RARITAN VALLEY COMMUNITY COLLEGE
ACADEMIC COURSE OUTLINE

NTWK 285 CyberOps Associate

I. Basic Course Information

A. Course Number and Title: NTWK 285 CyberOps Associate

B. New or Modified Course: New

C. Date of Proposal: Semester: Spring Year: 2023

D. Effective Term: Fall 2023

E. Sponsoring Department: Math & Computer Science

F. Semester Credit Hours**: 3**

G. Weekly Contact Hours**:** 4
Lecture**:** 2
Laboratory**:** 2
Out of class student work per week: 5

H. ☒ Prerequisite (s): NTWK 119-Networking Essentials or NTWK 270- CCNA 1 Introduction to Networks or permission from instructor

I. Additional Fees**:** None

J. Name and E-Mail Address of Department Chair and Divisional Dean at time of approval**:** Lori Austin – Lori.Austin@raritanval.edu (Chair), Sarah Imbriglio – Sarah.Imbriglio@raritanval.edu (Divisional Dean)

II. Catalog Description

(Prerequisite/s: NTWK 119-Networking Essentials or NTWK 270- CCNA 1 Introduction to Networks or permission of the instructor). This course focuses on security concepts, common network and application operations and attacks, and the type of data needed to investigate security incidents. In addition, a student will learn how to monitor alerts converted to incidents. Through a combination of lectures, hands-on labs, and self-study, a student will learn essential skills concepts, and technologies to be a contributing member

of a Cybersecurity Operations Center (SOC) including understanding the IT infrastructure. Operations, and vulnerabilities. This course prepares a student for the Cisco Certified CyperOps Associate certification and the role of a Junior or Entry-level cybersecurity operations analyst in a SOC. This course also earns you 30 Continuing Education (CE) credits towards recertification.

III. Statement of Course Need

A. Security is important, and the lack of it risks financial, legal, political, and public relations implications. Having the ability to design and implement secure networks is an essential skill required by a network engineer or an administrator. Cisco security technology implementations are the most widely deployed technology in the industry. Students will learn the fundamental skills, techniques, and the hands-on practice necessary to prevent and defend against cyberattacks as part of a SOC team. The course will also prepare the students for the 200-201 Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) exam which earns the Cisco Certified CyberOps Associate certification

B. This course does have lab component. Students are expected to use computers in the lab to work with various operating systems. A regular Computer Lab is sufficient.

C. This course generally transfers as a Computer Science Elective, dependent on the institution.

IV. Place of Course in College Curriculum

A. Free Elective
B. This course meets the program requirement for the Computer Networking and Cybersecurity, AAS and Certificate
C. Computer Elective from the Computer and Programming Electives List.
D. Course Transferability: for New Jersey schools go to the NJ Transfer website, www.njtransfer.org . For all other colleges and universities, go to their individual websites.

V. Outline of Course Content

This course addresses the following topics:

A. Security Operations Center (SOC)
B. Network Security Monitoring (NSM)
C. Cryptography
D. Security flaws in the TCP/IP protocol
E. Endpoint security technologies
F. Kill chain and diamond models for incident investigations
G. Data normalization and event correlation
H. Common attack vectors

I. Workflow management and automation

VI. A. Course Learning Outcomes:

After completion of this course, the student will be able to:

1. Analyze complex network threats and specify cybersecurity hardware and software to mitigate the threats. (GE-4)
2. Describe the Network Infrastructure and network security monitoring Tools
3. Explain the basic cryptography concepts, TCP/IP attacks and endpoint security technologies
4. Identify common attack vectors, malicious activity and patterns of suspicious behavior
5. Conduct security incident investigations and response
6. Explain the SOC workflow and automation

B. Assessment Instruments:

1. Quizzes
2. Lab exercises
3. Homework Assignments
4. Research Projects
5. Exams

VII. Grade Determinants

A. Individual homework and projects
B. Class participation
C. Quizzes
D. Exams
E. Final Exam

Modes of Teaching and Learning

A. Lecture/Discussion
B. Laboratory

VIII. Texts and Materials

Suggested Textbook – Cisco CyberOps Associte CBROPS 200-201 *Official Cert Guide*, Omar Santos, Cisco Press, Pearson Education, Inc, 2020.

Cisco Academy Online e-book

(Please Note: The course outline is intended only as a guide to course content and resources. Do not purchase textbooks based on this outline. The RVCC Bookstore is the sole resource for the most up-to-date information about textbooks.)

IX. Resources

A. Computer Lab for classroom instruction and exercises
B. Technology Support
    a. Cisco Packet Tracer

X. Honors Option

N/A