CHECKMARX

CxSAST

Static Application Security Testing

The Application is the New Perimeter

The cyberthreats to organizations take many forms, but attacks against software are the number one threat. Gone are the days when organizations could rely on perimeter defenses like firewalls to protect their sensitive data. Today, web applications are the new perimeter, and addressing Software Exposure is a top requirement for security, and a high priority issue in boardrooms.

Checkmarx CxSAST is part of the Checkmarx Software Exposure Platform addressing software security risk across the entire SDLC. CxSAST is a flexible and accurate static analysis solution used to identify hundreds of types of security vulnerabilities in both custom code and open source components. It is used by development, DevOps, and security teams to scan source code early in the SDLC across over 25 coding and scripting languages.

Why CxSAST

Unlike other SAST solutions, CxSAST provides the ability to eliminate vulnerabilities early in the SDLC. Integrations with build tools, Continuous Integration servers, IDEs, bug tracking solutions, and other development tools allows CxSAST to adapt to your existing software development lifecycle.

Pinpoint Accuracy for Remediation
CxSAST understands your software and how data moves through an application. Its “Best Fix Location” algorithm automatically highlights the best place to remediate issues, allowing developers to fix multiple vulnerabilities at a single point in the code.

Find Vulnerabilities Sooner
Unlike some static analysis offerings CxSAST scans uncompiled code and doesn’t require a completed build. No dependency configurations – no learning curve when switching languages. It even works from the developers’ IDE. This allows organizations to use CxSAST earlier in the software development lifecycle, when it is far less expensive and time consuming to fix coding errors.

The Right Choice for Agile and CI Teams
In Continuous Integration and Agile environments, security must be integrated into the development process. Other static analysis solutions don’t fit well due to their lengthy scan times. Checkmarx CxSAST solves this by using **incremental scanning** to analyze only newly introduced or modified code, reducing scanning time by up to 80%, and integrates with CI Servers to automate security testing.

Integrates with Your Workflow

No two development environments are exactly the same, and testing solutions need to be flexible to accommodate how you work. Checkmarx CxSAST integrates with CI and build servers, bug tracking solutions, and source repositories.

Complete Understanding of Identified Vulnerabilities

With Checkmarx, you can view the reasoning and proof of all scan results to understand the root cause of the vulnerabilities. You aren't limited to the rules everyone else uses. Checkmarx Open Query language allows organizations to have complete control of the intellectual research behind CxSAST.

Supported Coding Languages

Java · JS · PL SQL · Visual Basic · JSP · Ruby · .NET Core · Microsoft ASP.net

TypeScript · Scala · C++ · php · Perl · Groovy · Windows Mobile

OBJECTIVE-C · Microsoft C#.net · Apex Develop. On-Demand · GO · python · VBSCRIPT · HTML 5 · Microsoft .net

Comply with Regulatory Standards

Regulatory standards such as PCI-DSS, HIPAA, FISMA, and others require organizations to test for common vulnerabilities like those found in the OWASP Top 10 and the SANS Top 25. CxSAST finds these and more. Plus, with unique open query language, you can easily create your own security policy consisting of the vulnerabilities most important to your industry and organization.

Supported Standards

OWASP TOP 10 2013 · OWASP MOBILE TOP 10 · SANS SANA 25 · HIPAA · CWE MITRE CWE · FISMA · PCI DSS Certified · MISRA · BSIMM

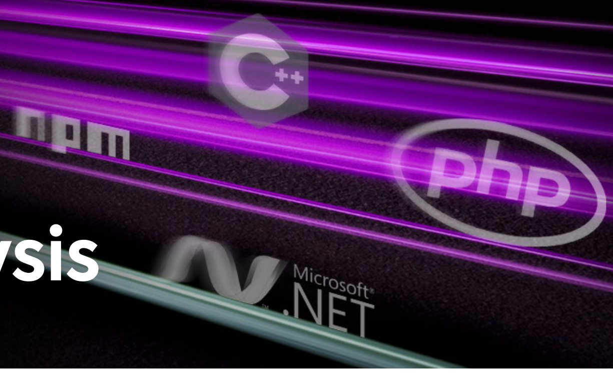
Flexible Deployment Options

CxSAST is available as a standalone product and can be effectively integrated into the Software Development Lifecycle (SDLC) to streamline detection and remediation. CxSAST can be deployed on-premise in a private data center or hosted via a public cloud.

