

SonarQube 소개 및 Edition 별 기능 비교

이 문서는 SonarQube 제품의 개요를 공유하기 위해 작성되었다.

이 문서를 통해 SonarQube의 기본 기능 및 Edition 별 기능 차이점을 확인할 수 있다.

- [SonarQube 주요 기능](#)
- [SonarQube Edition](#)
- [SonarQube Edition의 주요 기능](#)
 - [SonarLint IDE 개발 도구 연동](#)
 - [브랜치 분석](#)
 - [Pull Request Decoration](#)
 - [Taint analysis](#)
 - [분석 언어](#)
 - [분석 보고서의 병렬 처리](#)
 - [멀티 DevOps 플랫폼 인스턴스](#)
 - [PR 데코레이션을 위한 Monorepo 지원](#)
 - [보안 엔진 커스텀 구성](#)
 - [보안 리포트](#)
 - [포트폴리오 관리 및 PDF 보고서](#)
 - [프로젝트 PDF 보고서](#)
 - [Audit trailing](#)
 - [프로젝트 이전](#)
 - [테스트 / 스테이지 라이선스](#)
 - [Enterprise버전에서 제공하는 보고서 샘플](#)
 - [프로젝트 보고서](#)
 - [포트폴리오 보고서](#)
- [G2 Crowd Grid for Static Code Analysis](#)
- [시스템 구성도](#)

SonarQube 주요 기능

SonarQube 지속적인 인스펙션을 통해 조직의 코드 품질 강화 및 보안 취약성 예방을 도와주는 솔루션이다.

다음은 SonarQube가 제공하는 주요 기능이다.

- Java, Javascript, C#, C/C++, Python 등 30개 이상 다중 언어 분석 지원
 - 다음 사이트에서 SonarQube에서 지원하는 Rule을 확인할 수 있다.
 - [SonarSource Code Analyzers Rules Explorer](#)
- 프로젝트 단위로 코드 분석 현황 정보 및 대시보드 제공
- 코드의 버그, 보안취약점, 코드중복, 단위테스트 커버리지, 사이즈 등 다양한 측정 정보 제공
- 특정 기간 동안 다양한 코드 측정(품질요소)에 대한 트렌드 제공
- 품질 요구사항 설정을 통한 코드 품질 측정
- Git 연동을 통한 브랜치 기반의 코드 분석 지원
- Eclipse, IntelliJ, Visual Studio 등 주요 개발 IDE와 연동 및 분석 결과 알림 지원
- Maven, Ant, Gradle, MSBuild, Makefile 등 빌드 통합 제공
- Jenkins, Bamboo, TeamCity 등 다양한 CI 엔진과의 통합 제공
- LDAP, Crowd 등 사용자 디렉토리 연동을 통한 계정 관리

SonarQube Edition

SonarQube의 Edition별 기능 및 차이점은 다음과 같다.

기능	Developer	Enterprise	Data Center
사용 범위	소규모 팀 단위에서 사용	전사 조직 단위에서 사용	고가용성을 원하는 조직에서 사용
SonarLint IDE 개발 도구 연동	✓	✓	✓
브랜치 분석	✓	✓	✓
Pull Request Decoration	✓	✓	✓
Taint analysis	✓	✓	✓
분석 언어	25개 언어	30개 언어	30개 언어
분석 보고서의 병렬 처리		✓	✓
여러 DevOps 플랫폼 인스턴스		✓	✓
PR 데코레이션을 위한 Monorepo 지원		✓	✓
보안 엔진 커스터마이징		✓	✓

보안 리포트		✓	✓
포트폴리오 관리 및 PDF 경영진 보고서		✓	✓
프로젝트 PDF 보고서		✓	✓
출시 상태 및 품질을 기록하는 규제 보고서		✓	✓
Audit trailing		✓	✓
프로젝트 이전		✓	✓
테스트 / 스테이지 라이선스		2개	3개
컴포넌트 무결성			✓
Data resiliency			✓
Horizontal scalability			✓

SonarQube Edition의 주요 기능

SonarLint IDE 개발 도구 연동

IDE에 SonarLint가 설치되어있고 SonarQube와 연동되어있으면 서버에서 분석된 결과를 IDE의 SonarLint를 통해 알림을 받을 수 있다.

브랜치 분석

Git Branch 기반으로 개발을 할 경우, SonarQube의 하나의 프로젝트에서 Branch를 모아서 분석 결과를 추적할 수 있다.

