CYBERSECURITY ENGINEERING - B.S.

College of Aeronautics and Engineering
School of Engineering
www.kent.edu/cae

About This Program

Want to design the systems that stand up to today's most sophisticated cyber threats? The Cybersecurity Engineering program goes beyond code, preparing students to design, build and reinforce resilient systems that detect, withstand and recover from attacks to protect the critical infrastructure that powers everything from aviation and healthcare to defense and automation. Read more...

Contact Information

- cae@kent.edu | 330-672-2892
- Speak with an Advisor
- Chat with an Admissions Counselor

Program Delivery

- **Delivery:**
  - In person
- **Location:**
  - Kent Campus

Examples of Possible Careers

- Application security engineer
- Cloud security engineer
- Cybersecurity architect
- Cybersecurity engineer
- Cyber risk analyst
- Digital forensics analyst
- Governance, risk and compliance (GRC) analyst
- Identity and access management (IAM) engineer
- Incident response specialist
- Information security engineer
- Malware analyst
- Network security engineer
- Penetration tester (ethical hacker)
- Security consultant
- Security operations center (SOC) analyst
- Security operations manager

Admission Requirements

The university affirmatively strives to provide educational opportunities and access to students with varied backgrounds, those with special talents and adult students who graduated from high school three or more years ago.

Admission to the Cybersecurity Engineering major is selective.

New Students: Admission into this major requires:

- Minimum 3.0 high school GPA
- Completion of high school algebra II or a college-level algebra course with a minimum C grade

Students who do not meet the above requirements will be admitted to the **Computer Engineering Technology** major, provided they meet the minimum admission requirements.

Current Students: Students accepted into other Kent State programs may request to change their major to Cybersecurity Engineering once they meet the following criteria:

- Minimum 3.000 overall Kent State GPA (*starting with the fall 2026 admission term, minimum 12 credit hours completed at Kent State with a minimum 3.000 overall Kent State GPA is required)*
- Minimum C grade in both MATH 11022 and PHY 13001 (*starting with the fall 2026 admission term, minimum C grade in PHY 13001 is no longer required)*

Transfer Students: Admission into this major requires:

- Minimum 12 credit hours of college-level coursework
- Minimum 3.000 overall GPA
- Minimum C grade in both MATH 11022 and PHY 13001 (or their equivalents) (*starting with the fall 2026 admission term, minimum C grade in PHY 13001 is no longer required)*

Transfer students who have completed fewer than 12 credit hours of college-level coursework will be evaluated on both collegiate and high school records and must submit a final high school transcript.

Students from countries or schools that do not specify math topics on their transcripts must demonstrate a minimum C grade in all math courses.

International Students: All international students must provide proof of proficiency of the English language (unless they meet specific exceptions) through the submission of an English language proficiency test score or by completing English language classes at Kent State's English as a Second Language Center before entering their program. For more information, visit the admissions website for international students.

Program Requirements

Major Requirements

Code	Title	Credit Hours
Major Requirements (courses count in major GPA)		
CIS 44041	MANAGING CYBERSECURITY	3
CS 23022	DISCRETE STRUCTURES FOR COMPUTER SCIENCE	3
or MATH 23022	DISCRETE STRUCTURES FOR COMPUTER SCIENCE	
CS 47221	INTRODUCTION TO CRYPTOLOGY	3
ENGR 10005	INTRODUCTION TO CYBERSECURITY	3
ENGR 11001	INTRODUCTION TO ENGINEERING	2
ENGR 11002	INTRODUCTION TO ENGINEERING LABORATORY	1
ENGR 20000	PROFESSIONAL DEVELOPMENT IN ENGINEERING	1
ENGR 28105	FUNDAMENTALS OF NETWORKED INFRASTRUCTURE	2

