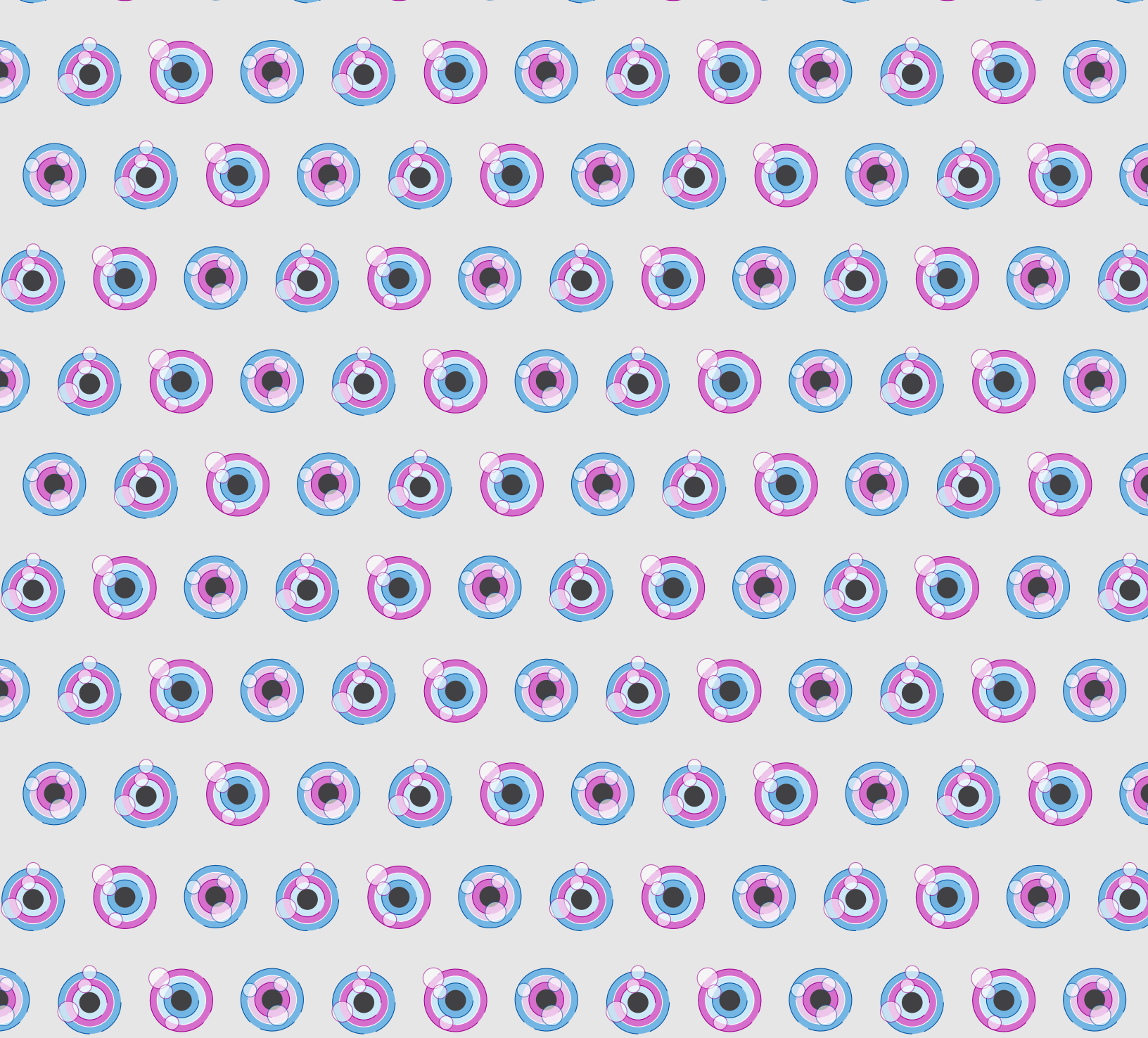


Certifications for Leadership in Cybersecurity (CLIC)

Final Report

November 2025

Blueprint

Table of contents

Acknowledgements

About the Future Skills Centre

The Future Skills Centre is a forward-thinking centre for research and collaboration dedicated to driving innovation in skills development so that everyone in Canada can be prepared for the future of work. We partner with policymakers, researchers, practitioners, employers and labour, and post-secondary institutions to solve pressing labour market challenges and ensure that everyone can benefit from relevant lifelong learning opportunities. We are founded by a consortium whose members are Toronto Metropolitan University, Blueprint, and The Conference Board of Canada, and are funded by the Government of Canada's Future Skills Program.

About Blueprint

Blueprint helps leaders use data and evidence to tackle complex public policy challenges across Canada.

We partner with government, community, philanthropic, and industry leaders to strengthen public systems and deliver better outcomes. We bring together policy analysts, evaluators, economists, data scientists, and implementation experts—people who know how to turn insight into action. Our work is grounded in deep subject-matter expertise, rigorous methods, and a real-world understanding of how systems operate and evolve. More than just an advisor, we're also partners in change. We provide key support at every stage of the policy and program lifecycle: from early strategy and design to implementation, evaluation, and continuous improvement.

As a consortium partner of the FSC, Blueprint works with partners and stakeholders to collaboratively generate and use evidence to help solve pressing future skills challenges.

About Rogers Cybersecure Catalyst (the Catalyst)

Rogers Cybersecure Catalyst is Toronto Metropolitan University's national centre for training, innovation and collaboration in cybersecurity. Since its founding in 2018, the Catalyst has grown into Canada's most active cybersecurity hub, earning a global reputation for delivering high-impact programs and driving innovative solutions to critical technology security challenges. A not-for-profit corporation, the Catalyst collaborates with governments at all levels, public and private organizations, and academic institutions. Headquartered in Brampton, Ontario's Innovation District, the Catalyst delivers its programs across Canada and around the world.

The CLIC *Final Report* is funded by the Government of Canada's Future Skills Program.

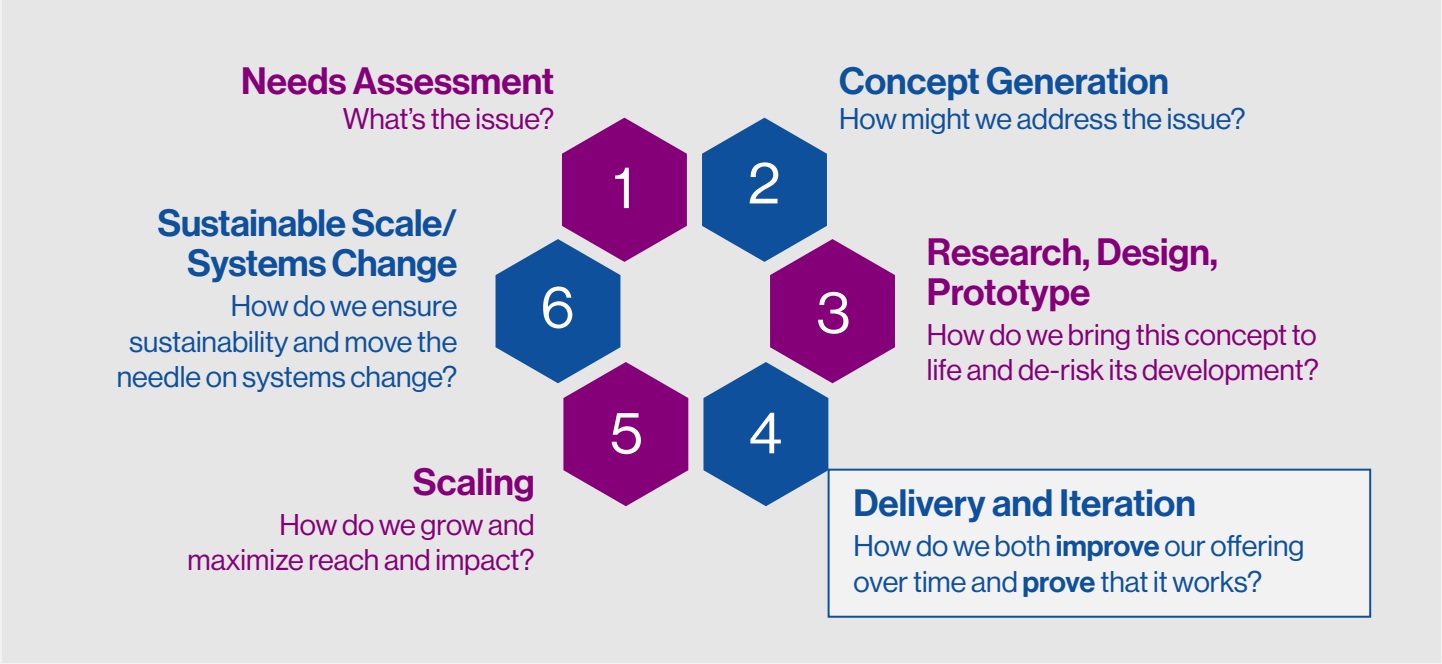
Future Skills Centre | Centre des Compétences futures | Blueprint | Canada

Preface

Canada's labour market is evolving rapidly, requiring responsive and evidence-based skills development programs. While many innovative programs emerge, scaling them beyond the pilot stage remains challenging. To address this, the **Future Skills Centre (FSC)** and **Blueprint** launched the **Scaling Up Skills Development Portfolio** and partnered with 11 organizations to support their scaling efforts. Blueprint works closely with each grantee to generate continuous evidence, moving beyond the traditional 'one study at a time' approach to enhance program improvement and scalability.

Aligned with the six-stage innovation cycle (see **Figure 1**), we focus on advancing interventions from the Delivery Phase (Stage 4) to the Scaling Phase (Stage 5), ultimately supporting Sustainable Systems Change at Stage 6. For more about our evidence generation approach and model, see our *Scaling Design Report*.

Figure 1 | The six-stage innovation cycle



1. Introduction

Canada's cybersecurity sector is under intense pressure, facing a dramatic surge in threats since the pandemic while grappling with a critical shortage of skilled talent. As demand for cybersecurity professionals climbs, traditional training pathways struggle to keep pace, and many positions remain vacant. Meanwhile, systemic barriers continue to limit participation by women, newcomers, and racialized professionals—groups whose diverse perspectives are essential to building resilient, multidisciplinary teams capable of countering global cyber threats.

For further context on sector needs, see **Box 1** on **p. 7**.

1.1. The Accelerated Cybersecurity Training Program (ACTP)

In response, 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. Delivered in partnership with the SANS Institute,[1] and supported by the Government of Canada, Rogers Communications, and RBC, this seven-month program combined industry-recognized SANS Institute training and certifications with career coaching to open pathways into cybersecurity for women, newcomers, and career changers. The Catalyst also worked closely with employers to co-develop curricula and ensure alignment with workforce needs, operating on the premise that employer-informed programming and tailored career supports would lead to stronger labour market outcomes.

In 2021, funding from the Future Skills Centre (FSC) allowed the Catalyst to expand ACTP to more students,[2] with a focus on recruiting BIPOC (Black, Indigenous, and People of Colour) learners, deepening its commitment to workforce diversity. As an FSC consortium partner, Blueprint published two ACTP evaluations: *A Race for Talent* (2022), examining employer hiring practices and needs; and *Future Talent* (2023), assessing early ACTP outcomes and sector relevance using participant and employer data. Reports found high learner satisfaction, increased employment and income rates, and strong post-graduation entry into cybersecurity roles, demonstrating ACTP's relevance and effectiveness.

1 The SANS Institute is a world leader in cybersecurity training and certification. SANS certifications are the highest and most rigorous assurance of cybersecurity knowledge and skills; graduates with these qualifications are in high demand.

2 Cohorts doubled in size from 2021 to 2023.

1.2. From ACTP to Certifications for Leadership in Cybersecurity (CLIC)

With ACTP's funding concluding in 2023, the Catalyst sought to build on its success through two successor programs. The first was Advanced Cyber Education (ACE)—another funded model, this time by Palette Skills—which provides cybersecurity professionals with at least 18 months of experience with intermediate skills and knowledge to assume more specialized roles.

The second was ACTP's tuition-based successor: Certifications for Leadership in Cybersecurity (CLIC). Developed as a streamlined version of ACTP, CLIC became the Catalyst's first participant-funded training program, aligning with a broader institutional goal of developing revenue-generating offerings to reduce reliance on external funding. CLIC retained several of ACTP's core components while adapting others to align within a tuition-based model. Developed with input from the Catalyst's Employer Advisory Council, CLIC's first and second cohorts launched in October 2023 and May 2024. Key adaptations from ACTP to CLIC are discussed in **section 2: Model design**.

1.3. About this report

This report examines CLIC's reach, uptake, learner experience, and short-term outcomes using administrative data, participant surveys and interviews, and Catalyst focus groups, collected from May 2024 to May 2025. We compare these findings to ACTP data (collected from 2021–2023) to assess how the transition to a tuition-based model affected program reach, quality, accessibility, and early outcomes. We also provide a high-level analysis of expenditures to assess the sustainability implications of the shift.

The report includes the following sections:

- **Model design (pp. 8–12)** describes ACTP and CLIC components and a programmatic theory of change: a roadmap connecting program activities to expected outcomes.
- **Methodology (pp. 13–16)** outlines our evaluation approach, learning agenda, data sources, and limitations.
- **Findings (pp. 17–38)** presents evidence on program reach, uptake, learner experience, early outcomes, and program costs.
- **Discussion and conclusions (pp. 39–41)** summarize our findings and unpack their implications.

Box 1 | Cybersecurity in Canada: Threats, talent shortages, and diversity needs

Cyber-attacks have surged over 100% since the pandemic, with cyber criminals exploiting vulnerabilities created by economic instability, remote work practices, and heightened public anxiety.[i] Manufacturing, energy, healthcare, government, and finance are among the most frequently targeted sectors.[ii] A 2023 ISC2 study reported that cybersecurity professionals believed threats were at their highest levels in five years—and only half of those surveyed believed their organizations were equipped to handle incidents over the next three.[iii]

Compounding these risks is an acute skills shortage. According to Public Safety Canada, the country faces a "shortage of cybersecurity talent … in all sectors."[iv] To illustrate, Canada required 25,000 cybersecurity specialists to meet demand in 2024,[v] but one in six jobs sat unfilled.[vi] Such demand is only poised to grow. After a 30% leap in sectoral employment between 2018 and 2020,[vii] job growth is projected to continue at a rate of 8.2% annually through to 2029.[viii] In practice, this shortage leaves roles vacant across private and public organizations, with some education programs unable to retain students long enough to graduate before they are hired.[ix] At the same time, rural regions struggle to attract cybersecurity talent at all, creating what are called geographic "deserts" of expertise.[x]

Bridging this gap requires tackling complex challenges—including the limitations of traditional training pathways. Budget cutbacks and layoffs have reduced organizations' capacity to recruit and retain qualified candidates, while stretched internal resources contribute to high rates of burnout among existing cybersecurity professionals.[xi] U.S.-based firms frequently lure top Canadian talent south with higher salaries, intensifying domestic recruitment pressures.[xii] Conventional academic routes into cybersecurity—often costly, lengthy, and light on experiential placements—do not always align with industry needs. Many professionals now view shorter-term certifications, including microcredentials, and hands-on experience, including work-integrating learning programs, as more valuable than formal degree programs in securing employment, advancing careers, and increasing retention.[xiii]

Addressing gaps also means engaging historically excluded groups, such as women, newcomers, and racialized professionals. In Canada, women have consistently made up less than 30% of the tech workforce over the past decade—and globally, most women in tech identify as white.[xiv] The picture in cybersecurity is even starker: only 20% of the workforce in Canada identifies as women, and merely 25% identify as BIPOC.[xv] Beyond questions of equity, broadening recruitment comes with tangible business and sector-wide benefits. Research shows that diverse teams achieve stronger financial performance, higher employee satisfaction, and enhanced organizational reputation.[xvi]

Diversity also has benefits for tech- and cybersecurity specifically. Diverse, multidisciplinary teams consistently outperform homogeneous groups in problem-solving and innovation[xvii]—capabilities vital for detecting and responding to cyber threats. In practice, organizations with inclusive cultures are better able to promote everyday cyber hygiene and participation across roles, not just among specialists.[xviii] An inclusive tech workforce can enable more diverse AI models, which in turn mean more rapid discovery of risks.[xix] Different perspectives enable greater resilience to ever-evolving threats. Newcomers bring international experience and multilingual abilities to a global threat landscape. Women, Indigenous, and racialized professionals bring different assessment approaches to predict threats from new angles and that target a greater variety of communities and industries.

