Enable and Educate Your Team

Year after year, organizations from start-ups to enterprise corporations face devastating breaches. Applications are rushed through development and lack basic security specifications. Security results fall to team members that lack the knowledge on how to remediate vulnerabilities findings quickly. The right training is not available to everyone who needs it. Luckily the NTT Application Security Platform provides the solution for mitigating these challenges throughout the DevSecOps process. NTT Application Security not only provides vulnerability findings but offers the comprehensive security education that your company needs.

NTT Application Security eLearning provides an interactive, role-based program that quickly brings everyone up to speed. Developers, managers, architects, testers, network security professionals, and even your business team must be aware of the risks and how to defend your organization's applications. NTT Application Security eLearning educates your team on secure programming patterns, processes, and tooling, all in an easy-to-use, self-paced accessible platform. Organizations can track who is on target with training and which employees require more focus.

NTT Application Security eLearning provides the security training needed to accelerate defense and remediation of your applications.

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

NTT Application Security 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

NTT Application Security's eLearning platform provides the necessary ingredients to develop and deploy a tailored Application Security Training Program. Covering a wide range of application security topics, you will have the ability to define role-based eLearning course curricula unique to the roles and responsibilities of key stakeholders within your product development teams. By implementing education across all your technical stakeholders during every stage of the secure development lifecycle, your teams will become more efficient at designing, implementing and verifying secure software.

	STAGE 1	STAGE 2	STAGE 3
Business Team	• OTTF • OWASP Top Ten • Foundations Exam	• Integrating Security Throughout the SDLC	
Secure Manager	• OTT4M • Foundational Exam for Managers	• Integrating Security Throughout the SDLC	
Secure Developer	• OTT4D • Foundational Exam For Developers • Integrating Security Throughout the SDLC	• Building Secure Applications Series • OWASP API Security Top Ten	• Building Secure Application Series • Docker and App Container Security
Secure Architect	• OTT4D • Foundational Exam For Developers • Integrating Security Throughout the SDLC	• Building Secure Applications Series • OWASP API Security Top Ten	• Building Secure Application Series • Docker and App Container Security • Threat Modeling
Secure Tester	• OTT4D • Foundational Exam For Developers • Integrating Security Throughout the SDLC	• Building Secure Applications Series	• Threat Modeling • Building Secure Application Series

Course Catalog

OWASP Top Ten Series

Welcome to the OWASP Top Ten Series. This Series of Courses provides participants with education regarding common security vulnerabilities facing web and mobile applications today as defined by the OWASP Top Ten Taxonomies. Courses are organized based on a role and technical level to provide a tailored experience for the entire software team at all stages of development.

COURSE	COURSE DESCRIPTION	DURATION
NEW **OWASP Top Ten Foundations Course** *(w/ optional OWASP Top Ten Foundational Exam)*	This course focuses on the most common security vulnerabilities and attack vectors facing applications today as defined by the OWASP Top Ten Project. Participants will explore the OWASP Top Ten at a high level by analyzing real-world examples and rich visualizations. Upon completion of the course, the participant will possess knowledge of the risks inherent in web applications.	1 hour
UPDATED **OWASP Top Ten for Managers** *(w/ optional OWASP Top Ten Foundational Exam)*	This course focuses on the most common security vulnerabilities and attack vectors facing applications today as defined by the OWASP Top Ten Project. Participants will explore the OWASP Top Ten at a high level by analyzing real-world examples and rich visualizations, with specific guidance geared toward product and project management. Upon completion of the course, participates will possess knowledge of the risks inherent in web applications.	1 hour
UPDATED **OWASP Top Ten for Developers** *(w/ optional OWASP Top Ten Foundational Exam)*	This series of eLearning modules focuses on the most common security vulnerabilities and attack vectors facing application developers today as defined by the OWASP Top Ten Project. Participants of these modules will explore the OWASP Top Ten through a detailed analysis of real-world examples, rich visualizations of attacks, as well as comprehensive discussions of mitigation strategies with supporting code examples. After completing these modules, participants will be able to more readily identify, mitigate, and prevent common security vulnerabilities within their applications.	3 hours
OWASP Mobile Top Ten for Developers	This course focuses on the most common security vulnerabilities and attack vectors facing mobile application developers today as defined by the OWASP Top Ten Mobile Project. Participants will explore the OWASP Mobile Top Ten through an analysis of real-world examples, rich visualizations of attacks, and discussions of mitigation strategies with supporting code examples. After completing this course, participants will be able to more readily identify, mitigate, and prevent common security vulnerabilities within their mobile applications.	3 hours
OWASP Mobile Top Ten for Managers	This course is designed to enable managers of mobile application development teams to enhance their understanding of the threats against mobile applications and their corresponding security controls.	1 hour
NEW **OWASP API Security Top Ten**	The OWASP API Security Top Ten course helps define and categorize those specific risks to the design, implementation, and deployment of APIs. This course will provide you with an understanding of these risks and how they can be mitigated by using secure programming practices. Participants will explore the OWASP API Security Top Ten by assessing real-world examples, rich visualizations of attacks, and thorough conversations of mitigation approaches with supporting code examples. After completing this course, participants will be able to more readily identify, mitigate, and prevent common security vulnerabilities within APIs.	1 hour