ENGR 28106	FUNDAMENTALS OF NETWORKED INFRASTRUCTURE LABORATORY	1
ENGR 35550	LAW AND ETHICS FOR ENGINEERS	2
ENGR 37777	CYBERSECURITY OPERATIONS	2
ENGR 37778	CYBERSECURITY OPERATIONS LABORATORY	1
ENGR 38105	IOT SECURITY IN ENGINEERING SYSTEMS	2
ENGR 38106	IOT SECURITY IN ENGINEERING SYSTEMS LABORATORY	1
ENGR 38205	NETWORK INSTRUMENTATION AND FORENSIC ANALYSIS	2
ENGR 38206	NETWORK INSTRUMENTATION AND FORENSIC ANALYSIS LABORATORY	1
ENGR 46305	NETWORK SECURITY	2
ENGR 46306	NETWORK SECURITY LABORATORY	1
ENGR 47200	SYSTEMS ENGINEERING	3
ENGR 48099	ENGINEERING CAPSTONE I (ELR) [1]	3
ENGR 48191	ADVANCED CYBERSECURITY SEMINAR	3
ENGR 48199	ENGINEERING CAPSTONE II (ELR) (WIC) [1, 2]	3
ENGR 48200	WIRELESS MESH NETWORK SECURITY	3
INS 29000	INTRODUCTION TO INSURANCE AND RISK	3
MATH 12003	ANALYTIC GEOMETRY AND CALCULUS II [3]	3-5
or MATH 20011	DECISION-MAKING UNDER UNCERTAINTY	
MATH 30011	BASIC PROBABILITY AND STATISTICS	3
PHIL 21002	INTRODUCTION TO FORMAL LOGIC (KMCR)	3
Engineering (ENGR) Upper-Division Elective (30000 or 40000 level)		3
Computer Science Electives, choose from the following: [3]		8
CS 10062 & CS 20062	PROGRAMMING FOR PROBLEM SOLVING IN SCIENCES and ADVANCED PROGRAMMING WITH PYTHON [3]	
CS 13001 & CS 23001	COMPUTER SCIENCE I: PROGRAMMING AND PROBLEM SOLVING and COMPUTER SCIENCE II: DATA STRUCTURES AND ABSTRACTION	
CS 13011 & CS 13012 & CS 23001	COMPUTER SCIENCE IA: PROCEDURAL PROGRAMMING and COMPUTER SCIENCE IB: OBJECT ORIENTED PROGRAMMING and COMPUTER SCIENCE II: DATA STRUCTURES AND ABSTRACTION	
Technical Upper-Division Elective (40000 level), choose from the following:		3
CAE 45092	AERONAUTICS AND ENGINEERING INTERNSHIP/COOPERATIVE EDUCATION (ELR) (WIC) [2]	
Any Computer Information Systems (CIS) Upper-Division course (40000 level)		
Any Computer Science (CS) Upper-Division course (40000 level)		
Any Criminology and Justice Studies (CRIM) Upper-Division course (40000 level)		
Any Engineering (ENGR) Upper-Division course (40000 level)		
Any Information Technology (IT) Upper-Division course (40000 level)		
Additional Requirements (courses do not count in major GPA)		
COMM 15000	INTRODUCTION TO HUMAN COMMUNICATION (KADL)	3
MATH 11022	TRIGONOMETRY (KMCR)	3
MATH 12002	ANALYTIC GEOMETRY AND CALCULUS I (KMCR)	5
PHY 13001 & PHY 13021	GENERAL COLLEGE PHYSICS I (KBS) and GENERAL COLLEGE PHYSICS LABORATORY I (KBS) (KLAB) [3]	5
or PHY 23101	GENERAL UNIVERSITY PHYSICS I (KBS) (KLAB)	
PHY 13002 & PHY 13022	GENERAL COLLEGE PHYSICS II (KBS) and GENERAL COLLEGE PHYSICS LABORATORY II (KBS) (KLAB) [3]	5
or PHY 23102	GENERAL UNIVERSITY PHYSICS II (KBS) (KLAB)	
UC 10001	FLASHES 101	1
Science or Mathematics Elective, choose from the following:		3-4
CHEM 10050	FUNDAMENTALS OF CHEMISTRY (KBS)	
CHEM 10060	GENERAL CHEMISTRY I (KBS)	
CHEM 10970	HONORS GENERAL CHEMISTRY I (KBS)	
ESCI 21062	ENVIRONMENTAL EARTH SCIENCE (KBS)	
MATH 21001	LINEAR ALGEBRA	
MATH 21002	APPLIED LINEAR ALGEBRA	
MATH 22005	ANALYTIC GEOMETRY AND CALCULUS III	
MATH 32051	MATHEMATICAL METHODS IN THE PHYSICAL SCIENCES I	
PHY 32511	ELECTRONICS	
Kent Core Composition		6
Kent Core Humanities and Fine Arts (minimum one course from each)		9
Kent Core Social Sciences (must be from two disciplines)		6
Minimum Total Credit Hours:		**120**

[1] ENGR 48099 and ENGR 48199 must be taken during the same academic year.