About Checkmarx

Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com or follow us on Twitter: @checkmarx.

CHECKMARX



Open Source Analysis

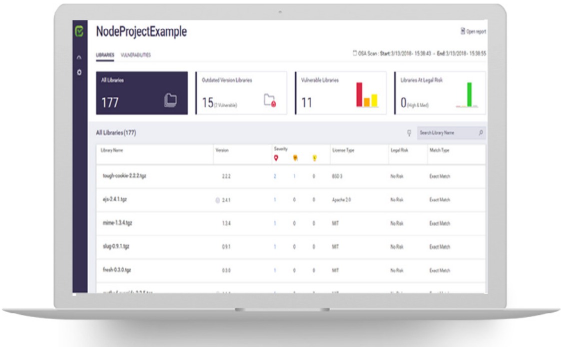
Take Control of your Open Source

Security vulnerabilities and the devastating effect they can have on your organization doesn't just impact in-house code, they also occur in open source components and libraries. Checkmarx Open Source Analysis (CxOSA) is an open source analysis solution that extends our CxSAST solution to detect, aggregate and manage open source components as part of the CI/CD toolchain.

CxOSA allows organizations to manage, control and prevent the security risks and legal implications introduced by open source components used as part of the software development process. Open source is free, it shortens time-to-market, and has a large development community to test and improve it. However, open source is like any other code - they have security vulnerabilities and bugs that can expose your organization to security risks. Therefore, security measures must be taken to continuously monitor and manage the use of open source components so you can remediate issues early in the development lifecycle.

Unique Solution Benefits

- **Continuously monitor open source code**
  Shift left, remediate earlier, lower costs
- **Integrates seamlessly into the full CxSAST solution**
  Single scanning of both open source and in-house code with easy management to a unified project view
- **Identifies open source vulnerabilities**
  Generate reports with mitigation advice via a unified reports dashboard
- **Easily define and enforce policies for organization compliance**
  Development organizations can set policies to suppress and enforce vulnerability libraries



NodeProjectExample

Open report

LIBRARIES VULNERABILITIES

OSA Scan : Start: 3/13/2018 - 15:38:43 → End: 3/13/2018 - 15:38:55

All Libraries 177

Outdated Version Libraries 15 (2 Vulnerable)

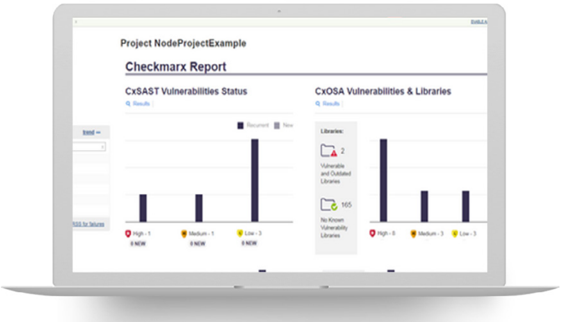
Vulnerable Libraries 11

Libraries At Legal Risk 0 (High & Med)

All Libraries (177)

Search Library Name

Library Name	Version	Severity			License Type	Legal Risk	Match Type
		🟥	🟧	🟨			
tough-cookie-2.2.2.tgz	2.2.2	2	1	0	BSD 3	No Risk	Exact Match
ejs-2.4.1.tgz	2.4.1	1	0	0	Apache 2.0	No Risk	Exact Match
mime-1.3.4.tgz	1.3.4	1	0	0	MIT	No Risk	Exact Match
slug-0.9.1.tgz	0.9.1	1	0	0	MIT	No Risk	Exact Match
fresh-0.3.0.tgz	0.3.0	1	0	0	MIT	No Risk	Exact Match



Project NodeProjectExample

Checkmarx Report

CxSAST Vulnerabilities Status

Results

CxOSA Vulnerabilities & Libraries

Results

Libraries:

2 Vulnerable and Outdated Libraries

165 No Known Vulnerability Libraries

Initiate and Automate

Initiate testing from a standard web browser or directly inside your build environment (such as Jenkins, Maven, TeamCity, Bamboo, MS-VSTS), and automatically run open source analysis scans with in-house code as part of the CI/CD toolchain. Results are aggregated and reports are generated for display in the web UI or build manager interface in a unified project view.