2. Model design

This section outlines how ACTP and CLIC were developed, delivered, and adapted. To understand the rationale behind design choices—and how they were expected to produce participant and employer outcomes—we begin with a theory of change (ToC).

2.1. Theory of change (ToC)

The ToC articulates the problem ATCP and CLIC sought to solve, the assumptions underlying their design, and the intended pathways to short-, medium-, and long-term outcomes. Developed collaboratively with the Catalyst, the ToC guides program design and data collection tools to enable meaningful comparative analysis. **Table 1** summarizes components; for a visual depiction, see **Appendix A**. Program differences in inputs and activities are noted in **section 2.2**.

Table 1 | Theory of change

Vision	Assumptions	Inputs and activities	Participant and employer outcomes	
ACTP and CLIC were both created in response to: • a shortage of qualified cybersecurity professionals; • the absence of career pathways into the field; and • the exclusion of underrepresented groups. They aim to build a competitive cybersecurity sector by expanding and diversifying employers' candidate pool.	Programs are grounded in the **assumptions** that: • reducing barriers to training enables more diverse professionals to succeed in the field; • employers value GIAC certifications and see them as assets in new hires; and • career supports and employer engagement can improve employment outcomes for learners	**Inputs** include: • funding, • SANS instructors, • technical curricula and GIAC certifications, • mentors and career coaches, and • employer partnerships. **Activities** include: • recruitment, admissions, and orientation, • career preparation (resume development, job search supports), and • technical training via webinars, mentor/TA calls, study groups, bootcamps, and exams.	**Participant short-term outcomes:** improved cybersecurity knowledge and skills; greater clarity on career pathways; stronger employer and peer networks; and improved job search capacity. **Medium-term outcomes:** increased interest from employers; progression through hiring stages; and improved career navigation and early advancement. **Long-term outcomes:** sustained, well-compensated careers and advancement into more senior cybersecurity roles	**Employer short-term outcomes:** access to a qualified, diverse pool of cybersecurity candidates and increased ability to recruit women and other underrepresented groups. **Medium-term outcomes:** more diverse hiring practices, patterns, and representation across teams. **Long-term outcomes:** reduced workforce gaps and more inclusive organizational cultures that support employee growth and business success.

2.2. ACTP and CLIC program components

Below, **Table 2** compares ACTP and CLIC, highlighting where the Catalyst retained features and where it introduced elements. We follow with a description of adaptations between programs. Curriculum details can be found in **Appendix B**.

Table 2 | Summary of ACTP and CLIC components (program differences highlighted)

Element	ACTP	CLIC
Target learners	Women (and non-binary), newcomers, new careers, BIPOC	Women (and non-binary)
Application	Program application, SANS-administered aptitude test,[3] video interview, statement of interest[4]	
Selection criteria	• New to cybersecurity • Demonstrated interest in cybersecurity • Must meet specific stream criteria (women, newcomers, or new careers)	• New to cybersecurity or up to one year of cybersecurity experience • Demonstrated interest in cybersecurity[5]
Format	Asynchronous self-study supported by a study schedule, peer collaboration, and periodic check-ins and support	
GIAC certificates	• Foundational Cybersecurity Technologies (GFACT) • Security Essentials Certification (GSEC) • Incident Handler Certification (GCIH)	• Foundational Cybersecurity Technologies (GFACT) • Security Essentials Certification (GSEC)
SANS courses	• Security Foundations (prep for the GFACT exam) • Security Essentials: Network, Endpoint, and Cloud (prep for the GSEC exam) • Hacker Tools, Techniques, and Incident Handling (prep for the GCIH exam) • Catalyst Cybersecurity Professional Practice Course[6]	• Security Foundations (prep for the GFACT exam) • Security Essentials: Network, Endpoint, and Cloud (prep for the GSEC exam) • Catalyst Cybersecurity Professional Practice Course

3 The aptitude test consists of 30 questions designed to measure skills such as logic, critical thinking, problem-solving, and computer knowledge.

4 Statements of interest ask about applicants' interest in cybersecurity, educational history, experience, skills and courses, career goals, and how the programs can help. Staff review each application holistically, considering the aptitude assessment, statements of interest, resumes, and video interviews. All applicants are contacted by email during the application process and receive an admission decision within 30 days of completing the full application. Participants may apply once per intake and reapply for future intakes should they be unsuccessful.

5 This selection criterion was relaxed during project implementation due to the limited number of applications.

6 The Professional Practice Couse expands participants' understanding of cybersecurity beyond technology to incorporate business operations, decision-making, and risk management.

Element	ACTP	CLIC
Instructors	Industry experts who are verified SANS instructors for SANS courses	
Duration	Seven months (with recommended 25+ hours per week of self-study)	Six months (with recommended 25+ hours per week of self-study)
In-program supports	• Weekly check-ins with SANS mentors • Study groups (optional) • Catalyst outreach/check-ins • Cyber Range[7] • Two GIAC practice tests per exam	• Weekly check-ins with TAs (ACTP grads admitted based on selection criteria) • Study groups (optional) • Catalyst outreach/check-ins • Cyber Range • Two GIAC practice tests per exam
Career supports	• Professional Practice course materials • Post-program job search support [8]	• Professional Practice course materials • Post-program job search support • Three on-demand career coaches available throughout (HR, professional, and technical) • Rogers job pool
Tuition	$500 registration fee	• $15,000 + HST[9] • Financing options and partnerships with Windmill Microlending, Achev Career Advancement Loans, and Better Jobs Ontario • $5,000 Rogers Communications and RBC-sponsored bursaries available for women
Course and certificate costs (market value)[10]	Up to $25,031 USD (approx. $34,543 CAD)	Up to $14,454 USD (approx. $19,947 CAD)

7 Students engage in the Catalyst Cyber Range, an experiential learning course and simulated corporate environment, teaching new ways of thinking and problem-solving through an array of real-world cyber-attack scenarios in a team-based environment.

8 Staff help learners develop a personalized career plan and navigate the nuances of job searching in the cybersecurity sector, assisting with choosing a career path, resume writing and critiquing, interview prep and mock interviews, building a professional network, one-on-one coaching, connection with employers (e.g., info sessions, employer coffee chats), connection with Catalyst alumni, employer recruitment events, job offer negotiation, and opportunities for promotion.

9 Tuition has increased to $16,500 + HST for recent and future CLIC cohorts.

10 Estimates were calculated using posted SANS course prices, converted from USD to CAD, and reflect the maximum cost incurred if SANS courses, practice tests, and exam attempts are purchased separately. Some bundles may be available when purchasing SANS courses and exams online.

The Catalyst made the following adaptations from ACTP to CLIC:

- **Recruitment.** ACTP targeted Canadian residents who are new to cybersecurity and offered dedicated streams for women, newcomers, career-changers, and BIPOC learners. CLIC removed these streams and broadened eligibility to include non-Canadian residents. In cohort 2, it introduced a limited number of **$5,000** bursaries for women and non-binary learners, funded by Rogers Communications and RBC. **Twenty-five** learners identifying as women received a bursary (**38%** of those who enrolled). As noted, the ACE Training Program is for individuals with more than 18 months of cybersecurity experience; those with less experience are directed to CLIC.
- **Content and duration.** ACTP ran for seven months and offered three GIAC certifications: GIAC Foundational Cybersecurity Technologies (GFACT), GIAC Security Essentials Certification (GSEC), and GIAC Incident Handler Certification (GCIH).[11] CLIC spans six months and offers GFACT and GSEC. This change was based on employer consultations and ACTP participant feedback, balancing cost, workload, and market relevance. Though still intensive, CLIC delivers fewer certifications over a similar period to reduce learner overload.
- **Supports.** In ACTP, check-ins were led by SANS mentors; in CLIC, they are led by teaching assistants (TAs).[12] The Catalyst tracks weekly learner study progress and conducts outreach based on responses to keep individuals on track.
- **Professional development.** Building on ACTP feedback, CLIC added access to three on-demand career coaches—HR, professional, and technical—to help learners explore specializations and align goals with their interests.
- **Rogers job pool.** As part of its partnership with the Catalyst, Rogers created a small pool of entry-level cybersecurity jobs that were reserved for Catalyst graduates and posted exclusively on the Catalyst's internal job board.
- **Tuition.** ACTP required a $500 registration fee. CLIC costs $15,000 + HST. If taken independently through SANS, GFACT and GSEC courses and certifications would cost nearly $20,000.

11 Certifications are from the SANS Institute's Global Information Assurance Certification (GIAC). Foundational Cybersecurity Technologies (GFACT) demonstrates that an individual has hands-on skills through labs in areas such as Linux, encryption, and programming, and essential knowledge in areas such as networking, computer hardware, virtualization, Windows server, and introductory security concepts. Security Essentials Certification (GSEC) validates knowledge of information security beyond simple technology and concepts. GSEC certification holders demonstrate they are qualified for hands-on IT system roles for security tasks. The Incident Handler Certification (GCIH) validates a practitioner's ability to detect, respond, and resolve computer security incidents using a wide range of essential security skills. Earners manage security incidents by understanding, defending against, and responding to common attack techniques, vectors, and tools.

12 CLIC TAs are ACTP alumni with a minimum of two years of cybersecurity experience in a technical role and who received high scores on ACTP exams (especially GSEC and GCIH).

2.3. Conditions for success

Blueprint and the Catalyst worked together to identify a set of conditions needed for CLIC's successful delivery. Understanding these conditions helps us interpret CLIC's performance and identify where adaptation may be helpful.

- **The Catalyst** must have the ability to maintain the resources and capacity to deliver CLIC and recruit target numbers of learners who are well-suited to cybersecurity; maintain and adapt CLIC to evolving sector needs; maintain and build new industry and SANS partnerships; and find available mentors and coaches to support learners.
- **Learners** must see value in certifications, curricula, and supports and feel they reflect their needs and interests; dedicate sufficient time needed to complete an accelerated program; and feel its value outweighs its costs.
- **Employers** must value the GIAC certificates earned; be committed to bringing more women into their organizations and the sector; sustain a need for entry-level positions and be willing to hire CLIC graduates; and see sufficient payoff for engaging in CLIC and continue providing and investing in bursaries and other learner supports.
- **The sector** must maintain a need for cybersecurity training programs for entry-level roles; and sustain the economic conditions—learner employment stability, living costs, household income, lending patterns, interest rates—necessary for learners to pay tuition.

ACTP demonstrated how a government-funded program—free to participants—addressed an urgent labour market shortage while advancing equity in a sector that continues to underrepresent women, newcomers, and BIPOC professionals.

3. Methodology

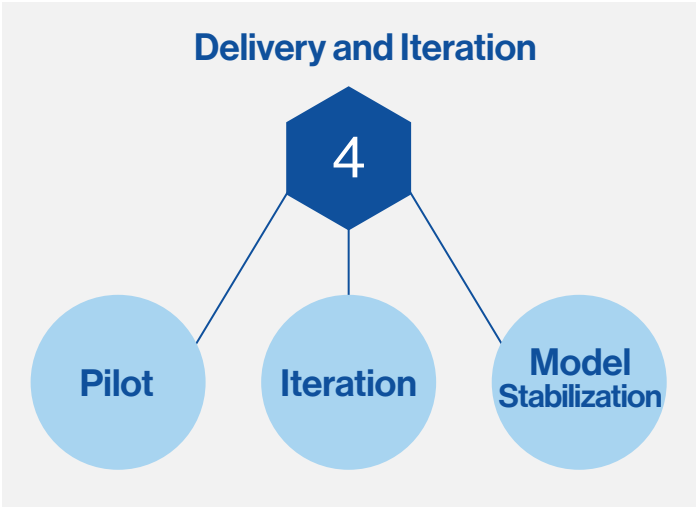
3.1. Blueprint's evidence generation approach

Based on the **Scaling Up Skills Development** innovation cycle described in the **Preface**, this intervention is positioned in **Stage 4: Delivery, Testing, and Iteration**. As part of FSC's grant-making process, each project was determined to have the potential to move to the fifth and sixth stages: **Scaling** and **Systems Change**.

Within the Delivery, Testing, and Iteration phase, there are three sub-phases, as shown in **Figure 2: a) Pilot; b) Iteration;** and **c) Model Stabilization**. Because CLIC was based on ACTP and adapted to a tuition-based model, we categorize it at **Stage 4b: Iteration**.

Organizations in this stage continue to generate evidence to strengthen design and delivery and improve their models. They are also keen to understand whether their intervention is achieving its intended outcomes and need flexible evaluation methods to generate evidence about effectiveness while allowing for continuous improvement. For the Catalyst, iterating on the successful ACTP model was a critical step towards a sustainable tuition-based successor.

Figure 2 | Delivery and iteration sub-phases



3.2. Learning agenda

This report answers questions in four areas:

- **Program reach and uptake.**
  - How did CLIC's positioning influence recruitment and program uptake?
  - What were CLIC learners' motivations to apply? Did they differ from ACTP learners?
  - Who is participating in CLIC? Is it reaching its intended audience?
- **Learner experience.**
  - How many learners completed the program?
  - Who withdrew from the program, and why?
  - Were learners who completed the program satisfied with CLIC?
  - How did user experience vary across the subgroups who completed the program?
- **Program outcomes.**
  - What were the short-term outcomes for CLIC graduates? How did they compare to those of ACTP graduates?
- **Cost.**
  - How did funding allocation differ between ACTP and CLIC?

3.3. Data sources and sample sizes

Blueprint analyzed reach, uptake, participant experiences, and short-term outcomes—self-indicated increases in skills, confidence, employment rates, and income—for the first two CLIC cohorts (referred to below as **CLIC 1** and **CLIC 2**). We conducted a cost analysis to understand changes in operating costs between the funded and tuition-based models.

We gathered quantitative and qualitative data, summarized in **Table 3**, including learner surveys,[13] interviews,[14] and administrative data provided by the Catalyst. After collecting data, Blueprint conducted an internal sensemaking process to discuss trends and recommendations. To contextualize CLIC results, we also drew on evaluation data from five ACTP cohorts (6–10), collected between 2021 and 2023. Further detail on ACTP data is available in the *Future Talent Evaluation Report* (2023).

Table 3 | Data sources and sample sizes[15]

Data sources	Dates	Descriptions	ACTP sample sizes	CLIC sample sizes
Administrative data	CLIC and ACTP data received Dec. 2024	Collected by the Catalyst during recruitment and program delivery.	N/A	N/A
Learner consent and baseline survey	CLIC: May 2024 ACTP: Oct. 2021–Feb. 2023	Administered to learners at the start of ACTP and CLIC 2 and at exit of CLIC 1 (due to delays) to capture demographic information and reasons for enrolment.	**Total:** 404/578 (70%)	**Total:** 82/127 (65%) CLIC 1: 32/69 (46%) CLIC 2: 50/58 (86%)
Exit survey	CLIC: May 2024–Nov. 2024 ACTP: June 2022–Oct. 2023	Administered to those who completed baseline survey and program to track satisfaction and immediate achievement of outcomes.	**Total:** 258/301 (86%)	**Total:** 51/81 (63%) CLIC 1: 22/41 (54%) CLIC 2: 29/40 (73%)

13 CLIC participants consenting to research were sent three surveys described in **Table 3**. Those who withdrew from CLIC received a withdrawal survey as soon as Blueprint was notified by the Catalyst. We conducted a descriptive analysis of survey data to determine the frequency of responses and cross tabulations to observe differences between various groups of participants. In some instances, two-tailed t-tests were conducted to examine differences in program experience and outcomes between different groups.

14 Interviews were one hour and explored education and background, including prior experience and interest in cybersecurity; motivations for enrolling in CLIC, application decision-making, and program expectations; program experience, including perceived difficulty and satisfaction (e.g., curriculum, pace, structure, and available supports); post-program next steps, including job search activities, Catalyst support, and perceived readiness for employment in cybersecurity; and reasons for leaving the program if applicable.

15 Survey denominators reflect the number of participants who were sent each survey. For CLIC baseline surveys, denominators differ from program enrolment numbers due to differences in when and how consent was captured for each CLIC cohort.

