CERTIFIED SECURE SOFTWARE LIFECYLCE PROFFESSONAL (CSSLP)

Who Should Attend

This course is intended for software developers, Engineers Architects, Penetration Testers and other IT professionals who have a minimum of four-years' experience in full-time Software Development Lifecycle (SDLC) in one or more of the eight domains covered in the CSSLP exam.

Course Objectives

Upon successful completion of this course, students will be able to:

- Prepare for and pass the CSSLP exam.
- Identify security software requirements.
- Follow secure coding practices.
- Develop a security testing strategy and plan.
- Choose a secure software methodology.
- Release software securely.

Course Outline

1 – SECURE SOFTWARE CONCEPTS

- Core Concepts
- Security Design Principles

2 – SECURE SOFTWARE REQUIREMENTS

- Identify Security Requirements
- Interpret Data Classification Requirements
- Identify Privacy Requirements

3 – SECURE SOFTWARE DESIGN

- Perform Threat Modeling
- Define the Security Architecture
- Model (Non-Functional) Security Properties and Constraints
- Evaluate and Select Reusable Secure Design
- Use Security Enhancing Architecture and Design Tools
- Use Secure Design Principles and Patterns

4 – SECURE SOFTWARE IMPLEMENTATION/PROGRAMMING

- Follow Secure Coding Practices
- Analyze Code for Security Vulnerabilities
- Implement Security Controls
- Fix Security Vulnerabilities
- Look for Malicious Code
- Securely Reuse Third Party Code or Libraries
- Securely Integrate Components
- Apply Security During the Build Process
- Debug Security Errors

5 – SECURE SOFTWARE TESTING

- Develop Security Test Cases
- Develop Security Testing Strategy and Plan
- Identify Undocumented Functionality
- Interpret Security Implications of Test Results
- Classify and Track Security Errors
- Secure Test Data
- Develop or Obtain Security Test Data
- Perform Verification and Validation Testing (e.g., IV&V)

6 – SOFTWARE LIFECYCLE MANAGEMENT

- Secure Configuration and Version Control
- Establish Security Milestones
- Choose a Secure Software Methodology
- Identify Security Standards and Frameworks
- Create Security Documentation
- Develop Security Metrics
- Decommission Software
- Report Security Status
- Support Governance, Risk and Compliance (GRC)

7 – SOFTWARE DEPLOYMENT, OPERATIONS AND MAINTENANCE

- Perform Implementation Risk Analysis
- Release Software Securely
- Securely Store and Manage Security Data
- Ensure Secure Installation
- Perform Post-Deployment Security Testing
- Obtain Security Approval to Operate
- Perform Security Monitoring (e.g., Managing Error Logs, Audits, Meeting SLA's, CIA Metrics)
- Support Incident Response
- Support Patch and Vulnerability Management
- Support Continuity of Operations

8 – SUPPLY CHAIN AND SOFTWARE ACQUISITION

- Analyze Security of Third Party Software
- Verify Pedigree and Provenance
- Provide Security Support to the Acquisition Process