ITMS 446 SYLLABUS

ITMS 446 Active Cyber Defense

Hours: 3 credit hours / 60 contact hours

Instructor: Louis McHugh

Textbook, title, author, and year: *TestOut CyberDefense Pro,* TestOut ISBN: 978-1-935080-73-2, 2021

Specific course information

a. **Catalog description:** This course covers the duties of cybersecurity analysts who are responsible for monitoring and detecting security incidents in information systems and networks, and for executing a proper response to such incidents. The course introduces tools and tactics to manage cybersecurity risks, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and handle incidents as they occur.
b. **Prerequisites:** ITMS 448 or ITMS 443.

Specific goals for the course

a. **Course Outcomes:** This course will address aspects of threat and vulnerability management; software and systems security; security operations and monitoring; incident response; and compliance and assessment necessary to prepare students to properly defend an enterprise against cyber attacks. This course and the concepts described in the class cover topics included in the CompTIA Cybersecurity Analyst (CySA+) professional certification.
b. **Course student outcomes:**
   Students completing this course will be able to:
   - Collect and use cybersecurity intelligence and threat data.
   - Recall and describe modern cybersecurity threat actors' types and tactics, techniques, and procedures.
   - Analyze data collected from security and event logs, and network packet captures.
   - Respond to and investigate cybersecurity incidents using appropriate forensic analysis techniques.
   - Assess information security risk in computing and network environments.
   - Implement a vulnerability management program.
   - Analyze and address security issues with an organization's network architecture.
   - Describe data governance controls and discuss their importance.
   - Describe and address security issues with an organization's software development life cycle.
   - Describe and address security issues with an organization's use of cloud and service-oriented architecture.

Topics to be covered

a. Threat Intelligence
b. Risk Mitigation
c. Social and Physical Security
d. Reconnaissance
e. Enumeration
f. Vulnerability Management
g. Identity and Access Management Security (IAM)
h. Cybersecurity Threats
i. Infrastructure Security
j. Wireless and IOT Security
k. Infrastructure Analysis
l. Software Assurance
m. Data Analysis
n. Incident Response