Toronto Metropolitan University

ROGERS cybersecure catalyst

Future Skills Centre | Centre des Compétences futures

# Preserving foundational skills in AI-enabled early-career cybersecurity work

*Final insights and recommendations from employer engagement and pilot testing across Canada*



Funded by the Government of Canada's Future Skills Program | Canada










Funded by the
Government of Canada's
Future Skills Program



# Introduction

Rogers Cybersecure Catalyst led a national developmental research project, Preserving Foundational Skills in AI-Enabled Early-Career Cybersecurity Work, which was funded by the Government of Canada's Future Skills Program. The initiative examined how AI is transforming early-career cybersecurity work and identified the foundational skills, competencies, and workforce development approaches needed to prepare Canadians for an AI-enabled future of work.

The project was grounded in an initial hypothesis that AI-enabled workflows may reduce opportunities for early-career professionals to develop and refine foundational skills through hands-on practice and repeated exposure to core technical tasks and workflows. This hypothesis was informed by the Catalyst's experience preparing thousands of learners for cybersecurity careers and ongoing engagement with employers who have reported changing expectations for entry-level talent as AI-enabled tools become more prevalent within cybersecurity operations.

The insights gathered directly informed the project's pilot training programs, which served as a rapid response to the challenges employers identified and allowed us to quickly test practical approaches for developing, preserving, and assessing the foundational skills employers considered most important.

This final report brings together the complete findings across the project journey. It concludes with recommendations and next steps for employers, training providers, and policymakers on supporting foundational skill development in an increasingly AI-enabled cybersecurity workforce.

# Methodology

The project examined how AI is transforming early-career cybersecurity work and the foundational skills, competencies and workforce development approaches needed for an AI-enabled future of work.

The project began with a hypothesis that AI-enabled workflows may reduce opportunities for early-career professionals to develop foundational skills through hands-on practice and repeated exposure to core technical tasks. To explore this, the Catalyst conducted more than 25 semi-structured consultations with employers and senior industry experts across Canada, representing a range of sectors, organization sizes, levels of AI adoption and geographic regions.

Findings from these consultations were further validated and refined through roundtables with more than 100 employers and cybersecurity professionals in Toronto, Vancouver and Yellowknife. Insights from this engagement informed an employer-informed Skills Transformation Framework and two pilot training iterations involving 55 early-career cybersecurity professionals. The pilots tested practical approaches to developing, preserving and assessing foundational skills in AI-enabled environments.

Findings from the consultations, roundtables and pilot programs were brought together to inform the recommendations and next steps outlined in this report for employers, training providers and Policymakers.

# What we heard from employers

## AI Adoption Remains Uneven Across Organizations

While interest in AI is widespread, employers reported significant variation in adoption, implementation, governance maturity, and workforce readiness. Some organizations described highly AI-enabled cybersecurity environments, while others remain in early experimentation or policy-development stages. As a result, the impact of AI on workflows, hiring expectations, and workforce development is occurring at different speeds across the cybersecurity ecosystem.

---

## AI is Enhancing Productivity in Early-Career Cybersecurity Workflows

Across employers who are already integrating AI-enabled tools into their cybersecurity workflows, there is consistent agreement that AI is improving operational efficiency, particularly within Security Operations Centre (SOC) environments.

**Employers described AI-enabled tools as:**

- Reducing triage and investigation time
- Providing contextual summaries of alerts and activity
- Helping teams manage larger volumes of work
- Supporting operational scalability

Employers provided examples ranging from AI-assisted alert triage and investigation support within Security Operations Centres (SOCs) to automated summarization of security events, recommendations for next investigative steps, and accelerated documentation and reporting activities. While the maturity of these implementations varied, organizations consistently reported productivity gains in routine and repeatable workflows.

While long-term impacts are still emerging, employers noted that AI is already reshaping workflows and expectations for junior talent.




*Preserving foundational skills in AI-enabled early-career cybersecurity work*

## Early-career professionals are increasingly expected to perform more advanced analytical and investigative work earlier in their careers

A significant theme emerging across consultations is the changing nature of entry-level cybersecurity work.

Employers noted that many traditional Level 1 responsibilities, including ticket triage, query writing, and incident timeline creation, are increasingly becoming automated or AI-assisted.

