

SecurityCompass

Application Security Training Curriculum



2024 Q3

Index

- 1** Why Security Compass?
- 2** Choose the content and deployment option that better fits your training program
- 3** Just-in-Time Training in SD Elements
- 4** Course Full Library Curriculum
- 5** Kontra Hands-On Labs Curriculum
- 6** Role-Based Training
- 9** Course Full Library Catalogue
- 18** Kontra Hands-On Lab Catalogue

Why Security Compass?

Our Application Security Training portfolio meets the needs of today's modern organizations tasked with delivering secure and compliant software by design. Our Courses and Kontra Hands-On Labs are tailored to meet each learner's goals for application security training. Meet your compliance requirements and lay the knowledge foundation for security by design.



SECURITY EXPERTISE

Security Compass, the Security by Design Company, is a leading provider of cybersecurity solutions, enabling organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its developer-centric threat modeling offering, SD Elements, and Application Security Training solutions help organizations release secure and compliant software to market quickly and cost effectively.



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 ISC2. This program offers role-based training paths that allow learners to earn an ISC2 certificate and share their achievement with their network through a social media badge.



FLEXIBILITY AND APPEAL

Already knowledgeable on specific security content? Go ahead and jump right to the quiz. Need more time to digest new information or updates? No problem - playback all or selected modules. Start and stop as you go. Need developers to learn defend and attack maneuvers to code securely? Engage them with bite-sized and interactive storytelling content with Kontra Hands-On Labs that are inspired by real world and recent scenarios. Our Courses and Kontra Hands-On Labs are designed to be adaptable, engaging and just-enough (think learning in minutes not hours) to keep security training digestible for learners.



UP-TO-DATE CONTENT

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

Choose the content and deployment option that better fit your training program

COURSE FULL LIBRARY

A curriculum of interactive courses, and role-based learning paths that optionally culminate in an exam for co-branded certification with ISC2. Available in custom packages to meet application security training needs for developers and other staff that support the development organization.

Subscription Plans for Courses

- Full Course Library
- ISC2 Secure Software Practitioner Suites (SSPs) only
- 5-Course and 1-Course Packages only
- Security Awareness Course only

KONTRA HANDS-ON LABS FULL LIBRARY

Immersive hands-on training labs for developers to understand and prevent real-world application security threats with language-specific code samples to secure the code.

Subscription Plans for Kontra Hands-On Labs

- Full Labs Library

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 ISC2 certificates.

DEPLOYMENT OPTIONS

We offer Software as a Service (SaaS) Learning Management System or you can import our Application Security Training 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 the best solution for organizations who need to scalably model software threats, identify countermeasures, and deliver secure, compliant code quickly. SD Elements' comprehensive approach to application security empowers DevSecOps teams to make software secure and compliant by design through automating threat modeling, generating application security requirements, and providing secure development and compliance best practices.

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 AI-LLM
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
Defending Terraform
Defending Go
Defending Typescript
HIPAA Privacy and Security
GDPR for Developers
Microservices

OpSec Fundamentals
OWASP Top 10 2021
PCI-DSS Compliance
PCI Secure Software Lifecycle
OAuth Security Fundamentals
PCI SSF
Ansible
Securing the Cloud

1000+ micromodules

Course Full Library Curriculum

Application Security

FUNDAMENTALS

APP101 AppSec Fundamentals **UPDATED**
SEC101 OWASP Top 10
SEC102 Defending Web Applications
DTM101 Developer-Centric Threat Modeling **UPDATED**
CSP102 Secure Software Requirements
CSP103 Secure Software Design
CSP104 Secure Software Coding
CSP105 Secure Software Testing
CSP106 Secure Software Acceptance & Deployment
OAU201 OAuth Sec. Fundamentals

SECURE CODING

API101 Defending Web APIs
JAV201 Defending Java
JAV301 Defending JSP
NET201 Defending .NET Framework
NET302 Defending .NET 6
PHP201 Defending PHP
CPP201 Defending C and C++
RUB201 Defending Ruby on Rails
GOL201 Defending Go
SCL201 Defending Scala
HTM201 Defending HTML5
PYT201 Defending Python
DJA101 Defending Django
JVS101 Defending JavaScript
NOD201 Defending Node.js
ANG101 Defending Angular
RCT201 Defending React
CBL101 Defending COBOL
TYP201 Defending TypeScript
LLM101 Defending AI for Developers
BSH201 Defending Bash
RST201 Defending Rust **NEW**

