Champlain COLLEGE SAINT-LAMBERT CONTINUING EDUCATION

Cybersecurity: Prevention & Intervention

AEC

LEA.D8

continuingeducation@crcmail.net
https://champlainsaintlambert.ca/continuing-education-hub

Cybersecurity: Prevention & Intervention

LEA.D8

Attestation of Collegial Studies (AEC)

TABLE OF CONTENTS

PROGRAM OBJECTIVE

The Cybersecurity Prevention and Intervention curriculum prepares students to enter the profession of **cybersecurity technician**. The cybersecurity technician occupation is **a specialization of the computer technician occupation.**

Graduates of this program will be able to ensure the protection of technological infrastructures by using tools to detect intrusions and security incidents and to implement risk mitigation or threat eradication measures.

CAREER PERSPECTIVES

This program is aimed at those seeking to work in the information technology and cybersecurity sectors. This program could also aim at graduates of other Champlain College AEC programs, such as the Information Technology Clients Support (LEA.1Q) and Cisco Certified Network Associate CCNA AEC (LEA.21) both offered in the Continuing Education department.

Graduates of this program will become specialists in cybersecurity. Currently, these types of individuals are in high demand as most organizations involved in these areas of activity are forced to hire individuals with their own segmented specializations. This program will allow graduates to possess a comprehensive knowledge and skillset of all implicated technologies and cybersecurity concepts.

FEES

Please refer to the Continuing Education department for the most up to date information. Fees per semester vary depending on number of course hours.

PROGRAM CONTENT

This program consists of 570 course hours and is given **online** on **Tuesday and Thursday evenings and Saturdays.**

COMPETENCIES ACQUIRED

Upon successfully completing the program, the student will be able to:

- Monitor a computer network from a cybersecurity perspective
- Analyze threats and risks
- Apply access control measures
- Assess compliance with policies and standards
- Manage software vulnerabilities
- Conduct intrusion tests
- Manage security incidents
- Implement and manage cybersecurity measures in the workplace

COURSES

Preventive Surveillance in Cybersecurity

Cyber Threat and Risk Analysis

Vulnerability Management

Cyber Defense

Conformity Assessment

Intrusion Testing

Cybersecurity Incident Management

Business Cybersecurity Management

Start date: October 10, 2023

End date: January 25, 2025

GENERAL ADMISSION REQUIREMENTS

To be admissible for this Cybersecurity – AEC (LEA.D8), applicants must meet the eligibility requirements in effect at the time as set forth in Article 4 of the College Education Regulations (RREC). In particular, applicants must have received instruction deemed sufficient by the College and meet at least one of the following conditions:

- The person has interrupted his or her full-time studies or has pursued full-time postsecondary studies for at least two consecutive sessions or one school year;
- The person is covered by an agreement between the college and an employer, or benefits from a government program;
- The person has interrupted their full-time studies for one session and has pursued full-time post-secondary studies for one session;
- The person holds a DEP (*Diplôme des études profesionnelles*).

PROGRAM SPECIFIC ADMISSION REQUIREMENTS

The person must have one of the following profiles:

Profile A

Have a college diploma (DEC) in computer science and have network management skills or an Attestation of Collegial Studies (AEC) in network management or training deemed sufficient.

Profile B

Have recognized relevant experience as a network management technician.

**Note*: If you are unsure about your eligibility for the program and whether or not you fit one of these profiles, please contact Ramzi Jouani with your CV before applying. He will review your CV and then be able to guide you further.

SELECTION CRITERIA

To be selected, the person may have to:

- Participate in a selection interview
- Complete a qualification test
- Provide proof of experience in network management (confirmation letter from the employer)
- Take an English or French entrance exam
- Provide a document demonstrating that they have never been convicted of an offence under the Canadian Criminal Code for which a pardon has not been obtained.

Conditions for obtaining the Attestation of Collegial Studies (AEC): All students enrolled in a program leading to the Attestation of Collegial Studies (AEC) must have successfully completed all courses in the program in order to obtain the attestation.

