010 612 0679
www.tlo.co.za

Cyber Secure Coder (Exam ITP-110)
3 Days

1. PROGRAMME OVERVIEW

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.

2. 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.

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

3. Technical Requirements

Hardware

- 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor
- 2 gigabytes (GB) RAM (32-bit or 64-bit)
- 20 GB available hard disk space (32-bit or 64-bit)
- Keyboard and mouse (or other pointing device)
- 1,024 x 768 resolution monitor recommended
- Projection system to display the instructor's computer screen
- Local area network and Internet connection recommended

Software

- Windows® 10/8.1/8/7/Vista (64-bit). This course was successfully keyed on Windows 10.
- Python version 2.7.13 (python-2.7.13.amd64.msi, provided with the course data files)

4. PROGRAMME OUTLINES

Module 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

Module 2: Handling Vulnerabilities
Handle Vulnerabilities Due to Software Defects and Misconfiguration
Handle Vulnerabilities Due to Human Factors
Handle Vulnerabilities Due to Process Shortcomings

Module 3: Designing for Security
Apply General Principles for Secure Design
Design Software to Counter Specific Threats

Module 4: Developing Secure Code
Follow Best Practices for Secure Coding
Prevent Platform Vulnerabilities
Prevent Privacy Vulnerabilities

Module 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

Module 6: Testing Software Security
Perform Security Testing
Analyze Code to find Security Problems
Use Automated Testing Tools to Find Security Problems

Module 7: Maintaining Security in Deployed Software
Monitor and Log Applications to Support Security
Maintain Security after Deployment

5. PROGRAMME METHODOLOGY

The programme is instructor led by an industry specialist. The programme is practical in nature and delegates will learn by given scenarios/case studies.