The Synopsys difference

Synopsys offers the most comprehensive solution for building integrity—security and quality—into your SDLC and supply chain. We’ve united leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in application security testing, is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. We don’t stop when the test is over. We offer onboarding and deployment assistance, targeted remediation guidance, and a variety of training solutions that empower you to optimize your investment. Whether you’re just starting your journey or well on your way, our platform will help ensure the integrity of the applications that power your business.

For more information go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com
Introduction

Our Curriculum

Introductory
  *Attack and Defense*
  *OWASP Top 10*
  *Principles of Software Security*

Defending
  *Defending*
  *Defending Android*
  *Defending C#*
  *Defending C and C++*
  *Defending HTML5*
  *Defending Java*
  *Defending JavaScript*
  *Defending IOS*
  *Defending PHP*
  *Defending Python and Django*

Securing
  *Securing Web Services*

Attacking
  *Attacking Web Applications*

Workshops
  *AWS DevOps*
  *Mobile Security*
  *Red Teaming*
  *Threat Modeling*
INTRODUCTION

Synopsys’s instructor-led courses are developed and taught by experts at the forefront of the software security field. Our instructors are certified security professionals who have hands-on experience working directly with clients on their security challenges.

Our curriculum includes training modules for professionals just starting out with software security as well as those who are looking to develop more advanced skills. Synopsys continuously develops its courses to accommodate the rapid changes in software security.

OUR CURRICULUM

Synopsys’s curriculum is a series of complementary courses designed to meet your organization’s needs.

You can select the courses that best match your level of experience, your role, and the development platforms in your organization. Our courses are grouped into the following software security activities:

1. **Introductory** – New to software security? Consider our Principles of Software Security or Attack and Defense course.

2. **Defending** – Learn defensive programming skills in context, in specific languages targeted to specific development platforms, so you can defend against attacks in your code.

3. **Securing** – Learn how to identify common vulnerabilities and essential strategies to secure your deployment and tech stack from external threats.

4. **Attacking** – Use your knowledge to test your applications for security vulnerabilities.


*We can work with you to select a curriculum that is right for your organization.*
In-Person or Virtual — Your Choice

If you choose traditional instructor-led training, our certified instructors will travel to the location of your choice. Our instructors are trained to engage your audience through group discussion and interactive hands-on labs designed to simulate real-world environments. On-site instructors can make course adjustments to better complement the needs, interests, and experience-level of your participants.

If you have a distributed workforce, your participants can avoid travel and time away from the office using our Virtual Instructor-led Training (VILT). VILT is separated into shorter sessions to optimize participant engagement. VILT can be delivered over consecutive working days or on a weekly basis, depending on your team’s preference. Virtual training is a cost-conscious alternative for supporting your employees’ professional development.

Synopsys utilizes a number of training strategies to assist in participant engagement, including hands-on labs using our cloud-based VM solution, breakout groups, live demonstrations, white boarding, videos, polling, and real-time assessments.

Instructor-led courses are held on your schedule in the format that works best for you.
Description

*Building security in* is about building software right the first time, and this course teaches students to do just that. Organized around a few major themes (e.g., data at rest, data in motion, input validation, output encoding), this course teaches some common use cases we want to support, and how to design and implement them securely. This course is not tied to any particular language or domain. Different use cases come from different contexts (e.g., web, embedded, thick client, mobile). Each is presented with its standard attacks and the standard solutions that defend against those attacks. Rather than follow industry-standard security taxonomies that categorize mistakes, this course is organized around common software user stories, and how to do them securely. Topics include proper use of encryption, and handling of data across module boundaries, validation and encoding, and authentication and authorization issues.

At the end of this course, students will have the foundational knowledge to expand their software security and learn specific engineering techniques such as defensive programming, threat modeling, and penetration testing.

### Intended Audience

- Developer
- Architect
- QA and Testing
- IS Security Team

### Delivery Format

- Traditional Classroom
- Virtual Classroom

### Class Duration

- 8 hours
Description

This course focuses on the most important security defects found in web applications, covering all issues in the latest Open Web Application Security Project (OWASP) Top 10. Each topic describes a vulnerability and provides practical guidance for remediation. This course also demonstrates some of these vulnerabilities and provides hands-on exercises where students learn the impact of these security issues can have on web applications. Developers with experience in any programming language can benefit from this course.

Intended Audience

» Developer
» Architect
» QA and Testing
» IS Security Team

Delivery Format

» Traditional Classroom
» Virtual Classroom

Class Duration

» 8 hours
The key to proactive computer security involves getting a risk management handle on the software security problem. This half-day course, created by the experts who literally wrote the book on software security, encompasses software security awareness and best practices for a general audience. Everyone involved in software production requires baseline knowledge of software security problems and risks, along with an overall understanding of approaches for producing better software.

The virtual classroom course is available with two flavors to choose from:

- **Vanilla** explains common problems in software security and describes an approach to infusing software security into the development process through risk management, software security touchpoints, and historical knowledge of software security vulnerabilities.
- **Requirements** focuses on introducing important cost-saving software security requirements early in the software development life cycle.

### Intended Audience
- Developer
- QA and Testing
- IS Security Team

### Delivery Format
- Virtual Classroom

### Class Duration
- 4 hours
Description

Our Defending course series provides a comprehensive overview of the security issues and common pitfalls affecting applications developed in the specific language or platform. Each course concentrates on areas related to defensive programming techniques and includes code analysis and remediation exercises. The course is also supported by several interactive demonstrations and hands-on lab exercises.

