COURSE DESCRIPTIONS

Master of Science in Cyber Security Operations and Leadership

PROGRAM DETAILS

The career-building online Master of Science in Cyber Security Operations and Leadership program (MS-CSOL) is ideal for bachelor-prepared students who are currently working in a wide range of cybersecurity roles, as well as those interested in pursuing professional opportunities in cybersecurity.

- 30 units completed in under 2 years
- 2 courses per term, 1 course at a time, 7 weeks for each course
- $995 per unit
- New students start this program in Spring, Summer or Fall

PROGRAM LEARNING OUTCOMES

The MS-CSOL program prepares students to achieve four specific outcomes:

1. Develop specialized field knowledge and integrate knowledge across content areas of cybersecurity.
2. Demonstrate critical inquiry through field-based approaches and methods and through effective and ethical information search strategies.
3. Apply learning across multiple contexts within the field, integrating knowledge and practice specifically relating to the areas of cybersecurity and leadership.
4. Reason ethically in evaluating general perspectives, policies, and/or practices relevant to cybersecurity as well as evaluating diverse points of view to include cultural, linguistic, sociopolitical and/or technological contexts.

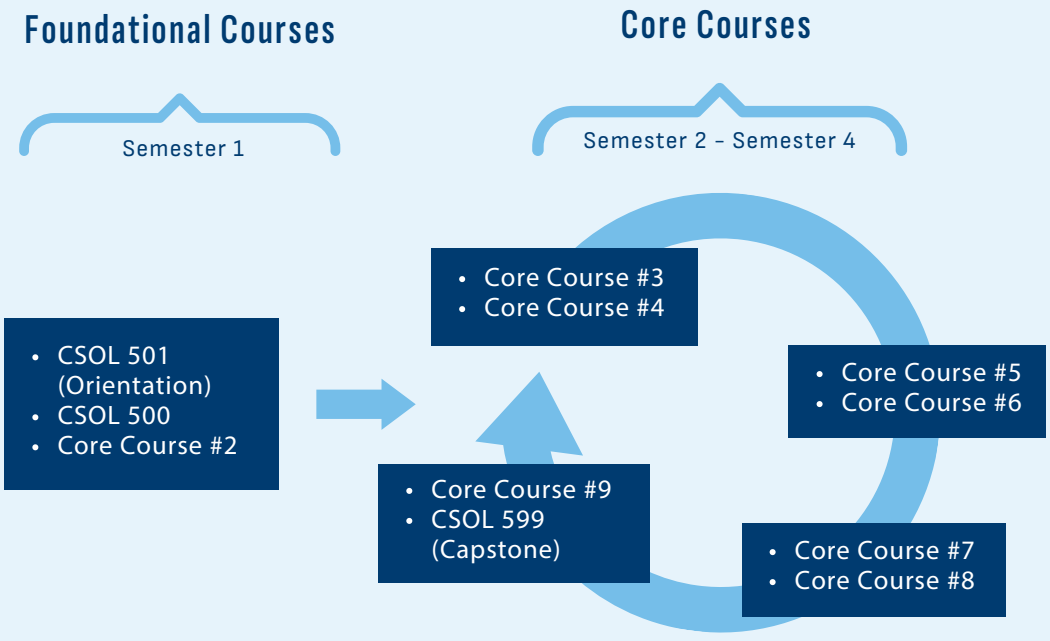
UNDERSTANDING THE COURSE CAROUSEL

Courses in the MS-CSOL 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.



Core Courses

CSOL 500: Foundations of Cyber Security
CSOL 510: Applied Cryptography
CSOL 520: Enterprise Security Architecture
CSOL 530: Governance & Risk in Cybersecurity
CSOL 540: Cybersecurity Law & Policy
CSOL 560: Secure Software Design and Development
CSOL 570: Fundamentals of Blue Team Operations
CSOL 580: Cyber Threat Intelligence
CSOL 590: Cyber Incident Response and Computer Network Forensics

COURSE DESCRIPTIONS

Master of Science in
Cyber Security Operations
and Leadership

FOUNDATIONAL COURSE

CSOL 500: FOUNDATIONS OF CYBER SECURITY

This course will feature a comprehensive overview of concepts and tools essential to the cybersecurity professional and review various types of cybersecurity techniques. The student will learn what cybersecurity means and what it protects as well as future trends and identifying the roles leaders can play in enhancing, supporting, and promoting cybersecurity in organizations. The course will outline a taxonomy of modern cyber terminology. This course will also set the stage for the program by explaining and instilling the “Business of Cyber” and "Cyber Culture" as a cybersecurity professional. The student will learn to view information as an asset to the organization, learn types of cybersecurity attacks, what are threat actors and threat vectors, the various roles of a cyber-professional, and the beginnings of designing a cybersecurity program. The student will also identify different types of threats to information and to the infrastructure and the operations that support it.

CORE COURSES

CSOL 510: APPLIED CRYPTOGRAPHY

This course introduces modern cryptography applications in the context of information security emphasizing practitioner-based approach. The course takes an executive perspective to demonstrate strategic integration of cryptography best practices and controls within enterprise cybersecurity programs and to strengthen the overall security posture of organizational assets and processes.

