

Cyber Secure Coder (Exam CSC-110)

Référence : CSC

Niveau : Début

Durée : 3 jours (21h.)

Tarif: Nous Contacter

Date: Juin Juillet Septembre

Contact: +225 22469017 / 74622582

Objectifs

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.

Public

This course is designed 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.

This course is also designed for students who are seeking the Logical Operations Cyber Secure Coder (CSC) Exam CSC-110 certification.

Pré-requis

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. Logical Operations provides a variety of courses covering software development that you might use to prepare for this course, such as:

- *Developing Secure Universal Windows® Platform Apps in C# and XAML*
- *Developing Secure iOS® Apps for Business*
- *Developing Secure Android™ Apps for Business*
- *Python® Programming: Introduction*
- *Python® Programming: Advanced*
- *Programming Google App Engine™ Applications in Python®*
- *HTML5: Content Authoring with New and Advanced Features*
- *SQL Querying: Fundamentals*

Contenu du cours

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

Topic A: Identify Security Requirements and Expectations

Topic B: Identify Factors That Undermine Software Security

Topic C: Find Vulnerabilities in Your Software

Topic D: Gather Intelligence on Vulnerabilities and Exploits

Lesson 2: Handling Vulnerabilities

Topic A: Handle Vulnerabilities Due to Software Defects and Misconfiguration

Topic B: Handle Vulnerabilities Due to Human Factors

Topic C: Handle Vulnerabilities Due to Process Shortcomings

Lesson 3: Designing for Security

Topic A: Apply General Principles for Secure Design

Topic B: Design Software to Counter Specific Threats

Lesson 4: Developing Secure Code

Topic A: Follow Best Practices for Secure Coding

Topic B: Prevent Platform Vulnerabilities

Topic C: Prevent Privacy Vulnerabilities

Lesson 5: Implementing Common Protections

Topic A: Limit Access Using Login and User Roles

Topic B: Protect Data in Transit and At Rest

Topic C: Implement Error Handling and Logging

Topic D: Protect Sensitive Data and Functions

Topic E: Protect Database Access

Lesson 6: Testing Software Security

Topic A: Perform Security Testing

Topic B: Analyze Code to find Security Problems

Topic C: Use Automated Testing Tools to Find Security Problems

Lesson 7: Maintaining Security in Deployed Software

Topic A: Monitor and Log Applications to Support Security

Topic B: Maintain Security after Deployment