# Cyber Security Analysis (Co-op and Non-Co-op Version)

Ontario College Graduate Certificate            Program Code: 1530X01FWO

1 Year

Ottawa Campus

## Our Program

**Become a cyber security professional safeguarding networks and data from existing and potential threats.**

The Cyber Security Analysis (CSA) Ontario College Graduate Certificate program is designed to prepare you to meet the market demand for cyber security professionals in the public and private sector.

Throughout the program, you focus analytically on key cyber security principles including threat and vulnerability management, event/incidents analysis, laws and ethics relating to security compliance and implementation, cryptographic solutions for data confidentiality and communication protection, cyber incident response, digital forensics processes, disaster recovery and business continuity following cyber incidents and related tools, security devices and appliances. You develop the skills and knowledge necessary to select and deploy the optimal tools and security solutions given unique scenarios.

Graduates possess the theoretical knowledge and hands-on skills on a dedicated cloud platform to assess, recommend, implement and troubleshoot various advanced security scenarios and countermeasures. Utilizing IT concepts and tools, you evaluate the technical aspects and risk levels of security solutions, threat hunting, penetration tests and vulnerability assessments. You also examine the legal process and proper evidence gathering procedures, effective design of corporate security policies, analysis and management of risks or threats as well as ethical and social implications related to security, privacy laws and compliance. Algonquin College's state-of-the-art computing facilities, with latest cyber-attack/defence tools support you to be well-prepared for entry into the field of cyber security. You gain exposure to real-world technologies currently used within industry including specialized networking brands and software. The Cyber Security Analysis curriculum has been designed to closely assist graduates in preparing to achieve a number of well-known industry certifications.

Students also have the option to gain real-world experience through a paid co-operative education (co-op) work term (see Additional Information for more details). Please note that places in the co-op work term are subject to availability and academic eligibility. Please note admission to the co-op program does not guarantee a co-op placement.

Graduates may find employment in a variety of security related domains in the private, corporate, industrial, governmental, or service sectors. Employment opportunities may be available in private security firms, security consulting firms, security vendors and their value-added resellers (VARs), law enforcement agencies, security operation center, cyber incident response groups, security and intelligence organizations or agencies, information technology consulting firms, communications carriers, information service providers or in government, business and public organizations in multiple fields outside IT/IS requiring security practitioners.

## Employment

Graduates may find employment in a variety of security related domains in the private, corporate, industrial, governmental or service sectors in a variety of roles including cyber security analyst, cyber security specialist/technician, cyber crime analyst, cyber security consultant, cyber security developer, cyber security design specialist, cyber security engineer, cyber security advisor, embedded cyber security specialist, cyber security solutions architect, cyber security business development leader, cyber security threat hunter, cyber vulnerability assessor, cyber defence operator, cyber forensics analyst, cyber security project manager, cyber security protection and

planning consultant, cyber security compliance specialist, cyber incident responder, disaster recovery planner, penetration tester, cyber security tester and evaluator, cyber security researcher, security operation analyst, cyber security policy analyst.

## Learning Outcomes

The graduate has reliably demonstrated the ability to:

- Develop and implement cyber security solutions to protect network systems and data.

- Plan and implement security assessment methodologies, vulnerability management strategies and incident response procedures to generate and communicate security analysis reports and recommendations to the proper level of the organization.

- Recommend processes and procedures for maintenance and deployment of cyber security solutions.

- Select and deploy optimal security appliances and technologies to safeguard an organization's network.

- Comply with existing industry policies, regulations, and ethics for information systems and information technology security solutions to ensure industry expectations and standards are met or exceeded.

- Analyze security risks to organizations and business processes to mitigate risk in compliance with industry standards.

- Plan and conduct disaster recovery, forensic investigations and incident responses to support Business Continuity of an organization.

- Implement and conduct penetration testing to identify and exploit an organizations' network system vulnerability.

- Perform various types of cyber analysis to detect actual security incidents and suggest solutions.

- Identify and apply discipline-specific factors that contribute to the local and global community through social responsibility, economic commitment and environmental stewardship.