*Please refer to the FAQ concerning **Bill 96** to see if you are exempt or what steps you must take in order to satisfy these government requirements to obtain your attestation.
https://champlainsaintlambert.ca/bill-96-faq-cont-ed/

COURSE DESCRIPTIONS

420-B01-LA	**Preventative Surveillance in Cybersecurity**	**75 hours**

This course will provide the students with an overview of cybersecurity prevention and response activities. It serves as a foundation for understanding the profession and situating the content covered by the program. At the end of the course, the students will be able to monitor a network in order to detect anomalies, intrusion attempts, or even worse, data exfiltration.

420-B02-LA	**Cyber Threat and Risk Analysis**	**75 hours**

This course enables students to better understand cybersecurity issues and to prioritize activities based on the cyber threats and risks faced by an organization. In a realistic context, students will learn how to identify and assess the importance of cyber threats and how to quantify risk, based on an assessment of the probability and impact of exploiting risk factors.

Several key concepts acquired in this course will be reused in other courses:

- Cyber threat analysis is used to guide surveillance activities and to prioritize cyber defense activities
- The risk analysis is also used to prioritize cyber defense activities, as well as the incident response plan
- The results of intrusion tests, compliance assessment and vulnerability assessment will also be subjected to a risk analysis to determine an appropriate course of action.

420-B05-LA	**Vulnerability Management**	**60 hours**

In this course, the students will learn how to detect and analyze software vulnerabilities on a network, as well as how to implement corrective measures in order to improve an organization's security posture while minimizing the impact on its operations. At the end of the course, students will be able to identify vulnerable components, understand how vulnerabilities can be exploited and the level of risk incurred by the organization, suggest corrective measures, evaluate their effectiveness in a test environment and deploy the solution on a host or on an entire network.

420-B03-LA	**Cyber Defense**	**90 hours**

This course enables students to secure and defend an IT infrastructure against malicious actors internal or external to the organization. From network architecture to privilege and access management, active defense techniques and cryptography to protect information and ensure business continuity in case of a cybersecurity incident. The students will learn how to assess and increase the resilience of the network and its components to different types of cyberattacks.

The skills acquired in this course will be reused in the Intrusion Testing and Cybersecurity Incident Management courses, where access control measures are directly tested.

Pre-requisite: 420-B01-LA

420-B04-LA	**Conformity Assessment**	**45 hours**

In this course, the students will learn how to audit a network and evaluate the security posture of an organization in a rigorous and methodical manner in order to verify its compliance with various reference frameworks and standards. It will also assess compliance with laws governing cybersecurity, particularly with respect to the protection of personal information.

Pre-requisites: 420-B01-LA, 420-B02-LA

420-B06-LA	**Intrusion Testing**	**90 hours**

In this course, students will become "ethical hackers", learning how to exploit security breaches in a preventive context according to clearly established rules of engagement. From test planning to the exploitation of security breaches, students will have to demonstrate a high level of respect for professional ethics. At the end of the course, they will be able to write a report that supports risk analysis and guides cyber defense and cybersecurity incident response activities.

Pre-requisites: 420-B01-LA

420-B07-LA	**Cybersecurity Incident Management**	**75 hours**

In this course, the students will learn how to manage cybersecurity incidents in a way that minimizes the impact on the confidentiality, integrity and availability of company information and services. By the end of the course, students will be able to develop and implement a response plan to various types of incidents in order to quickly identify and analyze the incident, contain compromised systems to reduce the risk of data leakage or hacking to other platforms, and eradicate the cause of the incident. Finally, they will produce a report detailing the incident, the findings and the recommendations to prevent a similar incident from occurring again.

Pre-requisites: 420-B01-LA, 420-B02-LA, 420-B03-LA

420-B08-LA	**Business Cybersecurity Management**	**60 hours**

This course enables the students to link all the notions acquired during the training program. It consists of an integration project within which the students will be responsible for the security of a network. They will have to defend it against intrusions, secure it by adding access control measures, characterize the attack surface and make a risk analysis of it. In addition, students will have to produce a compliance report in accordance with the security policies of the fictitious organization they are responsible for.

Pre-requisites: All previous courses

****Note:*** To progress in the program, each course must be passed successfully. Please note that by withdrawing from a course(s) or failing a course(s) within your AEC program, it may make it difficult or impossible for you to continue with your program at that time. It may delay you in the completion of your program, or it may hinder your opportunity to complete the program as the College cannot guarantee that the program will continue to be offered in the future. Students are expected to attend class sessions and all scheduled examinations.