Branch는 개발 방식에 따라 Short-lived와 Long-lived 코드 브랜치가 존재할 수 있으며, 해당 브랜치에서 안정성이 보장된 코드만이 Master 브랜치로 병합할 수 있다.

The screenshot displays the SonarQube web interface for a project named 'Azure DevOps extension for SonarQube'. The top navigation bar includes links for Projects, Portfolios, Issues, Rules, Quality Profiles, Quality Gates, and More. A search bar and a 'Log in' button are also present. The main content area shows the 'Overview' tab selected, with a 'QUALITY GATE STATUS' section indicating 'Passed' (All conditions passed). Below this, a list of branches and pull requests is shown, all with a 'Passed' status. The right sidebar contains 'Project Information' and 'Download project PDF report' link. The bottom section displays various quality metrics: 2 Security Hotspots (33.3% Reviewed), 1d 5h Debt, 435 Code Smells, 48.7% Coverage on 687 Lines to cover, 0.0% Duplications on 2k Lines, and 0 Duplicated Blocks. The interface also shows 'Reliability' and 'Security' scores as 'A'.

Pull Request Decoration

SonarQube 다양한 형상 관리 도구(Bitbucket, GitLab, GitHub)와 연동하여 Pull Request 시, SonarQube 분석 결과를 해당 형상 관리 도구에 알려줄 수 있다.

Taint analysis

테인트 분석은 사용자 데이터 조각을 추적하여 어떤 작업을 수행하기 전에 삭제되었는지 확인함으로써 사용자 데이터를 보호할 수 있게 해주는 기능이다.

Java, C#, PHP, Python, JavaScript, TypeScript, C, C++ 언어에 대해서 지원하며, 아래는 OWASP 분석의 예시를 보여준다.

분석 언어

소나큐브는 30개 이상의 프로그램 언어를 지원한다. 다음 링크를 통해 전체 언어와 룰셋을 확인할 수 있다.

- <https://rules.sonarsource.com/>

분석 보고서의 병렬 처리

기본적으로 프로젝트 분석은 한번에 하나씩 처리된다. 이 기능은 Worker를 여러개 두고 한 프로젝트에서 다중으로 분석을 처리할 수 있게 해준다.

멀티 DevOps 플랫폼 인스턴스

Github, Gitlab, Bitbucket, Azure DevOps와 통합을 할 수 있게 해주는 기능이다. 개발 버전에서는 1개만, 엔터프라이즈 버전에서는 여러개의 DevOps 플랫폼과 연동을 할 수 있게 해준다.

PR 데코레이션을 위한 Monorepo 지원

Github, Gitlab, Bitbucket, Azure DevOps 플랫폼의 Monorepo도 Pull Request 데코레이션을 지원합니다.

보안 엔진 커스텀 구성

특정 룰에 대한 보안 룰들을 커스텀 구성할 수 있게 해주는 기능이다. SQL Injection, XSS, Open Redirect, Code Injection 등 룰에서 sources, sanitizers, passthroughs, sinks 를 추가할 수 있게 해준다.

보안 리포트

보안 리포트는 소나큐브, PCI DSS, OWASP ASVS, OWASP Top10, CWE Top 25를 기준으로 소스코드에 보안 보고서를 보여준다. 다음은 보안 리포트의 예시 화면이다.

sonarqube
Projects
Portfolios
Issues
Rules
Quality Profiles
Quality Gates
More
?
Search for projects...
Log in

Azure DevOps extension for SonarQube
master
Last analysis of this Branch had 1 warning
February 8, 2023 at 5:27 PM
Version 5.11.1

Overview
Issues
Security Hotspots
Security Reports
Measures
Code
Activity
Project Information

Security Reports
Track the Vulnerabilities and Security Hotspots in your Project.
Download as PDF

SonarSource
PCI DSS
OWASP ASVS
OWASP Top 10
CWE Top 25
SANS Top 25

Vulnerabilities and Security Hotspots conforming to the OWASP Top 10 report.
Learn More

