WhiteHat eLearning
Computer-Based Training

Enable and Educate Your Team

Companies are at risk for breaches from common, easily-preventable attacks because Engineers, Developers, and Security teams do not understand application security concepts. Applications rushed through development lack basic security specifications; managers have little to no visibility into how their team members are engaged or if they understand training materials provided; the right training is not available to everyone who needs it; and custom training programs don't scale to a large number of users.

WhiteHat Security eLearning Platform can help you meet regulatory requirements for training via an interactive, role-based program that quickly brings everyone up to speed. Developers, managers, architects and testers, and even network security professionals must be aware of the many different types of application attacks, in order to defend your organization's web applications.

eLearning will educate your team through self-paced training on application threat modeling, best coding practices, mitigation, and defensive remediation, all in an easy-to-learn, web-based environment. The information learned from these modules can be used to produce guidelines for consistent secure programming practices throughout your organization. Organizations can track who is on target with training, and which employees require more focus. The role-based eLearning tracks within WhiteHat's computer-based training platform allow administrators to quickly and easily assign relevant materials wherever needed.

Accessible anytime, from anywhere

Our computer-based training platform can be internally or externally hosted. The SCORM compliant library can be hosted in your internal LMS or externally in our 24/7 cloud-based hosting environment. Your team will learn the latest risk mitigation and remediation techniques at your own pace with unlimited access for each participant.

Continuing Professional Education (CPE) credit

WhiteHat offers one-to-one mapping between hours spent on CBT courses and CPE credits. Your team will expand their body of knowledge in Application Security, PCI, Building Secure Applications, OWASP Top Ten, and Defensive Remediation.

Meets PCI requirements

Our CBT offering meets the PCI-DSS 6.5 and 12.6 requirement by training developers in secure coding techniques and preparing your team in cardholder data security.

Role-Based eLearning Paths

The role-specific training makes it easy to assign the appropriate classes for each team member, thereby improving employee retention of key concepts. Learning tracks are available within the eLearning portal for the following micro-degree specializations:

- **Application Security for Security Professionals** provides an overview of the basic risk categories of the OWASP Top 10, as well as guidelines on implementing AppSec for the SDLC.
- **Application Security for Developers** provides a deeper dive into how to identify and remediate the OWASP Top 10 risk categories, as well as threat modeling and defensive enterprise remediation.
- **Application Security Training specific to the Java Developer** provides deeper Java-specific security training, including the OWASP Top 10 risk categories as well as a deeper dive on Java Enterprise Edition and secure Java programming for mobile apps.
- **General Security Education** provides training for the entire enterprise; from the basics of physical and personal security through safeguarding data and your organization's virtual assets.

Course Descriptions

COURSE	DURATION	DESCRIPTION
OWASP Top 10 2017 for Developers	3 hours	Participants of this course will gain a foundational understanding of application security and secure programming practices based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Top Ten document.
OWASP Top 10 2017 for Managers	45 mins	Participants of this course will gain a foundational understanding of application security based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Top Ten document.
OWASP Top 10 2013-2017 Delta for Developers	1 hour	Participants of this course will gain a foundational understanding of application security and secure programming practices based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Top Ten 2017 document; for students who have already completed the OWASP Top Ten 2013 for Developers module.
OWASP Mobile Top 10 for Developers	3 hours	Participants of this course will gain a foundational understanding of mobile application security and secure programming practices based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Mobile Top Ten document.
OWASP Mobile Top 10 for Managers	45 mins	Participants of this course will gain a foundational understanding of mobile application security based on the threats and vulnerabilities outlined in the Open Web Application Security Project's Mobile Top Ten document.
Defensive Enterprise Remediation	1 hour	Participants of this course will gain a foundational understanding of mitigating specific classes of vulnerability with emphasis on the Java and C# programming languages.
Threat Modeling	1 hour	Participants of this course will gain an understanding of the threat modeling process and how it is used to identify and prioritize threats.
Building Secure ASP.NET Applications	1 hour	Participants of this course will gain a foundational understanding of writing secure software on ASP.NET based platforms.
Building Secure Mobile Applications	1 hour	Participants of this course will gain a foundational understanding of how to build secure mobile applications targeting the iOS and Android platforms.
Building Secure Java EE Applications	1 hour	Participants of this course will gain a foundational understanding of writing secure software on Java Enterprise Edition based platforms.
Building Secure JavaScript Applications	1 hour	Participants of this course will gain a foundational understanding of writing secure software using JavaScript for both the client and the server.
Building Secure Python Applications	1 hour	Participants of this course will gain a foundational understanding of writing secure software on Python based platforms.
Integrating Security Throughout the SDLC	1 hour	Participants will understand the most important and essential security activities which can be conducted throughout the SDLC to reduce security issues.
General Security Awareness	1 hour	Participants of this course will gain a foundational understanding of corporate security from physical access to logical controls and online safety.

Learn more about WhiteHat's application security products and solutions at whitehatsec.com/products.

WHITEHAT SECURITY, INC. 1741 Technology Dr. #300, San Jose, CA 95110 • 1.408.343.8300 • www.whitehatsec.com