SIU Southern Illinois University
CARBONDALE

Table of Contents

Cybersecurity Technology

Demand for cybersecurity jobs continues to grow and cybersecurity careers can be dynamic and exciting. Between emerging threats and new technological innovations, the field of cybersecurity is constantly changing, and the Cybersecurity Technology (CTEC) program will prepare students to take advantage of a variety of cybersecurity career opportunities. CTEC is a baccalaureate degree major that draws from the fields of computing, information technology, information assurance, and information security. Based on widely accepted cybersecurity curricular guides, the CTEC program provides students with the theoretical and conceptual knowledge essential to understanding the cybersecurity discipline as well opportunities to develop practical skills. Graduates enter the workforce as cybersecurity professionals ready to make a difference applying advanced skills to protect critical digital infrastructures and services.

Student Outcomes

Graduates of the program will have an ability to:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
2. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
3. Communicate effectively in a variety of professional contexts.
4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
6. Apply security principles and practices to maintain operations in the presence of risks and threats.

Bachelor of Science (B.S.) in Cybersecurity Technology Degree Requirements

Degree Requirements	Credit Hours	
University Core Curriculum Requirements		39
Require MATH 106 or MATH 108. Recommend PHIL 104 or PHIL 105, and ECON 113, PSYC 102 or SOC 108		
Foundation Course Requirements – ITEC 209, ITEC 216, ITEC 224, ITEC 225, ITEC 235, ITEC 236, ITEC 265, ITEC 280		24
Requirements for Major in Cybersecurity Technology		42
Required Major Courses – ITEC 312, ITEC 314, ITEC 370, ITEC 390, CTEC 328, CTEC 360, CTEC 375, CTEC 410, CTEC 418, CTEC 440, CTEC 461	33	

Degree Requirements	Credit Hours
Major Electives	9
General Electives	15
Total	120

Capstone Option for Transfer Students

The Capstone Option is available to qualified students entering the CTEC degree program. More information about the Capstone Option can be found within the University Core Curriculum tab of the Undergraduate Catalog. The CTEC degree program has signed Program Articulation Agreements with several community college computing-related degree programs in order to facilitate the transfer of community college students to SIU. These agreements take full advantage of the Capstone Option for admission to the Bachelor of Science in Cybersecurity Technology.

Cybersecurity Technology Courses

CTEC228 - Applied Offensive Cybersecurity Techniques This course introduces students to offensive cybersecurity techniques and tools and corresponding remediation and defensive strategies or system hardening principles to protect information systems. Students will gain hands-on experience in assessing and securing, Microsoft and Linux hosts, networks, and other types of assets. Knowledge of the legal aspects of offensive security, developing plans for effective penetration tests, planning and executing the phases of these assessments, and presentation of results will enhance overall cybersecurity expertise in both blue and red team scenarios. A grade of C or better is required. Prerequisites: ITEC 216 and ITEC 224 with grades of C or better. Credit Hours: 3

CTEC295 - Introduction to Cyber Defense Competition This course will introduce students to cyber defense competitions. Students will gain preparatory skills required for cyber defense competitions while working alongside more advanced students. Students who complete this course will be equipped to advance into CTEC 395 which prepares students for competitions and similar forums. A grade of C or better is required. Prerequisites: ITEC 209, ITEC 216, ITEC 224, and ITEC 235 each with a grade of C or better or concurrent enrollment in ITEC 235 or consent of instructor. Credit Hours: 3

CTEC328 - Security Analysis and Assessment of Info Systems This course will utilize security analysis tools to examine information systems, and networks. Infrastructure and physical assets will be examined to uncover potential vulnerabilities and security weaknesses. Emphasis will be placed on enterprise and open-source tools and using their results to create remediation plans to harden and fix security deficiencies. Social engineering and human security elements are also examined and the use of policy and training will be presented. A grade of C or better is required. Prerequisite: ITEC 216 with a grade of C or better. Credit Hours: 3

CTEC350 - Technical Career Subjects in Cybersecurity In-depth competency and skill development and exploration of innovative techniques and procedures used in business, industry, professions, and service occupations offered through various workshops, special courses, and seminars. Hours and credit to be individually arranged. Course may be classified as independent study. A grade of C or better is required. Special approval needed from the advisor. Credit Hours: 1-18

CTEC360 - Enterprise Security Policy, Tools, and Applications This course will introduce students to security policy, legal, and industry requirements that drive the technologies enterprises require to provide security protection for distributed networks in modern business computing environments. A reliance on partnerships with corporate and IT industry alliances and partnerships for resources and collaboration is a

key component of this course. A grade of C or better is required. Prerequisite: ITEC 216 with a grade of C or better. Credit Hours: 3

CTEC375 - Cyber Forensics This course focuses on building students' skills in a digital investigation with popular forensics tools. Topics include, but are not limited to, data acquisition, preservation, analysis and reporting, incident response, digital forensics process, and laws. Students will learn how to manage a digital forensics investigation in today's business environment. A grade of C or better required. Prerequisites: ITEC 209, ITEC 216, ITEC 224 with grades of C or better. Credit Hours: 3