☐ Show CWE distribution

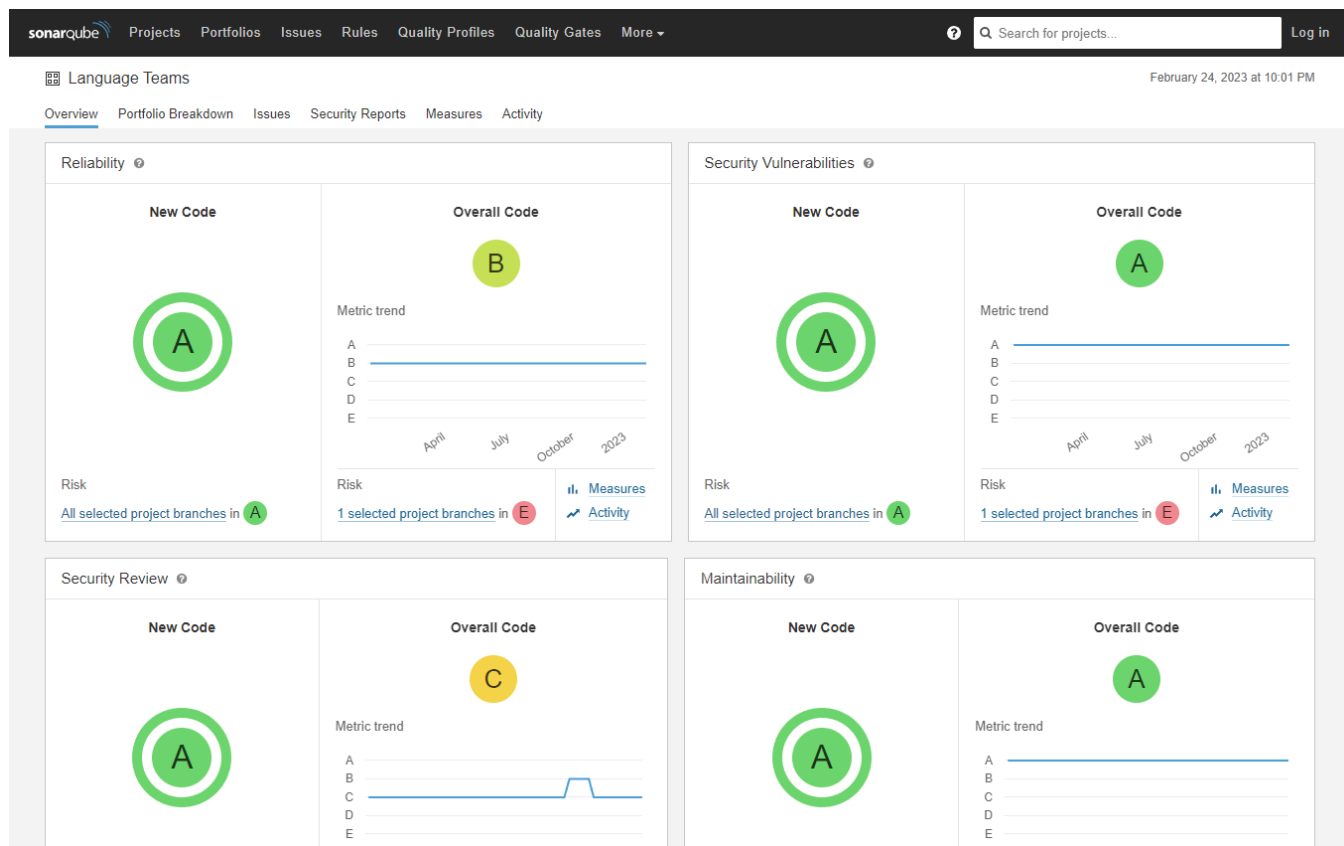
