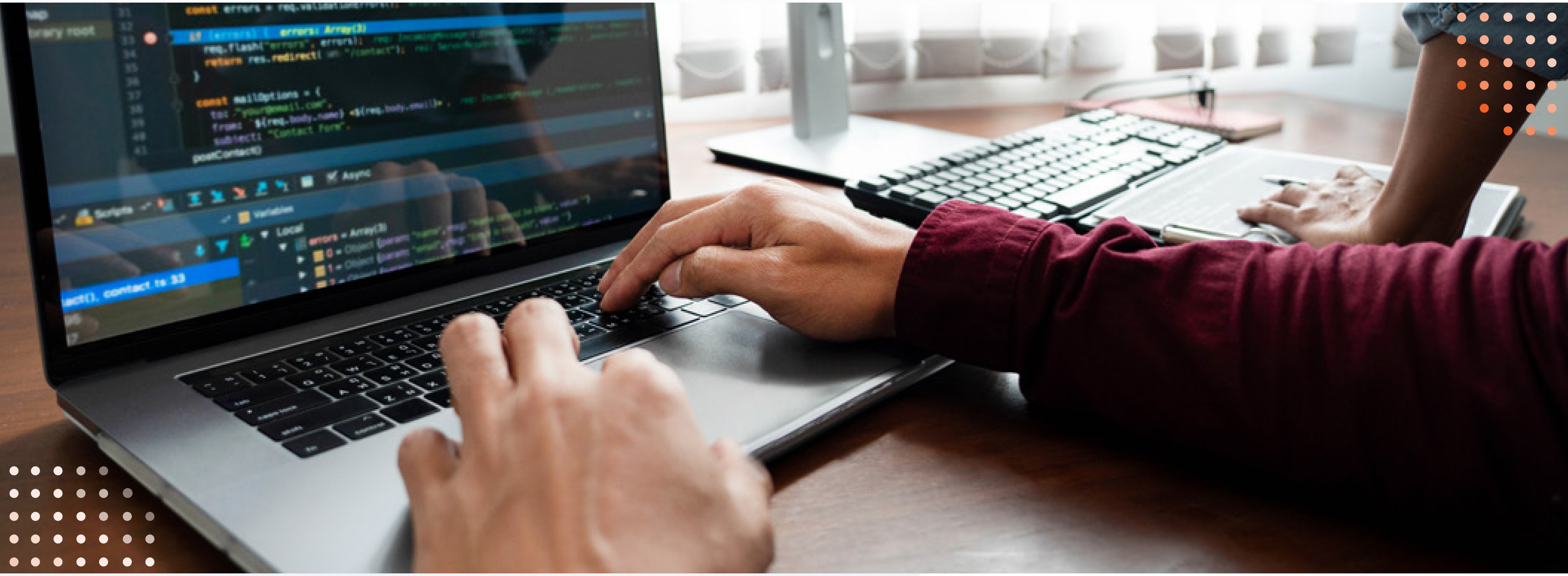
Security Compass

Training Curriculum



2022 Q2

Index

Why Security Compass?

Our software security training program meets the needs of today's modern organizations with adaptive courseware tailored to meet each student's learning goals. Our training courseware helps you meet compliance requirements and raise security standards across your organization.

SECURITY EXPERTISE

Security Compass is an expert in cybersecurity, offering not only training solutions but also professional services and SD Elements, a Balanced Development Automation platform that automates key portions of your proactive security processes such as threat modeling and generation of secure coding standards, and infuses secure development and deployment guidelines into your DevOps workflows.

INDUSTRY-RECOGNIZED CERTIFICATION

Our Software Security Practitioner (SSP) Suite is a unique program jointly developed and offered in partnership with the International Information System Security Certification Consortium (ISC)^2. This program offers role-based training paths that allow learners to earn an (ISC)^2 certificate and share their achievement with their network through a social media badge.

