FERRO TECHNICS INSTITUTE OF TECHNOLOGY

Registered Under The Ontario Career Colleges Act, 2005

PROSPECTUS

DIPLOMA IN CYBER-SECURITY

The Diploma in Cyber Security equips students with the essential skills to navigate and secure today's digital world. Through hands-on training in network security, ethical hacking, threat detection, and data protection, students gain expertise in identifying vulnerabilities, mitigating risks, and safeguarding information systems. Graduates are prepared for in-demand roles such as Cyber Security Analyst, Ethical Hacker, Information Security Specialist, and Incident Response Technician. This program opens doors to careers across industries, including finance, healthcare, government, and technology, where the need for skilled cyber security professionals continues to grow rapidly.

Delivery format:

In-person, Online Synchronous and Hybrid

Total Pogram Duration:

1270 Hrs / 50 Weeks

CONTACT

+1 (647) 401-1568

+1 (647) 333-1568

info@ftit.ca

1580 Brimley Road, Scarborough, ON M1P 3G9

www.ftit.ca

PROGRAM SUMMARY

Type of Learning	Total Instruction Hours	% Weight
Theory	**562.00**	44.25
Practical	**618.00**	48.66
Capstone Project	**90.00**	7.09

PROGRAM DELIVERY

Program Delivery	Instruction Weeks	Break Weeks	Total Duration	AVG Hours/Week
IN PERSON	**44**	**6**	**50**	**29**
HYBRID	**44**	**6**	**50**	**29**
ONLINE	**44**	**6**	**50**	**29**

DIPLOMA IN CYBER-SECURITY

#	Course Name	Instruction Hours	Course Details
1.	**Information Security**	70	In this course, students will gain an understanding of information security, security management, and security domains.
2.	**Network Systems and Countermeasures**	70	This course covers network security fundamentals, such as how hackers get access to online networks and how to utilize firewalls and VPNs as security remedies. Students study security from both a managerial and a technical standpoint.
3.	**Legal and Ethical Issues in IT Security**	60	This course examines the legal and ethical challenges that arise in the field of information technology.
4.	**Security Policies**	75	Students examine the fundamental parts of a written information security policy's structure and language, as well as typical policy content and other related documents, such as, procedure, standards, guidelines, and baselines.
5.	**Operating Systems Security**	75	This course introduces defence strategies through understanding of system and file permissions, password, identity and access management, the system Registry, Malware prevention, and encryption.
6.	**Wireless and Mobile Device Security**	75	This course investigates the transition from wired to wireless networking and its implications for business.
7.	**Mobile Application Security Design**	68	The fundamentals of detecting and exploiting defects in mobile applications on the iOS, Android, Blackberry, and Windows Mobile platforms are covered in this course.
8.	**Ethical Hacking and Network Defense**	75	This course teaches students how to identify and fix vulnerabilities in information systems infrastructure.
9.	**Ethical Hacker Tools and Incident Response**	71	Students investigate how assaults target networks and the methods used to carry them out.
10.	**Network Security and Penetration Testing**	68	Students investigate network security, focusing on the most recent threats and flaws.
11.	**Computer Forensics**	75	The goal of this course is to introduce students to computer forensics and investigation procedures.
12.	**Career Planning, Job Search and Employment**	48	This course will teach students how to prepare for jobs in cybersecurity industry
13.	**Ethical Hacking and Countermeasures: Attack Phases**	70	In a supervised lab setting, students learn how to scan, test, hack, and secure their own computers.
14.	**Ethical Hacking and Countermeasures: Threats & Defense**	74	Students will learn how intruders get access to higher levels of power and how to safeguard a system. Students also learn about Trojans and backdoors, among other approaches.
15.	**Ethical Hacking and Countermeasures: Web App. & Data**	68	In a supervised lab setting, students learn to scan, test, hack, and secure their own computers. Students will learn how intruders escalate their privileges and how to safeguard a system.
16.	**Ethical Hacking and Countermeasures: Edge Devices**	70	Students will learn about cryptography, hacking wireless networks, and avoiding network security mechanisms in this course (i.e. IDS, Firewalls, and Honeypots).
17.	**Ethical Hacking and Countermeasures: Cloud Computing and Endpoint Devices**	68	Students will learn about cryptography, hacking wireless networks, and avoiding network security mechanisms in this course (i.e. IDS, Firewalls, and Honeypots).
18.	**FTIT Capstone Project**	90	This initiative connects diverse program areas of study, cuts over subject matter borders, and emphasizes unifying principles in order to improve student performance. The emphasis is on building connections, which allows students to participate in relevant, meaningful activities that are linked to and performed in real life.