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 Security
CLD101 Cloud Security Fundamentals
AWS101 Defending AWS
AZR101 Defending Azure
CON101 Defending Containers
DOC201 Defending Docker
KUB201 Defending Kubernetes
TER201 Defending Terraform
ANS201 Defending Ansible

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

General Awareness

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

Kontra Hands-On Lab Curriculum

OWASP Top 10 for Web

- PYT202** Python (Django) - OWASP Top 10 for Web
- FSK201** Python (Flask) - OWASP Top 10 for Web
- JAV202** Java - OWASP Top 10 for Web
- NOD202** Node.js - OWASP Top 10 for Web
- GOL202** Go - OWASP Top 10 for Web
- PHP202** PHP - OWASP Top 10 for Web
- RUB202** Ruby - OWASP Top 10 for Web
- NET202** C# - OWASP Top 10 for Web
- SCL202** Scala - OWASP Top 10 for Web
- KOT201** Kotlin - OWASP Top 10 for Web
- PSD201** Pseudocode - OWASP Top 10 for Web

OWASP Top 10 for API

- JAV203** Java API - OWASP Top 10 for API **UPDATED**
- PYT203** Python (Django) API - OWASP Top 10 for API
- FSK202** Python (Flask) API - OWASP Top 10 for API
- NOD203** Node.js API - OWASP Top 10 for API
- GOL203** Go API - OWASP Top 10 for API
- PHP203** PHP API - OWASP Top 10 for API
- RUB203** Ruby API - OWASP Top 10 for API
- NET203** C# API - OWASP Top 10 for API

Front-End Top 5

- JVS202** JavaScript - Front-end Top 5
- ANG202** Angular - Front-end Top 5
- RCT202** React - Front-end Top 5
- TYP202** TypeScript - Front-end Top 5
- VUE201** Vue - Front-end Top 5

DevOps

- AWS202** AWS for Java - AWS Top 10
- DOC202** Docker CLI - Top 10
- DOC203** Docker Compose - Top 10
- KUB202** Kubernetes - Top 10
- TER202** Terraform - OWASP Top 10

OWASP Top 10 for Mobile

- AND202** Android (Java) - OWASP Top 10 for Mobile
- IOS202** Swift - OWASP Top 10 for Mobile
- IOS203** Objective-C - OWASP Top 10 for Mobile

OWASP Top 10 for LLM

- LLM201** LLM OWASP Top 10 **NEW**

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 ISC2™



SECURITY CHAMPION SUITE

The Security Champions Learning Path gives participants a comprehensive foundation in modern software security. Those who complete the learning path will understand the fundamental concepts of AppSec, how to implement security measures throughout the software development lifecycle, and how to promote strong DevSecOps practices and foster a strong security culture.

Learning Track:

- Security Champion Best Practices Modules
- DevSecOps Fundamentals
- Secure Software Requirements
- Secure Software Testing
- Secure Software Acceptance and Deployment
- Developer-Centric Threat Modeling



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 6



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



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
- Developer-Centric Threat Modeling



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 analyze 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

Course Full Library Catalogue

Application Security				
FUNDAMENTALS				
#	Course	Description	Time	Audience
APP101	AppSec Fundamentals <div>UPDATED</div>	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	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 <div>UPDATE SOON</div>	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
DTM101	Developer-Centric Threat Modeling <div>UPDATED</div>	Developer-centric Threat Modeling (DCTM) is a course for Security Architects, Security Champions, and Lead Developers who are interested in threat modeling for today's modern and Agile methodologies. This course covers threat modeling from the ground up and focuses on how developers can not only contribute to, but also run threat modeling in their organization. From best practices to threat modeling frameworks, and issue management to tooling, join Sam—a budding Security Champion—and Antoni—a cybersecurity and threat modeling expert—on their journey to bring developer-centric threat modeling to their organization, BitByBit.	80 mins	Lead Developers Product Managers / Project Managers Security Champions Architects

