DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

Fundamentals of Secure Application Development (APPSECFUNDS)

ID CM-APPSECFUNDS **Price** CAD 1,795 **Duration** 3 days

Who should attend

- Application Development Managers
- Software Engineers and Developers
- CISOs, CISAs and Security Professionals
- Software Testers
- QA Managers, Directors and Staff
- Test Management
- Business Analysts
- Project Managers
- IT Specialists (Security, Capacity Management, Networking…)

Course Content

The rules of information security aren't what they used to be. Hackers aren't kids in basements–they're state sponsored professionals and organized criminal groups all around the world. They break into systems and steal data any way they can.

Unfortunately, the vast majority of hacks are not due to insecure networks or misconfigured firewalls; they are a result of common software flaws that get coded into applications. Even with good information security policy and staff, the reality is that software developers are often underserved when it comes to security strategy. If their applications get built without attention to good software security practices, risk gets passed downstream and by the time an incident occurs it's too late to be proactive.

From proactive requirements to coding and testing, this course covers the best practices any software developer needs to avoid opening up their users, customers and organization to attack at the application layer. We teach only constantly updated best practices, and our experts answer your questions live in class. Return to work ready to build higher quality, more robustly protected applications.

Detailed Course Outline

Part 1: Secure Software Development

- Assets, Threats & Vulnerabilities
- Security Risk Analysis (Bus & Tech)
- Secure Dev Processes (MS, BSI…)
- Defense in Depth
- Approach for this course

Introductory Case Study

Part 2: The Context for Secure Development

- Assets to be protected
- Threats Expected
- Security Imperatives (int&external)
- Organization's Risk Appetite
- Security Terminology
- Organizational Security Policy
- Security Roles and Responsibilities
- Security Training for Roles
- Generic Security Goals & Requirements

Fast Lane
Consulting & Education Services, Inc.
900 Greenbank Road, Suite 536, K2J 4P6 Nepean, Canada
Toll Free: (855) 778-7246
info@fastlaneus.com

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

Exercise: Our Own Security Context

Part 3: Security Requirements

- Project-Specific Security Terms
- Project-Related Assets & Security Goals
- Product Architecture Analysis
- Use Cases & MisUse/Abuse Cases
- Dataflows with Trust Boundaries
- Product Security Risk Analysis
- Elicit, Categorize, Prioritize SecRqts
- Validate Security Requirements

Exercise: Managing Security Requirements

Part 4: Designing Secure Software

[list]
- High-Level Design
- Architectural Risk Analysis
- Design Requirements
- Analyze Attack Surface
- Threat Modeling
- Trust Boundaries
- Eliminate Race Objects

- Detail-Level Design
- Secure Design Principles
- Use of Security Wrappers
- Input Validation
- Design Pitfalls
- Validating Design Security
- Pairing Mem Mgmt Functions
- Exclude User Input from format strings
- Canonicalization
- TOCTOU
- Close Race Windows
- Taint Analysis

[/list]

Exercise: A Secure Software Design, Instructor Q and A

Part 5: Writing Secure Code

- Coding
- Developer guidelines & checklists
- Compiler Security Settings (per)
- Tools to use
- Coding Standards (per language)
- Common pitfalls (per language)
- Secure/Safe functions/methods
- Stack Canaries
- Encrypted Pointers
- Memory Initialization
- Function Return Checking (e.e. malloc)
- Dereferencing Pointers
- Integer type selection
- Range Checking
- Pre/post checking
- Synchronization Primitives
- Early Verification
- Static Analysis (Code Review w/tools)
- Unit & Dev Team Testing
- Risk-Based Security Testing
- Taint Analysis

Exercise: Secure Coding Q and A

Part 6: Testing for Software Security

- Assets to be protected
- Threats Expected
- Security Imperatives (int&external)
- Organization's Risk Appetite
- Static Analysis
- Dynamic Analysis
- Risk-Based Security testing
- Fuzz Testing (Whitebox vs Blackbox)
- Penetration Testing (Whitebox vs Blackbox)
- Attack Surface Review
- Code audits
- Independent Security Review

Exercise: Testing Software for Security

Part 7: Releasing & Operating Secure Software

Fast Lane
Consulting & Education Services, Inc.
900 Greenbank Road, Suite 536, K2J 4P6 Nepean, Canada
Toll Free: (855) 778-7246
info@fastlaneus.com

DELIVERY METHODS

ILT – Instructor-Led Classroom Training
ILT sessions are conducted in a physical classroom environment.

ILO – Instructor-Led Online Training
ILO sessions are conducted via WebEx in a VoIP environment

FLEX Classroom™ – Combined ILT & ILO
FLEX Classroom sessions are delivered via ILT and ILO giving you the ultimate flexibility.

- Incident Response Planning
- Final Security Review
- Release Archive
- OS Protections:
    - Address Space Layout Randomization
    - Non-Executable Stacks
    - W^X
    - Data Execution Prevention
- Monitoring
- Incident Response
- Penetration Testing

Exercise: A Secure Software Release

Part 8: Making Software Development More Secure

- Process Review
- Getting Started
- Priorities

Exercise: Your Secure Software Plan

Fast Lane
Consulting & Education Services, Inc.
900 Greenbank Road, Suite 536, K2J 4P6 Nepean, Canada
Toll Free: (855) 778-7246
info@fastlaneus.com