



# SECURITY TRAINING

Addressing software security effectively means applying a framework of focused activities throughout the software lifecycle in addition to implementing sundry security features such as encryption or authorization. Such activities allow software professionals to begin building the emergent property of security into software at the start and continue the process throughout the software lifecycle.

When it comes to security education for people involved in the production of software, there are four main areas upon which to concentrate:

- Understanding the breadth of the problem, the common attacks against software, and the effective security practices
- Managing software security from product planning through implementation and deployment
- Engineering software the right way from the ground up with solid implementation, design, and testing techniques
- Assessing applications from the perspective of architecture, code, and the running system

Given the variety of individuals involved in software production and the relatively large number of topics within software security, it is important to keep training centered on the most relevant information for a given role. Cigital provides training for multiple roles that can be mapped to individuals involved in a given software project, each with a specialized and customizable learning track:

- Software developers
- Architects and designers
- Development and project managers
- Business analysts and product managers
- Test and QA engineers and managers
- Security auditors and reviewers

In addition to our instructor-led courses, Cigital has a growing eLearning curriculum hosted on its own learning management system (LMS). SecureTraining eLibrary is a subscription-based online training offering providing on-demand, unlimited access to all hosted eLearning courses. Our portal removes the headaches associated with providing role-based training to large and distributed groups.

*Cigital enables organizations to roll out comprehensive training worldwide through our team of certified instructors, content licensing and customization agreements, and our eLearning portal.*

Digital courses are most often delivered as on-site, **instructor-led sessions**. Based upon a group's learning goals, many organizations choose several courses for assembly into a **multi-day track**.

To help make training more cost-effective, an organization may choose to license a **computer-based eLearning** version of a course. We are building these for all our courses, so please contact us for availability.

Digital offers other courses on **specialized topics** in application security. We also routinely work with customers to build **customized courses** that contain and explain organization-specific information.

## UNDERSTAND

### Foundations of Software Security

This course arms everyone with the basic tenets of software security, including core security concepts, principles of secure design, security activities in the SDLC, a security vulnerability overview, and a risk management process.

#### Learning objectives:

- Understand why software security is an integral part of all software production roles.
- Apply knowledge about implementation-level vulnerabilities as well as design-level flaws to your project.
- Direct future project initiatives based on the principles of “building security in” and the core concepts in software security.

#### Course versions:

- Executive briefing session (2 hours)
- Full course session (1 day or 2 days)
- eLearning module

### Attack & Defense

This course features a deep-dive into the mechanics of common attacks on software along with guidance on mitigation, prevention, and test strategies. Topics include input injection attacks, Web vulnerabilities, and business logic abuse.

#### Learning objectives:

- Apply detailed knowledge about common attacks to augment mitigation and testing strategies.
- Discuss common vulnerabilities in context with others that follow similar patterns.
- Use knowledge about various attacks to better understand and meet regulatory or internal compliance goals.

#### Course versions:

- Web application session (1 day)
- eLearning module

### Threat Modeling

This course features a step-wise approach to determining which threats and attacks are relevant for a given application and environment, and builds understanding of how architecture features help in attack resistance.

#### Learning objectives:

- Know how to enumerate attack vectors threats take advantage of.
- Use threat model data to specify compensating controls for specific attack vectors.
- Understand how the model can drive security testing.

#### Course versions:

- Foundation session (1 day)

## MANAGE

### Software Security Requirements

This course starts with definition of sound software requirements and leads into writing positive security requirements, eliciting requirements, abuse-case modeling, security best practices, and attack patterns.

#### Learning objectives:

- Create and derive actionable and testable security requirements based on an application's core functional requirements.
- Understand the breadth of areas that requirements should cover for security.
- Balance future software features against the associated security risks.

#### Course Versions:

- Foundation session (½ day)

### SOA, Web Services, and XML Security

This course details the fundamental building blocks in SOA and Web services systems through a focused case study. It discusses where standards do not help and shows how to manage security risks.

#### Learning objectives:

- Recognize how Web application risks apply in a Web services world.
- Be able to detect specific Web services and XML attack patterns.
- Recognize how to leverage standards and security protocols to proactively build security in.

