Washtenaw Community College Comprehensive Report

CSS 225 Cybersecurity Operations - CCNA Cyber Ops
Effective Term: Fall 2020

Course Cover

Division: Business and Computer Technologies
Department: Computer Science & Information Technology
Discipline: Computer Systems Security
Course Number: 225
Org Number: 13400
Full Course Title: Cybersecurity Operations - CCNA Cyber Ops
Transcript Title: CCNA Cyber Ops
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: CCNA Cybersecurity Operations is a hands-on, career-oriented course with an emphasis on practical experience to help students develop specialized skills to successfully handle the tasks, duties, and responsibilities of an associate-level Security Analyst working in a Security Operations Center (SOC).
Proposed Start Semester: Fall 2020
Course Description: In this course, students are introduced to Cybersecurity Operations. Students will develop the knowledge and skills needed to work as a Security Analyst with a Security Operations Center team. Security skills needed for monitoring, detecting, investigating, analyzing and responding to security events, thus protecting systems and organizations from cybersecurity risks, threats and vulnerabilities will be discussed. This course helps prepare students to take the Cisco Certified Network Associate (CCNA) exam.

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

Level 1

Requisites

Prerequisite
CSS 200 minimum grade "C"

General Education

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Explain cybersecurity operations network principles and protocols.

   Assessment 1

   Assessment Tool: Outcome-related questions on the departmentally-developed objective final exam
   Assessment Date: Fall 2022
   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: Departmentally-developed answer key
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty

   Assessment 2

   Assessment Tool: Departmentally-developed skills exam
   Assessment Date: Fall 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: Random sample of 50% of all students with the minimum of 1 full section
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty

2. Identify the technologies, tools, regulations and frameworks in a cybersecurity operations network.

   Assessment 1

   Assessment Tool: Outcome-related questions on the departmentally-developed objective final exam
   Assessment Date: Fall 2022
   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: Departmentally-developed answer key
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty

   Assessment 2

   Assessment Tool: Departmentally-developed skills exam
   Assessment Date: Fall 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: Random sample of 50% of all students with the minimum of 1 full section
   How the assessment will be scored: Departmentally-developed rubric

Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
Who will score and analyze the data: Department faculty

3. Apply knowledge and skills to monitor, detect, investigate, analyze and respond to security incidents.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed objective final exam
   Assessment Date: Fall 2022
   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: Departmentally-developed answer key
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty
   Assessment 2
   Assessment Tool: Departmentally-developed skills exam
   Assessment Date: Fall 2022
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: Random sample of 50% of all students with the minimum of 1 full section
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty

Course Objectives

1. Explain the role of the Cybersecurity Operations Analyst in the enterprise.
2. Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
3. Explain the features and characteristics of the Linux Operating System.
4. Analyze the operation of network protocols and services.
5. Explain the operation of the network infrastructure.
6. Classify the various types of network attacks.
7. Use network monitoring tools to identify attacks against network protocols and services.
8. Use various methods to prevent malicious access to computer networks, hosts, and data.
9. Explain the impacts of cryptography on network security monitoring.
10. Explain how to investigate endpoint vulnerabilities and attacks.
11. Evaluate network security alerts.
12. Analyze network intrusion data to identify compromised hosts and vulnerabilities.

New Resources for Course

Course Textbooks/Resources

Textbooks
Cisco Networking Academy. *CCNA Cybersecurity Operations Lab Manual*, 1 ed. Cisco Press, 2018, ISBN: 978-158713438.
Cisco Networking Academy. *CCNA Cybersecurity Operations*, 1 ed. Cisco Press, 2018, ISBN: 978-15871343.
Manuals
Periodicals
Software

NetLabs. WCC, CCNA Cyber Ops ed.
WCC provided NetLab access for completion of labs.

Equipment/Facilities

Level III classroom
Computer workstations/lab

Reviewer	Action	Date
Faculty Preparer:		
Cyndi Millns	*Faculty Preparer*	*Oct 30, 2019*
Department Chair/Area Director:		
Khaled Mansour	*Recommend Approval*	*Nov 01, 2019*
Dean:		
Eva Samulski	*Recommend Approval*	*Nov 04, 2019*
Curriculum Committee Chair:		
Lisa Veasey	*Recommend Approval*	*Dec 09, 2019*
Assessment Committee Chair:		
Shawn Deron	*Recommend Approval*	*Dec 17, 2019*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*Dec 18, 2019*