

## Fortify-SCA and SSC (FTSCA-250-200)

ID FTSCA-250-200 Price 3,000.— €(excl. tax) Duration 4 days

### Important notes for the booking of Open Text trainings

Please note that prepayment is required for participation in an Open Text training course. Participation in a training course is possible for 12 months after booking the course. Cancellations are excluded. For further information, please refer to our [General Terms and Conditions](#).

### Course Overview

This course provides participants with demonstrations and hands-on activities using a practical, Fortify solutions-based approach to identify and mitigate today's most common business security risks to applications. As a students, you will learn to scan, assess and secure applications using the Fortify Static Code Analyzer (SCA) and Software Security Center (SSC). This course includes hands-on activities to:

- Setup applications in Fortify Software Security Center (SSC)
- Successfully run static code application scans and analyze the scan results through multiple platforms including: Audit Workbench, Command Line, and Scan Wizard
- Identify security vulnerabilities from Fortify scan results and Smart View option
- Find, filter, categorize, group, and audit security vulnerabilities found in your code
- Utilize the Fortify IDE Plugins including Visual Studio and Eclipse with Security Assistant
- Manage applications in SSC, utilizing Audit Assistant and bug tracking

### Who should attend

This course is intended for application developers or security auditors who are new to or have been using the Fortify SCA and SSC to develop secure applications. It is also useful for development managers and application security champions.

### Prerequisites

To be successful in this course, you should have the following prerequisites or knowledge:

- Basic programming skills (able to read Java, C/C++, or .NET)
- Basic understanding of web technologies: HTTP Requests and Responses, HTML tags, JavaScript, and server-side dynamic content (JSP, ASP or similar)
- Knowledge of Web and Application development practices
- Experience developing and/or managing software development for security
- Have an understanding of your organization's compliance requirements
- 

### Course Objectives

Upon successful completion of this course, you should be able to:

- Scan applications thoroughly and correctly using Fortify
- Audit Fortify scan results to create a prioritized list of high-impact security findings
- Correctly and efficiently validate security findings
- Build a custom Data Flow Cleanse rule
- Integrate and manage projects through the SSC to ensure good processes

### Course Content

- Module 1: Fortify Architecture and Application Security Overview
- Module 2: Fortify SSC Setup
- Module 3: Fortify SCA Analyzers Metrics
- Module 4: Fortify Static Scanning
- Module 5: Auditing Fortify Scan Results
- Module 6: Data Validation
- Module 7: Analysis Trace and Remediating Vulnerabilities
- Module 8: Custom Rules
- Module 9: Utilize Fortify SSC (Software Security Center), Audit and Report
- Module 10: Bug Tracking Integration
- Module 11: Utilize Audit Assistant in SSC

## Detailed Course Outline

### Module 1: Fortify Architecture and Application Security Overview

- Identify the Fortify architectural structure and workflow
- Recognize the importance of application security in your Software Development Life Cycle (SDLC)

### Module 2: Fortify SSC Setup

- Recognize the Application version and Administration options
- Create an application version and update SSC Rulepacks
- Integrate Audit Workbench scan results with SSC application versions

### Module 3: Fortify SCA Analyzers Metrics

- Describe the automated scanning process
- Explain the function of each Analyzer
- Recognize how the findings are placed within each risk folder

### Module 4: Fortify Static Scanning

- Define the features and usage of Fortify's scanning options
- Recognize the different IDE plugins that integrate with Fortify SCA Analysis
- Successfully run Fortify scans in several ways, using:
  - Audit Workbench
  - Scan Wizard
  - Command Line
  - Eclipse
  - Visual Studio

### Module 5: Auditing Fortify Scan Results

- Verify your scan results in Audit Workbench
- Identify the findings in the Critical folder
- Utilize Smart View for a visual representation of the dataflow issues in your code
- Recognize findings categories in the Critical folder
- Apply the appropriate validation method to remediate a given vulnerability
- Filter, Audit, and suppress issues to reduce noise
- Find information, i.e. Details and Recommendations, to fix security issues

### Module 6: Data Validation

- Securely implement data validation
- Select the right data validation for a particular situation

- Extend data validation libraries

### Module 7: Analysis Trace and Remediating Vulnerabilities

- Properly read the analysis trace
- Audit vulnerabilities for:
  - SQL Injection
  - XSS
  - Log Forging
  - Cross-Site Request Forgery (CSRF)

### Module 8: Custom Rules

- Recognize how to use data flow cleanse rules to integrate data validation into Fortify
- Create a data validation rule

### Module 9: Utilize Fortify SSC (Software Security Center), Audit and Report

- Effectively navigate the Fortify SSC (Software Security Center)
- Review scan results upload and audit issues using SSC capabilities
- Generate reports to show outstanding issues, progress on security goals and a summary of the vulnerabilities detected during a scan

### Module 10: Bug Tracking Integration

- Utilize Bug tracking tool through the SSC and AWB

### Module 11: Utilize Audit Assistant in SSC

- Recognize the value for utilizing Audit Assistant
- Define the Fortify Scan Analytics tenant Prediction Policies
- Configure your SSC to utilize Audit Assistant
- Submit training data, issues, and review the AA results

# About Fast Lane



Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

## Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

## Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

## Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center



**Worldwide Presence**  
with high-end training centers  
around the globe



**Multiple Awards**  
from vendors such as AWS,  
Microsoft, Cisco, Google, NetApp,  
VMware



**Experienced SMEs**  
with over 19.000 combined  
certifications

### Germany

**Fast Lane Institute for Knowledge  
Transfer GmbH**  
Tel. +49 40 25334610  
info@flane.de / www.flane.de

### Austria

**ITLS GmbH**  
(Partner of Fast Lane)  
Tel. +43 1 6000 8800  
info@itls.at / www.itls.at

### Switzerland

**Fast Lane Institute for Knowledge  
Transfer (Switzerland) AG**  
Tel. +41 44 8325080  
info@flane.ch / www.flane.ch