Cybersecurity
A WIL Digital Initiative
Presented by the Information and Communications Technology Council

Welcome to ICTC's WIL Digital: Cybersecurity

ICTC's WIL Digital is an innovative Work Integrated Learning program that helps students gain insight and skills to advance learning and meaningful work experience.

COURSE OVERVIEW

The WIL Digital Cybersecurity course is an innovative and collaborative program developing the next generation of Cybersecurity (CS) talent driven by a network of technology-forward companies and partners. The course offers a highly practical, yet strategic learning journey for students and recent graduates, and combines:

1. On the job learning and work experience offered by companies actively leveraging or perusing capabilities
2. Interactive, industry-led stackable micro-learning modules supplementing on the job learning
3. Activation of students' self-development and self-learning skills

This *6-module*, online course will serve to introduce post-secondary students to the field of a diverse set of topics related to the field of CS. It will contextualize students' on the job learning, and provide a framework for further learning and career development by providing them with strategic insights, and industry experience.

Upon completion of this course, students will have a broad understanding of the different categories of CS, key terminology, and a range of industry applications. The course is not meant to be a comprehensive or inclusive overview of the industry, but rather empower learners to not only try to understand CS at a high level, but to further equip them to dive deeper into their specific areas of interest through supplemental readings, online resources, and on the job learning.

TARGETED AUDIENCE

This course is designed for students who are interested in developing fundamental skills in the subject of Cybersecurity, as an entry-level introduction to this topic. Students who are already proficient in this subject matter are encouraged to take another of the WIL Digital courses available, which provide an excellent lateral understanding of concepts associated with this course. If you are interested in studying a more in-depth version of this subject, please contact your course facilitator for options available.

TOPIC OVERVIEW

Each module is split into two sections: active practice and industry resources. The active practice section is hosted by industry leader Field Effect on the Cyber Range platform. The industry resources section is designed according to the National Initiative for Cybersecurity Education (NICE) framework by the Canadian organization CyberNB. The choice of this recognized framework allows the students to share that common reference with other agencies in the public sector, private sector and academia when it comes to understanding roles and responsibilities in cybersecurity careers.

COURSE FORMAT

You will be introduced to several different types of learning activities throughout the course. Below is a list of these activities, as well as a brief description of what it involves, and what is expected of you:

Module	Topic	Description	Details
1	Active Foundations of Cybersecurity	• Windows hardening • Suspicious and hidden files • Introduction to the NICE Cybersecurity Workforce Framework	Difficulty: Intermediate Ages: 18 and up Time commitment: 2 hrs per module, 10 hrs per case study Case Study Details: Students will review cyber forensic tools and build a digital footprint info dossier on the featured talent (Matt). Students are expected to apply the same tools to their own digital footprint privately, and complete a reflection activity on how to improve a digital footprint for future employment.
2	The Language of Cybersecurity	• Steganography • Encoding-decoding • Oversee and Govern	
3	Investigative Algorithms of Cybersecurity	• Hashes • Analyze and Investigate	
4	Critical Defense in Cybersecurity	• Basic Network Analysis • Collect, Operate and Maintain	
5	Attack methods of cybersecurity	• Firewalls • Protect and Defend	
6	Strategic methods of cybersecurity	• Active defense • Securely Provision	
Case Study	Google You – Cyberforensics	• Small group work with presentations reviewed by industry jurors	

Cybersecurity
A WIL Digital Initiative
Presented by the Information and Communications Technology Council

1.1 Windows Hardening

Section Overview

In this section, students will learn how to better protect a Windows computer system against basic threats and vulnerabilities by identifying security risks and applying standard hardening techniques to mitigate (reduce) those risks.

The section is set up as a hands-on learning experience focused on students who are first introduced to cyber security. Students should have a basic working familiarity with a Windows computer in order to complete this section.

Workload Expectations

The student should be able to complete Lab 1 of the section in 30-45 minutes. However, the actual time investment will depend on previous knowledge and on time spent on studying the suggested resources and doing optional tasks. Lab 2 is optional.