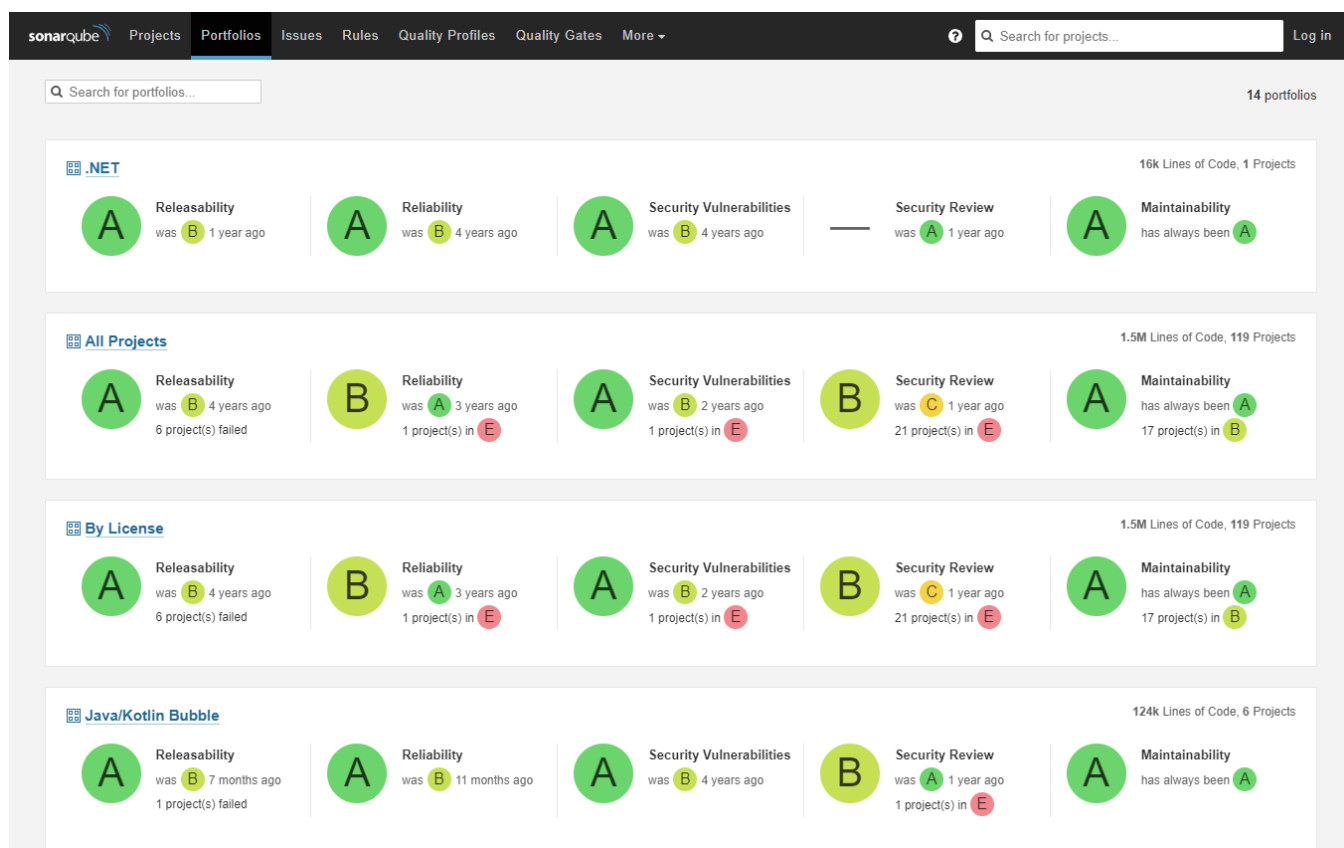
OWASP Top 10 - 2021