Data sources	Dates	Descriptions	ACTP sample sizes	CLIC sample sizes
Withdrawal survey	CLIC: May 2024–Apr. 2025 ACTP: Oct. 2021–Feb. 2023	Administered to learners who completed a baseline survey and withdrew from the program to capture satisfaction, reason for withdrawal, and employment status.	**Total:** 33/103 (32%)	**Total:** 14/42 (33%) CLIC 1: 8/28 (29%) CLIC 2: 6/14 (43%)
Three-month follow-up survey	CLIC: Aug. 2024–Mar. 2025 ACTP: Sept. 2022–Jan. 2024	Administered to learners who completed baseline and exit surveys three months after graduating to capture employment status, education enrolment, and social assistance receipt.	**Total:** 192/301 (64%)	**Total:** 39/59 (66%) CLIC 1: 14/21 (66%) CLIC 2: 25/38 (66%)
Graduate interviews	CLIC: June and Nov. 2024 ACTP: July 2022–Feb. 2023	Semi-structured, one-hour interviews conducted post-program to gather graduates' reasons for enrolment, experiences and satisfaction, and next steps.	**Total:** 22	**Total:** 12 CLIC 1: 7 CLIC 2: 5
Withdrawal interviews	CLIC: March 2025 ACTP: N/A	Semi-structured, one-hour interviews conducted post-withdrawal to gather learners' reasons for enrolment, experiences and satisfaction, next steps, and reasons for leaving.	N/A	**Total:** 3 CLIC 1: 2 CLIC 2: 1
Cost analysis	December 2024	Time- and cost-tracking worksheets, completed by Catalyst staff, estimating time spent to deliver program activities. Data were also provided for hard costs (e.g., assessments).[16]	N/A	N/A
Program staff focus group	CLIC: March–Apr. 2025 ACTP: N/A	Three 45-minute meetings with staff to discuss the design, delivery, and achievement of outcomes for CLIC.	N/A	Three meetings with 3–4 staff members

16 Blueprint developed time and cost tracking worksheets for the Catalyst to complete during CLIC delivery. These tools were used to estimate the time spent by different team members across key program delivery activities (e.g., recruitment and admissions, employer engagement, participant support). In addition to time estimates, Catalyst shared associated labour costs and hard costs for delivering ACTP and CLIC with Blueprint to support the overall cost analysis.

3.4. Data limitations

Findings in this report should be interpreted within the context of certain limitations:

- **Delayed data collection.** Because FSC project funding was confirmed only after CLIC 1 began, consent and baseline data collection were collected retroactively through exit and withdrawal surveys. This reduced sample size and increased the risk of recall bias.
- **Survey design changes.** Participant surveys were updated over time to reflect program changes, such as shifts in target learners and terminology (e.g., "mentors" in ACTP became "TAs" in CLIC). New questions were also added (e.g., prior cybersecurity experience, new career supports). These changes limit comparability across programs, especially on learner backgrounds and satisfaction.
- **Low and variable response rates.** CLIC survey response rates ranged from 33% to 66%, despite efforts to improve participation (e.g., reminders and extended deadlines). Low response rates reduce generalizability—particularly for withdrawal and follow-up surveys—and increase the risk of non-response bias. Reported reasons for withdrawal, for example, may not fully reflect the views of all learners.

3.5. Common outcomes framework

Our measurement approach includes both indicators that are specific to the CLIC and ACTP models and common indicators drawn from our common outcomes framework (see **Box 2**).

Box 2 | Common outcomes framework

Our measurement approach includes indicators that are specific to an intervention as well as a set of common indicators that are measured for every intervention in the Portfolio.

These common indicators are drawn from Blueprint's common outcomes framework, which was developed in consultation with our partners and was informed by review of employment-related outcomes frameworks and measurement approaches both within Canada and internationally. They include:

- Intermediate outcomes that reflect 'in-program' participant experiences and gains (e.g., program satisfaction and skills development).
- Long-term outcomes, such as employment and educational attainment.

Using a consistent approach to measuring outcomes is part of our commitment to understanding how each intervention in the Portfolio is reaching people across Canada. For the CLIC analysis, outcomes were only measured until three months due to the shorter delivery timeframe.

For more information, see **Appendix C**.

4. Findings

4.1. Program reach and uptake

CLIC's shift to a tuition-based model required a different recruitment strategy, affecting applicant volumes, admission criteria, attrition rates, and learner motivations to enrol.

4.1.1. How did CLIC's shift to a tuition-based model influence recruitment and program uptake?

- **ACTP** was positioned as a free training program to help people develop skills needed for employment in cybersecurity. Given low financial barriers and strong name recognition over four years of delivery, it is unsurprising that ACTP received over **900** applications per cohort (7,752 applications over 10 cohorts), on average. Candidates needed to demonstrate their interest in cybersecurity but required no prior work experience in the field. This was a funding requirement to ensure ACTP helped new professionals and provided accessible pathways for women, newcomers, career changers, and BIPOC learners. ACTP's application volume and interest-driven approach let staff apply rigorous selection criteria, admitting **14%** of applicants per cohort, on average. Of the **14%** admitted, **88%** enrolled (or began the program), meaning the drop-off from admission to enrolment was **12%**.
- As a new, tuition-based program, **CLIC** required substantial marketing to generate interest: promotional materials, social media campaigns, and information sessions.[17] In its marketing, CLIC was positioned as an accelerated route to employability, emphasizing labour market outcomes and career potential—for learners new to the sector *and* to those with some limited cybersecurity experience (as noted, those with over 18 months of experience were directed to ACE). CLIC saw significantly fewer applicants than ACTP (**350** per cohort, on average). To accommodate lower numbers of applicants, the Catalyst relaxed its criterion of demonstrated interest and admitted a larger proportion of applicants (**46%**, on average). Of the **46%** admitted, **47%** enrolled (or began the program). The attrition rate from admission to enrolment for CLIC 1 was **60%**; this dropped to **45%** in CLIC 2.

Table 4 and **Figure 3**, on the following page, show recruitment data from both programs—from applications received to drop-offs from admission to enrolment.

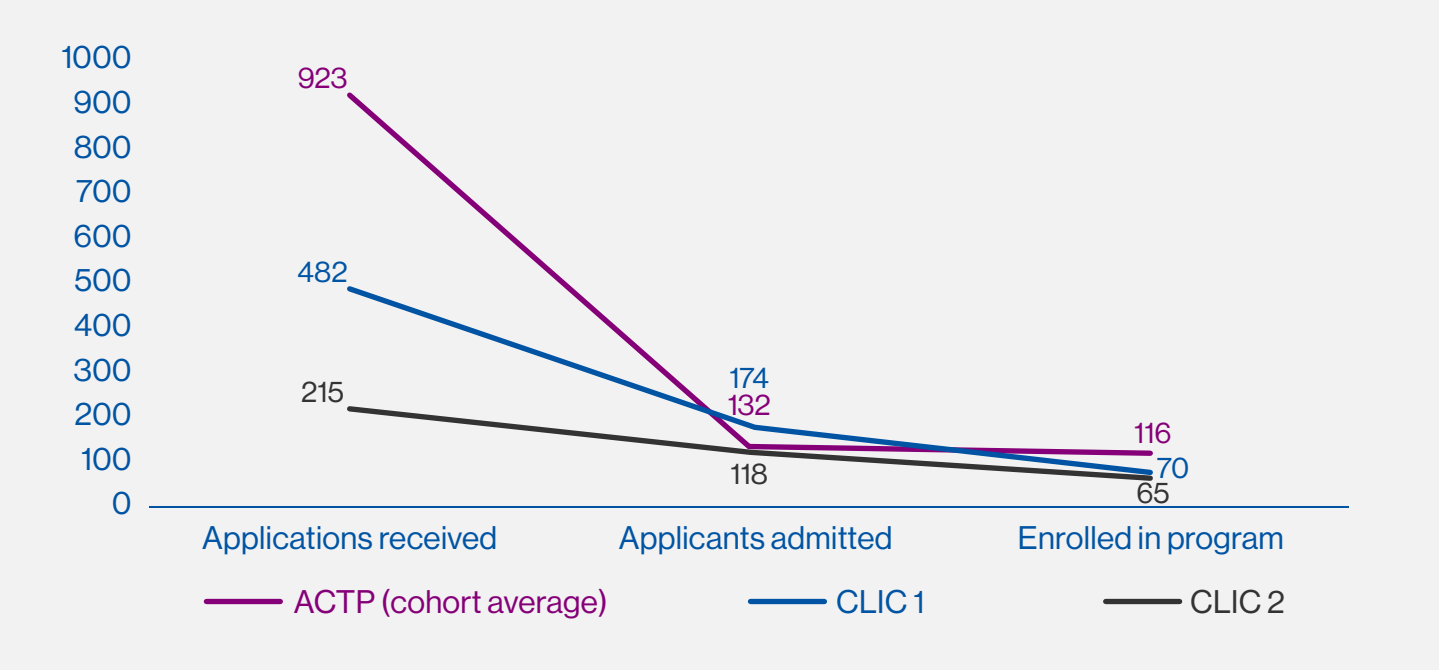
17 Promotions included digital campaigns (Meta, Google SEO), automated CRM workflows (drip emails), and one-on-one advising calls. The Catalyst hosted biweekly information sessions via its website and LinkedIn Live, promoted alumni stories and career coaching on social media, and leveraged its newsletter, TMU alumni LinkedIn group, Slack groups (e.g., City of Brampton, TMU), and partnerships with cybersecurity communities like WiCyS. Outreach included referrals, re-engagement with past applicants, and promotion on Eventbrite, MeetUp, and various LinkedIn groups. The Catalyst also engaged prospective learners at events such as SecTor, BSides, SiberX Women in Cybersecurity, and Scale Without Borders. Supporting materials included a financing guide, program package, schedule, and promotional videos.

Table 4 | Recruitment and admissions data for CLIC and ACTP

Program	# of information sessions and attendees	# of applications received	# and % of students admitted	# and % of admitted students who enrolled	% change from admission to enrolment
CLIC 1	14 (1,082 attended)	482	174 (36%)	70 (40%)	-60%
CLIC 2	9 (317 attended)	215	118 (55%)	65 (55%)	-45%
CLIC average of both cohorts	11.5	350	146 (46%)	68 (47%)	-53%
ACTP (avg. of cohorts 6–10)	N/A	923	132 (14%)	116 (88%)	-12%

Source. Administrative data

Figure 3 | Recruitment and admissions for CLIC and ACTP



Source. Administrative data

According to the Catalyst, the most common reasons for learners leaving the program from admission to program start included unexpected life events, such as changes in economic or financial circumstances, job loss, and family obligations.

4.1.2. Who participated in CLIC? Did CLIC reach its intended audience?

CLIC very nearly met its enrolment target: **96%** (**135/140**), with **100%** (**70/70**) in CLIC 1 and **93%** (**65/70**) in CLIC 2.[18]

CLIC's only explicit target audience were women and non-binary learners. As noted, the $5,000 Rogers Communications bursary helped subsidize program costs for **25** women learners (**38%** of those enrolled) at the beginning in CLIC 2. As shown in **Table 5**, **56%** of learners identified as women across both cohorts—nearly triple the percentage of cybersecurity workers in Canada identifying as women (**20%**).[xx]

Among CLIC learners, **80%** identified as BIPOC and **62%** were born outside of Canada. These proportions are slightly lower than in ACTP (**89%** and **85%**, respectively). While CLIC did not have the same requirement to recruit BIPOC and newcomer learners, it recruited over triple the percentage of cybersecurity workers identifying as BIPOC (**25%**).[xxi]

Table 5 | Socio-demographic comparison, CLIC and ACTP learners

Characteristics	**CLIC** (n=82)	**ACTP** (n=404)
Gender	Women 56% (46/82) Men 44% (36/82)	Women 53% (215/402) Men 45% (180/402) Another gender not listed 2% (7/402)
Age	20–29 years 27% (22/81) 30–39 years 38% (31/81) 40–49 years 26% (21/81) 50+ years 9% (7/81) Average age=36	20–29 years 29% (118/400) 30–39 years 51% (205/400) 40–49 years 15% (59/400) 50+ years 4% (18/400) Average age=35
Dependents	Primarily responsible for dependent < age 17 87% (34/39)	N/A
Identifying as BIPOC	80% (63/79)	87% (336/388)
Born in Canada	Born in Canada 38% (31/82) Born outside Canada 62% (51/82)	Born in Canada 16% (66/404) Born outside Canada 84% (338/404)
Location	Ontario 77% (62/81) Alberta 11% (9/81) Manitoba 4% (3/81) Nova Scotia 2% (2/81) British Columbia 1% (1/81) New Brunswick 1% (1/81) Quebec 1% (1/81) Yukon Territories 1% (1/81) I do not live in Canada 1% (1/81	Ontario 72% (290/404) Alberta 15% (61/404) British Columbia 4% (17/404) Nova Scotia 1% (6/404) Saskatchewan 2% (9/404) Manitoba 1% (6/404) New Brunswick 1% (5/404) Quebec 1% (6/404) Newfoundland <1% (1/404) I do not live in Canada 1% (3/404)

Source. Administrative data

18 Recruitment figures include one participant from CLIC 1 who deferred to CLIC 2 very shortly after enrolling and three participants in CLIC 2 who participated from Malaysia; these participants are counted toward recruitment targets but did not participate in the research and are not included in subsequent analysis.

At intake, ACTP and CLIC learners reported similar levels of current employment (**70%** and **61%**, respectively) and previous IT experience (**53%** and **56%**, respectively), as shown in **Table 6**. In CLIC, 27% of intake survey respondents reported current or previous employment in the cybersecurity sector or in a job related to it—and **22%** of *employed* participants reported that their current job was related to cybersecurity.[19] Although we did not ask ACTP participants directly about cybersecurity experience, only **3%** of employed ACTP learners reported having roles with at least **51%** of their tasks involving cybersecurity.

Table 6 | Employment-related experience

Characteristics at intake	CLIC (n=82)	ACTP (n=404)
Employed	**61%** (50/82)	**70%** (281/404)
With IT work experience	**56%** (41/73)	**53%** (212/403)
With current cybersecurity work experience	Employed respondents with current employment related to cybersecurity: **22%** (11/50)	Employed in roles with at least 51% of tasks related to cybersecurity: **3%** (9/279)

Source. CLIC and ACTP baseline surveys

Broadly speaking, there are four types of learners who participate in CLIC. As will be discussed in **section 4.2.3**, these differences influenced how individuals experienced the program.

1. **Highly technical with cybersecurity experience (27%).** These learners were working or had worked in a cybersecurity or related role at the time of enrolment. They typically held degrees in highly technical fields, such as engineering or computer science, and brought a strong background of technical knowledge and hands-on experience. In ACTP, learners with cybersecurity experience were rare.
2. **IT backgrounds (27%).** These learners entered CLIC without direct cybersecurity exposure but with employment experience in IT. In interviews, this group discussed having a broader range of educational and professional backgrounds (e.g., computer science, business, arts, management, etc.). These learners were also common in ACTP.
3. **Non-technical backgrounds (34%).** Learners in this group were new to cybersecurity, with no prior technical training or sector exposure. Interviews suggested a further divide: those who had taken introductory courses or

19 We asked the question, "In the past, have you ever had a job related to cybersecurity?" to CLIC participants who reported being unemployed but previously holding employment (n=30); **28%** (**5/18**) answered yes and **12** participants did not respond. The question, "Do you have any work experience in the cybersecurity sector?" was asked to all CLIC intake survey respondents (**n=82**); **25%** (**17/69**) said yes and **13** did not respond.

certifications, helping them build an interest in the field and understanding of CLIC's focus and certifications; and those who were exploring cybersecurity for the first time in CLIC. These learners were also common in ACTP.

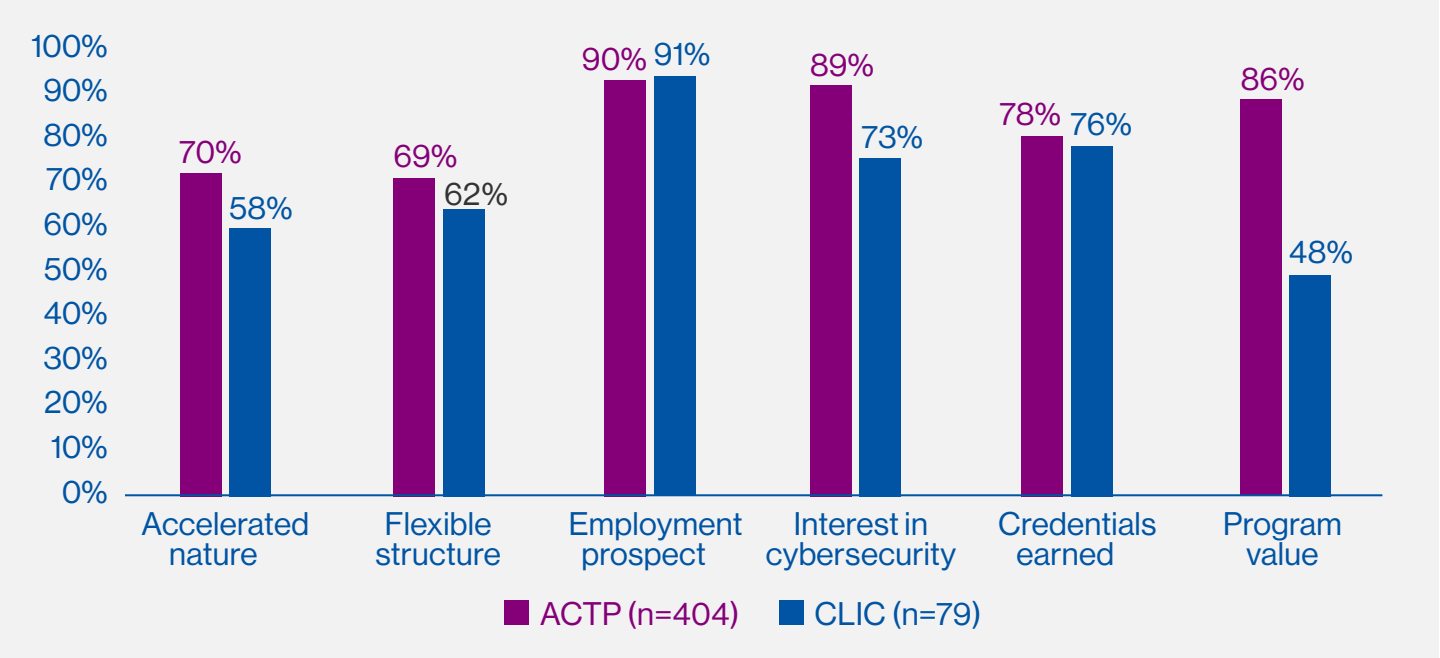
4. **Unknown (12%).** A small group of learners did not provide sufficient information about their past employment experience.

