sonarqube

SonarQube security capabilities

While you may already be familiar with SonarQube's robust code quality features, you might not know about its extensive security capabilities, all included with your license. SonarQube's Enterprise Edition empowers development teams with advanced security features to ensure your code is robust, secure, and compliant with industry standards. Below is a detailed overview of the security capabilities included:

feature	description	benefits
Static Application Security Testing (SAST)	Automated analysis to detect security vulnerabilities and coding flaws within the codebase.	Identify and fix vulnerabilities accurately and early, ensuring safer code deployment.
Security Hotspot Detection	Highlights sections of code that might be risky but need manual review to confirm.	Allows developers to focus on potentially vulnerable areas without overwhelming them with false positives.
deeper SAST	Detection of deeply hidden complex security vulnerabilities that occur due to the interaction of first-party code with open-source libraries (3rd-party code).	Provides in-depth security analysis and uncovers deeply hidden issues that arise from interaction with 3rd-party libraries/ code.
Security Engine Custom Configuration	Allows customization of security rules and configurations to fit specific needs.	Tailors the security analysis to the unique requirements of your project.
Secrets Detection	Accurately identifies hard-coded secrets, such as passwords and API keys, in the code.	Prevents accidental exposure of sensitive information, protecting you from security vulnerabilities.
Advanced Secrets Detection	Allows customization of secret detection rules to fit specific needs. Together with SonarLint, it prevents secrets from leaking and becoming a serious security breach.	Ensures the detection of unique or organization-specific secrets to reduce the risk of breaches.
Quality Gates that enforce code security and quality	Define and enforce security thresholds as part of your CI/CD pipeline.	Ensures only secure and quality code gets deployed to production.
Detailed Security Reports	Dedicated reports track the application's code security against standards such as OWASP Top 10, OWASP ASVS, CWE Top 25 (2021, 2020, and 2019), and PCI DSS.	Comprehensive compliance reports on security issues and remediation steps. Help teams understand and address security concerns effectively.