Manage Security Vulnerabilities

Detect vulnerable and outdated open source libraries to help you prioritize, manage and maintain your application's security posture. Leverage CxOSA to track thousands of common vulnerabilities exposures (CVE), security advisories, and bug trackers so that you will be up to date and receive remediation recommendations that need to be taken to ensure your applications remain secure. Furthermore, developers can also set policies to suppress vulnerability libraries and comply with organization policies.

Legal Compliance

Failure to comply with open source license requirements can also result in legal and business risks. CxOSA helps you ensure that you do not use components in a way that may risk your own intellectual property or impact the progress of your organization.

Vulnerability Management

CxOSA is aligned with CxSAST, allowing developers to manage in-house and open source vulnerabilities in the same manner. As both scans can be initiated together, both in-house and open source vulnerabilities can be managed together.

Policies Management

Set-up automated policies by defining your acceptance, rejection, and internal approval process protocols per open source license type, security vulnerability severity, software bug severity, library age and more. As soon as a developer attempts to add an open source component that is not acceptable according to your policies, you'll get an alert.

Optimize Open Source Selection

Open source selection is easy with the browser plugin. Developers can browse for open source components online and verify if they are appropriate from a security, quality, and license compliance perspective– even before they choose to start using it.

Language Coverage and Accuracy

CxOSA uses well-established vulnerability databases and supports all popular open source programing and scripting languages. The WhiteSource proprietary algorithm minimizes False Positives for faster remediation and reduced costs.

Supported Coding Languages

About Checkmarx

Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com or follow us on Twitter: @checkmarx.

CHECKMARX

CxIAST

Interactive Application Security Testing

Applications are the major attack vector when it comes to enterprise cyber-attacks. As awareness of the threat grows, more organizations realize that application security has many layers, including developer enablement, open-source assessment, static code analysis and dynamic (run-time testing) analysis.

CxIAST is an application security testing solution that detects vulnerabilities in running applications under test. By extending its portfolio into dynamic and continuous security testing, Checkmarx provides broader coverage, and improves time-to-market without compromising security.

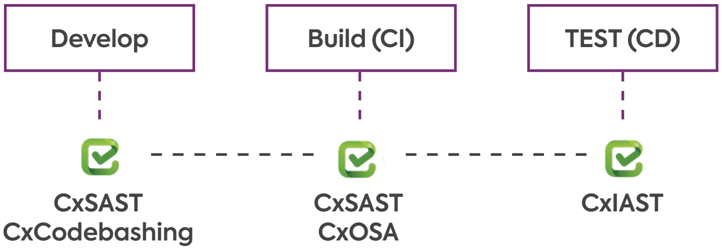
Security at the Speed of DevOps

CxIAST is purpose-built for DevOps and fits perfectly into your organization's CI/CD pipeline. It provides advanced vulnerability detection with zero impact on test cycle times, addressing the fast-paced software release timelines required today. An intelligent agent continuously monitors application behavior while CxIAST leverages existing functional testing tools to collect critical data points, and runs smart queries to detect security vulnerabilities. Resultant vulnerabilities are presented in an intuitive results dashboard to be assigned as security bugs and remediated.

- Global test automation market is being driven by rapid CI/CD adoption and estimated to be worth $85.8 billion by 2024 [1]
- Enterprise IAST adoption will have exceeded 30% by 2019 [2]

Complete Your AppSec Testing Portfolio

Legacy dynamic application security testing (DAST) solutions deploy as a Security Gate because long scan times delay production rollout. Now, with CxIAST continuous AppSec testing, delays are eliminated since vulnerabilities are detected in real-time. This fills a critical layer in your application security portfolio because certain vulnerabilities and flaws can only be detected on a running application. CxIAST is also simple to install, simple to operate and complements Checkmarx SAST, open source and developer enablement solutions.



Extends dynamic application security testing to multiple touch points across the SDLC