HANDS-ON LEARNING

Our new Virtual Lab complements our Enterprise Training solutions. It allows developers to deepen their understanding of common web application security risks in a safe environment so that they can defend against these risks more effectively.

FLEXIBILITY AND APPEAL

Already knowledgeable on a subject? Go ahead and jump right to the quiz. Need more time to digest new information? No problem - playback all or selected modules. Start and stop as you go. Our eLearning solution is adaptable, engaging and available in bite-sized units (approximately 10 minutes) to make learning easy and interesting.

UP-TO-DATE CONTENT

We add new and refresh existing courses consistently, as new threats emerge. We want to ensure your development teams are armed with the latest understanding of how to defend against threats.

Choose the Right Course Configuration and Deployment Option For Your Business

FULL LIBRARY

Give your team access to over 40 eLearning courses covering application security throughout the software lifecycle, operation security, compliance, and general security awareness.

With full access to our library, learners can take courses required for their roles as well as other courses of interest to complement their security knowledge.

ROLE-BASED TRAINING

Just tell us how many software engineering team members need training and let them choose the SSP Suite that's right for them. This option offers role-based training that's specially designed to meet the varying needs of software engineers across large teams. Students can use their SSP Suites training to obtain industry-recognized (ISC)² certificates.

HANDS-ON LEARNING

Upskill your developers to defend against common web application security risks through experiential learning in a safe environment.

Learn how to discover, exploit, and prevent the OWASP Top 10 vulnerabilities in our Virtual Lab.

DEPLOYMENT OPTIONS

We offer Software as a Service (SaaS) Learning Management System or you can import our eLearning modules into your own Learning Management System.

Just-in-Time Training in SD Elements

Integrate contextual training within your SDLC toolchain and as part of your developer workflow. We offer Just-in-Time training, an integral and exclusive part of SD Elements, focused on the relevant vulnerabilities or secure development techniques for your specific technology stack.

When developers get relevant just-in-time training while writing code, it ensures maximum retention — because they can implement their security knowledge right away.

What is SD Elements?

SD Elements is a balanced development automation platform that helps enterprises reduce software time to market while improving product security and compliance proactively. It automates key portions of your proactive security processes such as threat modeling, risk assessment, and generation of secure coding standards, and infuses secure development and deployment guidelines into your DevOps workflows.

What developer training topics are offered "Just-in-Time" in SD Elements?

Continuous Compliance
CCPA for Software Development
Cloud Security Fundamentals
Defending .NET Framework
Defending .NET 5
Defending Android
Defending C
Defending Databases
Defending Django
Defending HTML5
Defending React
Defending Angular
Defending Ruby

Defending iOS
Defending JSP
Defending Java
Mobile Security Fundamentals
Defending Node.js
Defending PHP 2022
Defending Python
Defending Web APIs
Defending Web Apps
Defending Containers
Defending Kubernetes
Defending Docker
Defending Azure
Defending AWS

HIPAA Privacy and Security
GDPR for Developers
Microservices
OpSec Fundamentals
OWASP Top 10 2021
PCI-DSS Compliance
PCI Secure Software Lifecycle
OAuth Security Fundamentals

600+ micromodules

Application Security

FUNDAMENTALS

- **APP101** - AppSec Fundamentals
- **SEC101** - OWASP Top 10 UPDATED
- **SEC102** - Defending Web Applications
- **SEC202** - Threat Model Express
- **CSP102** - Secure Software Requirements
- **CSP103** - Secure Software Design
- **CSP104** - Secure Software Coding
- **CSP105** - Secure Software Testing
- **CSP106** - Software Acceptance
- **OAU201** - OAuth Sec. Fundamentals NEW

SECURE CODING

- **API101** - Defending Web APIs
- **JAV201** - Defending Java
- **JAV301** - Defending JSP
- **NET201** - Defending .NET Framework
- **NET301** - Defending .NET 5
- **PHP201** - Defending PHP
- **CPP201** - Defending C and C++
- **RUB201** - Defending Ruby on Rails

