COURSE DESCRIPTIONS

Master of Science in
Cyber Security Engineering

PROGRAM LEARNING OUTCOMES

Offered through USD's Shiley-Marcos School of Engineering, the Master of Science in Cyber Security Engineering (MS-CSE) program prepares students to:

1. **Employ** the foundational concepts of cybersecurity and systems engineering principles to build and field secure systems throughout the entire secure systems development life cycle.
2. **Analyze** a system to determine the cybersecurity objectives, policies, and threats, and select appropriate and cost-effective security controls to mitigate risk.
3. **Perform** system security assessments by applying skills in security testing, forensics, incident response, and continuity planning.
4. **Demonstrate** the ability to write programs to automate cyber system tasks.
5. **Recognize** professional responsibilities and make informed judgments in cybersecurity practice based on legal and ethical principles.

PROGRAM FORMATS

100% ONLINE PROGRAM:

- 20-24 Months
- 30-36 Total Units
- $1,290 per unit
- New students start in Spring, Summer or Fall

ON-CAMPUS, PART-TIME PROGRAM:

- 20-24 Months
- 30-36 Total Units
- $2,000 per unit
- New students start in Spring, Summer or Fall

ON-CAMPUS, FULL-TIME PROGRAM:

- 18 Months
- 36 Total Units
- $2,000 per unit
- Intakes in Fall and Spring

cyberengineering@sandiego.edu | (619) 260-4585

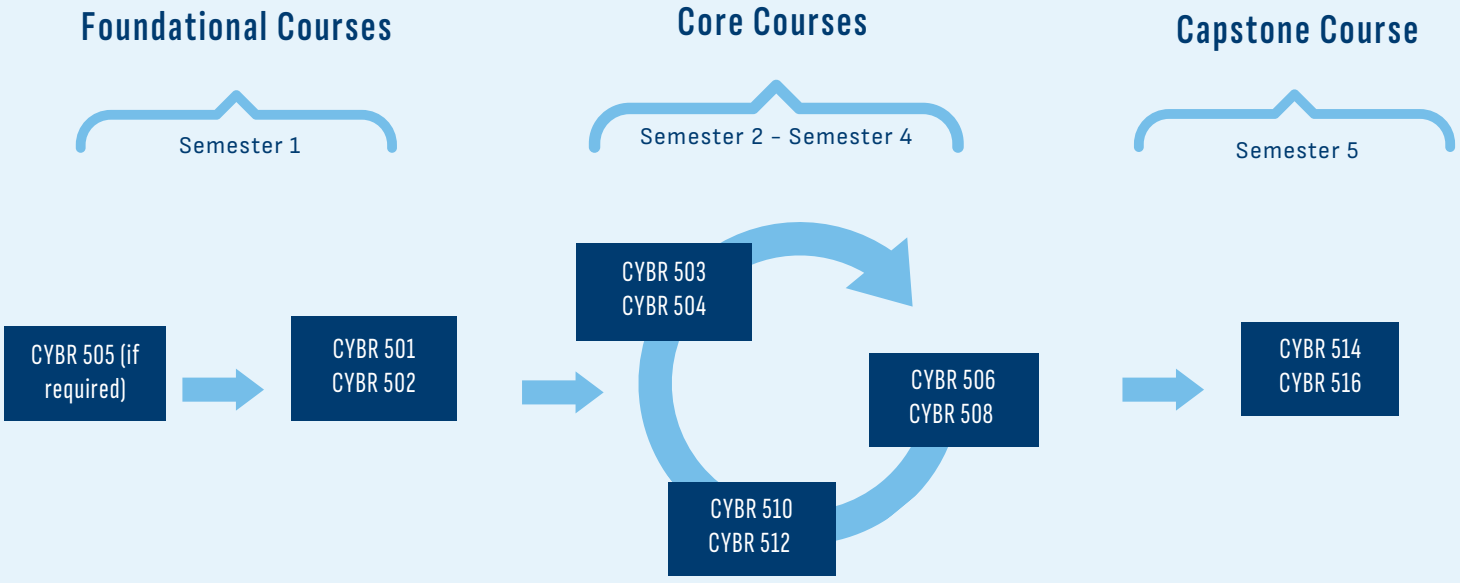
UNDERSTANDING THE COURSE CAROUSEL

Courses in the MS-CSE program are scheduled on a carousel, which allows new students to start at any time. All students will take foundational courses during their first term, which will prepare them for the core courses to follow.

The academic year is comprised of three 14-week terms, with breaks from one to three weeks between each term:

- Fall - courses start in September
- Spring - courses start in January
- Summer - courses start in May

Each course lasts a total of seven weeks with the only exception being introductory courses, which are 14 weeks. Students take two courses each semester, focusing intensively on one course at a time.



FOUNDATIONAL COURSES

CYBR 505: COMPUTATIONAL ROOTS OF CYBERSECURITY

Accelerated introduction to software systems with an emphasis on computer programming, computer architecture, and operating systems. Six hours of lecture-lab weekly.

