Miami Dade College

Course Description

CIS2350 | Cybersecurity Analysis | 4.00 credits

This course provides students an intermediate skills-level approach to cybersecurity analysis. Students learn to identify the phases of an attack, the motivations of the adversary, the resources and techniques they use, the intended effect, or end-game, and how to mitigate threats. Topics include intrusion detection and response, analytics and advanced threat visibility. Prerequisites: CTS1120 and CTS1134.

Course Competencies:

Competency 1: The student will demonstrate an understanding of computer networking environments by:

1. Describing current network environments
2. Describing network communications and hardware
3. Identifying issues related to networked environments, such as security, access control, fair use, privacy, and redundancy
4. Identifying emerging technologies and discussing related technical issues
5. Identifying issues such as security, privacy, and redundancy related to networked environments

Competency 2: The student will demonstrate fundamental proficiency in network security essentials by:

1. Describing common security threats to and vulnerabilities of computer systems and the corresponding best practices for mitigation
2. Defining and describing malicious software and techniques to protect systems from its effects
3. Describing Denial of Service attacks and means to defend against them
4. Identifying the risks and techniques of data loss and its prevention
5. Describing the principles and techniques of securing data storage and transmission
6. Identifying current encryption and authentication standards
7. Implementing security policies, including compliance and operational security
8. Enabling access control, identity management, and security logging
9. Managing client and network system security software and related updates
10. Describing the functions and characteristics of firewalls
11. Performing a ping sweep and port scan to identify network hosts and open TCP/UDP ports
12. Using a network protocol analyzer to capture and analyze network traffic for security issues

Competency 3: The student will develop secure coding and testing practices by:

1. Characterizing the stages of the system development life cycle
2. Identifying and using best practices to secure program code
3. Describing various code review models
4. Developing a test plan and test data
5. Documenting test results

Competency 4: The student will demonstrate an understanding of network access control systems and methodology by:

1. Comparing and contrasting access control techniques
2. Demonstrating an understanding of various access control models
3. Analyzing methods of server attacks
4. Demonstrating an understanding of the different types of intrusions and the different methods of intrusion detection
5. Monitoring the network using various intrusion detection resources to detect attacks
6. Investigating audit trails for signs of network intrusions

7. Performing penetration testing to find weaknesses in the access control systems

Competency 5: The student will perform security activities by:

1. Completing a security needs evaluation
2. Identifying and selecting security protocols
3. Identifying identity and access management practices
4. Implementing Defense-in-Depth strategies
5. Analyzing network, host, and application issues
6. Conducting a forensic analysis and investigation

Competency 6: The student will demonstrate an understanding of legal and ethical issues relative to the information technology environment by:

1. Describing customer and employee privacy issues and safeguards
2. Developing examples of acceptable use policies
3. Comparing organizational codes of ethics
4. Researching industry standards and codes of conduct for information technology professionals
5. Identifying and describing common security frameworks such as NIST and ITIL

Competency 7: The student will demonstrate an understanding of vulnerability analysis by:

1. Using threat modeling techniques
2. Discussing the root causes of vulnerabilities (e.g., memory corruption, improper sanitizing, design flaws, etc.)
3. Classifying threats, vulnerabilities, and exploits common in modern information systems, including buffer overflows, privilege escalation, rootkits, malware, return-oriented programming, and social engineering
4. Describing threats to identity and access
5. Performing reverse engineering and penetration testing activities to identify vulnerabilities
6. Explaining when vulnerabilities must be disclosed
7. Identifying and describing standard reconnaissance and intelligence-gathering activities
8. Designing and implementing a vulnerability assessment and management program
9. Identifying and performing incident response and forensic analysis activities

Competency 8: The student will demonstrate communication skills by:

1. Describing the roles of the cybersecurity professional in a business enterprise
2. Describing methods of logging incidents and reporting problem resolution
3. Presenting and following oral and written instructions
4. Demonstrating self-motivation and responsibility to complete an assigned task
5. Choosing appropriate actions in situations requiring effective time management
6. Applying principles and techniques for being a productive, contributing member of a team
7. Identifying and discussing intellectual property rights and licensing issues
8. Identifying and discussing issues contained within professional codes of conduct
9. Using appropriate communication skills, courtesy, manners, and dress in the workplace
10. Documenting problems and solutions in service reports and maintaining support records
11. Explaining the methods and best practices of interviewing end users to determine the symptoms and probable causes of system problems

Learning Outcomes

- Use quantitative analytical skills to evaluate and process numerical data
- Formulate strategies to locate, evaluate, and apply information.
- Use computer and emerging technologies effectively