4.1.3. What were CLIC learners' motivations to enrol? Did they differ from ACTP learners?

In our baseline surveys, learners were presented with a list of possible motivating factors to enrol in CLIC and asked to select all that applied. As shown in **Figure 4**, **91%** of learners indicated that gaining employment was their main reason for enrolling. This percentage was almost identical to ACTP's (**90%**).

Unlike ACTP, CLIC learners were less likely to report interest in cybersecurity as a motivator—**73%** compared to **89%** for ACTP.[20] They also rated other program features as less influential in their decision, such as the accelerated format (**58%** vs. **70%** for ACTP) and flexible structure (**62%** vs. **69%**). The largest difference between programs was sense of value: only **48%** of CLIC respondents noted it as a motivation to enrol compared to **86%** of ACTP respondents.

Figure 4 | Motivations to enrol in CLIC and ACTP



Source. CLIC: baseline survey, n=79 | ACTP: n=404

20 While fewer CLIC learners held specific interest in cybersecurity, most took steps to explore the sector and assess whether CLIC was a good fit. In interviews, learners described connecting with ACTP alumni, attending information sessions, and researching certifications. Some had obtained cybersecurity credentials, such as CompTIA+, ISC2 Certified in Cybersecurity, and post-graduate university certificates. Some had exposure to the sector through relationships with cybersecurity professionals (e.g., spouses, parents, friends). Many had heard of ACTP—and had unsuccessfully applied to it—and were familiar with the program's structure and success. Efforts to build an understanding of the field before transitioning were particularly important for those with less technical backgrounds and helped them determine whether CLIC was aligned with their goals and backgrounds.

In interviews, learners shared that they appreciated CLIC's training timelines, certifications, and structure, but stated that career opportunities and employment supports influenced their decisions to enrol most heavily. Tuition was seen as a major investment but justified by the potential for meaningful employment and the launch into a well-paid career.

> *"CLIC was a little more expensive than the other programs, but I felt like once I finished the York program, I'd have a certificate in risk management and a four-year business degree. But I'd be back in the same spot, not really knowing where to get a job. So, cost was definitely a factor, but it wasn't too much. If it led to a job, it would be worth it."*
>
> – CLIC learner, interview

> *"The best path that I saw was the CLIC program because it included the career mentorship, a TA, and you get to work with your peers. So, I felt like it's a one-stop shop. That's why, considering cost, time and everything included, CLIC makes the most sense."*
>
> – CLIC learner, interview

Interviewees noted that promotional materials—CLIC's website, advertising, and information sessions—emphasized job outcomes, employer connections, and industry relationships. These messages set expectations that CLIC offered a clear, reliable pathway into cybersecurity.

> *"The website and info sessions talk about connections to other companies that have roles in the space. There were testimonies from previous students who landed jobs at those companies, so there was some clear indication from those employers that they do value their relationship with the Catalyst."*
>
> – CLIC learner, interview

> *"U of T has a similar style where they offer a CompTIA+ certification. They were both similar, but I ended up going with CLIC. I think the big thing for me was there were more industry connections that I weighed a little bit more than anything else to be able to find a career or a job afterwards."*
>
> – CLIC learner, interview

The program maintained access for underrepresented groups, introduced new career supports, and continued to deliver industry-recognized credentials at below-market costs.

4.2. Learner experience

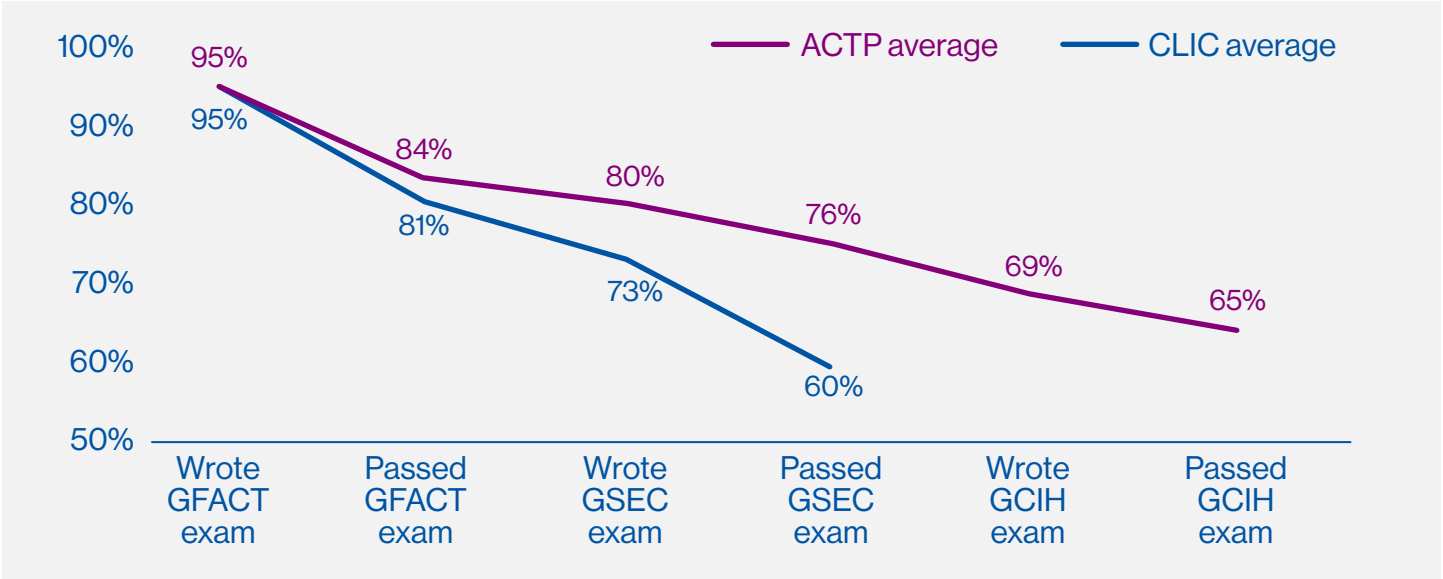
4.2.1. How many learners completed CLIC?

As shown in **Figure 5**, **60%** of enrolled learners passed the GSEC exam and thus completed CLIC.[21]

CLIC and ACTP cohorts show similarly high rates of writing and passing the GFACT exam: **95%** wrote the exam and **81%** passed in CLIC, and **95**% wrote and **84%** passed in ACTP. CLIC's main divergence point from ACTP (and largest point of attrition) was the GSEC exam—CLIC's endpoint and ACTP's midpoint. While **73%** of CLIC learners attempted the GSEC exam, only **60%** passed and completed the program; ACTP's pass rate for GSEC was **76%**.[22]

> [Running CLIC] requires more than financial engineering; it requires careful design choices that preserve equity, maintain quality, and adapt to market realities.

Figure 5 | Percentage of enrolled CLIC and ACTP participants who reached program exams



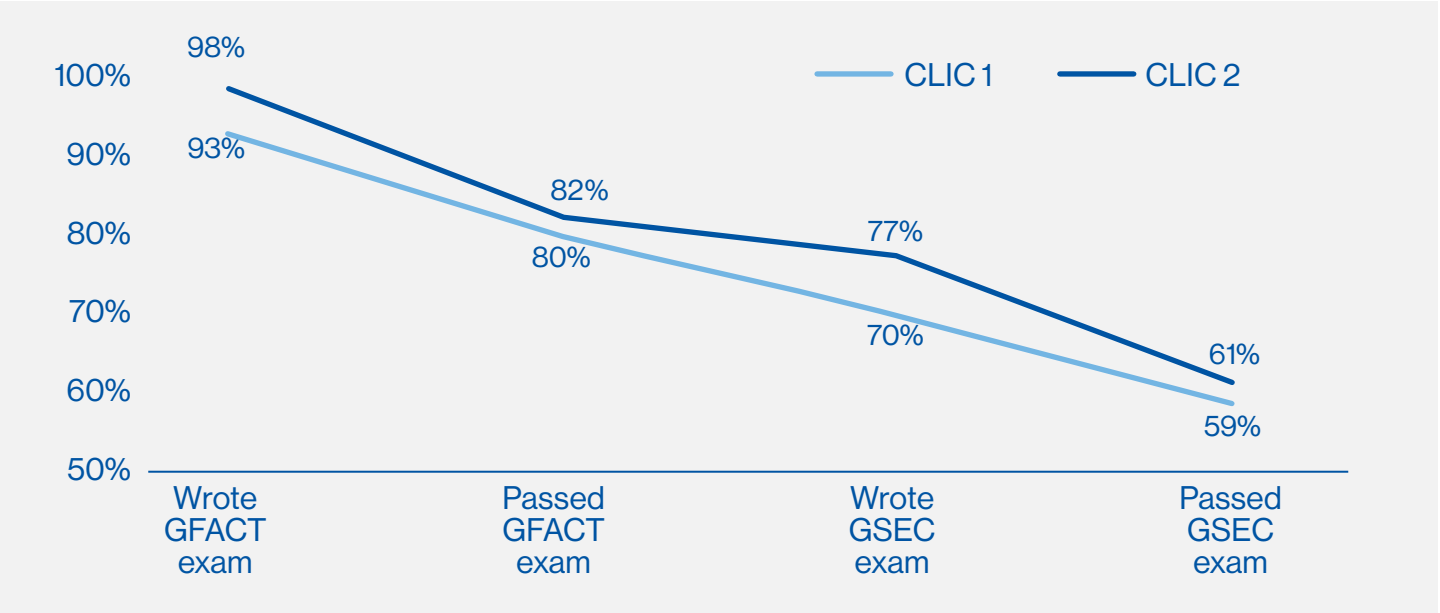
Source. Administrative data

21 The three Malaysian participants (described in footnote 18) in CLIC 2 were not included in this analysis of exams reached.

22 Following the third and final exam (GCIH), ACTP had a **68%** completion rate. The number of ACTP learners who completed the program was larger than the number of learners who passed the GCIH exam because **19** learners from the 10th cohort were part of an abridged program and not required to complete the GCIH exam to graduate.

As shown in **Figure 6**, a slightly higher percentage of students from CLIC 2 wrote and passed the GFACT and GSEC exams compared to CLIC 1.

Figure 6 | CLIC program exams reached per cohort



Source. Administrative data

A greater proportion of CLIC learners requested more time to complete the program than in ACTP: **58%** compared to **42%**. While ACTP learners were granted extensions on a case-by-case basis, CLIC learners had a formal extension policy and clear awareness of it.

4.2.2. Who withdrew from the program, and why?

Post-enrolment, **34%** of CLIC learners withdrew and **6%** deferred to the next cohort.[23] This is similar to the percentage of learners who withdrew from ACTP: **32%**. Note that findings below on learner-provided reasons for withdrawal may not be representative of all individuals: only **14** responded to the withdrawal survey and **three** participated in interviews. Similarly, only **33** ACTP learners completed the withdrawal survey.

Responding CLIC withdrawers cited three reasons for leaving: personal reasons (**36%**), challenges with the program's structure or format (**36%**), and misaligned expectations (**29%**). Responses are similar to those provided by ACTP learners, who cited personal reasons (**64%**), course pacing (**37%**), and structure or format (**15%**).

When citing personal reasons, CLIC respondents' decisions to withdraw were often unrelated to course content. As one learner stated:

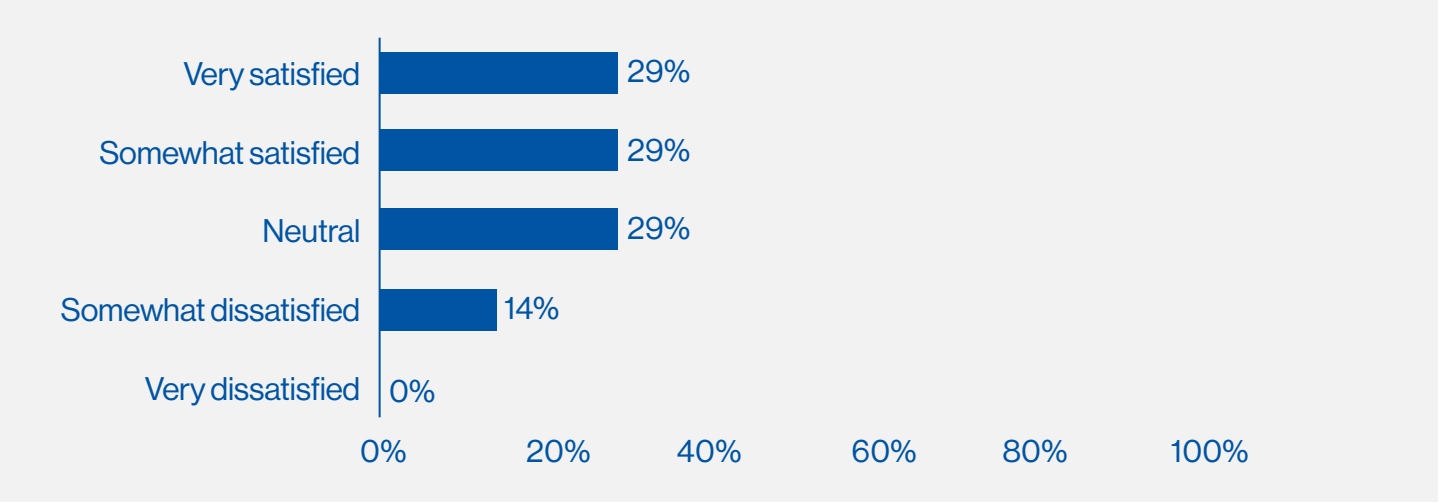
> *"My experience was great; my withdrawal was due to personal life issues that were overbearing and affected [my ability to] study at that time."*
>
> – CLIC learner, withdrawal survey

23 One learner deferred from CLIC 1 and seven deferred from CLIC 2. We do not have data on deferred learner completion rates.

Other withdrawers sometimes felt unprepared for CLIC's intensity, pace, and self-directed nature. Some wanted more live instruction, support, and a slower tempo—especially those working full-time or with limited technical experience, who struggled to absorb the material. One learner described falling behind and using the one-week break between courses to retake the GFACT exam. This caused them to start GSEC without a pause, which led to burnout. Catalyst staff noted that longer extensions after the first exam correlated with lower likelihood of re-writing and passing the GSEC exam.

