sonarsource

CASE STUDY

Global Technology Powerhouse Secures Manufacturing Execution Systems with SonarQube

With highly customized rules and integrations and a custom Quality Gate, developers use SonarQube daily to ensure clean and secure code in sensitive applications.

SUMMARY

+ Over 100 applications developed in C# .NET, JavaScript and C++
+ 600 developers using SonarQube for Code Quality & Code Security daily
+ Fully customized Azure DevOps dashboards using SonarQube's REST API
+ Integrated into developer workflow with Microsoft TFS and Microsoft Teams
+ 18 times faster with better results in direct SAST vendor comparison

"Security is part of our development process. In order to understand if you have a problem, you need to know the code and understand the risks. SonarQube helps us to find vulnerabilities and every morning SonarQube results are evaluated in our stand up meetings"

- Technical Team Lead

The Challenge

After a serious malware hit an industrial facility, one of the world's largest suppliers of power generation and transmission raised its game on security. Its division builds manufacturing execution systems (MES) that are connected to plants, controllers, and business applications with strategic customer information. To protect these, all vulnerabilities and defects must be fixed before a product can be released. But penetration tests and blackbox tools do not cover all parts of the code, and miss vulnerabilities. An in-house aggregator for open source code analysis tools was developed but quickly became too expensive to maintain and lacked language support, usability, and actionable results.

The Solution

During an internal audit, SonarQube was recommended for its speed and precision. Other established SAST products were evaluated but did not integrate well into the triaging workflow, didn't find enough issues, or were too slow. In direct comparison, SonarQube's static analysis took only 20 minutes, instead of many hours, and produced significantly better results out of the box. These were further optimized by using Quality Profiles. SonarQube's powerful REST API enabled the teams to tailor custom steps in Microsoft TFS, custom dashboards in Azure DevOps, and to send status messages in MS Teams.

The Results

After 4 years of using SonarQube, a shift of mind in the team is clearly visible. Security is driven by developers who know the code and understand the risks. Already 600 developers operating across three continents happily use SonarQube every day to review their pull requests, with more to join. In every morning's standup meeting, the teams discuss their Code Quality & Security score and how to improve. The build automatically breaks when the customized Quality Gate fails, so that severe code quality or security issues are detected before they can end up being exploited in production like in the past malicious computer worm attack.