Case Study

Leading Software Development House Implements CxSAST

Overview

Country: Worldwide

Industry: Software Development and Content Management

Profile: The company's goal is to help innovators everywhere plan, build and launch great software. More than 18,000 large and small organizations, including some of the biggest in the world, use this company's issue tracking, collaboration and software development products to work smarter and deliver quality results on time.

The Selection of Checkmarx

The company conducted an extensive due diligence process over a period of several months with a number of SAST vendors. Checkmarx's solution was selected because it offered a good balance of functionality, and cost and the company demonstrated a readiness to respond to our various specific requests.

The Requirements

This established software company boasts a large and complex code base consisting of several millions lines of code across a few products. The code is mostly written in Java. The code includes many components, third party plugins, and so on. The company was searching for a cost effective solution that can provide configuration flexibility and is capable of running on Mac OS. Another important factor was the need to analyze incomplete code samples with missing dependencies which will significantly reduce the time and resources required to audit a code sample for vulnerabilities. Lastly, it was important to find a solution that is coupled with strong and dedicated support, to assist with the implementation and configuration process.

The Alternatives

Prior to selecting Checkmarx, the company tried most of the mature products or services in the marketplace.

Implementation of Checkmarx

When Checkmarx was implemented over two years ago, the product was not as mature as it is today and so they were prepared for the inevitable tweaks and bugs to get the product to work smoothly. A few hiccups inevitably occurred, which were promptly handled by Checkmarx support team. Overall, it did not take long for the product to be fully installed and productive. The company currently uses Checkmarx for assessing third-party plugins before bundling those with their own products and SaaS services. The main concern is that plugins run at the same level of privileges as the rest of the JVM, so security vulnerability in these third- party software components is equal in severity to any vulnerability in the host product.

Following a successful implementation of Checkmarx, the company gradually expanded the use case to assessing shared components used within the entire product range. Eventually, the aim is to scan the millions LoC across its entire code base on a regular basis. The company is considering integrating Checkmarx into the SDLC so that every programmer at within their development teams will be able to scan their code using Checkmarx's IDE plugins for visual studio / Eclipse and to promote a secure coding methodology across the entire company.

> “
> ***Using Checkmarx is easier than other tools. Important - you do not need to integrate it into your build process, just throw source code at it, assuming you have tuned the signatures to your taste.***
>
> - Information Security Expert
> within the company

The Bottom Line

The security team’s overall impression with Checkmarx is that it is a flexible and easyto-use product. The team was extremely happy with the levels of support they received as it was both professional and timely despite the time zones differences. As is always the case with similar tools, the company was prepared for a few quirks with installing and tuning it, however the Checkmarx installation was easy.

www.checkmarx.com