Miami Dade College

Course Description

CIS4891 | Cyber Security Capstone Project | 4.00 credits

This upper-division course requires students to apply the knowledge and skills acquired for a cyber security project. Students will assess risk and define the cyber security requirements for a real-world scenario. Then they will design, implement and test the necessary cyber defenses to reduce the risk to an acceptable level in an emulated IT environment. Must be taken during the last semester before graduation and with a departmental permission. Prerequisite(s): Senior status. Department approval required.

Course Competencies:

Competency 1: The student will be able to formulate cyber security requirements by:

1. Defining the project purpose and the scope of work to be conducted in a real-world scenario
2. Determining the risk appetite of an organization
3. Describing the security posture of an organization
4. Listing the regulations and standards applicable to the scenario
5. Describing the cybersecurity requirements regarding confidentiality, integrity, availability, accountability, and authenticity

Competency 2: Students will be able to perform a risk assessment by:

1. Developing a list of assets from different types (hardware, software, data in motion, data at rest, data in memory)
2. Prioritizing the list of assets based on their value to the organization
3. Developing an exhaustive list of threats to each identified asset's confidentiality, integrity, and availability
4. Evaluating the impact and likelihood of the identified threats

Competency 3: The student will be able to design a solution to satisfy the cyber security requirements by:

1. Using cyber security principles such as defense-in-depth, diversity of defense, and least privilege
2. Considering alternative response approaches to mitigate risk (avoid, accept, mitigate, transfer)
3. Selecting appropriate cyber security controls (cyber defenses) that help protect, detect, and respond to the identified threats
4. Considering cybersecurity controls from administrative, physical, and technical types
5. Evaluating the residual risk
6. Addressing the solution's impact on the functionality and usability of the protected system
7. Developing an architecture diagram of the cybersecurity solution with the selected security controls at the different layers where they operate

Competency 4: The student will be able to implement the solution by:

1. Using an isolated simulated and/or virtual IT environment
2. Developing artifacts (scripts, training materials, security policies, configuration files, forensics procedures, intrusion detection rules, firewall rules, monitoring schedules, backup schedules, malware analysis reports, etc.) that address the targeted threats

Competency 5: The student will be able to validate the solution by:

1. Designing a test/validation plan for each of the identified threats
2. Using adequate penetration testing tools and techniques to test the cybersecurity controls and find new vulnerabilities
3. Reporting the newly identified vulnerabilities

Competency 6: The student will demonstrate the ability to effectively communicate and present the results of the project by:

1. Developing presentations that are polished, informative, and engaging
2. Demonstrating that all work products provided the right level and type of detail
3. Satisfactorily answering questions ranging from implementation detail to test methodology to the project's future evolution
4. Providing a self-reflection about the experience

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Formulate strategies to locate, evaluate, and apply information
- Use computer and emerging technologies effectively