CYBR 501: INTRODUCTION TO CYBERSECURITY CONCEPTS AND TOOLS

An introduction to the fundamentals of cybersecurity, including the notion of policy as the definition of "security" for a system and the concepts of threats, vulnerabilities, and risk. We will survey common attacks and mitigations, and the shortcomings of common, contemporary cybersecurity models. Students will practice aspects of networking, operating systems, and security test tools through computer virtualization and hands-on labs and will assemble a penetration testing Cybersecurity Sandbox with multiple virtual machines that they will use in subsequent courses and will demonstrate the use of a set of security test tools. Prerequisites: CYBR 505 (can be waived by MS-CSE Program Director based on student's academic and professional background)

CYBR 502: CYBERSECURITY NETWORK DEFENSE

This course is an introduction to fundamental concepts of computer network security and defense, including planning, architecture, system design and deployment, risk assessments, and identifying network security threats from a cybersecurity perspective. Cybersecurity network testing will be conducted in the virtualized Cybersecurity Sandbox that students implemented in CYBR 501. Prerequisites: CYBR 501

CORE COURSES

CYBR 503: CLOUD SECURITY OPS

This course focuses on securing modern cloud and virtualized environments using industry-standard architectures and frameworks. Topics include cloud service models and shared responsibility, identity and access management, Zero Trust principles, secure cloud networking, data protection, infrastructure-as-code security, container and Kubernetes security, and cloud threat detection and incident response. Students apply risk frameworks and security controls through hands-on labs conducted in the Cybersecurity Sandbox. Prerequisites: CYBR 501 and CYBR 502

CYBR 504: APPLIED CRYPTOGRAPHY

This course is an introduction to core principles of modern cryptography and applied cryptographic methods and systems. It includes description of common cryptographic algorithms, pseudorandom generators and encryption. Students will explore the application and assessment of cryptographic techniques for enforcing security policies. Class labs and project will be conducted in the Cybersecurity SandBox. Prerequisites: CYBR 501 and CYBR 502

CYBR 506: AI/ML SECURITY

This course introduces the security risks and defenses associated with artificial intelligence and machine learning systems. Students examine AI/ML threat models, data integrity and provenance, secure model pipelines, adversarial attacks, privacy risks, and governance frameworks such as the NIST AI Risk Management Framework. Through hands-on labs, students design, test, and defend ML systems against adversarial manipulation while assessing residual risk and compliance considerations. Prerequisites: CYBR 501 and CYBR 502

CORE COURSES

CYBR 508: PENETRATION TESTING & ADVERSARIAL OPERATIONS

This course provides hands-on experience in offensive security and adversarial operations. Topics include reconnaissance, vulnerability discovery, exploitation, privilege escalation, lateral movement, and adversary emulation aligned with the MITRE ATT&CK framework. Students conduct penetration testing engagements within a controlled lab environment, validate defensive detections, and produce professional technical and executive-level reports using the Cybersecurity Sandbox. Prerequisites: CYBR 501 and CYBR 502

CYBR 510: SECURITY TEST ENGINEERING

This course presents various methodologies for performing security testing to ensure a system correctly enforces the security policy. Topics include creating and configuring test environments based on security requirements; differentiating between functional testing and security testing; and types of testing such as static, dynamic, vulnerability, and penetration testing; Labs and projects for the course will utilize the Cybersecurity Sandbox. Prerequisites: CYBR 501 and CYBR 502

CYBR 512: INCIDENT DETECTION AND HANDLING

In this course techniques for assuring the continued operation of secure systems in contested environments will be explored. The course through lecture, labs and projects continue to students to use these techniques for the detection of, response to, and recovery from security incidents. Labs and projects for the course will utilize the Cybersecurity Sandbox. Prerequisites: CYBR 501 and CYBR 502

CAPSTONE COURSES

CYBR 514: CYBER ENGINEERING RESEARCH

In Research 1, students will be introduced to a multi domain international company that requires cybersecurity support to update and formalize the security of the enterprise. Student will be required to apply knowledge and skills learned throughout the Cybersecurity Engineering curriculum. The class will form a project team and break into work groups and in a virtual environment develop and implement an Information Systems Security Plan to secure a three-city international structure design private company (Design World Case Study). The groups will be provided a virtual environment with the enterprise systems design in place as per the Case study. Prerequisites: CYBR 501, CYBR 502, CYBR 503, CYBR 504, CYBR 506, CYBR 508, CYBR 510, and CYBR 512

CYBR 516: CYBER ENGINEERING RESEARCH II

In Research II, students will continue the implementation of the capstone case study introduced in Research I a multi domain international company that requires cybersecurity support to update and formalize the security of the enterprise. Students will be required to apply knowledge and skills learned throughout the Cybersecurity Engineering curriculum. The class will be provided a virtual environment with the enterprise systems design in place as per the Case study. Prerequisites: CYBR 501, CYBR 502, CYBR 503, CYBR 504, CYBR 506, CYBR 508, CYBR 510, CYBR 512, and CYBR 514