## Program of Study

| Level: 01 | Courses | Hours |
|-----------|---------|-------|
| CST8801 | Threat Management | 84.0 |
| CST8802 | Traffic Analytics | 56.0 |
| CST8803 | Vulnerability Management | 56.0 |
| CST8804 | Security Devices and Appliances | 56.0 |
| CST8805 | Applied Cryptography | 56.0 |
| GEP1001 | Cooperative Education And Job Readiness | 21.0 |
| Level: 02 | Courses | Hours |
| CST8806 | Digital Forensics | 56.0 |
| CST8807 | Penetration Testing | 56.0 |
| CST8808 | Cyber Incident Response | 56.0 |
| CST8809 | Business Continuity and Disaster Recovery | 56.0 |

| CST8812 | Capstone Project | 70.0 |
| GEP2001 | Co-op Job Search 1 | 21.0 |
| **Co-op: 01** | **Courses** | **Hours** |
| WKT8005 | Co-op Work Term | 0.0 |
| | | |

## Fees for the 2025/2026 Academic Year

Tuition and related ancillary fees for this program can be viewed by using the Tuition and Fees Estimator tool at  https://www.algonquincollege.com/ro/pay/fee-estimator/

Further information on fees can be found by visiting the Registrar's Office website at https://www.algonquincollege.com/ro/

Fees are subject to change.

Additional program related expenses include:

- Books and supplies cost approximately $1500 for the program.

## Admission Requirements for the 2026/2027 Academic Year

### Program Eligibility

-  Ontario College Diploma, Ontario College Advanced Diploma or degree, or equivalent in the areas of Information Systems (IS), Information Technology (IT), Telecommunications/ Networking, IT/IS Security, Computer/Electronic/Communication Engineering or equivalent;This includes, but is not limited to, courses showing technical knowledge/skills in Linux/Windows OS, LAN/WAN Technologies, IP Networking, Shell Scripting. TCP/IP Administration, IT Security, and IT Technical Support OR

-  A Graduate Certificate, Diploma, Advanced Diploma, or Degree from an accredited institution in a non-related field, with minimum three years of relevant practical field experience in an IT/IS Security position may be considered;

-  Applicants with international transcripts must provide proof of the subject specific requirements noted above and may be required to provide proof of language proficiency. Domestic applicants with international transcripts must be evaluated through the International Credential Assessment Service of Canada (ICAS) or World Education Services (WES).

-  IELTS-International English Language Testing Service (Academic) Overall band of 6.5 with a minimum of 6.0 in each band OR TOEFL-Internet-based (iBT)-overall 88, with a minimum in each component: Reading 22; Listening 22; Speaking 22; Writing 22; OR Duolingo English Test (DET) Overall 120, minimum of 120 in Literacy and no score below 105.

## Admission Requirements for 2025/2026 Academic Year

### Program Eligibility

-  Ontario College Diploma, Ontario College Advanced Diploma or degree, or equivalent in the areas of Information Systems (IS), Information Technology (IT), Telecommunications/ Networking, IT/IS Security, Computer/Electronic/Communication Engineering or equivalent.This includes, but is not limited to, courses showing technical knowledge/skills in Linux/Windows OS, LAN/WAN Technologies, IP Networking, Shell Scripting. TCP/IP Administration, IT Security, and IT Technical Support OR

-  A Graduate Certificate, Diploma, Advanced Diploma, or Degree from an accredited institution in a non-related field, with minimum three years of relevant practical field experience in an IT/IS Security position may be considered.

-  Applicants with international transcripts must provide proof of the subject-specific

-  Applicants with international transcripts must provide proof of the subject-specific requirements noted above and may be required to provide proof of language proficiency. Domestic applicants with international transcripts must be evaluated through the International Credential Assessment Service of Canada (ICAS) or World Education Services (WES).

-  IELTS-International English Language Testing Service (Academic) Overall band of 6.5 with a minimum of 6.0 in each band; OR TOEFL-Internet-based (iBT)-overall 88, with a minimum in each component: Reading 22; Listening 22; Speaking 22; Writing 22; OR Duolingo English Test (DET) Overall 120, minimum of 120 in Literacy and no score below 105.

## Application Information

**CYBER SECURITY ANALYSIS**
**Program Code 1530X01FWO**

Applications to full-time day programs must be submitted with official transcripts showing completion of the academic admission requirements through:

 https://www.ontariocolleges.ca/en
60 Corporate Court
Guelph, Ontario
N1G 5J3
1-888-892-2228

Applications are available online  https://www.ontariocolleges.ca/en

Applications for Fall Term and Winter Term admission received by February 1 will be given equal consideration. Applications received after February 1 will be processed on a first-come, first-served basis as long as places are available.