Categories	Security Vulnerabilities	Security Hotspots
A1 - Broken Access Control	0 A	2 E
A2 - Cryptographic Failures	0 A	0 A
A3 - Injection	0 A	1 E
A4 - Insecure Design	0 A	2 E
A5 - Security Misconfiguration	0 A	0 A
A6 - Vulnerable and Outdated Components	-	-
A7 - Identification and Authentication Failures	0 A	0 A
A8 - Software and Data Integrity Failures	0 A	0 A
A9 - Security Logging and Monitoring Failures	0 A	0 A

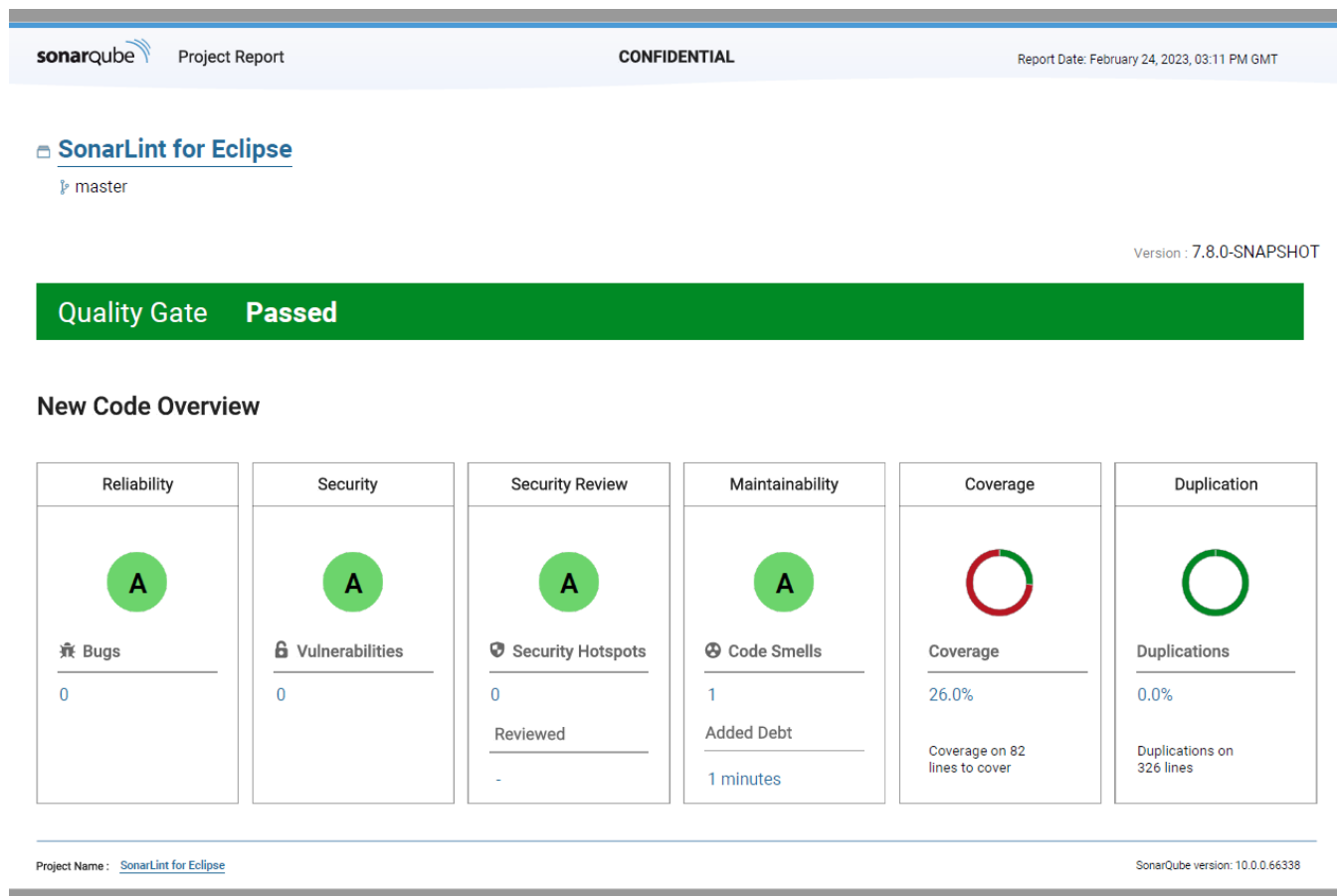
포트폴리오 관리 및 PDF 보고서

포트폴리오는 SonarQube에서 분석된 여러 프로젝트(저장소)를 묶어서 집계된 결과를 확인할 수 있게 구성할 수 있다.

기본 프로젝트의 Reliability, Security, Maintainability와 함께 품질 게이트를 실패한 비율을 Releaseability로 표시합니다. 이를 통해 해당 제품(서비스)를 릴리즈할지 결정할 수 있다.



프로젝트 보고서는 현재 프로젝트의 상태를 PDF로 다운로드 받을 수 있는 기능이다. 다음은 프로젝트 보고서의 예시를 보여준다.



Audit trailing

관리자 영역의 사용자 계정, 권한, 보안 설정, 프로젝트 생성, 삭제, 업데이트, 플러그인 설치 및 업데이트 등 변경 사항에 대한 감사 로그를 제공한다.

감사로그는 관리자 > Audit logs 에서 확인할 수 있다.

프로젝트 이전

프로젝트를 하나의 인스턴스에서 다른 인스턴스로 이전하는 기능이다. 이 기능을 통해 커뮤니티 버전의 프로젝트를 엔터프라이즈 버전의 SonarQube로 쉽게 이전할 수 있다.

테스트 / 스테이지 라이선스

엔터프라이즈 버전의 경우, 2개의 라이선스를 데이터 센터 버전의 경우 3개의 테스트 및 스테이지 라이선스를 제공한다.