#### Course Versions:

- Foundation session (1 day)
- Full course session (2 days)

### Creating Secure Mobile Applications

This course arms students with the knowledge of both the largest mobile threats as well as the principles necessary to combat those threats. It explains the basics of cellular networks, application loading, and secure mobile application design principles.

#### Learning objectives:

- Understand the basics of the cellular network and its salient security issues.
- Describe four types of application loading and associated security costs and benefits.
- Understand six major handset environments and associated development and security issues.
- “Think like an attacker” when conceiving, building, and testing your mobile software.

#### Course versions:

- Foundation session (1 day)

## COURSES

## ENGINEER

## Defensive Programming

These courses teach developers good approaches to writing secure code. To that end, the language-specific prescriptive guidance covers data validation, avoiding denial-of-service, secure error handling and logging paradigms, and engineering common security features.

**Learning objectives:**

- Implement common functional features using known-good techniques that provide built-in security assurance.
- Conduct low-level design such that robustness and resilience are first-class considerations.
- Understand the details and rationale behind properly avoiding common mistakes using defensive programming techniques.

**Course Versions:**

- Java Enterprise Edition session (1 day)
- C# for ASP.NET session (1 day)
- C/C++ session (1 day)
- VB.NET session (1 day)
- eLearning modules

## Risk-based Security Testing Strategy

This course teaches attendees how to create effective security test cases. Specific techniques include adding risk prioritization to test planning, discovering security tests from requirements, and test strategies to prevent common security defects.

**Learning objectives:**

- Map individual test cases back to the security problems they are meant to discover in order to ensure good coverage.
- Prioritize test-case development according to the most likely security problems facing a project.
- Develop a white-box testing strategy to better align testing efforts with real-world security risks.

**Course Versions:**

- Full course session (1 day)
- eLearning module

## Web 2.0 Security

This course examines the changing threat model associated with Web 2.0 technology patterns. Building secure applications based on these patterns requires that application designers understand this threat model in order to account for security in their designs. Ajax Dojo, Adobe Flex, and Microsoft Silverlight are covered.

**Learning objectives:**

- Understand the security ramifications of Web 2.0 design patterns.
- Extend your current threat modeling activities to address new Web 2.0 characteristics.
- Address new risks and help ensure software security.

**Course Versions:**

- Full course session (1 day)

## ASSESS

## Security Code Review

This course focuses on the techniques to audit source code for security vulnerabilities. Topics covered include process for conducting a code review, applying code navigation and static analysis tools, and manual analysis methods extending from tool findings.

**Learning objectives:**

- Lead a code review project to efficiently discover security bugs and implications.
- Map common code review findings back to root causes in previous phases of the SDLC.
- Leverage code scanning tools to get the most benefit and avoid common misconceptions about their coverage.

**Course Versions:**

- Foundation session (½ day)
- Fortify Source Code Analyzer (SCA) add-ons (½-4 days)

## Architecture Risk Analysis

This course highlights methods of finding design-level security flaws in software. Techniques include accurately capturing application architecture, threat modeling with attack trees, attack pattern analysis, and enumeration of trust boundaries.

**Learning objectives:**

- Extract architecture views of a software system suitable for security analysis.
- Apply a number of complementary techniques to find security vulnerabilities that cannot be easily discovered through tools.
- Weigh the comparative impact of design-level security flaws in order to prioritize remediation efforts.

**Course Versions:**

- Web application session (1 day)
- eLearning module

## Web Security Testing

These courses demonstrate basic methods of assessing a running application for security problems. The first focuses on the basics of HTTP and HTML and then presents techniques for conducting security tests and pinpointing likely flaws in business logic. The second focuses on rich internet applications.

**Learning objectives:**

- Demonstrate security risks by breaking security mechanisms and software business logic.
- Leverage application attack tools to get the most benefit and avoid common misconceptions about their coverage.
- Learn how to craft and conduct basic attacks in a hands-on environment.

**Course Versions:**

- Web Security Testing (1 day)
- Testing Rich Internet Applications (½ day)

The **role-based tracks** presented here are general recommendations based upon Cigital's experience with small and large customers across several business verticals.

