CYBERSECURITY ANALYTICS MASTER OF SCIENCE

Leading to a Master of Science Degree in Cybersecurity Analytics

Cybersecurity Analytics blends the disciplines of Cybersecurity and Data Science to give students deeper insight and analysis capabilities for modern enterprise-scale cybersecurity environments. Cybersecurity is a constantly growing discipline to protect organizational digital assets from unauthorized usage. Modern cybersecurity systems are producing an unprecedented amount of data through system logs, application events, security tool alerts, and more. Cybersecurity analytics is built on this collection of internal and external data such as logs, scans, and threat intelligence to identify anomalous events, and the tools to analyze and infer from these varied data sources are also developing at an accelerated rate. This provides an opportunity for a cybersecurity professional to capitalize on the data revolution and these tools by applying them to modern enterprise cybersecurity platforms. The goal of the Master of Science in Cybersecurity Analytics program is to enable students to become cybersecurity professionals proficient in data science tools and skills to expedite the response to cybersecurity events.

Program Educational Outcomes

The program educational outcomes for the Master of Science in Cybersecurity Analytics that align with the listed graduate student learning outcomes developed by the Office of Institutional Effectiveness are as follows:

- Apply predictive and probabilistic approaches to assess cyberrisk
- Design data-driven solutions that integrate cybersecurity concepts from the design phase through implementation
- Identify critical cybersecurity issues across different domains or industries
- Analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats

Student Outcomes

Wentworth published the following graduate student learning outcomes developed by the Office of Institutional Effectiveness in The Wentworth Model. Our graduate students will be able to demonstrate their mastery of these skills through the coursework required in the programs. The mapping of the Learning Outcomes to coursework will be as follows:

- Core Knowledge: advanced knowledge in a specialized area consistent with the focus of their graduate program, including critical thinking and problem-solving.
- Scholarly Communication: advanced proficiency in written and oral communication, appropriate to purpose and audience.
- Professionalism: advanced intellectual and organizational skills of professional practice, including ethical conduct.
- Research Methods and Analysis: quantitative and qualitative skills in the use of data gathering methods and analytical techniques used in typical research that is consistent with the focus of their graduate program.

The program has a thesis option with 33 required credit hours, and a non-thesis option with 36 required credit hours. Either option has the students undertake an individualized development experience, either as a two-course Thesis, or a two-course capstone project. Students must complete the course requirements with a cumulative GPA of at least 3.0, following Wentworth graduate school policies.

Thesis Option

Course	Title	Credits
SEMESTER 1		
DATA6000	APPLIED STATISTICS FOR RESEARCH	3
DATA6150	DATA SCIENCE FOUNDATIONS	3
COMP6500	ADVANCED NETWORK SECURITY	3
SEMESTER 2		
DATA6200	DATA MANAGEMENT	3
DATA6250	MACHINE LEARNING FOR DATA SCIENCE	3
COMP6550	THREAT INTELLIGENCE	3
SEMESTER 3		
COMP7500	THESIS I	3
*ELECTIVE		3
*ELECTIVE		3
SEMESTER 4		
COMP7550	THESIS II	3
*ELECTIVE		3
Total Credits		33

Non-Thesis Option

Course	Title	Credits
SEMESTER 1		
DATA6000	APPLIED STATISTICS FOR RESEARCH	3
DATA6150	DATA SCIENCE FOUNDATIONS	3
COMP6500	ADVANCED NETWORK SECURITY	3
SEMESTER 2		
DATA6200	DATA MANAGEMENT	3
DATA6250	MACHINE LEARNING FOR DATA SCIENCE	3
COMP6550	THREAT INTELLIGENCE	3
SEMESTER 3		
DATA6900	CAPSTONE I	3
*ELECTIVE		3
*ELECTIVE		3
SEMESTER 4		
DATA6950	CAPSTONE II	3
*ELECTIVE		3
Total Credits		33

Electives

A total of 12 semester credit hours of electives must be taken as a part of the program. Students may choose, after consultation with their primary advisor, among the electives offered each semester. The school may add to the list of available electives on a semester by semester basis. One of the electives must be either COMP6420 or COMP6520.

Course	Title	Credits
COMP6420	REVERSE ENGINEERING	3
COMP6520	MALWARE ANALYSIS	3

Course	Title	Credits
COMP6580	DIGITAL FORENSICS AND INCIDENT RESPONSE	3
COMP6555		