Learners who withdrew from CLIC reported lower levels of satisfaction than those who completed (see **section 4.2.3**.). However, as shown in **Figure 7**, **58%** of respondents still reported being satisfied with CLIC—likely reflecting those who left for personal reasons and unexpected circumstances.[24]

Figure 7 | CLIC satisfaction among withdrawing learners



Source. CLIC withdrawal survey | n=14

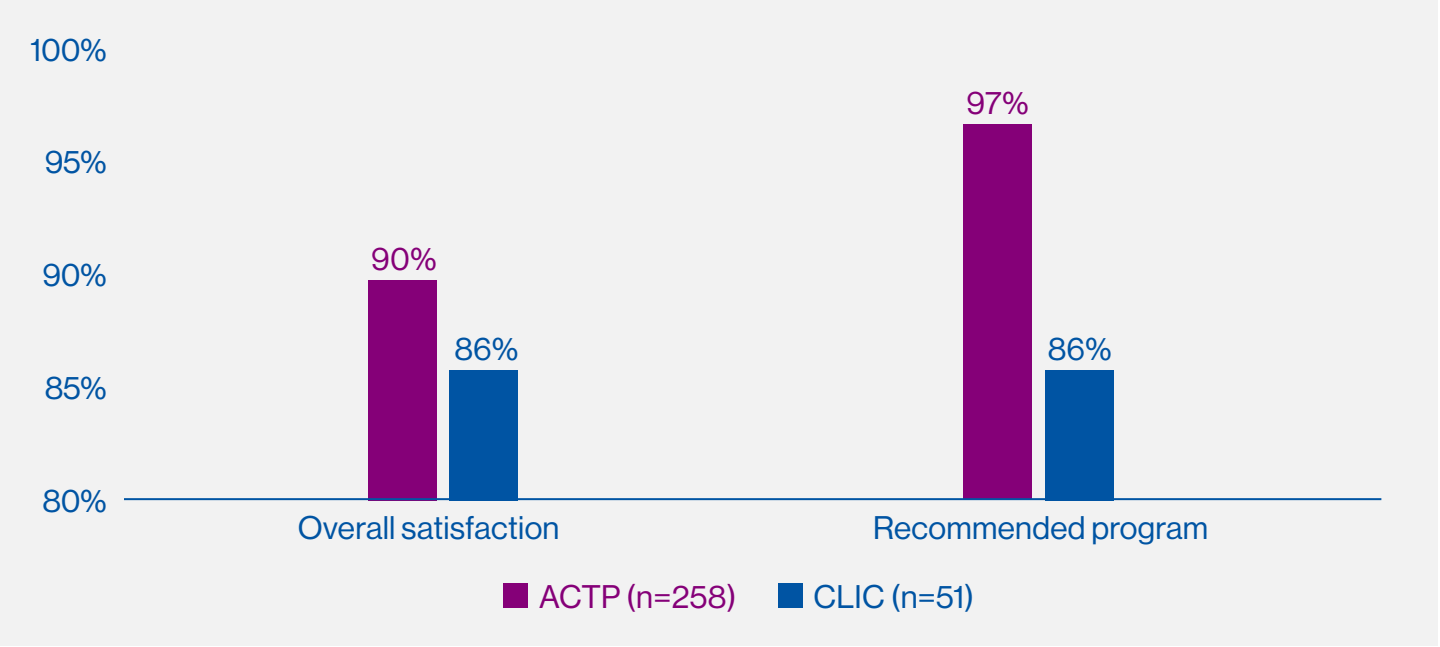
24 ACTP participants were not asked about their overall satisfaction on the withdrawal survey, but they were asked whether they would recommend the course; **73%** (**24/33**) said they were likely, very likely to, or had already recommended the program.

4.2.3. Were learners who completed the program satisfied with CLIC?

Overall satisfaction with CLIC courses

As shown in **Figure 8**, **86%** of exit survey respondents reported satisfaction with CLIC and **86%** would recommend it. These percentages are slightly lower than ACTP's, which achieved satisfaction and recommendation rates of **90%** and **97%**.

Figure 8 | Overall program satisfaction for CLIC and ACTP completers

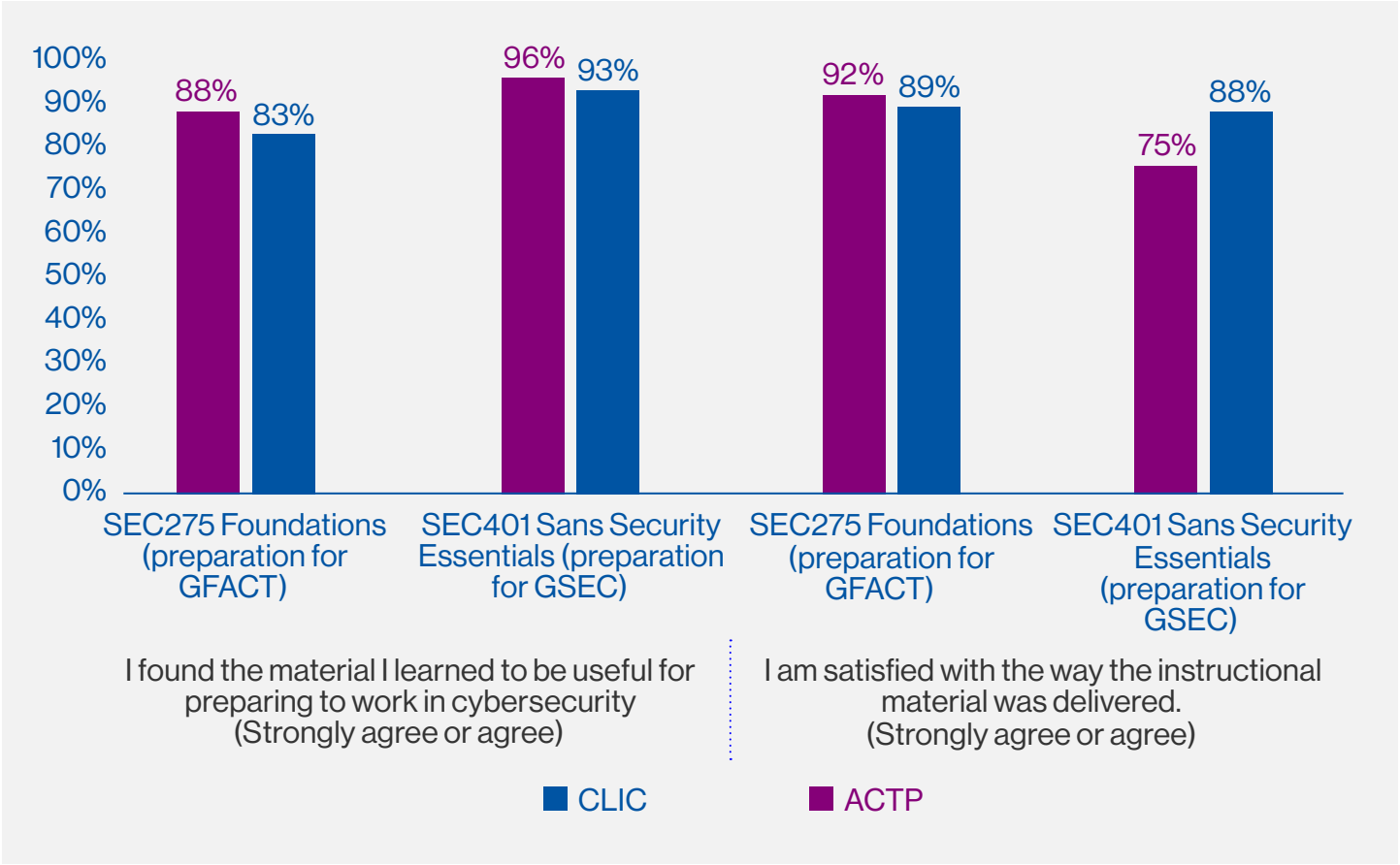


Source. CLIC: exit survey, n=51 | ACTP: n=258

For the Catalyst, these lessons provide a roadmap for refining CLIC to be more effective and sustainable.

As shown in **Figure 9**, CLIC and ACTP respondents who completed the program had similar perceptions of GFACT and GSEC course utility. However, CLIC learners were less satisfied with the way instructional materials were delivered in the GSEC course: at exit, **75%** were satisfied vs. **88%** of ACTP learners.

Figure 9 | Perceived utility of and satisfaction with course materials



Source. CLIC: exit survey | n=51; ACTP: exit survey | n=251-257

CLIC interviewees described the GFACT course as more manageable and easier-to-absorb, especially for those with cyber or IT experience. GSEC introduced more advanced concepts, hands-on labs, and advanced thinking. While the labs helped bridge theory and practice, they also increased the difficulty. Some interviewees noted that grasping the material alone was not sufficient—they needed to be able to apply their knowledge in integrated scenarios to succeed.

> *"The GFACT was more [about] concepts, and if you understood them, you would pass your exam. But the second [course], the labs part—you would fail the exam if you didn't understand the lab. The labs were integrating a lot of concepts at the same time."*
>
> – CLIC learner, interview

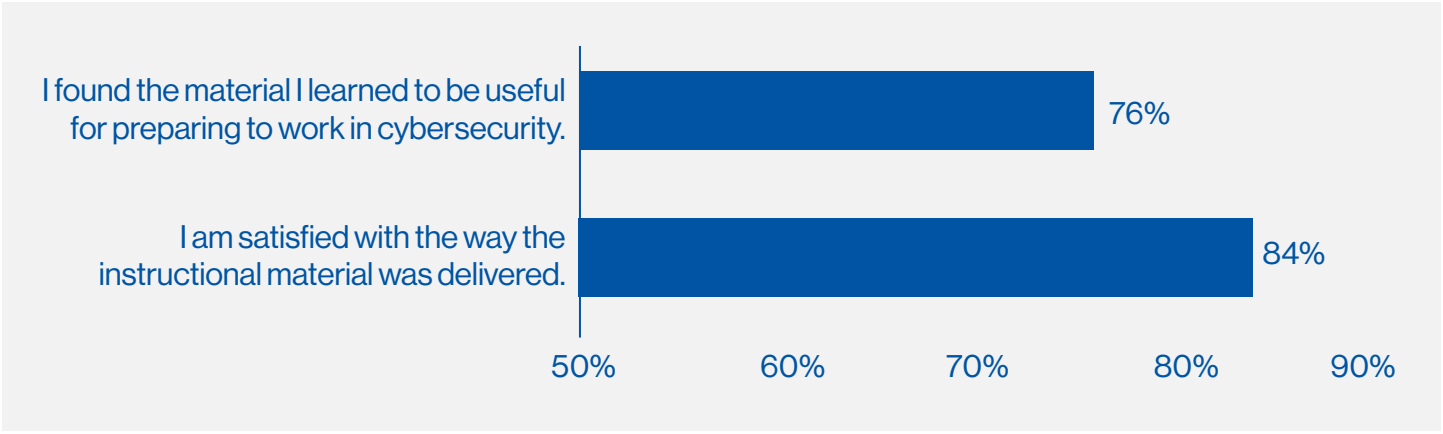
While interviewees appreciated CLIC's self-directed format, they held similar opinions to withdrawers: that CLIC, especially the second half, would benefit from more live instruction, time, and TA-led sessions to help them navigate the labs and prepare for the GSEC exam.

Satisfaction with job search and career supports

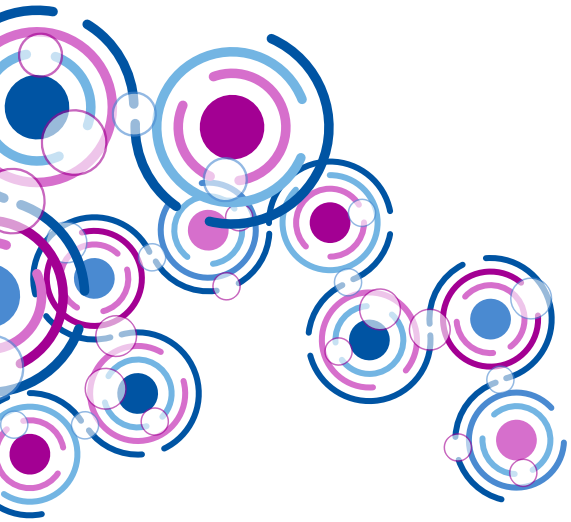
Most CLIC exit survey respondents noted satisfaction with the overall job search and career supports (**76%**) at rates close to those reported by ACTP learners (**79%**).

As shown in **Figure 10**, CLIC learners also found the Professional Practice Course satisfying (**84%**) and useful in their career search (**76%**). This course provides workshops and personalized one-on-one support to assist with job search preparation, including resume development, online profile enhancement (e.g., on LinkedIn), and interview coaching. We do not have comparative data from ACTP learners.

Figure 10 | Perceived satisfaction with and utility of the CLIC Professional Practice Course



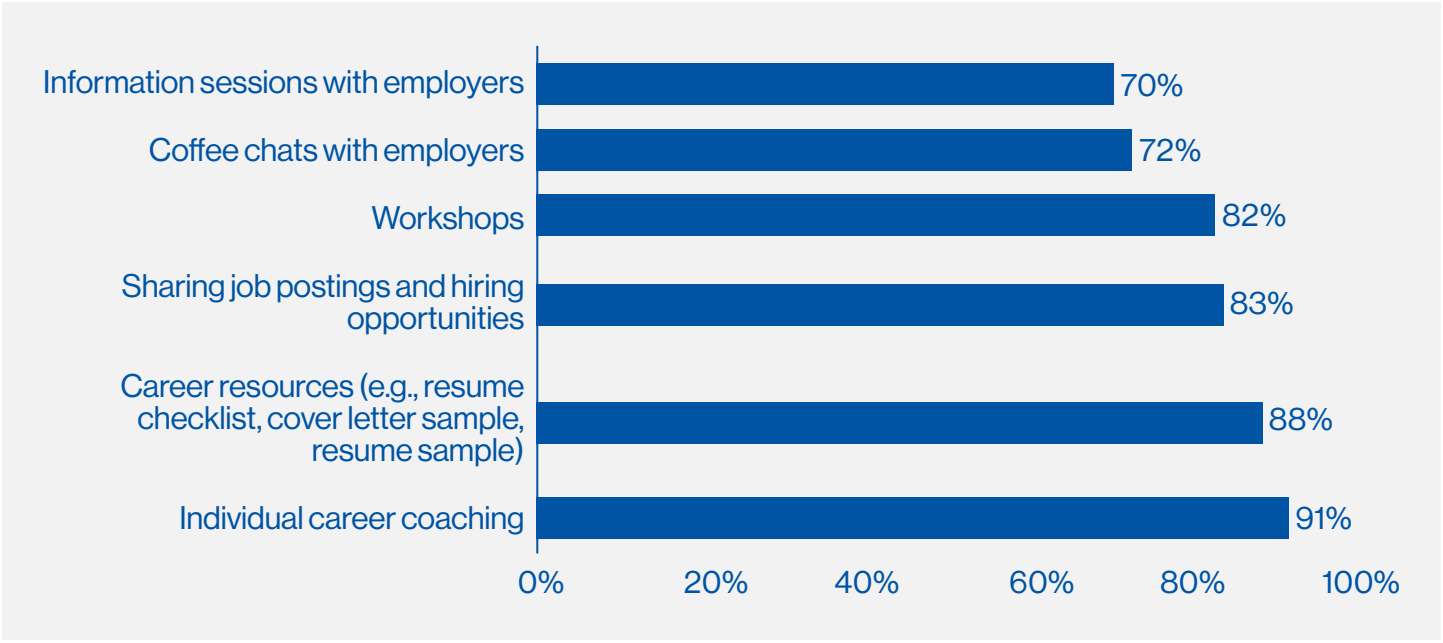
Source. CLIC: exit survey | n=51



For policymakers and practitioners, [CLIC] offer[s] an important case study in the trade-offs involved in sustaining and scaling programs once public funding ends.

As shown in **Figure 11**, CLIC learners were highly satisfied with the one-on-one career coaching (**91%**); resources (e.g., resume and cover letter tailoring) (**88%**); job posting and hiring opportunities (**83%**); and workshops (**82%**). Satisfaction was moderate for employer engagement: **72%** of learners were satisfied with employer coffee chats and **70%** with employer information sessions. As above, we do not have comparative data from ACTP learners.

Figure 11 | Learner satisfaction with CLIC job search and career supports



Source. Exit survey | n=34–49

In interviews and exit survey responses, CLIC learners valued the job board, and in particular its exclusive postings from the Catalyst's employer network. They appreciated that resumes were forwarded directly to employers—reducing competition and leveraging the Catalyst's reputation for high-quality candidates.

> *"I was satisfied with the job search and career support because of the personalized guidance and practical resources. The access to exclusive job listings and employer networks was invaluable, connecting me directly to opportunities in my field."*
>
> – CLIC learner, exit survey

> *"Those [employer] relationships were a big selling point."*
>
> – CLIC learner, interview

However, learners also noted limitations: postings were infrequent, and many roles were mid- to senior-level—not always well-suited to entry-level graduates.

> *"Initially I thought it was great, but [then] I expected more. [Over] two weeks, there's only [been] one role on the job board. I expected at least two or three roles per week."*
>
> – CLIC learner, interview

> *"Ninety-nine percent of [jobs listed] are for senior-level experience. The ones I was most excited about were the Rogers positions, which were provided by CLIC, but there's only five [positions] for each, and [with] previous cohorts, I guess they can apply as well."*
>
> – CLIC learner, interview

Some learners felt the job search support did not match expectations set during recruitment, which emphasized employer connections and employment outcomes.

