CYBERSECURITY (CYBR)

CYBR3110 | Systems Security I | Lecture/Laboratory (3 Credits)
Examine, configure and troubleshoot authentication and authorization applications supporting confidentiality and integrity. Topics include the basics of symmetric asymmetric encryption and their implementation for authentication and protection of data at rest and in transit as well as implementing patch management, hot fixes, and revision updates and their risks.

CYBR3120 | Software Security | Lecture/Laboratory (3 Credits)
Explore common issues with software security and methods of mitigating attack vectors. Topics include how software is made and maintained, cross site scripting, SQL Injection, the OWASP Top 10 Report, API Gateways and Security, and elements of pen-testing software.

CYBR3130 | Legal Issues & Policy | Lecture (2 Credits)
Examine the responsibilities of the cybersecurity professional in regards to standards, the law, and policy. Topics include data protection standards, common security policies in business, and proper communication with internal and external entities related to policy and supply risk management.

CYBR3140 | Cybersecurity Fundamentals | Lecture (2 Credits)
Discover the many career paths in the wide and growing field of cybersecurity. Explore the world of cybersecurity by researching and practicing industry roles.

CYBR3210 | Systems Security II | Lecture/Laboratory (4 Credits)
Examine methods of protecting against intrusions from within and without. Analyze public key infrastructure and its trust models. Other topics include advanced methods of authentication under the philosophy of "zero trust" as well as an integrated approach to reducing risk, reducing the attack surface, and continuous improvement of the security posture.
Prerequisite(s): CYBR3110
Corequisite(s): CYBR3220

CYBR3220 | Scripting for Cyber Professionals | Lecture/Laboratory (4 Credits)
Use various methods of scripting to automate, test, and secure a computer system. Scripting languages include common shell languages PowerShell and BASH as well as the popular Python language. Detect security issues and use scripts to mitigate the found vulnerability.
Prerequisite(s): CNTS1201, Or CNTS1202, Or CNTS2240
Corequisite(s): CYBR3210

CYBR3230 | Forensic Theory | Lecture (2 Credits)
Explore scientific theory, methods, and evidence preservation from a digital forensics perspective. Emphasis is on the fundamentals of forensic theory, attacker techniques, and procedures used in the cybersecurity profession.

CYBR3231 | Digital Forensic Theory | Lecture (2 Credits)
Explore scientific theory, methods, and evidence preservation from a digital forensics perspective. Emphasis is on the fundamentals of forensic theory, attacker techniques, and procedures used in the cybersecurity profession.

CYBR4110 | Network Security | Lecture/Laboratory (5 Credits)
Explore network security in theory. Examine and practice the use of tools used for protecting networks against malicious attacks. Topics include implementation of secure networking systems including intrusion detection and prevention systems, proxy servers, wireless and point of sales systems and firewall configurations.
Prerequisite(s): CNTS2201

CYBR4120 | Introduction to Cyber Warfare | Lecture (2 Credits)
Examine methods and techniques used to perform politically motivated attacks against other nation states for strategic or military objectives including cyber espionage. Identify diverse motivations of nation state actors, non-state actors such as terrorist groups, companies and politically or economically motivated groups and individuals. Explore both offensive and defensive techniques.
Prerequisite(s): CYBR3230

CYBR4130 | Operating Systems Forensics | Lecture/Laboratory (3 Credits)
Identify common operating system storage techniques. Examine common techniques to retrieve information at file and operating systems levels. Investigate additional artifacts for information that include memory, virtual memory, slack space, and swap spaces.
Prerequisite(s): CYBR3230

CYBR4131 | Operating Systems Forensics | Lecture/Laboratory (3 Credits)
Identify common operating system storage techniques. Examine common techniques to retrieve information at file and operating systems levels. Investigate additional artifacts for information that include memory, virtual memory, slack space, and swap spaces.
Prerequisite(s): CYBR3230

CYBR4210 | Cybersecurity Capstone | Capstone (5 Credits)
Demonstrate overall content knowledge of the program outcomes through a final project. Present project with explanation of skills required by a cybersecurity professional.
Prerequisite(s): CYBR4120 And CYBR4130

CYBR4220 | Network Forensics | Lecture/Laboratory (2 Credits)
Examine network data acquisition methods. Research network protocols vulnerabilities. Activities are related to monitoring and analysis of network data.
Prerequisite(s): CYBR4110

CYBR4221 | Network Forensics | Lecture/Laboratory (2 Credits)
Examine network data acquisition methods. Research network protocols vulnerabilities. Activities are related to monitoring and analysis of network data.
Prerequisite(s): CYBR4110