COURSE INFORMATION FORM

DISCIPLINE  Computer Science Information Systems
COURSE TITLE  Cyber Analytics
CR.HR  3  LECT HR.  2  LAB HR.  2  CLIN/INTERN HR.  CLOCK HR.

CATALOG DESCRIPTION
This course introduces students to the fundamental concepts of cyber analytics. Students will explore and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization. This course helps prepare students for the current CompTIA Cybersecurity Analyst (CySA+) certification exam.

PREREQUISITES
CSIS 270 with a grade of C or better

EXPECTED STUDENT OUTCOMES IN THE COURSE (ESO)
Upon completion of this course, the student will be able to:

1. Describe and demonstrate various network reconnaissance tools and strategies.
2. Recommend appropriate response, countermeasures, and compensating controls.
3. Compare and Contrast various security testing exercises.
4. Describe and demonstrate various vulnerability management tools and strategies.
5. Describe and demonstrate various cyber incident response tools and strategies.
6. Describe common policies, controls, and procedures.

GENERAL EDUCATION OUTCOMES (ESO)
Specify which general education outcomes, if any, are substantially addressed by the course. Numbers in parentheses identify the Expected Student Outcomes linked to the specific General Education Outcome.

Outcomes  ESO
PROGRAM-LEVEL OUTCOMES

CAREER AND TECHNICAL EDUCATION PROGRAM OUTCOMES
Specify which Career and Technical program outcomes, if any, are substantially addressed by the course by completing the “Career and Technical Education template” to show the relationship between course and program outcomes to assessment measures.

1. Use industry specific software and/or apply troubleshooting skills to solve problems
2. Create and defend solutions to real life business challenges
3. Demonstrate professional oral and written communication skills

CLASS-LEVEL ASSESSMENT MEASURES
Student accomplishment of expected student outcomes may be assessed using the following measures. (Identify which measures are used to assess which outcomes.)

1. Examination/Quizzes (1-6)
2. Class Discussion/Participation (1-6)
3. Exercises/Projects (1-6)
4. Written/Oral Reports (1-6)
Individual instructors may order this outline as fits the needs of their individual courses. In addition, they may place more emphasis on some areas than on others. What is assured is that this particular list is covered in the course. Other topics may be added to a course as the instructor sees fit, and as time and interest allow. An *asterisk can be used to mark an item as optional.

I. Threat Management
   A. Environmental reconnaissance techniques using appropriate tools and processes
   B. Network reconnaissance
   C. Responses and countermeasures
   D. Securing a corporate environment

II. Vulnerability Management
   A. Information security vulnerability management process
   B. Vulnerability scan output analysis
   C. Common vulnerabilities found within an organization

III. Cyber Incident Response
   A. Impact of an incident
   B. Forensics tools during an investigation
   C. Incident response process
   D. Support incident response
   E. Incident recovery and post-incident response process

IV. Security Architecture and Tool Sets
   A. Relationship between frameworks, common policies, controls, and procedures
   B. Remediation of security issues related to identity and access management
   C. Implementing compensating controls
   D. Software Development Life Cycle