CHECKMARX

Case Study
Time Inc.

Time Inc.

Overview

HQ: New York City, NY, United States

Industry: Media

Profile: Founded in 1922, Time Inc., now part of Meredith Corporation, is an American worldwide mass media corporation based in New York City. Time Inc. owns and publishes 100+ magazines including some of the world's most recognizable brands, such as Time, Fortune, Food & Wine, InStyle, People, Entertainment Weekly, and more. On February 1, 2018, Meredith Corporation acquired Time Inc. for $2.8 billion.

The Objective

aws

Time Inc. is a mass media corporation that shares news and stories impacting global dialog across multiple media platforms for nearly a century. With some of the world's biggest media brands under the umbrella of Time Inc., the company knew it had to completely secure their applications from continuous security threats.

The task was to find an application security testing solution that would fit right in with the company's existing development processes, tools, and be both scalable and dependable within Time Inc.'s speedy agile environment. Time Inc. sought a static code analysis tool in a locked down and managed environment that was only accessible internally to the company's network infrastructure to properly ensure security for highly sensitive information that would be contained within the platform.

With a large, dynamic development force spread out among continents that is working to build multiple software applications at any given time, the ideal solution had to be developer-friendly, generate high quality results, and report data to team leaders and management. After a comprehensive search for the right solution, Checkmarx was deployed to:

- Streamline the company's application security program in its fastpaced DevOps environment
- Effectively enhance and secure the Software Development Lifecycle (SDLC) so that vulnerabilities are found and fixed early in the process
- Enable developers to implement static code analysis in their coding and QA process

The Solution

Checkmarx Static Application Security Testing (CxSAST) was quickly and easily implemented to Time Inc.'s incredibly dynamic development teams. The solution is being used by multiple developers across EMEA, APAC, and North America, while the system is managed centrally. From the start of Time Inc.'s deployment of Checkmarx, developers were pleased with the ease of use and with the results displayed in a manner that enhanced their knowledge and understanding of code security.

CxSAST is primarily used for projects hosted on GitHub and Jenkins. Whenever developers write new code and alter existing code, a scan is automatically triggered by Checkmarx's scan engine. Once the code has been scanned and vulnerabilities detected, scan results are presented to developers and security experts with information about the vulnerabilities, where they are located, and with instructions on how to remediate.

Time Inc. utilizes CxSAST's plugins for GitHub and Jenkins. Developers easily remediate vulnerabilities and enforce the company's strong stance towards application security while working within their own familiar development environments.

AWS Deployment of Checkmarx

CxSAST is hosted on an isolated AWS environment, connected to the company's development environment via secure VPN. Time Inc. configured an inbound connection from GitHub to the AWS deployment using AWS's flexible configuration tools. This architecture allows scans to be triggered from GitHub to the Checkmarx AWS private hosting instance using webhooks. This design met Time Inc.'s compliance requirements and helped achieve a robust DevSecOps deployment.

The Results

Using Checkmarx allows the company to reduce employee resources and time spent on code review. Security issues are now handled at much earlier stages of the SDLC. The company has implemented an automated, secure SDLC with widespread developer adoption and ongoing code remediation. Today, Time Inc. is able to preserve its agile development flow with automatic incremental scans via CxSAST. The company benefits from:

- CxSAST's integration to GitHub, through which it creates webhooks, automatically updates and rescans code, and comments on commits. This feature alone has proven to be a great timesaver for managers while helping to ensure developers produce secure code.
- Checkmarx's many integration points allows the customer to connect to a variety of DevOps platforms, such as Jenkins. Software engineering teams can spin up a new server, then seamlessly connect to the hosted CxSAST solution.
- CxSAST's unique visual interface provides developers with a clear overview of security vulnerabilities in their code, including a step-bystep walkthrough explanation of the root problem and the specific details of where and how to fix the vulnerable code.
- Checkmarx performs security testing early in the SDLC thus enabling developers to fix issues while they're still fresh in their minds, well before the application is put into production. This minimizes the cost and amount of time required to fix.
- Streamlined processes which dictate steps for ongoing secure code analysis and vulnerability remediation.

The Bottom Line

As CxSAST continues to be used by Time Inc.'s development teams worldwide and shows a high level of satisfaction and employee adoption. Checkmarx's ability to quickly scan every major programming languages provides the organization with a large return on their investment.

To learn more, please visit us at www.checkmarx.com