ROCHESTER COMMUNITY AND TECHNICAL COLLEGE

COMMON COURSE OUTLINE

Course discipline/number/title: COMP 2049: Cybersecurity Systems

A. CATALOG DESCRIPTION

1. **Credits: 4**
2. **Hours/Week: 4 hours per week lecture**
3. **Prerequisites (Course discipline/number):** MATH 0099, COMP 2048
4. **Other requirements:** None
5. **MnTC Goals (if any):** NA

B. COURSE DESCRIPTION: This class examines the basic principles of cybersecurity systems and analysis, involving developing knowledge of current trends affecting security analysts within on-premise, cloud, and hybrid environments. Additionally, this class will develop knowledge related to proactive monitoring, threat detection, SIEM tooling, EDR, XDR, threat intelligence, and how to respond to threats. Students will leave equipped with with the practical skills needed for real-world applications and preparation for the CompTIA Cybersecurity Analyst (CySA+) exam.

C. DATE LAST REVISED (Month, year): November, 2023

D. OUTLINE OF MAJOR CONTENT AREAS:

1. Introduction to Cybersecurity Analyst
   a) CySA+ Exam Objectives
   b) Roles and Responsibilities of a Cybersecurity Analyst
2. Introduction to Cybersecurity Operational Processes
   a) Vulnerability and Risk Management
   b) Incident Response and Reporting
3. Threat Vectors and Threat Hunting
   a) Understanding Threat Vectors
   b) Basics of Threat Hunting
4. Threat Intelligence and SIEM Tooling
   a) What is Threat Intelligence?
   b) Security Information and Event Management (SIEM)
5. Endpoint Detection and Extended Detection (EDR and XDR)
   a) Endpoint Detection and Response (EDR)
   b) Extended Detection and Response (XDR)
6. Malicious Activity Identification Tools
   a) Commonly Used Tools
   b) Identifying Signs of Malicious Activity
7. Implementing Vulnerability Assessments
   a) Prioritizing Vulnerabilities
   b) Risk Management in Vulnerability Assessments
8. Incident Response and Management
   a) Incident Response Efforts
   b) Incident Management Lifecycle
9. Reporting and Communication Best Practices
   a) Executive Reporting
   b) Escalation Points and Security Metrics
10. Real-world Applications of Cybersecurity Analysis
    a) Case Studies in Threat Detection
    b) Proactive Monitoring Techniques
11. Cloud and Hybrid Environment Security
    a) Cloud Security Challenges and Solutions
    b) Hybrid Environment Considerations
12. Forensic Analysis in Cybersecurity
    a) Digital Forensics Tools and Techniques
    b) Legal and Ethical Considerations in Forensics

E. LEARNING OUTCOMES (GENERAL): The student will be able to:

1. Apply security processes to improve the security posture of the organization.
2. Distinguish between threat intelligence and threat hunting, applying each technique appropriately.
3. Develop vulnerability assessments with recommendations for mitigating attacks.
4. Apply attack method frameworks for incident response.
5. Develop reports related to security metrics for executive management consumption.
6. Identity and analyze attacks and malicious activity using various security tools.

F. LEARNING OUTCOMES (MNTC): NA

G. METHODS FOR EVALUATION OF STUDENT LEARNING: Methods may include but are not limited to:

1. Tests
2. Lab Exercises
3. Programming assignments
4. Comprehensive Final Exam

H. RCTC CORE OUTCOME(S). This course contributes to meeting the following RCTC Core Outcome(s):
Critical Thinking. Students will think systematically and explore information thoroughly before accepting or formulating a position or conclusion.

I. **SPECIAL INFORMATION (if any):** None