- **HTM201** - Defending HTML5
- **PYT201** - Defending Python
- **DJA101** - Defending Django
- **JVS101** - Defending JavaScript
- **NOD101** - Defending Node.js
- **ANG101** - Defending Angular
- **RCT201** - Defending React
- **CBL101** - Defending COBOL

SECURE MOBILE

- **MOB101** - Mobile Security Fundamentals
- **IOS201** - Defending iOS
- **AND201** - Defending Android

Operational Security

- **OPS101** - OpSec Fundamentals
- **DSO101** - DevSecOps Fundamentals
- **DAT101** - Defending Databases
- **CSP108** - Supply Chain and Software Acquisition
- **CLD101** - Cloud Security Fundamentals
- **AWS101** - Defending AWS
- **AZR101** - Defending Azure
- **CON101** - Defending Containers
- **DOC201** - Defending Docker
- **KUB201** - Defending Kubernetes
- **TER201** - Defending Terraform COMING SOON

Compliance

- **PRV101** - Privacy Fundamentals
- **CPA101** - CCPA for Software Development
- **HIP101** - HIPAA Privacy and Security
- **GDP101** - GDPR for Developers
- **PCI101** - PCI-DSS Compliance
- **PCI102** - PCI Secure Software Lifecycle
- **PCI103** - PCI SSF COMING SOON

General Awareness

- **SAW101** - Security Awareness
- **DVP101** - DevSecOps for Managers

The preceding course is a recommended preparatory course.

Role-Based Training

The **Software Security Practitioner Suites** are a series of on-demand learning courses that teach foundational elements of software security and language-specific secure coding. Each suite caters to your specific role, breaking down the learning so users efficiently learn only what they need. At the conclusion of the course, users will validate their skills by passing a certificate exam.

SecurityCompass (ISC)²

JAVA SUITE

The Java suite covers Java development, including fundamental coding concepts, design and implementation. Understand J2EE vulnerabilities common to the OWASP top 10, and see how these vulnerabilities affect Java web applications.

Learning Track:
- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Defending Java**

.NET SUITE

The .NET suite is designed to help students learn how to make secure software. Students will learn .NET vulnerabilities common to the OWASP Top 10 and see how these vulnerabilities affect .NET applications, and will learn defensive coding techniques that can be directly applied to their organization.

Learning Track:
- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Defending .NET 5**

PHP SUITE

The PHP suite informs students of PHP vulnerabilities common to the OWASP Top 10. Students will learn secure coding defenses and techniques for each vulnerability.

Learning Track:
- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Defending PHP**

C++ SUITE

The C++ suite presents common vulnerabilities in C/C++ software. Students will learn about safe memory management, insecure functions and how to defend against buffer overflow security concerns in unmanaged languages.

Learning Track:

- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Defending C and C++**

NODE.JS SUITE

Earners of the Defending Node.js Software Security Practitioner (SSP) Designation will acquire a deeper understanding of secure software coding and design techniques as well as learn the Node.js vulnerabilities common to the OWASP Top 10. Completion of the Node.js SSP Suite improves foundational knowledge of defensive coding that can be applied to a Node.js coding practitioner's daily tasks and will help improve their organization's overall security posture.

Learning Track:

- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Defending JavaScript**
- **Defending Node.js**

PYTHON SUITE

Earners of the Defending Python Software Security Practitioner (SSP) Designation will acquire a deeper understanding of secure software coding and design techniques as well as learn the Python vulnerabilities common to the OWASP Top 10. Completion of the Python SSP Suite improves foundational knowledge of defensive coding that can be applied to a Python coding practitioner's daily tasks and will help improve their organization's overall security posture.

Learning Track:

- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Defending Django**
- **Defending Python**

iOS SUITE

The iOS suite teaches students secure iOS coding techniques to defend against vulnerabilities such as insecure data storage, weak server side controls, lack of binary protections and more.

