CIT 264 - CYBERSECURITY ANALYTICS AND THREAT ANALYSIS

Course Description

In this course, students will learn how to employ data analytics to interpret and identify security vulnerabilities, threats, and risks to an organization. Students will configure and use various threat detection tools and learn how to secure and protect applications and systems within an organization. This course aligns with the CompTIA CySA+ certification exam. Group 2 course.

Credit Hours

3

Contact Hours

4

Lecture Hours

2

Lab Hours

2

Required Prerequisites

CIT 240, or instructor permission.

Recommended Prerequisites or Skills Competencies

Completion of CIT 256.

General Education Outcomes supported by this course

Critical Thinking - Direct

Course Learning Outcomes

Knowledge:

- Summarize techniques used to perform reconnaissance of a security system.
- Summarize assessment tools used to provide effective mitigation.
- Summarize ways to remediate authentication and access control issues.
- Summarize incident response methodologies.

Application:

- Apply reconnaissance techniques to identify potential threats and vulnerabilities.
- Use data to identify remediation strategies.
- Implement incident response strategies and best practices.

Integration:

- Evaluate forensic tools based on best practices.
- Discuss incident response strategies as they pertain to documented security breaches.

Human Dimension:

- Discuss how incident response impacts stakeholders.
- Collaborate work with others to complete a desired outcome.

Caring - Civic Learning:

- Explore ethical dilemmas related to security.
- Discuss corporate responsibility as it pertains to security.

Learning How to Learn:

- Seek out solutions to problems on their own.
- Research available resources on security.