SYLLABUS
PART I
EDISON STATE COMMUNITY COLLEGE
CYB 240S SYSTEM DEFENSE & INCIDENT RESPONSE
3 CREDIT HOURS

COURSE DESCRIPTION
Focuses on cybersecurity defense strategies for identifying, mitigating, and responding to threats. Topics include vulnerability assessment, threat hunting, system hardening, and network defense. Students gain hands-on experience using industry tools such as intrusion detection systems, firewalls, and logging solutions to secure systems and networks. The course prepares students for the CompTIA CySA+ certification. Discounted CompTIA CySA+ Certification Exam voucher available upon successful completion of this course. Prerequisite: CIS 214S, CIS 215S, and CYB 236S.

COURSE GOALS
The student will:

Bloom's Level		Program Outcomes
2	1. Explain the types of cyber threats, including malware, phishing, and social engineering.	4, 5
3	2. Apply security measures, including encryption and access controls, to protect systems and data.	3, 7, 8
4	3. Analyze network traffic to detect anomalies using tools such as IDS.	3, 7, 8
5	4. Develop incident response plans to contain and recover from cyber-attacks.	1, 3, 7
3	5. Implement system hardening techniques to reduce attack surfaces.	7, 8
5	6. Evaluate the effectiveness of security policies and procedures to enhance network security.	3, 5, 8
3	7. Configure monitoring tools to detect and prevent network attacks.	7, 8
4	8. Mitigate risks through vulnerability assessments.	3, 8
3	9. Prepare detailed reports on cybersecurity incidents and security postures.	2, 8
3	10. Manage network devices, including firewalls and intrusion prevention systems.	7, 8
5	11. Compare various cybersecurity frameworks and standards such as CIS and NIST.	3, 5
5	12. Design comprehensive network defense strategies based on current cybersecurity trends and threat intelligence.	3, 5, 7

CORE VALUES
The Core Values are a set of principles that guide in creating educational programs and environments at Edison State. They include communication, ethics, critical thinking, human diversity, inquiry/respect for learning, and interpersonal skills/teamwork. The goals, objectives, and activities in this course will introduce/reinforce these Core Values whenever appropriate.

TOPIC OUTLINE
1. Introduction to Cybersecurity Defense
2. Types of Cyber Threats

3. Vulnerability Assessments and Attack Surfaces
4. Risk Management and Security Controls
5. Intrusion Detection and Prevention Systems (IDS/IPS)
6. Security Testing and Penetration Testing Frameworks
7. System Hardening and Configuration Management
8. Threat Intelligence and Threat Hunting
9. Network Security Monitoring and Analysis
10. Incident Response and Recovery Strategies
11. Identity and Access Management (IAM) and Encryption
12. Security Orchestration, Automation, and Response (SOAR)
13. Forensics and Evidence Handling
14. Firewall Configurations and Network Security Devices
15. Reports for Compliance and Governance Logging
16. Final Project: Designing a Network Defense Strategy