Checkmarx

How to effectively manage the modern risks of open source code

When your devs use open source components and third-party libraries, you need to be able to find vulnerabilities and manage risk in an automated, repeatable, and consistent fashion. Yet traditional approaches to software composition analysis (SCA) are no longer working. Discover the how and why of effective implementation and use of next-gen SCA.

The Challenge

Security is one of the most significant challenges when using open source code. Vulnerable components are an open window to hackers who can easily exploit them, while operational and compliance risks also increase.

Take the initiative

It's time to lead the conversation and bridge the gap between development and security teams.

Understand what's being done to mitigate risks and if it's effective; scope the level of effort with current practices and identify inefficiencies; and evaluate the risk and opportunity cost in the absence or failure of these practices.

Three critical questions to ask yourself

1

Which open source libraries are used, and do they contain vulnerabilities?

- Generate a complete inventory of open source libraries and risks
- Track public common vulnerabilities and exposures (CVE) and those identified and curated by a dedicated security research team
- Accurately detect direct and transitive dependencies
- Track new vulnerabilities impacting previously scanned projects

Am I spending my time wisely on things that will have the biggest impact?

- Determine whether a vulnerability is in the application's execution path using other AST technologies (exploitable path)
- Identify how a vulnerable component has entered the application for effective remediation (dependency path)
- Prioritize remediation efforts by filtering out libraries that are used for development but not in production (dev dependencies)

2

3

How do I streamline open source risk assessment and remediation?

- Integrate into your CI/CD pipelines and the entire SDLC
- Facilitate information flow, deliver analysis results directly into build tools
- Automate ticket creation for accelerated remediation (such as Jira)
- Unify activities for both SCA and AST in use
- Initiate a scan and see results from one location within your build system

See exactly why the world's top organizations choose Checkmarx to make their software more secure

- **Trusted by 42 of Fortune 100**
- **Gartner MQ Leader in AST for 3rd consecutive year**
- **Forrester WAVE leader in SAST 2021**
- **In-house dedicated security research team**

Discover some of the high profile vulnerabilities that our globally recognized research team has identified

Checkmarx SCA (CxSCA) use cases and capabilities

Gain insight into your open source risk posture

- Accurate open source library detection
- Risk dashboard and detailed reporting across your organization
- New vulnerability alerting without the need to rescan
- Vulnerability trends over time (project level)
- Based on comprehensive database of both known CVE) vulnerabilities and unique (non-CVEs) ones

Efficiently triage scan results

Identify where the vulnerable library is coming from, and understand what component should be dealt with first: see a visualized presentation of the dependency structure, and where the vulnerability came into effect

Evaluate and address vulnerabilities

- Identify vulnerabilities from multiple sources and advisories (including CVEs and Checkmarx-exclusive vulnerabilities)
- Risk-rank vulnerabilities based on standardized severity metrics
- Take actionable remediation guidance from Checkmarx security researchers

Avoid and address license non-compliance

- Identify open source licenses associated with components in use
- Protect intellectual property and avoid litigation with detailed license risk metrics
- Support components with multiple licenses

Prioritize remediation efforts with exploitable path

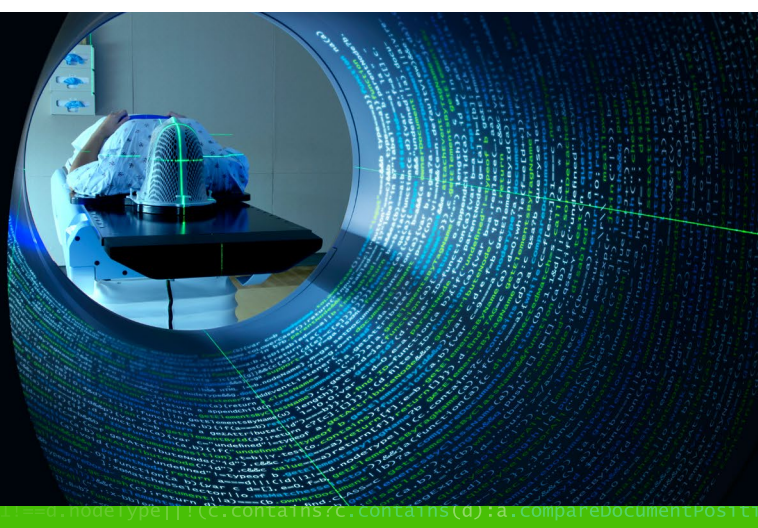
- Discover where open source is called within the developer's home-grown code
- This allows developers to recongize their high remediation priorities
- If something is not in the exploitable path, it is a lower priority

CxSCA supports a large number of language frameworks and package managers, and CI and build system integrations come out of the box.

How CxSCA works

CxSCA has an on-premises scan agent that scans your code base, and sends the results to the Checkmarx Cloud database.

Here, the scan results are matched to corresponding records in our database of libraries and vulnerabilities, and an analysis of the findings is displayed in the CxSCA web app (the user interface).



Get the complete picture: watch the video (17mins)

About Checkmarx

Checkmarx is the global leader in software security solutions for modern enterprise software development. Checkmarx delivers the industry's most comprehensive Software Security Platform that unifies with DevOps and provides static and interactive application security testing, software composition analysis, and developer AppSec awareness and training programs to reduce and remediate risk from software vulnerabilities. Checkmarx is trusted by more than 40 of the Fortune 100 companies and half of the Fortune 50, including leading organizations such as SAP, Samsung, and Salesforce.com. Learn more at www.checkmarx.com.

Checkmarx