CYBERSECURITY AND DEFENSE GRADUATE CERTIFICATE

Introduction

This certificate is designed for working professionals in the field of computer science, network and/or security operations. Students are highly recommended to have a background in Computer Science, but will be individually evaluated during the application process. It consists of graduate-level courses in cybersecurity, operating systems, and computer networks or cloud computing. The certificate program in Cyber Security and Defense will prepare Computer Science professionals to identify, analyze, and mitigate technical cybersecurity related vulnerabilities, exploits and attacks against network and critical cyber infrastructure. The coursework emphasizes practical technical skills, analysis and research focused on current cybersecurity issues.

Certificate Objectives

With the advent of greater network, application, and infrastructure connectivity there are more advanced methods of cyber-attack. This certificate program focuses on both the technical and analytical aspects of advanced cybersecurity and defense. Graduates of this certificate program will learn how to mitigate known cyber-related attacks against multiple network and infrastructure devices. Graduates will also learn how to design secure solutions, analyze new cyber-attacks and provide solutions that balance risk, security, privacy, cost, and operations. Each course in this certificate program provides project-based opportunities to extend technical skills in programming, network, operating system, infrastructure design and analysis as well as understanding prevention of cybersecurity breaches and incidents

Certificate Eligibility

A BS or equivalent in Computer Science is ideal. Applicants with BS degrees other than computer science will be individually evaluated for adequate knowledge in programming, algorithms, and system design and may be assigned additional courses to take as part of the certificate program to address deficiencies in their background.

Students currently in BS-CS degree or in CS Scholars (Dual BS-MS) program at CU Denver need to have completed the undergraduate Operating Systems & Computer Networks and the recommendation of their academic advisor

Program Requirements

Program Learning Outcomes

1. Demonstrate an in-depth understanding of cybersecurity principles and practices.

2. Identify and analyze various types of cyber and infrastructure threats and apply basic cybersecurity defense concepts to develop and assess defensive solutions against them.

3. Apply cybersecurity knowledge and skills to maintain operations in the presence of risks.

4. Understand the national needs in the area of cybersecurity and learn the necessary skills to advance their careers as practicing cybersecurity professionals.

5. Understand their professional responsibilities and make informed judgments in their cybersecurity practices based on legal and ethical principles.

Process to Attain Certificate Objectives

Students will need to complete a sequence of four separate graduate-level courses

Code	Title	Hours
CSCI 5742	Cybersecurity Programming and Analysis	3
CSCI 5743	Cyber and Infrastructure Defense	3
CSCI 5573	Operating Systems	3
CSCI 5765	Computer Networks	3
Total Hours		12

Students must take and pass each course with a grade of B- or better and earn a GPA of at least 3.0 to obtain the Cybersecurity and Defense Certificate.