> *"I did not get invited to any coffee chats with employers. I had one coffee chat opportunity with a CLIC alumnus. I feel like I missed something."*
>
> – CLIC learner, exit survey

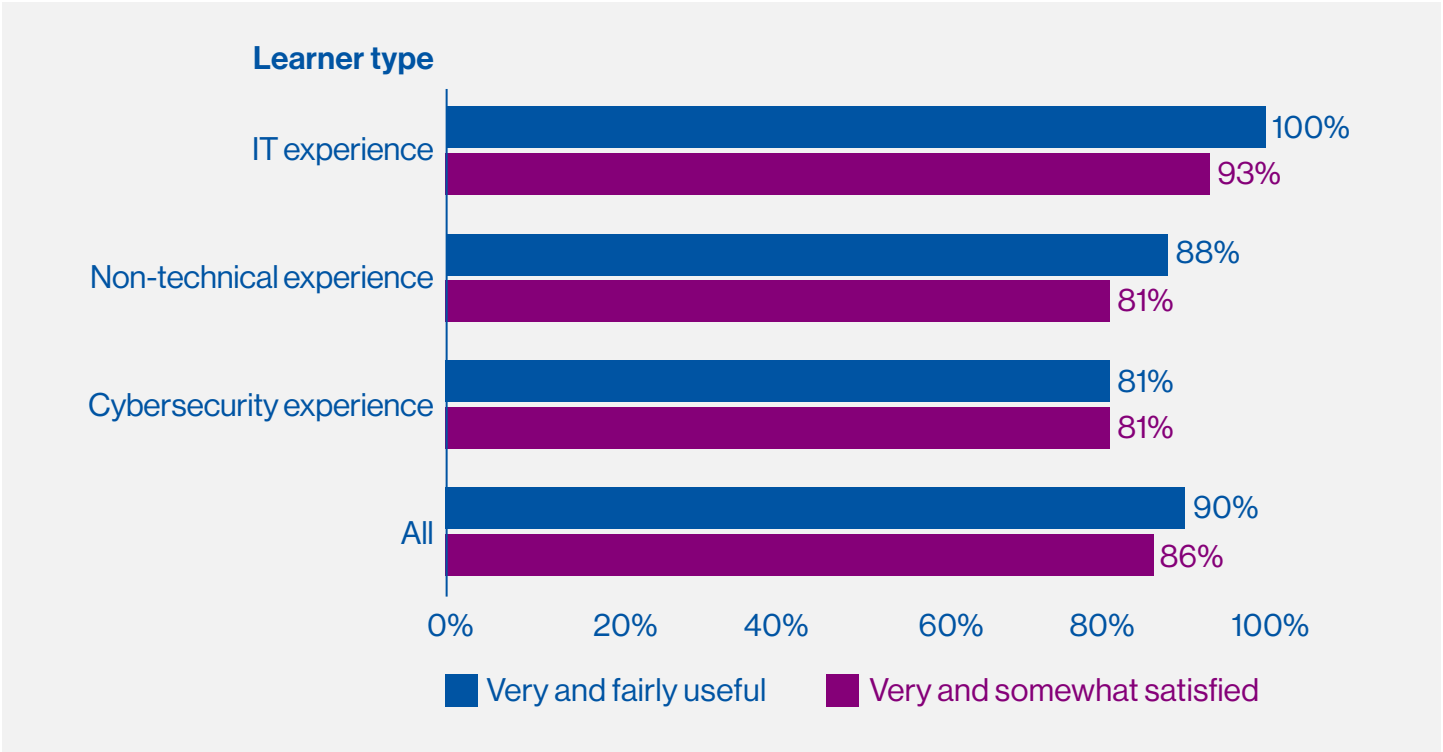
Overall, learners suggested improving employer engagement, expanding job listings, and extending post-program access to job boards and alumni networks to better support graduates.

When that funding ended, the Catalyst faced a challenge common across the skills development landscape: how to sustain a high-value program without external funding support ... this evaluation found that CLIC largely succeeded in this transition.

4.2.3. Were learners who completed the program satisfied with CLIC?

As noted above, overall program satisfaction in CLIC was high (**86%**). When asked about how useful CLIC was in preparing learners for a career in cybersecurity, **90%** responded that it was fairly or very useful. **Figure 12** shows positive response rates for these two questions, disaggregated across our three learner profiles (introduced in **section 4.1.2.**). Learners with some IT or broader technical backgrounds reported slightly higher satisfaction (**93%**) and perceived career utility (**100%**) than those with cybersecurity experience and non-technical experience.

Figure 12 | Learner satisfaction with CLIC job search and career supports



Source: Exit survey | n=51

Learners with IT experience. This group reported the highest satisfaction (**93%**) and perceived utility (**100%**). They found CLIC well-matched to their skills, balancing challenge with support. Although some found the GFACT repetitive, it helped to solidify foundational knowledge. Most agreed the GSEC was demanding as it introduced more advanced topics. Respondents emphasized the importance of time management, especially in the second half of the program, given its intensity.

> *"I found it rewarding. There were times when it was a little bit draining, but overall, you're learning interesting things, refreshing stuff you already know. I could see as I was going through the learnings how they were going to translate to the real world."*
>
> – CLIC learner, interview (IT experience)

Learners with non-technical backgrounds. Among these learners, **81%** reported satisfaction, but they also reported a steeper learning curve. Many struggled to keep pace and grasp complex concepts, especially in the GSEC portion, and expressed a greater need for live instructional support. Despite challenges, **88%** found CLIC useful for preparing for a cybersecurity career and valued the support provided.

> *"Difficult concepts combined with volume made CLIC difficult. For example, I could have spent the entire program working on Python. Sometimes you do end up pushing yourself through without fully understanding concepts or getting yourself to a level of understanding where you can do the exam."*
>
> – CLIC learner, interview (non-technical background)

Learners with cybersecurity experience. This group reported the lowest levels of satisfaction (**81%**) and perceived utility (**81%**) compared to others. While some found the GFACT certification too basic—mostly a refresher with limited new material—the GSEC was seen as insightful, relevant, and challenging, particularly the exam. Interviewees noted that GSEC content had strong real-world applicability and reinforced their knowledge. While some found the pace difficult to manage alongside full-time work, they appreciated and benefitted from the Catalyst's support tools (e.g., study schedule) for staying on track.

> *"I came from a certificate that covered what was in CLIC. I was not in trouble, at least for the GFACT, [but the GSEC] was much harder. But the first one, not at all. I knew exactly what was in the book, and I was like, 'Wow, I can't imagine how it might be for people who have never read a book in cybersecurity.'"*
>
> – CLIC learner, interview (cybersecurity experience)

4.3. Program outcomes

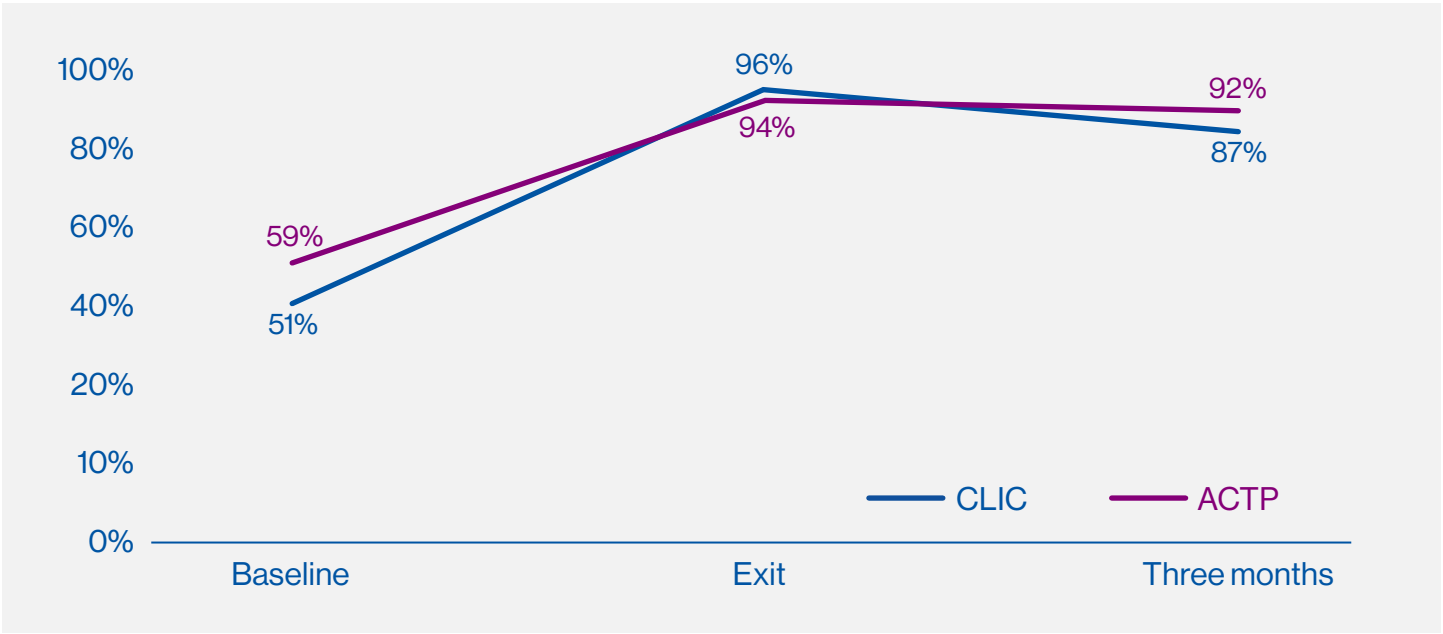
4.3.1. What were the short-term outcomes for CLIC graduates? How did they compare to those of ACTP graduates?

Our study design does not allow us to attribute certain outcomes to CLIC versus other factors (e.g., participation in other training programs, on-the-job experience). Therefore, findings below should be interpreted as correlational rather than causal. Survey attrition and low sample sizes mean data below are unlikely to be representative of all participants and should be interpreted with caution.

Skills, knowledge, and confidence

As shown in **Figure 13**, **96%** of graduates at program exit agreed that they had the skills and knowledge to be successful in a cybersecurity career, with **87%** agreeing at the three-month follow-up. These percentages were comparable to responses from ACTP participants.

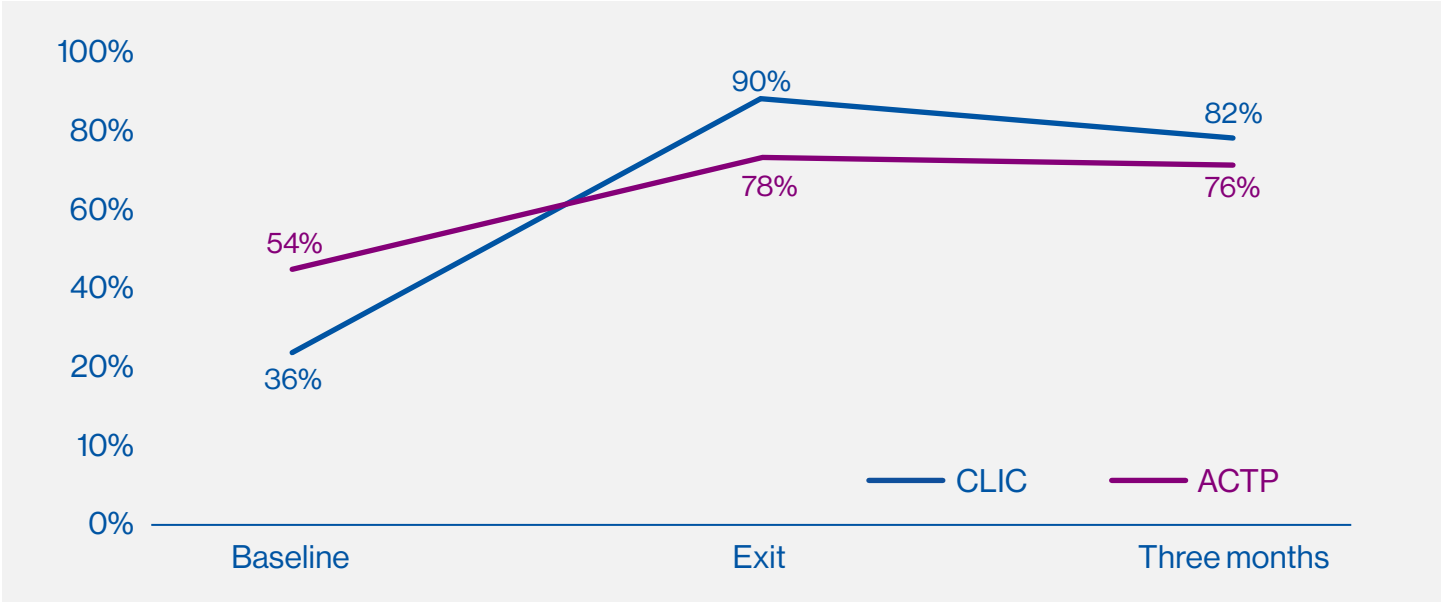
Figure 13 | CLIC and ACTP learners' cybersecurity knowledge and skills at three times



CLIC: baseline n=74; exit n=51; three-month n=39 | ACTP: baseline n=404; exit n=258; three-month n=191

As shown in **Figure 14**, at exit, **90%** of CLIC graduates felt confident in applying for a cybersecurity job. Though it decreased to **82%** three months later, the growth from baseline to follow-up was **46 percentage points** (ppt) (from **36%** to **82%**). ACTP graduates saw more modest growth from **54%** to **76%** (**+22 ppt**) but had a smaller decline in confidence after three months than CLIC (**two** vs. **eight ppt**).

Figure 14 | CLIC and ACTP learner confidence in applying for cybersecurity jobs at three times



CLIC: baseline n=74; exit n=51; three-month n=39 | ACTP: n=402; exit n=258; three-month n=191

CLIC interviewees noted how the technical training, practical application, and tailored job search supports improved their skills and readiness for cybersecurity roles. They built a strong technical foundation in concepts they could confidently discuss with employers. The labs and Cyber Range gave hands-on experience that reinforced learning and helped them feel ready to apply skills in real-life settings. As one learner stated, the labs let them "actually do the work," giving them the ability to speak with authority in interviews for cyber-focused jobs.

> *"I feel more confident when applying to jobs. I know these concepts, I can speak about them, and I can learn about them on the job. So, I feel ready to apply with the idea that if I don't know something, I can learn about it and be able to grasp it."*
>
> – CLIC learner, interview

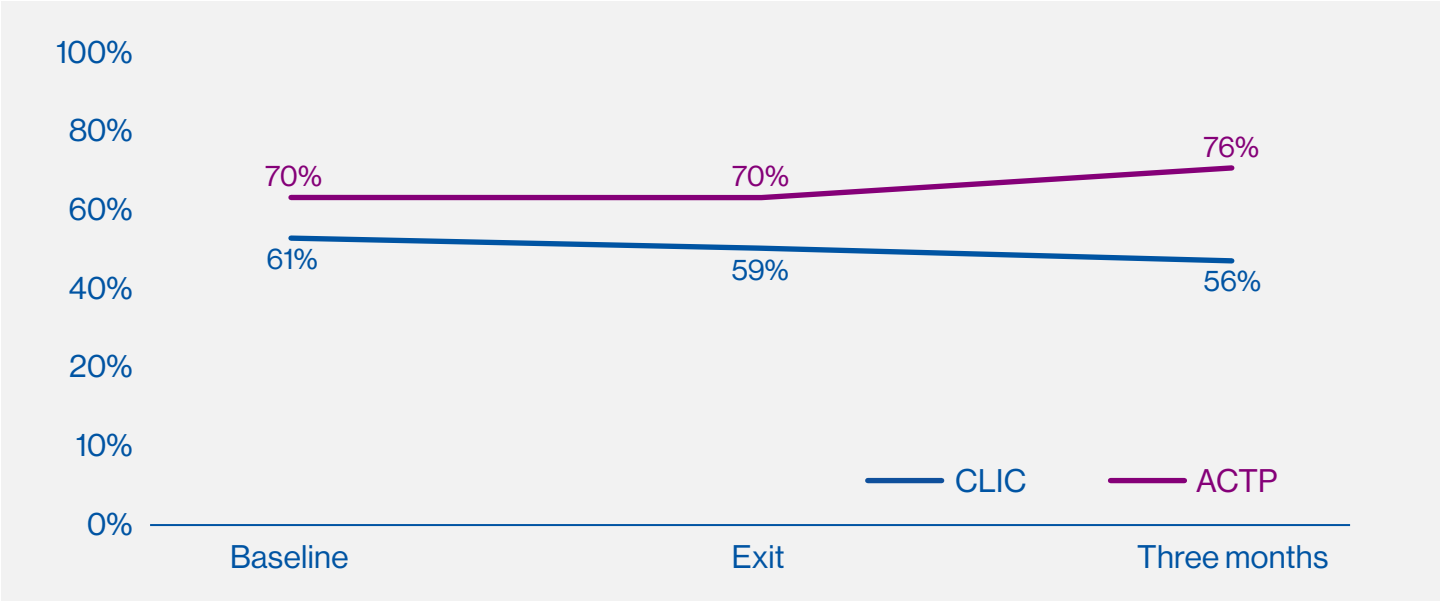
Learners highlighted how career supports (e.g., resume, cover letter, and interview prep) helped build their confidence, assuring them they were submitting strong applications that presented their skills and tailored their backgrounds to relevant roles.