- Defending Android
- Defending C# available in ASP.NET or Desktop emphasis
- Defending C and C++ available also in a two-day option
- Defending HTML5
- Defending Java available in EE or SE emphasis
- Defending JavaScript available in React or Angular emphasis
- Defending iOS available in Objective C or SWIFT emphasis
- Defending PHP
- Defending Python with Django

Intended Audience

» Developer

Delivery Format

» Traditional Classroom
» Virtual Classroom

Class Duration

» 8 hours
Description

The Securing Web Services course is intended for developers, engineers, and architects who work with backend web services APIs which may not necessarily have a User Interface (UI) or a UI component.

This course examines web services concepts and then takes a deep dive into several web services technologies such as WS-Security, Security Assertion Markup Language (SAML), and OAuth. This course also covers risks inherent to web services and how to properly threat model web services. Web service security is examined from the perspective of the message, the channel, and the service itself.

The lab component of this course allows students to gain an understanding of and practice with some of the real-world security issues inherent to web services. The lab is intentionally written with a programming language and framework that are popular but with which most developers are not familiar: Python and Flask. This allows students to focus on secure design and secure coding concepts without being too concerned with the implementation details of a particular language.

Intended Audience

- Developer
- Architect
- QA and Testing

Delivery Format

- Traditional Classroom
- Virtual Classroom

Class Duration

- 8 hours
Web applications are ubiquitous and plentiful. In fact, the web is the *de facto* delivery mechanism for both consumer-grade and business-critical functionality these days. As such, the web is also the most common target for application-level attacks.

This hands-on one-day course describes the goals, processes and risks with attacking web applications. It introduces students to the basics of web application architecture and web security testing including the OWASP Top 10 vulnerabilities. A portion of the course is dedicated to lab exercises where students are provided the opportunity to test for the most commonly occurring web based vulnerabilities.

The course also discusses other aspects of security testing including risk rating of findings, communicating findings to different groups and creating test plans.

### Intended Audience
- Developer
- QA and Testing
- IS Security Team

### Delivery Format
- Traditional Classroom
- Virtual Classroom

### Class Duration
- 8 hours
Cloud computing has grabbed the world’s attention not only for its pervasive, on-demand, convenient usage, but for its ability to be vulnerable to data breaches and novel forms of attack. Since most software uses the cloud in various shared capacities (development, hosting, or integration with third-party code), threats from hackers are inevitable. This hands-on workshop equips students to understand this new landscape of converged infrastructure and shared services, its existing and emerging threats, and provides them with secure mitigation methods.

The AWS DevOps Workshop course is a deep dive into cross-discipline information and perspective among developers, operations, and information security personnel. The course enables students to identify areas for cross-pollination between development and operations that enhance application, infrastructure, and network security.

This course assumes the following baseline student knowledge:

- Conceptual familiarity with:
  - Common AWS services: EC2, VPC, RDS, KMS, and IAM
  - Docker
  - Chef, or another infrastructure-as-code tool such as Puppet, SaltStack, or Ansible
- Operational familiarity with:
  - Linux CLI environment

Intended Audience

- Developer
- Architect
- QA and Testing
- IS Security Team

Delivery Format

- Traditional Classroom
- Virtual Classroom

Class Duration

- 8 hours
Mobile Security

**Description**

This modular course can be delivered as a one-day or two-day training.

The following topics are available:

**Mobile First AppSec:** Mobile First AppSec (application security) describes what application security teams must consider when testing mobile applications.

**Overview of Mobile Platforms:** This module provides an overview of the architecture and security controls in today’s two most popular mobile operating systems: Google’s Android and Apple’s iOS.

**Protecting Client-side Code:** Attackers target mobile applications for many reasons. This module presents the techniques and tools for making reverse engineering and tampering with mobile applications more difficult, as well as the limitations of these techniques.

**Mobile Payments:** This module explores the attack surfaces of mobile payment architectures, including NFC-based (Near Field Communication) wallets. It examines the design of the mobile payment clients and the back-end applications, reviews the known attacks against these systems, and explores countermeasures against these attacks.

**Intended Audience**

» Architect

**Delivery Format**

» Traditional Classroom
» Virtual Classroom

**Class Duration**

» 8 hours
» 16 hours (2 days)
Red Teaming

Description

Organizations are continually faced with growing and evolving threats against their digital assets and infrastructure. Red Teaming is a goal-based assessment approach which allows organizations to gain insight into how their security posture is when faced with a real threat. This hands-on course introduces students to the concepts of Red Teaming and how it is different than traditional vulnerability testing. The course will also include guidance for the organization on creating and maintaining their own internal Red Teams. Lastly, students in this course will be introduced to the physical, social, and electronic testing methods which can be utilized during Red Team engagements.

Available in one-day or two-day options:

• The 1-day course can be customized to focus solely on the business aspects of the program, the technical aspects of testing, or a mix of both within the allotted time.
• The 2-day course is intended for practitioners and managers who are looking to begin a red teaming program within their company.

Intended Audience

» Management
» IS Security Team

Delivery Format

» Traditional Classroom

Class Duration

» 8 hours
» 16 hours (2 days)
Penetration testing and secure code review can uncover many types of security issues in an application; however, there are defects that simply cannot be found with these traditional analysis techniques. Discovering weaknesses in the design of a system is the specific goal of threat modeling. Organizations benefit from this software design analysis because you can perform it without code to discover potential vulnerabilities early in the development cycle.

This course details Synopsys’ threat modeling process and methodologies to teach students how to identify the assets, security controls, and threat agents for a given system. The course goes on to show how this information can be used to create a list of attacks and propose appropriate mitigations. The course focuses on system threat models used to build a holistic view of the security posture of a system based on the application and its associated infrastructure. The course is also supported by multiple hands-on lab exercises that allow students to learn by actually going through the threat model process.

**Intended Audience**

- Developer
- Architect
- QA and Testing
- IS Security Team

**Delivery Format**

- Traditional Classroom
- Virtual Classroom

**Class Duration**

- 8 hours