

## The AppSec Awareness Solution for DevOps

### Product Benefits

- **Leveraging Over 13 years of AppSec Experience** - An integral part of Checkmarx, CxCodebashing makes use of real-world examples and best practices gleaned from years of experience with over 1400 customers around the globe.
- **Training and Beyond** - Providing security teams with the communication, engagement, training, and assessment tools they need to execute comprehensive AppSec awareness campaigns for developers throughout the year.
- **Developer-Centric** - Developers “wear the hacker’s hat” as they see all the moving parts of the application stack that are relevant to explain the specific vulnerability in an interactive lesson.
- **Built to Scale** - Easily manage and track large enterprise teams in CxCodebashing with drill-down dashboard analytics and built-in support for major SAML/SSO providers.
- **Just-in-Time Remediation Support** - Vulnerabilities detected in Checkmarx Static Application Security Testing (CxSAST) include an easy-to-follow link to the relevant CxCodebashing lesson.

### Product Overview

Whether used as standalone solution or integrated with Checkmarx SAST, Codebashing is a hands-on, interactive solution that fits into developers' daily routines in bite-size, on-demand training relevant to challenges faced in their code. Codebashing cultivates a culture of software security that empowers developers to take security into their own hands and be comfortable doing so. Leverage just-in-time training to educate developers on specific challenges they are facing, without diverting them from accomplishing their main task - writing secure code quickly.

### Product Features

#### Raise the AppSec bar

CxCodebashing allows you to raise the baseline AppSec knowledge across your entire development team in a fast, scalable, and positive manner. Managers have full control and visibility – they can easily assign specific programming language courses to their teams and continuously track their progress.

#### Learn while coding

Unlike traditional classroom or video-based training, CxCodebashing is a fun, hands-on, interactive solution that fits into your developers' daily routines. Developers receive bite-size, on-demand sessions that are relevant to the specific challenges they are facing in their code.

#### Find and Fix in one go

Checkmarx offers a unique integration between our Static Application Security Testing (CxSAST) solution and our secure coding education solution. Vulnerabilities identified by static analysis are linked to relevant, practical training lessons providing quick and pointed remediation guidance. Developer see why a problem happened, how to fix it, and more importantly, how to prevent making the same mistake again in less than 5 minutes per lesson.

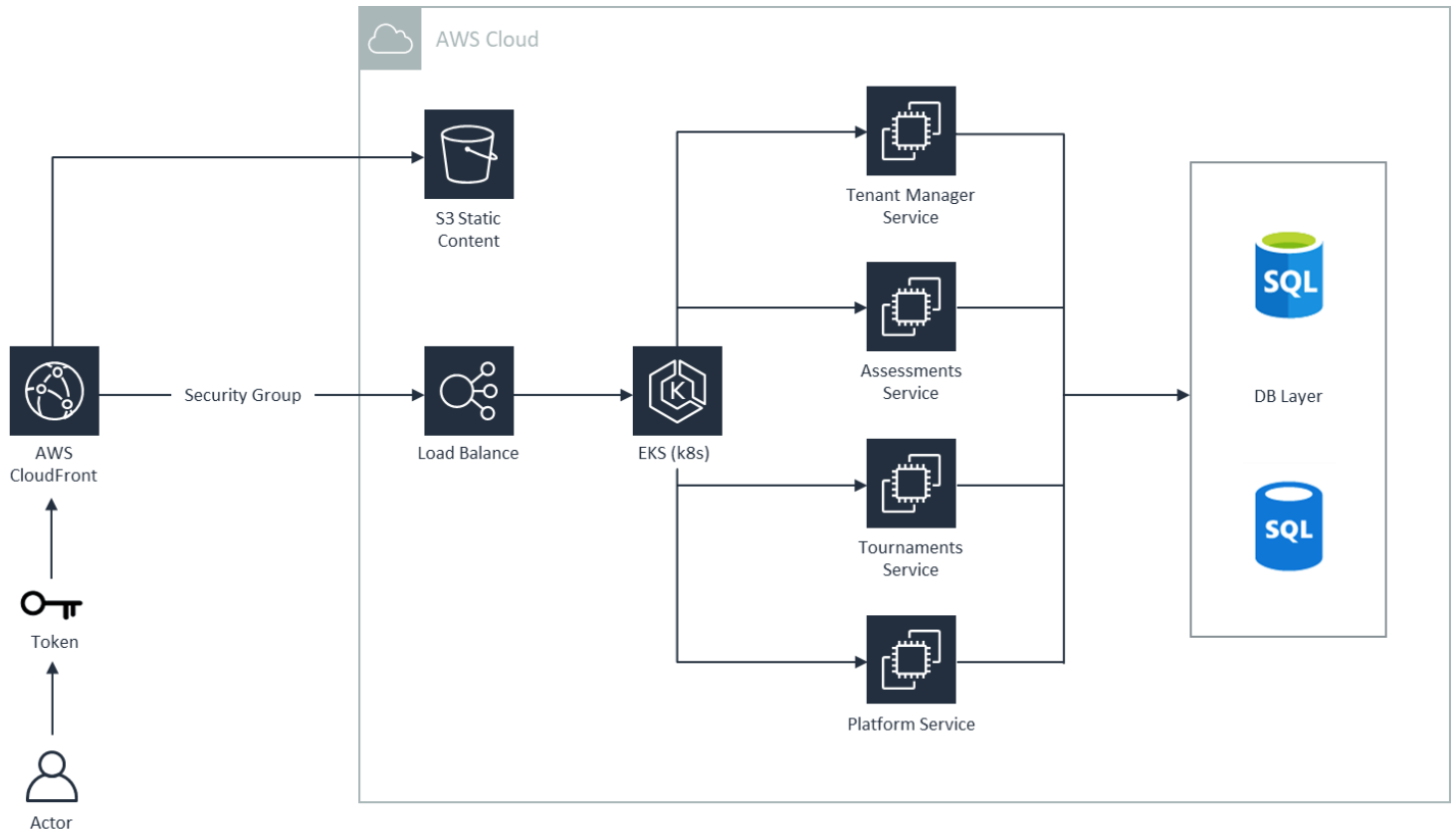
#### Comply with regulatory standards

CxCodebashing is compatible with regulatory standards like PCI-DSS that require either “role based security training” or, more specifically, “developer security training”.

## How it works

The Checkmarx Software Security Platform provides a centralized foundation for operating your suite of software security solutions for Static Application Security Testing (SAST), Interactive Application Security Testing (IAST), Software Composition Analysis (SCA), and application security training and skills development.

Built to address every organization's needs, the Checkmarx Software Security Platform provides the full scope of options: including private cloud. Allowing a range of implementation options ensures customers can start securing their code immediately, rather than going through long processes of adapting their infrastructure to a single implementation method.



### Supported Languages and Frameworks



### Vulnerability Coverage

- SQL Injection
- XXE Injection
- Command Injection
- Session Fixation
- Use of Insufficiently Random Values
- Reflected XSS
- Persistent (Stored) XSS
- DOM XSS
- Directory (Path) Traversal
- Privileged Interface Exposure
- Leftover Debug Code
- Authentication Credentials In URL
- Session Exposure within URL
- User Enumeration
- Horizontal Privilege Escalation
- Vertical Privilege Escalation
- Cross Site Request Forgery (POST)
- Cross Site Request Forgery (GET)
- Click Jacking
- Insecure URL Redirect
- Insecure TLS Validation
- Insecure Object Deserialization
- Components with Known Vulnerabilities

Solution available in [AWS Marketplace](#)