Early-career professionals are increasingly expected to perform more advanced analytical and investigative work earlier in their careers, often leveraging AI-enabled tools to support portions of the investigative process. Several employers described these roles as operating at a “Level 1.5” rather than a traditional entry-level capacity, requiring stronger judgment, investigation, and contextual understanding.

**Employers also described a shift in workflows:**

- From manual triage toward AI-assisted investigation
- From manually writing queries to validating AI-generated outputs
- From task execution toward oversight, reasoning, and decision-making

This shift is contributing to what many employers describe as an “entry-level paradox,” in which organizations increasingly seek job-ready candidates while traditional entry-level learning opportunities continue to evolve. Several employers described cybersecurity as increasingly becoming a “second-job profession,” in which foundational IT and systems experience is viewed as critical to effective cybersecurity investigation and decision-making.



## Foundational Technical Knowledge and Applied Professional Competencies Remain Essential as AI Adoption Evolves

When asked how skills are changing, which capabilities are here to stay, and which may evolve in AI-enabled cybersecurity environments, employers were strongly aligned on the core capabilities required for effective early-career cybersecurity performance. Employers consistently identified two broad categories of foundational competencies they look for in early-career talent. Employers believed these competencies would remain essential as AI adoption evolves.

### Foundational technical knowledge

- Networking fundamentals (e.g., DNS, DHCP, HTTP)
- Systems and infrastructure understanding
- Cybersecurity fundamentals and investigative processes

### Applied professional competencies within cybersecurity contexts

- Critical thinking
- Communication
- Prioritization and decision-making
- Investigative logic
- Explainability and reasoning
- Stakeholder communication
- Adaptability and professional judgment

Importantly, employers consistently emphasized that these applied capabilities are not secondary “soft skills,” but core competencies that underpin effective cybersecurity performance.

Across consultations, employers emphasized that cybersecurity increasingly operates as both a technical and business function. As AI reshapes portions of technical work, employers are placing growing importance on judgment, communication, business awareness, and enterprise readiness.

Many employers also expressed the view that these human-centered capabilities will remain essential and may become even more important in AI-enabled cybersecurity environments, particularly as organizations continue emphasizing human oversight and decision-making.

Roundtable participants added that foundational knowledge becomes more meaningful when it is connected to a real operational context. Participants emphasized the value of gaining technical or operational experience before or alongside deeper cybersecurity specialization and identified rotations and cross-functional exposure as possible ways to build systems understanding, judgment, professional networks, and enterprise awareness

## AI is Shifting How Skills are Applied

While foundational skills remain essential, employers consistently noted that the way these skills are applied is evolving.

**Examples raised during consultations included:**

- Query writing is shifting from manual creation toward the validation of AI-generated outputs
- Analysts are increasingly expected to verify AI recommendations and identify inaccuracies
- Growing emphasis on explainability and the ability to justify decisions without relying solely on AI-generated responses

**This shift is driving demand for capabilities such as:**

- AI literacy
- Hallucination detection and validation
- Understanding AI-enabled and agentic systems
- Operating effectively within AI-augmented environments while maintaining human oversight

Across conversations, employers consistently emphasized that cybersecurity readiness is increasingly demonstrated by the ability to analyze, interpret, validate, and act — not simply execute predefined tasks. Several employers also noted that demonstrating these capabilities is becoming more challenging through traditional assessments alone, particularly as AI tools become increasingly embedded in day-to-day work. This concern contributed to broader discussions around evolving approaches to hiring, assessment, and proof of readiness.

Roundtable participants emphasized that validating AI means more than catching an obvious mistake. Early-career cybersecurity professionals need the curiosity and confidence to ask better questions, think independently, and know when an answer needs to be challenged or investigated further.

---

## Skills That Require Consistent Practice May Become Harder to Develop

Employers consistently identified several foundational capabilities that may become more difficult to develop as opportunities for hands-on practice evolve.

**Areas of concern raised during consultations included:**

- Erosion of foundational technical knowledge
- Decline in manual analysis and investigative troubleshooting skills
- Weakening investigative logic and understanding “the why” behind alerts
- Reduced opportunities to develop critical thinking and analytical reasoning
- Weakening communication and explainability skills
- Reduced curiosity and exploratory learning

A recurring theme was the potential for “loss of practice,” in which reduced exposure to foundational technical tasks may limit early-career professionals' opportunities to build a deeper understanding through repeated hands-on experience.