Learning Track:

- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Mobile Security Fundamentals**
- **Defending iOS**

ANDROID SUITE

The Android suite teaches secure coding concepts for Android applications. This includes secure Android coding techniques to defend against vulnerabilities such as insecure data storage, weak server side controls, lack of binary protections and more.

Learning Track:

- **AppSec Fundamentals**
- **Secure Software Design**
- **Secure Software Coding**
- **OWASP Top 10**
- **Mobile Security Fundamentals**
- **Defending Android**

SOFTWARE ARCHITECT SUITE

The Software Architect suite teaches students the key techniques to reducing risk in the development lifecycle by understanding how to correctly identify threats.

Learning Track:

- **AppSec Fundamentals**
- **Secure Software Requirements**
- **Secure Software Design**
- **OWASP Top 10**
- **Software Acceptance**
- **Threat Model Express**

PROJECT MANAGER SUITE

The Project Manager suite analyzes the full development lifecycle, depicting secure coding, requirements and design. Students will have the ability to define important security criteria to allow software to be promoted to release.

Learning Track:

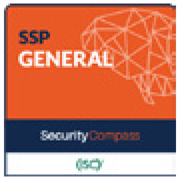
- **AppSec Fundamentals**
- **Secure Software Requirements**
- **Software Acceptance**
- **Supply Chain and Software Acquisition**

QA SUITE

The Q/A suite provides students with the ability to analyzes code and understand the principles of secure testing and testing software from a security perspective.

Learning Track:

- **AppSec Fundamentals**
- **OWASP Top 10**
- **Secure Software Testing**
- **Software Acceptance**



GENERAL SUITE

The General Suite provides students with fundamental security education, that they can directly apply to their position. Students will learn the 10 most prevalent web application security issues by OWASP and also gain foundational knowledge on application security.

Learning Track:

- **Security Awareness**
- **OWASP Top 10**
- **AppSec Fundamentals**

Application Security

FUNDAMENTALS

#	Course	Description	Time	Audience
APP101	AppSec Fundamentals	AppSec Fundamentals has been designed to provide insight into application security. Starting with key terminology and concepts, the course then provides an overview of the necessity of holistic security from the outset, the importance of protecting customer information, the requirements for managing risk at a business level, and incorporating security best practices into your software life cycle. Understanding these ideas will help you to better appreciate the challenges — and opportunities — in application security today.	75 mins	General Staff
SEC101 UPDATED	OWASP Top 10 (2021)	Discover the top 10 most important web application vulnerabilities in the OWASP 2021 list, the most recent list in this standard. Covers all top 10 items, describing each vulnerability, why it happens from a business risk perspective, how hackers exploit it, and how best to defend against these issues.	140 mins	General Staff, Developers
SEC102	Defending Web Applications	This course will explore the most common security concepts for web application developers who are new to application security. You'll learn how to address general web application security issues by incorporating defense mechanisms in your code.	75 mins	Developers
SEC202	Threat Model Express	Students will learn about the attacks that their apps may face and then an informal approach to threat modeling. Students will first learn the steps in executing a TME, and then they will engage in a guided fictional exercise.	60 mins	Developers, Architect
CSP102	Secure Software Requirements	Gathering the correct requirements to build secure software is one of the more difficult aspects to ascertain. Students will understand key techniques to reducing risk in the SDLC by understanding how to correctly identify requirements.	50 mins	Developers
CSP103	Secure Software Design	Understand the considerations and compromises that must be made when it comes to designing secure software. Students will learn about techniques to design secure software such as Threat Modeling and best practices to securing third party technologies that are often associated with modern software.	85 mins	Developers
CSP104	Secure Software Coding	Understand the considerations and compromises that must be made when it comes to designing secure software. Students will learn about techniques to design secure software such as Threat Modeling and best practices to securing third party technologies that are often associated with modern software.	40 mins	Developers