International applicants applying from out-of-country can obtain the International Student Application Form at  https://algonquincollege.my.site.com/myac360/s/self-registration-page  or by contacting the Registrar's Office.

For further information on the admissions process, contact:

Registrar's Office
Algonquin College
1385 Woodroffe Ave
Ottawa, ON K2G 1V8
Telephone: 613-727-0002
Toll-free: 1-800-565-4723
TTY: 613-727-7766
Fax: 613-727-7632
Contact:  https://www.algonquincollege.com/ro/

## Additional Information

**CO-OP INFORMATION**
The Cyber Security Analysis co-op program is open to domestic students only and not available to international students. All applicants apply directly to the non-co-op version of this program through OntarioColleges.ca. Students may elect to participate in the co-op version, two terms prior to the first co-op work term, subject to availability and academic eligibility.

Co-operative education (Co-op) allows students to integrate their classroom learning with a real-world experience through paid work terms. Two academic terms prior to the cooperative education work term, students are required to actively participate in and successfully complete the self-directed co-op course, readiness activities and workshops.

Students must actively conduct a guided, self-directed job search and are responsible for securing approved program-related paid co-op employment. Students compete for co-op positions alongside students from Algonquin College and other Canadian and international colleges and universities. Algonquin College's Co-op Department provides assistance in developing co-op job opportunities and guides the overall process, but does not guarantee that a student will obtain employment in a co-op work term. Co-op students may be required to relocate to take part in the co-op employment opportunities available in their industry and must cover all associated expenses; e.g., travel, work permits, visa applications, accommodation and all other incurred expenses.

Co-op work terms are typically 14 weeks in duration and are completed during a term when students are not taking courses. For more information on your program's co-op level(s), visit the courses tab on your program's webpage.

For more information on co-op programs, the co-op work/study schedule, as well as general and program-specific co-op eligibility criteria, please visit
https://www.algonquincollege.com/coop-career-centre/

**Certifications:**
The program will assist graduates to be prepared to write certain industry certifications. Additional education or work experience may be required depending on the certification.

## Contact Information

**Program Coordinator(s)**

- Arsalan Parsaei,  mailto:csacoord@algonquincollege.com , 613-727-4723

## Course Descriptions

### CST8801 Threat Management

Every organization needs to protect themselves from different types of cyber threats; they must manage these by refining and analyzing threat intelligence about cyber-attacks. Students employ tactical, operational and strategic level threat management skills as well as identify legal and regulatory issues related to information technology, issues of compliance to laws and regulations and security clearances. Applying these skills in the lab, students respond to different scenarios to analyze risk associated with various threats and quantify them to manage and mitigate the risks toward an organization based on security policies and frameworks used in industry.

Prerequisite(s): none
Corerequisite(s):none

### CST8802 Traffic Analytics

Sophisticated attackers know how to blend malicious activities with legitimate traffic and go undetected in a victim network, so only the skilled network analyst knows how to find them. Students develop their traffic analysis skillset to help detect and prevent malicious activities. Through theory and hand-on activities, students deploy the core tasks and techniques for TCP/IP and traffic analysis for evidence of reconnaissance and breach patterns on the network.

Prerequisite(s): none
Corerequisite(s):none

### CST8803 Vulnerability Management

Every organization needs to be aware of different types of possible vulnerabilities that can lead to breaches in their IT business system. Students use best practices for managing and preventing vulnerability including requirements, processes, and tools to support proper remediation using data classification, asset inventory, point-in-time data analysis, change management and trend analysis. Applying these skills in the lab scenarios, students manage and remediate different types of vulnerabilities in the system.

Prerequisite(s): none
Corerequisite(s):none

### CST8804 Security Devices and Appliances

The proper design and implementation of common security appliances in the overall security solution are critical to a secure environment. Students explore advanced firewall/ Intrusion Detection Systems (IDS)/ Intrusion Prevention Systems (IPS) rules and management, integrating IPS and firewall capabilities, centralized logging and analysis, active alert systems, smart security appliances, along with Network Access Control (NAC) and 802.1x mechanisms. In lab, students engage in hand-on activities to explore industry-standard security appliances.

5

Prerequisite(s): none
Corerequisite(s):none

### CST8805 Applied Cryptography

Securing communications channels, along with transported data, is a cornerstone of information security, which is concerned with the three 'pillars' of confidentiality, integrity and availability of information. Students identify the differences between as well as the weakness and strength of various cryptographic options to help select the best solution for information systems. Students explore concepts and tools related to data security and integrity in lab-based scenarios using mechanisms such as authentication, access control, cryptographic systems and secure communications.

