Secure Software Design focuses on the variety of elements needed to address and implement secure software acquisition and development throughout the software development life cycle (SDLC). It covers the end-to-end principles and addresses people, technology (tools), and processes to design and develop consistently secure applications. Additionally, this course underscores the importance and value of the defense in depth principle across the entire SDLC. Finally, this course introduces techniques to adapt common security activities to modern software development practices, including Agile/Scrum and DevOps. There are no prerequisites for this course.

Competencies

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

- **Security in the SDLC**
  The graduate applies appropriate software security controls to each phase of the Software Development Lifecycle (SDLC) in order to design and develop secure applications.

- **The Human Element**
  The graduate demonstrates strategies to address the human element in order to design and develop secure applications.

- **Building Security In**
  The graduate implements security practices for development in order to honor the principles of “Building Security In.”

- **Security Control Effectiveness**
  The graduate assesses the effectiveness of software security controls in order to make adjustments as needed.

- **Addressing Defects and Vulnerabilities**
The graduate evaluates software defects and vulnerabilities in order to develop strategies to remediate those defects and to prevent future occurrences.

Getting Started

Welcome to Secure Software Design! In this uCertify course you will encounter videos, labs, and interactive knowledge checks. Complete each lesson and deepen your grasp of the main concepts using the tools provided. Competency will be demonstrated by the successful completion of an objective assessment. The pacing guide, included in the Welcome section of the course, provides a suggested weekly plan for working through the materials in a timely manner.

Assessments

- **Pre-Assessment: Secure Software Design (ALO2)**
  - Status: Not Attempted
  - Time Allotted: **150 minutes**
  - # of Items: **70**
  - Code: **PAKA**

- **Objective Assessment: Secure Software Design**
  - Status: Not Attempted
  - Time Allotted: **150 minutes**
Diagnostic: Secure Software Design

STATUS: Not Attempted

TIME ALLOTTED: 150 minutes

# OF ITEMS: 17

CODE: XAKA

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.

On objective assessments, you will be charged a retake fee for the third attempt and every attempt thereafter. For more information click here.

Course Instructor Group

cmsecurity@wgu.edu

Schedule an Appointment with any Course Instructor