Carnegie Mellon University
Software Engineering Institute

CERT Cybersecurity Engineering and Software Assurance Professional Certificate

Improve the software assurance of your systems and increase your overall cybersecurity.

Overview

The SEI offers certificate programs in different software-engineering-related topics that acknowledge your professional accomplishments in a technical curriculum. One of these certificates is the CERT Cybersecurity Engineering and Software Assurance Professional Certificate, which covers the technical areas that include engineering software-reliant systems and implementing strategies that instill cybersecurity in acquired systems.

As your organization acquires, builds, deploys, and maintains software-reliant systems, you encounter opportunities and risks. How you deal with these opportunities and risks can determine how successful your organization meets its business objectives.

The Focus Has Changed

Traditionally, organizations focused solely on the capabilities and performance of software-reliant systems and evaluated them by answering questions such as What can they do? How fast can they do it? How accurate are the results? and How much do they cost?

Today, organizations must also consider quality attributes such as security, reliability, and adaptability. These attributes largely determine a system's suitability for use in its target environment, and that environment is challenging.

The Challenges You Face

Attackers continually find new ways to circumvent security controls and infiltrate systems. Likewise, security practices and technologies evolve to keep pace with this changing landscape. A software-reliant system that isn't designed, operated, and sustained with security in mind is a target for adversaries to attack. The consequences of such attacks can include massive unforeseen costs, mission failure, exposed sensitive data, destruction of property, and even loss of life. To protect your organization, it must adapt to the changes in the environment, whether they are problems posed by attackers or solutions supplied by researchers and developers.

About the Certificate Program

Earning a CERT Cybersecurity Engineering and Software Assurance Professional Certificate prepares you to develop, acquire, and protect systems that must exist in environments where they interact with multiple systems, some of which are untrustworthy. You learn to navigate the continual change and evolving threats and risks in these environments. You get access to the most current knowledge and expertise, and develop skills to protect your software-reliant systems.

The certificate program teaches you to recognize the knowledge areas critical to software assurance. By earning this certificate, you demonstrate that you know how to identify security requirements early in the development or acquisition lifecycle, at the same time as you identify functional requirements. You learn how to monitor security risks as they change throughout the lifecycle and across the supply chain, and you learn about the complexity and risks in your supply chain and how to deal with them. Completing this certificate program proves that you understand the gaps in supply chain risk management and know how to develop an acquisition strategy to drive your organization's supply chain structure.

Certificate Program Components

The following components make up the CERT Cybersecurity Engineering and Software Assurance Professional Certificate program.

COMPONENT	OBJECTIVES
Software Assurance Methods in Support of Cybersecurity Engineering In this course, you study the CERT Cybersecurity Engineering curriculum and learn about the areas critical to software assurance: security requirements, risk analysis, and software supply chain assurance. You learn the concepts and resources available to address software security assurance across the acquisition and development lifecycles.	**In the course, you** • learn methods to support cybersecurity in the context of current software realities, the software landscape, and the principles of software assurance • learn about the cybersecurity lifecycle in relation to requirements engineering, assured design, assured software development, and software quality models • discuss mission assurance and the Security Engineering Risk Analysis (SERA) method • apply software assurance to acquisition and supply chain risk management
SQUARE Workshop In this workshop, you learn common techniques for identifying security requirements in the software development lifecycle. You learn specifically how to use the Security Quality Requirements (SQUARE) method to prevent and minimize security vulnerabilities. With the SQUARE method, you also learn how to identify functional and security requirements at the same time.	**During the workshop, you** • discuss the challenges of security requirements engineering and identify security requirements • explore how methods for identifying functional requirements may not work for security requirements • are introduced to security risk analysis, security requirements elicitation, and security requirements identification
Security Engineering Risk Analysis (SERA) Tutorial In this tutorial, you learn the SERA method, a systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain. With SERA, you focus on addressing design weaknesses as early in the lifecycle as possible, before deployment. Through a series of exercises, you apply the SERA method to a mock acquisition of a critical emergency system.	**With SERA, you learn** • how to review risk management concepts as applied to software engineering and systems engineering • a method of risk analysis applied to software engineering • to apply the SERA steps to a realistic system acquisition scenario • how to identify and address cybersecurity weaknesses during the design phase of the software development lifecycle
Supply Chain Risk Management Course In this course, you explore the complex, multi-layered information and communication technologies related to an organization's supply chain, focusing specifically on software. You learn about effective acquisition security risk management, including discussing how to develop a sound acquisition strategy that defines supply-chain-related actions.	**In this course, you** • identify gaps in current supply chain risk management practices • explore different types of supply chain relationships • are guided through developing an acquisition strategy to drive your organization's supply chain structure
Advanced Threat Modeling Course This course is a deep dive into the threat modeling techniques that were introduced in the SQUARE Workshop. The STRIDE Methodology is expanded and three additional threat modeling techniques are taught, including the most recently developed threat modeling method.	**In this course, you** • learn about the role of threat modeling in the security development lifecycle • develop the ability to apply any of the four threat models to a system • assess new threat modeling methods for applicability in a system environment
CERT Cybersecurity Engineering and Software Assurance Professional Certificate Examination This examination evaluates your understanding of the material you learned in the above components to earn the CERT Cybersecurity Engineering and Software Assurance Professional Certificate. You take this examination at your convenience over a six-hour period. To obtain the certificate, you must achieve a passing score of 80%.	**This examination proves that you have a solid understanding of the following concepts:** • cybersecurity engineering • risk management • software assurance • threat modeling

