
Cyber Connexion
Jumpstart your cybersecurity career
— Powered by —
The Fields Institute

Cyber Connexion is an intensive cybersecurity upskilling program that gives diverse talent in Canada the skills to quickly transition into high-demand careers at leading organizations.

HOW IT WORKS

JOB-READY SKILLS

Our course material is constantly updated to anticipate the needs of the Canadian cybersecurity job market. We work with an Advisory Board of industry leaders to ensure our participants leave the program with the relevant skills and knowledge to land impactful jobs.

NETWORKING OPPORTUNITIES

We work with an expansive network of employers who understand the value our graduates bring to their organizations. Participants receive first-hand accounts of how the industry works from guest speakers, while gaining access to exclusive networking events and mentorship opportunities.

CONTINUAL SUPPORT

Our participants work with career coaches to hone the soft skills they need to land their first cybersecurity job, including interview preparation, resume building and networking skills. We also offer post-graduation support in the form of one-on-one coaching sessions and networking opportunities.

IMPORTANT DATES

PART-TIME • 16 WEEKS

NOV 27	APPLICATION DEADLINE
DEC 4	START DATE
MAR 15	END DATE

FULL-TIME • 8 WEEKS

JAN 25	APPLICATION DEADLINE
FEB 5	START DATE
MAR 25	END DATE

GETTING STARTED

APPLY

You will be asked for your CV, LinkedIn and GitHub profiles.

INTERVIEW

A Program Lead will invite you to a 30-minute call.

ACCEPT OFFER

Successful applicants will be contacted and offered a spot in the upcoming cohort.

TUITION FEES

Pay program fees beforeclasses begin.

PROGRAM BEGINS

You will receive detailed instructions on how to prepare for your coursework and access the program.

WHAT YOU WILL LEARN

CYBERSECURITY AWARENESS & PRIVACY LAWS

Participants will learn how cybersecurity practice is shaped by the basic goals of confidentiality, integrity and availability. They will also learn to distinguish between the various types of adversaries and how their diverse capabilities and goals shape our approaches to security.

COMPUTER NETWORKING

Participants will learn to reason about network communications using the OSI reference model. We will cover how this model is supported by various networking protocols as well as physical and virtual implementations of network infrastructure.

RISK MANAGEMENT & BUSINESS CONTINUITY

Participants will learn how security policy is designed and implemented at the highest levels to ensure that an organization's security posture matches their strategic goals. They will also learn how standardized frameworks such as NIST, COBIT and PCI DSS help organizations systematically implement and assess their security policies.

DEFENSIVE SECURITY

Participants will learn fundamental concepts for securing IT systems. Topics include security fundamentals for Linux and Windows environments, vulnerability management, SIEM solutions such as Splunk, incident response strategies, forensic analysis, and application security. An emphasis is placed on gaining practical, hands-on experience with the most important tools of the trade.

CLOUD SECURITY

Participants will learn about cloud architecture and how to apply concepts from previous modules to cloud environments. Topics such as firewalls, access controls, and zero-trust architecture will be taught and applied in a cloud environment.

PRIVILEGED ACCESS MANAGEMENT (PAM)

Participants learn how to use PAM tools and policies for a last line of defense to thwart the adversaries once they infiltrate. Learn how to identify, verify, protect and monitor privileged accounts.

CRYPTOGRAPHY: IDENTITY & ACCESS MANAGEMENT (IAM)

Participants will learn important concepts of modern cryptography such as asymmetric and symmetric encryption techniques, hashing, digital signatures and the challenges posed by quantum computing.

SECURING NETWORKS

After learning how networks are designed and implemented, participants will discover how controls are integrated at the various layers of the networking stack to achieve security goals. We will discuss protocols such as SSL, TLS and IPSec, tools such as firewalls and intrusion detection systems, and explore the role of auditing in assessing the quality of our technical controls.

TENABLE VULNERABILITY MANAGEMENT

Participants will learn a cloud-based vulnerability management solution through Tenable, along with how to use four categories of scan templates: Vulnerability Scans, Configuration Scans, Tactical Scans, and Inventory Collection inside an AWS environment.

Eligibility Requirements

- Eligible to work in Canada.
- Actively seeking to join the Canadian workforce in the cybersecurity space.
- Possess a formal degree or certificate in a STEM or STEM-related field (i.e., science, biology, math, engineering, computer science) or experience in a technical role in: IT, Military, or other related industries.

  Note: We welcome applications from individuals who have a strong desire to begin a new career in cybersecurity but do not possess a formal degree and/or work experience in the areas stated above. Please inquire for more details.

- Fluent in spoken and written English.
- Available to join live online sessions for the duration of the program, and complete assignments and project work for an additional 10 hours per week.

  Note: Cyber Connexion prioritizes candidates that exhibit exceptional teamwork, listening and problem-solving skills.

cyberconnexion.ca/eligibility

SONYA GOULET
Cybersecurity Program Manager
sgoulet@fields.utoronto.ca

AARON CRIGHTON
Academic Liaison
acrighto@fields.utoronto.ca