Secure by Design

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **3 Days**

Overview

With the increase in cyber-attacks on business, it's time to start building security into new systems developments right from the start. The majority of successful cyber-attacks depend on exploiting a few well-known common vulnerabilities. This course, updated for 2018, will show you how security can be designed into, managed and maintained within a development lifecycle.

Prerequisites

There are no specific pre-requisites for this course. However a general understanding of development practices and a broad understanding of current threats would be desired. There are group exercises, and instructor led ‘hands-on’ labs within each module of this course. Delegates can observe the instructor demonstrations or engage fully with each hands-on lab, subject to experience.

The intended audience for this course is primarily Project Managers, Business Analysts, Junior Developers and Designers. Plus anyone with an interest in building and maintaining secure systems lifecycle.

Note: This course is not designed for the experienced software developer and does not cover hands-on coding.

What You Will Learn

- Understand the main Secure Development Lifecycle (SDLC) Models, and their principal differences
- Be able to choose which SDLC model is most appropriate in a given situation.
- Learn how to apply secure development techniques from the initial design stage and throughout a development lifecycle
- Understand the latest (2017) OWASP vulnerabilities and how to counter/mitigate them
- Learn about useful system design tools
- Discover resources to help introduce and use secure design and development best practices
- Learn Threat Modelling methodologies and techniques
- Understand the benefits of code review
- Understand various testing strategies
- Learn about encryption, securing and compromising passwords and meta data
- An introduction to the classification of security flaws and application security

Outline

Module 1 - Secure Development Lifecycle (SDLC)

- An overview of the main SDLC models
- Development models (Inc. DevSecOps)
- Configuration and source code management
- Risk analysis tools
- Privacy by Design

Module 2 - Secure By Design

- Secure development processes
- Threat modelling
- Risk mitigation
- Security best practice
- Secure design architecture

Module 3 – Introduction to Application Security (OWASP 2017)

- Vulnerabilities and mitigations available to any development environment
- Attack vectors and security controls
- The OWASP (2017) Top 10 in detail
- Vulnerability 1 (2017) – Injection
- Vulnerability 2 (2017) – Broken Authentication
- Vulnerability 3 (2017) – Sensitive Data Exposure
- Vulnerability 4 (2017) – XML External Entities (XXE)
- Vulnerability 5 (2017) – Broken Access Controls
- Vulnerability 6 (2017) – Security Misconfigurations
- Vulnerability 7 (2017) – Cross-Site Scripting
- Vulnerability 8 (2017) – Insecure Deserialization
- Vulnerability 9 (2017) – Using Components with Known Vulnerabilities
- Vulnerability 10 (2017) – Insufficient Logging and Monitoring

Module 4 – Introduction to Defensive Coding

- Secure coding techniques and principles.
- Methods of testing code, and code test analysis
- Using, compromising and defending encryption, hashes and passwords
- Classification of security flaws