CertNexus Cyber Secure Software Developer™ (CSSD) Exam CSD-110

Course Number:

CNX0022

Course Length:

5 days

Overview:

The stakes for software security are high, and yet many development teams overlook it until it's too late—if they address it at all. To ensure successful implementation, it is crucial for developers to manage security and privacy issues throughout the entire software development lifecycle, rather than addressing them only after coding or during delivery preparation.

This course presents an approach for dealing with security throughout all phases of the software development lifecycle. You will identify the fundamentals of security, including the vulnerabilities and attacks that compromise it. You will also employ general strategies for addressing security risks to your software projects, as well as specific tactics for identifying and remediating those risks. Ultimately, you will acquire the skills it takes to secure all facets of a software project, beyond just the code itself.

Course Objectives:

In this course, you will employ best practices to develop secure software.

You will:

- Identify fundamental security concerns in software development.
- Leverage the secure software development lifecycle (SSDLC).
- Define secure software requirements.
- Design software for security.
- Implement security protections in software.
- Test software security.
- Maintain security in deployed software.
- Prepare to defend against cyber attacks.

Target Student:

This course is designed for any business professional involved in the software development process who desires or is required to develop highly secure software for organizational use. Candidates may be programmers, testers, architects, or any other personnel whose daily job duties involve directly building software; or, they may be project leaders, software engineers, and DevOps personnel who perform additional technical and non-technical duties as part of the overall software development lifecycle.

This course is also designed to assist candidates in preparing for the CertNexus Cyber Secure Software Developer™ (CSSD) Exam CSD-110 certification.

Course Prerequisites:

Although this course uses languages like Python®, SQL, and JavaScript® to demonstrate various programming concepts, you do not need to have experience in any specific 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:

- *Introduction to Programming with Python® (Second Edition)*
- *Advanced Programming Techniques with Python® (Second Edition)*
- *R Programming for Data Science*
- *Web Development with HTML5, CSS, and JavaScript™*
- *SQL Querying: Fundamentals (Third Edition)*

Course Content

Lesson 1: Identifying Fundamental Security Concerns in Software Development

Topic A: Identify the Need for Software Security

Topic B: Identify Factors That Undermine Software Security

Topic C: Identify Fundamental Principles of Cybersecurity

Topic D: Identify Common Vulnerabilities in Software

Topic E: Identify Common Attacks and Exploits Against Software

Lesson 2: Leveraging the Secure Software Development Lifecycle

Topic A: Apply the Builder/Breaker Approach

Topic B: Incorporate SSDLC Practices and Methodologies

Topic C: Apply SSDLC Practices in the Use of AI

Topic D: Incorporate Governance, Risk Management, and Compliance (GRC) in the SSDLC

Topic E: Identify Key Roles in the SSDLC

Topic F: Foster a Security-First Organizational Culture

Lesson 3: Defining Secure Software Requirements

Topic A: Define Compliance Requirements

Topic B: Define Security Requirements

Lesson 4: Designing for Security

Topic A: Apply General Principles for Secure Design

Topic B: Define the Security Architecture

Topic C: Conduct Threat Modeling

Lesson 5: Implementing Security Protections

Topic A: Implement Cryptography

Topic B: Implement Application Security Parameters and Configurations

Topic C: Implement Access Control

Topic D: Protect Database Access

Topic E: Implement Error Handling and Logging

Lesson 6: Testing Software Security

Topic A: Perform Security Tests

Topic B: Analyze Software to Identify Security Issues

Lesson 7: Maintaining Security in Deployed Software

Topic A: Implement Secure Deployment Processes

Topic B: Ensure Device Security

Topic C: Monitor Deployed Software

Topic D: Maintain Security After Deployment

Topic E: Decommission Legacy Assets

Lesson 8: Preparing to Defend Against Cybersecurity Attacks

Topic A: Identify the Stages of the Cyber Kill Chain

Topic B: Continuously Analyze the Cybersecurity Landscape

Topic C: Continuously Improve Secure-Coding Knowledge and Skills