[1] TMR, March 2016

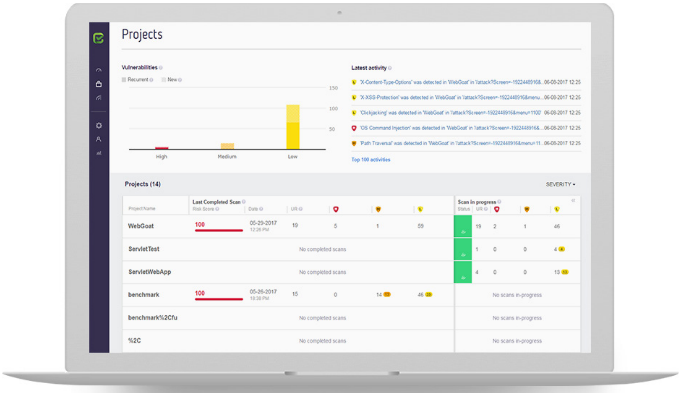
[2] Gartner Magic Quadrant, March 2017

How It Works

CxIAST has an agent that is customizable and instruments in-house functions unique to your organizational and compliance policies. The Checkmarx open query language allows you to modify existing security rules and even write your own. CxIAST identifies the full context for detecting vulnerabilities, and since data values pass through the running code, it can identify vulnerabilities quickly, accurately, and with minimum false positives.

CxIAST Key Benefits

- Improves time-to-market without compromising security
- Leverages dynamic application security testing for DevOps and CI/CD workflows
- Complements Checkmarx SAST, open source analysis, and developer enablement solutions
- Accurately monitors the behavior of applications and detects vulnerabilities in real-time, including OWASP Top Ten



Latest activity

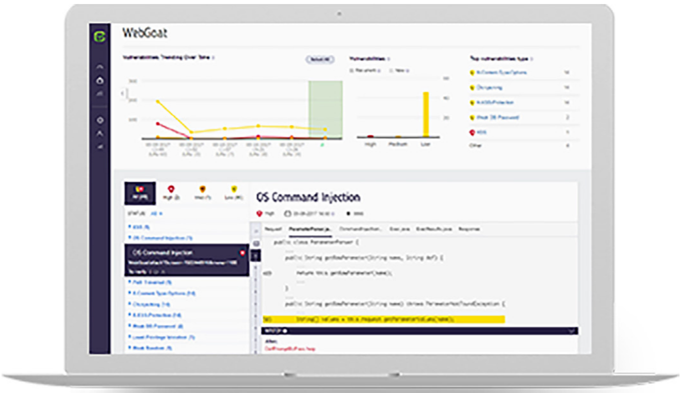
- 'X-Content-Type-Options' was detected in 'WebGoat' in '/attack?Screen=-19224489168... 06-08-2017 12:25
- 'X-XSS-Protection' was detected in 'WebGoat' in '/attack?Screen=-1922448916&menu... 06-08-2017 12:25
- 'Clickjacking' was detected in 'WebGoat' in '/attack?Screen=-1922448916&menu=1100' 06-08-2017 12:25
- 'OS Command Injection' was detected in 'WebGoat' in '/attack?Screen=-19224489168... 06-08-2017 12:25
- 'Path Traversal' was detected in 'WebGoat' in '/attack?Screen=-1922448916&menu=11... 06-08-2017 12:25

Top 100 activities

Projects (14) SEVERITY ▾

	Last Completed Scan						Scan in progress				
Project Name	Risk Score	Date	UR	H	M	L	Status	UR	H	M	L
WebGoat	100	05-29-2017 12:26 PM	19	5	1	59		19	2	1	46
ServletTest			No completed scans					1	0	0	4 4
ServletWebApp			No completed scans					4	0	0	13 13
benchmark	100	05-26-2017 18:38 PM	15	0	14 13	46 39		No scans in-progress			
benchmark%2Cfu			No completed scans					No scans in-progress			
%2C			No completed scans					No scans in-progress			

Monitored Projects View



Application Dashboard

Vulnerability Coverage

CxIAST detects both input related and application vulnerabilities, including the OWASP Top Ten and more.

- SQL Injection
- XSS Injection
- OS Command Injection
- Path Traversal
- XPath Injection
- Parameter Tampering
- Open Redirect
- Trust Boundary Violation
- Cross-Site Request Forgery
- Decentralized RCE Vulnerability
- And more...

About Checkmarx

Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com or follow us on Twitter: @checkmarx.

CHECKMARX

CxCodebashing
Game-Like AppSec Training

Best Innovation in
Mobile Development
DEVIES Awards
2018

CxCodebashing is an interactive AppSec training platform built by developers for developers. CxCodebashing sharpens the skills developers need to avoid security issues, fix vulnerabilities, and write secure code in the first place. With CxCodebashing, access to engaging secure coding training is one click away – for the entire development team.