> *"Yes, I feel prepared. I think the GSEC certification prepared us the most, and apart from it, the resume and cover letter writing sessions helped us identify how to make your resume stand out."*
>
> – CLIC learner, interview

Employment and annual salary

In baseline, exit, and three-month follow-up surveys, we asked learners if they were employed or not (without specifying form of employment). As shown in **Figure 15**, CLIC participants reported a small overall *decline* in employment from baseline (**61%**) to follow-up (**56%**). ACTP saw an *increase* in employment from **70%** to **76%** over the same period.

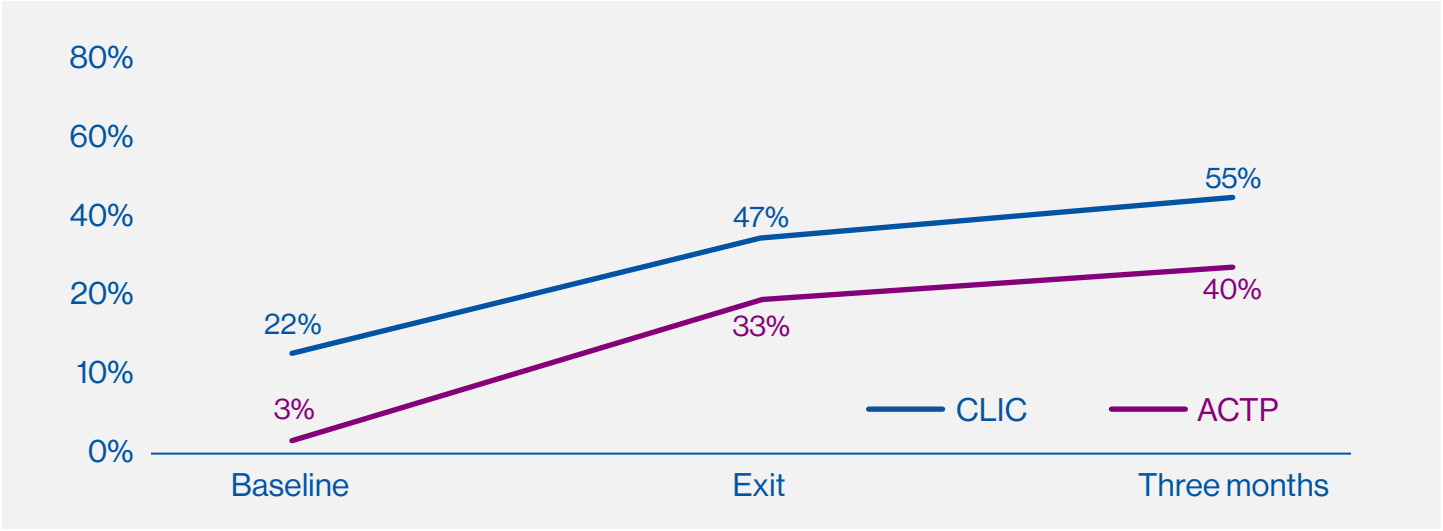
Figure 15 | Employment among ACTP and CLIC learners over time



CLIC: baseline n=82; exit n=51; three-month n=39 | ACTP: baseline n=404; exit n=258; three-month n=192

As shown in **Figure 16**, **55%** of CLIC grads who indicated they were employed three months after the program reported working in cybersecurity—up from **22%** at baseline (**+33 ppt**). ACTP graduates saw a greater increase from **3%** to **40%**, or **37 ppt**.

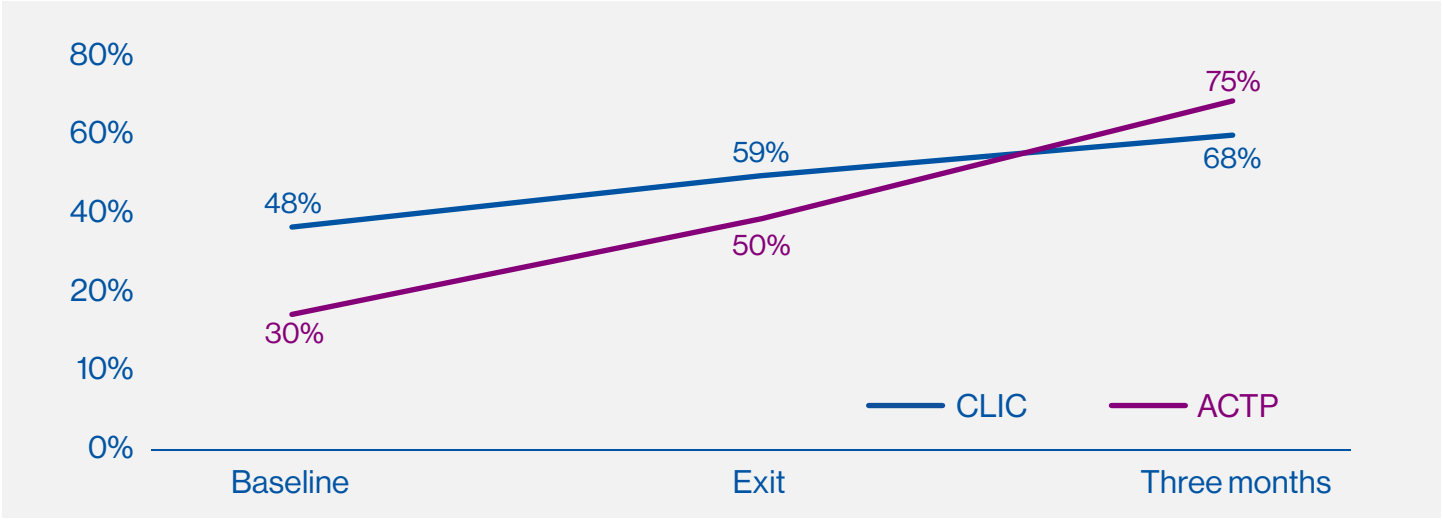
Figure 16 | Employment in cybersecurity among employed CLIC and ACTP learners over time



CLIC: baseline n=50; exit n=30; three-month n=22 | ACTP: baseline n=35; exit n=21; three-month n=120[25]

As shown in **Figure 17**, the number of CLIC graduates reporting earning at least **$60,000** per year grew from **48%** to **68%** by the three-month follow-up (**+20 ppt**): a smaller increase compared ACTP's growth from **30%** to **75%** (**+45 ppt**).

Figure 17 | Percentage of CLIC and ACTP learners earning $60,000 or greater over time



CLIC: baseline n=35; exit n=29; three-month n=22| ACTP: baseline n=387; exit n=247; three-month n=146

25 This question was asked on the intake and exit surveys for ACTP cohort 6. It was asked to all ACTP cohorts on the three-month survey. If we restrict our attention to ACTP cohort 6 at three-months, **59%** (**13/22**) of employed respondents reported having a position related to cybersecurity. Results should be interpreted with caution.

CLIC interviewees appreciated how the program built their skills and confidence, but they noted frustration finding work in the sector. They attributed challenges to labour market conditions beyond the Catalyst's control: competitive markets shaped by layoffs, reduced hiring rates, and caution among employers. Many noted that entry-level opportunities had become scarce, with more positions requiring prior cybersecurity work experience. Some highlighted regional demand for cyber jobs (e.g., within vs. beyond Ontario) or a decline in remote jobs. These issues may also help explain dips in learners' confidence and sense of knowledge about their cybersecurity skills between the exit survey and three-month follow-up.

In focus group discussions, Catalyst staff generally shared these viewpoints, noting that employment outcomes were shaped in part by changing labour market conditions (anticipated in CLIC's theory of change). They described fewer entry-level cybersecurity roles available than in previous years in which ACTP was delivered and CLIC graduates being more particular in choosing their next role.

4.4. Costs

Below, we summarize findings from our cost analysis, which considers how changes in funding sources from ACTP to CLIC affected program delivery costs—and how such changes may influence CLIC's sustainability. A more detailed technical summary has been provided to the Catalyst.

4.4.1. How did funding allocation differ between ACTP and CLIC?

- **The Catalyst increased marketing spend from ACTP to CLIC.** To help build awareness of the program, the Catalyst dedicated financial resources to marketing, reflecting the need to establish a new, tuition-based offering. This cost dropped considerably in CLIC 2 but was still much higher than ACTP's spend.
- **The Catalyst decreased labour costs from ACTP to CLIC with efficiencies, including the Professional Practice Course and leadership and employment team.** Labour structure was leaner in CLIC than in ACTP. During ACTP, the Catalyst was developing content, establishing employer connections, and fulfilling government requirements, which in turn led to greater demands on staff and leadership time. Generally, CLIC had lower per-cohort costs in most labour categories, achieved through the following ways:
  - Existing relationships developed during ACTP allowed the employment team to streamline employer engagement and job search supports.
  - Having built sector-specific knowledge during ACTP, the Catalyst delivered the Professional Practice Course internally, eliminating the need for external instructors and consultants.
  - Other savings came from the greater operational efficiency for program staff, and reducing time required for reporting and administrative tasks associated with government funding. These led to an overall reduction in leadership and staff time.
- **ACTP and CLIC 2 had similar costs per enrolment.** While CLIC 2 reduced labour costs and removed one GIAC certification,

creating opportunities for more efficient delivery, other factors offset these savings. Additional marketing needs and the higher costs of running smaller cohorts meant that overall costs per enrolment remained comparable between ACTP and CLIC.

- **Delivery costs and tuition suggest financial sustainability.** Overall, the cost of delivering CLIC was broadly comparable to the tuition participants paid. In CLIC 1, delivery costs exceeded tuition—unsurprising for a new program that required significant upfront investment, particularly in marketing. In CLIC 2, however, delivery costs fell below the tuition charged. This indicates that the model can, in principle, be financially sustainable on a per-enrolment basis. Due to limitations in the cost data (such as the treatment of partial refunds for withdrawals), we were unable to extend this comparison to cost per completion.
- **Tuition costs were lower than market value of certifications.** The market cost of completing the GFACT and GSEC (including training and exams) directly through the SANS Institute is estimated at **$19,950**. With a tuition fee of **$15,500** + HST (or **$17,515**, total), CLIC learners realized a cost savings of approximately **$2,435** (or **$8,085** for women receiving a bursary from Rogers Communications and RBC). Importantly, learners also received additional Catalyst supports, such as through the job board, Professional Practice Course, and access to career coaches and Cyber Range.

When funding ended, the Catalyst faced a challenge common across the skills development landscape: how to sustain a high-value program without external funding support … this evaluation found that CLIC largely succeeded in this transition.

5. Discussion and conclusions

5.1. Summary of findings

From May 2024 to May 2025, the Catalyst delivered CLIC, a tuition-based program for **135** participants across two cohorts. Targeting women and non-binary people with little or no cybersecurity experience, the program aimed to build skills and foster professional networks needed to gain meaningful employment. This evaluation assessed CLIC's effectiveness compared to its predecessor, ACTP, a government-funded program. Our evaluation showed:

- **Increased investment in marketing to build awareness and attract applicants.** To launch a tuition-based model, the Catalyst invested in marketing to build brand awareness, positioning CLIC as an employment- and career-focused program. Compared to ACTP, CLIC attracted fewer applicants, admitted a larger share, and saw a higher drop-off from admission to program start.
- **Effective engagement of target population.** CLIC reached **96%** of its recruitment target and reached its intended audience of women and non-binary learners (**56%** across two cohorts), recruiting them at approximately three times the rate they are employed in cybersecurity. Consistent with ACTP's equity goals, about **80%** of enrolled learners identified as BIPOC and **62%** were not born in Canada. CLIC also reached a higher proportion of learners with current or previous experience in cybersecurity compared with ACTP. Nearly all (**91%**) participants were motivated to enrol in CLIC by perceived career and employment opportunities.
- **Moderate retention and completion rates.** Post-enrolment, **34%** withdrew (similar to ACTP) and **6%** deferred to the next cohort. Withdrawals were due to personal issues, program structure, and misaligned expectations. **Eighty-two percent** of CLIC learners passed the GFACT exam and **60**% passed the GSEC (and thus completed CLIC). **Seventy-six percent** of ACTP students passed the GSEC and **68%** completed ACTP.
- **Strong satisfaction and perceived usefulness.** Those who completed CLIC reported high satisfaction (**86%**) and were likely to recommend the program (**86%**). Most found courses and certifications useful for preparing for a cybersecurity career, though many suggested adding live instruction, structured TA support, and more time for the GSEC. Most learners were satisfied with career supports, but suggested deeper employer engagement, more relevant job postings, and extended alumni supports. When comparing learner profiles, those with IT experience reported higher satisfaction and perceived utility than those with cybersecurity experience or nontechnical learners.
- **Positive gains in knowledge and confidence.** Among CLIC graduates, **96%** reported they had the skills and knowledge to be successful in a cybersecurity career upon graduation and **90%** of graduates felt confident in applying for a cybersecurity job.
- **Lower employment outcomes compared to ACTP.** CLIC saw mixed employment results. From baseline to three months post-graduation, overall employment among CLIC

learners fell from **61%** to **56%**. However, **55%** of graduates employed three months post-program reported working in cybersecurity—an increase of **33 ppt**—and the share earning **$60,000** increased by **20 ppts**. ACTP graduates experienced stronger gains across all of these measures. CLIC participants and Catalyst staff attributed limited employment progress to weaker market conditions, employer caution, and regional constraints. Survey data on employment outcomes for CLIC should be interpreted with caution due to small sample size and significant attrition.

- **CLIC showed tuition can cover per-learner delivery costs.** As the model shifted from public funding to tuition, the cost mix changed—GIAC licenses remained the dominant fixed expense while new costs (notably marketing and recruitment) emerged—yet CLIC 2 still delivered per-enrolment costs on par with ACTP. It also set tuition below the market price of the equivalent certifications.

5.3. Discussion

CLIC tested whether a publicly funded training model could transition into a sustainable, tuition-based program without sacrificing quality, access, or outcomes. Our results show high learner satisfaction, valuable skills development, and the potential for financial sustainability (i.e., tuition covered cost per enrolment). CLIC preserved several elements of the core learning experience and continued to support underrepresented groups while introducing new employment supports, like dedicated career coaching.

At the same time, findings suggest some opportunities for stronger alignment between what the program delivers and the needs of candidates, learners, and employers. These elements may be considered as part of continuous quality improvement processes—typically involved in the business operations of any high-quality training program.

Alignment between learner background and program design

Learners' experiences with CLIC varied depending on their prior training and experience. For participants from non-technical backgrounds, the program's pace and intensity—especially the GSEC component—were particularly challenging, with many requesting extensions or withdrawing due to difficulty with the self-directed format. By contrast, learners with prior cybersecurity experience sometimes found the introductory GFACT material less valuable.

These findings highlight the challenge of meeting the needs of both entry-level and more experienced learners within a single program. Going forward, segmenting participants by background and tailoring supports—for example, by offering additional scaffolding for non-technical learners or more advanced options for experienced participants—could help ensure the program delivers value across its diverse learner base.

Alignment between graduate competencies and employer expectations

CLIC significantly expanded career supports compared to ACTP—introducing one-on-one coaching, curated job boards, and priority resume forwarding. These services helped graduates feel confident and prepared to pursue roles in the sector.

However, early outcome data indicate that CLIC graduates were less likely than ACTP peers to secure employment within three months. While our study did not include direct input from cybersecurity employers, evidence suggests that labour market shifts—toward more experienced and mid-senior roles, with fewer entry-level opportunities—may have contributed to these results.

Further research with employers would help identify the specific barriers to hiring CLIC graduates. Factors may include limited awareness of the program, uncertainty about whether certifications and the Cybersecurity Week experience sufficiently demonstrate job-readiness, or a mismatch with evolving role requirements. Addressing these issues would allow the Catalyst to refine CLIC and strengthen hiring outcomes.

