CYBERSECURITY (CYBR)

CYBR2500 SECURITY PRINCIPLES
The course introduces computer and network security concepts and techniques. Theoretical concepts of security are examined as well as implementing system and network security. (4 credits) fall, spring

CYBR3500 NETWORK SECURITY
This course covers all aspects of securing and protecting a local area network from threats and vulnerabilities. Students configure, test, and validate standard network services and devices at all layers of the network. ***Prerequisites:*** *COMP1100 and CYBR2500 (4 credits)*

CYBR3550 COMPUTER SECURITY
This course covers all aspects of securing and protecting a computer system from threats and vulnerabilities. Topics include password hashing and protection, virus detection, server security hardening, and application software protection. ***Prerequisites:*** *CYBR2500 (4 credits) summer*

CYBR3590 APPLIED CRYPTOGRAPHY
This course is an introduction to the basic theory and practice of cryptographic techniques used in modern information security systems. Cryptography provides important tools for ensuring the privacy, authenticity, confidentiality, and integrity of data involved in modern information systems. This course examines the progress from historical symmetric encryption standards and protocols to the modern public key encryption processes. Basic concepts of ciphers, blocks, hashes, MACs, and key rotation strategies are discussed. Different implementation approaches and their performance impacts are presented, along with potential attack strategies and their efficacy. ***Prerequisites:*** *COMP2350 and CYBR2500 (4 credits) summer*

CYBR4500 OFFENSIVE SECURITY
This course identifies the tools, techniques, strategies, and motivations of system intruders. In doing so, this course provides students with the skills necessary to ethically search, identify, and perform active assessment of enterprise systems, typically called penetration testing. Thus students are able to preemptively identify the mechanisms by which attacks are perpetrated and the methods by which they can be prevented, defended or remediated. The hands-on activities are based on environments that minimize risk, and possible legal, ethical, or network availability issues.***Prerequisites:*** *CYBR2500 (4 credits) spring*

CYBR4550 INCIDENT RESPONSE & BUSINESS CONTINUITY
This course covers the process and implementation of incident response plans that adhere to appropriate business continuity plans. Students design, implement, and test incident response processes for a variety of scenarios to ensure that the recovery time of their systems is within the limits specified in a continuity plan for an organization. Different incident response strategies, such as SAN PICERL, Lockheed Cyber Kill Chain, MITRE ATT&CK, etc. are investigated. The tools, techniques and methodologies for enacting the incident response plan, processes, and procedures will be utilized. Critical documents such as Disaster Recovery Plan, Business Impact Analysis Plan, and Business Continuity Plans are analyzed, developed, and assessed. ***Prerequisites:*** *CYBR3550 (4 credits) summer*

CYBR5500 SENIOR PROJECT
This course provides the opportunity for students to participate in the design and implementation of solutions for a large project in a team-based environment. The scope of projects are in the cybersecurity field. Students are required to provide written documentation and give oral presentations about their projects. The projects are chosen in conjunction with the instructor for the course. ***Prerequisites:*** *CYBR4500 (4 credits) summer*

CYBR5740 ADVERSARIAL ROBUSTNESS IN MACHINE LEARNING
This course examines a broad range of adversarial attacks targeting machine learning and deep learning systems, with an emphasis on their implications for security and privacy, and explores the challenges and emerging strategies for designing robust and trustworthy models. (3 credits) fall

CYBR6420 REVERSE ENGINEERING
This course introduces the concepts for reverse engineering of both binary (compiles) and interpreted software. Key concepts and tools for analysis of the construction and operation of software are critical to the course. Students gain practical experience with assemblers and disassemblers, source code debugging, hex editors, code auditing, and different binary file formats. This course focuses on 32- and 64-bit architectures (Intel and AMD) for the Microsoft Windows platform. Alternative architectures, such as ARM and Power, are will be covered as contrasting options. (3 credits) fall, spring, summer

CYBR6520 MALWARE ANALYSIS
This course introduces fundamental concepts of active malware analysis. The course defines and develops the skills needed to analyze and dissect modern malicious software threats. Students develop a workflow that includes the use of static and dynamic tools to assess and reverse engineer a variety of file formats commonly used by threat actors. Assemblers and disassemblers for 32-bit and 64-bit architectures are utilized to analyze files and code samples. Basic reporting strategies and outlets are discussed. (3 credits) fall, spring, summer

CYBR6550 THREAT INTELLIGENCE
This course addresses the evolving discipline of threat intelligence as it applies to threat hunting. The course focuses on the challenges of threat hunting in enterprise-scale networks, and the options available to address these challenges. Different threat hunting models are presented and discussed for usage in strategic, operational, and tactical environments. The course also addresses threat actor motivations, capabilities, and tactics in order to better implement data-driven collection, evaluation, identification, collation, correlation, and action. (3 credits) fall, spring, summer