

CN-CSC CYBER SECURE CODER



| DURATION | LEVEL | TECHNOLOGY | DELIVERY METHOD | TRAINING CREDITS |
|----------|--------------|----------------|----------------------|------------------|
| 3 Days | Intermediate | Cyber Security | Classroom or Virtual | N/A |

INTRODUCTION

The stakes for software security are very high, and yet many development teams deal with software security only after the code has been developed and the software is being prepared for delivery. As with any aspect of software quality, to ensure successful implementation, security and privacy issues should be managed throughout the entire software development lifecycle. This course presents an approach for dealing with security and privacy throughout the entire software development lifecycle. You will learn about vulnerabilities that undermine security, and how to identify and remediate them in your own projects. You will learn general strategies for dealing with security defects and misconfiguration, how to design software to deal with the human element in security, and how to incorporate security into all phases of development.

AUDIENCE PROFILE

This course is designed primarily for:

- Software developers, testers, and architects who design and develop software in various programming languages and platforms including desktop, web, cloud, and mobile, and who want to improve their ability to deliver software that is of high quality, particularly regarding security and privacy.
- Students seeking the Cyber Secure Coder certification

PREREQUISITES

This course presents secure programming concepts that apply to many different types of software development projects. While this course uses Python, HTML, and JavaScript to demonstrate various programming concepts, you do not need to have experience in these languages to benefit from this course. However, you should have some programming experience, whether it be developing desktop, mobile, web, or cloud applications.

COURSE OBJECTIVES

In this course, you will employ best practices in software development to develop secure software. You will:

- Identify the need for security in your software projects.
- Eliminate vulnerabilities within software.
- Use a Security by Design approach to design a secure architecture for your software.
- Implement common protections to protect users and data.
- Apply various testing methods to find and correct security defects in your software.
- Maintain deployed software to ensure ongoing security.

COURSE TOPICS

Lesson 1: Identifying the Need for Security in Your Software Projects

- Identify Security Requirements and Expectations
- Identify Factors That Undermine Software Security
- Find Vulnerabilities in Your Software
- Gather Intelligence on Vulnerabilities and Exploits

Lesson 2: Handling Vulnerabilities

- Handle Vulnerabilities Due to Software Defects and Misconfiguration
- Handle Vulnerabilities Due to Human Factors
- Handle Vulnerabilities Due to Process Shortcomings

Lesson 3: Designing for Security

- Apply General Principles for Secure Design
- Design Software to Counter Specific Threats

Lesson 4: Developing Secure Code

- Follow Best Practices for Secure Coding
- Prevent Platform Vulnerabilities
- Prevent Privacy Vulnerabilities

Lesson 5: Implementing Common Protections

- Limit Access Using Login and User Roles

- Protect Data in Transit and At Rest
- Implement Error Handling and Logging
- Protect Sensitive Data and Functions
- Protect Database Access

Lesson 6: Testing Software Security

- Perform Security Testing
- Analyze Code to find Security Problems
- Use Automated Testing Tools to Find Security Problems

Lesson 7: Maintaining Security in Deployed Software

- Monitor and Log Applications to Support Security

- Maintain Security after deployment

ASSOCIATED CERTIFICATIONS & EXAM

The Cyber Secure Coder exam (#CSC-210) will certify that the successful candidate has the knowledge, skills, and abilities to design and develop a variety of applications for various platforms, analyze security concerns outside of specific languages and platforms, use a number of testing and analysis tools, and mitigate against common threats to data and systems.

Upon completion of this course, delegates will receive an MIE attendance certificate.