Washtenaw Community College Comprehensive Report

CSS 197 Cybersecurity Essentials
Effective Term: Fall 2025

Course Cover

College: Business and Computer Technologies
Division: Business and Computer Technologies
Department: Computer Science & Information Technology
Discipline: Computer Systems Security
Course Number: 197
Org Number: 13400
Full Course Title: Cybersecurity Essentials
Transcript Title: Cybersecurity Essentials
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: New Course
Change Information:
Rationale: This course addresses the current lack of a 100-level CSS course and is designed for beginning students who are interested in completing an introductory cybersecurity course but do not already have experience in the IT industry. It equips students with entry-level job skills across the three domains: Endpoint Security, Network Defense, and Cyber Threat Management. These domains provide an integrated and comprehensive entry-level curriculum. This course has been designed to prepare students to take a successful first step on their cybersecurity career journey. Additionally, it maps to a relevant entry-level industry certification.
Proposed Start Semester: Fall 2025
Course Description: In this course, students will build a foundation for success in cybersecurity-related careers. It teaches comprehensive cybersecurity concepts and skills at the entry level, from threat mitigation and defense to post-incident forensics. Students will progress from basic cybersecurity concepts to experiences in assessing vulnerabilities and risks by the end of the course. This course aligns with Cisco Certified Support Technician (CCST) Cybersecurity certification.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

No Level Required

Requisites

Prerequisite minimum grade "C-"; may enroll concurrently
CNT 196
or
Prerequisite
Cisco Certified Support Technician (CCST) Networking certification, or equivalent experience is required.

General Education

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Recognize the various elements of modern network security systems.
   Assessment 1
   Assessment Tool: Outcome-related Cisco checkpoint exam
   Assessment Date: Fall 2025
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key
   Standard of success to be used for this assessment: 70% of students will score 70% or higher.
   Who will score and analyze the data: Departmental faculty will analyze the Cisco-provided results.

2. Recognize the proper configuration of a modern endpoint security system.
   Assessment 1
   Assessment Tool: Outcome-related Cisco checkpoint exam
   Assessment Date: Fall 2025
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key
   Standard of success to be used for this assessment: 70% of students will score 70% or higher.
   Who will score and analyze the data: Departmental faculty will analyze the Cisco-provided results.

3. Distinguish the various elements of modern network defense.
   Assessment 1
   Assessment Tool: Outcome-related Cisco checkpoint exam
   Assessment Date: Fall 2025
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Answer key
   Standard of success to be used for this assessment: 70% of students will score 70% or higher.
   Who will score and analyze the data: Departmental faculty will analyze the Cisco-provided results.

4. Recognize security alerts and incident response procedures.
   Assessment 1
   Assessment Tool: Outcome-related Cisco checkpoint exam

Assessment Date: Fall 2025
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: All students
How the assessment will be scored: Answer key
Standard of success to be used for this assessment: 70% of students will score 70% or higher.
Who will score and analyze the data: Departmental faculty will analyze the Cisco-provided results.

5. Identify the steps to perform a basic vulnerability assessment.

Assessment 1

Assessment Tool: Outcome-related Cisco checkpoint exam
Assessment Date: Fall 2025
Assessment Cycle: Every Three Years
Course section(s)/other population: All sections
Number students to be assessed: All students
How the assessment will be scored: Answer key
Standard of success to be used for this assessment: 70% of students will score 70% or higher.
Who will score and analyze the data: Departmental faculty will analyze the Cisco-provided results.

Course Objectives

1. Explain how threat actors execute some of the most common types of cyber attacks.
2. Explain basic network security principles.
3. Explain how TCP/IP vulnerabilities enable network attacks.
4. Recommend measures to mitigate threats.
5. Explain how devices and services are used to enhance network security.
6. Use Windows administrative tools.
7. Implement basic Linux security.
8. Evaluate endpoint protection and the impacts of malware.
9. Use cybersecurity best practices to improve confidentiality, integrity, and availability.
10. Explain approaches to network security defense.
11. Implement some of the various aspects of system and network defense.
12. Implement access control lists (ACLs) to filter traffic and mitigate network attacks.
13. Explain how firewalls are implemented to provide network security.
14. Implement Zone-Based Policy Firewall using the command-line interface (CLI).
15. Recommend cloud security requirements based on a given cloud scenario.
16. Determine the cryptographic techniques that are required to ensure confidentiality, integrity, and authenticity.
17. Explain how security technologies affect security monitoring.
18. Use different types of logs and records to store information regarding hosts and the network.
19. Explain the process of evaluating alerts.
20. Create documents and policies related to cybersecurity governance and compliance.
21. Use tools for network security testing.
22. Evaluate threat intelligence sources.
23. Explain how endpoint vulnerabilities are assessed and managed.
24. Select security controls based on risk assessment outcomes.
25. Use incident response models and forensic techniques to investigate security incidents.

New Resources for Course

Course Textbooks/Resources

Textbooks
Manuals
Periodicals

Software

Equipment/Facilities

Level III classroom
Computer workstations/lab

Reviewer	**Action**	**Date**
Faculty Preparer:		
Edward Szurek	*Faculty Preparer*	*Oct 30, 2024*
Department Chair/Area Director:		
Scott Shaper	*Recommend Approval*	*Oct 31, 2024*
Dean:		
Eva Samulski	*Recommend Approval*	*Nov 06, 2024*
Curriculum Committee Chair:		
Randy Van Wagnen	*Recommend Approval*	*Apr 24, 2025*
Assessment Committee Chair:		
Jessica Hale	*Recommend Approval*	*Apr 26, 2025*
Vice President for Instruction:		
Brandon Tucker	*Approve*	*Apr 28, 2025*