CSOL 520: ENTERPRISE SECURITY ARCHITECTURE

This course will introduce the student to the importance of architectural and network security at the enterprise level. Security architecture frameworks will be used to explore enterprise security architectures. Students will identify threats to today's networks and learn to identify appropriate security tools to safeguard these networks. The course will discuss how to evaluate the complexities of securing new types of networks such as cloud configurations and the Internet of Things

CSOL 530: GOVERNANCE & RISK IN CYBERSECURITY

This course discusses and explains the fundamentals of risk governance, the processes to follow, compliance regulation, and the security controls to implement for specific cybersecurity environments and situations. Information and information systems are subject to serious threats that can have adverse impacts on organizational operations (including mission, functions, image, and reputation). Cyber-attacks are often aggressive, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. There is also a geopolitical part to cybersecurity as well that is discussed throughout this course. Successful attacks on public and private sector information systems can affect organizational assets, individuals, other organizations, and the Nation by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. This can result in serious damage to the national and economic security interests of the United States.

CORE COURSES

CSOL 540: CYBERSECURITY LAW & POLICY

This course provides students with an introduction to and discusses the relationship between cybersecurity, cybersecurity law and privacy law, and "reasonable security measures". The students will learn the responsibilities of a cybersecurity professional and cybersecurity counselor. The course will explore laws, regulations, and policies; enforcement, compliance, and litigation; consumer data privacy; US federal, state, and EU laws; and future trends.

CSOL 560: SECURE SOFTWARE DESIGN AND DEVELOPMENT

This course will provide an in-depth study of the principals and tenets of the design and development process of secure software used to provide enhanced cyber security. It will review the traditional models of software development, with the idea that a developer or project manager must strategize for security before starting development. Students will understand how to gather and plan for security requirements in development. The course will explore how vulnerabilities can be mapped and planned for. Students will understand how to run an effective development process, culminating with - implementation, and how to review and test software. Finally, the course will introduce the concept of software assurance and its role in the cyber security paradigm.

CSOL 570: FUNDAMENTALS OF BLUE TEAM OPERATIONS

Active defense of an enterprise is not only the responsibility of the equipment, applications, and security processes of an organization but is ultimately driven by Blue Team actions. Whether as a team, designated position, or assigned set of additional responsibilities, understanding and performing Blue Team actions are essential aspects of an effective cybersecurity program. Some of the fundamental concepts for Blue Team operations include "Defending the Castle" by environment and threat landscape awareness, establishing "normal" vs "abnormal" for your environment, understanding Threat Hunting tools and techniques, as well as the components of some of the more significant threats to your organization such as lateral movement, malware, ransomware, and Command & Control. This course will also briefly introduce the concepts and relationships between the Blue Team with the related White, Red, and Purple Teams.

CORE COURSES

CSOL 580: CYBER THREAT INTELLIGENCE

The purpose of this course is to provide an introduction to Cyber Threat Intelligence (CTI) with direct application to corporate (commercial) cyber security operations. It examines the basics of the intelligence life cycle, the analytical frameworks of intelligence, and the types of cyber threat intelligence. The course includes the fundamentals of open source intelligence, refining information into actionable intelligence, and anticipating threats to the cyber domain. The focus is to give you the skills to develop and implement a Cyber Threat Intelligence Program, with an objective, and a timely, relevant quantitative threat assessment tailored to your specific industry. Topics include business competitive intelligence, and cyber threat assessment with a review of past and current threats coupled with an examination of business case studies to highlight the role of intelligence (both failures and successes) in cyber security operations.

CSOL 590: CYBER INCIDENT RESPONSE AND COMPUTER NETWORK FORENSICS

This course will introduce the principles and general practice of incident response, including an overview to digital and network forensics. It will define what constitutes an incident, what is meant by incident response, the attack lifecycle, and goals of incident response. The course will discuss building an incident response team, the steps in the process, and preparing for incident response. Students will understand the process of detecting and characterizing an incident, collecting and analyzing data, and the process of remediation. The course will then provide a deeper dive into the practice of digital forensics, specifically focusing on computer, mobile, network, and database forensics. It will outline the investigative and analysis process, survey tools, digital evidence, and briefly touch on the law.

CAPSTONE COURSE

CSOL 599: REAL-WORLD CYBERSECURITY CASE STUDY

In the final course of the program, students demonstrate the specialized knowledge, principles, and strategies learned throughout the program by critically assessing a real-world cybersecurity problem. Students will demonstrate achievement of the program learning outcomes by tying together the major concepts, skills, and examples of ethical leadership that were included in the program curriculum. The Capstone is the culmination of all coursework from the program to prepare students to develop into skilled cybersecurity professionals. The final project is centered on a case study relating to a current cybersecurity issue, trend, and/or event. Prerequisites: CSOL 500, CSOL 510, CSOL 520, CSOL 530, CSOL 540, CSOL 560, CSOL 570, CSOL 580, and CSOL 590.