#	Course	Description	Time	Audience
CSP105	Secure Software Testing	Understand the principles to secure testing and testing software from a security perspective. Students will understand the fundamentals to setting up testing frameworks to promote software resiliency.	40 mins	Developers
CSP106	Software Acceptance	Understand how to generate criteria for software acceptance. The focus will be acceptance from a security standpoint and how students can define important security criteria being allowing software to be promoted to release.	25 mins	Developers
OAU201 NEW	OAuth Security Fundamentals	OAuth Security Fundamentals spans five modules. This course is designed for Security Architects and Software Developers. It is recommended that all learners are familiar with the security fundamentals of authentication and authorization, as described in the OWASP Top 10.	90 mins	Security Architects Software Developers
SECURE CODING				
API101	Defending Web APIs	This course discusses defenses against the common vulnerabilities of today's RESTful Web APIs. We'll cover the security of connecting to APIs, validating input and output, communication channels, and common attacks.	75 mins	Developers
CBL101	Defending COBOL	This course is designed as an introduction to safeguarding mainframes that use the COBOL programming language. While COBOL implementations may vary extensively based on their platforms and environments, this course aims to provide an implementation-agnostic overview of COBOL's most common vulnerabilities.	30 mins	Developers
CPP201	Defending C and C++	Software vulnerabilities often occur in C/C++ languages because they do not have strong protection mechanisms. Students will learn about how the inherent characteristics of these languages can be exploited to cause a range of vulnerabilities. This course also takes a look at some of the coding standards widely used by the Software Engineering Institute.	60 mins	Developers
PYT201	Defending Python	Students will learn how to use secure database queries, avoid risky Python functions, handle serialization safely, validate, encode and sanitize input, protect files and folders, and secure temporary files. Students will complete this course with an understanding of important defenses against various vulnerabilities.	35 mins	Developers

#	Course	Description	Time	Audience
DJA101	Defending Django	Learn about Django's built-in security features and other layers of protection to your app. Learn how to set up your projects securely to prevent attacks at run-time and how to secure the admin console. Students will also learn how to identify secure and insecure practices to protect your application against common attacks.	40 mins	Developers
HTM201	Defending HTML5	Learn about HTML standards designed to defend against vulnerable JavaScript, AJAX, JSON and iFrames. Students will learn the new technologies available in HTML5 to safely perform cross-domain requests as well as the use of offline storage, cross-origin resource sharing (CORS), cross-domain messaging (CDM), and iFrame sandboxing. Students gain a defensive understanding of the business risks to HTML5 mash-ups.	60 mins	Developers
JAV201	Defending Java	This course will build upon high-level application security concepts and how they relate to the Java environment. We will cover various threats and their defenses that are relevant to Java applications in JDK 6 through 10, including many common frameworks like Java EE / Jakarta EE and Spring.	90 mins	Developers Architects
JAV301	Defending JSP	Understand how to defend your Java web apps against attacks. Using code samples from Java Server Pages, this course covers a variety of techniques for securing against such vulnerabilities as SQL injection, cross-site scripting/request forgery, man-in-the-middle attacks and more.	90 mins	Developers
NET201	Defending .NET Framework	Understand .NET 4.8 vulnerabilities common to the OWASP top 10, and see how these vulnerabilities affect .NET web applications. Students will learn secure coding defenses for each vulnerability.	60 mins	Developers
NET301	Defending .NET 5	This course covers secure application development using C# in ASP.NET CLD. Students will learn about software vulnerabilities and how hackers exploit them, followed by techniques for coding to defend against a variety of attacks.	80 mins	Developers
JVS101	Defending JavaScript	Defending JavaScript is a course for basic and intermediate developers who have some knowledge of application security fundamentals. This course takes a code agnostic approach to secure coding to identify and defend against common risks for front-end JavaScript vulnerabilities. While the focus is on the front-end, there are considerations for back-end security where it applies to the front-end as well. These topics include, cross-site scripting, injection attacks, broken authentication and broken access control, security misconfiguration, and general best practices.	60 min	Developers