[2] A minimum C grade must be earned to fulfill the writing-intensive requirement.

[3] Preferred option for students: CS 10062, CS 20062, MATH 20011, PHY 13001 (and lab), PHY 13002 (and lab).

Graduation Requirements

Minimum Major GPA	Minimum Overall GPA
2.500	2.250

Roadmap

This roadmap is a recommended semester-by-semester plan of study for this program. Students will work with their advisor to develop a sequence based on their academic goals and history. Courses designated as critical (!) must be completed in the semester listed to ensure a timely graduation.

	Semester One		Credits
	ENGR 11001	INTRODUCTION TO ENGINEERING	2
	ENGR 11002	INTRODUCTION TO ENGINEERING LABORATORY	1
	MATH 11022	TRIGONOMETRY (KMCR)	3
	UC 10001	FLASHES 101	1
	Computer Science Elective		4
	Kent Core Requirement		3
		Credit Hours	**14**
	Semester Two		
	COMM 15000	INTRODUCTION TO HUMAN COMMUNICATION (KADL)	3
	ENGR 10005	INTRODUCTION TO CYBERSECURITY	3
	MATH 12002	ANALYTIC GEOMETRY AND CALCULUS I (KMCR)	5
	PHIL 21002	INTRODUCTION TO FORMAL LOGIC (KMCR)	3

	Kent Core Requirement		3
		Credit Hours	**17**
	Semester Three		
	ENGR 20000	PROFESSIONAL DEVELOPMENT IN ENGINEERING	1
	ENGR 28105	FUNDAMENTALS OF NETWORKED INFRASTRUCTURE	2
	ENGR 28106	FUNDAMENTALS OF NETWORKED INFRASTRUCTURE LABORATORY	1
	INS 29000	INTRODUCTION TO INSURANCE AND RISK	3
	PHY 13001 & PHY 13021 or PHY 23101	GENERAL COLLEGE PHYSICS I (KBS) and GENERAL COLLEGE PHYSICS LABORATORY I (KBS) (KLAB) or GENERAL UNIVERSITY PHYSICS I (KBS) (KLAB)	5
	Kent Core Requirement		3
		Credit Hours	**15**
	Semester Four		
	CS 23022 or MATH 23022	DISCRETE STRUCTURES FOR COMPUTER SCIENCE or DISCRETE STRUCTURES FOR COMPUTER SCIENCE	3
	PHY 13002 & PHY 13022 or PHY 23102	GENERAL COLLEGE PHYSICS II (KBS) and GENERAL COLLEGE PHYSICS LABORATORY II (KBS) (KLAB) or GENERAL UNIVERSITY PHYSICS II (KBS) (KLAB)	5
	Computer Science Elective		4
	Kent Core Requirement		3
		Credit Hours	**15**
	Semester Five		
	ENGR 38105	IOT SECURITY IN ENGINEERING SYSTEMS	2
	ENGR 38106	IOT SECURITY IN ENGINEERING SYSTEMS LABORATORY	1
	ENGR 47200	SYSTEMS ENGINEERING	3
	MATH 12003 or MATH 20011	ANALYTIC GEOMETRY AND CALCULUS II or DECISION-MAKING UNDER UNCERTAINTY	3-5
	MATH 30011	BASIC PROBABILITY AND STATISTICS	3
	Kent Core Requirement		3
		Credit Hours	**15**
	Semester Six		
	CIS 44041	MANAGING CYBERSECURITY	3
	CS 47221	INTRODUCTION TO CRYPTOLOGY	3
	ENGR 37777	CYBERSECURITY OPERATIONS	2
	ENGR 37778	CYBERSECURITY OPERATIONS LABORATORY	1
	ENGR 38205	NETWORK INSTRUMENTATION AND FORENSIC ANALYSIS	2
	ENGR 38206	NETWORK INSTRUMENTATION AND FORENSIC ANALYSIS LABORATORY	1
	ENGR 46305	NETWORK SECURITY	2
	ENGR 46306	NETWORK SECURITY LABORATORY	1
		Credit Hours	**15**
	Semester Seven		
	ENGR 35550	LAW AND ETHICS FOR ENGINEERS	2
!	ENGR 48099	ENGINEERING CAPSTONE I (ELR)	3
	ENGR 48191	ADVANCED CYBERSECURITY SEMINAR	3
	Engineering (ENGR) Upper-Division Elective (30000 or 40000 level)		3
	Kent Core Requirement		3
		Credit Hours	**14**
	Semester Eight		
!	ENGR 48199	ENGINEERING CAPSTONE II (ELR) (WIC)	3
	ENGR 48200	WIRELESS MESH NETWORK SECURITY	3
	Science or Mathematics Elective		3-4
	Technical Upper-Division Elective (40000 level)		3
	Kent Core Requirement		3
		Credit Hours	**15**
		Minimum Total Credit Hours:	**120**