Learning Outcomes and Objectives

Upon completion of the section, the students will be able to:

- Assess and configure basic Windows Security Settings on a Windows 10 pro machine according to best practices.
- Auto login (disable) and screensaver settings (set screensaver password)
- Account Policy Security settings (Password Policy and Account Lockout Policy Settings) based on resources and/ or scenario requirements.
- Windows Update (automatic update)
- Windows Defender Firewall settings (default)
- Virus and Threat Detection (default)
- Remote access (disable)
- Assess and configure appropriate user accounts and privileges on a Windows 10 computer.
  - Set up user and guest accounts with appropriate user rights to reduce cyber security risks.
  - Disable, delete, or rename user, guest, and administrator accounts to reduce cyber security risks.
- Detect basic security risks and threats and apply the appropriate hardening strategies to mitigate the risks.

Section Format

Students will be presented with two scenarios in which they have to better secure a Windows10 computer based on the information given in the scenario. Each scenario is presented in a lab which contains a Windows10 Virtual Machine (VM). This VM has no access to internet.

In the first lab, the scenario will guide students through basic Windows 10 hardening steps by having the students perform several tasks per step. Resources are provided. If the resource is a link, students are expected to use the internet browser of their own system to access it.

In the second lab students are presented with a new scenario and accompanying VM. The challenges in this lab will be like the first lab. However, the big difference is that there is no guidance; the student must rely on his newly acquired knowledge and skills as well on his research skills to complete the challenge. Students are expected to read the scenario and assess the security risks. Based on their assessment they determine what strategies they will apply to mitigate these security risks.

FIELD EFFECT

Click the link below to start the module, and enter your username and password on the login page:

https://ictc-cyberranges.fieldeffect.net/CyberReact/login

Windows Hardening

In this course, students will learn how to better protect a Windows computer system against basic threats and vulnerabilities by identifying security risks and applying standard hardening techniques.

Cybersecurity
A WIL Digital Initiative
Presented by the Information and Communications Technology Council

2.3 NICE Framework; Oversee and Govern

Section Overview

This section will give the learner a good understanding of roles in cybersecurity leadership and what key skills are most important in this type of position.

Key Topics

- The importance of stakeholder engagement to supervise, manage, and advise
- The importance of understanding business objectives
- The importance of non-technical skills for future success

Learning Outcomes and Objectives

- To review the category oversee and govern
- To demonstrate options within the field of governance in cybersecurity to learners

Cybersecurity
A WIL Digital Initiative
Presented by the Information and Communications Technology Council

3.2 NICE Framework; Analyze and Investigate

Section Overview

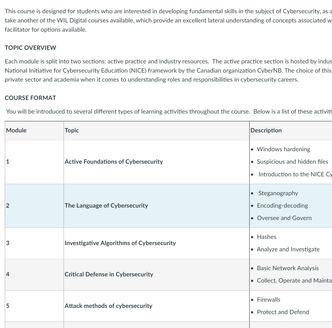
This section will give the learner a good understanding of roles that perform highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence. The viewer will also learn the main soft skills that you need when you investigate cybercrimes.

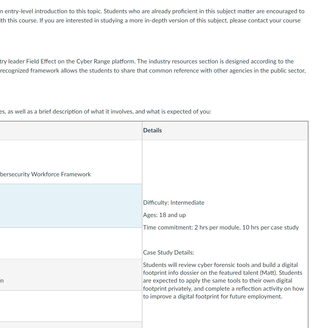
Key Topics

- Cyber intelligence analysis
- Cybercrime investigation disciplines
- Employment requirements
- Associated career opportunities

Learning Outcomes and Objectives

- To provide learners with the different types of cybersecurity analysis that are recognized within the NICE Framework
- To provide use cases and employment paths related to cybercrimes and their prevention

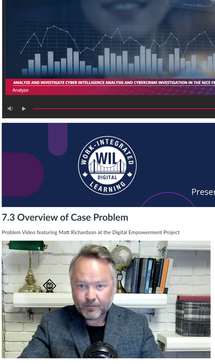




Cybersecurity
A WIL Digital Initiative
Presented by the Information and Communications Technology Council

7.3 Overview of Case Problem

Problem Video featuring Matt Richardson at the Digital Empowerment Project



Video Transcript:

[media description: White man, sitting in front of camera, facing forward, wearing a grey blazer and black shirt. Behind him are white shelves with books.]