#	Course	Description	Time	Audience
CSP102	Secure Software Requirements	Secure Software Requirements is for anyone involved in the gathering of functional, security or operational requirements, including security professionals, software professionals, architects, product managers, project managers, and program managers.	80 mins	Developers
CSP103	Secure Software Design <div>UPDATE SOON</div>	The design phase of software development is one of the most important phases in the Software Development Life Cycle. The Security Software Design domain will provide the learner with an understanding on how to ensure that software security requirements are included in the design of the software. Learners will gain knowledge of secure design principles and processes and be exposed to different architectures and technologies for securing software.	85 mins	Developers
CSP104	Secure Software Coding	Secure Software Coding was created to provide Certified Secure Software Lifecycle Professionals (CSSLP) with an understanding of the importance of programming concepts that can effectively protect software from vulnerabilities. Learners will touch on topics such as software coding vulnerabilities, defensive coding techniques and processes, code analysis and protection, and environmental security considerations that should be factored into software.	40 mins	Developers
CSP105	Secure Software Testing	In Secure Software Testing, you'll start by taking a big-picture look at modern software testing practices. Then you'll learn how to test your source code during development. Following that, you'll see how you can incorporate secure testing strategies in the later stages of testing. And finally, you'll look at secure testing strategies you can use later in the software development lifecycle.	75 mins	Junior Developers, Managers
CSP106	Secure Software Acceptance & Deployment	Secure Software Acceptance and Deployment is for software development professionals and security professionals who are responsible for securing different phases of the SDLC, including software engineers, architects, DevOps engineers, DevSecOps engineers, development managers, project managers, product managers, and QA analysts.	60 mins	Managers, DevOps Engineers
OAU201	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

#	Course	Description	Time	Audience
API101	Defending Web APIs	Defending Web APIs is for software developers, architects, and security architects. This course focuses on best practices for securing Web APIs throughout the software development lifecycle.	70 mins	Software Developers, Architects, Software Architects
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
DJA201	Defending Django	In this course, you'll learn what you need to do to take advantage of Django's built-in security features and provide other layers of protection to your app. You'll learn how to set up your projects securely to prevent attacks at run-time and how to secure the admin console.	70 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	Defending Java is for Java developers and Java architects. This course focuses on best practices for addressing threats against Java applications. Suggested prerequisite courses include Defending Web Applications, OWASP Top 10, and Secure Software Design.	120 mins	Java Developers Java Architects

#	Course	Description	Time	Audience
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
NET302	Defending .NET 6 <div>UPDATE SOON</div>	By the end of this course, learners will be able to identify common vulnerabilities in .NET web applications, and learn how to address them, defend against attacks that target the people who use your web applications, use logging effectively in an ASP.NET web application, protect services you build with ASP.NET Web API, and ensure that the sensitive information you handle during development stays secret.	75 mins	C# Developers, Web Application, 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.	60 min	Developers
NOD201	Defending Node.js	This course is designed for Node and Web developers who have some familiarity with Web application security. Node is one of the most commonly used open-source Web technologies for building scalable web applications. For this reason, it's important to understand its security risks and how to implement defensive coding techniques and configurations.	60 mins	Node.js Developers Web Developers
PHP201	Defending PHP	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

#	Course	Description	Time	Audience
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 applications 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
TYP201	Defending TypeScript	In the four modules of this course, we'll explore how to protect TypeScript applications by detecting, scoring, fixing, and monitoring vulnerabilities that could otherwise lead to attacks.	45 mins	Developers Testers Security Professionals
GOL201	Defending Go	Defending GoLang is for software development professionals and security professionals who are responsible for securing different phases of the SDLC.	60 mins	Developers
LLM101	Defending AI	Defending AI is a course for anyone interested in learning more about the cybersecurity threats that affect AI systems, but is focused on Software Developers who use Large Language Models (LLMs), generative AI, and other AI tools. This course provides an overview of best security practices for using these tools and examines how the field is evolving rapidly. As more organizations begin to leverage AI in their day-to-day activities, it becomes increasingly important to practice AI security hygiene.	70 mins	Developers
SCL201	Defending Scala	While Scala and Java share many similarities in terms of security, many Scala-focused security solutions are not yet ready for production. Defending Scala covers best security practices along the SDLC when working with Scala and is targeted to Developers and Testers. This course is recommended for intermediate learners who have completed AppSec Fundamentals and the OWASP Top 10, or equivalent.	55 mins	Scala Developers Testers
BSH201	Defending Bash	Defending Bash is a course designed to cover best security practices along the SDLC for Developers, SysAdmins, DevOps professionals, Data Engineers, and more. This course is designed for intermediate students who have already familiar with basic security concepts. While this course is designed to address security concerns Bash, a Unix command language, it also applies to any command-line interface shell.	45 mins	SysAdmins DevOps Professionals Data Engineers

RST201	Defending Rust NEW	Defending Rust is a course tailored for Rust developers and testers who seek to enhance their knowledge of secure coding practices in Rust. This course offers an in-depth look at the security features of Rust, the best practices for maintaining a secure development environment, and techniques for safe memory management. As Rust continues to gain traction for its performance and safety, understanding how to mitigate security risks becomes crucial. This course equips you with the skills to implement secure programming patterns and safeguard the supply chain, ensuring robust and secure Rust applications.	90 mins	Rust Developers
--------	------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------	-----------------