To keep up with the relentless development pace, companies have to empower developers to take ownership of application security – and prioritize vulnerabilities like any other software defect. Developers need help learning and sharpening their application security skills, however, existing training solutions are ineffective and slow developers from accomplishing their main task – writing code. Even with periodic security training, it is usually boring and detached from the developer's normal work routine, so any knowledge gained fades quickly rendering the training experience ineffective.

Learn By Doing

CxCodebashing teaches developers the principals of common AppSec vulnerabilities and secure coding techniques. This helps them sharpen and maintain their application security skills in the most efficient way. CxCodebashing is unique because developers can access an entire library of high-quality, purpose built learning modules when it is needed most – when a vulnerability is detected and needs to be remediated. Once they have run through the quick to play hands-on training, they return directly to work equipped with the new or reinforced knowledge to resolve the problem.

What Makes CxCodebashing Different?

Innovation Cycle

User Focused

No Boring Videos

Microsoft

"Codebashing is a true innovator in the AppSec training space, we're excited to be on that journey with them. As a site-wide license customer, many 10's of 1000's of Microsoft Engineers have access to the Codebashing training platform."

fitbit

"We're seeing enthusiastic, viral adoption by new-found friends of the security team. Simultaneously awesome, useful and terrifying!"

Key Benefits

- **Game-like:** developers can "wear the hackers hat" as they work through a learning module and absorb the information as quickly as possible
- **Hands-on:** see all the moving parts of the application stack that are relevant to explaining the vulnerability
- **Interactive:** bring everything to life in an interactive and intuitive way
- **Fun:** developers can roll up their sleeves and play while learning
- **Enterprise ready:** drill-down dashboard analytics & built-in support for major SSO/SAML providers

How CxCodebashing Works

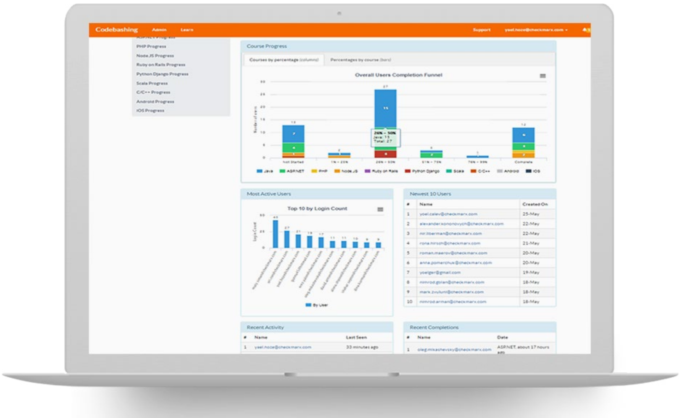
Each course catalog covers the top application security vulnerabilities specific to that programming language. Each module takes developers through a combined and engaging experience. As the developer interacts with the elements within each module, they receive insights on how secure development techniques are employed to defend against application exploits for the same, or similar vulnerability classes.

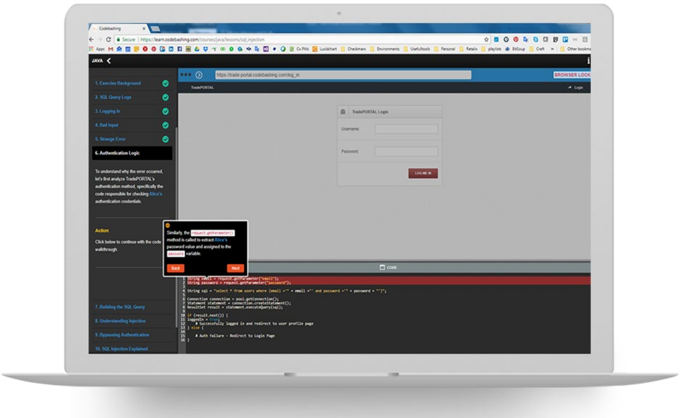
Engagement Features

- Share modules with other developers
- Create LinkedIn certificates for modules successfully completed
- Promote with training module notifications
- Reward with gamification badges and celebrate success

> "CxCodebashing has enabled Sky to roll out our secure coding training initiative to thousands of our developers across our engineering departments at a scale which would otherwise be impossible to manage with conventional approaches."

> "An innovative and scalable training solution, which has given our devs exposure to security vulnerabilities through the entire stack, all accessible using just a browser."


Dashboard Tracks Usage Statistics


Interactive Bite-Sized Code Walkthrough

Supported Coding Languages

About Checkmarx

Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com or follow us on Twitter: @checkmarx.