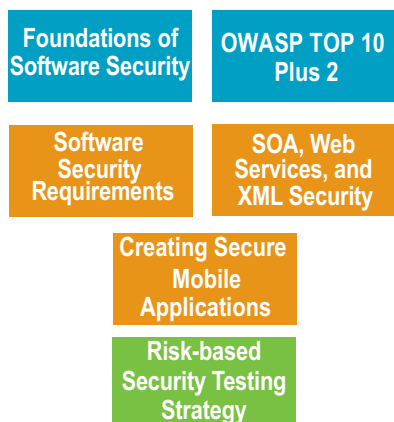
To **jump-start skills improvement for a project team or department**, Cigital recommends choosing 2-5 courses from the role-based tracks for back-to-back delivery. Besides lowering cost, multi-day delivery reinforces and helps attendees retain critical concepts.

Typically, we work with a given organization to customize both order of and delivery method for knowledge transfer as well as long-term strategy to most **efficiently improve your organization's software security maturity level**.



## DEVELOPERS

Focusing on people that actually write the code comprising a software project, the developer's track starts with basic awareness. Since developers focus on software at the code level, priority is given to the courses that teach prescriptive guidance on implementation, expand the breadth of a developer's knowledge about common attacks, and demonstrate the techniques of assessing code in an ongoing project. For more advanced practitioners, expanding towards proactive design guidance and design assessment techniques is also highly recommended.



## ANALYSTS

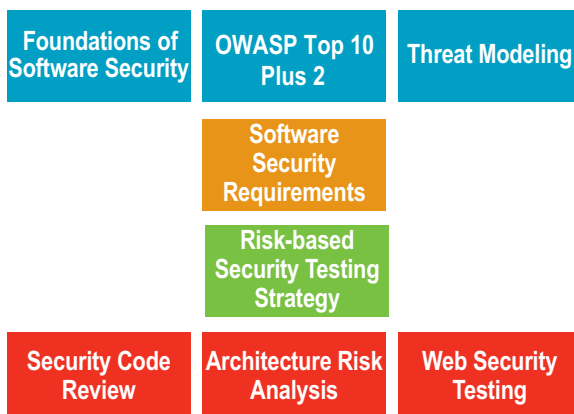
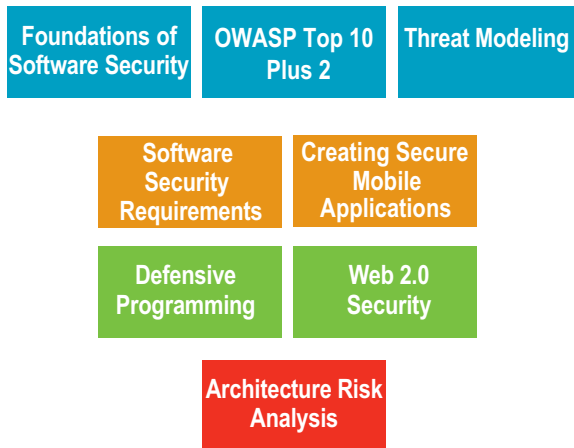
For the people that manage the direction of a product either directly or through the requirements process, the analyst's track begins with basic awareness. From there, knowledge around specifically managing requirements and features in a security-conscious way is imparted before branching out to the breadth of common attacks and defenses. For more advanced practitioners, extending skills toward general application security management across a project and testing strategy is also highly recommended.



## TESTERS

Directed toward people that plan quality assurance and testing activities for a project, the tester's track starts with basic awareness. Because the test planner's role is critical in ensuring security problems are prevented over time, focus is given to the proactive techniques for designing test-cases with security in mind. As with other roles, it is also important to ensure that knowledge about common security problems is well understood. For more advanced practitioners, building skills in top-down security requirements and penetration techniques is also highly recommended.

# TRACKS



## ARCHITECTS

For people responsible for specification of high-level design and software architecture, the architect's track begins with basic awareness. From there, proactive and prescriptive design guidance is prioritized in order to enable the design phase to produce more robust applications by default. After that, focus is given to expanding knowledge about common attacks and defenses as well as assessing the design of ongoing software projects. For more advanced practitioners, building skills in the areas of secure implementation and product-level security requirements is also highly recommended.