SECURE MOBILE

#	Course	Description	Time	Audience
MOB101	Mobile Security Fundamentals	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.	60 mins	Developers, Architects
IOS201	Defending iOS	Explore defenses against common vulnerabilities in iOS applications developed with Objective-C and Swift.	70 mins	Developers, Architects
AND201	Defending Android UPDATE SOON	Explore defenses against common vulnerabilities in Android applications developed with Java and Kotlin.	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

#	Course	Description	Time	Audience
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 Security	Supply Chain Security is a course for Software Developers and Managers. It focuses on discussing the vulnerabilities throughout the supply chain, from third-party software to mitigating risk with suppliers. This course provides best practices you can apply to defend against the security vulnerabilities you are likely to encounter as you build out your supply chain.	75 mins	Developers Managers
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
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 <div>UPDATE SOON</div>	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
TER201	Defending Terraform	This course is part of the line of defending against threats to Infrastructure as Code (IaC). Defending Terraform builds on the foundations of cloud security.	60 mins	DevOps Engineers, DevOps Managers
ANS201	Defending Ansible	Defending Ansible is for anyone involved in deploying and configuring IT infrastructure, including DevOps and DevSecOps professionals.	70 mins	DevOps, DevSecOps

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
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 was designed for developers whose organizations and applications must comply with PCI DSS.	70 mins	Developers, 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
PCI103	PCI SSF	This course examines the PCI SSF (Software Security Framework) and the PCI Security Software Standard (PCI SSS or S3), which is a component of PCI SSF. The framework was designed by the PCI Council to encourage developers to design and implement more secure software and will replace the Payment Application Data Security Standard (PA DSS) in 2022.	55 mins	Developers, DevOps, PMs, PCI Assessors

General Awareness

#	Course	Description	Time	Audience
SAW101	Security Awareness	By the end of this course, you will be able to explain the consequences of poor information security habits, and how to protect sensitive information about you or your company from attackers. You will also be able to promote a corporate culture that prioritizes security so that your company can significantly reduce the risk of data breaches and other malicious activities that could compromise its operations and reputation.	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

Kontra Hands-On Lab Catalogue

OWASP Top 10 for Web

#	Course	Content	Time	Audience
PYT202	Python (Django) - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Python (Django) Developers
FSK201	Python (Flask) - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Python (Flask) Developers
JAV202	Java - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Java Developers
NOD202	Node.js - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Node.js Developers

GOL202	Go - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Go Developers
PHP202	PHP - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior PHP Developers
RUB202	Ruby - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Ruby Developers
NET202	C# - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior C# Developers
SCL202	Scala - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Scala Developers

KOT201	Kotlin - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Kotlin Developers
PSD201	Pseudocode - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Pseudocode Developers

OWASP Top 10 for API

#	Course	Content	Time	Audience
JAV203 UPDATED	Java API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior Python (Django) Developers
PYT203	Python (Django) API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior Python (Django) Developers
FSK202	Python (Flask) API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior Python (Flask) Developers
NOD203	Node.js API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior Node.js Developers

GOL203	Go API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior Go Developers
PHP203	PHP API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior PHP Developers
RUB203	Ruby API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior Ruby Developers
NET203	C# API - OWASP Top 10 for API	Security Misconfiguration, XXE Injection, Insufficient Logging & Monitoring, SQL Injection, Mass Assignment, Broken Function Level Authorization, Lack of Resources & Rate Limiting, Broken User Authentication, Broken Object Level Authorization, Excessive Data Exposure, Improper Assets Management	120 mins	Junior C# Developers
AWS202	AWS for Java - AWS Top 10	Lambda XXE Injection, Dangerous Dependencies, Excessive Logging, Misconfigured AWS Cognito profile allows self-registration, Misconfigured AWS Cognito Attributes, Misconfigured Reverse Proxy, Lambda Command Injection, Weak S3 POST Upload Policy, S3 Directory Traversal, S3 Bucket Authenticated Users 'WRITE' Access, S3 Bucket Public 'READ' Access, Subdomain Takeover	120 mins	DevOps
DOC202	Docker CLI - Top 10	Exposed Docker Socket, Container Resources Limitation, Privileged Containers, Host Update, Unsegregated Container Network, Improper Write Permissions for Volumes and Host Filesystem, Sensitive Data Leak via Docker Images, Unverified Container Images, Minimal Base Image, Insecure Container Registries	72 mins	DevOps
DOC203	Docker Compose - Top 10	Exposed Docker Socket, Container Resources Limitation, Privileged Containers, Host Update, Unsegregated Container Network, Improper Write Permissions for Volumes and Host Filesystem, Sensitive Data Leak via Docker Images, Unverified Container Images, Minimal Base Image, Insecure Container Registries	72 mins	DevOps

