CYBERSECURITY (CYB)

CYB-101 INTRODUCTION TO INFORMATION SECURITY (3 Credits)
This course is an elective to introduce students in any major to the Information Security field. Students will be introduced to main domains of Information Security and Information Assurance as represented in the COMPTIA Certification exam Security Plus. Upon successful completion of this course as documented through writing, objective testing, case studies, laboratory practice, and/or classroom discussion, the student will be able to: Define information security and explain why it is important Identify types of attackers, analyze vulnerabilites, attacks and suggest appropriate defenses. Descrive various software security applications and vulnerability scanning tools. Explain the different types of logical and physical access control. Understand and explain authentication, authorization and accounting as it relates to compter security. Define and explain risk, risk management, and penetration testing.

CYB-180 SPECIAL TOPICS IN CYBERSECURITY (3 Credits)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CS-132

CYB-202 CYBERSECURITY ETHICS (3 Credits)
This course introduces students to ethical questions that come up in all areas of cybersecurity. We will discuss the ethical ramifications of several different types of hacks. We will explore ethical management in Cybersecurity and explore the concept of ethical hacking.

CYB-333 INFORMATION SECURITY (3 Credits)
This course is designed to introduce students to the development of information security policies and planning. Information systems, and the tools and techniques needed to establish, monitor and maintain information security will be examined.
Prerequisite(s): TAKE CS-131 CYB-101

CYB-354 INTRO TO NETWORK SECURITY (3 Credits)
Introduction to network security auditing. Students will learn how to perform the different phases of an audit, including discovery and penetration, as well as how to prevent hackers from controlling your network. This course introduces various tools to help students in the auditing process. Students will be exposed to international standards, along with time-tested methods for auditing a network efficiently, and they will be able to use specific, practical tools for counteracting network attacks. Finall y, they will be able to analyze all findings and make informed recommendations for establishing the best security possible in a given scenario.
Prerequisite(s): TAKE CS-254
Corequisite(s): TAKE CYBL-354

CYB-355 COMPUTER CRIME (3 Credits)
Computer criminals are becoming ever more technically sophisticated, and it's an increasing challenge to keep up with their methods. This course will focus on computer crimes, what they are, how to prevent them, and how to detect, investigate prosecute them if they do occur and prevent them. Topics such as the impact of computer crimes, digital forensics, as well as computer crime laws will also be covered.
Prerequisite(s): TAKE CS-254

CYB-360 DIGITAL FORENSICS (3 Credits)
This course will provide an introduction to, and develop a foundation in, core concepts related to the field of digital forensics. Topics include an overview of computer crime, computer forensics law, forensic acquisition in lab and field environments, digital triage, mobile devices, identification of forensic artifacts in various operating systems, network forensics, report writing, ethical considerations in forensics, and courtroom testimony. The course will include lectures and hands on experiences using a vareity of forensic tools.
Prerequisite(s): Take CYB-355

CYB-365 INVESTIGATIVE SOFTWARE TOOLS (3 Credits)
Intelligence led policing and intelligence based investigative strategies are coming to the forefront of law enforcement. Private industry is alwso becoming increasingly aware of the strategic intelligence model as it applies to corporate planning, competitce practices and maintaining corporate integrity. This course is designed to introduce students to several key software tools that are widely used and considered essential for intelligence research and criminal investigations. These software tools will include, but not be limited to, Analyst Notebook, iBase, and Idea. Students will be given a thorough understanding of how to apply these tools in the course of the intelligence process and/or during the course of a criminal investigation. The course will culminate with students preparing a project using all the software tools introduced during the course.

CYB-380 SPECIAL TOPICS IN CYBERSECURITY (1-3 Credits)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CS-132

CYB-380A SP TOP IN CYBERSECURITY: ADVANCED CYBERSECURITY (3 Credits)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CS-380C

CYB-380B SP TOP IN CYBERSECURITY:CYBERSECURITY INVESTIGATION (3 Credits)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CYB-101

CYB-380C SPECIAL TOPICS: LAW & POLICIES INVESTIGATION (3 Credits)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CYB-101

CYB-380D SP TOP: THREAT HUNTING FOR MS WINDOWS (3 Credits)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CYB-101

CYB-380E SP TOP.HOW ETHICAL HACKERS CAN COUNTER BLACK HAT HACKERS (1 Credit)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CYB-101

