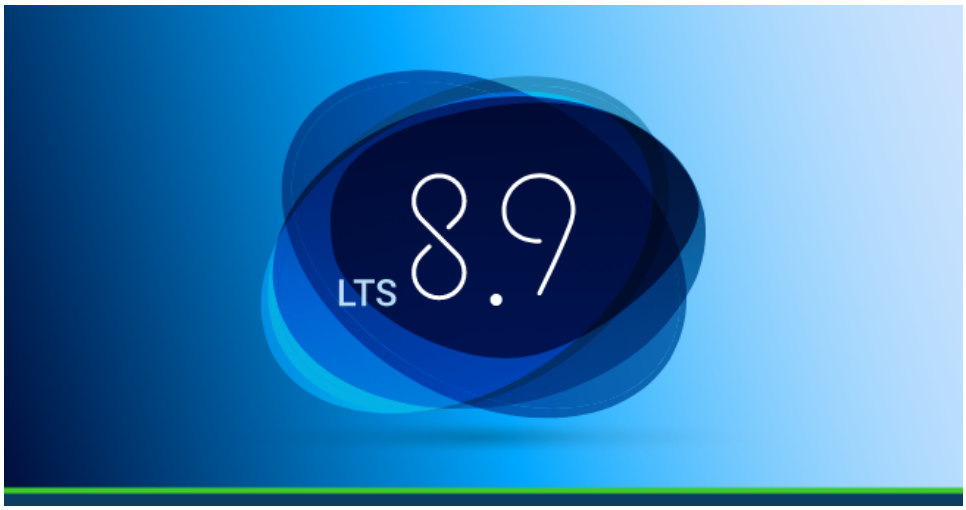
SonarQube 8.9 LTS

이 문서는 2021년 5월 4일 출시된 SonarQube 8.9 LTS 릴리즈 노트를 공유하기 위해 작성 되었다.

https://www.sonarqube.org/sonarqube-8-9-lts/



개발자의 Code Secutiry에 대한 책임의식

개발자는 더 많은 언어와 룰, 더 나은 탐지 및 향상된 워크플로우를 위하여 정적 애플리케이션 보안 테스트(SAST)로 Code Security를 제어합니다.

비교 불가한 SAST 정밀도- JavaScript 등을 포함

Security Vulnerability (보안 취약성) 탐지는 새로운 언어, 새로운 규칙 및 향상된 탐지 엔진으로 크게 확대되어 Java, C #, PHP, Python, JavaScript, TypeScript, C 및 C ++의 보안 분석에서 탁월한 정밀도와 성능을 제공합니다.
크게 확대된 분석 범위 및 깊이 외에도 이러한 결과들에 대한 개발자 액세스도 확대했습니다. 문제는 IDE, SonarLint, SonarQube 자체 및 Commercial 버전의 PR 데코레이션에서 발생합니다.

개선 사항 중 :

- Python, JavaScript, TypeScript, C 및 C++에 대한 SAST 분석 추가
- Java 및 C #에 대한 전체 OWASP Top 10 커버리지와 다른 언어에 대한 상당한 커버리지 포함
- C 및 C++ 용 POSIX 함수에서 버퍼 오버 플로우 감지

Commercial 버전은 연결 모드에서 이러한 오염 분석 문제를 SonarLint에 동기화 할 수있는 기능과 함께
삽입 취약점, 액세스 제어 중단, XSS 및 안전하지 않은 역직렬화를 찾기위한 오염 분석 룰이 추가되었습니다.

개발자가 안전한 코드를 작성하도록 Security Hotspot(보안 핫스팟) 검토

보안상 중요한 코드에 주의를 기울이고 잠재적 영향을 진단할 수 있는 도구를 사용하여 보안 핫스팟은 개발자가 보다 안전한 코드를 작성할 수 있도록 도와줍니다.
보안 핫스팟 언어의 범위를 TypeScript, C 및 C++로 확장했습니다. 이제 보안 핫스팟을 검색할 수 있는 인터페이스를 갖추게 되었습니다. 한 번의 클릭으로 SonarLint를 통해 IDE에서 열 수 있습니다.

보고 및 구성으로 명확성과 정확성 향상 EE DCE

보안 보고에는 상위 보고서의 PDF 다운로드와 함께 CWE Top 25 2019 및 CWE Top 25 2020이 모두 포함됩니다.
또한 자체 개발 프레임 워크를 사용하는 경우, 오염 분석 구성은 높은 정확도를 위하여 코드 보안을 올릴 수있는 UI를 제공합니다.

더 보기→

Cloud? On-prem? 여러분의 플랫폼을 보장합니다.

코드가 Cloud에 있든 On-prem, Saas 또는 자체 관리에 있든지, 코드 리포지토리 플랫폼 통합은 더 빠르고 더 나은 코드를 작성할 수 있게 도와줍니다.
초기 프로젝트 가져오기부터 실패한 Quality Gate에 대한 파이프라인 실패까지 거의 다 보장합니다.

간소화된 프로젝트 설정

간소화된 프로젝트 설정은 코드 리포지토리가 어떤 플랫폼이든지(GitHub, GitLab, Azure DevOps 및 Bitbucket; on-prem 및 cloud)
프로젝트를 가져오기 위한 쉬운 인터페이스를 제공합니다.

