CYBERSECURITY - ADVANCED TECHNICAL CERTIFICATE (ATC)

Explore More About This Program: https://cwi.edu/program/cybersecurity

Certificate Quick Facts

- **Instructional School:** Science, Technology, and Math
- **Department:** Computer Science and Information Technology
- **Program Code:** CSEC.ATC
- **Program Type:** Career and Technical Education
- **Available Fully Online:** No
- **Eligible for Federal Financial Aid:** Yes

NOTE: Courses required for this program *may* have an additional fee; more information can be found on the Special Course Fees web page.

Certificate Requirements

Course	Course Title	Min Credits
General Education Requirements		
Select one of the following:		3
GEM 1 - Written Communication course		
GEM 2 - Oral Communication course		
GEM 3 - Mathematical Ways of Knowing course		3
GEM 6 - Social & Behavioral Ways of Knowing course		3
Major Requirements		
CSEC 110	Introduction to Hardware and Client Operating Systems	4
CSEC 123	Network Fundamentals	4
CSEC 125	Basic Network Routing	4
CSEC 127	Server Operating Systems	4
CSEC 129	Fundamentals of Linux	4
CSEC 131	Introduction to Information Security	4
CSEC 246	Securing a Directory Services Infrastructure	4
CSEC 248	Advanced Cybersecurity	4
CSEC 252	Introduction to Programming for Cybersecurity	4
CSEC 255	Ethical Hacking and Countermeasures	4
CSEC 257	Introduction to Digital Forensics	4
CSEC 290	Cybersecurity Capstone	4
Minimum Credit Hours Required		**57**

Certificate Plan: Fall Start

The course sequence listed below is strongly recommended in order to complete your program requirements. Many Career and Technical Education (CTE) courses have prerequisites and/or corequisites that have been accounted for within this Plan of Study Guide. Please register for your major requirements each semester as shown below using the Student Planning tool in myCWI. Consult your advisor for any questions regarding this plan.

NOTE: The required general education courses may be completed during any semester the student prefers, including summer semesters.

NOTE: The certificate plan below is for the traditional, in-person option. Students interested in the accelerated online option should meet with their advisor for additional information and assistance with course planning.

First Year

Fall		Credit Hours
First 5-Week Course Session		
CSEC 110	Introduction to Hardware and Client Operating Systems	4
Second 5-Week Course Session		
CSEC 123	Network Fundamentals	4
Third 5-Week Course Session		
CSEC 125	Basic Network Routing	4
Full 16-Week Course Session		
Select one of the following:		3
GEM 1 - Written Communication course		
GEM 2 - Oral Communication course		
	Total Semester Credit Hours	**15**

Spring

First 5-Week Course Session		
CSEC 127	Server Operating Systems	4

Second 5-Week Course Session		
CSEC 129	Fundamentals of Linux	4
Third 5-Week Course Session		
CSEC 131	Introduction to Information Security	4
Full 16-Week Course Session		
GEM 3 - Mathematical Ways of Knowing course		3
	Total Semester Credit Hours	**15**

Second Year

Fall

First 5-Week Course Session		
CSEC 246	Securing a Directory Services Infrastructure	4
Second 5-Week Course Session		
CSEC 248	Advanced Cybersecurity	4
Third 5-Week Course Session		
CSEC 252	Introduction to Programming for Cybersecurity	4
Full 16-Week Course Session		
GEM 6 - Social & Behavioral Ways of Knowing course		3
	Total Semester Credit Hours	**15**

Spring

First 5-Week Course Session		
CSEC 255	Ethical Hacking and Countermeasures	4
Second 5-Week Course Session		
CSEC 257	Introduction to Digital Forensics	4
Third 5-Week Course Session		
CSEC 290	Cybersecurity Capstone	4
	Total Semester Credit Hours	**12**
	Minimum Credit Hours Required	**57**

Program Learning Outcomes

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

- Apply computational, communication, and human relations skills to meet industry expectations.
- Demonstrate safety practices per industry standard.
- Display a working knowledge of implementing, managing, and securing a network infrastructure including web servers, email servers, and file and print servers as required by industry.
- Articulate the common body of knowledge (CBK) for security professionals with two years of security experience as required by industry.
- Demonstrate industry standard proficiencies in network penetration testing, “white hat” hacking, and deployment of preventative countermeasures.
- Implement forensically sound techniques in crime scene investigation including the collection, processing, preservation, and analysis of forensic evidence.
- Meet CompTIA Security+ Certification requirements.