Cybersecurity Architecture and Engineering – C726

Overview

Cybersecurity Architecture and Engineering prepares students to implement and manage security engineering tasks and processes using secure design principles grounded in positive security engineering. It covers the fundamental concepts of confidentiality and integrity security models along with applied cryptography for implementation of these models. Additionally, this course helps students assess and mitigate vulnerabilities found in security designs, architectures, and solutions. Finally, this course introduces techniques to design and implement physical security controls for data centers and other large implementations of IT. There are no prerequisites for this course.

Competencies

- **Readiness**
  This competency exists to assess the readiness of students.

- **Security Architecture in Practice**
  The graduate designs a multi-level target security architecture to support the organization's security policy and technology choices and to include applicable policy guidance.

- **Countering Threats and Vulnerabilities**
  The graduate assesses the vulnerabilities within the Internet of Things (IoT) and web-based, mobile, and embedded systems.

- **Threat Identification**
  The graduate identifies threats and vulnerabilities applicable to business systems and assets

- **Security Architecture and Engineering Requirements**
  The graduate designs technical specifications based on an organization’s security requirements.

Learning

https://my.wgu.edu/courses/course/15760027
Getting Started

Welcome to Cybersecurity Architecture and Engineering. In this course, you will examine how to analyze requirements, assess risks, and design systems that mitigate threats to an organization's operations. The topics and pacing section provides a suggested weekly plan for working through the course in a timely manner. This course employs uCertify learning resources that contain the reading materials and knowledge checks, as well as Pluralsight videos, necessary to understand the subject matter. You will demonstrate competency in this course by the successful completion of a performance assessment.

Assessments

Performance Assessment: Cybersecurity Architecture and Engineering - ACP2

- Task 1: Not Submitted
  - NOT SUBMITTED
  - View Task

- Task 2: Not Submitted
  - NOT SUBMITTED
  - View Task

Diagnostic: Cybersecurity Architecture and Engineering

- STATUS: Not Attempted
- TIME ALLOCATED: 150 minutes
- # OF ITEMS: 14
- CODE: XACP

A score of Competent or Exemplary is required to pass all assessments. Passing a preassessment does not guarantee you will pass the high stakes assessment.
Course Instructor

Course Instructor Group

- cmsecurity@wgu.edu
- Schedule an Appointment with any Course Instructor

Course Instructor Responsibility

- How to Work with Course Instructors