CYB-380F SP TOP.PSYCHOLOGY OF A HACKER (1 Credit)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CYB-101

CYB-380G SP TOP:PRACTICAL HACKING/CYBERSECURITY WITH PYTHON (3 Credits)
An intensive study of an aspect of computer science not fully treated in a regularly scheduled course.
Prerequisite(s): CYB-101

CYB-410 INTRO TO CRYPTOGRAPHY (3 Credits)
In this course, the key terms, concepts and principles of cryptography are defined and explained. Application of cryptographic techniques to ensure confidentiality, integrity, authentication, access control, and non-repudiation issues will also be covered. Other topics will include the history of classical cryptographic and cryptanalytic techniques, modern symmetric and asymmetric algorithms, Federal Information Processing Standard (FIPS) algorithms, random and pseudo-random number generators and cryptographic hash functions.
Prerequisite(s): MATH-207 CS-254 CYB-333

CYB-411 INTRO TO PENETRATION TESTING (3 Credits)
To protect an organization's critical information and assests, cybersecurity professionals must regularly assess an information system's security controls through a process called penetration testing. This course will introduce students to the overall process and principles, as well as more deeply explore the identification of systems, services, and vulnerabilities. Students will be expected to stay up-to-date on emerging security flaws throughout the course, and understand the need for life-long learning in this domain.
Prerequisite(s): CYB-202 CYB-354 CYB-333
Corequisite(s): Take CYBL-411

CYB-413 CYBERSECURITY OPERATIONS (4 Credits)
To protect an organization's critical information and assets, cybersecurity professionals regularly assess an information system's security controls through understanding the evolving networks, systems, and end user use of them. This understanding will help in determining the most effective way of instrumenting the networks and systems to prevent and alert on unusual behaviors and events. The course will emphasize combining contextual enterprise knowledge with threat actor tactics, techniques, and procedures to create targeted detection, prevention, and response policies and processes.
Prerequisite(s): CS-255
Corequisite(s): Take CYBL-411

CYB-491 INTERNSHIP IN CYBERSECURITY (1-3 Credits)
This course provides students with on-the-job training and experience which is not obtainable in classroom situations. The student is expected to secure a full-time position which involves significant work in an area of cybersecurity. Each internship is individually arranged, subject to the approval of the cybersecurity faculty.

CYB-492 IND STUDY IN CYBERSECURITY (1-3 Credits)
Independent study or project in some area of cybersecurity and its application under supervision of cybersecurity faculty.

CYBERSECURITY LAB (CYBL)

CYBL-101 INTRO TO INFORMATION SECURITY LAB (1 Credit)
Corequisite(s): TAKE CYB-101

CYBL-354 INTRO TO NETWORK SECURITY LAB (1 Credit)
Introduction to network security auditing. Students will learn how to perform the different phases of an audit, including discovery and penetration, as well as how to prevent hackers from controlling your network. This course introduces various tools to help students in the auditing process. Students will be exposed to international standards, along with time-tested methods for auditing a network efficiently, and they will be able to use specific, practical tools for counteracting network attacks. Finall y, they will be able to analyze all findings and make informed recommendations for establishing the best security possible in a given scenario.
Prerequisite(s): Take CYB-354TAKE CS-254

CYBL-411 INTRO TO PENETRATION TEST LAB (1 Credit)
Lab component of CYB-411. Through the laboratory component, students will analyze code to identify common flaws, build, and test running systems for vulnerabilities. Students will also learn to document and prioritize risks and technical recommenations for addressing security vulnerabilites. Students will be expected to stay up-to-date on emerging security flaws throughout the course, and understand the need for life-long learning in this domain.
Prerequisite(s): CYB-354 CYB-333
Corequisite(s): Take CYB-411

CYBL-413 CYBERSECURITY OPERATIONS LAB (0 Credits)
To protect an organization's critical information and assets, cybersecurity professionals regularly assess an information system's security controls through understanding the evolving networks, systems, and end user use of them. This understanding will help in determining the most effective way of instrumenting the networks and systems to prevent and alert on unusual behaviors and events. The course will emphasize combining contextual enterprise knowledge with threat actor tactics, techniques, and procedures to create targeted detection, prevention, and response policies and processes.
Prerequisite(s): CS-255
Corequisite(s): Take CYB-413