Hello, and we're back. Let's begin with today's essential question "would you hire you?" Based on what you find online about yourself, your behaviour, your attitude, skills and qualifications? Would your footprint or your image lead you to hire you? That's our essential question. We'll begin with a brief overview of the steps we're going to follow. Number one, the proverbial rabbit hole, as we know when we go online to do research, is very easy to get off track and stumble into unrelated areas and essentially get lost in the noise that the Internet is. There's a lot of data and a lot of information. So number one, professional investigation 101, go in with a plan. So a simple framework, it needn't be complicated. Begin by collecting some high level surface information on the subject. Today's activity you're going to start by looking me up. You're going to do a background check on me. We use me as an example because I'm an easy one. There's a fair bit out there and I've done a lot of different things. So there's really no shortage of information you'll find about me, my career, and my life online. We will begin the framework high level, grab some keywords, pen and paper, throw it in a text document. Stuff that would include my name, Matt Richardson. Where I live, or work. So, I'm known to be in Belleville and Trenton area, Ontario. Also, what types of experience do I have, what am I known for a quick search for me, one of the key things you'll find is Internet safety. So my list of keywords, I might begin with something like Matt or sorry, Matt Richardson, Belleville and Internet safety. Once I have those key words, I just put together a few search strings, which for anyone unfamiliar, we will be using boolean search operators and creating strategic search strings that will exclude on irrelevant results, and even limit the number of duplicates. The name of the game is exclusions. You want to see what's there about me, but you don't want to see seven million hits about every Matt Richardson in the world. We will look at some of the top platforms that people are going to look you up on. Facebook, Instagram, Twitter, LinkedIn are very big ones. Obviously, Google and Bing and search engine results are going to be used in their decision making. So we're going to look at the top platforms that HR professionals are going to use to look us up online to decide if we're a good fit for their organization. Also, you know, what do you want to look for? Some things that what you don't want to see is anything exhibiting bad judgement, partying, anything that's hateful or very importantly, unkind or disrespectful. That is the number one way to torpedo your chances right there. Skill, to a degree, can be taught. Skill comes with experience, which comes only with time. But character is not so easily taught. People that are kind and respectful, that show leadership skills, recognize others, that showcase their best and brightest colours online, are going to stand out in a positive way.

So now that we have a framework and a game plan in place before we go online, you are going to be introduced to some intermediate and advanced search techniques straight from the open source intelligence or OSINT playbook. You're also going to be introduced to some new tools. The tools are going to provide you are free. They don't even require accounts. They're simple in their interface, but they're powerful. We're also going to- you're going to begin with me, working individually or in groups to do a background check on Matt Richardson, Belleville, Internet safety as discussed, and you may be asked to do a presentation or a debrief on your findings. You will then be asked to turn the lens on yourself, take my name out, replace it with yours, take out Belleville, replace it with your city or town. Take out Internet safety and replace it with something you might be known for. If it's coaching minor hockey, or winning an academic competition, or a scholarship. You're going to begin to take mine out, and place your in. And and very importantly, to do some reflection. Questions you might ask yourself - would I like me? Am I a nice person? Do I show that I have qualifications and skills or even intellectual curiosity? Am I, as a student sharing industry articles, making comments on what I've learned? Am I showing myself in a positive light? So you will be asked to reflect on me, but then to do so on yourself.

Very importantly, we're all made mistakes. What do you do if you need to clean up or fix your profile, your your footprint, your online image? And the good news is that this can be done. And finally, if you don't have much of one, not everybody does. That's still good to know because that tells you the opportunity is there to begin to build an image online that's positive and to do so when the platforms that are going to be searched, when people are deciding our futures.

Funded by the Government of Canada | Canada