CANADIAN COLLEGE OF TECHNOLOGY AND BUSINESS

CYBERSECURITY RISK MANAGEMENT with CO-OP

PROGRAM OUTLINE

Full-Time Diploma Program

Total Program Duration: 2440 Hours (106 Weeks)
Classroom Instruction: 1220 Hours (53 Weeks)
Co-op Work Placement: 1220 Hours (53 Weeks)

PROGRAM DESCRIPTION

This Cybersecurity Risk Management with Co-op program, will prepare students to understand in-depth information, network and computer vulnerability challenges, conduct ethical decisions that determine the system's vulnerability and plan organizational cybersecurity programs. Students will be able to monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (IDS/IPS, end-point protection, servers, and workstations).

Studying cybersecurity risk management will equip you with the skills and knowledge to enter several different roles including: Applications Analyst, Systems implementation Manager, Network Systems Engineer, Systems Security Analyst, Computer Analyst, Systems Security Planner, Internet Systems Administrator, and Network Support Technician.

The program is design for individuals keen to begin their career as a Cybersecurity Analyst, this diploma program will set you on the right path. Develop your IT skills to enter this dynamic and opportunity-filled sector.

CAREER OCCUPATION PROGRAM

NOC: 2171, 2281

This program prepares students for the following career occupations:

Cybersecurity Analyst, IT Consultant, Systems Consultant, Data Processing Consultant, Systems Security Planner, Systems Auditor, Computer Network Technician, System Administrator, GRC Analyst

ADMISSION REQUIREMENTS

Admission requirements may not be waived by either the student or the Canadian College of Technology and Business (CCTB).

No funding may be disbursed to the student or received by CCTB until all admission requirements are met.

A payment plan can be offered to a student if a student loan is not an available option.

Requirements:

1. Good command of English language. IELTS 5.5 or equivalent outlined below

Instruction at CCTB is conducted in English.

Students must be in possession of one of the English Language Equivalencies in the list below.
Language proficiency requirements are admission requirements and may not be waived by either the institution or the student.

The following are accepted:
• English Grade 12 (from a high school program in Canadian, US, UK, or other English-speaking country)
• Communications Grade 12 (from a high school program in Canadian, US, UK, or other English-speaking country)
• IB (International Baccalaureate) English A1/A2 (HL or SL)
• IELTS: (International English Language Testing System) Band 5.5 or higher
•TOEFL: (Test of English as a Foreign Language) IBT 46-59 or higher
• CAEL: (Canadian Academic English Language Assessment) Score of 50 or higher
• PTE: (Pearson Test of English) Score of 45.4 or higher
• CLB: (Canadian Language Benchmarks) Level 6 or higher
• TOEIC: (Test of English for International Communication) Score 605-690 or higher

• Successful completion of a Designated ESL school program with level equivalent to tests outlined in section above OR from an established pathway partner of CCTB.
•Applicants may choose to complete the TLGC Online Pre-Arrival Test and receive customized language study plan based on the applicant's test results if a passing grade is not achieved.

•Applicants that are not in possession of one of the credentials above, are advised to enroll in The Language Gallery Canada (TLGC) UPP (University Pathway Program). Successful completion of TLGC UPP level 4.5 is recognized by CCTB in lieu of the aforementioned assessments.

2. High school diploma or equivalent from an approved government institution of applicant's home country, or applicant is minimum 19 years of age
3. Students are required to have and use their personal computers in class

LEARNING OBJECTIVES

After completing this program, students will be able to:

- Use the English language for effective verbal and written communication on at professional level
- Use tools to provide consistent website design Identify introductory JavaScript features such arrays, loops, and conditional statements
- Create reports to summarize and consolidate data Implement basic security for logins, databases, and objects
- Analyze user feedback to refine a design and grow a system
- Understand the basics of Cybersecurity, roles, and processes

