



COURSE DETAILS

INTENDED AUDIENCE

Software development professionals and their managers; personnel responsible for software or application security, and testing, and those interested in secure software concepts.

LENGTH

Five Days; Days 1-4 (0900-1700)
Day 5 (0900-1500)

COST

\$2499 including course notebook and exercise materials. Refreshments and catered lunch provided.

PREREQUISITES

It is recommended that attendees in this highly-technical course have a background in software development. Basic familiarity with C, C++, and Java would be helpful.

This course may also be offered by arrangement at customer sites. Contact Outbreak Security for further information.

Outbreak Security

7 West Queens Way
Hampton, VA 23669 USA
1.757.265.0891

www.outbreaksecurity.com

ADVANCED SOFTWARE SECURITY

Overview:

Software vulnerability and software exploits are the root cause of a majority of computer security problems. In fact, software is the target of choice for real hackers. The key to proactive computer security thus involves getting a risk management handle on the software security problem. This comprehensive two-day course—designed by the experts who *literally wrote the book on software security*—encompasses software security awareness and best practices through a combination of lecture and hands-on exercises.

Topics Include:

- Common Attacks & Risks
- Safe Design Principles
- Risk Analysis Methodologies
- Seven Types of Coding Errors
- Static Code Analysis
- Security Testing Tools & Techniques
- Software and IT Security Integration
- Toward a Software Security Initiative

Exercises during this class include conducting architectural risk analyses, exploring software abuse case studies, placing architectural risk analysis concepts into practice, conducting a rudimentary software code review using commercial software analyzers, and using assorted security testing tools.



Objectives

This course will help participants learn why software developers, architects and managers need to make software security an integral part of their jobs. understand the state of the art in software security best practices and how they apply to their organization, learn why risk management requires a clear understanding of business context and how to use business-case justification of security design to strike the proper balance between security and business, understand security bugs at the implementation level as well as security flaws at the design level and how to identify and eradicate them throughout the software development lifecycle, and gain a clear understanding of how software can be exploited in order to improve their organization's ability to build solid secure code.

About Outbreak:

Outbreak Security was established in 2007 by four distinguished information security professionals whose operational and executive information security and incident handling experience in the government, military, and private sector dates back to 1988 and the birth of the incident response community. Outbreak's instructors are also Visiting Scientists at the Software Engineering Institute at Carnegie Mellon University and have taught numerous incident handling courses there for the CERT/CC.

Instructor biographies and corporate information may be found at www.outbreaksecurity.com.