Cyber Operations (CYB) Courses

CYB1005 Introduction to Cyber Security Operations
This course is designed to provide an introduction to the range of disciplines that are fundamental to protecting cyber assets in the modern world. Students learn what cyber security and operations are, how they have evolved over the past decades, and how the cyber security framework can be applied across a wide range of contexts and industries. This course also provides an introduction to the various technical and non-technical skills that are fundamental in the cyber security and operations field. Students are provided with academic foundations to pursue further study in the cyber field.
Offered at Online, Providence
3 Semester Credits

CYB2010 Computer Architecture with Assembly Language Programming
This course is designed to provide students with an understanding of the relationship between hardware and software through the use of the machine and assembly language facilities. Topics include how simple statements translate into processor commands and how various types of storage and programming structures are implemented in the system. Program design, charting, coding, debugging, testing, execution and documentation are accomplished for all concepts that are introduced. Advanced understanding of the relationship between hardware and software is accomplished through the use of assembly language and higher level language (C programming language) facilities. Creating programs that interface with computer hardware is explored. Additional topics include using debug, decision structures, looping structures, addressing constructs, data types, program segments, memory models, subroutines, arrays, video, keyboard and file I/O, parallel processing, terminate-and-stay-resident programs, recursion, inter-language communication, device drivers and embedded programming concepts.
Prerequisite(s): CSIS1112.
Offered at Online, Providence
3 Semester Credits

CYB3001 Foundations of Digital Forensics
This course introduces students to the principles of digital forensics. The essentials covered in this class include computer system storage fundamentals, operating systems and data transmission, computer network architecture, digital forensics best practices, proper evidence collection and storage, and federal rules and criminal codes. Upon successful completion of this class, the student is ready to proceed into more advanced and technical classes such as computer forensics, mobile device forensics, network forensics, and malicious code forensics.
Prerequisite(s): CSIS1101, CSIS2045, CYB1005.
Offered at Providence
3 Semester Credits

CYB3011 Software Reverse Engineering
This course is designed to introduce students to the tools and process of software reverse engineering, and how to apply the tools and process for the purpose of discovering malicious code, reconstructing higher level code and documentation where none exist, discovering opportunities for improvement of existing code, and assuring the appropriate use of code.
Prerequisite(s): CSIS2045, CYB2010 or ENGN2014.
Offered at Providence
3 Semester Credits

CYB3023 Large Scale Distributed Systems
This course is designed to introduce the principles and implementation techniques of distributed database systems and explore trends and issues concerning database application development. Students apply theory and practice by building a distributed database with web access.
Prerequisite(s): CSIS1112, CSIS2030.
Offered at Providence
3 Semester Credits

CYB3038 HCI/Usable Security
This course focuses on how to design and build secure systems with human-centric focus. Basic principles of HCI (including the basics of humans' cognitive abilities, principles of usability, design techniques and evaluation methods) are discussed. Through professionally focused exercises, students apply these techniques to the design, building, evaluation and critique of secure systems, while developing security measures that respect human performance and their goals within the system. Focus is on authentication devices, password protection techniques, browsing security, social media and mobile device security.
Prerequisite(s): ITEC3050.
Offered at Online, Providence
3 Semester Credits

CYB3205 Malware Forensics
This course introduces students to the fundamentals of malicious code and malicious code analysis. The student is introduced to actual malicious code samples and examines how they work and interact with vulnerable machines. The student learns how to perform basic analysis in an attempt to reverse engineer malicious code capabilities and to perform post-mortem forensic analysis on compromised machines. The student is also introduced to virtual machines and their important role in conducting malicious code forensic analysis in a safe environment.
Prerequisite(s): CSIS1112, CYB3001.
Offered at Providence
3 Semester Credits

CYB3220 Network Forensics
This course immerses students into the world of network forensics. The essentials covered in this class include network forensics investigative methodology, network technical fundamentals, evidence acquisition, packet and flow analysis, network intrusion detection and analysis, and forensic reporting. Upon successful completion of this class, the student is ready to conduct real-world network forensic investigations in a laboratory setting utilizing industry-recognized tools and methodology.
Prerequisite(s): CYB3001, ITEC2081.
Offered at Providence
3 Semester Credits

CYB4010 Computer and Network Forensics
This course introduces students to the nature of digital evidence, the tools and techniques used to acquire such evidence, and the practices used to preserve its integrity through the use of lectures and hands-on exercises. Students are also introduced to the process of testifying and ethics for the expert witness.
Prerequisite(s): Senior status.
Offered at Online, Providence
3 Semester Credits

CYB4026 Cyber Intelligence
This course examines the emerging stages to the current operational and political impact of cyber intelligence. Students explore a full range of cyber capabilities from exploitation, attack and defense. Students analyze and discuss several case studies that demonstrate the challenges and benefits of cyber intelligence to the cyber operations and security environment. This course demonstrates how cyber security and operations have changed the nature of intelligence collections, operations and analysis across the intelligence communities.
Prerequisite(s): CYB3038.
Offered at Online, Providence
3 Semester Credits

CYB4032 Perimeter Protection and Vulnerability Assessment
This course examines the threat from computer hackers and the countermeasures to protect against such attacks, including security policies, security hardware and software technologies, vulnerability analysis, security assessments, penetration testing, and vulnerability scanners. Topics include types of network security, varieties of attacks, fundamentals of firewalls, firewall practical applications, intrusion detection systems, encryption, virtual private networks, operating system hardening, defending against virus attacks, Trojan horses and spyware, security policies, assessing a system, security standards, and computer-based espionage and terrorism.
Prerequisite(s): ITEC3075.
Offered at Providence
3 Semester Credits

CYB4044 Active Cyber Defense and Countermeasures
This course is based on the concept that current, traditional "boxed" defense solutions are no longer working and attackers are becoming more and more successful as a result. Emphasis is on new strategies for IT security professionals to be successful. Topics include tools for proactive defense, such as annoyance, attribution and attack.
Prerequisite(s): CYB4032.
Offered at Providence
3 Semester Credits

CYB4050 Exploitation & Incident Response
This course introduces students to the arts and skillsets of traditional “Red” and “Blue” teams. Participants are immersed into worlds of computer exploitation and incident response, providing the unique experience of learning how to compromise a machine/network and then uncovering and documenting the evidence left behind. In addition, the course teaches the student to utilize a variety of open source tools to exploit weaknesses in a typical networked environment. The class introduces defense techniques aimed at common system/network weaknesses. Topics include physical security, social engineering, reconnaissance, port/network and vulnerability scanning, creating custom exploits, weaponizing documents, and anti-virus evasion.
Prerequisite(s): CYB3205, CYB3220.
Offered at Providence
3 Semester Credits