Toronto Metropolitan University

ROGERS cybersecure catalyst

Cybercrime Investigation Foundations

February 2025 Course Overview

Cybercrime Investigation Foundations

The Cybercrime Investigations Foundations (CIF) course is a boot camp offered by the Rogers Cybersecure Catalyst, designed to prepare officers to meet the performance expectations of an entry-level Cybercrime Investigator.

Upon successful completion of the course, learners will be able to:

- Describe the fundamentals of cybercrime investigation
- Describe IT infrastructure elements and how the Internet facilitates cybercriminal activity
- Integrate digital evidence collection into practice
- Interpret crypto tracing results
- Identify common cybercriminal TTPs and IoCs
- Assess cybercrime intelligence requirements
- Respond to the impacts of cybercrime
- Lead discussions on cybercrime investigative capabilities

Learn from subject matter experts—CIF is delivered by experienced cybersecurity facilitators and brings in a range of topical guest speakers, including law enforcement, crown attorneys, corporate counsel, and more. The cost for attending the course is $3,600 + HST per seat.

Please contact Serena Jerkovic (serena.jerkovic@torontomu.ca) if you have any questions about the course.

FAQs

Who is the course for?

The target audience for CIF is new or prospective cybercriminal investigators or analysts who will be/are employed in cybercriminal investigation teams.

Learners may be experienced law enforcement officers with a limited understanding of technology, tech crime, or cybercrime. They have traditional investigative and inquiry skills but are not necessarily familiar with the investigation of cybercrime, tactics for understanding and responding to victims' consequences, or how to engage technical subject matter experts during an investigation.

When is the course?

The CIF course is delivered in a hybrid format, consisting of mandatory in-person classes and pre-requisite online activities. Before attending the in-person class, learners are expected to complete 10 hours of e-learning (pre-reading/self-study with quizzes).

The boot camp portion of the course will run for five days (M—F), and class is scheduled each weekday from 0830 - 1630.

We are currently running registration for a February 10 - 14, 2025 delivery.

Where will the in-person course be delivered?

The course is delivered in person at Catalyst's Classroom in Brampton, Ontario (1 Nelson St. W).

How was the course developed?

The course was developed by Catalyst's Senior Cyber Advisors in collaboration with members of Canadian law enforcement in cybercrime. Designed to prepare learners for essential skills in the workplace, the course is outcome-oriented and practical. The course follows a continuous development model and continuously evolves based on the feedback from our learners and the changing cybercrime landscape. To date, the course curriculum has been influenced by stakeholders from federal, provincial, and municipal levels of law enforcement.

FAQs

Why attend a Catalyst training course?

The Cybercrime Investigation Foundations course is divided into defined modules, each with action-led learning objectives directly tied to job requirements. Catalyst training is practical and dynamic. It takes advantage of engaging instructional strategies, including group discussions and hands-on experience in the Catalyst Cyber Range. This is a hands-on program as opposed to a primarily lecture-based program.

What is the Catalyst Cyber Range

The Catalyst Cyber Range is a unique cybersecurity training platform that supports experiential learning in an ultra-realistic enterprise environment. Powered by RHEA Group's state-of-the-art technology, the Cyber Range features a customizable technology platform and an array of real-world cybersecurity scenarios.

These cybersecurity scenarios simulate realistic attacks and breaches, providing learners with the experience of working through real-life cyber events. Similar to pilot training in a flight simulator, the Cyber Range provides a thoroughly realistic training environment. For more information on our Cyber Range, watch the informational video at the following link: cybersecurecatalyst.ca/watch-experience-the-catalyst-cyber-range/

How is the course assessed?

This is a pass/fail course. To pass the program, candidates will be required to participate in all modules, successfully complete assignments, as well as the summative assessments. There will be formative assessments throughout the program to offer participants feedback and provide the instructor insight into individual progress and where additional support may be required.

The final summative assessment will evaluate the participant's ability to meet critical performance requirements in cybercrime investigation planning and conduct, including the identification and collection of digital evidence within a realistic virtualized environment.

Learners will receive a certificate upon successful completion of the course.

More information on the programming

The CIF course relies on a variety of instructional materials, including:

- Pre-reading materials and a Learner Handbook which prepare learners and guides them through each module
- Engaging in-class sessions, including interactive lectures, Cyber Range exercises, facilitated discussions, panel discussions, expert presentations, case studies, scenario-based activities, and a table-top exercise.

Please find a list of the course modules and learning outcomes on the next page.

From our past learners

"The Cyber Range scenario was very good and very user-friendly. Was very good to see this perspective as a police officer."

CIF Learner, 2023

"On the Cyber Range - this was an amazing opportunity and allowed an authentic hands-on experience. Well done!"

CIF Learner, 2023

"Good course overall; the instructors were very knowledgeable and stepped up when challenged."

CIF Learner, 2024

Course Curriculum

Note: Sequence of modules is subject to change; topics are final.

Module	Learning Objectives & Content
Introduction to Cybercrime	• Defining cybercrime and cyber-enabled crime—Criminal Code of Canada • Cybercriminals and motivations—types of cybercrime and cyber-enabled crime • Ransom group operations
Cyber Threat Intelligence	• Threat intelligence process and tools • International cooperation • Current issues
Cybercrime Investigative Process	• Describe the fundamentals of cybercrime investigation • Respond to victim impacts • Integrate digital evidence into practice
Cybercrime Intrusions	• Describe how the Internet facilitates cybercriminal activity ◦ Review of IT infrastructure and networking ◦ Exploiting vulnerabilities and the cyber kill chain
Intrusion Analysis & Identification of Evidence / IoCs	• Identify common cybercriminal TTPs and IoCs ◦ MITRE ATT&CK framework and threat actor TTPs • Integrate digital evidence into practice ◦ Identifying support and expertise in identifying and gathering evidence ◦ Different types of logs and how to obtain them ◦ Digital correspondence ◦ Artifacts from attack, based on the type of attack
Tech Analysis & Attribution	• Integrate digital evidence into practice

Course Curriculum

Note: Sequence of modules is subject to change; topics are final.

Module	Learning Objectives & Content
Intelligence Gathering	• OSINT tools and processes • Introduction to the Dark Web
Cryptocurrency	• Analyze and synthesize cybercrime information from multiple sources (including crypto tracing reports, intelligence, etc.)
Working with Prosecution	• Current and emerging issues (case law and decisions) • Better practices with POs, Warrants, and related authorities • Court prep and testifying as a witness
Leadership in Cybercrime	• Working with the media • Current and emerging issues in policing cybercrime • Organizational structure and support • The business case for a cybercrime investigation capability • Team selection, resourcing, and development

Toronto Metropolitan University

ROGERS cybersecure catalyst

Catalyst Corporate Training & Cyber Range

Get in touch

catalyst.corporate@torontomu.ca
cybersecurecatalyst.ca