Enterprise버전에서 제공하는 보고서 샘플

프로젝트 보고서



Project.pdf

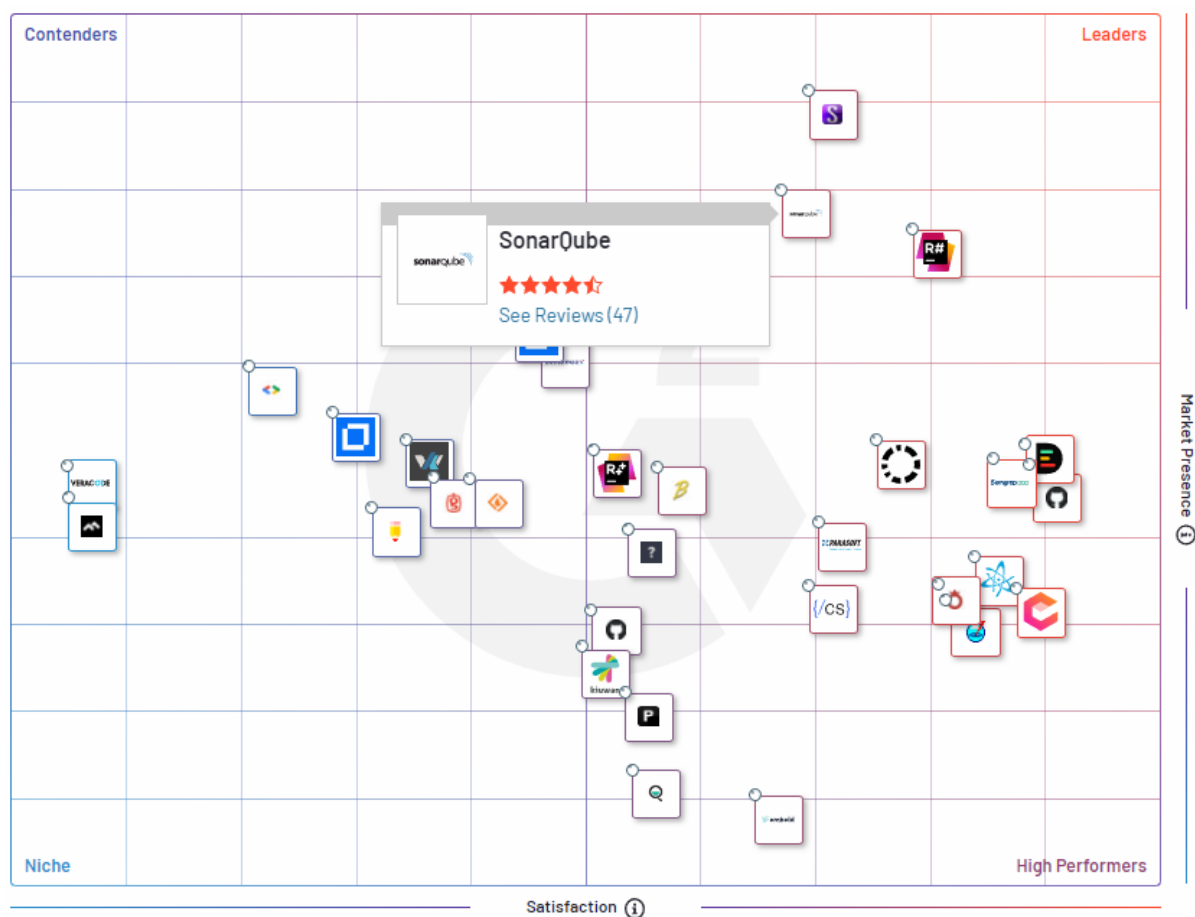
포트폴리오 보고서



Portfolio.pdf

G2 Crowd Grid for Static Code Analysis

SonarQube도 이제는 글로벌 2등으로 빠르게 성장하고 있다.



시스템 구성도

소나큐브는 복수의 sonar-scanner/lint (IDE plugin) + SonarQube 서버로 구성된다.

- Sonar-scanner: 컴파일이 필요한 소스코드 유형은 빌드 시점에서 빌드 로그와 빌드 산출물 정보 수집
- SonarLint: SonarQube 서버와 연동하여 IDE (Eclipse, MSDEV, ...)에서 interactive하게 정적분석 결과 확인
- SonarQube: Sonar-scanner에서 업로드한 소스코드 정보 분석 및 결과 제공

