MOORE NORMAN
TECHNOLOGY CENTER

Course Syllabus

Preparation for CompTIA CySA+ (Cybersecurity Analyst)

CN352

Hours : In Class 48 Clinical 0 Total 48

Description

Break into the Cyber Security field. CySA+ certified skills are in-demand. You will learn and gains the skills necessary to provide the defense of those information systems in a cyber security context, including protection, detection, analysis, investigation and response processes. You will learn through our unique Lecture-Lab-Review approach, to configure threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization. Tuition includes books and Test Prep for certification preparation, everything you need to enter the exam confident in your skill set.
The U.S. Bureau of Labor Statistics (BLS) predicts that information security analysts will be the fastest growing overall job category, with 32 percent overall growth between 2018 and 2028. (Much faster than average) CySA+ is government approved. CompTIA CySA+ meets the ISO 17024 standard and is approved by U.S. Department of Defense to fulfill Directive 8570.01-M requirements.
While MNTC provides you with learning resources to prepare for a successful exam experience, certification exams must be scheduled through PearsonVUE. Exam may be taken in our Assessment Center. Certification Exam is not included. Student discounts are as much as 50%.

Prerequisites

CN350 Preparation for CompTIA Security+ certification is highly recommended. If you have experience but are not sure how to assess your skill level, please call Rick Spaulding, program coordinator, at (405) 801-5704 to discuss your situation.

Books

CompTIA Cybersecurity Analyst+ Print and eBook - ISBN: CYS-001-SPBK-2018 (Included)

Student Labs (LOD) - ISBN: CYS-001-STLB-2018 (Included)

Learning Objectives

1. Threat Management
a. Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes
b. Given a scenario, analyze the results of a network reconnaissance
c. Given a network-based threat, implement or recommend the appropriate response and countermeasure
d. Explain the purpose of practices used to secure a corporate environment

2. Vulnerability Management
a. Given a scenario, implement an information security vulnerability management process
b. Given a scenario, analyze the output resulting from a vulnerability scan
c. Compare and contrast common vulnerabilities found in the targets within an organization

3. Cyber Incident Response
a. Given a scenario, distinguish threat data or behavior to determine the impact of an incident
b. Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation
c. Explain the importance of communication during the incident response process
d. Given a scenario, analyze common symptoms to select the best course of action to support incident response
e. Summarize the incident recovery and post-incident response process

4. Security Architecture and Tool Sets
a. Explain the relationship between frameworks, common policies, controls, and procedures
b. Given a scenario, use data to recommend remediation of security issues related to identity and access management
c. Given a scenario, review security architecture and make recommendations to implement compensating controls
d. Given a scenario, use application security best practices while participating in the Software Development Life Cycle

(SDLC)
e. Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies

Teaching Philosophy

We believe that instructors, staff, and administrators have a shared responsibility to provide: 1) innovative course design and instruction; 2) a safe, learner-centered environment; and 3) an authentic learning experience.

Teaching Methods

Methods include lecture, class discussion and demonstrations.

Evaluation Methods

Student success is based on participation in class activities and the completion of exercises. A certificate of completion requires 100% attendance and completion of all assigned activities.

Grading Policy

Student success is based on participation in class activities and the completion of exercises. A certificate of completion requires successful completion of all assigned work within the established time frame. Types of graded assignments will be projects, review questions, activities, assignments and tests
Grading Policy:
A = 90 - 100%
B = 80 - 89%
C = 70 - 79%
D = 60 - 69%
F = Below 60%
A course grade of D does not qualify the course as a prerequisite to other courses.

Student Responsibilities

To ensure a quality and safe learning environment, students are required to follow the Post-Secondary Student Behavior policy #560. This policy can be found at www.mntc.edu/board-policies. Printed copies are available upon request.

Students are expected to attend class and participate in class discussions and activities, complete out of class assignments and exams in class.

Students must be on time and meet the attendance policy set for this class which is 80% attendance.