Several employers raised concerns that individuals may increasingly be able to complete tasks without fully understanding the underlying systems or reasoning behind them.

# Implications for Hiring, Training, and Assessment

## *Implications for Hiring*

### The Entry-Level Paradox

Employers consistently emphasized growing tension between hiring expectations and available entry pathways into cybersecurity roles.

Organizations increasingly expect early-career professionals to arrive job-ready while requiring prior IT or operational experience to access many entry-level roles.

As AI changes portions of traditional Level 1 work, employers raised questions around how early-career professionals will continue to gain foundational operational experience.

---

### Limitations of Traditional Assessment and Hiring Approaches

Employers consistently raised concerns about the limitations of traditional hiring and assessment approaches in AI-enabled environments.

Several organizations noted that candidates increasingly rely on AI tools during interviews, technical assessments, certifications, and day-to-day technical tasks.

As a result, employers expressed growing interest in more applied approaches to assessing readiness, including:

- Proof of work and technical portfolios
- Simulation-based and scenario-based assessments
- Assessments completed both with and without AI assistance
- Evaluation of reasoning, explainability, and decision-making

Several employers emphasized that certifications and theoretical knowledge alone are no longer viewed as sufficient indicators of readiness.

---

### Hiring for potential alongside current skills

Roundtable discussions further expanded on this theme by suggesting that employers may need to shift from a place of hiring for skills alone to hiring for potential. As the pace of technological change accelerates, roundtable participants highlighted curiosity, judgment, critical thinking, problem-solving, and a willingness to learn as important indicators of an individual's capacity to develop and adapt over time. This may require hiring approaches that assess not only what candidates can demonstrate at the point of hiring but also their ability to learn, reason through unfamiliar problems, and adapt as the technologies and demands of cybersecurity roles continue to evolve.

# Implications for Training and Assessment

A strong theme emerging across consultations is the need for more practical, applied, and scenario-based learning and assessment models.

**Areas of concern raised during consultations included:**

- Testing skills with and without AI assistance
- Evaluating the ability to verify and challenge AI outputs
- Emphasizing explainability, reasoning, and judgment
- Prioritizing proof of work over credentials alone
- Creating opportunities for hands-on investigative problem-solving

**Examples discussed during consultations included:**

- AI validation scenarios
- Explainability exercises for non-technical audiences
- Applied troubleshooting and investigation assessments
- Dual-mode assessments completed with and without AI assistance

Many employers also highlighted growing interest in portfolios, simulations, and real-world scenarios as more authentic indicators of readiness than certifications alone.

---

## Pilot testing: translating employer insights into practice

To respond quickly to the challenges identified by employers, the Catalyst designed a two-day pilot program to test practical approaches for developing, preserving, and assessing foundational skills in AI-enabled cybersecurity work. The pilot focused on five skill categories captured in the Skills

Transformation Framework: foundational IT and cybersecurity knowledge; AI literacy and human oversight; critical thinking and investigative skills; communication and explainability; and enterprise and operational readiness.

**Across two iterations, the pilot combined hands-on learning and interactive workshops, which included:**

- A cyber range session to strengthen understanding of cybersecurity fundamentals through guided simulation and practical application
- A guided tabletop exercise in which participants worked through realistic incident scenarios to assess risk, make decisions under pressure, communicate with stakeholders, collaborate with team members, and translate technical findings into business-relevant actions
- An AI literacy learning lab to explore and develop practical skills to evaluate, use, validate, and question AI-enabled tools
- An action-planning wrap-up session, which included a learning and training plan takeaway and additional resources to aid continuous professional development

Fifty-five early-career cybersecurity professionals participated across the two pilot iterations. Participant and facilitator feedback suggests the program's practical, hands-on nature was a key strength, providing meaningful opportunities to practice the skills employers identified as important. The skills explored throughout the program were consistently rated positively, with participants indicating that they expect to apply their learning in their work or professional development soon after the program.

The pilots also provided an opportunity to refine the approach in real time. Feedback from the first iteration highlighted the need for a more deliberate connection between the AI and cybersecurity components, particularly within the cyber range simulation and tabletop exercise. This integration was strengthened in the second iteration, and together, both iterations of the pilot program provided early evidence of how the employer insights could be translated quickly into practical learning experiences.

