SDL Fundamentals Course

Advanced Level

1-Day Course

Syllabus

AppSec Labs Ltd.

info@appsec-labs.com | https://appsec-labs.com | 23 HaTa'as St., Kfar Saba 44641 Israel | T: +972-9-7485005 | F: +972-9-7730595

SDL Fundamentals Course: Advanced Level
1-day course

Seminar Description

Secure programming from the requirement to release is the best defense against hackers.

This seminar will focus on the Microsoft SDL methodology in addressing and integrating security throughout the development lifecycle.

The training will focus on how security architect and developers should implement SDL practices from Microsoft perspective in waterfall and Agile programing model and for on premise VS cloud application.

In addition, the training will demonstrate live, real time hacking methods, analyze the code deficiency doing live threat model, analyzing insecure design that enabled the attack and most importantly, understand how to prevent such vulnerabilities by adopting secure coding best practices in order to secure applications.

At the end of this training the student will have better understanding for SDL process and the way it's implemented at Microsoft R&D center, and will also be familiar with tools and methods to use during SDL, as well as how to perform threat analysis for applications during design stage.

Target Audience

Members of the software development team:

- Designers & Architects
- Developers
- Security trustees and teams

Prerequisites

Before attending this seminar, students should be familiar with:

- Basic Knowledge of Applications & Programming concepts
- Basic Knowledge of Microsoft SDL process

Course topics

Introduction to Application Security

- Why we need information security?
- What is application security?
- Security trends and motivation
- The cost of a vulnerability breach
- Common hacking from development prospective
  - Fraud
  - Identity theft
  - Privilege escalation
  - Phishing
  - Sensitive information disclosure & data theft
- Real-life examples
- Common privacy and security standards

SDL Overview

- SDL Objectives
- Motivation for SDL
- Origins of the Microsoft SDL
- Waterfall VS. Agile
- SDL Flow
- Assigning security requirements to SDL projects

Pre-SDL: Security Training

- Core security training
- The need for security training
- Training criteria & frequency
- Training methods
- Training – takeaways

Phase One: Requirements

- The importance of security requirement
- Establishing security requirements
- Tracking security bugs
- Security risk assessment
- Privacy
- Requirements in the Cloud
- Demo: analyzing security requirements for cloud service
- Requirements – takeaways

Phase Two: Design

- Establishing security requirements
- Attack surface reduction
- Cloud security services – Azure & AWS case study
- SDL Developer Starter Kit- Secure Design Principles
- Threat Modeling
  - STRIDE VS. DREAD Model
  - Demo – Good/Bad threat model
  - Demo - using the TM tool
  - Lab - threat modeling
- Diagraming
- Cloud threats
- Mitigation strategies
- Design phase in the Cloud
- Design - takeaways

Phase Three: Implementation

- Tools for secure coding
  - BinScope
  - Visual Studio Code Analysis tools
  - FxCop
- Manage VS. unmanaged code
- Unsafe functions and Banned APIs
- Security features
- Static analysis
- Secure coding guidelines
- Secure implementation in the Cloud
- Demo – code review
- Implementation – takeaways

Phase Four: Verification

- Dynamic analysis
- Security testing methods
- Fuzz testing
- Penetration testing
- Cloud top 10 vulnerabilities
- Tools and methods for security verification
  - Demo: using fiddler for Fuzzing and Penetration testing
  - Demo: Burp
  - Demo SSL Scanner
- Reevaluate attack surface
- Attack Surface Analyzer
- Verification – takeaways

Phase Five: Release

- Creating an incident response plan
- Privacy Escalation Response Framework (PERF)
- IR Cloud VS. on-Premise
- Final Security Reviews (FSR)
- Security bug bar
- Release & Archive
- Release – takeaways

Post-SDL: Response

- Executing an incident response plan
- Executing an incident response plan
- Microsoft Security Response Center
- Security Bulletins
- Security Advisories
- Microsoft Baseline Security Analyzer (MBSA)
- Response – takeaways