KUB202	Kubernetes - Top 10	Overly Permissive RBAC Configurations, Missing Network Segmentation Controls, Broken Authentication Mechanisms, Misconfigured Cluster Components, Inadequate Logging and Monitoring, Lack of Centralized Policy Enforcement, Insecure Workload Configurations, Secrets Management Failure, Supply Chain Vulnerabilities, Vulnerable Kubernetes Components - Security Audit	72 mins	DevOps
TER202	Terraform - OWASP Top 10	Lack of Infrastructure Policy Enforcement, Supply Chain Vulnerabilities, Misuse of Terraform Modules, Misconfigured Cluster Components, Inadequate Monitoring and Auditing, Insecure State Management, Insecure Storage of Sensitive Data, Missing Network Segmentation Controls, Insufficient Validation of Input Data, Insecure Workload Configurations	72 mins	DevOps

OWASP Top 10 for Mobile

#	Course	Content	Time	Audience
AND202	Android (Java) - OWASP Top 10 for Mobile	COMING SOON	TBC	Junior Android (Java) Developers
IOS202	Swift - OWASP Top 10 for Mobile	Sensitive Data in Login Fields, Local Authentication, Keychain Persistence, SSL/TLS Pinning, Insecure Communication, Unprotected Application Access, Insecure local SQLite Database, Insecure URL Cache, Insecure URL Scheme, Insecure Data Storage	222 mins	Junior Swift Application Developers
IOS203	Objective-C - OWASP Top 10 for Mobile	Sensitive Data in Login Fields, Local Authentication, Keychain Persistence, SSL/TLS Pinning, Insecure Communication, Unprotected Application Access, Insecure local SQLite Database, Insecure URL Cache, Insecure URL Scheme, Insecure Data Storage	222 mins	Junior Objective-C Application Developers

OWASP Top 10 for LLM

#	Course	Content	Time	Audience
LLM201 NEW	LLM OWASP Top 10	TBC	TBC	Junior LLM Developers

Front-End Top 5 and DevOps

#	Course	Content	Time	Audience
PYT202	Python (Django) - OWASP Top 10 for Web	Components with Known Vulnerabilities, Cross Site Request Forgery, DOM XSS, Server Side Request Forgery, Token Exposure in URL, Command Injection, SQL Injection, Horizontal Privilege Escalation, Vertical Privilege Escalation, User Enumeration, Directory Traversal, Clickjacking, XML Injection, Insecure URL Redirect, Session Fixation, PII data in URL, Weak Randomness, Header Injection, Leftover Debug Code, Stored Cross Site Scripting, Forced Browsing, Reflected XSS	222 mins	Junior Python (Django) Developers
JVS202	JavaScript - Front-end Top 5	Untrusted Template Usage XSS, Cross Site Request Forgery, Direct DOM Manipulation XSS, Components with Known Vulnerabilities, Untrusted HTML Rendering XSS	50 mins	Junior JavaScript Developers
ANG202	Angular - Front-end Top 5	Untrusted Template Usage XSS, Cross Site Request Forgery, Direct DOM Manipulation XSS, Components with Known Vulnerabilities, Untrusted HTML Rendering XSS	50 mins	Junior Angular Developers
RCT202	React - Front-end Top 5	Cross Site Request Forgery, Direct DOM Manipulation XSS, Components with Known Vulnerabilities, Untrusted HTML Rendering XSS	40 mins	Junior React Developers
TYP202	TypeScript - Front-end Top 5	Untrusted Template Usage XSS, Cross Site Request Forgery, Direct DOM Manipulation XSS, Components with Known Vulnerabilities, Untrusted HTML Rendering XSS	50 mins	Junior TypeScript Developers
VUE201	Vue - Front-end Top 5	Untrusted Template Usage XSS, Cross Site Request Forgery, Direct DOM Manipulation XSS, Components with Known Vulnerabilities, Untrusted HTML Rendering XSS	50 mins	Junior Vue Developers

About Security Compass

Security Compass, the Security by Design Company, is a leading provider of cybersecurity solutions, enabling organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its developer-centric threat modeling offering, SD Elements, and Application Security Training solutions help organizations release secure and compliant software to market quickly and cost effectively. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defense, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and UK. For more information, please visit www.securitycompass.com

info@securitycompass.com

www.securitycompass.com

SecurityCompass