- Understand the concept of Governance, Risk, and Compliance
- Understand Cybersecurity Standards, Laws, and Policy
- Understand critical elements in penetration testing
- Practical implementation of SIEM tools
- Counteract weaknesses in information security
- Perform various cyber-attacks
- Describe the basic concepts in penetration testing
- Define different Penetration methods
- Understand the different penetration testing tools
- Formulate project scope
- Gain Knowledge of SOC processes, procedures, technologies, and workflows.
- Gain a basic understanding and in-depth knowledge of security threats, attacks, vulnerabilities, attacker's behaviors, cyber kill chain, etc.
- Able to recognize attacker tools, tactics, and procedures to identify indicators of compromise (IOCs) that can be utilized during active and future investigations.
- Able to monitor and analyze logs and alerts from a variety of different technologies across multiple platforms (IDS/IPS, end-point protection, servers, and workstations).
- Gain knowledge of the Centralized Log Management (CLM) process.
- Able to perform Security events and log collection, monitoring, and analysis.
- Gain experience and extensive knowledge of Security Information and Event Management.
- Gain knowledge of administering SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Understand the architecture, implementation and fine-tuning of SIEM solutions (Splunk/AlienVault/OSSIM/ELK).
- Gain hands-on experience in SIEM use case development process.
- Able to develop threat cases (correlation rules), create reports, etc.
- Learn use cases that are widely used across the SIEM deployment.
- Plan, organize, and perform threat monitoring and analysis in the enterprise.
- Able to monitor emerging threat patterns and perform security threat analysis.
- Gain hands-on experience in the alert triaging process.
- Able to escalate incidents to appropriate teams for additional assistance.
- Able to use a Service Desk ticketing system.
- Able to prepare briefings and reports of analysis methodology and results.
- Gain knowledge of integrating threat intelligence into SIEM for enhanced incident detection and response.
- Able to make use of varied, disparate, constantly changing threat information.
- Gain knowledge of Incident Response Process.
- Gain understating of SOC and IRT collaboration for better incident response.

PROGRAM EVALUATION METHODS AND COMPLETION REQUIREMENTS

CCTB evaluates students using a variety of methods including projects, assignments, presentations, assessments, quizzes, and exams. Students will be given a performance evaluation before 30% of the hours of instruction of the program are completed. This evaluation will address any academic concerns that the college may have regarding student performance and/or learning outcomes. This evaluation will also ensure the student comprehensively understands the grading system, and what actions they can take moving forward to achieve or maintain a higher grade.

To complete the program, students will be required to achieve a minimum grade of 65% in each course, as well as complete the work experience component of their program.

The work experience component of the program includes a performance-based evaluation conducted by the placement host and an analysis report created by the student relating to their work experience that must submitted to the faculty.

Additionally, to successfully complete the program, students must maintain a minimum attendance rate of 75%.

If a course is failed, the student must re-take the course within the next available cohort. The course re-take fee is $1100.

Would you please reference the CCTB Dispute Resolution and Grade Appeal Policy

HOMEWORK HOURS

A minimum of 1 - 2 hours of homework between lectures is to be expected.

DELIVERY METHODS

Combination of distance education and in-class instruction

PROGRAM MATERIALS

CCTB will provide resources in the form of custom learning materials.

CCTB will provide software tools and user licenses.

Instructors will provide students with additional educational resources specific to each module's subject matter. These resources will be used in conjunction with the class lectures.

These resources and learning materials will be made available online via the CCTB Canvas learning management system. Students are required to log in to gain access to the e-materials.
The following books students require to buy:

- Grabosky, P., & Smith, R. (2012). Cybercrime. Lawbook Co.
- Pande, J. (2017). Introduction to Cyber Security. Technology, 7(1), 11-26.
- Comer, D. E., & Droms, R. E. (2003). Computer networks and internets. Prentice-Hall, Inc.
- White, G. B., Fisch, E. A., & Pooch, U. W. (2017). Computer system and network security. CRC press.

- Ray, J. M. (Ed.). (2014). Research data management: Practical strategies for information professionals. Purdue University Press.
- Beaulieu, A. (2009). Learning SQL: Master SQL Fundamentals. O'Reilly Media, Inc.
- Lutz, M., & Lutz, M. (1996). Programming python (Vol. 8). O'Reilly.
- Certified Ethical Hacker (CEH) Version 9 Pearson uCertify Course and Labs Access Card (Certification Guide) Misc. Supplies – Oct. 12 2017 by Michael Gregg
- CompTIA Security+ Get Certified Get Ahead: SY0-601 Study Guide Paperback – June 1 2021 by Darril Gibson

Students must have and use their personal computers in class.

PROGRAM ORGANIZATION

1.	Introduction to Data Communication and Networking	60 HRS
2.	Computer Systems and Server Administration	120 HRS
3.	Website Development	60 HRS
4.	Introduction to Programming	80 HRS
5.	Cybersecurity Terminology and Language	80 HRS
6.	Introduction to Internet Programming and Web Applications	60 HRS
7.	Introduction to Database Management Systems (DBMS)	80 HRS
8.	Linux Operating Systems and Networking	60 HRS
9.	Software Analysis and Design	60 HRS
10.	Security Operations and Management	80 HRS
11.	Cyber attacks and Methodology	60 HRS
12.	Cyber Incidents, events and logging	60 HRS
13.	Incident Detection with SIEM	80 HRS
14.	Incident Detection with Threat Intelligence	80 HRS
15.	Incident Response	60 HRS
16.	SIEM Capstone Project	80 HRS
17.	Cybersecurity Interview and Strategies	60 HRS
18.	Work Experience	1220HRS
	Total Duration	**2440HRS**