일단 프로젝트를 가져오면, NET, C, C ++ 및 Objective-C 프로젝트에 대한 언어 별 튜토리얼과 함께
GitHub Actions, Jenkins, GitLab CI, 또는 Azure DevOps Pipelines에서 분석을 설정하는 튜토리얼이 안내됩니다.

이제부터 사용하는 CI에 상관없이 실패 분석에 대한 파이프라인을 실패할 수 있습니다.

스테로이드에 대한 PR 분석 DE EE DCE

코드 리포지토리 플랫폼 통합은 온보딩에서 멈추지 않고 온프레미스 및 클라우드 모두에서 GitHub, Bitbucket, Azure DevOps 및 GitLab에 대한 PR 데코레이션을 지원합니다.
Enterprise Edition은 단일 보고서에 PR 데코레이션을 추가합니다.

뿐만 아니라 Developer Edition은 대부분의 워크플로우(Jenkins, GitHub Actions, Gitlab CI, Azure Pipeline 및 Bitbucket Pipeline)에 대한 자동 브랜치 및 PR 환경 구성도 제공합니다.

더 보기→

보다 쉬워진 SonarQube

SonarQube를 보다 쉽고 안전하게 사용할 수 있습니다. SonarQube는 Docker Hub 및 DoD의 Iron Bank에서 에디션 별 Docker 이미지를 사용하여
미국 국방부 표준 (예 : STIG 강화)에 따라 보안이 강화되었습니다. 여기에 Kubernetes 지원을 위한 Helm 차트가 추가되어 SonarQube를 보다 쉽게 배포할 수 있습니다.

핫 데이터베이스 백업을 지원하므로 일상적인 유지 보수도 더 간편합니다. 업그레이드 중에 점진적 가용성으로 업그레이드가 쉬워졌습니다.
이제 SonarQube는 재인덱싱이 완료되기도 전에 분석 및 제한된 탐색이 가능합니다.

더 보기→

SonarQube와 함께 Python 개발에 온보딩할 시간

SonarQube는 파이썬을 위한 동급 최고의 정적 코드 분석을 제공하기 위해 필요한 모든 작업을 수행합니다.

이번 LTS는 개발자들이 기대하는 까다로운 버그 및 취약성을 포착하기 위해 심층 분석을 추가합니다.
파이썬은 모든 언어 구조, 프레임 워크 및 유형을 통해 문제를 올바르게 추적하기 위하여 최대 3.9 버전의 언어를 지원합니다.
또한 다른 도구에서 전환하는 팀의 경우 Pylint 및 Flake8 보고서를 쉽게 가져올 수 있으며 사용자 지정 규칙을 작성할 수 있습니다.

그리고 무엇보다 주입 결함과 같은 오염 분석 취약성을 탐지하기위한 오염 분석 규칙이 Commercial Edition에서 지원됩니다.

더 보기→

개발자가 원하는 규칙&성능을 제공하는 C++

C++ Core Guidelines의 포괄적인 범위와 C++ 17 특정 규칙들의 집합을 통해 다음과 같은 최신 모범 사례를 쉽게 확인할 수 있습니다.
여러 표준 버전을 사용하는 경우 품질 프로파일을 쉽게 관리할 수 있습니다. 사용하는 모든 버전에 대한 규칙을 활성화하면 프로젝트가 컴파일하는 표준 버전을 기준으로 해당 규칙을 활성화합니다.
더불어 분석 성능을 몇 가지 개선하고 추가 컴파일러에 대한 다양한 지원을 추가했습니다.

이는 POSIX 함수에서 버퍼 오버플로 탐지를 포함한 보안 중심 규칙의 주요 확장 외에 추가입니다.

마지막으로 Community Edition 사용자는 새로 도입된 CLion 용 SonarLint와 VisualStudio 용 SonarLint에서 C++ 분석을 무료로 사용할 수 있습니다.

더 보기→

Clean as You Code, 모범 사례가 앞으로 이동

첫번째로 재작성된 프로젝트 홈페이지를 찾을 수 있습니다. 새로운 인터페이스는 새로운 코드의 품질과 보안을 전면과 중앙에 배치하여 Clean as You Code 에 더욱 집중할 수 있도록 도와줍니다.
둘째, 테스트를 올바르게 작성할 수 있도록 Java, PHP 및 C#에 규칙을 추가했습니다.
마지막으로, 모든 Commercial 버전에서 애플리케이션을 사용할 수 있도록하여 더 많은 팀들이 하나의 집계된 통합 프로젝트에서 함께 프로젝트의 품질을 검토할 수 있도록 했습니다

가장 안전한 LTS!

코드의 보안뿐만아니라 SonarQube의 전반적인 환경에 대한 보안에도 주의하고있습니다.

- SonarQube 자체와 내부 빌드 파이프라인에 추가 강화를 적용
- SonarSource에서 제공하는 라이브러리로만 SonarQube의 라이브러리 로딩을 제한
- API를 통해서 사용이 가능하도록 핵심 기능에 대한 플러그인 액세스를 제한
- 플러그인 Marketplace에 부가적인 제어 기능 추가

SonarQube 관리자에게 기본 관리자 자격 증명을 변경하도록 강제하는 등 간단하지만 효과적인 새 보호 조치를 찾을 수 있습니다.

SonarQube 8.9 LTS 다운 및 업그레이드 가이드

- SonarQube 다운 받기
- SonarQube 업그레이드 가이드