CTEC377 - Practical Topics and Training in Cybersecurity Industry Intensive study of selected topics relevant to the cybersecurity industry with an emphasis on content, curriculum, and preparation for industry certifications. Offered as need arises and as time and interests permit. Maybe repeated for up to nine hours total. May be transferred in as elective CTEC credit from other programs and institutions. A grade of C or better is required. Special approval needed from the advisor. Credit Hours: 1-9

CTEC381 - Special Topics in Cybersecurity Intensive study of selected topics relevant to the cybersecurity environment. Offered as need exists and as time and interests permit. May be repeated for up to nine hours total. A grade of C or better is required. Special approval needed from the advisor. Credit Hours: 1-9

CTEC392 - Special Projects in Cybersecurity Students will work with current cybersecurity technology to solve problems and develop projects individually or in a team environment. A grade of C or better is required. Special approval needed from the instructor. Credit Hours: 1-6

CTEC395 - Cyber Defense Competition This course provides practical application of cyber defense and penetration testing methodologies in a fully operational corporate network environment. Skills required for cyber defense competition include implementation and evaluation of a network, risk assessment, incident response, and management, as well as performing under time limitations in a team format. Students who successfully complete this course will be equipped to participate in the Collegiate Cyber Defense Competition (CCDC) or similar forums. A grade of C or better is required. Prerequisites: ITEC 209, 216, 224, and 235 all with a grade of C or better and consent of instructor. Credit Hours: 3

CTEC399 - Individual Study in Cybersecurity Provides student with the opportunity to develop a special program of studies to fit a particular need not met by other offerings. Enrollment provides access to the resources and facilities of the entire institution. Each student will work under the supervision of a sponsoring faculty member. A grade of C or better is required. Special approval needed from the sponsor. Credit Hours: 1-18

CTEC410 - Web Security This course focuses on technologies behind web applications and servers, how applications and servers are exploited, and the defense mechanisms which can be used for server and application hardening. Hands-on labs on vulnerability detection and exploitation will be used to provide practical experience. A grade of C or better is required. Prerequisites: ITEC 216 and ITEC 236 with grades of C or better. Credit Hours: 3

CTEC417 - Wireless Communication & Security This course provides a comprehensive overview of wireless communications through an examination of the wireless channel, signal modulation, encoding and transmission techniques, antennae theory, and error control. Uses of wireless technologies in local, personal, and mobile networks will be examined. An emphasis will be placed on security measures and techniques in wireless communications. A grade of C or better is required. Prerequisites: ITEC 216 and ITEC 224 both with a grade of C or better. Credit Hours: 3

CTEC418 - Cloud Security This course focuses on protecting data and applications in cloud-based systems. Topics include, but are not limited to, security management strategies, managing user access, securing networks and applications, and vulnerability management. A grade of C or better is required. Prerequisites: ITEC 216 and ITEC 235 with grades of C or better. Credit Hours: 3

CTEC440 - Software Security This course provides a broad introduction of the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis. Students will be exposed to the techniques needed for the practice of effective software security approaches. A grade of C

or better is required. Prerequisites: ITEC 209 and ITEC 216 each with a grade of C or better or consent of instructor. Credit Hours: 3

CTEC461 - Principles of Cryptography This course provides a broad introduction to cryptography. Students will learn how various cryptographic schemes work and explain how they are used in practice. The course focuses on the classical goals of cryptography such as data confidentiality, authenticity and integrity. Grade of C or better required. Prerequisites: ITEC 209, ITEC 280 each with a grade of C or better or consent of instructor. Credit Hours: 3

CTEC465 - Introduction to Machine Learning with Applications in Information Security This course offers a thorough grounding in machine learning concepts, along with practical advice on applying these tools and techniques in real-world data mining situations. It gives an overview of many concepts, techniques, and algorithms in machine learning such as decision trees, rule based classification, support vector machines, Bayesian networks, and clustering. Students will be introduced to the major applications of each of the topics, with some of the applications drawn from the field of information security. A grade of C or better is required. Prerequisites: ITEC 209 and ITEC 265 each with a grade of C or better. Credit Hours: 3

Cybersecurity Technology Faculty

AlSobeh, Anas, Assistant Professor, Computer Science, Ph.D., Utah State University, 2015; 2023. Software engineering, web technology/services, machine learning, artificial intelligence, and cybersecurity analysis.

Imboden, Thomas, Associate Professor, Information Technology, M.S., DePaul University, 2007; 2008. Networking, cybersecurity.

Martin, Nancy, Associate Professor, Information, Technology, Ph.D., Southern Illinois University Carbondale, 2006; 2007. IS/IT education, assessment.

Sissom, James D., Associate Professor, Information Technology, M.P.Ad., Southern Illinois University Carbondale, 1996; 2003. E-learning, data analytics, higher ed information technology.

Woodward, Belle S., Associate Professor, Information Technology, M.A., Webster University, 1997; 2004. Privacy, ethics and technology, women in computing.

Yang, Ning, Assistant Professor, Information Technology, Ph.D., Southern Illinois University, 2020; 2020. Security of internet of things, emerging networking technologies for connected vehicles, machine learning for security.

Last updated: 04/19/2024