CHECKMARX
choose what developers use

CASE STUDY:
GLOBAL AGILE ENTERPRISE SOFTWARE COMPANY REDUCES RISK AND IMPROVES DEVELOPER SECURITY KNOWLEDGE

OVERVIEW

INDUSTRY:

Enterprise Software

PROFILE:

An enterprise software organization which has designed, developed, and deployed thousands of business management applications for organizations in every vertical required a flexible, scalable SAST solution that could analyze source code for early detection of vulnerabilities.

The challenge for any enterprise software company is to build and deploy apps that will be used around the world for all kinds of needs. This organization in particular had an even bigger challenge - its' commitment to application security for the organization and its' customers.

SOLUTION:

Working with Checkmarx, the enterprise software company was able to greatly reduce their application portfolios attack surface and improve developer's secure coding standards by integrating security testing and remediation earlier into their software development lifecycle (SDLC), assisted by CxSAST's easy-to-use and customizable platform.

THE REQUIREMENTS

The enterprise software company has customers in verticals ranging from banking and government to technology, healthcare and manufacturing corporations, each with their own security requirements and regulatory compliances to maintain. The task was to find a security testing solution that would fit well with existing security and development processes and be both dependable and scalable within the company's agile environment.

As part of the company's application development offerings, customers are able to send the company a checklist of security items to cover in every project, and the company needed a highly powerful tool that would enable the company to check off every requirement, no matter the programming language or time constraints.

The company was already using a binary code analysis tool built in-house, but wanted to extend security analysis to uncompiled source code throughout the SDLC. As such, the company required a source code analysis solution which can cover a wide range of programming languages over multiple projects with quick turnaround times, while delivering consistently accurate results at the same time.

With a large, agile development force spread out among continents and building multiple solutions at any given time, the solution had to be developer-friendly and also generate high quality results and report data to the product owners and management. Buy-in from developers was crucial to the decision on a SAST solution, as was the ability to continuously monitor the overall security posture of their application portfolio in the company's internal dashboard.

In addition to having developers on board with the chosen SAST solution, it was also crucial that the tool helps teach developers best coding practices and allowed different teams to create different policies for source code analysis, depending on their skill levels and projects.

THE ALTERNATIVES

The company trialed other common static code analysis solutions at the same time as their CxSAST PoC. Previous SAST solutions offered unsatisfactory results, leading the company to choose Checkmarx.

THE SELECTION OF CHECKMARX

This organization decided on Checkmarx for several reasons.

Firstly, Checkmarx's Java language analysis proved to be superior to the other solutions the organization was looking at, which due to its significant use throughout the company was crucial to their final decision.

In addition, the company's developers were pleased with the ease of use and results, displayed in a manner that enhanced their knowledge and understanding of code security. Developers also found CxSAST's 'Best Fix Location' functionality a time-saver, helping them find the most efficient places in the code to fix numerous issues.

The company had requirements for adding in custom policy queries for each of their development teams, and CxSAST's ability to enable the organization to control detection and minimize false positives was another reason the company selected Checkmarx.

THE IMPLEMENTATION

CxSAST was quickly and easily implemented as a distributed environment. The solution is being used by multiple development teams across APAC, EMEA and North America, while the system is managed centrally.

Every six months, the company has a major release, while updates are continuously released in their agile development environment. Currently, each project scan is reviewed by the security teams before it is sent back to the relevant development team with the input.

Using Checkmarx has allowed the company to reduce resources spent on code review and pen-testing, as security issues are now handled at much earlier stages of the SDLC.

Part of CxSAST's implementation within the company including tweaking and additional customizations to reduce the false positive rate to a negligible number, which was performed by the company's security manager together with Checkmarx's professional service team, accomplished both locally and remotely.

BUSINESS BENEFITS OF CHECKMARX

With the implementation of CxSAST, this organization was able to:

- Scale their development efforts by performing security testing early in the SDLC, enabling developers to fix issues while they're still fresh in their minds and helping to improve secure coding.
- Streamline control over security analysis and remediation: Developers view results on their own platforms, while management views security analysis results in internal dashboards, eliminating the need for additional monitoring tools.
- Better align the applications they build to customer security requirements by adding custom queries and analysis of the most popular coding languages.

THE BOTTOM LINE

As CxSAST continues to be rolled out in the company's development teams around the world, satisfaction around the results continues to roll in. CxSAST's unique ability to quickly and efficiently scan any of the major programming languages and help developers locate the best place to fix security vulnerabilities has allowed the company to vastly improve its security processes and reduce both development time and business resources.

"Checkmarx helps us improve our application security significantly, while reducing the resources spent on code security analysis and providing a priceless education to our developers."

– The Organization's Corporate Security Officer