University of San Diego

MS IN CYBER SECURITY ENGINEERING

FULL-TIME PROGRAM

Take the Next Step and Transform Your Career

Earn Your MS in Cyber Security Engineering

This on-campus full-time (FT) Master of Science in CyberSecurity Engineering (MS-CSE) program is offered through USD's Shiley-Marcos School of Engineering. The MS-CSE (FT) program emphasizes critical skills for cyber practitioners (public and private) in ethics, applied and theoretical technical knowledge and skills, cross- domain learning, and a mission-centric focus who protect the prosperity and safety of the community and nation. The program is academically rigorous focusing on the engineering aspects of software and hardware security.

Course of Study

The 30-unit program consists of ten courses. Courses are offered over three semesters every year; fall, spring, and summer. Each semester lasts 14 weeks. Students take Three or four courses per semester. Courses run for seven weeks each with a one or two week break in between semesters. This intensive format allows students to focus on completing the degree program in one year (three semesters).

Who is the program for?

Bachelor-prepared traditional students and professionals who desire to affect positive change in engineering solutions to mitigate cybersecurity threats and need a full-time one-year program. It is designed for those coming from traditional educational paths, military, intelligence community, industry, government, law, ecommerce, technology industries and public safety agencies.

Subject to change.

Admission Requirements

- Bachelor's degree from an accredited institution
- Bachelor's GPA of 3.0 or higher
- TOEFL scores of 120 or minimum Duolingo English Test score of 120 (if applicable)
- Statement of purpose
- Letter of support from the candidate's employer or two letters of reference
- Resume showing information technology experience as demonstrated through academic or career experience
- Students are required to bring a laptop to all courses

Program Objectives

Prepare to take on modern cybersecurity engineering challenges and contribute positively to organizations and communities.

1. Developing an engineering knowledge and skill base that will allow mitigation of advanced persistent threats toward the goal of increased cybersecurity
2. Developing individuals capable of cutting-edge innovation, creating the next generation of cyber tools and solutions, and becoming thought leaders in the domain
3. Engaging in a strategy of integration with local and national stakeholders
4. Advancing the science and practice of cybersecurity engineering and education for the nation

cyberengineering@sandiego.edu

MS IN CYBER SECURITY ENGINEERING PROGRAM CURRICULUM DESIGN

The MS-CSE program consists of 10 courses total. Each student will take 2 foundational courses (CYBR 501 and 502), 6 core courses (CYBR 503, 504, 506, 508, 510, and 512) and 2 capstone courses (CYBR 514 and 516). Students will follow the curriculum path as prescribed below.

Semester	Summer		Spring		Fall	
A	CYBR 501 (3 Units)	CYBR 502 (3 Units)	CYBR 506 (3 Units)	CYBR 510 (3 Units)	CYBR 514 (3 Units)	CYBR 504 (3 Units)
B	CYBR 503 (3 Units)		CYBR 508 (3 Units)	CYBR 512 (3 Units)	CYBR 516 (3 Units)	
	Total Units	9	**Total Units**	12	**Total Units**	9

For this on-campus program, courses are taught in 7-week blocks with two blocks (A & B) for each semester (14 Weeks). These courses meet twice a week for three-hour sessions.

Foundational Courses

- CYBR 501 - Introduction to Cybersecurity Concepts and Tools
- CYBR 502 - Cybersecurity Network Defense

Core Courses

- CYBR 503 - Cybersecurity Domain
- CYBR 504 - Applied Cryptography
- CYBR 506 - Security System Life Cycle
- CYBR 508 - Secure Network Engineering
- CYBR 510 - Security Test Engineering
- CYBR 512 - Incident Detection and Handling

Capstone Courses

- CYBR 514 - Cyber Engineering Research I
- CYBR 516 - Cyber Engineering Research II

NATIONAL CENTERS OF ACADEMIC EXCELLENCE IN CYBERSECURITY

Subject to change.

WASC
Senior College and
University Commission