University Requirements

All students in a bachelor's degree program at Kent State University must complete the following university requirements for graduation.

NOTE: University requirements may be fulfilled in this program by specific course requirements. Please see Program Requirements for details.

Flashes 101 (UC 10001)	1 credit hour
Course is not required for students with 30+ transfer credits (excluding College Credit Plus) or age 21+ at time of admission.	
Diversity Domestic/Global (DIVD/DIVG)	2 courses
Students must successfully complete one domestic and one global course, of which one must be from the Kent Core.	
Experiential Learning Requirement (ELR)	varies
Students must successfully complete one course or approved experience.	
Kent Core (see table below)	36-37 credit hours
Writing-Intensive Course (WIC)	1 course
Students must earn a minimum C grade in the course.	
Upper-Division Requirement	39 credit hours
Students must successfully complete 39 upper-division (numbered 30000 to 49999) credit hours to graduate.	
Total Credit Hour Requirement	120 credit hours

Kent Core Requirements

Kent Core Composition (KCMP)	6
Kent Core Mathematics and Critical Reasoning (KMCR)	3
Kent Core Humanities and Fine Arts (KHUM/KFA) (min one course each)	9
Kent Core Social Sciences (KSS) (must be from two disciplines)	6
Kent Core Basic Sciences (KBS/KLAB) (must include one laboratory)	6-7
Kent Core Additional (KADL)	6
Total Credit Hours:	**36-37**

Program Learning Outcomes

Graduates of this program will be able to:

1. Identify, formulate and solve complex engineering problems by applying principles of engineering, science and mathematics.
2. Apply engineering design to produce solutions that meet specified needs with consideration of public health, safety and welfare, as well as global, cultural, social, environmental and economic factors.

3. Communicate effectively with a range of audiences.
4. Recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in a global, economic, environmental and societal context.
5. Function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks and meet objectives.
6. Develop and conduct appropriate experimentation, analyze and interpret data and use engineering judgment to draw conclusions.
7. Acquire and apply new knowledge as needed, using appropriate learning strategies.

The educational objectives of the program are the following:

1. Drive positive change in the community by engaging in careers in the field of cybersecurity, information systems and other engineering disciplines in a manner that promotes excellence and integrity.
2. Practice forward-thinking through continued education by way of graduate education, professional development and other continued self-motivated learning.
3. Successfully navigate the ever-changing trajectory of the world, practicing compassion while striving to meet personal career goals.

Full Description

The Bachelor of Science degree in Cybersecurity Engineering prepares students with problem-solving skills and a resourceful mindset to tackle cybersecurity threats in engineering systems. The program provides students with a working knowledge of analysis and evaluation of components and systems with respect to security and maintaining operations in the presence of risks and threats, with an emphasis on engineered systems. Students gain the understanding and skills necessary to address security issues pertaining to stakeholder needs and requirements (from a system engineering perspective) considering the lifecycle of the system from the outset. Design and development of systems, their components and associated networks to increase trustworthiness is a driving concern.