Prerequisite(s): none
Corerequisite(s):none

### CST8806 Digital Forensics

Digital forensics is an indispensable tool to reconstruct the process used for any security breach or to help determine what was compromised. Specialized techniques, tools, and ethical analysis, along with a deep understanding of the affected technologies, are employed to answer the digital forensic questions to understand what happened. Students develop skills in digital forensic techniques and tools used in investigations of cybercrimes or corporate policy violations. In lab-based scenarios, students apply forensic methodology and techniques, analyze evidence acquisition and handling, and interact with law enforcement using forensic best practices.

Prerequisite(s): CST8802 and CST8803
Corerequisite(s):none

### CST8807 Penetration Testing

Penetration testing is recognized as the best way to evaluate the effectiveness of security and incident response controls, processes and procedures. It is therefore a skill in high demand. Students develop practical skills to conduct penetration tests including planning testing projects, applying Security Evaluation and Audit standards, identifying requirements for successful penetration testing. Students role play the attack team and the defense team to practice these skills in a lab-environment.

Prerequisite(s): CST8803
Corerequisite(s):none

### CST8808 Cyber Incident Response

Although there are systems in place to prevent attacks, at times, breaches occur, and cyber security teams should be equipped with incident response protocols. Students explore incident handling, incident response methodology, critical thinking, and they contribute to the development of Computer Security Incident Response Teams and Capabilities and perform incidence response tasks. Applying these skills in the lab, students develop incidence response skills to figure out what went wrong, how to mitigate against an attack, to stop the attack and determine how to ensure it never happens again.

Prerequisite(s): CST8801
Corerequisite(s):none

### CST8809 Business Continuity and Disaster Recovery

As cyber threats increase and the tolerance for downtime decreases, business continuity and disaster recovery gain importance. These practices enable an organization to get back online after problems occur as well as reduce the risk of data loss, reputational harm and improve operations while decreasing the chance of emergencies. Students participate in the planning and implementation of mechanisms designed to safeguard enterprises from serious disruption to normal business activities. Through hands-on scenarios, students examine Business Recovery

6

Planning, Disaster Continuity Planning and Business Recovery Planning.

Prerequisite(s): none
Corerequisite(s):none


### CST8812 Capstone Project

The role of a cyber security analyst is to assess the existing security posture of an organization and recommend solutions for improvement. Through an applied project, students implement a comprehensive information security analysis from the planning and design phase through presentation of the final product for a given scenario. Participating in an in-depth culminating project allows students to integrate and utilize the knowledge and skills obtained throughout the program.

Prerequisite(s): CST8801 and CST8802 and CST8803 and CST8804 and CST8805
Corerequisite(s):none


### GEP1001 Cooperative Education And Job Readiness

Students are guided through a series of activities that prepare them to conduct a professional job search and succeed in the workplace. Through a detailed orientation students learn the cooperative education program policies and procedures related to searching and securing a work term opportunity. Students identify their strengths and transferable skills and participate in workshop-style sessions that focus on cover letter and resume development, interview techniques and job search strategies. Students learn how to navigate a web-based resource centre, which is used to post employment and cooperative education job opportunities. Students reflect on workplace success, ethics and responsibilities.

Prerequisite(s): none
Corerequisite(s):none


### GEP2001 Co-op Job Search 1

Students are guided through a self-directed co-op job search using Algonquin's web-based resource centre, HireAC, as well as independent resources. Students will access information on key job search processes, including Co-op and Career Centre job search procedures and how to declare a self-developed job that meets co-op guidelines. Students will apply and further develop their knowledge on networking, interview techniques and job search strategies to improve their chances of success in securing co-op employment through a competitive job search process. Additional support is provided through individual coaching and group sessions, including job application reviews, mock interviews and assistance for students experiencing unique employment challenges.

Prerequisite(s): none
Corerequisite(s):none


### WKT8005 Co-op Work Term

This optional co-op placement provides students with experiential opportunities within the field. Students attain relevant positions that involve a variety of activities allowing application of principles and concepts developed during previous study. Although centred in public and private institutions located in Eastern Ontario, co-op employment opportunities may be sought throughout Canada and abroad.

Prerequisite(s): CST8801 and CST8802 and CST8803 and CST8804 and CST8805 and CST8806 and CST8807 and CST8808 and CST8809 and CST8812
Corerequisite(s):none