5.3. Conclusion

ACTP demonstrated how a government-funded program—free to participants—addressed an urgent labour market shortage while advancing equity in a sector that continues to underrepresent women, newcomers, and BIPOC professionals. With high satisfaction and strong early employment outcomes, ACTP established itself as a model for inclusive skills development programs in cybersecurity.

When that funding ended, the Catalyst faced a challenge common across the skills development landscape: how to sustain a high-value program without external funding support. CLIC was their response—a tuition-based (or participant-funded) model that sought to maintain quality, equity, and impact.

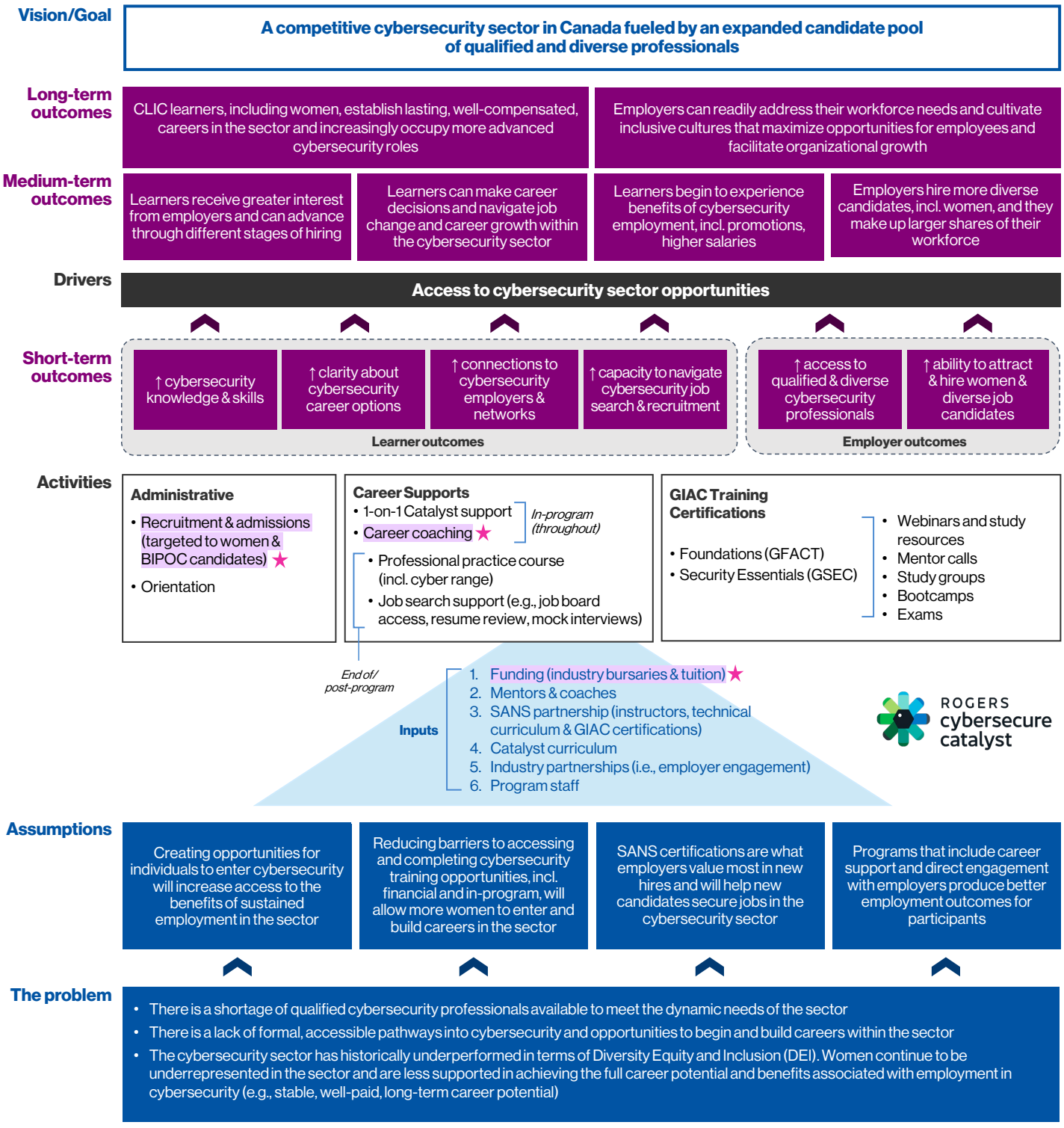
This evaluation found that CLIC largely succeeded in this transition. Learners reported high satisfaction and improved skills and confidence in a continuously evolving labour market. The program maintained access for underrepresented groups, introduced new career supports, and continued to deliver industry-recognized credentials at below-market costs.

Savings found in labour and the reduced number of certifications were offset by new expenses needed for marketing, recruitment, and smaller cohort sizes. While tuition covered the per-enrolment cost of delivery, sustainability will depend on whether learners continue to see value in the certifications, employer networks, and job opportunities. Charging tuition also influenced who applied for CLIC; this requires ongoing attention to cohort composition and alignment between learner backgrounds, certifications, and labour market needs.

CLIC demonstrates both the promise and the complexity of pivoting from a fully funded to a tuition-based model. For the Catalyst, these lessons provide a roadmap for refining CLIC to be more effective and sustainable. For policymakers and practitioners, they offer an important case study in the trade-offs involved in sustaining and scaling programs once public funding ends. In practice, doing so requires more than financial engineering; it requires careful design choices that preserve equity, maintain quality, and adapt to market realities, in addition to lowering costs for long-term success.

Appendix A

Figure A1 | CLIC theory of change



Note. Changes from ACTP are highlighted in pink.

Appendix B

Table B1 | CLIC curriculum details

Course	Description	Certification and Key Focus Areas
SANS SEC275 – Security Foundations	SEC275 equips participants with essential skills in computers, technology, and security, forming a strong foundation for a cybersecurity career. The course offers hands-on labs and exercises designed by experts using the latest techniques. By completion, learners gain both theoretical knowledge and practical expertise to engage with industry professionals confidently.	Prepares learners for the GIAC Foundational Cybersecurity Technologies (GFACT) exam. Key focus areas include: • Computer components and concepts • Operating systems, containers, and virtualization • Linux • Networking fundamentals • The Web: Search engine and servers • Practical programming – Python and C Windows Foundations • Advanced computer hardware (e.g., CPU and memory) • Encryption • Introduction to basic security concepts • Introduction to forensics • Introduction to reconnaissance, exploitation, and privilege escalation • Introduction to network and computer infiltration (e.g., lateral movement)
SANS SEC401 – Security Essentials: Network, Endpoint, and Cloud	SEC401 provides foundational and advanced security skills for protecting critical information across networks, endpoints, and cloud environments. Designed for both newcomers and experienced professionals, the course emphasizes applying security concepts through a modern defensive strategy. It includes over 18 hours of hands-on training to deepen technical proficiency.	Prepares learners for the GIAC Security Essentials (GSEC) Network Security and Cloud Essentials exam. Key focus areas include: • Vulnerability management and response • Data security technologies • Windows and Azure security • Linux, AWS, and Mac security

Course	Description	Certification and Key Focus Areas
Cybersecurity Professional Practice Course	This course expands participants' understanding of cybersecurity beyond technology, focusing on its impact on business operations, decision-making, and risk management. Designed to complement technical training, it integrates industry feedback and employer insights. Interactive sessions develop key competencies such as strategic thinking, compliance, communication, and teamwork, offering a competitive edge in the cybersecurity field.	Key focus areas include: • Cybersecurity organizational strategy • Cybersecurity and compliance • Cybersecurity ethics • Cybersecurity global contexts • Communicating cybersecurity issues • Business perspectives in cybersecurity • Onboarding into a cyber team
Experiential Learning: Catalyst Cyber Range	CLIC students engage in hands-on cybersecurity exercises within the Catalyst Cyber Range, a simulated corporate environment. Participants respond to realistic cyber threats, including an Incident Response + Ransomware scenario, experiencing both offensive and defensive roles. They infiltrate servers like a hacker, then counteract attacks using commercial security tools. Led by an expert instructor, each session includes an orientation and debrief for maximum learning impact.	Key focus areas include: • Experience of an actual cybersecurity incident (safely) • Hands-on experience using commercial tools • Preparation for job interviews with practical experience • Applying skills practically

Source. CLIC Program Package

Table B2 | ACTP curriculum details

Course	Description	Certification
SANS SEC275 –Foundations: Computers, Technology and Security	Students developed fundamental skills and knowledge in key IT subject areas, such as computer components and concepts, operating systems, containers and virtualization, Linux, networking fundamentals, Python and C, Windows foundations, advanced computer hardware, encryption, basic security concepts, forensics, reconnaissance, exploitation, and privilege escalation, and network and computer infiltration.	Prepared learners for the GFACT (GIAC Foundational Cybersecurity Technologies) exam, which was taken as part of the training program.
SANS SEC401 – Security Essentials: Network, Endpoint, and Cloud	Taught advanced cyber defense skills, such as access control, incident response, network security, DNS, TCP-IP, disaster recovery, security policy, defense-in-depth, windows security, and Unix/Linux security. Examples of tools participants gained skills with included TCP Dump, Wireshark, John the Ripper, Nmap, Packet Analyst, Snort, Tripwire, Powershell, and Process Hacker.	Prepared learners for the GSEC (GIAC Security Essentials Certification) exam, which was taken as part of the training program.
Hacker Techniques, Exploits, and Incident Handling	Taught advanced incident handling and hacker tool techniques in areas such as incident response, reconnaissance, malware, web application security, penetration testing, and vulnerability assessment. Participants learned to understand attackers' tactics and strategies in detail, giving them experience in identifying vulnerabilities and discovering intrusions. They learned about common attack techniques, vectors, and tools and defending/responding to such attacks. Examples of skill areas and tools learned include memory analysis, Metasploit attack and detect, Nessus, SQL injection, cross-site scripting, Windows command line kung-fu, DOS attacks, and Linux attack detection.	Prepared learners for the GCIH (GIAC Certified Incident Handler) exam, which was taken as part of the training program.
Cybersecurity Professional Practice Course	Provided participants with a broadened understanding of the cybersecurity landscape and a recognition that cybersecurity issues go far beyond technology. Participants will recognize how cybersecurity impacts business operations, decision making, strategic planning, and assessments of overall corporate risk and governance. Participants will also learn new ways of thinking and problem-solving in team-based environments	

Source. Accelerated Cybersecurity Training ProgramAppendix A

Appendix C

Table C1 | Common outcomes framework

	Outcome	Indicators
Socio-demographics	Sex & gender	Sex at birth
		Self-identified gender
	Age	Age
	Location	Province
		Region and municipality
	Marital status	Marital status
	Children & dependents	Children | Dependents | Household size
	Household Income	Household income
	Education	Highest credential obtained
		Location of highest credential attainment
	Indigenous identity	Self-identified Indigenous identity
	Francophone status and languages spoken	First language spoken
		Official languages
		Language spoken at home
		Other languages spoken (at home)
	Citizenship status	Place of birth
		Year of arrival
		Citizenship status
	Racial identity	Self-identification as member of racialized group
	Disability	Self-identified disability
Employment status and history	Employment	Employment status
		Nature of employment (permanent, temporary, full/part-time)
	Earnings	Hours worked per week
		Wages
		Annual earnings
	Industry and occupation of employment	NAICS code of job
		NOC code of job
	Work history	Time since last employed
		NOC code of job
		NAICS code of job
	Income source	Income sources

	Outcome	Indicators
Intermediate outcomes	Program completion	Successful completion of planned activities
	Participant satisfaction	Satisfaction with program
		Perceived utility of Program
		Likelihood to recommend
Customized intermediate outcomes	Skills gains	Measured gains in specific skills
	Program-specific credential attainment	Attainment of program-specific credentials
Long-term outcomes	Employment and retention	Employment status
		Nature of employment (permanent, temporary, full/ part-time)
		Retention
	Earnings	Hours worked / week
		Wages
		Annual earnings
	Benefits	Presence of benefits including paid leave, health and dental coverage, pension plan
	Industry and occupation of employment	NAICS code of job
		NOC code of job
	Job satisfaction	Satisfaction with job
		Perceived opportunity for career advancement
		Perceived job security
	Enrolment in further education	Enrolment in further education
		Type of training
		Field of study
	Credential attainment	Attainment of high school or PSE credentials
		Field of study credentials

Endnotes

i Natalucci, F., Qureshi, M. S., & Suntheim, F. (2024, April 9). Rising cyber threats pose serious concerns for financial stability. *IMF Blog*. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

ii The Conference Board of Canada. (2022). *Strengthening Canada's digital defences: A cybersecurity playbook*. https://www.conferenceboard.ca/product/strengthening-canadas-digital-defences-a-cybersecurity-playbook/

iii ISC2. (2023). *ISC2 cybersecurity workforce study.* https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf

iv Public Safety Canada. (2023). *Cyber careers within the Government of Canada.* Government of Canada. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cbr-crr-wrnss/index-en.aspx

v Herron, C., & Quan, T. (2022). *Cybersecurity talent development: Protecting Canada's digital economy.* Information and Communications Technology Council (ICTC). https://ictc-ctic.ca/reports/cybersecurity-talent-development

vi In 2024, there were 2,900 unfilled job postings for Information Security roles alone. See:

Canadian Cybersecurity Network News. (2024). *Cybersecurity job market analysis 2024: Key findings and insights.* https://canadiancybersecuritynetwork.com/cybervoices/cybersecurity-job-market-analysis-2024-key-findings-and-insights

vii This represents $900M in GDP. See: Innovation, Science, and Economic Development Canada. (2022). *State of Canada's cybersecurity industry.* https://ised-isde.canada.ca/site/aerospace-defence/sites/default/files/attachments/2022/State_Cybersecurity_eng_0.pdf

viii Fourrage, L. (2025). *Canada cybersecurity job market: Trends and growth areas for 2025.* Nucamp. https://www.nucamp.co/blog/coding-bootcamp-canada-can-canada-cybersecurity-job-market-trends-and-growth-areas-for-2025

ix The Conference Board of Canada. (2022).

x Herron, C., & Quan, T. (2022). *Cybersecurity talent development: Protecting Canada's digital economy.* ICTC. https://ictc-ctic.ca/reports/cybersecurity-talent-development

xi Bradley, T. (2024). The cybersecurity burnout crisis is reaching the breaking point. *Forbes*. https://www.forbes.com/sites/tonybradley/2024/10/15/the-cybersecurity-burnout-crisis-is-reaching-the-breaking-point/

xii The average cybersecurity analyst salary in the U.S. exceeds Canadian compensation by more than 50%—a key driver of cross-border attrition. See:

Masse, B. (2025, January 29). Here's how Canadian tech salaries compare to the U.S. *The Logic*. https://thelogic.co/news/usa-canada-tech-salaries/

Herron & Quan. (2022).

xiii In-demand certifications include CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), CEH (Certified Ethical Hacker), CCNA (Cisco Certified Network Associate), and CCSP (Certified Cloud Security Professional). See:
Canadian Cybersecurity Network. (2024). Canada's cybersecurity challenge: Over-reliance on advanced certifications. *Yahoo! Finance.* https://ca.finance.yahoo.com/news/canadas-cybersecurity-challenge-over-reliance-101905324.html
ISC2. (2023).
Herron & Quan. (2022).

xiv Ivus, M., & Watson, M. (2022). *Gender equity in Canada's tech ecosystem: Attracting, retaining, and supporting entry- and mid- level talent.* Information and Communications Technology Council. https://ictc-ctic.ca/sites/default/files/ictc-admin/resources/admin/ict001genderreportdesignfnl-2.pdf

xv Herron and Quan. (2022).

xvi McKinsey & Company. (2023). *Diversity matters even more: The case for holistic impact.* https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-matters-even-more-the-case-for-holistic-impact

xvii Korn Ferry. (2024). *How diverse teams increase innovation and growth.* https://www.kornferry.com/insights/featured-topics/diversity-equity-inclusion/how-diverse-teams-increase-innovation-and-growth

xviii The Conference Board of Canada. (2021).

xix Microsoft Security. (2019). CISO series: Better cybersecurity requires a diverse and inclusive approach to AI and machine learning. *Microsoft Security Blog*. https://www.microsoft.com/en-us/security/blog/2019/07/31/ciso-series-cybersecurity-requires-diverse-inclusive-ai-machine-learning/

xx Herron and Quan. (2022).

xxi Herron and Quan. (2022).

Future Skills Centre | Centre des Compétences futures

Blueprint

Canada