CYBERSECURITY, POST-DEGREE PROFESSIONAL CERTIFICATE

Students will prepare for careers dealing with networking and system administration fundamentals, with the primary focus being defensive strategies to securing networks and systems. Skills acquired will assist students in preparing to take nationally and internationally recognized industry certification exams.

Program contact: Learn more (http://www.tri-c.edu/programs/information-technology)

Financial Assistance funds cannot be applied towards this program. Request for eligibility to utilize Financial Assistance funds for this program is currently pending.

This certificate will be automatically awarded when the certificate requirements are completed. If you do not want to receive the certificate, please notify the Office of the Registrar at RegistrarOffice@tri-c.edu.

Learn more here (http://catalog.tri-c.edu/pathways/business/information-technology-cybersecurity) about how certificate credits apply to the related degree.

Related Degrees and Certificates

- Information Technology - Cybersecurity, Associate of Applied Business (http://catalog.tri-c.edu/programs/information-technology-cybersecurity-aab)

Program Admission Requirements

- High School Diploma/GED.
- ENG-0990 Language Fundamentals II or appropriate score on English Placement Test.
- MATH-0955 Beginning Algebra with "C" or higher or appropriate score on Math Placement Test.
- Applicant must have already completed an associate degree or higher from an accredited college or university.
- Information technology networking background and/or experience in the field.
- Basic programming skills required.
- 18 years of age or older.
- Background check required.

Program Learning Outcomes

This program is designed to prepare students to demonstrate the following learning outcomes:

1. Apply principles of security to install, configure, maintain, and secure business operations.
2. Take continuous, pro-active measures to intimately know and understand the complete physical and logical structure of your network so that during normal operations and monitoring, security issues can be quickly identified, isolated and resolved, including measures to prevent future occurrences.
3. Apply fundamental concepts of operating systems, business applications, networking, security, backup and recovery procedures to troubleshoot, maintain, and support hardware and software to ensure efficient and effective business operations.
4. Explain what a risk assessment is, what types of assessments there are and how it can impact an organization. Also explain drivers to information security policy/standard development, security governance, compliance to external regulation and internal policies and standards.
5. Identify common industry security frameworks and explain why these exist. (NIST, Cyber Security Framework, CYBER, COBIT, ISO27001, etc.)
6. Apply analytical, critical and creative thinking and problem solving/troubleshooting techniques to reduce risk in business operations.
7. Plan, organize, and prioritize tasks in order to meet project deadlines.
8. Understand and apply legal, privacy, and ethical concepts; recognize and assess legal, privacy, and ethical issues; and demonstrate ethical, privacy, and legal behavior.

Suggested Semester Sequence

Course	Title	Credit Hours
Summer Semester		
ITNT-2320	Network Administration I	3
ITNT-2370	Network Security Fundamentals	3
	Credit Hours	6
First Semester		
EET-1302	Cisco I: Basic Networking Technologies	3
EET-1312	Cisco II Basic Routing and Switching	3
ITNT-2380	Linux Administration	3
IT-2750	Scripting Fundamentals for Cybersecurity	3
	Credit Hours	12
Second Semester		
IT-2710	Advanced Topics in Network Security	3
IT-2720	Ethical Hacking and Systems Defense	3
IT-2730	Intrusion Detection/Prevention Systems Fundamentals	3
	Credit Hours	9
	Total Credit Hours	27