CANADIAN COLLEGE OF TECHNOLOGY AND BUSINESS

DIPLOMA IN CYBERSECURITY ANALYST PRACTICUM

PROGRAM OUTLINE

Full-Time Program
480 Hours of Classroom Instruction
120 Hours of Practicum
600 Total Hours in Duration
42 Weeks in Total (Including Breaks)

CANADIAN COLLEGE OF TECHNOLOGY AND BUSINESS

PROGRAM DESCRIPTION

This one-year program is ideal for those looking to becoming familiar with all aspects of cybersecurity such as blockchain, big data and the IoT (Internet of Things). This program is powered by CompTIA, giving you the knowledge to build a solid foundation towards the Security+ certification.

Students will gain the ability to anticipate information security risks, implement new ways to protect networks, and prevent cyberattacks of various types. Through lab activities and cutting-edge tools, students will build the professional skills required to pursue a career in cybersecurity.

CAREER OCCUPATION PROGRAM

NOCs: 2171, 0213, 2147, 2281

This program prepares students for the following career occupations:

Systems Specialist, Systems Security Planner, Systems Security Analyst, System Auditor, Systems Analyst, Internet Security Analyst, Computer Systems Analyst, Computer Analyst, Applications Analyst, Internet Systems Administrator, Computer Network Manager, Systems implementation Manager, Network Systems Engineer, Network Test Engineer, System Administrator, Server Administrator, Network Support Technician, Network Support Analyst, Network Operator, Network Controller, Network Administrator

ADMISSION REQUIREMENTS

Admission requirements may not be waived by either the student nor 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 student loan is not an available option.

Requirements:

- Good command of English language (See Language Proficiency Policy)
- High school diploma or equivalent from an approved government institution of applicant's home country, or applicant is minimum 19 years of age
- Students are required to have and use their own personal computer in class

LEARNING OBJECTIVES

After completing this program, students will be able to:

- Describe the different types of hackers
- Understand key elements of a cyberattack
- Understand regulatory concepts in the cyber world

- Access the Darknet
- Demonstrate how blockchain, IOT and botnet technologies can be used in the cybersecurity domain
- Describe the basis and structure of an abstract layered protocol model
- Understand Basic concepts of protocols and servers
- Understand the fundamental hardware components
- Be able to monitor and parse data in transit, at rest, and in use for security diagnostics
- Utilize protocols currently in use within the Internet and design network protocols.
- Identify security and ethical issues in computer networking.
- Perform installation of virtual machines
- Analyze and monitor network traffic
- Define different OS environments
- Perform base database queries using the Structured Query Language (SQL)
- Perform advanced operations using SQL
- Utilize basic network communication processes
- Define digital certificates & digital signatures
- Understand basics of encryption
- Illustrate the difference between symmetric and asymmetric encryption
- Describe the basics of public key architecture
- Define various encryption tools and methods
- Utilize some of the prominent techniques for encryption such as DES, SHA, Salting, and message authentication
- Solve basic cryptography tasks
- Using cryptographic technology to secure data
- Define various types of scans and vulnerabilities
- Understand the different types of cybersecurity attacks and exploits
- Understand key elements in penetration testing
- 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
- Perform penetration testing with Kali Linux
- Maintain access to different operation systems
- Use different password cracking methods
- Analyze penetration test results
- Compare the penetration test results data to all network documentation
- Report Drafting and Delivery
- Describe SOC, NOC, ISP, MSSP events
- Define different planning protection strategy
- Design and implement a cyber protection strategy
- Execute a complex and effective attack campaign
- Acquire different approaches for dealing with senior managers and clients during cyber-attacks

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 co-op/ practicum component of their program.

The co-op/practicum 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.

Please reference the CCTB Dispute Resolution and Grade Appeal Policy

HOMEWORK HOURS

A minimum of 2.5 - 3 hours of homework between lectures is to be expected.

DELIVERY METHODS

- Combined delivery (both in-class and distance)

REQUIRED PROGRAM MATERIALS

Resources in the form of custom learning materials will be provided by CCTB.

Software tools and user licenses will be provided by CCTB.

Instructors will provide students with additional educational resources that will be specific to the subject matter of each course. 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 login to gain access to the e-materials.

Students must have and use their own personal computer in class.

Additional Recommended Learning Materials (not required):

- 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.
- Zacker, C., & Warren, A. (2017). MCSA Windows Server 2016 Exam Ref 3-Pack: Exams 70-740, 70-741, and 70-742. Microsoft Press.
- 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.
- Graham, I. S. (1995). The HTML sourcebook. John Wiley & Sons, Inc.
- Lutz, M., & Lutz, M. (1996). Programming python (Vol. 8). O'Reilly.
- Graves, K. (2010). CEH certified ethical hacker study guide. John Wiley & Sons.
- Gregg, M. (2017). Certified Ethical Hacker (CEH) Version 9 Pearson uCertify Course and Labs Access Card.
- Dulaney, E., Easttom, C., Chapple, M., & Seidl, D. (2017). CompTIA Complete Cybersecurity Study Guide 2-Book Set: Exam SY0-501 and Exam CSA-001.
- Dulaney, E. (2017). CompTIA Security+ Deluxe Study Guide: Exam SY0-501. SYBEX Inc.

PROGRAM ORGANIZATION

1.	Introduction to Cybersecurity	60 HRS
2.	Computer Networks	60 HRS
3.	Communications, Operating Systems and Data Management	60 HRS
4.	Programming Languages for Cybersecurity	60 HRS
5.	Concepts and Practical Implications of Encryptions	60 HRS
6.	Information Security in the Cyber World	60 HRS
7.	Penetration Testing	60 HRS
8.	Hackathon	60 HRS
	Practicum Placement	120 HRS
	Total Duration	**600 HRS**