CHECKMARX

AppSec Accelerator™

Transform Your SDLC to a Secure SDLC

Development organizations are increasingly recognizing the benefits of implementing Application Security Testing early in the Software Development Lifecycle (SDLC). This ensures that software is secure and development remains agile. To achieve this, developers need to take ownership of application security. However, organizations frequently lack the internal resources and expertise to make this critical transition.

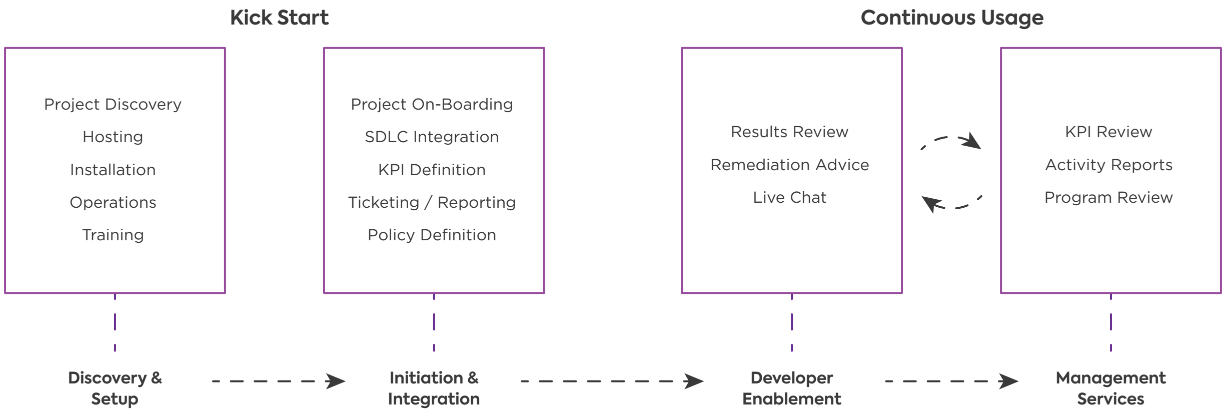
Streamline Your AppSec

With AppSec Accelerator, we help you streamline and automate your Application Security Testing and embed it into your development culture. Our team of Application Security Experts are on hand to ensure you succeed in your move to a secure SDLC.

Fast-Track Your AppSec Program

We provide the software, expertise, and assistance so you can focus on your business.

- A trusted partner to help organizations make the transition to a secure SDLC
- Leverage over ten years of experience
- to help developers deliver secure software faster
- Enables rapid ramp-up, setup, and deployment of your AppSec program
- Experts in over 20 coding and scripting languages and their frameworks
- Developer assistance on demand via live chat



What is a Secure SDLC?

A Secure Software Development Lifecycle (S-SDLC) is achieved by introducing application security processes, such as secure coding best practices, security testing, and remediation, throughout the SDLC.

AppSec Accelerator Offering

AppSec Accelerator includes comprehensive services to help you realize your secure SDLC transformation:

Discovery & Setup

- Identify application security requirements and timeline
- Assist with setting up security policies and compliance
- Define KPIs to understand program
- AWS Private Hosting - for other options, please contact your local sales representative
- Installation and service setup

Project Initiation & Integration Services

- Project onboarding with scan tuning to increase detection accuracy
- Integrate CxSAST into the developer's CI environment so that developers run scans and view results as an automated part of the development process
- Recommend and help integrate scan results into ticketing and reporting systems
- Assistance defining an operations dashboard so that results can be reported and KPIs measured

Developer Enablement Services

- On-demand developer access to Checkmarx experts
- Results reviews to explain detected vulnerabilities and how they impact the application
- Remediation guidance helps fix vulnerabilities earlier with faster rollout and reduced costs

Management Services

- Activity reports, monitor status of scans, and track open bugs
- KPI review provides analysis of key activity trends
- Program Review - takes a strategic look at the AppSec program's status, objectives, and KPIs
- On-going support for system operations and administration by monitoring, alerting, patching, updating, etc.

Optional Add-Ons

- CxOSA - an open source analysis solution to detect and manage security vulnerabilities in open source components and libraries
- CxCodebashing - an interactive, game-like AppSec training platform that teaches developers the principles of common AppSec vulnerabilities and secure coding techniques.

About Checkmarx

Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com or follow us on Twitter: @checkmarx.