Course Catalog

Building Secure Applications Series

Welcome to the Building Secure Application Series. This series of courses provides a thorough language-specific assessment of common vulnerabilities facing applications today. This series assumes participants have experience in building applications with the specified language and are familiar with the OWASP Top Ten vulnerabilities. We recommend participants complete the OWASP Top Ten for Developers Course before beginning any of the Building Secure Applications courses for completeness.

COURSE	COURSE DESCRIPTION	DURATION
UPDATED **Building Secure .NET Applications**	This course will provide participants with the secure programming practices necessary to build secure .NET applications resilient to frequent attacks, including but not limited to directory traversal, cross-site scripting, and Injection. Finally, we will discuss several key .NET security controls that can be used to mitigate some of the most prevalent attacks facing applications today.	1 hour
UPDATED **Building Secure Java Applications**	This course will provide participants with the secure programming practices necessary to build secure Java applications resilient to common attacks. This course will examine several essential Java security controls that can be used to diminish some of the most prevalent attacks facing applications today.	1 hour
UPDATED **Building Secure JavaScript Applications**	This course will provide participants with the secure programming practices necessary to build secure client-side and server-side JavaScript applications resilient to conventional attacks. This course will examine several crucial JavaScript security controls that can be used to mitigate some of the most prevalent attacks facing applications today.	1 hour
Building Secure Python Applications	This course will provide participants with the secure programming practices necessary to build Python applications resilient to widespread attacks. This course will examine many major Python security controls that can be used to mitigate some of the most prevalent attacks facing applications today.	1 hour
Building Secure Ruby Applications	This course will provide developers with the secure programming practices necessary to build Ruby and Ruby on Rails applications resistant to common attacks. This course will examine several Ruby security controls that can be implemented to mitigate some of the most prevalent attacks facing applications today.	1 hour
UPDATED **Building Secure Mobile Applications**	This course will provide participants with the secure programming practices necessary to build secure mobile applications. Finally, we will summarize numerous key mobile security controls that can be used to avert some of the most prevalent attacks facing applications today.	1 hours
NEW **Building Secure C/C++ Applications**	This course will provide you with the secure programming practices necessary to build secure applications resilient to vulnerabilities commonly introduced using C/C++.	30 minutes

Course Catalog

Operations Series

This series of courses provide specific guidance into operational topics to support software development teams in creating safe and secure applications. Each of these courses covers a stand-alone security process with specified guidance. To better understand security risks and secure development practices, it is recommended that participants watch the appropriate OWASP Top Ten Courses.

COURSE	COURSE DESCRIPTION	DURATION
UPDATED **Integrating Security Throughout the SDLC**	The Integrating Security throughout the Software Development Life Cycle (SDLC) course raises awareness of the critical security activities necessary to build secure software for any and all product team members, providing resources to help formalize a secure SDLC and guidance on auditing existing activities to find gaps in your existing program.	1 hour
NEW **Deriving Security Requirements within the SDLC Planning Phase**	Welcome to the Deriving Security Requirements within the SDLC Planning Phase course. Deriving security requirements from business requirements is an essential step in improving the security of the software delivered by your team. This course will review the concept of a security requirements practice and a security requirements framework and explore an example of how a product team may work through the creation of security requirements applicable to their business needs.	20 minutes
Threat Modeling	This course will provide participants with a foundational understanding of the identification, classification, and rating of threats that face our application architectures. In addition, participants will gain exposure to capturing threat modeling diagrams using Microsoft's Threat Modeling Tool.	1 hour
NEW **Docker and Application Container Security**	This course is designed to introduce the fundamental security activities that can be performed to help improve the security of Docker containers and their running applications.	30 minutes

Security Awareness Series

This series of courses provide general guidance into common workplace security risks pertaining to a company's digital assets

COURSE	COURSE DESCRIPTION	DURATION
General Security Awareness	This course will provide participants with the tools necessary to recognize common workplace security risks, including but not limited to network sniffing, social engineering, phishing, and data theft. Also, we will summarize several key security controls that can be used to mitigate some of the most prevalent attacks found in the modern workplace.	1 hour
NEW **Security Considerations for Extended Telework**	This course provides further security awareness training specific to safeguarding your organization's assets while working remotely from home or in public locations.	15 minutes
NEW **Privacy Series**	We will provide an introduction to the GDPR document; we will walk through the fundamental concepts and core principles underlining the GDPR. Specifically, we will be going through the segments of the document most relevant to businesses and organizations.	30 minutes

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

NTT Application Security