## Priority areas for continued action and learning

**The findings point to six priority areas for continued action, testing, and research:**

- How can foundational IT and cybersecurity knowledge be effectively developed and assessed in AI-enabled environments?
- How can investigative reasoning and critical thinking be preserved as AI automates portions of technical workflows?
- What communication and explainability capabilities are most important for early-career cybersecurity professionals?
- What level of AI literacy and validation capability should employers expect from entry-level talent?
- How can human oversight and professional judgment be strengthened within AI-augmented workflows?
- How can enterprise readiness and business-context awareness be developed and demonstrated more effectively?

Together, these areas represent the intersection of preserved, evolving, and emerging competencies within AI-enabled cybersecurity work.



### *Governance and practical risk decision-making emerged as additional priorities*

An additional priority emerged through the roundtable discussions that was not captured in early findings or tested through the pilot program: greater emphasis on governance, assurance, and practical risk decision-making. Roundtable participants noted that these areas often receive less attention than technical cybersecurity skills, reinforcing the view that cybersecurity is both a technical and business function.

Early-career cybersecurity professionals may have strong technical knowledge but limited exposure to how organizations assess, manage, and accept risk. As organizations adopt AI, secure adoption will depend not only on technical controls but also on effective governance, processes, business investment, clear guardrails, and clear ownership of risk.

---

### *Ethical judgement and responsible AI use also emerged as important considerations*

AI ethics and ethical decision-making may require greater emphasis in both training and workplace development. Skills such as critical thinking and ethical judgment will be increasingly important to help professionals assess not only what AI can do but also what it should do and how it can be used responsibly.

## Conclusion

Employer engagement suggests that AI is not eliminating early-career cybersecurity roles but reshaping how work is performed, how readiness is assessed, and how foundational skills are developed and practiced.

**As the project concludes, key contributions and learning include:**

- Validated insights that foundational technical knowledge, critical thinking, investigative skills, and the ability to apply human judgment remain essential as AI becomes more integrated into cybersecurity work
- The development of a skills transformation framework that translates employer insights into a practical framework for understanding and developing the foundational skills needed to work effectively alongside AI
- Early evidence suggests that simulation-based learning can create meaningful opportunities to practice and demonstrate foundational skills that may be difficult to develop or assess through traditional approaches.

## *Recommendations and next steps*

The findings from this project point to several practical opportunities for action, with employers, HR teams, training providers, governments, and funders each playing a role in strengthening workforce readiness for AI-enabled work.

| Audience | Recommended Actions |
|---|---|
| **Employers & Cybersecurity Leaders** | • Clearly identify the foundational skills required for early-career roles and distinguish between skills that are genuinely required at entry and those that can be developed on the job<br>• Provide operational or rotational exposure. Where possible, provide learners and training providers with opportunities to engage with authentic workplace scenarios, tools, and workflows<br>• Use applied assessments to evaluate reasoning, judgment, and performance with and without AI |
| **HR & Talent Teams** | • Align hiring practices with evolving entry-level roles by working alongside hiring managers to ensure job descriptions, screening criteria, and experience requirements reflect the skills and capabilities actually needed for early-career cybersecurity roles<br>• Assess learning potential alongside current skills |
| **Training Providers & Post-Secondary Institutions** | • Connect learning more directly to workplace practice<br>• Move beyond generic AI literacy toward applied, role-specific learning that reflects real workplace contexts<br>• Integrate governance, risk, and responsible AI into applied learning<br>• Design assessments that require learners to demonstrate foundational skills, critical thinking, and human judgment alongside AI tools<br>• Build stronger employer and work-integrated learning partnerships. |
| **Governments & Funders** | • Enable institutions, employers, and training providers to test new approaches to skills development, assessment, and workforce transition<br>• Invest in applied pilots, work-integrated learning, and employer-training partnerships |
| **Across the Ecosystem** | • Continue tracking how entry-level work changes across sectors and levels of AI adoption<br>• Test whether these approaches improve hiring and workplace readiness over time; continue validating findings with employers, HR, learners, and training providers |

## *Continued action, testing, and learning*

The findings provide a clear basis for action now, while recognizing that early-career roles and skill requirements will continue to evolve as AI adoption increases. Employers, training providers, and policymakers should begin applying and testing these approaches while continuing to track workplace changes and evaluate which training, assessment, and hiring models are most effective.