## MANAGERS

Directed toward people responsible for execution of activities across many phases of the SDLC, the manager's track starts with basic awareness. Since many activities are being managed at a high level, priority is given to teaching sound management techniques for building and following a long-term project security roadmap. Since responsibility is often shared between execution and direction, the next steps are to ensure solid understanding of security requirements and feature trade-offs. For more advanced practitioners, expanding the breadth of knowledge about common attacks as well as big-picture testing strategies for security is also highly recommended.

## AUDITORS

Focusing on people charged with conducting security reviews and jumping into projects in order to perform extra security checks, the auditor's track begins with basic awareness. Since typical job responsibilities revolve around assessment, priority is given to ensuring a solid understanding of attacks and defenses as well as techniques to assess running software systems and the code that comprises them. For more advanced practitioners, expanding assessment skills to the architecture and requirements level is also highly recommended.

Cigital has **extensive experience delivering comprehensive solutions** to companies in a variety of verticals.

For a **custom plan to address your organization's educational goals**, or to address other drivers, please contact us for a consultation.



## INSTRUCTOR-LED

Traditional classroom delivery of Cigital courses is the most effective way to deliver intensive skills improvement to a group of software professionals. After passing trainer certification, Cigital instructors are available to deliver on-site training world-wide.

### Key points:

- Take-away printed materials for each attendee
- Interactive instructors using projectors and whiteboards
- Classroom discussions encouraging questions and answers
- Group and/or individual exercises coaxing critical thinking
- Typical class size is 20, although other sizes can be accommodated



## CONTENT LICENSE

Our SecureTraining eLibrary portal is available as an annual license and contains our growing eLearning curriculum. We also offer organizations the opportunity to license the content for internal delivery. This allows larger organizations to cost-effectively deploy training to widespread developers using their existing learning management systems.

### Key points:

- All eLearning modules available in the Cigital portal
- Licensing fees based on target audience size
- Instructor-led courses include student handbooks, instructor handbook, and lab exercises
- Computer-based courses include deployment-ready content with voice-over and graphics



## CUSTOMIZATION

For customers who purchase either instructor-led delivery or content licensing, Cigital offers customization services to augment the course content with organization-specific details. Ranging from a simple logo addition to extensive details about internal policies, customized content improves retention and relevance.

### Key points:

- Customization performed by consulting services on top of delivery or licensing
- Augment lecture examples and exercises with customer-specific architecture/code
- Tailor discussions to specific internal technologies or resources
- Pinpoint relevant internal policies, standards, or guidelines as they occur in the course

# DELIVERY

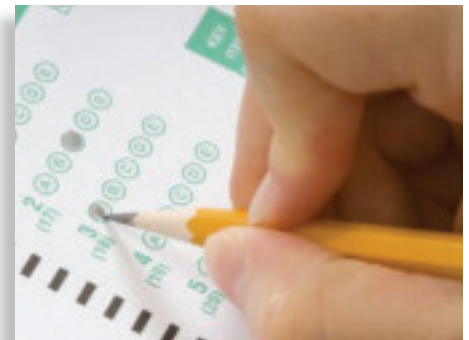
## DROP-IN TRAINING SOLUTION

Founded in experience working with dedicated training groups, Cigital makes it easy for organizations to adopt a comprehensive software security training curriculum with very little effort. Using the role-based learning tracks as a guide, centralized training groups can schedule and track individual progress without needing to build it all from the ground up.



## CERTIFICATION PROGRAMS

Cigital can quickly create a proficiency maturity program for any organization. For each course in the curriculum, Cigital can offer lightweight quizzes as well as more comprehensive certification exams. Following the progression of courses for each education track, the certification exams can be used to checkpoint professional development for employees, including use of advanced placement tests for more experienced staff.



## REGULATORY COMPLIANCE

To help with the increase in the number of regulations and standards with which an organization must comply, Cigital's curriculum covers the critical topics that employees must understand. Since the specific details of each regulation can differ significantly, please contact us for a solution to fit your needs.





**CONTACT US**

**PHONE** 800-824-0022

**EMAIL** [training@cigital.com](mailto:training@cigital.com)

**WEB** [www.cigital.com](http://www.cigital.com)

**Cigital, Inc**  
**21351 Ridgetop Circle**  
**Suite 400**  
**Dulles, VA 20166**