#	Course	Description	Time	Audience
NOD101	Defending Node.JS	Understand the security risks when developing and deploying applications in Node.js. Implement defensive coding techniques and configurations to support secure coding for Node.js.	60 mins	Developers
PHP201 UPDATED	Defending PHP 2022	This course has been developed for PHP developers and web application architects who want to defend against common security vulnerabilities found in PHP applications and have completed OWASP Top 10 as a prerequisite.	105 mins	PHP Developers, Web App Architects
ANG101	Defending Angular	Defending Angular is divided into three parts. Part one helps software developers investigate how the Angular development paradigm impacts security. Part two explores a set of best practices for building, deploying, and maintaining Angular applications. And Part 3 investigates how to implement authentication and authorization in Angular applications.	120 mins	Developers
RUB201	Defending Ruby on Rails	Defending Ruby on Rails was created for developers who already have some experience coding in Python and developing web applications with the Ruby platform, and will focus on creating secure web applicattions in Ruby.	40 mins	Developers
RCT201	Defending React	Defending React.js was created for developers familiar with JavaScript and with limited experience in application security. This course focuses on best practices for addressing the primary threats against applications using the open source library React.js for JavaScript.	55 mins	Developers
SECURE MOBILE				
MOB101	Mobile Security Fundamentals	In this code-agnostic course, students will learn important mobile security concepts to build more secure mobile applications. We will dive into understanding what the risks are to developing insecure mobile applications and how hackers can target the app, the infrastructure and the mobile device itself. Students will learn about the current threat landscape with different mobile operating systems, un-official means of loading applications on devices and the business risk to developing insecure mobile applications.	60 mins	Developers, Architects
IOS201	Defending iOS	Explore defenses against common vulnerabilities in iOS applications developed with Objective-C and Swift. This course covers industry best practices in secure coding as it relates to authentication and authorization, session management, secure data transfers, secure data storage, cryptography, and secure data ingestion.	70 mins	Developers, Architects

#	Course	Description	Time	Audience
AND201	Defending Android	Explore defenses against common vulnerabilities in Android applications developed with Java and Kotlin. This course covers industry best practices in secure coding as it relates to authentication and authorization, secure data transfers, secure data storage, cryptography, and secure data ingestion.	70 mins	Developers, Architects

Operational Security

#	Course	Description	Time	Audience
OPS101	OpSec Fundamentals	This course covers the fundamental concepts of Operations Security in terms of installation and deployment, access control and identity management, the Security Operations Centre, Business Continuity and Disaster Recover, and enterprise data backup and disposal.	60 mins	Ops Engineers, System Admins
DS0101	DevSecOps Fundamentals	This course introduces the philosophy and best practices behind DevSecOps. It covers how an organization can build a DevSecOps program and application development pipeline that can keep up with the pace of modern development without sacrificing software security.	60 mins	Developers, Architects, Ops Engineers, System Admins
DAT101	Defending Databases	Understand the vulnerabilities that affect your databases. We'll cover a variety of techniques for securing your databases against such vulnerabilities as SQL injection, buffer overflows, protocol vulnerabilities, and more. Students will also learn some best practices for managing a database to keep it and its data safe.	60 mins	Developers
CSP108	Supply Chain and Software Acquisition	Understand how to identify risks when sourcing software from the supply chain. Students will learn about risk management, protecting intellectual property, procurement and best practices when outsourcing software to suppliers.	80 mins	Developers
CLD101	Cloud Security Fundamentals	This course aims to teach you about common security concerns surrounding cloud-based applications and to some extent, cloud providers. Students will also learn about best practices and security concepts involved when creating applications for the cloud, all the way from requirements to deployment.	60 mins	Developers
AWS101	Defending AWS	Defending AWS was created for DevOps and Ops Engineers who have some familiarity with application security. This course focuses on configuring AWS to defend against the most common security threats using best practices.	60 mins	DevOps Engineers, Ops Engineers