Ongoing engagement with employers, HR teams, learners, and training providers will help ensure these approaches remain practical, relevant, and grounded in changing workplace realities.

# Acknowledgements

We extend our sincere thanks to the employers, industry leaders, and organizations who generously contributed their time to this project and helped shape the insights reflected in this report.

| | |
|---|---|
| **Andrew Buckles** | VP of Cyber Services<br>***ISA Cybersecurity*** |
| **Andrew Cilla** | Cyber Director<br>***KeyData Cyber*** |
| **Biren Patel** | SOC Manager<br>***Ontinue*** |
| **Carlos Chalico** | Partner, Cybersecurity: Data Protection & Privacy<br>***EY*** |
| **Crawford McAlpine** | Senior Manager, Cyber Security Operations Centre<br>***Rogers Communications*** |
| **Daniel Pinsky** | *CSO* |
| **Darren Chin** | *Practice Leader* |
| **Farshad Abasi** | Founder Chief Security Officer<br>***Forward Security*** |
| **Geordie Cree** | President<br>***Cree Cybersecurity*** |
| **Hardeep Mehrotara** | Vice President Cyber Security<br>***QuadReal Property Group*** |
| **Harnoor Singh** | Associate Director of Cyber and Technology Risk<br>***RBC*** |
| **Jaclyn Parent** | Manager, Cyber Vulnerability<br>***Metrolinx*** |
| **Kevin Loen** | Head of AL Data and Infrastructure |
| **Kevin Sahota** | Manager, Security Operations & Analytics<br>***Wawanesa Insurance*** |
| **Lina Dabit** | Executive Director<br>***Optiv Canada*** |

# Acknowledgements


| | |
|---|---|
| **Logan Schmidt** | Director of Computing Programs & Associate Teaching Professor<br>***Northeastern University Vancouver*** |
| **Mac Batty** | Manager, Security Operations<br>***Arctic Wolf*** |
| **Manisha Singh** | Senior Manager, Security Advisory |
| **Megan Ritchie** | Senior Manager, Digital Forensics, Bell Defence Centre<br>***Bell*** |
| **Milos Stojadinovic** | Fellow of Cyber Security (VP)<br>***RBC*** |
| **Mitch Kelsey** | Head, Cybersecurity Managed Services<br>***CDW Canada*** |
| **Moein Mashayekhi** | Senior Cyber Defender (Senior SOC Analyst)<br>***Ontinue*** |
| **Nitin Bedi** | Vice President, Cyber Services<br>***ISA Cybersecurity*** |
| **Parth Patel** | Cyber Incident Response Manager |
| **Penny Longman** | CEO<br>***NKST*** |
| **Peter Buckley** | Founder<br>***Buckley Cyber Consulting*** |
| **Rob Antonishen** | Director of Cyber Security & Compliance<br>***BC Hydro*** |
| **Roopam Chandi** | Director Strategy Information Security & Risk Management<br>***Manulife*** |
| **Sacha Blasiak-Priestley** | Global Leader - Cloud Security<br>***BDO*** |
| **Santosh Somasekhara** | Senior Manager, Cyber Security, Financial Crimes Unit<br>***BMO*** |
| **Shamnad Shaffi** | Principal, IT Security |
| **Simon Wong** | Associate Partner, Cybersecurity<br>***EY Canada*** |
| **Sneha Jain** | Clinical Innovation and System Optimization, Regional Home and Community Care - Director<br>***Fraser Health*** |
| **Vanessa Thomas** | Office of the Information & Privacy Commissioner of British Columbia<br>***IPC*** |
| **Vivek Khindria** | President and Principal<br>***Risk Embrace*** |










Funded by the
Government of Canada's
Future Skills Program



Toronto Metropolitan University

ROGERS cybersecure catalyst

Future Skills Centre | Centre des Compétences futures

Funded by the Government of Canada's Future Skills Program

Canada

# Contact us

Rogers Cybersecure Catalyst

*cybersecurecatalyst.ca*

*programs@cybersecurecatalyst.ca*