Cybersecurity
Associate of Applied Science

General Program Information: 410-287-1000 or information@cecil.edu

The Cyber Security program prepares students to enter the workforce or transfer to a four-year institution for continued study in computer cyber security. Cyber security specialists apply computer security techniques to work with industry, government, and academia to solve computer networking and security related challenges. Students with bachelor's degrees in computer cyber security continue their education in graduate school or enter the workforce as a network, forensic, or computer security expert.

The computer literacy requirement will be met throughout the course work in the degree program

	General Education Requirements	***Gen. Ed. Code***	***Credits***
ART/HUM	Arts and Humanities Elective[1]	H	3
BIO or PHY	Biology with Lab Electives or Physics with Lab Electives	SL	4
CSC 104	Computer Science Fundamentals	I	3
EGL 101	College Composition	E	3
EGL 102	Composition and Literature	H	3
MAT	Math Elective	M	4
PSY 101	Introduction to Psychology	SS	3
SOC SCI	Social Science Elective[2]	SS	3
	Program Requirements		
CSC 109	Introduction to Programming		3
CSC 110	Ethics in Information Technology (I)		3
CSC 140	Introduction to Networking[3]		3
CSC 141	Information Security Fundamentals[3]		3
CSC 151	Introduction to Computer Forensics and Investigations[3]		3
CSC 225	Tactical Perimeter Defense		3
CSC 235	Strategic Infrastructure Security		3
CSC 266	Cisco Certified Network Associate I[3]		4
CSC	CSC Electives		9

Total Credits Required in Program:60

[1] Selection may not include EGL designation

[2] Social Science Elective must be a course designation other than PSY

[3] Certification option courses

Upon successful completion of this program, students will be able to:

- Demonstrate proficiency in a programming language
- Configure and secure Windows and Unix/Linux server and clients, routers, firewalls, email, networks, and other network security appliances and software
- Demonstrate an understanding of networking standards, protocols, and the OSI model
- Identify and describe security measures for different types of network attacks, operating systems, software, databases, websites, social engineering and physical security
- Demonstrate an understanding of computer forensics, data acquisition, analysis, tools, and crime scene investigation and documentation requirements for corporate or legal testimony
- Explain the function of cryptography and encryption to secure data, public key infrastructure, hashing, and digital signatures along with other data protection techniques
- Create an effective security policy and disaster recovery plan, addressing business requirements related to confidentiality, integrity and availability