#	Course	Description	Time	Audience
AZR101	Defending Azure	Defending Azure was created for DevOps and Ops Engineers who have experience using Microsoft Azure and familiarity with application security. This course focuses on configuring Azure to defend against the most common security threats.	60 mins	DevOps Engineers, Ops Engineers
CON101	Defending Containers	Defending Containers helps DevOps engineers understand and implement strategies to secure containers. This course covers fundamental concepts of containerization, what's required for hardening your build environment, operating system, and container engine, and how to ensure security while running multiple containers at scale by restricting network activity and using logging and monitoring.	45 mins	DevOps Engineers
DOC201	Defending Docker	Defending Docker was created for DevOps and Ops Engineers who have experience using Docker and familiarity with application security. This course focuses on configuring the Docker platform to defend against the most common security threats.	40 mins	DevOps Engineers, Ops Engineers
KUB201	Defending Kubernetes	Defending Kubernetes builds on the foundations of Defending Containers. This course covers best practices for securing systems that use Kubernetes. You'll look at security considerations that range over every stage of Kubernetes development, including the build phase, deployment, and runtime.	80 mins	DevOps Engineers, Ops Engineers

Compliance

#	Course	Description	Time	Audience
PRV101	Privacy Fundamentals	In today's technology landscape, large scale data breaches make headlines leading to questions about how companies are using and protecting sensitive, regulated, and personal information. In this course, you will learn about the fundamentals of privacy and data protection, and explore how it is relevant to building secure software.	45 mins	Developers, Risk and Compliance Personnel, General Staff
CPA101	CCPA for Software Development	This course will introduce you to the California Consumer Privacy Act (CCPA) and its effect on you as a software developer. After taking this course, you should be able to adopt CCPA compliance in your daily tasks and identify a non-compliance risk at the very beginning.	20 mins	Developers, General Staff

#	Course	Description	Time	Audience
HIP101	HIPAA for Privacy and Security	HIPAA for Software Development helps developers and software architects meet HIPAA requirements by covering the objectives of HIPAA compliance, the roles of Covered Entities and Business Associates, and the key privacy and security requirements for safeguarding protected health information. The course then discusses strategies for protecting various types of information and responding to potential breaches of protected health information.	40 min	Developers, Architects
GDP101	GDPR for Developers	We know that developers would rather spend their time coding than worrying about if their application is compliant with the General Data Protection Regulation (GDPR). We created this course to be focused on development and practical to developers so that they could get the essentials of meeting GDPR requirements without learning everything about it. Who has time for that?	60 mins	Developers, Architects
PCI101	PCI-DSS Compliance	This course is designed to provide PCI-DSS awareness training to individuals with PCI-DSS compliance responsibilities. In this course, you will gain fundamental knowledge of PCI to develop effective security responsibilities, safeguards, and processes.	40 mins	General Staff
PCI102	PCI Secure Software Lifecycle	The Payment Card Industry Secure Software Lifecycle (PCI SSLC) course provides guidelines for designing, developing, and maintaining secure software through secure governance, engineering, software and data management, and communications. While these guidelines are provided by the payment card industry, PCI SSLC provides a strong baseline of secure development for all software.	40 mins	Developers, Architects

General Awareness

#	Course	Description	Time	Audience
SAW101	Security Awareness	This course explains how bad information security behavior affects you and your company. You will also learn how to protect sensitive information about you or your company from attackers.	40 mins	General Staff
DVP101	DevSecOps for Managers	In this course, students will learn about DevOps before exploring how security fits into the picture. Understand the benefits of a DevOps model, the difficulties in transitioning to it, and how to achieve DevSecOps.	30 mins	Technology Managers

About Security Compass

We designed our software security training to meet the agile needs of today's modern organizations, with adaptive courseware that can be tailored to meet the learning goals of individual students. Whether you are trying to reach compliance or raise security standards across an organization, our training is flexible enough to meet your educational needs.

info@securitycompass.com

www.securitycompass.com

Security Compass