector.

Learners and employers suggested the Catalyst can expand their positive influence by working directly with communities, including Indigenous communities, to show people from marginalized groups that cybersecurity can be a viable career. Similarly, the Catalyst can leverage their existing and blossoming relationships with employers to advocate that graduates of ACTP are viable candidates to fill their vacant cybersecurity roles. In doing so, the Catalyst could help recalibrate the standard expectations for entry-level cybersecurity roles and show that ACTP graduates can meet the industry's talent needs.

To support DEI in the cybersecurity sector, the Catalyst could facilitate coordination between cybersecurity managers and HR teams to improve hiring of new entrants.

Through our engagement with learners and employers, we frequently heard that fragmentation between cybersecurity teams and HR teams poses a challenge to moving the needle in terms of DEI. Because HR teams are not as close to cybersecurity roles as cybersecurity teams, they do not always have access to key technical information on job requirements that could allow for flexibility in job postings or preliminary screening interviews without compromising the needs of the role.

A strong partnership between cybersecurity managers and HR teams could support the sector in becoming more diverse, equitable and inclusive. In their unique position of building relationships with both cybersecurity candidates and the industry, the Catalyst could explore creating employer toolkits to better bridge HR knowledge with organizational cybersecurity needs. By helping employers develop hiring strategies that are better attuned to the skillsets of new entrants into the sector, the Catalyst has an opportunity to promote the organizational change necessary to promote DEI in the workplace.



References

(ISC)2. (2021). *A resilient cybersecurity profession charts the path forward: (ISC)2 cybersecurity workforce study*. https://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/ISC2%20Cybersecurity%20Workforce%20Study%202021.pdf

Lake, S. (2022, June 30). 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, September 1). Hackers wanted: Canada faces a troubling shortage of cybersecurity talent. *The Globe and Mail*. https://www.theglobeandmail.com/business/article-canada-faces-a-troubling-shortage-of-cybersecurity-workers/

Future Skills Centre | Blueprint