4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

Software Development Security Training

Cost: $1265.00/person

Length: 4 Days

Summary: Software Development Security Training course is designed for professionals who demonstrate a globally recognized level of competence, as defined in a common body of knowledge, by assuring security throughout the software lifecycle. They incorporate security when planning, designing, developing, acquiring, testing, deploying, maintaining, and/or managing software to increase its trustworthiness.

This four day program is comprised of a total of eight domains. The modular format is designed to organize and chunk information in order to assist with learning retention as participants are guided through the CSSLP course materials. Each module/domain includes one or more of the following design approaches to support knowledge retention and transfer:

- **Presentation -** The facilitator explains content to participants using PowerPoint to guide the presentation. Multiple examples are used to clarify points.
- **Short Lecture/Discussion -**The facilitator engages participants in conversation by asking questions and encouraging them to respond. Participants are encouraged to provide examples from their experience.
- **Group Activity** - Participants work in small teams of three or four. The facilitator debriefs the entire class at the end of the activity.
- **Individual Activity** - Individuals work on their own to complete an action plan, worksheet, or evaluation.

Objectives

- The goal of the **Security Software Concepts** module is to provide the learner with concepts related to the core software security requirements and foundational design principles as they relate to issues of privacy, governance, risk, and compliance. Learners will understand the software methodologies needed in order to develop software that is secure and resilient to attacks.
- The goal of **the Security Software Requirements** module is to provide the learner with concepts related to understanding the importance of identifying and developing software with secure requirements. The learner will be able to incorporate security requirements in the development of software in order to produce software that is reliable, resilient, and recoverable.
- The design phase of **secure software development** is one of the most important phases in the Software Development Lifecycle. The Security Software Design module provides the learner with an understanding of how to ensure that software security requirements are included in the design of the software. Learners will gain knowledge of secure design principles and processes, and be exposed to different architectures and technologies for securing software.
- The **Security Software Implementation/Coding** module provides the learner with an understanding of the importance of programming concepts that can effectively protect software from vulnerabilities. Learners will touch on topics such as software coding

4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

vulnerabilities, defensive coding techniques and processes, code analysis and protection, and environmental security considerations that should be factored into software.

- The **Security Software Testing** module addresses issues pertaining to proper testing of software for security, including the overall strategies and plans. Learners will gain an understanding of the different types of functional and security testing that should be performed, the criteria for testing, concepts related to impact assessment and corrective actions, and the test data lifecycle.
- The **Software Acceptance** module provides an understanding of the requirements for software acceptance, paying specific attention to compliance, quality, functionality, and assurance. Participants will learn about pre- and post-release validation requirements and well as pre-deployment criteria.
- The **Software Deployment, Operations, Maintenance, and Disposal** module provides the learner with knowledge pertaining to the deployment, operations, maintenance, and disposal of software from a secure perspective. This is achieved by identifying processes during installation and deployment, operations and maintenance, and disposal that can affect the ability of the software to remain reliable, resilient, and recoverable in its prescribed manner.
- The **Supply Chain and Software Acquisition** module provides the learner with knowledge on how to perform effective assessments on an organization's cyber-supply chain, and describes how security applies to the supply chain and software acquisition process. Learners will understand the importance of supplier sourcing and being able to validate vendor integrity, from third-party vendors to complete outsourcing. Finally, learners will understand how to manage risk through the adoption of standards and best practices for proper development and testing across the entire lifecycle of products.

Course Content

DOMAIN 1 - SECURE SOFTWARE CONCEPTS

- Module 1: Concepts of Secure Software
- Module 2: Principles of Security Design
- Module 3: Security Privacy
- Module 4: Governance, Risk, and Compliance
- Module 5: Methodologies for Software Development

DOMAIN 2 - SECURITY SOFTWARE REQUIREMENTS

- Module 1: Policy Decomposition
- Module 2: Classification and Categorization
- Module 3: Functional Requirements - Use Cases and Abuse Cases
- Module 4: Secure Software Operational Requirements

DOMAIN 3 - SECURE SOFTWARE DESIGN

- Module 1: Importance of Secure Design
- Module 2: Design Considerations
- Module 3: The Design Process
- Module 4: Securing Commonly Used Architectures

DOMAIN 4 - SECURE SOFTWARE IMPLEMENTATION/CODING

- Module 1: Fundamental Programming Concepts
- Module 2: Code Access Security
- Module 3: Vulnerability Databases and Lists

4350 Executive Drive, Suite 100
San Diego, CA 92121
San Diego (858) 546-1400

- Module 4: Defensive Coding Practices and Controls
- Module 5: Secure Software Processes

DOMAIN 5 - SECURITY SOFTWARE TESTING

- Module 1: Artifacts of Testing
- Module 2: Testing for Secure Quality Assurance
- Module 3: Types of Testing
- Module 4: Impact Assessment and Corrective Action
- Module 5: Test Data Lifecycle Management

DOMAIN 6 - SOFTWARE ACCEPTANCE

- Module 1: Software Acceptance Considerations
- Module 2: Post-Release

DOMAIN 7 - SOFTWARE DEPLOYMENT, OPERATION, MAINTENANCE AND DISPOSAL

- Module 1: Installation and Deployment
- Module 2: Operations and Maintenance
- Module 3: Disposal of Software

DOMAIN 8 - SUPPLY CHAIN AND SOFTWARE ACQUISITION

- Module 1: Supplier Risk Assessment
- Module 2: Supplier Sourcing
- Module 3: Software Development and Test
- Module 4: Software Delivery, Operations, and Maintenance
- Module 5: Supplier Transitioning