The Certificate Experience

As a student in the CERT Cybersecurity Engineering and Software Assurance Professional Certificate program, you complete five eLearning courses in CERT STEPfwd. These courses include 15 hours of instruction and 16 exercises that help you learn, apply what you've learned, and develop new skills. After you complete the coursework, you take a capstone examination that assesses your understanding of the subject matter covered in all of the eLearning you've completed.

Once you register for the CERT Cybersecurity Engineering and Software Assurance Professional certificate, you have daily 24-hour access to course materials for 12 months. During those 12 months, you can move at your own pace through course materials at your convenience and review and repeat individual sections as often as you like.

Once you successfully complete the certificate program, you receive an official certificate from the SEI and the option of having your name and accomplishment published on the SEI website.

The course slides and transcripts of each lecture are available to download. All referenced technical reports are included as downloadable content.

The curriculum and materials are based on the book titled *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance* (SEI Series in Software Engineering) by Nancy Mead and Carol Woody.

Who Should Attend

This certificate is designed for software acquirers and developers, software and system assurance managers, systems engineers, and software engineers.

Prerequisites

Students must have a basic understanding of software assurance and familiarity with the challenges of system security.

Equip Your Organization for Success

To apply the latest security practices and technologies successfully, you need to have the right knowledge, skills, and experience. Learn more about and apply to register for the CERT Cybersecurity Engineering and Software Assurance Professional Certificate: **https://sei.cmu.edu/education-outreach/credentials/credential.cfm?customel_datapageid_14047=33881**.

STEPfwd: Your eLearning Environment

The SEI offers flexible remote training in CERT STEPfwd (Simulation, Training, and Exercise Platform). STEPfwd makes components from traditional classroom training available online. Using a web browser, you access course components, including training sessions, transcripts, and exercises.

STEPfwd's "anytime, anywhere" access enables you to see training sessions, use hands-on training labs, and complete exercises—all to improve your skills through realistic and flexible training scenarios.

To use CERT STEPfwd effectively, you need the following:

- web browsers: Internet Explorer 7+ or Firefox 3+
- Adobe Flash version 10+ (for lecture and demo access)
- JRE Version 6+ (for lab access)
- computer system and network settings that allow access to streaming video from Internet sources
- minimum client resolution of 1280 x 1024 (to enable proper video and lab player display)
- Internet connection of 384 Kbps or greater (to sustain downloads with no more than 230 ms of latency)

Training courses provided by the SEI are not academic courses for academic credit toward a degree. Any certificates provided are evidence of the completion of the courses and are not official academic credentials.

About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu